Коди та автомати: основи алгебраїчної теорії

Олег Гутік

7 листопада 2021 р.

Зміст

Передмова

Розділ 1

Попередні відомості

У цьому розділі ми вводино основні поняття та доводимо багато результатів, які будуть необхідні для викладення матеріалу даного курсу. Цей розділ не призначений для систематичного читання, а лише для посилань.

Перші три підрозділи містять позначення та основні поняття та терміни. Кожен з наступних підрозділів – це вступ до теми, яка не повністю розглядається в цій книзі. Ці підрозділи стосуються головним чином теорії автоматів. Ми формулюємо теорему Кліні і показуємо, як побудувати мінімальний автомат з даного автомата. Визначено синтаксичні моноіди. Ці поняття та результати будуть обговорюватися в іншому контексті в розділі 9. Ми вводимо формальні степеневі ряди та вагові автомати. Отримано деякі основні властивості та доведено частини теореми Перрона-Фробеніуса.

1.1 Поняття

Надалі через

$$\mathbb{N}, \quad \mathbb{Z}, \quad \mathbb{Q}, \quad \mathbb{R} \quad \text{і} \quad \mathbb{C}$$

ми позначатимемо множини натуральних, цілих, раціональних, дійсних і комплексних чисел, відповідно. Надалі вважатимемо, що 0 – натуральне число, тобто $0 \in \mathbb{N}$. Покладемо

$$\mathbb{R}_+ = \{x \in \mathbb{R} \colon x \geqslant 0\}.$$

Надалі в тексті курсу лекцій, через

$$\binom{m}{n} = \frac{n!}{m!(n-m)!}$$

позначатимемо біноміальний коефіцієнт натуральних чисел n і m, де $n \geqslant m$.

Для довільних дійсних чисел x і y позначимо

$$[x, y) = \{z \in \mathbb{R} \colon x \leqslant z < y\}.$$

Надалі вважатимемо, що множина $[x, x)$ є порожньою для довільного дійсного числа x.

Для довільних двох підмножин X і Y множини Z позначимо

$$X \setminus Y = \{x \in Z \colon x \in X, x \notin Y\}.$$

Також часто, через $\overline{X}$ позначатимемо доповнення до підмножини X в множині Z. *Елемент* x та *одноелементну множину* $\{x\}$ ми, як правило, не будемо розрізняти. *Множину всіх підмножини множини* X позначатимемо через

$$\mathfrak{P}(X).$$

Зазвичай символ відображення ми записуватимемо ліворуч від аргумента

$$f(x),$$

але з деякими вийнятками: коли ми розглядаємо композицію дій на множині, дія записується праворуч від аргумента. Зокрема, символ підстановки ми записуватимемо праворуч від аргумента:

$$(x)\sigma.$$

Розбиттям непорожньої множини X називається сім'я

$$\{X_i \colon i \in \mathscr{I}\}$$

непорожніх підмножин множини X така, що

$$X = \bigcup_{i\in\mathscr{I}} X_i \qquad \text{та} \qquad X_i \cap X_j = \varnothing$$

для різних $i, j \in \mathscr{I}$. Зазвичай, ми визначатимемо розбиття так:

$$\text{“Нехай } X = \bigcup_{i\in\mathscr{I}} X_i \text{ — розбиття множини } X\text{.”}$$

Потужність множини X позначатимемо через $\mathrm{Card}(X)$.

1.2 Моноїди

Напівгрупою називається множина із заданою на ній бінарною асоціативною операцією. Зазвичай ця операція називається множенням, або просто напівгруповою операцією, і вважається мультиплікативною. Добуток двох елементів a та b напівгрупи S записуватимемо так:

$$a \cdot b.$$

Також часто, для спрощення викладу ми опускатимемо символ множення, якщо зрозуміло, яка напівгрупова операція визначена: писатимемо ab замість $a \cdot b$.

Елемент a напівгрупи S називається *одиницею* або *нейтральним елементом* в S, якщо

$$az = za = z$$

для довільного елемента $z \in S$. Надалі одиницю напівгрупи S позначатимемо через 1_S, або просто через 1 у випадку коли відомо про яку напівгрупу йде мова. Очевидно, якщо напівгрупа S містить одиницю то ця одиниця єдина. Напівгрупа, яка містить одиницю, називається *моноїдом*.

Для довільної напівгрупи S на множині $\mathfrak{P}(S)$ можна ввести наступним чином напівгрупову операцію:

$$XY = \{xy \colon x \in X, y \in Y\}, \qquad X, Y \subseteq S.$$

Очевидно, якщо напівгрупа S містить одиницю 1_S, то $\{1_S\}$ – одиниця в $\mathfrak{P}(S)$ з вище визначеною напівгруповою операцією, а отже у цьому випадку $\mathfrak{P}(S)$ є моноїдом.

Піднапівгрупою напівгрупи S називається непорожня підмножина A в S, яка замкнена стосовно множення, тобто $AA \subseteq A$. У цьому випадку мт також будемо говорити, що S індукує на множині A напівгрупову операцію. Піднапівгрупа A моноїда M з одиницею 1_M називається *підмоноїдом* в M, якщо $1_M \in A$. Очевидно, що піднапівгрупа з власною одиницею (тобто моноїд) моноїда не обов'язково є підмоноїдом. Для цього достатньо розглянути відрізок $[0, 1]$ з напівгруповою операцією

$$xy = \min\{x, y\}, \qquad \text{для} \quad x, y \in [0, 1],$$

для якого кожен відрізок $[0, a]$, де $0 < a < 1$, з індукованою з $([0, 1], \min)$ напівгруповою операцією є моноїдом, який не є підмоноїдом в $([0, 1], \min)$.

Морфізмом (*гомоморфізмом*) напівгруп S і T називається таке відображення $\varphi \colon S \to T$, що

$$\varphi(st) = \varphi(s)\varphi(t),$$

для всіх $s, t \in S$, а якщо крім того S і T — моноїди та $\varphi(1_S) = 1_T$, то відображення $\varphi \colon S \to T$ називається *морфізмом* (*гомоморфізмом*) моноїдів S і T.

Конгруенцією на напівгрупі S називається відношення еквівалентності θ[1] таке, що

$$s \equiv t \mod \theta \qquad \Longleftrightarrow \qquad usv \equiv utv \mod \theta, \quad \text{для всіх } u, v \in S.$$

Нехай $\varphi \colon S \to T$ — морфізм напівгруп. Тоді відношення θ на напівгрупі S, означене

$$s \equiv t \mod \theta \qquad \Longleftrightarrow \qquad \varphi(s) = \varphi(t), \qquad s, t \in S,$$

[1] У теорії напівгруп відношення $s \equiv t \mod \theta$ традиційно записують у вигляді $(s, t) \in \theta$, або $s\theta t$.

є конгруенцією на S. У цьому випадку конгруенція θ на S називається *ядром* гомоморфізма $\varphi\colon S \to T$. Навпаки, якщо θ — конгруенція на напівгрупі S, то на фактормножині S/θ класів еквівалентності за відношенням θ визначена напівгрупова операція та природне (канонічне) відображення $\pi\colon S \to S/\theta$ є морфізмом напівгруп, а у випадку, коли S — моноїд, то канонічне відображення $\pi\colon S \to S/\theta$ є морфізмом моноїдів.

Елемент s напівгрупи S називається *ідемпотентом*,[2] якщо $ee = e$. Якщо напівгрупа S мітить ідемпотент e, то eSe є моноїдом, який є піднапівгрупою в S. Легко бачити, що eSe є найбільшим моноїдом, який міститься в S і e є його одиницею, і в цьому випадку ми будемо називати eSe *моноїдом локалізованим* в ідемпотенті e.

Елемент 0 напівгрупи S називається *нулем*, якщо

$$0s = s0 = 0$$

для довільного елемента $s \in S$. Очевидно, якщо напівгрупа S містить нуль, то він єдиний. Аналогічно, як і у випадку одиниці нуль напівгрупи S будемо позначати через 0 або 0_S.

Нехай M — моноїд. Множина усіх оборотних зліва та справа елементів моноїда M є групою, яка називається *групою одиниць* моноїда M.

Циклічна напівгрупа (*циклічний моноїд*) — це напівгрупа (моноїд) M, яка породжена одним елементом (містить породжуючий елемент), тобто

$$M = \{a^n\colon n \in \mathbb{N}\}$$

(з $a^0 = 1_M$) для деякого елемента $a \in M$. Циклічний нескінченний моноїд ізоморфний адитивній напівгрупі невід'ємних цілих чисел, а нескінченна циклічна напівгрупа, що не є моноїдом, ізоморфна[3] адитивній напівгрупі натуральних чисел (без нуля). Якщо M — скінченна циклічна напівгрупа (скінченний циклічний моноїд), то індексом напівгрупи M називається таке найменше натуральне число i таке, що існує ціле число $r \geqslant 1$ і виконується рівність

$$a^{i+r} = a^i. \tag{1.1}$$

Найменше натуральне число r, для якого виконується рівність (1.1), називається *періодом* напівгрупи (моноїда) M. Пара, яка складається з індексу i та періоду r визначає моноїд, який має $i + r$ елементів:

$$M_{i,r} = \left\{1, a, a^2, \ldots, a^{i-1}, a^i, \ldots, a^{i+r-1}\right\}.$$

Напівгрупова операцію моноїда $M_{i,r}$ для зручності зображена на рис. 1.1.

За виконання умови $i \geqslant 1$ моноїд $M_{i,r}$ містить два ідемпотента. Справді, припустимо, що $a^j = a^{2j}$. Тоді, або $j = 0$, або $j \geqslant i$ та j і $2j$ є еквівалентними (рівними) за $\mod p$, звідки випливає, що $j \equiv 0 \mod p$. Навпаки, якщо $j \geqslant i$ та $j \equiv 0 \mod p$, то $a^j = a^{2j}$.

[2] Надалі рівність $ee = e$ ми будемо записувати $e^2 = e$. Також для кожного елемента a напівгрупи S визначимо $a^{n+1} = a^n a$, для довільного натурального числа n

[3] Бієктиний гомоморфізм $\varphi\colon S \to T$ напівгруп (моноїдів) S і T називається *ізоморфізмом*. Напівгрупи (моноїди) S і T називається *ізоморфними*,, якщо існує ізоморфізм $\varphi\colon S \to T$.

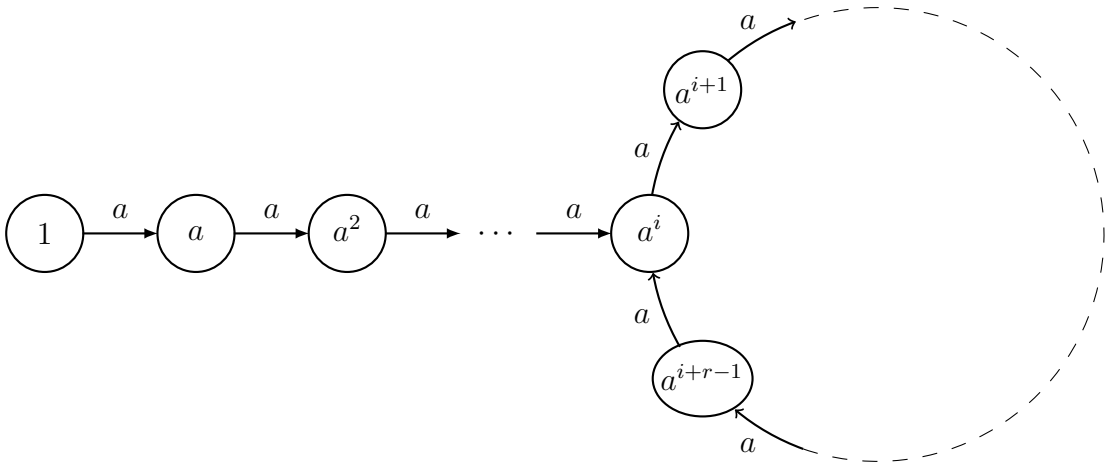


Рис. 1.1: Моноїд $M_{i,r}$

Таким чином, єдиним ідемпотентом, який відмінний від одиниці в моноїді $M_{i,r}$ є елемент $e = a^j$, де j — єдине ціле число з множини

$$\{i, i+1, \ldots, i+r-1\},$$

яке є кратним числу r.

Нехай M — моноїд. Для довільних елементів $x, y \in M$ означимо

$$x^{-1}y = \{z \in M \colon xz = y\} \qquad \text{і} \qquad xy^{-1} = \{z \in M \colon x = zy\}.$$

Для довільних непорожніх підмножин X і Y моноїда M вище означені поняття продовжуються до таких понять

$$X^{-1}Y = \bigcup_{x \in X} \bigcup_{y \in Y} x^{-1}y \qquad \text{і} \qquad XY^{-1} = \bigcup_{x \in X} \bigcup_{y \in Y} xy^{-1}.$$

Множина $X^{-1}Y$ називається *лівою часткою* множини Y, а множина XY^{-1} — *правою часткою* множини X. Легко бачити, що наступні тотожності виконуються для підмножин X, Y і Z моноїда M, і їхнє доведення ми залишаємо читачеві:

$$(XY)^{-1}Z = Y^{-1}(X^{-1}Z) \qquad \text{і} \qquad X^{-1}(YZ^{-1}) = (X^{-1}Y)Z^{-1}.$$

Позначення $X^{-1}Y$ не слід плутати з добутком оберненого з іншим елементом у деякій групі. Є такий випадок, коли може виникнути плутанина, а саме в розділі 14, де буде знайдено "застереження".

Для довільної непорожньої підмножини X моноїда M означимо

$$F(X) = M^{-1}XM^{-1},$$

яку надалі будемо називати *множиною множників* елементів у множині X. Очевидно, що виконується рівність

$$F(X) = \{m \in M \colon (\exists u, v \in M)[umv \in X]\}.$$

Ми деколи використовуватимемо символ $\overline{F}(X)$ для позначення доповнення до множини $F(X)$ в моноїді M, тобто

$$\overline{F}(X) = M \setminus F(X).$$

Відношенням на множині Q називається довільна підмножина декартового квадрату $Q \times Q$ множини Q. *Добутком* двох відношень m і n на множині Q називається відношення mn на Q, яке визначається так:

$$(p, r) \in mn \quad \Longleftrightarrow \quad \text{існує } q \in Q \text{ такий, що } (p, q) \in m \text{ і } (q, r) \in n.$$

Множина $\mathfrak{P}(Q \times Q)$ усіх відношень на множині Q є моноїдом стосовно операції добутку відношень. Два важливих відношення на множині Q — це *відношення рівності*

$$\mathrm{id}_Q = \{(q, q) \colon q \in Q\}$$

та *порожнє відношення* або *нульове відношення*, яке збігається з порожньою підмножиною в $Q \times Q$. Відношення рівності id_Q є одиницею моноїда $\mathfrak{P}(Q \times Q)$, а порожнє відношення є нулем в $\mathfrak{P}(Q \times Q)$.

Моноїд відношень деякої непорожньої множини Q — це підмоноїд моноїда $\mathfrak{P}(Q \times Q)$. Моноїд M відношень на множині Q називається *транзитивним*, якщо для всіх $p, q \in Q$ існує елемент $m \in M$ такий, що $(p, q) \in m$.

1.3 Слова

Нехай A — непорожня множина, яку ми надалі будемо називати *алфавітом*. *Словом* w над алфавітом A називається скінченна послідовність елементів множини A:

$$w = (a_1, a_2, \dots, a_n), \qquad a_i \in A.$$

Множина всіх слів над алфавітом A позначається через A^* і на A^* визначено бінарну операцію дописування слів, яку ще називають *конкатенацією*:

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_m) = (a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m).$$

Очевидно, що конкатенація слів є бінарною асоціативною операцією. Це дозволяє нам записувати

$$w = a_1 a_2 \cdots a_n$$

замість $w = (a_1, a_2, \dots, a_n)$, ототожнюючи кожен елемент $a \in A$ з послідовністю (a). Елемент алфавіта називається *літерою*. Порожня послідовність називається *порожнім словом* і позначається через 1 або ε. Очевидно, що порожнє слово є одиницею стосовно операції конкатенація. Таким чином, множина A^* слів наділена структурою моноїда. Моноїд A^* називається *вільним моноїдом* над множиною A. Множина непорожніх слів над алфавітом A позначається через A^+ і називається *вільною напівгрупою* над A. Очевидно, що $A^+ = A^* \setminus \{1\}$.

Довжиною $|w|$ слова $w = a_1 a_2 \cdots a_n$ з $a_i \in A$ називається кількість n літер в слові w. Очевидно, що $|1| = 0$. Функція $w \longmapsto |w|$ є морфізмом з вільного моноїда A^* на адитивний моноїд натуральних чисел $\mathbb{N}$. Для довільного натурального числа n означимо

$$A^{(n)} = \{w \in A^* \colon |w| \leqslant n-1\} \qquad \text{та} \qquad A^{[n]} = \{w \in A^* \colon |w| \leqslant n\}.$$

Зокрема, $A^{(0)} = \varnothing$ й $A^{[0]} = \{1\}$.

Для довільної непорожньої підмножини B алфавіту A через $|w|_B$ позначимо кількість літер слова w, які є елементами алфавіту B. Таким чином, для довільного слова w над алфавітом A маємо, що

$$|w| = \sum_{a \in A} |w|_{\{a\}}.$$

Для довільного слова $w \in A^*$ через

$$\operatorname{alph}(w) = \big\{a \in A \colon |w|_{\{a\}} > 0\big\}$$

позначимо множину всіх літер алфавіту A, які зустрічаються в слові w. Також для підмножини X вільного моноїда A^* покладемо

$$\operatorname{alph}(X) = \bigcup_{x \in X} \operatorname{alph}(x).$$

Слово $w \in A^*$ називається *множником* слова $x \in A^*$, якщо існують слова $u, v \in A^*$ такі, що $x = uwv$. Очевидно, що відношення "*бути множником*" є частковим порядком на вільному моноїді A^*. Множник w слова x є *власним*, якщо $w \neq x$.

Слово $w \in A^*$ називається *префіксом* слова $x \in A^*$, якщо існує слово $u \in A^*$ таке, що $x = wu$. Префікс w слова x є *власним*, якщо $w \neq x$. Очевидно, що відношення "*бути префіксом*" є знову частковим порядком на вільному моноїді A^* і таке відношення називається *префіксним частковим порядком* на вільному моноїді A^*. Якщо x і w — слова деякого вільного моноїда, то ми писатимемо $w \leq x$, якщо w є префіксом слова x і $w < x$, якщо w є власним префіксом слова x, тобто коли $w \leq x$ і $w \neq x$. Префіксний частковий порядок на вільному моноїді A^* має таку фундаментальну властивість:

> *якщо для деяких слів x, u та v вільного моноїда A^* виконуються умови*
>
> $$u \leq x \qquad \text{і} \qquad v \leq x,$$
>
> *то елементи u та v є порівняльними у вільному моноїді A^*, тобто $u \leq v$ або $v \leq u$.*

Іншими словами, якщо $wu = w'u'$, то виконується одна з умов: або існує елемент $s \in A^*$ такий, що $w = w's$ (і також $su = u'$), або існує елемент $t \in A^*$ такий, що $w = w't$ (і тоді $u = tu'$).

Зовсім симетрично, назвемо слово $w \in A^*$ *суфіксом* слова $x \in A^*$, якщо існує слово $u \in A^*$ таке, що $x = uw$. Суфікс w слова x є *власним*, якщо $w \neq x$. Підмножина $P \subset A^*$ *префіксно-замкненою*, якщо P містить префікси всіх своїх елементів, тобто

$$uv \in P \quad \Longrightarrow \quad u \in P.$$

Дуально вводиться поняття *суфіксно-замкненої* множини.

Розглянемо лінійно впорядкований алфавіт A. *Лексикографічний* або *алфавітний* порядок на вільному моноїді A^* визначається так:

> *$u \prec v$ якщо u є власним префіксом слова v, або $u = ras$, $v = rbt$, $a < b$ для $a, b \in A$ та $r, s, t \in A^*$.*

Для лексикографічного порядку виконується така властивість:

$$u \prec v \qquad \Longleftrightarrow \qquad wu \prec wu, \qquad \text{для} \quad u, v, w \in A^*.$$

Розрядний порядок на вільному моноїді A^* визначається так:

> *$u < v$ якщо $|u| < |v|$, або якщо $|u| = |v|$ й $u \prec v$ в лексикографічному порядку.*

Оберненим словом до слова $w = a_1 a_1 \cdots a_n$, де $a_i \in A$, називається слово

$$\widetilde{w} = a_n \cdots a_2 a_1.$$

Операцію взяття оберненого слова до слова w ми також будемо позначати $w^\sim$, тобто $w^\sim = \widetilde{w}$. Зауважимо, що для довільних слів u та v вільного моноїда A^* виконується рівність

$$(uv)^\sim = \widetilde{v}\,\widetilde{u}.$$

Оберненою множиною $\widetilde{X}$ до підмножини X вільного моноїда A^* називається множина $\widetilde{X} = \{\widetilde{x} \colon x \in X\}$.

Факторизацією слова $w \in A^*$ називається послідовність слів $\{u_1, u_2, \ldots, u_n\}$ вільного моноїда A^* $(n \geqslant 0)$ така, що

$$w = u_1 u_2 \cdots u_n.$$

Для довільної підмножини X вільного моноїда A^* через X^* позначимо підмоноїд A^*, породжений підмножиною X, тобто

$$X^* = \{x_1 x_2 \cdots x_n \colon n \geqslant 0,\ x_i \in X\},$$

а через X^+ — піднапівгрупу в A^*, породжену підмножиною X, тобто

$$X^+ = \{x_1 x_2 \cdots x_n \colon n \geqslant 1,\ x_i \in X\}.$$

Очевидно, що

$$X^+ = \begin{cases} X^* \setminus \{1\}, & \text{якщо} \quad 1 \notin X; \\ X^*, & \text{якщо} \quad 1 \in X. \end{cases}$$

З означення моноїда X^* випливає, що кожне слово w моноїда X^* допускає хоча б одну факторизацію $w = x_1 x_2 \cdots x_n$, елементи якої належать множині X. Така факторизація називається X-*факторизацією*. Ми часто використовуватимо образне зображення X-факторизації, наведене на рис. 1.2.

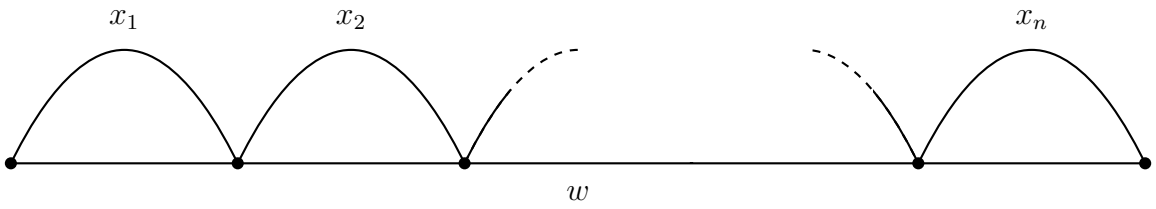


Рис. 1.2: X-факторизація слова w

Слово $x \in A^*$ називається *примітивним*, якщо x не є степенем жодного іншого слова. Отже, слово x вільного моноїда A^* є примітивним тоді і тільки тоді, коли з рівності $x = y^n$, де $y \in A^*$ і $n \geqslant 0$, випливає рівність $x = y$. Зауважимо, що порожнє слово не є примітивним.

Два слова x і y вільного моноїда A^* називаються *спряженими*, якщо існують слова $u, v \in A^*$ такі, що

$$x = uv \qquad \text{і} \qquad y = vu$$

(див. рис. 1.3). Ми часто говоримо в цьому випадку, що слово y є спряженим до слова x. Два спряжені слова отримуються одне з одного циклічною перестановкою літер. Точніше, нехай відображення $\gamma \colon A^* \to A^*$ визначено так:

$$\gamma(1) = 1 \qquad \text{і} \qquad \gamma(av) = va, \qquad \text{для} \quad a \in A,\ v \in A^*. \tag{1.2}$$

Очевидно, що так визначення відображення $\gamma \colon A^* \to A^*$ є бієктивним. Два слова x і y є спряженими тоді і лише тоді, коли існує невід'ємне ціле число n таке, що

$$x = \gamma^n(y).$$

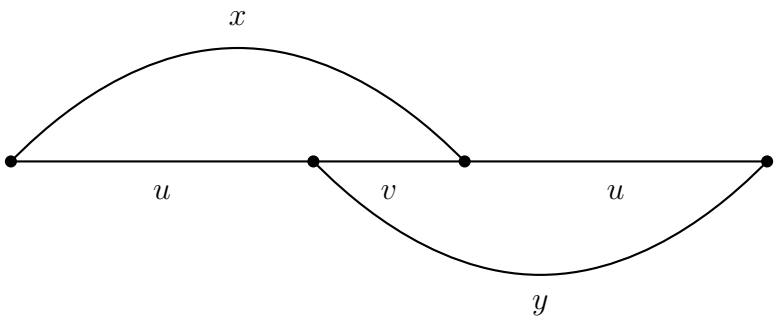


Рис. 1.3: Два спряжені слова x і y

З вище сказаного випливає, що відношення спряженості слів на вільному моноїд A^* є відношенням еквівалентності на A^*. *Класом спряженості* на A^* називається клас цього відношення еквівалентності. Клас спряженості на вільному моноїді A^* називається також називається *намистом*. *Довжиною намиста* називається довжина слів у класі спряженості. Намисто є *примітивним*, якщо кожне слово в класі спряженості є примітивним.

Твердження 1.3.1. *Кожне непорожнє слово у вільному моноїді A^* є степенем єдиного примітивного слова в A^*.*

Доведення. Нехай $x \in A^+$ і δ — звуження відображення $\gamma\colon A^* \to A^*$, визначеного за формулою (1.2), на клас спряженості слова x. Тоді δ^k є тотожним відображенням класу спряженості слова x тоді і лише тоді, коли слово x є степенем слова довжини, що ділить число k.

Нехай p — порядок відображення δ, тобто є найбільшим спільним дільником цілих чисел k таких, що δ^k є тотожним відображенням класу спряженості слова x. Оскільки δ^p є тотожним відображенням класу спряженості слова x, то існує слово r довжини p таке, що $x = r^e$ з $e \geqslant 1$. Слово r є примітивним, бо в протилежному випадку вснувало б слово s довжини q таке, що $r \in \{s\}^*$, а це у свою чергу, означає, що $x \in \{s\}^*$. Останнє суперечить визначенню числа p. З отриманого протиріччя випливає існування примітивного слова такого, що слово x є степенем цього примітивного слова в A^*. Для доведення єдиності, розглянемо слово $t \in A^*$ таке, що $x \in \{t\}^*$ і нехай $|t| = k$. Оскільки δ^k є тотожним відображенням класу спряженості слова x, то ціле число k є кратним числа p. Отже, отримуємо, що $t \in \{r\}^*$. Отож, якщо t — примітивне слово, то $t = r$. □

Нехай $x \in A^+$. Єдине примітивне слово r таке, що $x = r^n$ називається *коренем* слова x. Число n у цьому випадку називається *порядком* слова x.

Твердження 1.3.2. *Два непорожні спряжені слова в A^+ мають одинакові порядки та їх корені є спряженими.*

Доведення. Нехай $x, y \in A^+$ — два спряжені слова, і нехай i — натуральне число таке, що $y = \gamma^i(x)$. Покладемо r і s — корені x і y, відповідно, і нехай n — порядок слова x. Тоді

$$y = \gamma^i(r^n) = \big(\gamma^i(r)\big)^n .$$

Звідси випливає, що $\gamma^i(r) \in \{s\}^*$. Помінявши місцями слова x і y, отримаємо $\gamma^j(s) \in \{r\}^*$. Таким чином, ми отримуємо, що $\gamma^i(r) = s$ і $\gamma^j(s) = r$. Отже слова r і s є спряженими, а отже x і y мають одинакові порядки. □

Твердження 1.3.3. *Усі слова в класі спряженості вільного моноїда A^* мають одинакові порядки. Якщо $\mathcal{C}$ — клас спряженості слів довжини n з порядком e, то*

$$\mathrm{Card}(\mathcal{C}) = \tfrac{n}{e}.$$

Доведення. Нехай $x \in A^n$ і $\mathcal{C}$ — клас спряженості слова x. Нехай δ — звуження відображення $\gamma\colon A^* \to A^*$, визначеного за формулою (1.2), на клас $\mathcal{C}$ і p — порядок відображення δ. Коренем слова x є слово r довжини p таке, що $x = r^e$. Отже, $n = pe$. Покладемо

$$\mathcal{C} = \left\{x, \delta(x), \ldots, \delta^{p-1}(x)\right\}.$$

Усі елементи класу $\mathcal{C}$ є різними, оскільки p є порядком відображення δ. Таким чином, отримуємо $\mathrm{Card}(\mathcal{C}) = p$. □

Тепер визначимо кількість суміжних класів слів фіксованої довжини над скінченним алфавітом. Нехай A — алфавіт з k літерами. Для всіх чисел $n \geqslant 1$, *кількість класів спряженості* примітивних слів у вільному моноїд A^* довжини n будемо позначати через $\ell_n(k)$. Таке позначення можна оправдати тим, що це число залежить лише від числа k, а не від алфавіту A.

Перші значення цієї функції, для $k = 2, 3, 4$, викладено в табл. 1.1. Очевидно,

n	1	2	3	4	5	6	7	8	9	10	11	12
$\ell_n(2)$	2	1	2	3	6	9	18	30	56	99	186	335
$\ell_n(3)$	3	3	8	18	48	116	312	810				
$\ell_n(4)$	4	6	20	60	204	670						
$\ell_n(5)$	5	10	40	150	624							

Табл. 1.1: Кількість $\ell_n(k)$ примітивних класів спряження над k-літерним алфавітом.

що $\ell_n(1) = 1$, якщо $n = 1$, і $\ell_n(1) = 0$ в інших випадках. Тепер для довільного натурального числа $n \geqslant 1$ маємо, що

$$k^n = \sum_{d|n} d \cdot \ell_d(k), \tag{1.3}$$

де d набуває усіх значень дільників числа n. Справді, кожне слово довжини n належить рівно одному класу спряження слів довжини n. Кожен клас має $d = n/e$ елементів, де e є порядком слів цього класу. Оскільки існує стільки класів, слова яких мають порядок n/e, скільки є класів примітивних слів з довжиною $d = n/e$, то виконується формула (1.3).

Ми можемо отримати явний вираз для чисел $\ell_n(k)$, використовуючи функцію Мьобіуса, яку ми зараз введемо.

Функцією Мьобіуса[4] (the Möbius function) називається відображення $\mu\colon \mathbb{N}\setminus\{0\}\to\mathbb{N}$, яке визначається так: $\mu(1)=1$ і

$$\mu(n)=\begin{cases}(-1)^n, & \text{якщо } n \text{ є добутком } i \text{ різних первинних чисел;}\\ 0, & \text{в інших випадках.}\end{cases}$$

Твердження 1.3.4 (формула Мьобіуса оберненого перетворення). *Нехай* $\alpha\colon \mathbb{N}\setminus\{0\}\to\mathbb{N}$ *і* $\beta\colon \mathbb{N}\setminus\{0\}\to\mathbb{N}$ *— деякі відображення. Тоді*

$$\alpha(n)=\sum_{d|n}\beta(d)\qquad (n\geqslant 1) \tag{1.4}$$

тоді і лише тоді, коли

$$\beta(n)=\sum_{d|n}\mu(d)\cdot\alpha(n/d)\qquad (n\geqslant 1). \tag{1.5}$$

Доведення. Через $\mathcal{S}$ позначимо множину всіх функцій $\mathbb{N}\setminus\{0\}$ в $\mathbb{N}$. Означимо напівгрупову операцію на $\mathcal{S}$ так:

$$(f*g)(n)=\sum_{n=de}f(d)\cdot g(e),\qquad f,g\in\mathcal{S}.$$

Безпосередньо перевіркою доводиться, що з так визначеною напівгруповою операцією множина $\mathcal{S}$ є комутативним моноїдом, причому одиницею в $\mathcal{S}$ є відображення $I\colon \mathbb{N}\setminus\{0\}\to\mathbb{N}$, визначене за формулою:

$$I(n)=\begin{cases}1, & \text{якщо } n=1;\\ 0, & \text{в усіх інших випадках.}\end{cases}$$

Нехай $\iota\in\mathcal{S}$ — постійне відображення таке, що $\iota(n)=1$ для всіх $n\in\mathbb{N}\setminus\{0\}$. Покажемо, що виконується рівність

$$\iota*\mu=I. \tag{1.6}$$

Справді, $(\iota*\mu)(1)=1$. Якщо $n\geqslant 2$, то нехай

$$n=p_1^{k_1}p_2^{k_2}\dots p_m^{k_m}$$

— розклад натурального числа n на первинні множники. Якщо число d ділить n, то $\mu(d)\neq 0$ тоді і лише тоді, коли

$$d=p_1^{l_1}p_2^{l_2}\dots p_m^{l_m}$$

де степені l_i дорівнюють 0 або 1. Тоді

$$\mu(d)=(-1)^t\qquad\text{з}\qquad t=\sum_{i=1}^{m}l_i.$$

[4]Нагадаємо, що натуральне число $j>0$ називається *первинним*, якщо воно має лише два дільники: 1 і j. У теорії чисел первинні числа також називають *простими*.

Звідси випливає, що

$$(\iota * \mu)(n) = \sum_{d|n} \mu(d) = \sum_{t=0}^{m} (-1)^t \binom{m}{t} = 0.$$

Нехай тепер $\alpha, \beta \in \mathcal{S}$. Тоді формула (1.4) еквівалентна рівності $\alpha = \iota * \beta$ і формула (1.5) еквівалентна рівності $\beta = \mu * \alpha$, а за (1.6) отримуємо, що ці формули є еквівалентними. □

Безпосередньо з формули (1.3) та твердження 1.3.4 випливає таке твердження.

Твердження 1.3.5. *Кількість класів спряженості примітивних слів довжини n над алфавітом з k літер обчислюється за формулою*

$$\ell_n(k) = \frac{1}{n} \sum_{d|n} \mu(n/d) \cdot k^d.$$

Слово $w \in A^+$ називається *необлямованим*, якщо w не має власного непорожнього префіксу, який є суфіксом слова w. Іншими словами, слово w є необлямованим тоді і лише тоді, коли з $w \in uA^+ \cap A^+u$ випливає, що $u = 1$. Якщо слово w є необлямованим, то очевидно, що виконується така рівність

$$wA^* \cap A^*w = wA^*w \cup \{w\}.$$

Виконується наступна властивість.

Твердження 1.3.6. *Нехай A — алфавіт, який містить хоча б дві літери. Тоді для кожного слова $u \in A^+$ існує слово $v \in A^*$ таке, що слово uv є необлямованим.*

Доведення. Нехай a — перша літера слова u. Тоді покладемо b — довільна літера з $A \setminus \{a\}$. Далі ми перевіримо, що слово $w = uab^{|u|}$. Кожен непорожній префікс t слова w починається з літери a. Він не може бути суфіксом слова w, оскільки $|t| > |u|$. Але тоді ми маємо, що $t = sab^{|u|}$ для деякого слова $s \in A^*$, і також $t = uab^{|s|}$. Таким чином, ми отримали, що $|s| = |u|$, звідки випливає, що $t = w$. □

Нехай A — довільний алфавіт. *Вільна група* $A^{\odot}$ над алфавітом A визначається наступним чином. Нехай $\overline{A}$ — копія алфавіту A, яка не перетинається з A. Позначимо через $a \mapsto \overline{a}$ бієктивне співвідношення між алфавітом A та його копією $\overline{A}$. Дане поняття розширимо, поклавши $\overline{\overline{a}} = a$ для всіх $a \in A \cup \overline{A}$. Нехай δ — симетричне відношення, визначене

$$ua\overline{a}v \equiv uv \mod \delta, \qquad \text{для всіх} \quad u, v \in \left(A \cup \overline{A}\right)^* \quad \text{і} \quad a \in A \cup \overline{A}.$$

Нехай ρ — рефлексивне[5] та транзитивне[6] замикання відношення δ на $\left(A \cup \overline{A}\right)^*$. Тоді

[5] *Рефлексивне замикання* S відношення R на множині X визнається так:

$$S = R \cup \{(x, x) \colon x \in X\}$$

Іншими словами, рефлексивне замикання відношення R — це об'єднання R з відношенням рівності на множині X.

[6] *Транзитивне замикання* T відношення R на множині X визнається так:

$$T = \bigcup_{n=1}^{\infty} R^n = R \cup RR \cup RRR \cup \cdots.$$

ρ є конгруенцією на вільному моноїді $\left(A \cup \overline{A}\right)^*$. Фактор-моноїд $A^{\odot} = \left(A \cup \overline{A}\right)^* / \rho$ є групою. Справді,

$$a\overline{a} \equiv 1 \mod \rho,$$

для всіх $a \in A \cup \overline{A}$. Таким чином, ми отримали, що образи породжуючих елементів є оборотними в $A^{\odot}$. З останнього випливає, що усі елементи в $A^{\odot}$ є оборотними, а отже $A^{\odot}$ є групою.

Нехай A — довільний алфавіт. *Вільним комутативним моноїдом* $A^{\oplus}$ над алфавітом A називається фактор-напівгрупа за конгруенцією, яка поролжена парами (ab, ba) для $a, b \in A$, $a \neq b$. Якщо

$$A = \{a_1, a_2, \ldots, a_k\},$$

то моноїд $A^{\oplus}$ можна ототожнити з адитивним моноїдом за допомогою відображення

$$a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} \mapsto (n_1, n_2, \ldots, n_k).$$

Означимо відображення $\alpha\colon A^* \to A^{\oplus}$ за формулою

$$\alpha(w) = \prod_{a \in A} a^{|w|_a}.$$

Безпосередньо перевіркою доводиться, що так означене відображення $\alpha\colon A^* \to A^{\oplus}$ є морфізмом моноїдів.

1.4 Автомати

Нехай A — довільний непорожній алфавіт. *Автомат* над алфавітом A складається з:

- *множини станів* Q,
- підмножини $I \subseteq Q$, яка називається *множиною початкових станів*,
- підмножини $T \subseteq Q$, яка називається *множиною кінцевих станів*, та
- *множини переходів* $E \subseteq Q \times A \times Q$.

Автомат позначатимемо через

$$\mathcal{A} = (Q, I, T).$$

Автомат $\mathcal{A} = (Q, I, T)$ називається *скінченним*, якщо множина його станів Q є скінченною.

Шляхом в автоматі $\mathcal{A}$ називається послідовність

$$c = (f_1, f_2, \ldots, f_n)$$

послідовних переходів

$$f_i = (q_i, a_i, q_{i+1}), \qquad i = 1, \ldots, n.$$

У цьому випадку ціле число n називається *довжиною* шляху c, а слово $w = a_1 a_2 \ldots a_n$ будемо називати *міткою* шляху c. Також, у цьому випадку ми говоритимемо, що стан q_1 — *початковим* станом шляху c, а стан q_{n+1} — *кінцевим* станом шляху c. Надалі вище описаний шлях записуватимемо так:

$$c\colon q_1 \xrightarrow{w} q_{n+1}.$$

За згодою, для кожного стану $q \in Q$ автомата $\mathcal{A} = (Q, I, T)$ існує шлях довжини 0 зі стану q в q. Міткою такого шляху є порожнє слово.

Шлях $c\colon i \longrightarrow t$ в автоматі $\mathcal{A} = (Q, I, T)$ називається *успішним*, якщо $i \in I$ та $t \in T$. Будемо говорити, що множина слів *розпізнувана* автоматом $\mathcal{A} = (Q, I, T)$ і будемо позначати її через $L(\mathcal{A})$, якщо вона є множиною міток успішних шляхів цього автомата.

Стан $q \in Q$ автомата $\mathcal{A} = (Q, I, T)$ називається *доступним*, якщо існує шлях $c\colon i \longrightarrow q$ для $i \in I$ і *кодоступним*, якщо снує шлях $c\colon q \longrightarrow t$ для $t \in T$. Автомат називається *впорядкованим* (*обрізаним*), якщо кожен його стан одночасно є доступним і кодоступним. Нехай P — множина усіх доступних і кодоступних станів автомата $\mathcal{A} = (Q, I, T)$, і нехай

$$\mathcal{A}^0 = (Q, I \cap P, T \cap P).$$

Тоді, очевидно, що автомат $\mathcal{A}^0$ є впорядкованим і крім того $L(\mathcal{A}) = L(\mathcal{A}^0)$. Автомат $\mathcal{A}^0$ називається *впорядкованою частиною* автомата $\mathcal{A}$.

Автомат можна розглядати як мультиграф з мітками, наділений двома відмінними множинами вершин: початковими та кінцевими станами. Мультиграф, який має множину станів Q автомата $\mathcal{A} = (Q, I, T)$ за множину вершин і множину переходів E за множину ребер, називається *основним графом* автомата $\mathcal{A}$. Автомат $\mathcal{A}$ називається *сильно зв'язним*, якщо його основний граф є сильно зв'язним, тобто для

довільної пари (p, q) станів автомата $\mathcal{A}$ (вершин основного графа автомата $\mathcal{A}$) існує шлях з p в q.

Нехай $\mathcal{A} = (Q, I, T)$ — автомат над непорожнім алфавітом A. Для кожного слова $w \in A^*$ позначимо через $\varphi_{\mathcal{A}}(w)$ таке відношення на множині станів Q автомата $\mathcal{A}$

$$(p, q) \in \varphi_{\mathcal{A}}(w) \quad \Longleftrightarrow \quad p \xrightarrow{w} q.$$

З означення цього відношення випливає, що $\varphi_{\mathcal{A}}$ є морфізмом з вільного моноїда A^* в моноїд усіх відношень на множині станів Q автомата $\mathcal{A}$. Підмоноїд $\varphi_{\mathcal{A}}(A^*)$ моноїда усіх відношень на множині станів Q автомата $\mathcal{A}$ називається *моноїдом переходів* автомата $\mathcal{A} = (Q, I, T)$.

Очевидно, що автомат є сильно зв'язним тоді і лише тоді, коли його моноїд переходів є транзитивним.

Автомат $\mathcal{A} = (Q, I, T)$ називається *детермінованим*, якщо $\mathrm{Card}(I) = 1$ і виконується імплікація

$$(p, a, q), (p, a, r) \in E \qquad \Longrightarrow \qquad q = r.$$

Отже, для кожного стану $p \in Q$ і кожної літери $a \in A$ існує не більше одного стану $q \in Q$ такого, що $p \xrightarrow{a} q$. Для $p \in Q$ і $a \in A$ означимо

$$p \cdot a = \begin{cases} q, & \text{якщо } (p, a, q) \in E; \\ \varnothing, & \text{в іншому випадку.} \end{cases}$$

Часткове відображення з $Q \times A$ в Q, означене вище, можна продовжити до часткового відображення $Q \times A^* \rightharpoonup Q$ (на множину всіх слів), поклавши $p \cdot 1 = p$ для всіх $p \in Q$, і для $w \in A^*$ й $a \in A$ так:

$$p \cdot wa = (p \cdot w) \cdot a.$$

Звідси випливає, що для довільних слів $u, v \in A^*$ виконується рівність

$$p \cdot uv = p \cdot u \cdot v. \tag{1.7}$$

Вище означене часткове відображення називається *функцією* (*відображенням*) *переходів* автомата $\mathcal{A} = (Q, I, T)$. За цим означенням отримуємо, що $I = \{i\}$ і

$$L(\mathcal{A}) = \{w \in A^* \colon i \cdot w \in T\}.$$

Автомат $\mathcal{A} = (Q, I, T)$ називається *повним*, якщо для довільного стану $p \in Q$ та довільної дітери $a \in A$ існує хоча б один стан $q \in Q$ такий, що $p \xrightarrow{a} q$.

Твердження 1.4.1. *Для довільного автомата $\mathcal{A}$ існує повний детермінований автомат $\mathcal{B}$ такий, що*

$$L(\mathcal{A}) = L(\mathcal{B}).$$

Більше того, якщо автомат $\mathcal{A}$ — скінченний, то автомат $\mathcal{B}$ можна вибрати скінченним.

Доведення. Нехай $\mathcal{A} = (Q, I, T)$. Означимо автомат $\mathcal{B} = (R, u, V)$, прийнявши $R = \mathfrak{P}(Q)$, $u = I$ та

$$V = \{S \subset Q \colon S \cap T \neq \varnothing\}.$$

Означимо функцію переходів автомата $\mathcal{B}$ так: для довільного стану $S \in R$ та довільної літери $a \in A$ покладемо

$$S \cdot a = \left\{ q \in Q \colon \exists\, s \in S \text{ таке, що } s \xrightarrow{a} q \right\}.$$

Очевидно, що автомат $\mathcal{B}$ є повним і детермінованим, і легко бачити, що $L(\mathcal{A}) = L(\mathcal{B})$, а якщо автомат $\mathcal{A}$ — скінченний, то автомат $\mathcal{B}$ є скінченним також. □

Приклад 1.4.2. На рис. 1.4 наведено недетермінований автомат, що розпізнає усі

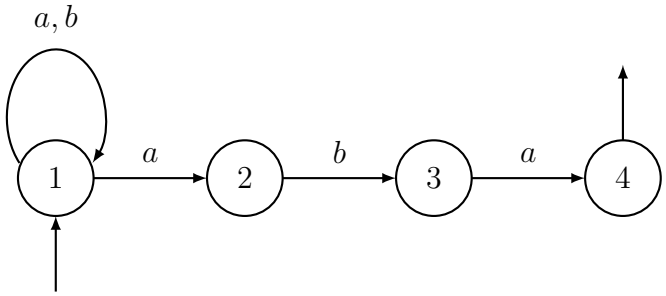


Рис. 1.4: Недетермінований автомат, який розпізнає множину слів $X = \{a, b\}^* aba$.

слова алфавіту $A = \{a, b\}$, які мають суфікс aba. Детермінований автомат, отриманий з даного автомата конструкцією, викладеною в доведенні твердження 1.4.1, зображено на рис. 1.5. Часто буває так, що обидва автомат $\mathcal{A}$ та визначений стосовно

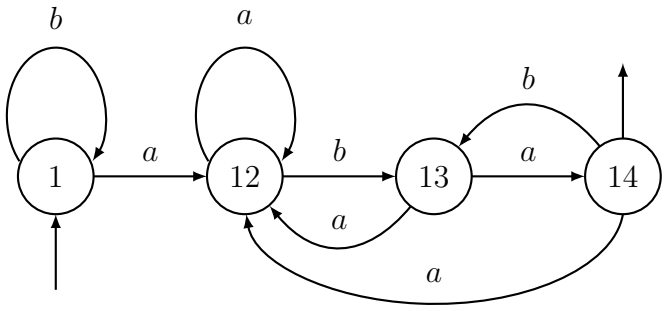


Рис. 1.5: Детермінований автомат, який розпізнає множину слів $X = \{a, b\}^* aba$.

нього доведенні твердження 1.4.1 автомат $\mathcal{B}$ мають однакову кількість станів.

Нехай $\mathcal{A} = (Q, i, T)$ — детермінований автомат над алфавітом A. Для кожного стану $q \in Q$ означимо

$$L_q = \{ w \in A^* \colon q \cdot w \in T \}.$$

Два стани $p, q \in Q$ називаються *невідокремлюваними*, якщо $L_p = L_q$ і *відокремлюваними* в протилежному випадку. Детермінований автомат називається *зведеним* або *мінімальним*, якщо довільні два різні його стани є відокремлюваними.

Нехай X – підмножина вільного моноїда A^*. Означимо спеціальний автомат $\mathcal{A}(X)$ наступним чином. Станами автомату $\mathcal{A}(X)$ є непорожні множини вигляду $u^{-1}X$ для $u \in A^*$. Початковим станом є множина $1^{-1}X$, а кінцевими станами є такі, які містять порожнє слово. Функція переходу визначена для стану $Y = u^{-1}X$ і літери $a \in A$ так:

$$Y \cdot a = a^{-1}Y.$$

Зауважимо, що цим ми визначили часткове відображення. Тоді отримуємо

$$L(\mathcal{A}(X)) = X.$$

Легко бачити, що за індукцією можна довести рівність $X \cdot w = w^{-1}X$ для довільного слова $w \in A^*$. Таким чином, ми отримали, що

$$w \in L(\mathcal{A}(X)) \quad \Longleftrightarrow \quad 1 \in X \cdot w \quad \Longleftrightarrow \quad 1 \in w^{-1}x \quad \Longleftrightarrow \quad w \in X.$$

Автомат $\mathcal{A}(X)$ є зведеним. Справді, для $Y = u^{-1}X$ маємо

$$L_Y = \{v \in A^* \colon Y \cdot v \in T\} = \{v \in A^* \colon uv \in X\}.$$

Таким чином, отримуємо, що $L_Y = Y$.

Автомат $\mathcal{A}(X)$ називається *мінімальним автоматом* підмножини X слів вільного моноїда A^*. Ця термінологія виправдана та мотивована наступним твердженням.

Твердження 1.4.3. *Нехай $\mathcal{A} = (Q, i, T)$ — впорядкований детермінований автомат і $X = L(\mathcal{A})$. Нехай $\mathcal{A}(X) = (P, j, S)$ — мінімальний автомат множини X. Тіді відображення $\varphi \colon Q \to P$, $\varphi(q) = L_q$ є сюр'єктивним і задовольняє наступні умови*

$$\varphi(i) = j, \qquad \varphi(T) = S \qquad i \qquad \varphi(q \cdot a) = \varphi(q) \cdot a.$$

Доведення. Нехай $q \in Q$ і $u \in A^*$ — таке слово, що $i \cdot u = q$. Тоді

$$L_q = \{w \in A^* \colon q \cdot w \in T\} = u^{-1}X.$$

Оскільки автомат $\mathcal{A}$ є впорядкованим, то $L_q \neq \varnothing$. Звідси випливає, що $L_q \in P$. Таким чином, ми отримуємо, що φ є відображенням з Q в P. Далі покажемо, що відображення $\varphi \colon Q \to P$ є сюр'єктивним. Нехай $u^{-1}X \in P$. Тоді $u^{-1}X \neq \varnothing$. Таким чином $i \cdot u \neq \varnothing$ і поклавши $q = i \cdot u$, отримуємо $L_q = u^{-1}X = \varphi(q)$. Звідки випливає, що відображення $\varphi \colon Q \to P$ є сюр'єктивним.

Нарешті, для стану $q = i \cdot u$ отримуємо

$$\varphi(q \cdot a) = L_{q \cdot a} = (ua)^{-1}X = (u^{-1}X) \cdot a = L_q \cdot a,$$

що і завершує доведення твердження. □

Якщо припустити, що автомат $\mathcal{A}$ в твердженні 1.4.3 є зведеним, то відображення $\varphi \colon Q \to P$ є биекцією, яка ототожнює автомат $\mathcal{A}$ з мінімальним автоматом. У цьому сенсі існує лише один мінімальний автомат, який визначає вибрану множину X слів вільного моноїда A^*.

Нехай $\mathcal{A} = (Q, i, T)$ — детермінований автомат над алфавітом A. Відношення еквівалентності ρ на множині станів Q називається *конгруенцією*, якщо для всіх

станів p і q та літер $a \in A$ виконується наступне твердження: *якщо* $p \equiv q \mod \rho$ *і значення* $p \cdot a$ *та* $q \cdot a$ *визначені, то* $p \cdot a \equiv q \cdot a \mod \rho$.

Фактор-автомат автомата $\mathcal{A} = (Q, i, T)$ за конгруенцією ρ, який позначатимемо через $\mathcal{A}/\rho$, визначається наступним чином. Станами автомата $\mathcal{A}/\rho$ є класи еквівалентностей відношення ρ множини станів Q, його початковими станами є початкові стани автомата $\mathcal{A}$, а кінцевими станами Є кінцеві стани автомата $\mathcal{A}$. Функція переходів автомата $\mathcal{A}/\rho$ визначається так: якщо q — стан автомата $\mathcal{A}/\rho$ й a — літера алфавіту A, то значення визначено, коли існує стан p автомата $\mathcal{A}$ в класі q такий, що $p \cdot a$ визначено, і в цьому випадку $q \cdot a$ є класом стану $p \cdot a$. Означення є коректним, оскільки ρ є конгруенцією на множині станів Q автомата $\mathcal{A}$.

Наприклад, відношення еквівалентності на множині станів детермінованого автомата $\mathcal{A} = (Q, i, T)$, яке визначене

$$p \equiv q \textit{ тоді і лише тоді, коли стани } p \textit{ і } q \textit{ є невідокремлюваними},$$

є конгруенцією. Якщо автомат $\mathcal{A}$ є впорядкованим, то фактор-автомат за так визначеною конгруенцією є мінімальним автоматом множини $L(\mathcal{A})$.

Нехай $\mathcal{A} = (Q, i, T)$ — детермінований автомат над алфавітом A. Розглянемо множину $\mathcal{F}$ усіх часткових відображень з Q в Q. Ці часткові відображення будемо записувати справа: якщо $q \in Q$ і $m \in \mathcal{F}$, то образ стану q стосовно часткового відображення m позначатимемо через qm. Композиція часткових відображення визначається так:

$$q(mn) = (qm)n.$$

Таким чином, на множині $\mathcal{F}$ усіх часткових відображень з Q в Q існує структура моноїда.

Нехай φ — відображення, яке кожному слову $w \in A^*$ ставить у відповідність часткове відображення з Q в Q, означене за формулою

$$q\varphi(w) = q \cdot w.$$

Відображення φ є морфізмом з вільного моноїда A^* в моноїд $\mathcal{F}$. Підмоноїд $\varphi(A^*)$ моноїда $\mathcal{F}$ називається *моноїдом переходів* автомата $\mathcal{A}$. Це узгоджується з термінологією для загальних автоматів, оскільки часткові відображення є частковим випадком бінарних відношень.

Зауважимо, що поклавши $L(\mathcal{A})$, отримуємо

$$\varphi^{-1}\varphi(X) = X. \tag{1.8}$$

Справді $w \in \varphi^{-1}\varphi(X)$ тоді і лише тоді, коли $\varphi(w) \in \varphi(X)$, що еквівалентно $i\varphi(w) \in T$, а це означає, що $w \in X$.

Будемо говорити, що морфізм φ з моноїда M на моноїд N *розпізнає* підмножину моноїда M, якщо

$$\varphi^{-1}\varphi(X) = X.$$

Підмножина X моноїда M називається *розпізнаваною*, якщо вона розпізнається морфізмом на скінченний моноїд.

Нехай X — підмножина вільного моноїда A^*. Для слова $w \in A^*$ пара (u, v) слів таких, що $uwv \in X$ називається *контекстом* слова w у множині X. Через $\Gamma(w)$ позначимо множину усіх контекстів слова w, яка визначається так

$$\Gamma(w) = \{(u, v) \in A^* \times A^* \colon uwv \in X\}.$$

Синтаксичною конгруенцією підмножини X вільного моноїда A^* називається відношення еквівалентності $\sim_X$ на A^* визначається так:

$$w \sim_X w' \qquad \Longleftrightarrow \qquad \Gamma(w) = \Gamma(w').$$

Безпосередньо звичайною перевіркою доводиться, що відношення $\sim_X$ є конгруенцією на вільному моноїді A^*. Фактор-моноїд $A^*/\sim_X$ називається *синтаксичним моноїдом* множини X. Надалі цей фактор-моноїд позначатимемо через $\mathcal{M}(X)$, а через φ_X — канонічний морфізм з вільного моноїда A^* в моноїд $\mathcal{M}(X)$. Зауважимо, що морфізм $\varphi_X \colon A^* \to \mathcal{M}(X)$ розпізнає множину X.

Твердження 1.4.4. *Нехай X — підмножина вільного моноїда A^* і $\varphi \colon A^* \to M$ — сюр'єктивний морфізм на моноїд M. Якщо морфізм φ розпізнає множину X, то існує сюр'єктивний морфізм $\psi \colon M \to \mathcal{M}(X)$ такий, що*

$$\varphi_X = \psi \circ \varphi.$$

Доведення. Достатньо показати, що

$$\varphi(w) = \varphi(w') \qquad \Longrightarrow \qquad \varphi_X(w) = \varphi_X(w'). \tag{1.9}$$

Справді, якщо твердження (1.9) виконується, то для елемента $m \in M$ значення $\psi(m)$ визначено, як єдиний елемент в $\varphi_X(\varphi^{-1}(m))$. Для доведення твердження (1.9) розглянемо $(u, v) \in \Gamma(w)$. Тоді $uwv \in X$. Тоді маємо, що $\varphi(u)\varphi(w)\varphi(v) \in \varphi(X)$. З рівності $\varphi(w) = \varphi(w')$ випливає, що $\varphi(u)\varphi(w')\varphi(v) \in \varphi(X)$. Оскільки морфізм φ розпізнає множину X, то маємо, що $uw'v \in X$, а отже $(u, v) \in \Gamma(w')$. □

Твердження 1.4.5. *Нехай X — підмножина вільного моноїда A^*. Синтаксичний моноїд множини X ізоморфний моноїдові переходів мінімального автомата $\mathcal{A}(X)$.*

Доведення. Нехай M — моноїд переходів автомата $\mathcal{A}(X) = (Q, i, T)$ і $\varphi \colon A^* \to M$ — канонічний морфізм. З рівності (1.8) випливає, що морфізм φ розпізнає множину X. За твердженням 1.4.4 існує сюр'єктивний морфізм $\psi \colon M \to \mathcal{M}(X)$ такий, що $\varphi_X = \psi \circ \varphi$.

Достатньо показати, що морфізм $\psi \colon M \to \mathcal{M}(X)$ є ін'єктивним. Для цього розглянемо елементи $m, m' \in M$ такі, що $\psi(m) = \psi(m')$. Нехай $w, w' \in A^*$ такі, що $\varphi(w) = m$ і $\varphi(w') = m'$. Тоді $\varphi_X(w) = \varphi_X(w')$. Для доведення рівності $\varphi(w) = \varphi(w')$ розглянемо стан $p \in Q$, і нехай $u \in A^*$ таке слово, що $p = u^{-1}X$. Тоді

$$p\varphi(w) = p \cdot w = (uw)^{-1}X = \{v \in A^* \colon (u, v) \in \Gamma(w)\}.$$

Оскільки $\Gamma(w) = \Gamma(w')$, то маємо, що $p\varphi(w) = p\varphi(w')$. Таким чином, отримуємо рівність $\varphi(w) = \varphi(w')$, з якої випливає, що $m = m'$. □

Далі ми наводимо коротке описання властивостей, специфічних для скінченних автоматів.

Теорема 1.4.6. *Для підмножини X вільного моноїжа A^* наступні умови є еквівалентними:*

(i) *множина X розпізнається скінченним автоматом;*
(ii) *мінімальний автомат $\mathcal{A}(X)$ є скінченним;*
(iii) *сім'я множин $u^{-1}X$, для довільного слова $u \in A^*$, є скінченною;*
(iv) *синтаксичний моноїд $\mathcal{M}(X)$ є скінченним;*
(v) *множина X розпізнавана.*

Доведення. $(i) \Longrightarrow (ii)$ Нехай $\mathcal{A}$ — скінченний автомат, який розпізнає множину X. За твердженням 1.4.1 можемо вважати, що автомат $\mathcal{A}$ є детерміністичним. За твердженням 1.4.3 мінімальний автомат $\mathcal{A}(X)$ також є скінченним.

Еквівалентність $(ii) \Longleftrightarrow (iii)$ очевидна.

Імплікація $(ii) \Longrightarrow (iv)$ випливає з твердження 1.4.5 і з того факту, що моноїд переходів скінченного автомату є завжди скінченним.

Імплікація $(iv) \Longrightarrow (v)$ очевидна.

$(v) \Longrightarrow (i)$ Нехай $\varphi\colon A^* \to M$ — сюр'єктивний морфізм на скінченний моноїд M і припустимо, що морфізм φ розпізнає множину X. Нехай $\mathcal{A} = (M, 1, \varphi(X))$ — детерміністичний автомат з функцією переходів, яка визначається так: $m \cdot a = m\varphi(a)$. Тоді $1 \cdot w \in \varphi(X)$ тоді і лише тоді, коли $\varphi(w) \in \varphi(X)$, а це виконується тоді і тільки тоді, коли $w \in X$. Як наслідок отримуємо, що $L(\mathcal{A}) = X$. □

Твердження 1.4.7. *Сім'я розпізнаваних підмножин вільного моноїда A^* замкнена стосовно всіх булевих операцій: об'єднання, перетину та доповнення.*

Доведення. Нехай $X, Y \subset A^*$ — дві розпізнувані підмножини вільного моноїда A^*. Нехай $\mathcal{A} = (P, i, S)$ і $\mathcal{B} = (Q, j, T)$ — повні детерміністичні автомати такі, що $X = L(\mathcal{A})$ і $Y = L(\mathcal{B})$. Означимо повний детерміністичний автомат

$$\mathcal{C} = (P \times Q, (i, j), R)$$

з функцією переходу

$$(p, q) \cdot a = (p \cdot a, q \cdot a).$$

Тоді:

(i) для $R = (S \times Q) \cup (P \times T)$ маємо $L(\mathcal{C}) = X \cup Y$;
(ii) для $R = S \times T$ маємо $L(\mathcal{C}) = X \cap Y$;
(iii) для $R = S \times (Q \setminus T)$ маємо $L(\mathcal{C}) = X \setminus Y$,

що і завершує доведення твердження. □

Твердження 1.4.8. *Нехай $\alpha\colon A^* \to B^*$ — морфізм вільних моноїдів A^* і B^*. Якщо Y — розпізнувана підмножина в B^*, то $X = \alpha^{-1}(Y)$ — розпізнувана підмножина в A^*.*

Доведення. Оскільки Y — розпізнувана підмножина в B^*, то $Y = \varphi^{-1}(\varphi(Y))$, де $\varphi\colon B^* \to M$ — сюр'єктивний морфізм на скінченний моноїд M. Визначимо відображення $\psi\colon A^* \to M$ за формулою $\psi = \varphi \circ \alpha$. Легко переконатися, що виконується рівність $X = \psi^{-1}(\psi(X))$. □

Твердження 1.4.9. *Якщо X — розпізнувана підмножина вільного моноїда A^*, то $Y^{-1}X$ — розпізнувана підмножина в A^*, для довільної підмножини $Y \subseteq A^*$.*

Доведення. Виконується рівність

$$u^{-1}(Y^{-1}X) = \bigcup_{y \in Y} (yu)^{-1}X.$$

Оскільки X — розпізнувана підмножина вільного моноїда A^*, то існує скінченна кількість множин вигляду $(yu)^{-1}X$, а отже існує скінченна кількість множин вигляду $u^{-1}(Y^{-1}X)$. Звідси випливає, що $Y^{-1}X$ — розпізнувана підмножина в A^*. □

Розглянемо тепер слабке узагальнення автомата. *Асинхронним автоматом* на алфавіті A називається автомат $\mathcal{A} = (Q, I, T)$, переходи якого можна помітити або літерами алфавіту A, або ж порожнім словом. Таким чином, множина переходів асинхронного автомата задовольняє умову

$$F \subset Q \times (A \cup \{1\}) \times Q.$$

Для асинхронного автомата поняття шляху, успішного шляху чи розпізнуваної множини вводяться аналогічно, як і для звичайного автомата.

Твердження 1.4.10. *Для довільного асинхронного автомата $\mathcal{A}$ існує скінченний автомат $\mathcal{B}$ такий, що $L(\mathcal{A}) = L(\mathcal{B})$.*

Доведення. Нехай $\mathcal{A} = (Q, I, T)$ — асинхронний автомат. Нехай $\mathcal{B}$ — автомат, отриманий з автомата $\mathcal{A}$, заміною переходів трійками (p, a, q) таких, що існує шлях $p \xrightarrow{a} q$ в автоматі $\mathcal{A}$. Тоді ми отримуємо

$$L(\mathcal{A}) \cap A^+ = L(\mathcal{B}) \cap A^+.$$

Якщо $I \cap T \neq \varnothing$, то обидві множини $L(\mathcal{A})$ та $L(\mathcal{B})$ містять порожнє слово, а отже збігаються. В протилежному випадку множини $L(\mathcal{A})$ та $L(\mathcal{B})$ з точністю до порожнього слова, і наше твердження випливає з твердження 1.4.7, оскільки множина $\{1\}$ є розпізнаваною. □

Поняття асинхронного автомата використаємо для доведення наступного твердження.

Твердження 1.4.11. *Якщо підмножина X вільного моноїда A^* є розпізнаваною, то підмоноїд X^* в A^* є розпізнаваною множиною також. Якщо підмножини X і Y вільного моноїда A^* є розпізнаваними, то множина XY є розпізнаваною.*

Доведення. Нехай $\mathcal{A} = (Q, I, T)$ — скінченний автомат, який розпізнає множину X. Через E позначимо множину його переходів. Нехай $\mathcal{B}$ — асинхронний автомат, отриманий з автомату $\mathcal{A}$ додаванням до множини E трійок $(t, 1, i)$, для $t \in T$ й $i \in I$.

Ми стверджуємо, що $L(\mathcal{B}) = X^+$. Справді, включення $X^+ \subseteq L(\mathcal{B})$ є очевидним. Доведемо, що виконується обернене включення. Нехай $c\colon i \xrightarrow{w} j$ — успішний шлях в автоматі $\mathcal{B}$. З означення автомата $\mathcal{B}$ випливає, що цей шлях має вигляд

$$c\colon i_1 \xrightarrow{w_1} t_1 \xrightarrow{1} i_2 \xrightarrow{w_2} t_2 \xrightarrow{1} \cdots \xrightarrow{1} i_n \xrightarrow{w_n} t_n,$$

причому $i = i_1$, $j = t_n$ і немає шляху $c_k\colon i_k \xrightarrow{w_k} t_l$, який містить перехід помічений порожнім словом. Тоді $w_1, w_2, \cdots, w_n \in X$, а отже $w \in X^+$. Звідси випливає, що піднапівгрупа X^+ вільного моноїда A^* є розпізнаваною множиною, а отже, моноїд $X^* = X^+ \cup \{1\}$ є розпізнаваною множиною.

Нехай тепер $\mathcal{A} = (P, I, S)$ і $\mathcal{B} = (Q, J, T)$ — два скінченні автомати з множинами переходів E та F, відповідно. Нехай $X = L(\mathcal{A})$ й $Y = L(\mathcal{B})$. На зменшуючи загальності, можемо вважати, що $P \cap Q = \varnothing$. Нехай $\mathcal{C} = (P \cup Q, I, T)$ — асинхронний автомат з множиною переходів

$$E \cup F \cup (S \times \{1\} \times J).$$

Безпосередньо перевіркою доводиться, що $L(\mathcal{C}) = XY$. □

Далі ми дамо інше описання розпізнаваних множин вільного моноїда A^*. Нехай M — моноїд. Найменша сім'я $\mathcal{R}$ підмножин моноїда M, яка задовольняє такі умови:

(*i*) кожна скінченна підмножина моноїда M є елементом сім'ї $\mathcal{R}$;
(*ii*) якщо $X, Y \in \mathcal{R}$, то $X \cup Y \in \mathcal{R}$ та $XY \in \mathcal{R}$;
(*iii*) якщо $X \in \mathcal{R}$, то $X^* \in \mathcal{R}$,

називається сім'єю *раціональних підмножин* моноїда M. Третю з цих операцій будемо називати *зірка-операцією* або просто $*$-*операцією*. Обєднання, перетин та $*$-операція називаються *раціональними операціями*.

Твердження 1.4.12. *Нехай $\alpha\colon A^* \to B^*$ — морфізм вільних моноїдів A^* і B^*. Якщо X — раціональна підмножина в A^*, то $Y = \alpha(X)$ — раціональна підмножина в B^*.*

Доведення. Очевидно, що твердження виконується для скінченної підмножини X в A^*, і якщо твердження виконується для двох підмножин X_1 і X_2 вільного моноїда A^*, то воно виконується для їх об'єднань, їх перетинів та для X_1^* і X_2^*. Таким чином, наше твердження виконується для довільної раціональної підмножини вільного моноїда A^*. □

Теорема 1.4.13 (Кліні). *Нехай A – скінченний алфавіт. Підмножина X вільного моноїда A^* є розпізнаваною тоді і лише тоді, коли X є раціональною.*

Доведення. Позначимо через $\mathsf{Rec}(A^*)$ і $\mathsf{Rat}(A^*)$ сім'ю розпізнаваних підмножин та сім'ю раціональних підмножин вільного моноїда A^*, відповідно. Спочатку доведемо включення $\mathsf{Rat}(A^*) \subseteq \mathsf{Rec}(A^*)$. Добре відомо, що кожна скінченна підмножина X вільного моноїда A^* є розпізнаваною. Більше того, з тверджень 1.4.7 і 1.4.11 випливає, що сім'я $\mathsf{Rec}(A^*)$ задовольняє умови (*ii*) та (*iii*) означення раціональних підмножин вільного моноїда A^*. Отже, виконується включення $\mathsf{Rat}(A^*) \subseteq \mathsf{Rec}(A^*)$.

Для доведення включення $\mathsf{Rec}(A^*) \subseteq \mathsf{Rat}(A^*)$ розглянемо розпізнавану підмножину X вільного моноїда A^*. Нехай $\mathcal{A} = (Q, I, T)$ — скінченний автомат, який розпізнає множину X. Покладемо $Q = \{1, 2, \ldots, n\}$ і

$$X_{i,j} = \left\{ w \in A^*\colon i \xrightarrow{w} j \right\},$$

для $1 \leqslant i, j \leqslant n$. Ми маємо, що виконується рівність

$$X = \bigcup_{i \in I} \bigcup_{j \in T} X_{i,j}.$$

Тому достатньо довести, що кожна підмножина $X_{i,j}$ вільного моноїда A^* є раціональною. Для кожного натурального числа $k \in \{0, 1, \ldots, n\}$ через $X_{i,j}^{(k)}$ позначимо множину таких слів $w \in A^*$, що існує шлях $c\colon i \xrightarrow{w} j$, який проходить лише через стани $l \leqslant k$, крім, можливо, для станів i, j. Іншими словами, ми маємо $w \in A^*$ тоді і лише тоді, коли $w = a_1 a_2 \cdots a_m$ з

$$c\colon i \xrightarrow{a_1} i_1 \xrightarrow{a_2} i_2 \xrightarrow{a_3} \ldots \xrightarrow{a_{m-1}} i_{m-1} \xrightarrow{a_m} j$$

і $i_1 \leqslant k, \ldots, i_{m-1} \leqslant l$. Тоді виконуються такі умови:

$$X_{i,j}^{(0)} \subseteq A \cup \{1\}, \tag{1.10}$$

$$X_{i,j}^{(n)} = X_{i,j}, \tag{1.11}$$

$$X_{i,j}^{(k+1)} = X_{i,j}^{(k)} \cup X_{i,k+1}^{(k)} \left(X_{k+1,k+1}^{(k)}\right)^* X_{k+1,j}^{(k)}, \qquad (0 \leqslant k < n). \tag{1.12}$$

Оскільки алфавіт A є скінченним, то з (1.10) випливає, що $X_{i,j}^{(0)} \in \mathsf{Rat}(A^*)$. Також за індукцією за умови (1.12) отримуємо, що $X_{i,j}^{(k)} \in \mathsf{Rat}(A^*)$ для довільного натурального числа k, а тоді за умовою (1.11) маємо, що $X_{i,j} \in \mathsf{Rat}(A^*)$. □

У випадку нескінченного алфавіта розпізнавані слова не обов'язково є раціональними: наприклад, сам алфавіт є розпізнаваним, але не раціональним. Однак будь-яка розпізнавана множина є оберненим образом стосовно морфізму, який зберігає довжини слів, розпізнаваної множини X над скінченним алфавітом. Справді, цей морфізм ототожнює літери з самими образами у синтаксичному моноїді множини X. Для спільного використання називатимемо *регулярними* розпізнавані множини вільного моноїда A^*. Теорема 1.4.13 стверджує, що регулярні множини та раціональні множини збігаються у випадку скінченних алфавітів.

Наслідок 1.4.14. *Сім'я регулярних множин над скінченним автоматом є замкненою стосовно булевих операцій, раціональних операцій, образів і прообразів при морфізмах, та лівих і правих частках довільних множин.*

Описання раціональної множини через об'єднання, добуток та $*$-операцію називається *раціональним* або *регулярним зображенням*. Наприклад, множина X усіх слів над алфавітом $\{a, b\}$, які містять парну кількість літери a, має раціональне зображення $X = (b \cup ab^*a)^*$. Рівняння (1.10)–(1.12) забезпечують ефективну процедуру обчислення раціонального зображення для множини, які розпізнаються деяким скінченним автоматом.

Приклад 1.4.15 (продовження прикладу 1.4.2)**.** Множина X слів з суфіксом aba над алфавітом $A = \{a, b\}$ має регулярне зображення A^*aba. Рівняння (1.10)–(1.12), застосовані до автомату зображеному на рис. 1.5, приводять до тої ж множини слів до регулярного зображення

$$b^*a(a \cup b(ab)^*a \cup b(ab)^*aa)^*b(ab)^*a.$$

1.5 Перетворювачі

Перетворювач $\mathcal{T} = (Q, I, T)$ над вхідним алфавітом A та вихідним алфавітом B складається з множини Q станів разом з двома виділеними підмножинами I та T множини станів Q називається множинами *початкових* і *кінцевих* станів, і множини E переходів, яка є наборами (p, u, v, q), де p і q — стани, u — слово над алфавітом A та v — слово над алфавітом B. Перехід також позначається через

$$p \xrightarrow{u|v} q.$$

Перетворювач називається *скінченним*, якщо множина його станів скінченна.

Як і в автоматах, *шляхом* у перетворювачі $\mathcal{T}$ називається послідовність

$$c = (f_1, f_2, \ldots, f_n)$$

послідовності переходів

$$f_i = (q_i, u_i, v_i, q_{i+1}), \qquad 1 \leqslant i \leqslant n.$$

У цьому випадку натуральне число n називається *довжиною* шляху c. Слово

$$w = u_1 u_2 \cdots u_n$$

називається *вхідною міткою* шляху c, а слово

$$z = v_1 v_2 \cdots v_n$$

— *вихідною міткою* шляху c. Стан $p = q_1$ називається *початком* шляху c, а стан $q = q_{n+1}$ — *кінцем* шляху c. У цьому випадку ми використовуватимо позначення

$$c\colon p \xrightarrow{w|z} q.$$

Шлях $i \xrightarrow{x|y} t$ називається *успішним*, якщо i є початковим станом, а t є кінцевим станом.

Перетворювач $\mathcal{T}$ визначає бінарне відношення між словами над двома алфавітами наступним чином. Пара (x, y) належить цьому відношенню якщо вона є міткою успішного шляху. Таке відношення називається відношенням *реалізованим* перетворювачем $\mathcal{T}$. Це відношення можна уявляти, як многозначне відображення з вхідних слів у вихідні слова, і також як многозначне відображення з вихідних слів у вхідні слова.

Перетворювач називається *літерним*, якщо кожна вхідна мітка є літерою. Будемо говорити, що перетворювач є *з простим входом*, якщо для довільної пари переходів

$$(p, u, v, q), \quad (p, u', v', q)$$

з однаковими початком і кінцем, з рівності $u = u'$ випливає рівність $v = v'$. Це гарантує, що у випадку коли стерти вихідні мітки, то не буде багатозначних переходів.

Літерний перетворювач з простим входом природно визначає автомат над його вхідним алфавітом, називається його *вхідним автоматом*, отриманий забування вихідних міток.

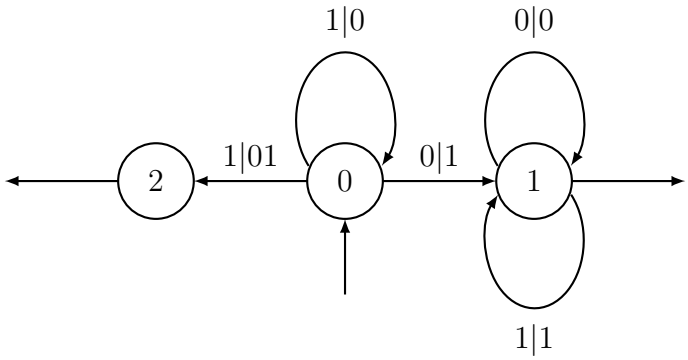


Рис. 1.6: Перетворювач, який додає 1 до числа, заданого у двійковій системі, з бітом найвищої ваги справа.

Приклад 1.5.1. Перетворювач, зображений на рис. 1.6 має два кінцевих стани 1 і 2. Лише успішні шляхи з 0 до 2 мають мітки

$$(1^n, 0^n 1)$$

і успішні шляхи з 0 до 1 мають мітки

$$(1^n 0w, 0^n 1w)$$

для деякого натурального числа n і деякого слова w. Таким чином, перетворювач відображає бінарні зображення додатних цілих чисел N в бінарні зображення множини $N + 1$. Цей перетворювач є літерним і з простим входом.

1.6 Напівкільця та матриці

Множина K із заданими на ній двома операціями "$+$" і "$\cdot$", що задовольняють такі властивості:

(i) множина K є комутативним моноїдом стосовно операції "$+$" (що називається адитивною) з одиницею, яка позначається через 0;
(ii) множина K є моноїдом стосовно операції "$\cdot$" (що називається мультиплікативною) з одиницею, яка позначається через 1;
(iii) операція "$\cdot$" є дистрибутивною стосовно адитивної операції "$+$";
(iv) $0 \cdot x = x \cdot 0 = 0$, для всіх $x \in K$,

називається *напівкільцем*.

Очевидно, що кожне кільце є напівкільцем. Наведемо інші приклади напівкілець. Множини натуральних чисел $\mathbb{N}$ та множина невід'ємних дійсних чисел $\mathbb{R}_+$ з індукованими зі звичайного кільця дійсних чисел, є напікільцями.

Булеве напівкільце $\mathcal{B}$ складається з двох елементів 0 і 1, та з операціями

$$0 + 0 = 0, \quad 0 + 1 = 1 + 0 = 1, \quad 0 \cdot 1 = 1 \cdot 0 = 0 \cdot 0 = 0.$$

Напівкільце $\mathcal{B}$ точно визначається рівністю

$$1 + 1 = 1.$$

Іншим можливим значенням для адитивної операції є $1+1 = 0$, і ця рівність визначає поле $\mathbb{Z}/2\mathbb{Z}$.

Більш загально, для довільного цілого числа $d \geqslant 0$ розглянемо множину

$$\mathcal{B}(d) = \{0, 1, \ldots, d+1\}.$$

Множина $\mathcal{B}(d)$ є напівкільцем стосовно адитивної та мультиплікативної операцій, які визначаються, відповідно, так:

$$\min\{i + j, d + 1\} \qquad \text{і} \qquad \min\{i \cdot j, d + 1\}, \qquad \text{для} \quad i, j \in \mathcal{B}(d).$$

Зокрема маємо, що $\mathcal{B}(0) = \mathcal{B}$.

Для довільного моноїда M множина $\mathfrak{P}(M)$ є напівкільцем стосовно операцій об'єднання та поточкового множення в моноїді M.

Напівкільце K називається *впорядкованим*, якщо на K визначено частковий порядок $\leq$, який задовольняє такі умови:

(i) 0 — найменший елемент в $(K, \leq)$;
(ii) виконуються такі імплікації:

$$x \leq y \qquad \Longrightarrow \qquad x + z \leq y + z,$$

$$x \leq y \qquad \Longrightarrow \qquad x \cdot z \leq y \cdot z, \quad z \cdot x \leq z \cdot y.$$

Впорядковане напівкільце K називається *повним*, якщо для довільної непорожньої підмножини X в K існує її точна верхня грань в K. Це є єдиний елемент k кільця K такий, що

(*i*) $x \in X \quad \Longrightarrow \quad x \leq k$;
(*ii*) якщо $x \leq k'$ для всіх $x \in X$, то $k \leq k'$.

У цьому випадку писатимемо $k = \sup(X)$, або $k = \sup\{x\colon x \in X\}$, або $k = \sup_{x\in X}(x)$.

Напівкільце $\mathcal{B}$ є повним. Напівкільця $\mathbb{N}$ і $\mathbb{R}_+$ не є повними, але їх можна поповнити наступним чином. Для $K = \mathbb{N}$ або $K = \mathbb{R}_+$ покладемо

$$\mathcal{K} = K \cup \{\infty\},$$

де $\infty \notin K$. Операції напівкільця K продовжимо до $\mathcal{K}$, поклавши для кожного елемента $x \in K$:

(*i*) $x + \infty = \infty + x = \infty$;
(*ii*) якщо $x \neq 0$, то $x\infty = \infty x = \infty$;[7]
(*iii*) $\infty\infty = \infty$ і $0\infty = \infty 0 = 0$.

Продовживши порядок напівкільця K до $\mathcal{K}$ поклавши $x \leq \infty$ для всіх $x \in K$, отримуємо, що множина $\mathcal{K}$ є лінійно впорядкованим кільцем. $\mathcal{K}$ є повним напівкільцем, оскільки довільна підмножина в $\mathcal{K}$ є обмеженою зверху, а отже має точну верхню грань.

Означимо

$$\mathcal{N} = \mathbb{N} \cup \{\infty\} \qquad \text{і} \qquad \mathcal{R}_+ = \mathbb{R}_+ \cup \{\infty\}$$

є повними напівкільцями отриманими застосуванням вище викладеної конструкції до напівкілець $\mathbb{N}$ і $\mathbb{R}_+$, відповідно. Якщо $\mathcal{K}$ — повне напівкільце, то сума нескінченної сім'ї $\{x_i\}_{i\in I}$ елементів напівкільця $\mathcal{K}$ визначається так

$$\sum_{i\in I} x_i = \sup\left\{\sum_{j\in J} x_j\colon J \ - \ \text{скінченна множина в } I\right\}. \tag{1.13}$$

У випадку напівкільця $\mathcal{R}_+$ це означення дає звичайне поняття сумовної сім'ї: сім'я $\{x_i\}_{i\in I}$ елементів напівкільця $\mathcal{R}_+$ є *сумовною*, якщо сума (1.13) є скінченною.

Зокрема, для послідовності $\{x_n\}_{n\geqslant 0}$ елементів повного кільця ми маємо

$$\sum_{n\geqslant 0} x_n = \sup_{n\geqslant 0}\left\{\sum_{i\geqslant n} x_i\right\}, \tag{1.14}$$

оскільки кожна скінченна підмножина натуральних чисел $\mathbb{N}$ міститься в деякому інтервалі $\{0, 1, \ldots, n\}$. Більше того, якщо $I = \bigcup\limits_{j\in J} I_j$ — розбиття індексуючої множини I, то

$$\sum_{i\in I} x_i = \sum_{j\in J}\left(\sum_{i\in I_j} x_i\right). \tag{1.15}$$

Нехай P і Q — довільні непорожні множини і K — напівкільце. $P \times Q$-*матрицею* з коефіцієнтами з напівкільця K називається відображення

$$m\colon P \times Q \to K.$$

[7] Надалі для спрошення викладу, як і в теорії напівгруп, опускатимемо символ "$\cdot$" мультиплікативної операції в напівкільці.

Ми позначатимемо через

$$(p, m, q) \qquad \text{або} \qquad m_{p,q}$$

значення відображення m в точці $(p, q) \in P \times Q$. Також ми говоритимемо, що m є *K-відношенням* між множинами P та Q. Якщо $P = Q$, то будемо говорити, що m є *K-відношенням* над множиною Q. Множина усіх K-відношень між множинами P та Q позначається через

$$K^{P \times Q}$$

Нехай $m \in K^{P \times Q}$ — K-відношення між непорожніми множинами P та Q. Для $p \in P$ *рядок* індексу p $P \times Q$-матриці m позначатимемо через m_{p*}. Він є елементом множини K^Q і визначений за формулою

$$(m_{p*})_q = m_{p,q}.$$

Аналогічно, *стовпець* індексу q $P \times Q$-матриці m позначатимемо через m_{*q}, і він є елементом множини K^P.

Нехай P, Q і R — довільні три непорожні множини ш K — довільне повне напівкільце. Для $m \in K^{P \times Q}$ і $n \in K^{Q \times R}$ добуток mn визначається як елемент множини $K^{P \times R}$ так. Значення цього добутку на елементі $(p, r) \in P \times R$ дорівнює

$$(mn)_{p,r} = \sum_{q \in Q} m_{p,q} n_{q,r}.$$

У випадку, коли $P = Q = R$, то з отриманою так асоціативною бінарною операцією множина $K^{Q \times Q}$ є моноїдом. Одиницю цього моноїда позначатимемо через id_Q або I_Q.

Моноїдом K-відношень над множиною Q називається підмоноїд моноїда $K^{Q \times Q}$. Він зокрема містить одиницю id_Q.

1.7 Формальні ряди

Нехай A — алфавіт K — напівкільце. *Формальним рядом* (або просто *рядом*) над алфавітом A з коефіцієнтами в напівкільці K називається відображення

$$\sigma\colon A^* \to K.$$

Значення формального ряду σ в слові $w \in A^*$ позначатимемо через (σ, w). Надалі через K^{A^*} та $K\langle\langle A\rangle\rangle$ позначатимемо множину усіх формальних рядів над алфавітом A з коефіцієнтами в напівкільці K. Через $K\langle A\rangle$ позначатимемо множину усіх формальних рядів $\sigma \in K\langle\langle A\rangle\rangle$ таких, що $(\sigma, w) = 0$ для всіх, крім скінченної кількості слів $w \in A^*$. Елемент множини $K\langle A\rangle$ називається *поліномом* або *многочленом* над алфавітом A з коефіцієнтами в напівкільці K. *Степінь полінома* $p \neq 0$ — це максимальна довжина слова $w \in A^*$ такого, що $(p, w) \neq 0$. Степінь полінома p позначається через $\deg(p)$. Степінь 0-полінома, тобто такого полінома p, що $p = 0$, дорівнює $-\infty$.

Формальний ряд $\sigma \in K\langle\langle A\rangle\rangle$ можна продовжити до лінійного відображення з $K\langle A\rangle$ в напівкільце K, поклавши

$$(\sigma, p) = \sum_{w \in A^*} (\sigma, w)(p, w),$$

для $p \in K\langle A\rangle$. Таке продовження є коректним, оскільки p є поліномом. Нехай $\sigma, \tau \in K\langle\langle A\rangle\rangle$ і $k \in K$. Означимо формальні ряди $\sigma + \tau$, $\sigma\tau$ і $k\sigma$ так:

$$(\sigma + \tau, w) = (\sigma, w) + (\tau, w), \tag{1.16}$$

$$(\sigma\tau, w) = \sum_{uv = w} (\sigma, u)(\tau, v), \tag{1.17}$$

$$(k\sigma, w) = k(\sigma, w). \tag{1.18}$$

У формулі (1.17) сума виконується над $1 + |w|$ парами (u, v) такими, що $w = uv$, а отже вона є скінченною сумою. Множина $K\langle\langle A\rangle\rangle$ містить два спеціальних елементи, які позначаються через 0 і 1, та визначаються так:

$$(0, w) = 0 \qquad \text{і} \qquad (1, w) = \begin{cases} 1, & \text{якщо } w = 1; \\ 0, & \text{в інших випадках.} \end{cases}$$

Зазвичай, ми позначатимемо $\sigma^n = \underbrace{\sigma\sigma\cdots\sigma}_{n\text{-разів}}$ і $\sigma^0 = 1$ для довільного формального ряду $\sigma \in K\langle\langle A\rangle\rangle$. Стосовно операцій визначених формулами (1.16) і (1.17) множина $K\langle\langle A\rangle\rangle$ є напівкільцем. Також, можна показати, якщо K — повне впорядковане напівкільце, то $K\langle\langle A\rangle\rangle$ також є повним впорядкованим напівкільцем.

Носієм формального ряду $\sigma \in K\langle\langle A\rangle\rangle$ називається множина

$$\operatorname{supp}(\sigma) = \{w \in A^*\colon (\sigma, w) \neq 0\}.$$

Відображення $\sigma \mapsto \operatorname{supp}(\sigma)$ є ізоморфізмом з напівкільця $\mathcal{B}\langle\langle A\rangle\rangle$ на напівкільце $\mathfrak{P}(A^*)$.

Сім'я $\{\sigma_i\}_{i\in I}$ формальних рядів називається *локально скінченною*, якщо для кожного слова $w \in A^*$ множина $\{i \in I\colon (\sigma_i, w) \neq 0\}$ є скінченною. У цьому випадку формальний ряд σ позначений

$$\sigma = \sum_{i\in I} \sigma_i$$

може бути визначений за формулою

$$(\sigma, w) = \sum_{i\in I} (\sigma_i, w). \tag{1.19}$$

Це означення є коректним, оскільки в сумі (1.19) лише скінченна кількість виразів відмінна від 0. Звичайною перевіркою доводиться, що для локально скінченної сім'ї $\{\sigma_i\}_{i\in I}$ елементів множини $K\langle\langle A\rangle\rangle$ та для довільного елемента τ з $K\langle\langle A\rangle\rangle$ виконується рівність

$$\tau\left(\sum_{i\in I} \sigma_i\right) = \sum_{i\in I} \tau\sigma_i.$$

Постійним термом формального ряду $\sigma \in K\langle\langle A\rangle\rangle$ називається елемент $(\sigma, 1)$ напівкільця K. Якщо формальний ряд σ має нульовий постійний терм, то сім'я $\{\sigma^n\}_{n\geqslant 0}$ є локально скінченною, оскільки носій формального ряду σ^n не містить слів довжини менше за n. Позначимо

$$\sigma^* = \sum_{n\geqslant 0} \sigma^n \qquad \text{і} \qquad \sigma^+ = \sum_{n\geqslant 1} \sigma^n.$$

Формальний ряд σ^* називається *зіркою* формального ряду σ. Зауважимо, що виконуються рівності

$$\sigma^* = 1 + \sigma^+ \qquad \text{і} \qquad \sigma^*\sigma = \sigma\sigma^* = \sigma^+.$$

Твердження 1.7.1. *Нехай K — кільце з одиницею і $\sigma \in K\langle\langle A\rangle\rangle$ — формальний ряд такий, що $(\sigma, 1) = 0$. Тоді елемент $1 - \sigma$ оборотний і*

$$\sigma^* = (1 - \sigma)^{-1}. \tag{1.20}$$

Доведення. Маємо

$$1 = \sigma^* - \sigma^+ = \sigma^* - \sigma^*\sigma = \sigma^*(1 - \sigma),$$

і симетрично

$$1 = \sigma^* - \sigma^+ = \sigma^* - \sigma\sigma^* = (1 - \sigma)\sigma^*,$$

що завершує доведення твердження. □

Для довільної непорожньої підмножини Z вільного моноїда A^* через $\underline{X}$ позначимо *характеристичний ряд* множини X, який визначається так

$$(\underline{X}, x) = \begin{cases} 1, & \text{якщо } x \in X; \\ 0, & \text{в інших випадках.} \end{cases}$$

Ми розглянемо характеристичний ряд $\underline{X}$ множини X як елемент напівкільця $\mathbb{N}\langle\langle A\rangle\rangle$. Коли $X = \{x\}$ ми зазвичай писатимемо x замість $\underline{x}$. Зокрема, оскільки сім'я $\{\underline{x}\}_{x\in X}$ є локально скінченною, то маємо

$$\underline{X} = \sum_{x\in X} x.$$

Більш загально, для довільного формального ряду $\sigma \in K\langle\langle A\rangle\rangle$ маємо, що

$$\sigma = \sum_{w \in A^*} (\sigma, w) w.$$

Твердження 1.7.2. *Нехай X і Y — непорожні підмножини вільного моноїда A^*. Тоді*

$$(\underline{X} + \underline{Y}, w) = \begin{cases} 0, & \text{якщо } w \notin X \cup Y; \\ 1, & \text{якщо } w \in (X \setminus Y) \cup (Y \setminus X); \\ 2, & \text{якщо } w \in X \cap Y. \end{cases}$$

Зокрема, для $Z = X \cup Y$ маємо

$$\underline{X} + \underline{Y} = \underline{Z} \qquad \text{тоді і лише тоді, коли} \qquad X \cap Y = \varnothing.$$

Для двох непорожніх підмножин X і Y вільного моноїда A^* добуток XY називається *однозначним*, якщо слово $w \in XY$ має лише одну факторизацію $w = uv$ з $x \in X$, $y \in Y$.

Твердження 1.7.3. *Нехай X і Y — непорожні підмножини вільного моноїда A^*. Тоді*

$$(\underline{X}\,\underline{Y}, w) = \operatorname{Card}\{(x, y) \in X \times Y \colon w = xy\}$$

Зокрема, для $Z = XY$ маємо

$$\underline{X}\,\underline{Y} = \underline{Z} \qquad \text{тоді і лише тоді, коли добуток } XY \text{ є однозначним.}$$

Наступне твердження дуже близько наближається до основного предмета цього курсу лекцій. У ному описані коефіцієнти зірки характеристичного ряду.

Твердження 1.7.4. *Якщо X — непорожня підмножина вільної напівгрупи A^+, то*

$$((\underline{X})^*, w) = \operatorname{Card}\{(x_1, x_2, \ldots, x_n) \colon n \geqslant 0,\ x_i \in X,\ w = x_1 x_2 \cdots x_n\}. \tag{1.21}$$

Доведення. За означенням моноїда $(\underline{X}^*)$ маємо, що

$$((\underline{X})^*, w) = \sum_{k \geqslant 0} \left((\underline{X})^k, w\right).$$

Застосувавши твердження 1.7.3, отримуємо

$$\left((\underline{X})^k, w\right) = \operatorname{Card}\{(x_1, x_2, \ldots, x_k) \colon x_i \in X,\ w = x_1 x_2 \cdots x_k\},$$

звідки отримуємо формулу (1.21). □

Приклад 1.7.5. Формальні ряди $\underline{A^*}$ й $\underline{A}^*\underline{A}^*$ задовольняють рівності

$$\underline{A^*} = (1 - \underline{A})^{-1} = \sum_{w \in A^*} w \qquad \text{і} \qquad (\underline{A}^*\underline{A}^*, w) = 1 + |w|.$$

Тепер означимо *добуток Адамара двох рядів* двох рядів $\sigma, \tau \in K\langle\langle A\rangle\rangle$ як ряд $\sigma \odot \tau$, який визначається наступним чином

$$(\sigma \odot \tau, w) = (\sigma, w)(\tau, w).$$

Так визначений добуток двох формальних рядів є дистрибутивний стосовно адитивної операції напівкільця, тобто $\sigma \odot (\tau + \tau') = \sigma \odot \tau + \sigma \odot \tau'$. Якщо напівкільце K задовольняє умову

$$xy = 0 \qquad \Longrightarrow \qquad x = 0 \quad \text{або} \quad y = 0,$$

то

$$\operatorname{supp}(\sigma \odot \tau, w) = \operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau).$$

Зокрема, для підмножин X і Y вільного моноїда A^* і $Z = X \cap Y$ маємо

$$\underline{Z} = \underline{X} \odot \underline{Y}.$$

Для двох формальних рядів $\sigma, \tau \in \mathbb{Z}\langle\langle A\rangle\rangle$ ми писатимемо $\sigma \leq \tau$ у випадку $(\sigma, w) \leq (\tau, w)$ для всіх слів $w \in A^*$.

Нехай A — довільний алфавіт і K — довільне напівкільце. Через $K[[A]]$ позначимо *множину усіх формальних рядів з комутативними змінними над алфавітом A з коефіцієнтами з напівкільця K*. Тоді $K[[A]]$ є множиною усіх відображень x вільного комутативного моноїда $A^{\oplus}$ в напівкільце K.

Канонічний морфізм $\alpha\colon A^* \to A^{\oplus}$ лінійно продовжується до морфізму з $K\langle\langle A\rangle\rangle$ в $K[[A]]$. Образ формального ряду $\sigma \in K\langle\langle A\rangle\rangle$ стосовно морфізму α визначається для слова $w \in A^{\oplus}$ за формулою

$$(\alpha(\sigma), w) = (\sigma, \alpha^{-1}(w)) = \sum_{\alpha(v)=w} (\sigma, v).$$

Множину усіх комутативних поліномів над алфавітом A з коефіцієнтами з напівкільця K позначатимемо через $K[A]$.

1.8 Степеневі ряди

Степеневим рядом зі змінною t, який пов'язаний з послідовністю a_n дійсних чисел, називається формальна сума

$$f(t) = \sum_{n\geqslant 0} a_n t^n.$$

Нехай r — фіксоване дійсне число. Будемо говорити, що *ряд збігається* для значення r змінної t, якщо сума $\sum_{n\geqslant 0} a_n r^n$ є коректно визначеною та скінченною. У протилежному випадку, кажемо, що $f(t)$ є *розбіжним* для $t = r$. *Радіус збіжності* степеневого ряду $f(t)$ є нескінченним, якщо $f(t)$ збігається для всіх дійсних чисел r. В іншому випадку це невід'ємне дійсне число ρ таке, що $f(t)$ збігається для $0 \leqslant r < \rho$ і розбігається для $r > \rho$. Можна показати, що $\rho = \lim\limits_{n\to\infty} \inf |a_n|^{\frac{1}{n}}$. Степеневий ряд може збігатися, чи розбігатися у випадку $t = \rho$.

У випадку $0 \leqslant r < \rho$ ряд збігається. Таким чином, визначене відображення з $[0, \rho)$ в множину невід'ємних дійсних чисел. Наприклад, ряд $\sum_{n\geqslant 0} t^n$ визначає на інтервалі $[0, 1)$ раціональну функцію $t \mapsto \dfrac{1}{1-t}$.

Приклад 1.8.1. Для довільного додатнього дійсного числа α радіус збіжності степеневого ряду $\sum_{n\geqslant 0} \dfrac{t^n}{n^\alpha}$ дорівнює 1. Відомо, що він розбігається для $t = 1$ і збігається коли $\alpha < 2$ і збігається у випадку $\alpha \geqslant 2$.

Степеневі ряди, які розглядаються в цьому підрозділі, є спеціальним класом формальних рядів, які розглядались у підрозділі 1.7, коли алфавіт є одноточковою множиною. Зокрема, звичайні операції суми, добутку та зірки виконуються і в цьому випадку.

Нехай X — множина слів над алфавітом A. *Породжуючим рядом* множини X називається степеневий ряд

$$f_X(t) = \sum_{n\geqslant 0} \mathrm{Card}(X \cap A^n) t^n.$$

Позаяк для всіх $n \geqslant 0$, виконується нерівність $\mathrm{Card}(X \cap A^n) \leqslant k^n$, де $k = \mathrm{Card}(A)$, то отримуємо, що радіус збіжності степеневого ряду f_X щонайменше дорівнює $1/k$. Послідовність $(u_n)_{n\geqslant 0}$, де $u_n = \mathrm{Card}(X \cap A^n)$ називається *розподілом довжини* множини X.

Твердження 1.8.2. *Нехай $f(t) = \sum a_n t^n$ — степеневий ряд з невід'ємними дійсними коефіцієнтами та зі скінченним радіусом збіжності ρ. Нехай $g(t)\colon [0, \rho) \to \mathbb{R}^+$ — функція, визначена для $r \in [0, \rho)$ за формулою $g(r) = \sum a_n r^n$. Тоді*

$$f(\rho) = \lim_{r\to\rho, r<\rho} g(r).$$

Зокрема, обидві величини є одночасно скінченними або нескінченними.

Доведення. Спочатку припустимо, що степеневий ряд $f(t)$ збігається для $t = \rho$, і покладемо $s = f(\rho)$. Для довільного $\varepsilon > 0$ існує натуральне число N таке, що

$$s_N = a_0 + a_1\rho + \ldots + a_N\rho^N$$

задовольняє нерівність $s \geqslant s_N > s - \varepsilon/2$. Покладемо

$$p(t) = a_0 + a_1 t + \ldots + a_N t^N.$$

Тоді існує дійсне число $r < \rho$ таке, що $s_N \geqslant p(t) > s_N - \varepsilon/2$. Для $r \leqslant x < \rho$, отримуємо

$$f(\rho) \geqslant f(x) = g(x) \geqslant g(r) > p(r) > s_N - \varepsilon/2 \geqslant f(\rho) - \varepsilon.$$

Звідси випливає, що $g(x)$ наближається до $f(\rho)$, коли x наближається до ρ.

Далі, якщо величина $f(\rho)$ є нескінченною, то для довільного числа $M > 0$ існує натуральне число N таке, що

$$s_N = a_0 + a_1\rho + \ldots + a_N\rho^N > 2M.$$

Покладемо знову

$$p(t) = a_0 + a_1 t + \ldots + a_N t^N.$$

Тоді існує дійсне число $r < \rho$ таке, що $p(r) > s_N/2$. Для $r \leqslant x < \rho$, отримуємо

$$f(x) = g(x) \geqslant g(r) > p(r) > s_N/2 \geqslant M.$$

Звідси випливає, що $g(x)$ наближається до нескінченності у випадку, коли x наближається до ρ. □

Отже, для степеневого ряду $f(t) = \sum\limits_n a_n t^n$ з невід'ємними коефіцієнтами і радіусом збіжності ρ, ми можемо позначити, виразом $f(r)$, для $0 \leqslant r \leqslant \rho$, суму $\sum\limits_n a_n r^n$ і значення функції, визначеної через f для $t = r$, з тією властивістю, що ці обидва значення є одночасно скінченними або нескінченними.

Зауважимо, що це твердження виконується тільки тому, що коефіцієнти a_n є невід'ємними. Справді, розглянемо для прикладу ряд

$$f(t) = \sum_n (-1)^n t^n.$$

Радіус збіжності цього ряду дорівнює 1, і $g(t) = \dfrac{1}{1+t}$. Ми маємо $g(1) = 1/2$, хоча ряд $f(t)$ розбігається для $t = 1$.

Степеневий ряд

$$f(t) = \sum_{n \geqslant 0} a_n t^n$$

з дійсними коефіцієнтами можна отримати формально. Результатом є наступний степеневий ряд

$$\sum_{n \geqslant 0} a_n t^{n-1},$$

який ми позначатимемо через $f'(t)$. Нехай ρ — радіус збіжності ряду f. Для $r < \rho$ значення $f'(r)$ дорівнює значенню в точці r похідної функції, визначеної степеневим рядом f.

З твердження 1.8.2 випливає

Твердження 1.8.3. *Нехай* $f(t) = \sum_{n\geqslant 0} a_n t^n$ *— степеневий ряд з невід'ємними дійсними коефіцієнтами. Нехай* ρ *— радіус збіжності ряду* f*. Тоді*

$$f'(\rho) = \sum_{n\geqslant 0} n a_n \rho^{n-1}.$$

Наступне твердження дає метод обчислення радіуса збіжності зірки степеневого ряду.

Твердження 1.8.4. *Нехай* $f(t) = \sum a_n t^n$ *— степеневий ряд з невід'ємними дійсними коефіцієнтами і з постійним термом нуль. Розглянемо степеневий ряд*

$$g(t) = \frac{1}{1 - f(t)} = \sum_{n=0}^{\infty} f(t)^n,$$

який є зіркою степеневого ряду $f(t)$*, і позначимо через* ρ_f *і* ρ_g *радіуси збіжності рядів* f *і* g*, відповідно. Тоді* $\rho_g \leqslant \rho_f$*, і якщо* $\rho_g < \rho_f$*, то* ρ_g *є єдиним додатнім дійсним числом таким, що* $f(\rho_g) = 1$*.*

Доведення. Коефіцієнти ряду $g(t)$ є більшими, або рівними за відповідні коефіцієнти ряду $f(t)$, а отже виконується нерівність $\rho_g \leqslant \rho_f$. Припустимо тепер, що $\rho_g < \rho_f$. Тоді ряд $f(t)$ збігається для $r = \rho_g$. Використовуємо той факт, що ряд $f(t)$ визначає неперервну функцію в її інтервалі збіжності.

Припустимо спочатку, що $f(r) < 1$. Тоді існує дійсне число s з $r < s < \rho_f$ таке, що $f(s) < 1$. Звідси випливає, що $g(s) < \infty$, що суперечить тому, що $s > \rho_g$.

Припустимо, що $f(r) > 1$. Тоді існує дійсне число s з $0 < s < r$ таке, що $f(s) > 1$. Звідси випливає, що $g(s) = \infty$, що суперечить тому, що $s < \rho_g$.

Таким чином, отримуємо, що $f(r) = 1$. □

1.9 Невід'ємні матриці

Ми тепер розглянемо властивості невід'ємних матриць. Нехай Q — множина індексів. Для двох Q-векторів v і w з дійсними координатами, ми писатимемо $v \leqslant w$, якщо $v_q \leqslant w_q$ для всіх $q \in Q$ і $v < w$, якщо $v_q < w_q$ для всіх $q \in Q$. Вектор v будемо називати *невід'ємним* (відп. *додатнім*), якщо $v \geqslant 0$ (відп. $v > 0$). Тут і надалі ми позначатимемо через 0 нуль-вектор або нуль-матрицю відповідного розміру. Аналогічно, для двох $Q \times Q$-матриць M і N з дійсними коефіцієнтами, ми писатимемо $M \leqslant N$, коли $M_{p,q} \leqslant N_{p,q}$ для всіх $p, q \in Q$ і $M < N$, якщо $M_{p,q} < N_{p,q}$ для всіх $p, q \in Q$. $Q \times Q$-матриця M називається *невід'ємною* (відп. *додатною*), якщо $M \geqslant 0$ (відп. $M > 0$). Часто будемо використовувати елементарний факт, якщо $M > 0$ і $v \geqslant 0$ з $v \neq 0$, то $Mv > 0$.

Комплексне число λ називається *власним значенням* матриці M, якщо матриця $\lambda I - M$ не є оборотною. У цьому випадку існують вектори $v, w \neq 0$ такі, що $Mv = \lambda v$ і $wM = \lambda w$. Вектори w і називаються *лівим* і *правим власним вектором*, які відповідають власному значенню λ. *Спектральним радіусом* матриці називається модуль її власних значень.

Невід'ємна матриця M називається *стохастичною*, якщо сума її елементів на кожному рядку дорівнює 1. Еквівалентно матриця є стохастичною, якщо вектор v з усіма компонентами, що дорівнюють 1 є (правим) власним вектором для власного значення 1.

Твердження 1.9.1. *Спектральний радіус стохастичної матриці дорівнює* 1.

Доведення. Нехай λ — власне значення стохастичної $n \times n$-матриці M і v — її правий власний вектор. Розділивши всі компоненти векторoа v на максимум їх модуля, можемо вважати, що $|v_j| \leqslant 1$ для $1 \leqslant j \leqslant n$ і $|v_i| = 1$ для деякого i. Тоді з рівності $\lambda v_i = \sum_{i=1}^{n} M_{ij} v_j$ випливає, що

$$|\lambda| \leqslant \sum_{i=1}^{n} M_{ij} |v_j| \leqslant \sum_{i=1}^{n} M_{ij} = 1,$$

що і треба було довести. □

Матрицею переходів автомата $\mathcal{A}$ над алфавітом A з множиною станів Q називається $Q \times Q$-матриця M з коефіцієнтами

$$M_{p,q} = \operatorname{Card} \{a \in A \colon p \cdot a = q\}.$$

Нехай $k = \operatorname{Card} A$. Матриця M/k є стохастичною. Відповідний правий власний вектор є вектором, у якого всі компоненти дорівнюють 1. Він також є власним вектором матриці M для власного значення k. За твердженням 1.9.1, спектральний радіус матриці M/k дорівнює 1, і таким чином спектральний радіус матриці M дорівнює k.

Якщо M — матриця суміжності графа G, то корисним способом уяви про власний вектор v матриці M є те, що він присвоює кожній вершині q вагу v_q. Рівність $Mv = \lambda v$ відповідає умові, що для кожної вершини p, якщо скласти ваги кінців всіх ребер, що починаються з вершини p, ця сума дорівнює λ разів ваги вершини p.

Невід'ємну матрицю M називають *незвідною*, якщо для довільних індексів p і q існує ціле число k, таке, що $M^k_{p,q} > 0$, де через M^k позначається k-а степінь матриці M. У протилежному випадку матрицю M називається *звідною*. Легко переконатися, що матриця M є незвідною тоді і тільки тоді, коли $(I + M)^n > 0$, де n — розмірність матриці M. Також легко довести, що матриця M є звідною, якщо існує перестановка індексів така, що M в ній стає блочно трикутною, тобто має вигляд

$$M = \begin{bmatrix} U & V \\ 0 & W \end{bmatrix}, \tag{1.22}$$

де U і W — матриці розмірності > 0.

Наступний твердження є частиною теореми, відомої як теорема Перрона–Фробеніуса. Воно, зокрема, стверджує, що спектральний радіус невід'ємної матриці є її власним значенням.

Теорема 1.9.2 (**теорема Перрона–Фробеніуса**). *Будь-яка невід'ємна матриця M має дійсне власне значення ρ_M таке, що $|\lambda| \leqslant \rho_M$ для будь-якого власного значення λ_M, і в цьому випадку власному значенню ρ_M відповідає невід'ємний власний вектор v. Якщо матриця M є незвідною, то власному значенню ρ_M відповідає додатній власний вектор v.*

Зауважимо, що такий самий результат виконується як для правого, так і для лівого власних векторів.

Перед доведенням теореми 1.9.2 ми викладемо результат незалежного характеру, який буде використаний у доведенні цієї теореми. Послідовність $(M_n)_{n\geqslant 0}$ дійснозначних $m \times m$-матриць називається *збіжною*, якщо, поклавши $M_n = \left(a^{(n)}_{p,q}\right)$, кожна з дійсних послідовностей $\left(a^{(n)}_{p,q}\right)_{n\geqslant 0}$ збігається. Будемо говорити, що ряд $\sum M_n$ матриць *збігається*, якщо послідовність $(S_m)_{m\geqslant 0}$, яка визначається

$$S_m = \sum_{n\leqslant m} M_n,$$

збігається.

Твердження 1.9.3. *Нехай M — $m \times m$-матриця з дійсними коефіцієнтами. Якщо спектральний радіус ρ матриці M задовольняє умову $\rho < 1$, то ряд $\sum\limits_n M_n$ збігається.*

Доведення. Покладемо $N(z) = I - Mz$, де I — одинична матриця та z — змінна. Многочлен $N(z)$ можна розглядати одночасно, як многочлен з коефіцієнтами в кільці $m \times m$-матриць, або як $m \times m$-матрицю з коефіцієнтами в кільці многочленів з дійсними коефіцієнтами зі змінною z. Многочлен $N(z)$ є оборотним у обидвох структурах, і до нього обернений многочлен

$$N(z)^{-1} = (I - Mz) - 1$$

у свою чергу, можна розглядати як степеневий ряд з коефіцієнтами в кільці $m \times m$-матриць, або як матрицю чиї коефіцієнти є раціональними дробами зі змінною z.

Радіус збіжності оберненої матриці $N(z)^{-1}$, що розглядається як степеневий ряд зі змінною z з матричними коефіцієнтами, дорівнює мінімуму радіуса збіжність елементів матриці $N(z)^{-1}$, розглянутої як матриці степеневого ряду розширення раціональних дробів. Усі ці раціональні дроби мають знаменник $\det(I - Mz)$. Таким чином, цьому радіус збіжності розширення кожного раціонального дробу є не менше ніж $1/\rho$. Отже, радіус збіжності матриці $N(z)^{-1}$ є не менше ніж $1/\rho$. □

Доведення теореми 1.9.2. Спочатку покажемо, що можна звести доведення до випадку, коли матриця M є незвідною. Справді, якщо матриця M є звідною, то ми можемо розглядати її у блочно-трикутний вигляді, як у рівності (1.22). Застосувавши за індукцією теорему до матриць U і W, ми отримуємо невід'ємні власні вектори u і v для власних значень ρ_U і ρ_V матриць U і V. Ми доведемо, що число $\max\{\rho_U, \rho_V\}$ є власним значенням матриці M з деяким невід'ємним власним вектором.

Якщо $\rho_U \geqslant \rho_V$, то ρ_U є власним значенням матриці M з відповідним власним вектором $\begin{bmatrix} u \\ 0 \end{bmatrix}$. Якщо $\rho_U < \rho_V$, то ми показуємо, що ρ_V є власним значенням матриці M для власного вектора $\begin{bmatrix} u' \\ v \end{bmatrix}$, де

$$u' = \left(\sum_{n \geqslant 0} U^n \rho_V^{-n} \right) v = (I - U/\rho_V)^{-1} v.$$

Позаяк $\rho_U < \rho_V$, то ряд $\sum_{n \geqslant 0} U^n \rho_V^{-n}$ збігається за твердженням 1.9.3, і він збігається до матриці з невід'ємними коефіцієнтами, оскільки кожна матриця U^n має невід'ємні коефіцієнти. Звідси випливає, що вектор u' має невід'ємні коефіцієнти. Більше того з

$$Vv = \rho_V v = \rho_V (I - U/\rho_V) u' = \rho_V u' - Uu',$$

отримуємо, що

$$M \begin{bmatrix} u' \\ v \end{bmatrix} = \rho_V \begin{bmatrix} u' \\ v \end{bmatrix}.$$

Це доводить, що $\rho_M \geqslant \max\{\rho_U, \rho_V\}$. Навпаки, якщо λ — власне значення матриці M з відповідним власним вектором $\begin{bmatrix} u \\ v \end{bmatrix}$, то λ є власним значенням матриці W у випадку $v \neq 0$, і λ є власним значенням матриці U у випадку $v = 0$. Це доводить, що

$$\rho_M = \max\{\rho_U, \rho_V\}.$$

Припустимо тепер, що матриця M є незвідною. Для будь-якого невід'ємного Q-вектора $v \neq 0$, покладемо

$$r_M(v) = \min \{(Mv)_i / v_i \colon 1 \leqslant i \leqslant n,\ v_i \neq 0\}.$$

Таким чином, $r_M(v)$ є найбільшим дійсним числом r таким, що $Mv \geqslant rv$. Для довільного дійсного числа $\lambda \neq 0$ маємо $r_M(\lambda v) = r_M(v)$. Більше того, відображення $v \mapsto r_M(v)$ є неперервним на множині невід'ємних ненульових векторів.

Множина X невід'ємних векторів v таких, що $\|v\| = 1$ є компактною. Означимо власне значення $\rho_M = \max\{r_M(w)\colon w \in X\}$. Позаяк кожна дійснозначна неперервна функція на компактній множині набуває свого найбільшого значення на цій множині, то існує елемент $x \in X$ такий, що $r_M(x) = \rho_M$. Позаяк $M(v) = r_M(\lambda v)$ для $\lambda \neq 0$, то отримуємо, що $\rho_M = \max\{r_M(w)\colon w \geqslant 0,\ w \neq 0\}$.

Ми доведемо, що $Mx = \rho_M x$. За означенням відображення r_M маємо, що $Mx \geqslant \rho_M x$. Покладемо $y = Mx - \rho_M x$. Тоді $y \geqslant 0$. Припустимо, що $Mx \neq \rho_M x$. Тоді $y \neq 0$. З нерівності $(I + M)^n > 0$, випливає, що вектор $(I + M)^n y$ є додатнім. Але

$$(I + M)^n y = (I + M)^n (Mx - \rho_M x) = M(I + M)^n x - \rho_M (I + M)^n x = Mz - \rho_M z,$$

де $z = (I + M)^n x$. Це доводить, що $Mz > \rho_M z$, звідки випливає нерівність $rM(z) > \rho_M$, а це суперечить означенню власного значення ρ_M. Таким чином, ρ_M є власним значенням з невід'ємним власним вектором.

Далі покажемо, що $\rho_M \geqslant |\lambda|$ для кожного дійсного або комплексного власного значення λ матриці M. Справді, нехай v — власний вектор, який відповідає власному значенню λ. Тоді $Mv = \lambda v$. Нехай $|v|$ — невід'ємний вектор з координатами $|v_i|$. Тоді $M|v| \geqslant |\lambda||v|$ за нерівністю трикутника. За означенням відображення r_M звідси випливає нерівність $r_M(|v|) \geqslant |\lambda|$, а отже виконується нерівність $\rho_M \geqslant |\lambda|$.

Ми вже довели, що власному значенню ρ_M відповідає невід'ємний власний вектор x. Тепер перевіримо, що $x > 0$. Але це є очевидним, оскільки $(I+M)^n x = (1+\rho_M)^n x$, звідки випливає, що $(1 + \rho_M)^n x > 0$ і отже $x > 0$. □

Приклад 1.9.4. Нехай $M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. Власними значеннями матриці M є числа

$$\varphi = \frac{1 + \sqrt{5}}{2} \qquad \text{і} \qquad \varphi = \frac{1 - \sqrt{5}}{2},$$

які є коренями рівняння $z^2 - z - 1 = 0$. Власному значенню ϖ відповідає невід'ємний лівий власний вектор $[\varphi, 1]$.

Як приклад застосування теореми 1.9.2, отримуємо таке твердження.

Твердження 1.9.5. *Кожна стохастична матриця має невід'ємний лівий власний вектор для власного значення* 1.

Доведення. Нехай M — стохастична матриця. За твердженням 1.9.1, її спектральний радіус дорівнює 1. За теоремою 1.9.2 існує відповідний невід'ємний лівий власний вектор. □

Нагадаємо, що матриця переходів детермінованого автомата над k-літерним алфавіту має радіус збіжності k і має відповідний правий власний вектор з усіма компонентами,що дорівнюють 1. За теоремою 1.9.2, вона також має лівий власний вектор з невід'ємними компонентами, які відповідають власному значенню k.

Нехай k – ціле число. *k-наближений власний вектор* невід'ємної матриці M, за визначенням, є вектор $v \neq 0$ з цілими невід'ємними компонентами такий, що

$$Mv \leqslant kv.$$

Знову, якщо припустити, що M — матриця суміжності графа G, то наближений власний вектор матриці M ставить у відповідність кожній вершині q невід'ємне ціле число v_q, а векторне нерівність $Mv \leqslant kv$ відповідає умові, що для кожної вершини p сума ваг кінців всіх ребер, що починаються при вершині p, є не більша за k разів ваги вершини p. Нам буде потрібне таке твердження.

Твердження 1.9.6. *Нерозкладна невід'ємна матриця M з цілими коефіцієнтами зі спектральним радіусом λ допускає додатній k-наближений власний вектор тоді і лише тоді, коли $k \geqslant \lambda$.*

Доведення. Спочатку припустимо, що $k > \lambda$. Розглянемо матрицю $N = kI - M$. Позаяк $k > \lambda$, то маємо, що $\det(N) > 0$ а отже матриця N є оборотною. Більше того, оскільки

$$N^{-1} = (I + M/k + M^2/k^2 + \ldots)/k$$

і матриця M є нерозкладною, то матриця N^{-1} є додатною. Нехай v — стовпчик матриці N^{-1}. Ми маємо, що $Nv \geqslant 0$, а отже $Mv \leqslant kv$. Тоді кожен стовпчик матриці N^{-1} є додатнім k-наближеним власним вектором матриці M.

Якщо $k = \lambda$, то за теоремою 1.9.2 існує додатній вектор v такий, що $Mv = kv$. Позаяк спектральний радіус λ є цілим числом, то координати вектора v можна вибрати так, шоб вони були цілими числами.

На завершенні доведемо обернене твердження: якщо матриця M опускає додатній вектор такий, що $Mv = kv$, то $k \geqslant \lambda$. Розглянемо матрицю $N = \frac{1}{\lambda}M$. За теоремою 1.9.2 існує додатній вектор w такий, що $Nw = w$. Маємо, що з $Nv \leqslant (k/\lambda)v$ випливає нерівність $N^n v \leqslant (k/\lambda)^n v$ для всіх $n \geqslant 1$. Якщо $\lambda > k$, то права частина цієї нерівності прямує до 0 у випадку, коли $n \to \infty$, а отже матриця N^n прямує до нуль-матриці, а це суперечить тому, що $N^n w = w$ для $w > 0$. □

Приклад 1.9.7. Нехай

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

Спектральний радіус матриці M є строго менше за 2 і $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ є її 2-наближеним власним вектором.

1.10 Вагові автомати

Нехай A — алфавіт. З кожним автоматом $\mathcal{A} = (Q, I, T)$ над алфавітом A з множиною ребер E пов'язана функція

$$\mu_{\mathcal{A}} \colon A \to \mathcal{N}^{Q \times Q},$$

яка визначається за формулою

$$(p, \mu_{\mathcal{A}}(a), q) = \begin{cases} 1, & \text{якщо } (p, a, q) \in E; \\ 0, & \text{в іншому випідку.} \end{cases}$$

Ця функція продовжується до морфізму, який позначатимемо через $\mu_{\mathcal{A}}$, з вільного моноїда A^* в моноїд $\mathcal{N}^{Q \times Q}$ $\mathcal{N}$-відмношень над станами Q (див. підрозділ 1.6). Зокрема, ми маємо

$$\mu_{\mathcal{A}}(1) = I_Q,$$

де I_Q — тотожне відмношення над множиною станів Q, і для $u, v \in A^*$ виконується умова

$$(p, \mu_{\mathcal{A}}(uv), q) = \sum_{r \in Q} (p, \mu_{\mathcal{A}}(u), r)(r, \mu_{\mathcal{A}}(v), q).$$

Морфізм $\mu_{\mathcal{A}}$ називається *зображенням, асоційованим* з автоматом $\mathcal{A}$. Відповідність між морфізмом $\mu_{\mathcal{A}}$ і морфізмом $\varphi_{\mathcal{A}}$, визначеним у підрозділі 1.4), визначається так:

$$(p, q) \in \varphi_{\mathcal{A}}(w) \qquad \Longleftrightarrow \qquad (p, \mu_{\mathcal{A}}(w), q) \neq 0.$$

Твердження 1.10.1. *Нехай $\mathcal{A} = (Q, I, T)$ — автомат над алфавітом A. Для всіх $p, q \in Q$ і $w \in A^*$, величина $(p, \mu_{\mathcal{A}}(w), q)$ дорівнює (можливо нескінченній) кількості шляхів з вершини p до вершини q з міткою w.*

В автоматі $\mathcal{A} = (Q, I, T)$ шлях $c \to t$ називається *успішним*, якщо $i \in I$ і $t \in T$. *Поведінкою автомата* $\mathcal{A} = (Q, I, T)$ називається формальний степеневий ряд $|\mathcal{A}|$, який визначається за формулою

$$(|\mathcal{A}|, w) = \sum_{i \in I, t \in T} (i, \mu_{\mathcal{A}}(w), t). \tag{1.23}$$

Множина, яка розпізнається автоматом $\mathcal{A}$ є носієм формального степеневого ряду $|\mathcal{A}|$. Вона є в точності лише множиною всіх міток успішних шляхів та позначається через $L(\mathcal{A})$, як і в підрозділі 1.4.

Твердження 1.10.2. *Нехай $\mathcal{A} = (Q, I, T)$ — автомат над алфавітом A. Для всіх слів $w \in A^*$ поведінка $(|\mathcal{A}|, w)$ автомата $\mathcal{A}$ $(p, \mu_{\mathcal{A}}(w), q)$ дорівнює (можливо нескінченній) кількості шляхів з міткою w.*

Більш компактне написання формули (1.23) полягає в

$$(|\mathcal{A}|, w) = I \mu_{\mathcal{A}}(w) T. \tag{1.24}$$

Тут елемент $I \in \mathcal{N}^Q$ розглядається як рядок вектора й елемент $T \in \mathcal{N}^Q$ як стовпчик вектора, причому в обидвох числа 0 і 1 є коефіцієнтами.

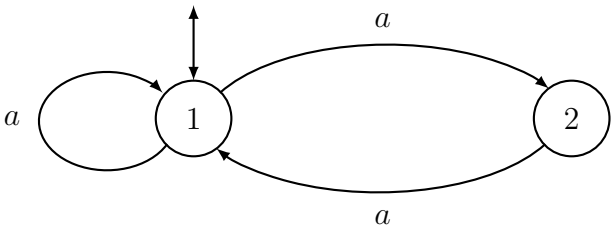


Рис. 1.7: Автомат Фібоначчі

Приклад 1.10.3. Нехай $\mathcal{A}$ — автомат, зображений на рис. 1.7, з $I = T = \{1\}$. Його поведінкою є формальний степеневий ряд

$$|\mathcal{A}| = \sum_{n \geqslant 0} f_{n+1} a^n,$$

де f_n — n-те *число Фібоначчі*. Числа Фібоначчі визначають рекурентно:

$$f_0 = 0, \qquad f_1 = 1 \qquad \text{і} \qquad f_{n+1} = f_n + f_{n-1} \quad (n > 0).$$

Для $n \geqslant 1$ маємо

$$\mu_{\mathcal{A}}(a^n) = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}.$$

Твердження 1.10.4. *Нехай $\mathcal{A} = (Q, I, T)$ — автомат над алфавітом A. Для кожного цілого числа d множина $\{w \in A^* \colon (|\mathcal{A}|, w) = d\}$ є регулярною.*

Доведення. Нехай M — моноїд $Q \times Q$-матриць над кільцем $\mathcal{B}(d)$. Для кожного слова w покладемо $\alpha(w)$ — $Q \times Q$-матриця над напівкільцем $\mathcal{B}(d)$, отримана з матриці $\mu_{\mathcal{A}}(w)$ заміною кожного її елемента $\mu_{\mathcal{A}}(w)_{p,q}$ значенням $\min\{d+1, \mu_{\mathcal{A}}(w)_{p,q}\}$. Позаяк кожна така заміна є морфізмом з напівкільця $\mathcal{N}$ на напівкільце $\mathcal{B}(d)$, то відображення α є морфізмом з вільного моноїда A^* на моноїд M. Множина слів

$$\{w \in A^* \colon (|\mathcal{A}|, w) = d\}$$

є розпізнаною морфізмом α; вона є справді множина слів w таких, що $I\alpha(w)T$ (обчислена в $\mathcal{B}(d)$) дорівнює d. □

Для кожного автомата $\mathcal{A} = (Q, I, T)$, ми пов'язуємо автомат, який позначатимемо $\mathcal{A}^*$ і називається *зіркою* автомата $\mathcal{A}$, канонічною конструкцією, що складається з двох таких кроків. Нехай $\omega \notin Q$ — новий стан, і нехай

$$\mathcal{B} = (Q \cup \omega, \omega, \omega) \tag{1.25}$$

є автоматом з переходами

$$F = E \cup \widehat{I} \cup \widehat{T} \cup \widehat{O},$$

де E — множина переходів автомата $\mathcal{A} = (Q, I, T)$ і

$$\widehat{I} = \{(\omega, a, q) \colon \text{існує елемент} \quad i \in I \quad \text{такий, що} \quad (i, a, q) \in E\}, \tag{1.26}$$

$$\widehat{T} = \{(q, a, \omega)\colon \text{існує елемент} \quad t \in T \quad \text{такий, що} \quad (q, a, t) \in E\}, \tag{1.27}$$

$$\widehat{O} = \{(\omega, a, \omega)\colon \text{існують} \quad i \in I,\ t \in T \quad \text{такі, що} \quad (i, a, t) \in E\}, \tag{1.28}$$

За означенням, автомат $\mathcal{A}^*$ є впорядкованою частиною автомата $\mathcal{B}$.

Така термінологія є зручною для автомата вигляду $\mathcal{A} = (Q, 1, 1)$, який має лише один початковий стан, що є також єдиним кінцевим станом.

Шлях

$$c\colon p \xrightarrow{w} q$$

називається *простим*, якщо він не є нуль-шляхом (тобто $w \in A^+$) і якщо $r \neq 1$ для кожної факторизації

$$c\colon p \xrightarrow{u} r \xrightarrow{v} q$$

шляху c на два ненульові шляхи.

Довільний шлях c зі стану p у стан q є або нульовим шляхом, або простим, або він розкладається єдиним чином як

$$c\colon p \xrightarrow{u} 1 \xrightarrow{x_1} 1 \xrightarrow{x_2} 1 \cdots 1 \xrightarrow{x_n} r \xrightarrow{v} q,$$

де кожен з цих $n + 2$ шляхів є простим.

Твердження 1.10.5. *Нехай $X \subset A^+$ і $\mathcal{A}$ — автомат такий, що $|\mathcal{A}| = \underline{X}$. Тоді*

$$|\mathcal{A}^*| = (\underline{X})^*. \tag{1.29}$$

Доведення. Позаяк $\mathcal{A}^*$ — впорядкована частина автомата $\mathcal{B}$, визначеного за формулою (1.25), то достатньо довести, що $|\mathcal{B}| = |\mathcal{A}|^*$.

Нехай S — степеневий ряд, означений наступним чином: для всіх $w \in A^*$ покладемо (S, w) — кількість простих шляхів з стану ω в стан ω з міткою w. За попередніми зауваженнями маємо

$$|\mathcal{B}| = S^*.$$

Отже залишилось довести, що

$$S = \underline{X}.$$

Нехай $w \in A^*$. Якщо $w = 1$, то

$$(S, 1) = (\underline{X}, 1) = 0,$$

оскільки простий шлях не є нуль-шляхом. Якщо $w = a \in A$, то $(S, a) = 1$ тоді і лише тоді, коли $a \in X$, згідно формули (1.28). Припустимо, що $|w| \geqslant 2$. Покладемо $w = aub$ з $a, b \in A$ і $u \in A^*$. Кожен простий шлях $c\colon \omega \xrightarrow{w} \omega$ факторизується однозначно так

$$c\colon \omega \xrightarrow{w} p \xrightarrow{a} q \xrightarrow{b} \omega$$

для деяких $p, q \in Q$. Існує хоча б один успішний шлях

$$i \xrightarrow{a} p \xrightarrow{u} q \xrightarrow{b} t$$

в автоматі $\mathcal{A}$. Цей шлях є унікальним, тому що поведінка автомата A є характеристичним рядом. Якщо існує інший простий шлях $c'\colon \omega \xrightarrow{w} \omega$ в автоматі $\mathcal{B}$, то існує інший успішний шлях, що має мітку w в автоматі $\mathcal{A}$, а це є неможливим. Таким чином, існує щонайбільше один простий шлях $c\colon \omega \xrightarrow{w} \omega$ в автоматі $\mathcal{B}$ і такий шлях існує тоді і лише тоді $w \in X$. Отже, $S = \underline{X}$, що і треба було довести. □

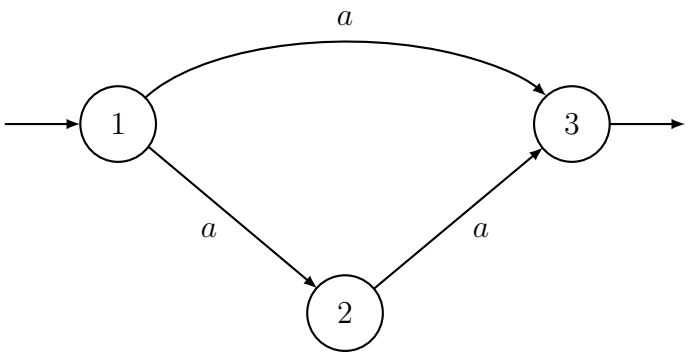


Рис. 1.8: Автомат з поведінкою $\underline{X}$, для $X = \{a, aa\}$

Приклад 1.10.6. Нехай $X = \{a, a^2\}$. Тоді $\underline{X} = |\mathcal{A}|$ для автомата, зображеного на рис. 1.8, з $I = \{1\}$, $T = \{3\}$. Автомат $\mathcal{A}^*$ є автоматом, зображеним на рис. 1.7 з точністю до перейменування стану ω. Таким чином,

$$((\underline{X})^*, a^n) = f_n$$

для $n \geqslant 0$.

Приклад 1.10.7. Нехай $X = \{aa, ba, baa, bb, bba\}$. Тоді $\underline{X} = |\mathcal{A}|$ для автомата, зображеного на рис. 1.9, з $I = \{1\}$, $T = \{4\}$. Відповідний автомат $\mathcal{A}^*$ зображено на

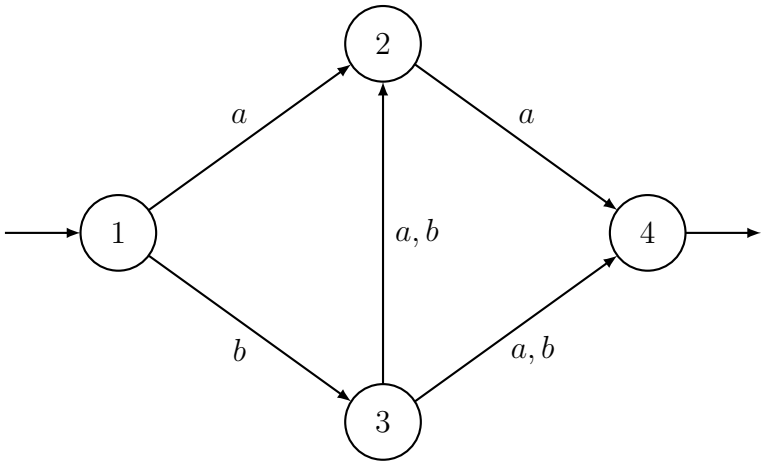


Рис. 1.9: Автомат з поведінкою $\underline{X}$, для $X = \{aa, ba, baa, bb, bba\}$

рис. 1.10.

Тепер поширимо попередні означення на більш загальний випадок, коли мітки ребер автомата можуть мати вагу. Нехай A — алфавіт і K — напівкільце. Скінченний *ваговий автомат* $\mathcal{A} = (Q, I, T)$ над алфавітом A та з вагами в кільці K визначається скінченною множиною Q з двома відображеннями $I\colon Q \to K$, $T\colon Q \to K$ і відображенням

$$E\colon Q \times A \times Q \to K.$$

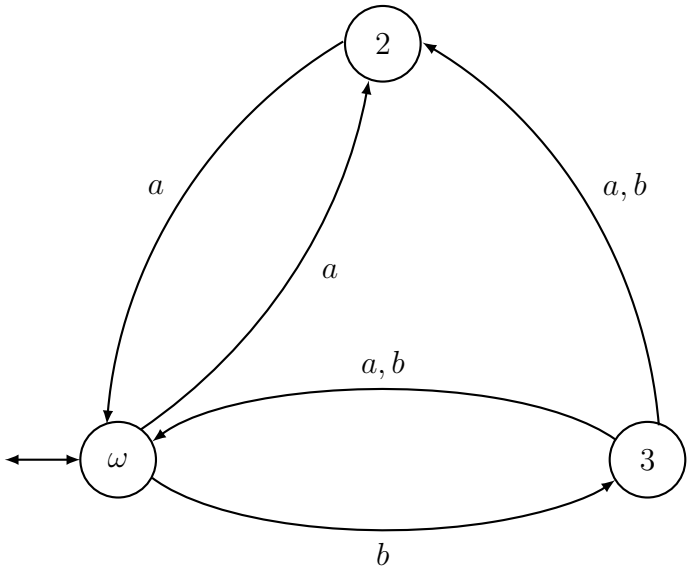


Рис. 1.10: Автомат, який розпізнає X^*, для $X = \{aa, ba, baa, bb, bba\}$

Якщо $E(p, a, q) = k \neq 0$, то будемо говорити, що (p, a, q) є ребром з міткою a та вагою k і позначатимемо це так $p \xrightarrow{ka} q$. Якщо c є шляхом

$$p \xrightarrow{k_1 a_1} q_1 \longrightarrow \cdots \longrightarrow q_{n-1} \xrightarrow{k_1 a_1} q$$

у зваженому автоматі $\mathcal{A}$, то його міткою є слово $x = a_1 \cdots a_n$, а вагою — добуток $|c| = k_1 \cdots k_n$. Ми позначатимемо такий шлях так $c\colon p \xrightarrow{x} q$. *Поведінкою* вагового автомата $\mathcal{A}$ називається ряд, який позначається через $|\mathcal{A}|$ та визначається за формулою

$$(|\mathcal{A}|, x) = \sum_{c\colon p \xrightarrow{x} q} I(p)|c|T(q).$$

Оскільки для кожного слова $x \in A^*$ існує лише скінченна кількість шляхів з міткою x, то така сума є коректно визначеною. Поведінка також називається *рядом, розпізнуваним* ваговим автоматом. Ряд u називається *K-раціональним*, якщо він є поведінкою вагового автомата з вагами в напівкільці K. Ми особливо цікавимося $\mathbb{N}$-раціональними рядами.

Тепер запропонуємо альтернативну форму ряду розпізнаваного ваговим автоматом $\mathcal{A} = (Q, I, T)$ над алфавітом A. Означимо морфізм μ з вільного моноїда A^* в мультиплікативний моноїд $Q \times Q$-матриць з коефіцієнтами в напівкільці K, поклавши

$$\mu(a)_{p,q} = E(p, a, q)$$

для $a \in A$. Тоді для кожного слова $x \in A^*$ маємо, що

$$(|\mathcal{A}|, x) = I\mu(x)T,$$

і тут I розглядається як вектор-рядок, а T — як вектор-стовпчик. У цьому випадку морфізм μ називається *матричним зображенням* вагового автомата $\mathcal{A} = (Q, I, T)$

Приклад 1.10.8. Кожен автомат можна розглядати як ваговий автомат з вагами в Булевому напівкільці $\mathcal{B}$, або в напівкільці $\mathbb{N}$. В останньому випадку поведінка — це кількість успішних шляхів.

Приклад 1.10.9. Ваговий автомат зображений на рис. 1.11, має цілочисельні ваги й алфавіт з однією літерою. Для простоти цю літеру не вказано, а вага ребра не вказується, якщо вона дорівнює 1. Значення поведінки на слові довжини n дорівнює n^2.

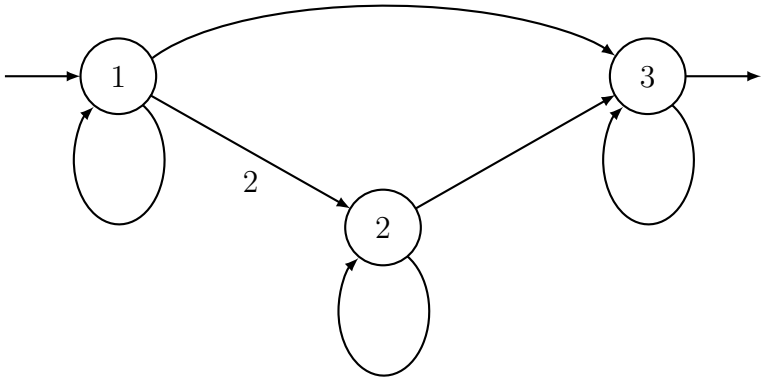


Рис. 1.11: Ваговий автомат над алфавітом, який складається з однієї літери

Справді, позначимо через u_n, v_n і w_n суму ваг шляхів довжини n, які закінчуються в стані 3 і починаються в станах 1, 2 і 3, відповідно. Маємо, що $w_n = 1$ для всіх $n \geqslant 0$. Далі, з форми автомата випливає, що $v_{n+1} = v_n + w_n$ для $n \geqslant 0$, звідки отримуємо, що $v_n = n$. На завершенні маємо, що $u_{n+1} = u_n + 2v_n + w_n$, а отже $u_n = n^2$ для всіх $n \geqslant 0$.

Нехай $\mathcal{A} = (Q, I, T)$ — ваговий автомат над алфавітом A. Коли множина початкових станів I автомата $\mathcal{A}$ є одноточковою, тобто $I(i) = 1$ для деякого $i \in Q$, і $I(q) = 0$ для $q \neq i$, то символ I будемо замінювати на i. Аналогічно будемо робити у випадку множини кінцевих станів T є одноточковою.

Ваговий автомат $\mathcal{A} = (Q, i, t)$ називається *впорядкованим* (*обрізаним*), якщо для кожного стану q, існують шлях з i до q і шлях з q до t. Кажуть, що ваговий автомат $\mathcal{A}$ є *нормалізовним*, якщо не має ребер, що входять в i s не виходить з t і $i \neq t$.

Твердження 1.10.10. *Кожен $\mathbb{N}$-раціональний ряд з нульовим сталим членом можна розпізнати нормалізовним ваговим автоматом.*

Доведення. Нехай $\mathcal{A} = (Q, I, T)$ — ваговий автомат над алфавітом A, який розпізнає ряд з нульовим сталим членом, з відображенням вершин $E\colon Q \times A \times Q \to K$. Нехай i та t — два стани, які не є в Q. Визначимо ваговий автомат $\mathcal{B} = (Q', i, t)$ з множиною станів $Q' = Q \cup \{i, t\}$ і відображенням вершин $F\colon Q' \times A \times Q' \to K$ наступним чином

$$F(p, a, q) = E(p, a, q) \qquad \text{для} \quad p, q \in Q,$$

$$F(i, a, q) = \sum_{p \in Q} I(p) E(p, a, q) \qquad \text{для} \quad q \in Q,$$

$$F(p,a,t) = \sum_{q\in Q} E(p,a,q)T(q) \qquad \text{для} \quad p \in Q,$$

$$F(i,a,t) = \sum_{p,q\in Q} I(p)E(p,a,q)T(q).$$

Співвідношення між матричним зображенням ν автомата $\mathcal{B}$ та матричним зображенням μ автомата $\mathcal{A}$ визначається так:

$$\nu(a) = \begin{bmatrix} 0 & I\mu(a) & I\mu(a)T \\ 0 & \mu(a) & \mu(a)T \\ 0 & 0 & 0 \end{bmatrix},$$

де i та t вважається як перший і останній індекс, відповідно. Легко перевірити, що подібна форма виконується для будь-якого слова $w \in A+$, і таким чином $\nu(w)_{i,t} = I\mu(w)T$. Це виконується також для $w = 1$, тому що $i \neq t$ і $I\mu(w)T = 0$ за припущенням. Це доводить, що автомати $\mathcal{A}$ і $\mathcal{B}$ розпізнають один і той же ряд. □

Тепер розглянемо степеневий ряд, тобто ряд від однієї змінної.

Твердження 1.10.11. *Для довільної раціональної множини X вільного моноїда A^*, породжуючий ряд $f_X(z)$ є $\mathbb{N}$-раціональним.*

Доведення. Нехай $\mathcal{A}$ — детерміністичний скінченний автомат, який розпізнає множину X, і нехай $\mathcal{B}$ — ваговий автомат, отриманий заміною усіх міток в автоматі $\mathcal{A}$ символом z. Очевидно, що автомат $\mathcal{B}$ розпізнає ряд $\sum_{n\geqslant 0} \mathrm{Card}(X \cap A^n)z^n$. □

Для взятого ряду $u(z) = \sum_{n\geqslant 0} u_n z^n$ з цілими коефіцієнтами та з нульовим сталим коефіцієнтом $u_0 = 0$, через $u^*(z)$ ми позначатимемо ряд, який визначається за формулою

$$u^*(z) = 1/(1 - u(z)).$$

Твердження 1.10.12. *Нехай $u(z) = \sum_{n\geqslant 0} u_n z^n$ — $\mathbb{N}$-раціональний ряд з нульовим сталим коефіцієнтом. Нехай $\mathcal{A} = (Q, i, t)$ — нормалізовний ваговий автомат, який розпізнає ряд $u(z)$. Нехай $\overline{Q} = Q \setminus \{t\}$ і нехай $\overline{\mathcal{A}} = (\overline{Q}, i, i)$ — ваговий автомат отриманий ототожненням станів i й t. Тоді поведінкою автомата $\overline{\mathcal{A}}$ є ряд $u^*(z)$.*

Доведення. Нагадаємо, що шлях від стану i до i є *простим*, якщо він не проходить через стан i проміжним чином. Для кожного цілого $n > 0$, коефіцієнт u_n є сумою ваг простих шляхів довжини n зі стану i до i в автоматі $\overline{\mathcal{A}}$. Справді, оскільки автомат $\mathcal{A}$ є нормалізовним, кожному простому шляхові $\overline{c}$: $i \to i$ в автоматі $\overline{\mathcal{A}}$ відповідає єдиний шлях з стану i в стан t в автоматі $\mathcal{A}$, і навпаки.

Для $r \geqslant 1$ покладемо $u(r)^{(n)}$ — сума ваг шляхів зі стану i в стан i, що проходять рівно $r-1$-разів через стан i. Покладемо

$$u^{(r)}(z) = \sum_{n\geqslant 0} u_n^{(r)} z^n \qquad \text{і} \qquad u^{(0)}(z) = 1.$$

Ряд $u^{(*)}(z) = \sum_{r \geqslant 0} u^{(r)}(z)$ є поведінкою автомата $\overline{\mathcal{A}}$.

Далі $u^{(r)}(z) = u(z)^r$ для $r \geqslant 0$. Позаяк

$$u^*(z) = \sum_{r \geqslant 0} u(z)^r,$$

то отримуємо, що $u^*(z) = u^{(*)}(z)$. □

Зауважимо, що це твердження пов'язане з твердженням 1.10.5, яка може бути використаним для надання альтернативного доведення. Справді, якщо $A = (Q, i, t)$ — нормалізований автомат, то в автоматі $\mathcal{A}^*$ і стан i є більш недоступним і стан t є більше доступним. Таким чином, обрізаний автомат є ідентичним з автоматом $\overline{\mathcal{A}}$.

Приклад 1.10.13. Нехай $u(z) = z + z^2$. Ваговий автомат $\mathcal{A}$, зображений на рис. 1.12, з $i = 1$ та $t = 3$. Ваговий автомат $\mathcal{A}$, зображений на рис. 1.13,

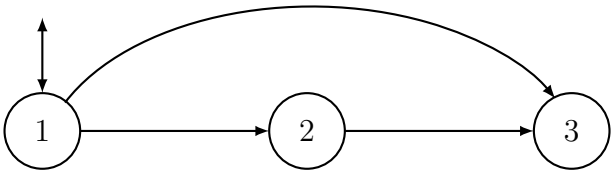


Рис. 1.12: Ваговий автомат, який розпізнає $z + z^2$

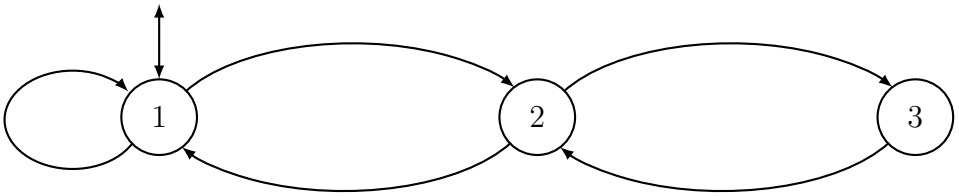


Рис. 1.13: Ваговий автомат, який розпізнає $1/(1 - z - z^2)$

Наступне твердження стосується вагових автоматів з вагами в $\mathbb{N}$ з невід'ємними матрицями. Розширюємо означення *матриці суміжності* для вагових автоматів. Для вагового автомата $\mathcal{A} = (Q, I, T)$ над алфавітом A його матриця суміжності M є $Q \times Q$-матрицею, яка означена так:

$$M_{p,q} = \sum_{a \in A} E(p, a, q),$$

де $E(p, a, q)$ — вага ребра (p, a, q).

Твердження 1.10.14. *Нехай* $u(z) = \sum_{n \geqslant 0} u_n z^n$ — $\mathbb{N}$-*раціональний ряд, який розпізнається впорядкованим ваговим автоматом* $\mathcal{A}$ *з матрицею переходів* M. *Тоді радіус збіжності ряду* $u(z)$ *є оберненим до максимального власного значення матриці* M.

Доведення. Нехай λ — максимальне власне значення матриці M, яке існує і є додатнім за теоремою Перрона-Фробениуса (теорема 1.9.2). Нехай ρ — радіус збіжності ряду $u(z)$, і для всіх $p, q \in Q$, $\rho_{p,q}$ — радіус збіжності ряду

$$u_{p,q}(z) = \sum_{n \geqslant 0} M_{p,q}^n z^n.$$

Тоді $1/\lambda = \min \rho_{p,q}$, оскільки ряд $\sum_{n \geqslant 0} M^n z^n$ збігається для $|z| < 1/\lambda$. Далі, оскільки автомат $\mathcal{A}$ є впорядкованим, то ряд $u_{p,q}(z)$ збігається за умови, коли ряд $u(z)$ збігається, а отже $\rho_{p,q} \geqslant \rho$ для всіх $p, q \in Q$. З іншого боку $\rho \geqslant \min \rho_{p,q}$ оскільки u є невід'ємною лінійною комбінацією рядів $s_{p,q}$. Звідси випливає, що $\rho = \min \rho_{p,q}$, а це завершує доведення. □

Приклад 1.10.15. Ваговий автомат $\mathcal{A}$, зображений на рис. 1.14, розпізнає ряд

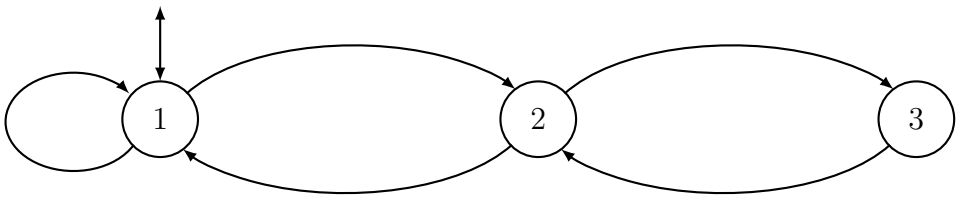


Рис. 1.14: Ваговий автомат, який розпізнає $(1 - z^2)/(1 - 2z^2)$

$$u(z) = \frac{1}{1 - \dfrac{z^2}{1 - z^2}} = \frac{1 - z^2}{1 - 2z^2} = 1 + z^2 + 2z^4 + 3z^6 + 4z^8 + \dots.$$

Радіус збіжності ряду $u(z)$ дорівнює $\sqrt{2}/2$. Матрицею переходу автомата $\mathcal{A}$ є

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Власними значеннями цієї матриці є 0 і $\pm\sqrt{2}$.

1.11 Імовірнісні розподіли

Для алфавіту A відображення $\pi\colon A^* \to [0,1]$ таке, що $\pi(1) = 1$ і

$$\sum_{a\in A} \pi(wa) = \pi(w). \tag{1.30}$$

для всіх $w \in A^*$ називається *розподілом імовірності* або коротко *розподілом* на алфавіті A^*. Умова (1.30) називається *умовою когерентності*. Звідси випливає, що

$$\sum_{x\in A^n} \pi(x) = 1$$

для всіх цілих $n \geqslant 0$. Справді, це виконується для $n = 0$ і для $n > 0$ маємо

$$\sum_{x\in A^n} \pi(x) = \sum_{x\in A^{n-1}} \sum_{x\in A} \pi(ya) = \sum_{x\in A^{n-1}} \pi(y) = 1,$$

де з першої до останнього рівності виконується за умовою когерентності, а остання рівність виконується за індукцією. Розподіл називається *додатним*, якщо $\pi(w) > 0$ для всіх слів w.

Ці поняття пов'язані зі звичайною теорією ймовірностей. Це буде описано в розділі 13. Зокрема, умова когерентності (1.30) дозволяє інтерпретувати розподіл як ймовірність, що відповідає послідовності випадкових наборів літер слова зліва направо.

Як частковий випадок, *розподіл Бернулллі* є морфізмом з A^* в $[0,1]$ такий, що $\sum_{x\in A} \pi(x) = 1$. Очевидно, що розподіл Бернуллі є розподілом ймовірності. Він є додатним тоді і тільки тоді, коли $\pi(a) > 0$ для всіх літер a. Розподіл Бернуллі відповідає послідовності незалежних випробувань з однаковою ймовірністю. *Рівномірний розподіл Бернуллі* визначається так:

$$\pi(a) = 1/\operatorname{Card}(A), \qquad \text{для всіх} \quad a \in A.$$

Для ймовірнісного розподілу π на A^* покладемо

$$\pi(X) = \sum_{x\in X} \pi(x),$$

для довільної підмножини X вільного моноїда A^*, Ця величина може як бути скінченною так і нескінченною. *Породжуючий ряд ймовірностей* множини $X \subset A^*$ — це ряд

$$F_X(t) = \sum_{n\geqslant 0} \pi(X \cap A^n) t^n.$$

Зокрема, $F_X(1) = \pi(X)$. У випадку однорідного розподілу Бернуллі, породжуючий ряд ймовірностей пов'язаний з (звичайним) породжуючим рядом так:

$$f_X(t) = F_X(kt), \tag{1.31}$$

де $k = \operatorname{Card}(A)$. Справді, у цьому випадку маємо

$$\operatorname{Card}(X \cap A^n) = k^n \pi(X \cap A^n).$$

Ваговий автомат можна використати для визначення розподілу ймовірності на вільному моноїда A^*. Нагадаємо, що *матрицею переходів* (*суміжності*) вагового автомата $\mathcal{A} = (Q, I, T)$ над алфавітом A є $Q \times Q$-матриця P, яка визначається так:

$$P_{p,q} = \sum_{a \in A} E(p, a, q).$$

Розглянемо ваговий автомат $\mathcal{A} = (Q, I, T)$ з невід'ємними дійсними вагами. Автомат $\mathcal{A} = (Q, I, T)$ називається *стохастичним*, якщо $\sum_{p \in Q} I(p) = 1$ і $T(q) = 1$ для всіх $q \in Q$ та його матриця переходів P є стохастичною.

Для стохастичного автомата $\mathcal{A} = (Q, I, T)$ відображення, визначене за формулою $\pi(x) = (|\mathcal{A}|, x)$ є розподілом ймовірностей, називається *розподілом ймовірностей*, визначеним стохастичним автоматом $\mathcal{A}$. Справді, $\pi(1) = \sum_{p \in Q} I(p) = 1$. Далі, нехай μ — матриця зображень автомата $\mathcal{A}$. Матрицею переходів автомата $\mathcal{A}$ є матриця $P = \sum_{a \in A} \mu(a)$. Тоді $PT = T$ і

$$\sum_{a \in A} \pi(xa) = \sum_{a \in A} I\mu(xa)T = I\mu(x)\left(\sum_{a \in A} \mu(a)T\right) = I\mu(x)PT = I\mu(x)T = \pi(x),$$

що показує, що відображення π задовольняє умові когерентності. Розподіл імовірностей, визначений стохастичним автоматом, часто називають *прихованим ланцюгом Маркова*.

Окремий випадок стохастичного автомата виникає, коли кінцевий стан ребра є в бієкції з його міткою. Іншими словами, це виконується, якщо

$$a = a' \qquad \Longleftrightarrow \qquad q = q'$$

для ребер $E(p, a, q) \neq 0$, $E(p', a', q') \neq 0$. У цьому випадку, множину кінцевих станів ребер можна ототожнити з алфавітом. Розподіл ймовірностей, визначений таким стохастичним автоматом називається *ланцюгом Маркова*.

Приклад 1.11.1. Нехай $A = \{a, b\}$. Розподіл імовірностей на автоматі $\mathcal{A}$, визначений так:

$$\pi(ax) = 2^{-|x|}, \quad \pi(bx) = 0 \qquad \text{для всіх} \quad x \in A^*,$$

визначений стохастичним автоматом зображеним на рис. 1.15 з $I = \begin{bmatrix} 1 & 0 \end{bmatrix}$. Матри-

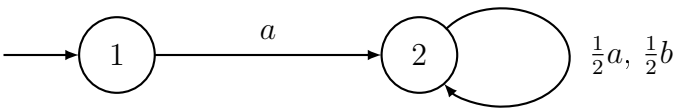


Рис. 1.15: Стохастичний автомат

чне зображення задається так:

$$\mu(a) = \begin{bmatrix} 0 & 1 \\ 0 & 1/2 \end{bmatrix}, \qquad \mu(b) = \begin{bmatrix} 0 & 0 \\ 0 & 1/2 \end{bmatrix}.$$

Так означений імовірнісний розподіл не є ланцюгом Маркова, оскільки 2 є кінцем ребер з мітками a та b.

1.12 Ідеали в моноїді

Нехай M — моноїд. *Правим ідеалом* моноїда M називається непорожня підмножина R в M така, що

$$RM \subseteq R,$$

або еквівалентно, що $rm \in R$ для всіх $r \in R$ і $m \in M$. Позаяк M є моноїдом, то маємо, що $RM = R$ тому, що M містить одиничний елемент. *Лівим ідеалом* моноїда M називається непорожня підмножина L в M така, що $ML \subseteq L$. *Двобічний ідеал* або просто *ідеал* моноїда M — це непорожня підмножина I в M така, що

$$MIM \subseteq I.$$

Двобічний ідеал є одночасно лівим і правим ідеалом. Зокрема, моноїд M є ідеалом в собі.

Якщо моноїд M містить нуль 0, то множина $\{0\}$ є двобічним ідеалом, який містить в кожному іншому ідеалі моноїда M.

Ідеал I (відп., лівий, правий ідеал) називається *мінімальним*, якщо

$$J \subseteq I \quad \Longrightarrow \quad J = I,$$

для довільного ідеала J (відп., лівого, правого ідеала). Якщо моноїд M містить мінімальний двобічний ідеал, то він єдиний, оскільки довільний непорожній перетин ідеалів є знову ідеалом. Якщо моноїд M містить нуль 0, то множина $\{0\}$ є мінімальним двобічним ідеалом в M. Ідеал $I \neq= \{0\}$ (відп., лівий, правий ідеал) називається 0-мінімальним, якщо

$$J \subseteq I \qquad \Longrightarrow \qquad J = 0 \quad \text{або} \quad J = I,$$

для довільного ідеалу J (відп., лівого, правого ідеалу) моноїда M. Для кожного елемент m моноїда M множина

$$R = mM$$

є правим ідеалом, який є найменшим правим ідеалом, що містить елемент m. Аналогічно множина $L = Mm$ є найменшим лівим ідеалом, який містить елемент m і множина $I = MmM$ є найменшим двобічним ідеалом, що містить елемент m.

Означимо відношення еквівалентності $\mathscr{R}$, $\mathscr{L}$, $\mathscr{J}$ і $\mathscr{H}$ на моноїді M так:

$$\begin{aligned}
m\mathscr{R}m' &\Longleftrightarrow mM = m'M,\\
m\mathscr{L}m' &\Longleftrightarrow Mm = Mm',\\
m\mathscr{J}m' &\Longleftrightarrow MmM = Mm'M,\\
m\mathscr{H}m' &\Longleftrightarrow mM = m'M \quad \text{і} \quad Mm = Mm'.
\end{aligned}$$

Тому маємо:

(*i*) $m\mathscr{R}m'$ тоді і лише тоді, коли існують $u, u' \in M$ такі, що $m' = mu$ і $m = m'u'$;
(*ii*) $m\mathscr{L}m'$ тоді і лише тоді, коли існують $u, u' \in M$ такі, що $m' = um$ і $m = u'm'$;
(*iii*) $m\mathscr{J}m'$ тоді і лише тоді, коли існують $u, u', v, v' \in M$ такі, що $m' = umv$ і $m = u'm'v'$.

Очевидно, що $\mathscr{R} \subseteq \mathscr{J}$, $\mathscr{L} \subseteq \mathscr{J}$ і $\mathscr{H} = \mathscr{R} \cap \mathscr{L}$.

Твердження 1.12.1. *Відношення $\mathscr{R}$ і $\mathscr{L}$ комутують: $\mathscr{R}\mathscr{L} = \mathscr{L}\mathscr{R}$.*

Доведення. Нехай $m, n \in M$ такі, що $m\mathscr{R}\mathscr{L}n$. Тоді існує елемент $p \in M$ такий, що $m\mathscr{R}p$ і $p\mathscr{L}n$ (див. рис. 1.16). Тоді за означенням існують $u, u', v, v' \in M$ такі, що

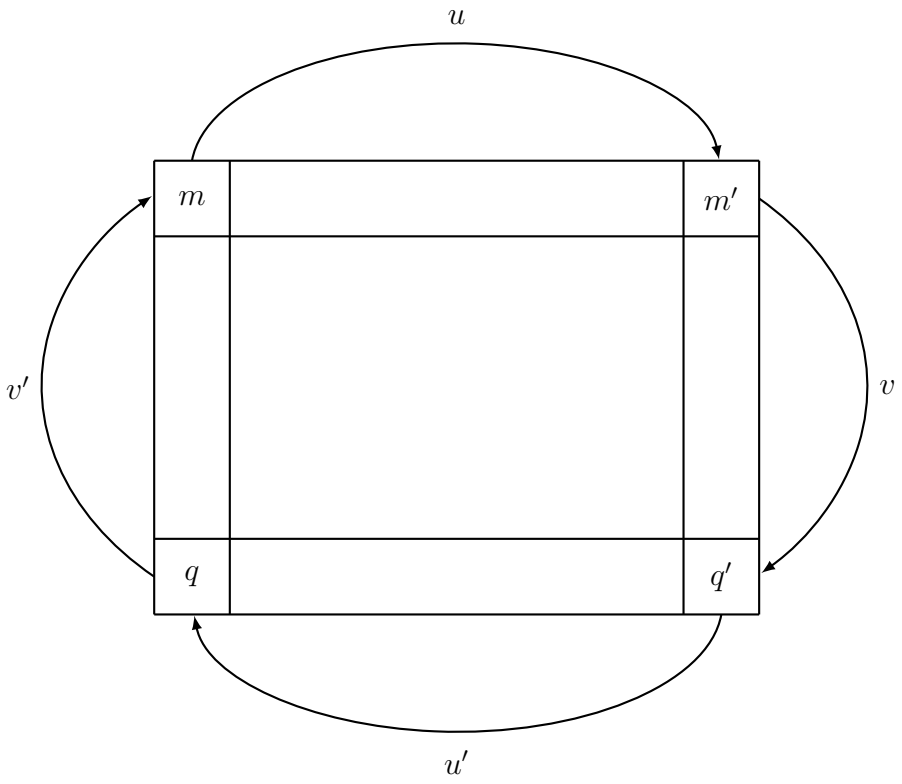


Рис. 1.16: Відношення $\mathscr{R}\mathscr{L} = \mathscr{L}\mathscr{R}$

$p = mu$, $m = pu'$, $n = vp$, $p = v'n$. Покладемо $q = vm$. Тоді отримуємо

$$q = vm = v(pu') = (vp)u' = nu \qquad \text{і} \qquad n = vp = v(mu) = (vm)u = qu.$$

Звідки випливає, що $q\mathscr{R}n$. Крім того, маємо

$$m = pu' = (v'n)u' = v'(nu') = v'q.$$

Позаяк $q = vm$, то за визначенням елемента q отримуємо, що $m\mathscr{L}q$. Отож, маємо, що $m\mathscr{L}q\mathscr{R}n$, а отже $m\mathscr{L}\mathscr{R}n$. Це доводить включення $\mathscr{R}\mathscr{L} \subseteq \mathscr{L}\mathscr{R}$. Доведення оберненого включення є аналогічним. □

Оскільки відношення $\mathscr{R}$ і $\mathscr{L}$ комутують, то відношення $\mathscr{D}$, означене

$$\mathscr{D} = \mathscr{R}\mathscr{L} = \mathscr{L}\mathscr{R},$$

і відношенням еквівалентності. Отже отримуємо включення

$$\mathscr{H} \subseteq \mathscr{L} \subseteq \mathscr{D} \subseteq \mathscr{J} \qquad \text{і} \qquad \mathscr{H} \subseteq \mathscr{R} \subseteq \mathscr{D} \subseteq \mathscr{J}.$$

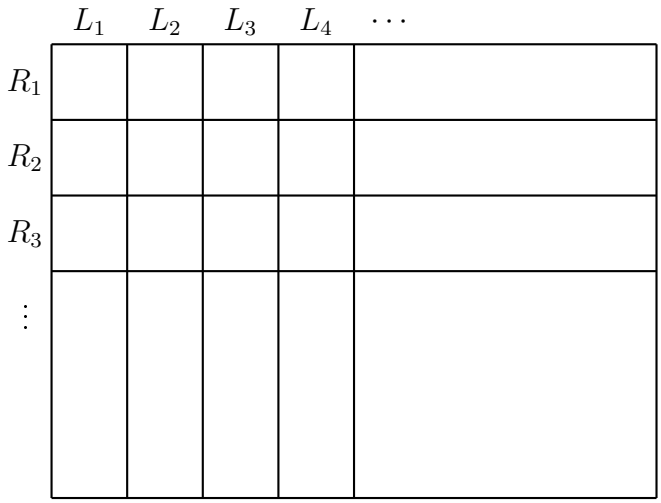


Рис. 1.17: "egg-box"-схема $\mathscr{D}$-класу

Класи відношення $\mathscr{D}$, які називаються $\mathscr{D}$-класами, можна зобразити у вигляді так званої "egg-box"-схеми, що зображена на рис. 1.17. $\mathscr{R}$-класи на рис. 1.17 зображені рядками та $\mathscr{L}$-класи стовпчиками. Квадрати, які є перетинами деяких $\mathscr{R}$- і $\mathscr{L}$-класу є $\mathscr{H}$-класами. Відношення еквівалентності $\mathscr{L}$, $\mathscr{R}$, $\mathscr{D}$, $\mathscr{H}$ і $\mathscr{H}$ на напівгрупах введені Гріном в праці [85] і називаються *відношеннями Гріна* в теорії напівгруп. Детальніше про відношення Гріна див. монографію Кліффорда та Престона [4, 52].

Надалі через $L(m)$, $R(m)$, $D(m)$, $H(m)$ і $J(m)$, відповідно, будемо позначати $\mathscr{L}$, $\mathscr{R}$, $\mathscr{D}$, $\mathscr{H}$ і $\mathscr{H}$-клас елемента $m \in M$. Очевидно, що

$$H(m) = R(m) \cap L(m) \qquad \text{і} \qquad R(m), L(m) \subseteq D(m) \subseteq J(m).$$

Твердження 1.12.2. *Нехай m і m' — $\mathscr{R}$-еквівалентні елементи моноїда M. Нехай $u, u' \in M$ такі, що*

$$m = m'u' \qquad \textit{і} \qquad m' = mu.$$

Тоді відображення

$$\rho_u \colon q \mapsto qu \qquad \textit{і} \qquad \rho_{u'} \colon q' \mapsto q'u'$$

є бієкціями з класу $L(m)$ на клас $L(m')$, і більше того вони є взаємно-оберненими, які відображають $\mathscr{R}$-клас на самого себе.

Доведення. Спочатку перевіримо, що правий зсув ρ_u відображає клас $L(m)$ на клас $L(m')$. Якщо $q \in L(m)$, то $Mq = Mm$, а отже $Mqu = Mmu = Mm'$. Отож, $qu = \rho_u(q)$ належать множині $L(m')$. Аналогічно, отримуємо, що зсув $\rho_{u'}$ відображає клас $L(m')$ в клас $L(m)$.

Припустимо, що $q \in L(m)$ і обчислимо $\rho_{u'}\rho_u(q)$. Оскільки $q\mathscr{L}m$, то існують $v, v' \in M$ такі, що $q = vm$, $m = v'q$ (див. рис. 1.18). Оскільки $muu' = m'u' = m$, то маємо, що

$$\rho_{u'}\rho_u(q) = quu' = vmuu' = vm = q.$$

Це доводить, що $\rho_{u'}\rho_u$ — тотожне відображення множини $L(m)$. Аналогічно доводиться, що $\rho_u\rho_{u'}$ — тотожне відображення множини $L(m')$.

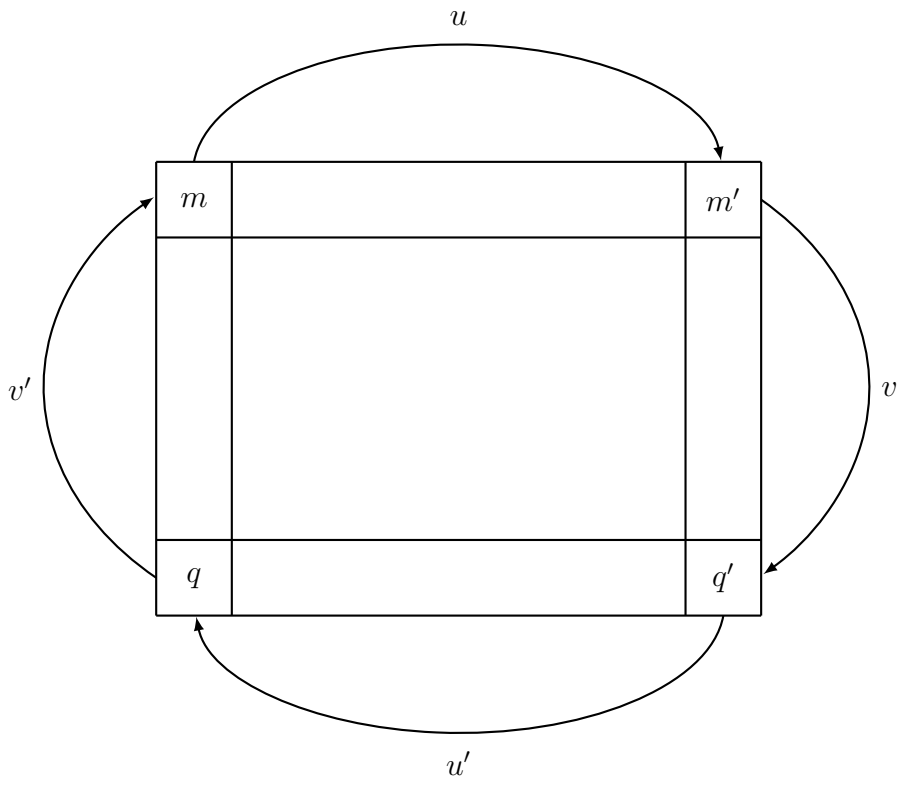


Рис. 1.18: Взаємні бієкції

Нарешті, оскільки $quu' = q$ для всіх $q \in L(m)$, то елементи q і $\rho_u(q)$ лежать в одному $\mathscr{R}$-класі. □

Твердження 1.12.2 має наступний наслідок, який обґрунтовують правильну форму рис. 1.17.

Твердження 1.12.3. *Довільні два $\mathscr{H}$-класи, що містяться в одному $\mathscr{D}$-класі мають однакову потужність.*

Тепер розглянемо задачу локалізації ідемпотентів в ідеалі. Перший результат описує $\mathscr{H}$-клас ідемпотента.

Твердження 1.12.4. *Нехай M — моноїд і $e \in M$ — ідемпотент. Тоді $\mathscr{H}$-клас ідемпотента e є групою одиниць моноїда eMe.*

Доведення. Нехай $m \in H(e)$. Тоді

$$e = mu, \qquad m = eu', \qquad e = vm, \qquad m = v'e,$$

для деяких $u, u', v, v' \in M$. Таким чином, отримуємо, що $em = e(eu') = eu' = m$ і $me = (v'e)e = v'e = m$. Звідси випливає, що $m \in eMe$. Оскільки

$$m(eue) = mue = e \qquad \text{і} \qquad (eve)m = evm = e,$$

то елемент m є одночасно оберненим справа й оберненим зліва в M. Отож, елемент m належить до групи одиниць моноїда eMe. Навпаки, якщо $m \in eMe$ є оборотним справа й оборотним зліва, то маємо $mu = vm = e$ для деяких $u, v \in eMe$. Позаяк $m = em = me$, то отримуємо, що $m \mathscr{H} e$. □

Твердження 1.12.5. *$\mathscr{H}$-клас моноїда є групою тоді і лише тоді, коли цей клас містить ідемпотент.*

Доведення. Нехай H — $\mathscr{H}$-клас моноїда M. Якщо H містить ідемпотент e, то $H = H(e)$ є групою за твердженням 1.12.4. Обернене твердження є очевидним. □

Твердження 1.12.6. *Нехай M — моноїд і $m, n \in M$. Тоді $mn \in R(m) \cap L(n)$ тоді і лише тоді, коли множина $R(n) \cap L(m)$ містить ідемпотент.*

Доведення. Якщо множина $R(n) \cap L(m)$ містить ідемпотент e, то

$$e = nu, \qquad n = eu', \qquad e = vm \qquad \text{і} \qquad m = v'e,$$

для деяких $u, u', v, v' \in M$. Отож, отримуємо

$$mnu = m(nu) = me = (v'e)e = v'e = m,$$

а отже $mn\mathscr{R}m$. Аналогічно доводиться, що $mn\mathscr{L}n$. Отож, $mn \in R(m) \cap L(n)$.

Навпаки, якщо $mn \in R(m) \cap L(n)$, то $mn\mathscr{R}m$ і $n\mathscr{L}mn$. За твердженням 1.12.2 правий зсув на елемент n є бієкцією з класу $L(m)$ на клас $L(mn)$. З того, що $n \in L(mn)$ випливає існування елемента $e \in L(m)$ такого, що $en = n$. Оскільки домноження справа на n зберігає $\mathscr{R}$-класи, то отримуємо додатково, що $e \in R(n)$. Таким чином, існує елемент $u \in M$ такий, що $e = nu$. Внаслідок цього отримуємо

$$nunu = enu = nu,$$

а отже елемент $e = nu$ є ідемпотентом множини $R(n) \cap L(m)$. □

Твердження 1.12.7. *Нехай M — моноїд і D — D-клас моноїда M. Тоді такі умови є еквівалентними:*

(i) D містить ідемпотент;
(ii) кожен $\mathscr{R}$-клас в D містить ідемпотент;
(iii) кожен $\mathscr{L}$-клас в D містить ідемпотент.

Доведення. Очевидно, що достатньо довести імплікацію $(i) \Rightarrow (ii)$. Нехай $e \in D$ — ідемпотент. Нехай R — $\mathscr{R}$-клас в класі D. $\mathscr{H}$-клас $H = L(e) \cap R$ є непорожнім. Нехай n — елемент класу H (див. рис. 1.19). Позаяк $n\mathscr{L}e$, то існують $v, v' \in M$ такі, що

$$n = ve \qquad \text{і} \qquad e = v'n.$$

Нехай $m = ev'$. Тоді $mn = e$, оскільки

$$mn = (ev')n = e(v'n) = ee = e.$$

Більше того, маємо, що $m\mathscr{R}e$ оскільки $mn = e$ і $m = ev'$. Таким чином, елемент $e = mn$ міститься в $R(m) \cap L(n)$. Тоді за твердженням proposition-1.12.6, клас $R = R(n)$ містить ідемпотент. □

$\mathscr{D}$-клас, для якого виконується хоча б одна з умов твердження 1.12.7 називається *регулярним*.

Рис. 1.19: Пошук ідемпотента в класі R

Твердження 1.12.8. *Нехай H — $\mathscr{H}$-клас моноїда M. Тоді такі умови є еквівалентними:*

(i) існують $h, h' \in H$ такі, що $hh' \in H$;
(ii) H — підгрупа в M.

Доведення. $(i) \Longrightarrow (ii)$ Якщо $h, h' \in H$, то за твердженням 1.12.6 клас H містить ідемпотент, а твердженням 1.12.5 він є групою.

Імплікація $(ii) \Longrightarrow (i)$ є очевидною. □

Тепер ми вивчатимемо мінімальний і 0-мінімальний ідеали в моноїді. Нагадаємо, що якщо моноїд M містить мінімальний ідеал, то він єдиний. Однак моноїд M може містити декілька 0-мінімальних ідеалів.

Нехай M — моноїд, що містить нуль 0. Будемо говорити, що моноїд M є *первинним*, якщо для довільних $m, n \in M \setminus \{0\}$, існує елемент $u \in M$ такий, що $mun \neq 0$.

Твердження 1.12.9. *Нехай M — первинний моноїд. Тоді:*

(1) *якщо моноїд M містить 0-мінімальний ідеал, то він єдиний;*
(2) *якщо моноїд M містить 0-мінімальний правий (відп. лівий) ідеал, то M містить 0-мінімальний ідеал, і цей ідеал є об'єднанням усіх 0-мінімальних правих (відп. лівих) ідеалів моноїда M;*
(3) *якщо моноїд M одночасно містить 0-мінімальний правий ідеал і 0-мінімальний лівий ідеал, то його 0-мінімальний ідеал складається з регулярного $\mathscr{D}$-класу та нуля.*

Доведення. (1) Нехай I та J — два 0-мінімальні ідеали в M. Нехай $m \in I \setminus \{0\}$ і $n \in J \setminus \{0\}$. Позаяк моноїд M є первинним, то існує елемент $u \in M$ такий, що $mun \neq 0$. Тоді з $mun \in J$ випливає, що $I \cap J \neq \{0\}$. Позаяк множина $I \cap J$ є ідеалом, то отримуємо, що $I \cap J = I = J$.

(2) Нехай R — 0-мінімальний правий в M. Спочатку доведемо, що або $mR = \{0\}$ або множина mR є 0-мінімальним правим ідеалом в моноїді M для всіх $m \in M$.

Насправді, безпосередньо перевіркою доводиться, що mR є правим ідеалом в M для довільного $m \in M$. Припустимо, що $mR \neq \{0\}$ і нехай $R' \neq \{0\}$ — правий ідеал в M, який міститься в mR. Покладемо $S = \{r \in R\colon mr \in R'\}$. Тоді $R \neq mS$ і $S \neq \{0\}$ оскільки $R' \neq \{0\}$. Більше того, S є правим ідеалом, оскільки R' є правим ідеалом у M. Позаяк $S \subseteq R$, то з того, що R є 0-мінімальним правим ідеалом випливає рівність $S = R$. Це доводить, що $mR = R'$, і як наслідок отримуємо, що mR є 0-мінімальним правим ідеалом.

Нехай I — об'єднання усіх 0-мінімальний правих ідеалів моноїда M. Тоді I є правим ідеалом у M, і з попередніх міркувань випливає, що I є лівим ідеалом у M. Нехай $J \neq \{0\}$ — ідеал моноїда M. Тоді

$$RJ \subseteq R \cap J \subseteq R,$$

для довільного 0-мінімального правого ідеалу R моноїда M. Ми маємо, що $RJ \neq \{0\}$ оскільки для довільних $r \in R \setminus \{0\}$ і $m \in J \setminus \{0\}$, існує елемент $u \in M$ такий, що $rum \neq 0$, звідки отримуємо, що $rum \in RJ \setminus \{0\}$. Позаяк R є 0-мінімальним правим ідеалом моноїда M і $R \cap J$ — правий ідеал у M, який відмінний від $\{0\}$, то $R \cap J = R$. Отож, $R \subseteq J$. Звідси випливає включення $I \subseteq J$. Таким чином множина I міститься в кожному ненульовому ідеалі моноїда M, а отже I є 0-мінімальним ідеалом у M.

(3) Нехай I — 0-мінімальний ідеал моноїда M і $m, n \in I \setminus \{0\}$. За твердженням (2) правий ідеал mM і лівий ідеал Mn є 0-мінімальними. Позаяк моноїд M є первинним, то існує елемент $u \in M$ такий, що $mun \neq 0$. З того, що правий ідеал mM є 0-мінімальним отримуємо, що $mM = munM$, а отже $m\mathscr{R}mun$. Аналогічно доводиться, що $mun\mathscr{L}n$. Звідси випливає, що $m\mathscr{D}n$. Отже, ми довели, що множина $I \setminus \{0\}$ міститься в $\mathscr{D}$-класі. І навпаки, якщо $m \in I \setminus \{0\}$, $n \in M$ і $m\mathscr{D}n$, то існує елемент $k \in M$ такий, що $mM = kM$ і $Mk = Mn$. Внаслідок цього отримуємо

$$I = MmM = MkM = MnM$$

і звідси випливає, що $n \in I \setminus \{0\}$. Це завершує доведення того, що множина $I \setminus \{0\}$ є $\mathscr{D}$-класом.

Далі доведемо, що множина $I \setminus \{0\}$ є регулярним $\mathscr{D}$-класом. За твердженням 1.12.7 достатньо довести, що множина $I \setminus \{0\}$ містить ідемпотент. Нехай $m, n \in I \setminus \{0\}$.

Позаяк моноїд M є первинним, то існує елемент $u \in M$ такий, що $mun \neq 0$. Позаяк правий ідеал mM є 0-мінімальним і оскільки $mun \neq 0$, то $mM = muM = munM$. Отож, $mun \in R(m)$. Симетрично, оскільки Mn — 0-мінімальний лівий ідеал, то $Mn = Mun = Mmun$, звідки отримуємо, що $mun \in L(n)$. Таким чином, $mun \in R(m) \cap L(n)$ і використавши твердження 1.12.6, отримуємо, що множина $R(n) \cap L(m)$ містить ідемпотент. Цей ідемпотент належить до $\mathscr{D}$-класу елемента n, а отже він міститься в $I \setminus \{0\}$. □

Наслідок 1.12.10. *Нехай M — первинний моноїд. Якщо M містить* 0*-мінімальний правий ідеал і* 0*-мінімальний лівий ідеал, то моноїд M містить єдиний* 0*-мінімальний ідеал I, який є об'єднанням усіх* 0*-мінімальних правих (відп. лівих) ідеалів. Цей ідеал складається з регулярного $\mathscr{D}$-класу та нуля* 0*. Більше того, виконуються такі обчислювальні правила:*

(1) *$m\mathscr{R}mn$ для $m \in I \setminus \{0\}$ і $n \in M$ таких, що $mn \neq 0$;*

(2) $m\mathscr{R}nm$ *для* $m \in I \setminus \{0\}$ *і* $n \in M$ *таких, що* $nm \neq 0$;
(3) $H^2 = H$ *або* $H^2 = \{0\}$ *для кожного* $\mathscr{H}$*-класу* $H \subseteq I \setminus \{0\}$.

Доведення. Перша група тверджень є простим наслідком твердження 1.12.9.

Доведемо твердження (1). Ми маємо, що $mnM \subseteq mM$. Оскільки mM є 0-мінімальним правим ідеалом і $mn \neq 0$, то отримуємо рівність $mnM = mM$.

Доведення твердження (2) є симетричним.

На завершенні, для доведення твердження (3) припустимо, що $H^2 \neq \{0\}$. Нехай $h, h' \in H$ — такі елементи, що $hh" \neq 0$. Тоді за твердженнями (1) і (2) отримуємо $h\mathscr{R}hh'$ і $h'\mathscr{L}hh'$. Позаяк $h\mathscr{L}h'$ і $h'\mathscr{L}hh'$, то $h\mathscr{L}hh'$. Таким чином, отримуємо, що $hh' \in H$, а отже H є групою за твердженням 1.12.8. □

Наведемо тепер твердження, що відповідають твердженню 1.12.9 і наслідку 1.12.10 для мінімальних ідеалів замість 0-мінімальних ідеалів. Це, звичайно, представляє інтерес лише в тому випадку, коли моноїд не містить нуля.

Твердження 1.12.11. *Нехай* M *— моноїд.*

(1) *Якщо* M *містить мінімальний правий (відп. лівий) ідеал, то* M *містить мінімальний ідеал, який є об'єднанням усіх мінімальних правих (відп. лівих) ідеалів.*
(2) *Якщо* M *містить мінімальний правий ідеал і мінімальний лівий ідеал, то його мінімальний ідеал* I *є* $\mathscr{D}$*-класом. Усі* $\mathscr{H}$*-класи в* I *є групами.*

Доведення. Нехай 0 — елемент, ще не є елементом моноїда M і нехай $M_0 = M \cup \{0\}$ – моноїд M з приєднаним нулем 0. Моноїд M_0 є первинним.

Ідеал I (відп. правий ідеал R, лівий ідеал L) моноїда M э мінімальним тоді і лише тоді, коли $I \cup \{0\}$ (відп. $R \cup \{0\}$, $L \cup \{0\}$) є 0-мінімальний ідеал (відп. правий ідеал, лівий ідеал) моноїда M_0. Більше того, звуження на M відношень $\mathscr{R}$, $\mathscr{L}$, $\mathscr{D}$, $\mathscr{H}$ у моноїді M_0 збігається з відповідними відношеннями в M. Таким чином, твердження (1) і (2) можна вивести з твердження 1.12.9 і наслідку 1.12.10. □

Наслідок 1.12.12. *Нехай* M *— моноїд, що містить мінімальний правий ідеал і мінімальний лівий ідеал. Тоді* M *містить мінімальний ідеал, який є об'єднанням усіх мінімальних правих (відп. лівих) ідеалів. Цей ідеал є* $\mathscr{D}$*-класом і всі його* $\mathscr{H}$*-класи є групами.*

1.13 Групи підстановок

У цьому розділі ми наводимо деякі елементарні результати й означення щодо груп підстановок.

Нехай G — група та H — підгрупа групи G. *Правими суміжними класами* підгрупи H у G називаються множини вигляду Hg, де $g \in G$. Рівність $Hg = Hg'$ виконується тоді і лише тоді, коли $gg'^{-1} \in H$. Отож, праві суміжні класи підгрупи H в G є розбиттям групи G.

Коли група G є скінченною, то через $[G : H]$ позначається *індекс* підгрупи H в G. Це число одночасно дорівнює відношенню $\operatorname{Card}(G)/\operatorname{Card}(H)$ і кількості правих суміжних класів підгрупи H у групі G.

Нехай Q — множина. *Симетрична група* над Q складається з усіх підстановок множини Q і позначається через $\mathfrak{S}_Q$. У випадку, коли $Q = \{1, 2, \dots, n\}$ ми писатимемо $\mathfrak{S}_n$ замість $\mathfrak{S}_{\{1,2,\dots,n\}}$. Також символ підстановки записуватиметься справа від аргументу. Таким чином, для $g \in \mathfrak{S}_Q$ і $q \in Q$ образ елемента q стосовно відображення g будемо позначати через qg.

Групою підстановок над множиною Q називається довільна підгрупа групи $\mathfrak{S}_Q$. Наприклад, *альтернативна група* над множиною $\{1, 2, \dots, n\}$, яка позначається через $\mathfrak{A}_Q$, є групою підстановок, що складається з усіх *парних* підстановок, тобто підстановок, які є добутками парної кількості транспозицій.

Нехай G — група підстановок над множиною Q. *Стабілізатором* точки $q \in Q$ називається підгрупа в G, яка складається з усіх підстановок групи G, що не рухають точку q, тобто

$$H = \{h \in G \colon qh = q\}.$$

Група підстановок над множиною Q називається *транзитивною*, якщо для довільних $p, q \in Q$ існує елемент $g \in G$ такий, що $pg = q$.

Твердження 1.13.1. *Нехай G — група та H — підгрупа в G. Нехай Q — множина правих суміжних класів підгрупи H в G. Нехай φ — відображення з G в $\mathfrak{S}_Q$, означене для $g \in G$ і $Hk \in Q$ за формулою*

$$(Hk)\varphi(g) = H(kg).$$

Тоді відображення φ є морфізмом з G в $\mathfrak{S}_Q$ і група підстановок $\varphi(G)$ є транзитивною. Більше того, підгрупа $\varphi(G)$ є стабілізатором точки $H \in Q$.

Навпаки, нехай G — транзитивна група підстановок над множиною Q, $q \in Q$ і H — стабілізатор точки q. Тоді відображення γ з G в Q, означене за формулою

$$\gamma \colon g \mapsto qg,$$

індукує бієкцію α з множини правих суміжних класів підгрупи H на Q за формулою

$$\alpha(Hk)g = \alpha(Hkg),$$

для всіх $k, g \in G$.

Доведення. Спочатку доведемо пряму частину твердження. Тоді відображення φ коректно означене, оскільки з $Hk = Hk'$ випливає, що $Hkg = Hk'g$. Це відображення є морфізмом, оскільки $\varphi(1) = 1$ і

$$(Hk)\varphi(g)\varphi(g') = (Hkg)\varphi(g') = Hkgg' = (Hk)\varphi(gg').$$

Група підстановок $\varphi(G)$ є транзитивною, оскільки для $k, k' \in G$, маємо, що

$$(Hk)\varphi(k^{-1}k') = Hk'.$$

На завершенні, для всіх $h \in H$ відображення $\varphi(h)$ не рухає суміжний клас H, і навпаки, якщо $\varphi(g)$, з $g \in G$, не рухає суміжний клас Hg, то $Hg = H$, а отже $g \in H$.

Тепер доведемо обернене твердження. Припустимо, що $Hg = Hg'$. Тоді $gg'^{-1} \in H$, і таким чином $qgg'^{-1} = q$, показує, що $qg = qg'$, а отже $\gamma(g) = \gamma(g')$. Звідси випливає, що ми можемо визначити відображення α, поклавши $\alpha(Hg) = \gamma(g)$. Позаяк група G є транзитивною, то відображення γ є сюр'єктивним, і таким чином також відображення α є сюр'єктивним. Для доведення ін'єктивності відображення α припустимо, що $\alpha(Hg) = \alpha(Hg')$. Тоді $qg = qg'$, звідки отримуємо, що $qgg^{-1} = q$. Таким чином, відображення gg^{-1} не рухає точку q. Отже $gg'^{-1} \in H$, звідки випливає, що $Hg = Hg'$.

Остання формула є безпосереднім наслідком того факту, що обидві сторони рівності дорівнюють qkg. □

Нехай G — транзитивна група підстановок над скінченною множиною Q. *Порядком* групи G називається число $\mathrm{Card}(Q)$.

Твердження 1.13.2. *Нехай G — транзитивна група підстановок над скінченною множиною Q, $q \in Q$ і H — стабілізатор точки q. Тоді порядок групи G дорівнює індексу підгрупи H у групі G.*

Доведення. Відображення $\alpha\colon Hg \mapsto qg$ з твердження 1.13.1(2) є бієкцією з множини правих суміжних класів підгрупи H на множину Q. Звідси випливає, що $\mathrm{Card}(Q) = [G : H]$. □

Дві групи підстановок G над Q і G' над Q' називаються *еквівалентними*, якщо існує бієктивне відображення α з Q на Q' й ізоморфізм φ з G на G' такі, що

$$\alpha(qg) = \alpha(q)\varphi(g),$$

для всіх $q \in Q$ і $g \in G$, або еквівалентно, що

$$q'\varphi(g) = \alpha((\alpha^{-1}(q'))g),$$

для $q' \in Q'$ s $g \in G$.

Як приклад, розглянемо групу підстановок G над множиною Q, і нехай H — стабілізатор деякого елемента q в Q. За твердженням 1.13.1(2) група G є еквівалентною деякій групі підстановок над множиною правих суміжних класів підгрупи H, отриманих дією групи G на суміжних класах її підгрупи H.

Інший приклад розглядає довільних два стабілізатори H і H' двох точок q і q' в транзитивній групі підстановок G над множиною Q. Тоді H і H' є еквівалентними. Справді, оскільки група G є транзитивною, то існує елемент $g \in G$ такий, що $qg = q'$.

Тоді елемент g визначає бієкцію $\alpha\colon Q \to Q$ за формулою $\alpha(p) = pg$. Відображення $\varphi\colon H \to H'$, визначене за формулою $\varphi(h) = g^{-1}hg$ є ізоморфізмом, і крім того маємо, що

$$\alpha(ph) = \alpha(p)\varphi(h),$$

для всіх $p \in Q$ і $h \in H$.

Нехай G — транзитивна група підстановок над множиною Q. *Еквівалентністю імпримітивності* групи G називається відношення еквівалентності θ на множині Q, яке є стійким стосовно дії групи G. Це еквівалентно тому, що

$$p \equiv q \mod \theta \qquad \Longrightarrow \qquad pg \equiv qg \mod \theta,$$

для всіх $g \in G$. Розбиття, породжене деякою еквівалентністю імпримітивності групи G на множині Q називається *розбиттям імпримітивності*.

Нехай θ — еквівалентність імпримітивності групи G. Дія групи G на класах еквівалентності θ визначає транзитивну групу підстановок, яка позначається через G_θ і називається *фактором імпримітивності* групи G для відношення θ.

Для довільного елемента q множини Q через $[q]$ позначимо клас еквівалентності $q \mod \theta$, і нехай K_q — транзитивна група підстановок над класом $[q]$, утворена звуженнями підстановок g на $[q]$ таких, що g не рухає елементи класу $[q]$, тобто це перевірка того, що $[q]g = [q]$.

Група K_q називається *групою, яка індукована групою* G на клас $[q]$.

Доведемо, що всі групи K_q, $q \in Q$ є еквівалентними. Справді, нехай $q, q' \in Q$ і $g \in G$ є такими, що $qg = q'$. Звуження α елемента g на клас $[q]$ є бієкцією з $[q]$ на $[q']$. Очевидно, що відображення α є ін'єктивним. Воно є сюр'єктивним, оскільки якщо $p \equiv q' \mod \theta$, то $pg^{-1} \equiv q \mod \theta$ і $\alpha(pg^{-1}) = p$. Нехай φ — ізоморфізм з групи K_q на групу $K_{q'}$, який визначається за формулою

$$p'\varphi(k) = \alpha(\alpha^{-1}(p')k) \qquad \text{для} \quad k \in K_q.$$

Це доводить, що групи K_q і $K_{q'}$ є еквівалентними. Зокрема, усі класи еквівалентності за $\mod \theta$ мають однакову потужність.

Кожна з еквівалентних транзитивних груп підстановок K_q називається *індукованою групою* групи G на класах еквівалентності імпримітивності θ і позначається через G^θ.

Якщо $d = \mathrm{Card}(Q)$ — степінь групи G, e — порядок групи G_θ і f — порядок групи G^θ, то $d = ef$. Справді, e є кількістю класів еквівалентності імпримітивності θ і f є спільною потужність кожного з класів за відношенням $\mod \theta$.

Транзитивна група підстановок G над множиною Q називається *примітивною*, якщо лише еквівалентності імпримітивності групи G є відношенням рівності й універсальним відношенням на множина Q.

Твердження 1.13.3. *Нехай G — транзитивна група підстановок над множиною Q, $q \in Q$ і H — стабілізатор елемента q. Група G є примітивною тоді і лише тоді, коли H — максимальна підгрупа в G.*

Доведення. Припустимо спочатку, що група G є примітивною. Нехай K — підгрупа в G така, що $H \subseteq K \subseteq G$. Розглянемо сім'ю підмножин множини Q, які мі мають вигляд qKg для $g \in G$. Довільні такі дві підмножини або збігаються, або не перетинаються. Справді, припустимо, що для деяких $k, k' \in K$ і $g, g' \in G$, маємо, що $qkf = qk'g'$. Тоді $qkgg'^{-1}k'^{-1} = q$, звідки випливає, що $kgg'^{-1}k'^{-1} \in H \subseteq K$. Отже $gg'^{-1} \in K$, звідки випливає, що $Kg = Kg'$, а отже $qKg = qKg'$. Таким чином, множини qKg утворюють розбиття множини Q, яке очевидно є розбиттям імпримітивності. Позаяк G — примітивна група, то маємо, що або $qK = \{q\}$, або $qK = Q$. У першому випадку $K = H$. У другому випадку маємо, що $K = G$, оскільки для довільного $g \in G$ існує деякий елемент $k \in K$ такий, що $qk = qg$, звідки випливає, що $gk^{-1} \in H \subseteq K$, а отже $g \in K$. Це завершує доведення того, що H є максимальною підгрупою в G.

Навпаки, нехай H — максимальна підгрупа групи G і θ — еквівалентність імпримітивності групи G. Означимо підгрупу

$$K = \{k \in G \colon qk \equiv q \mod \theta\}$$

в G. Тоді $H \subseteq K \subseteq G$, звідки випливає, що $K = H$ або $K = G$. Якщо $K = H$, то клас елемента q збігається з q, а отже відношення θ збігається з відношенням рівності на Q. Якщо $K = G$, то то клас елемента q збігається з множиною Q, а отже θ є універсальним відношенням на Q. Таким чином, група G є примітивною. □

Транзитивна група підстановок G над множиною Q називається *регулярною*, якщо всі елементи з $G \setminus \{1\}$ не мають нерухомих точок. Легко перевіряється, що в цьому випадку маємо, що виконується рівність

$$\mathrm{Card}(G) = \mathrm{Card}(Q).$$

Твердження 1.13.4. *Нехай G — транзитивна група підстановок над множиною Q і $q \in Q$. Група G є регулярною тоді і лише тоді, коли стабілізатор елемента q є одноелементною групою.*

Нехай $k \geqslant 1$ — ціле число. Група підстановок G над множиною Q називається *k-транзитивною*, якщо для довільних впорядкованих k-наборів

$$(p_1, p_2, \ldots, p_k) \in Q^k \qquad \text{і} \qquad (q_1, q_2, \ldots, q_k) \in Q^k,$$

які складається з різних елементів, існує елемент $g \in G$ такий, що

$$p_1 g = q_1, \quad p_2 g = q_2, \quad \ldots, \quad p_k g = q_k.$$

1-транзитивні групи є в точності транзитивними групами. Кожна k-транзитивна група для $k \geqslant 2$ є, очевидно, також $(k-1)$-транзитивною. Група $\mathfrak{S}_n$ є n-транзитивною.

Твердження 1.13.5. *Нехай $k \geqslant 1$ — ціле число. Група підстановок G над множиною Q є k-транзитивною тоді і лише тоді, коли звуження на множину $Q \setminus \{q\}$ стабілізатора елемента $q \in Q$ є $(k-1)$-транзитивним.*

Доведення. Необхідність є очевидною. Доведемо достатність.

Припустимо, що звуження на множину $Q \setminus \{q\}$ стабілізатора елемента $q \in Q$ є $(k-1)$-транзитивним для групи підстановок G над множиною Q, і нехай

$$(p_1, p_2, \ldots, p_k) \in Q^k \qquad \text{і} \qquad (q_1, q_2, \ldots, q_k) \in Q^k$$

— довільні впорядковані k-набори різних елементів. Позаяк група G є транзитивною, то існує елемент $g \in G$ такий, що $p_1 g = q_1$. Нехай H — стабілізатор точки q_1. Позаяк звуження підгрупи H на множину $Q \setminus \{q_1\}$ є $(k-1)$-транзитивним, то існує елемент $h \in H$ такий, що

$$p_2 gh = q_2, \ldots, p_k gh = q_k.$$

Оскільки $p_1 gh = q_1$, то підстановка $g' = gh$ задовольняє умову

$$p_1 g' = q_1, p_2 g' = q_2, \ldots, p_k g' = q_k.$$

Звідси випливає, що група G k-транзитивною. □

2-транзитивна група також називається *подвійно транзитивною*.

Твердження 1.13.6. *Кожна подвійно транзитивна група підстановок є примітивною.*

Доведення. Нехай G — подвійно транзитивна група підстановок над множиною Q. Розглянемо еквівалентність імпримітивності θ групи G. Якщо відношення θ не є рівністю на множині Q, то існують два різних елемента $q, q' \in Q$ такі, що $q \equiv q' \mod \theta$. Нехай $q'' \in Q$ — елемент відмінний від q. Позаяк група G є 2-транзитивною, то існує елемент $g \in G$ такий, що $qg = q$ і $q'g = q''$. Позаяк θ є еквівалентністю імпримітивності, то $q \equiv q'' \mod \theta$. Отже, θ є універсальним відношенням на множині Q. Звідси випливає, що група G є примітивною. □

Обернене висловлення до твердження 1.13.6 є хибним. Справді, для будь-якого первинного числа p циклічна група, породжена підстановкою $(12 \cdots p)$, є примітивною, але не подвійною транзитивною.

Цікавий випадок, коли обернене твердження до твердження 1.13.6 є істинним, описаний у знаменитій теоремі Шури (теорема 11.6.1), яка буде викладена в розділі 11.

Нотатки до розділу 1

Кожна з тем, які розглядаються в цій главі, є частиною теорії, яку ми розглядали лише дуже поверхнево. Більш повне викладення теорії слів можна знайти у монографії Лотара [131, 132]. Для автоматів (підрозділ 1.4) ми дотримуємось позначень з монографії Ейленберга [62]. Теорема 1.4.13 доведена Кліні.

Наше означення повного півкільця менш загальне, ніж у монографії [62], але цього буде достатньо для наших викладок. Повна постановка теореми Перрона–Фробеніуса (теорема 1.9.2) включає додаткові твердження, включаючи описання власних значень з максимальним модулем (див. [1, 2, 71]). Функцію r_M іноді називають *функцією Віланда*.

Наші подання ідеалів в моноїдах (підрозділ 1.12) описано більш докладно в монографіях Кліффорда та Престона [4, 52] або Лаллемана [5, 116]. Поняття первинного моноїда не є класичним, але добре вписується в ситуацію, яку ми знайдемо в розділі 9. 0-мінімальні ідеали первинних моноїдів зазвичай називаються цілком 0-простими напівгрупами. Для напівкілець і формальних рядів див. монографію [62] або [34].

Розділ 2

Коди

Перші два підрозділи містять декілька еквівалентних означень кодів і вільних підмоноїдів. У підрозділі 2.3 ми наводимо метод для перевірки того, що фіксована множина слів є кодом.

У підрозділі 2.4 ми використовуємо розподіли Бернуллі, щоб дати необхідну умову для того, що множина була кодом (теорема 2.4.5). Питання використання методів теорії ймовірності буде детальніше розроблено в розділі 13.

У підрозділі 2.5 вводиться вводить поняття повної множини. Це в певному сенсі поняття, дуальне до коду. Основний результат цього розділу (теорема 2.5.16) описує повні коди з використанням результатів про розподіли Бернуллі. У підрозділі 2.6 вводиться операція композиції кодів і встановлено декілька властивостей цієї операції. В останньому розділі вводиться префіксний граф коду як інструмент для описання ефективного алгоритму тестування, коли скінченна множина є кодом.

2.1 Означення

Цей підрозділ містить означення понять коду, префіксного (суфіксного, біфіксного) коду, максимального коду і кодуючого морфізму, а також у ньому наведені приклади цих понять.

Нехай A — алфавіт. Підмножина X вільного моноїда A^* називається *кодом* над A, якщо для всіх $n, m \geqslant 0$ та $x_1, \ldots, x_n, x'_1, \ldots, x'_m \in X$, з умови

$$x_1 \cdots x_n = x'_1 \cdots x'_m \tag{2.1}$$

випливає, що

$$n = m \qquad \text{і} \qquad x_i = x'_i \quad \text{для} \quad i = 1, \ldots, n. \tag{2.2}$$

Іншими словами, множина X є кодом, якщо будь-яке слово вільного моноїда X^* може бути однозначно записано як добуток слів у алфавіті X, тобто має унікальну факторизацію словами алфавіту X. Зокрема, код ніколи не містить порожнього слова 1. Зрозуміло, що будь-яка підмножина коду є кодом. Зокрема, порожня множина також є кодом. Елемент коду іноді називається *кодовим словом*.

Означення коду можна перефразувати так:

Твердження 2.1.1. *Якщо підмножина X вільного моноїда A^* є кодом, то довільне бієктивне відображення з деякого алфавіту B на X продовжується до ін'єктивного*

морфізму з B^* в A^*. Навпаки, якщо існує ін'єктивний морфізм $\beta\colon B^* \to A^*$ такий, що $X = \beta(B)$, то множина X є кодом.

Доведення. Нехай $\beta\colon B^* \to A^*$ — морфізм такий, що β відображає бієктивно алфавіт B на X. Нехай $u, v \in B^*$ — слова такі, що $\beta(u) = \beta(v)$. Покладемо $u = b_1 \cdots b_n$, $v = b'_1 \cdots b'_m$, де $n, m \geqslant 0$, $b_1 \dots b_n, b'_1 \cdots b'_m \in B$. Позаяк відображення $\beta\colon B^* \to A^*$ є морфізмом, то маємо, що

$$\beta(b_1) \cdots \beta(b_n) = \beta(b'_1) \cdots \beta(b'_m).$$

Але множина X є кодом і $\beta(b_i), \beta(b'_j) \in X$ для $i = 1, \dots, n$ і $j = 1, \dots, m$. Тоді $n = m$ і $\beta(b_i) = \beta(b'_i)$ для $i = 1, \dots, n$. Отже відображення β є ін'єктивним на B. Отож $b_i = b'_i$ для $i = 1, \dots, n$, і $u = v$. Звідси випливає, що $\beta\colon B^* \to A^*$ — ін'єктивний морфізм.

Навпаки, нехай $\beta\colon B^* \to A^*$ — ін'єктивний морфізм. Якщо

$$x_1, \cdots, x_n = x'_1, \cdots, x'_m \tag{2.3}$$

для деяких $n, m \geqslant 0$ та

$$x_1, \dots, x_n, x'_1, \dots, x'_m \in X = \beta(B),$$

то розглянемо літери $\beta(b_i), \beta(b'_j) \in B$ такі, що $\beta(b_i) = x_i$ і $\beta(b'_j) = x_j$, де $i = 1, \dots, n$ і $j = 1, \dots, m$. Позаяк морфізм $\beta\colon B^* \to A^*$ є ін'єктивним, то рівності (2.3) випливає, що $b_1 \cdots b_n = b'_1 \cdots b'_m$. Таким чином, отримуємо, що $n = m$ і $b_i = b'_i$ для $i = 1, \dots, n$, і звідси випливає, що $x_i = x'_i$ для $i = 1, \dots, n$. □

Ін'єктивний морфізм $\beta\colon B^* \to A^*$ вільних моноїдів такий, що $X = \beta(B)$, називається *морфізмом кодування* для коду X. Для довільного коду $X \subset A^*$ існування морфізму кодування для X доводиться просто: достатньо взяти будь-яку бієкцію множини B на X і продовжити її до морфізму з B^* в A^*. У цьому контексті алфавіт B називається *вихідним алфавітом*, а алфавіт A — *алфавітом каналу*.

Твердження 2.1.1 є першопричиною для термінології, оскільки слова в коді X кодуються літерами множини B. Процедура кодування складається з прив'язки до слова $b_1 b_2 \cdots b_n$ ($b_i \in B$), яке є вихідним текстом кодованого повідомлення $\beta(b_1)\beta(b_2)\cdots\beta(b_n)$ над алфавітом каналу за допомогою використання морфізму кодування β. Той факт, що морфізм кодування β є ін'єкційним, гарантує нам, що кодований текст однозначно розшифровується, щоб отримати оригінальний текст.

Приклад 2.1.2. Для довільного алфавіту A множина $X = A$ є кодом. Більш загально, якщо $p \geqslant 1$ — ціле число, то $X = A^p$ — це код, який називається *однорідним кодом* слів довжини p. Справді, якщо елементи множини X задовольняють рівняння (2.1), то з постійності довжини слів у X випливає висновок (2.2).

Приклад 2.1.3. Над алфавітом, що складається з однієї літери a, непорожня підмножина вільного моноїда a^* є кодом тоді і тільки тоді, коли він є одноелементною та відмінною від одиниці 1 вільного моноїда a^*.

Приклад 2.1.4. Множина $X = \{aa, baa, ba\}$ над алфавітом $A = \{a, b\}$ є кодом. Справді, якщо припустити протилежне, то існує слово w у вільній напівгрупі X^+, мінімальної довжини, що має дві різні факторизації:

$$w = x_1 x_2 \cdots x_n = x'_1 x'_2 \cdots x'_m$$

$(n, m \geqslant 0,\ x_i, x'_j \in X)$. Позаяк w — слово мінімальної довжини, то $x_1 \neq x'_1$. Отже, слово x_1 є власним префіксом слова x'_1, або навпаки слово x'_1 є власним префіксом слова x_1.

Припустимо, що слово x_1 є власним префіксом слова x'_1 (див. рис. 2.1). В іншому

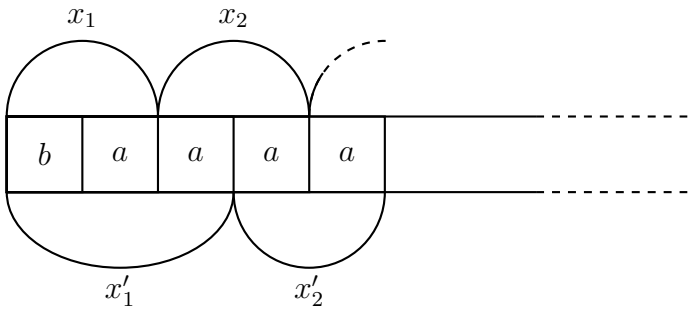


Рис. 2.1: Початок подвійної факторизації

випадку міркування аналогічні. Проаналізувавши множину X, отримуємо

$$x_1 = ba \qquad \text{і} \qquad x'_1 = baa.$$

Це в свою чергу означає, що

$$x_2 = aa \qquad \text{і} \qquad x'_2 = aa.$$

Отже

$$x'_1 = x_1 a \qquad \text{і} \qquad x'_1 x'_2 = x_1 x_2 a,$$

а якщо ми припустимо, що

$$x'_1 x'_2 \cdot x'_p = x_1 x_2 \cdots x_p a,$$

то звідси випливає, що

$$x_{p+1} = aa \qquad \text{і} \qquad x'_{p+1} = aa.$$

Таким чином, отримуємо, що

$$x'_1 x'_2 \cdot x'_{p+1} = x_1 x_2 \cdots x_{p+1} a,$$

а це суперечить тому, що слово w має дві різні факторизації.

Приклад 2.1.5. Множина $X = \{a, ab, ba\}$ над алфавітом $A = \{a, b\}$ не є кодом, оскільки слово $w = aba$ має дві різні факторизації

$$w = (ab)a = a(ba).$$

Наступний наслідок з твердження 2.1.1 ми будемо часто використовувати.

Наслідок 2.1.6. *Нехай A та C — алфавіти й $\alpha\colon A^* \to C^*$ — ін'єктивний морфізм. Якщо X є кодом над алфавітом A, то образ $\alpha(X)$ є кодом над алфавітом C. Якщо Y є кодом над алфавітом C, то повний прообраз $\alpha^{-1}(Y)$ є кодом над алфавітом A.*

Доведення. Нехай $\beta\colon B^* \to A^*$ — морфізм кодування для коду X. Тоді $\alpha(\beta(B)) = \alpha(X)$ і позаяк $\alpha \circ \beta\colon B^* \to C^*$ є ін'єктивним морфізмом, то з твердження 2.1.1 випливає, що образ $\alpha(X)$ є кодом над алфавітом C.

Навпаки, нехай $X = \alpha^{-1}(Y)$ і нехай $n, m \geqslant 1$, $x_1, \ldots, x_n, x'_1, \ldots, x'_m \in X$ будуть такі, що

$$x_1 \cdots x_n = x'_1 \cdots x'_m.$$

Тоді

$$\alpha(x_1) \cdots \alpha(x_n) = \alpha(x'_1) \cdots \alpha(x'_m).$$

Нехай тепер Y є кодом. Тоді $n = m$ і $\alpha(x_i) = \alpha(x'_i)$ для $i = 1, \ldots, n$. З ін'єктивності морфізму $\alpha\colon A^* \to C^*$ випливає, що $x_i = x'_i$ для $i = 1, \ldots, n$, а отже множина X є кодом. □

Наслідок 2.1.7. *Нехай A — алфавіт. Якщо підмножина X вільного моноїда A^* є кодом над A, то X^n є кодом над A для довільного додатнього цілого числа n.*

Доведення. Нехай $\beta\colon B^* \to A^*$ — морфізм кодування для коду X. Тоді $X^n = \beta(B^n)$. Але B^n є кодом. Далі застосуємо наслідок 2.1.6. □

Приклад 2.1.8. Ми покажемо, що добуток двох кодів не обов'язково є кодом. Розглянемо множини

$$X = \{a, ba\} \qquad \text{і} \qquad Y = \{a, ab\},$$

які очевидно є кодами над алфавітом $A = \{a, b\}$. Покладемо $Z = XY$. Тоді

$$Z = \{aa, aab, baa, baab\}.$$

Позаяк слово $w = aabaab$ має дві різні факторизації:

$$w = (aa)(baab) = (aab)(aab),$$

то множина Z не є кодом над алфавітом A.

Далі ми введемо важливий клас кодів, які називаються префіксними кодами.

Нехай A — довільний алфавіт. Підмножина X вільного моноїда A^* називається *префіксною*, якщо жоден елемент множини X не є власним префіксом іншого елемента з X. Це означення еквівалентне такій умові: підмножина X вільного моноїда A^* є префіксною, якщо

$$x \leqslant x' \quad \Longrightarrow \quad x = x', \tag{2.4}$$

для всіх $x, x' \in X$, Це можна перефразувати так: довільні два різни елементи множини X є непорівнянними в префіксному порядку.

Безпосередньо з умови (2.4) випливає, що префіксна множина X, яка містить порожнє слово, складається з порожнього слова. Суфіксні множини визначаються симетричним чином. Підмножина X вільного моноїда A^* називається *суфіксною*, якщо жоден елемент множини X не є власним суфіксом іншого елемента з X. Підмножина X вільного моноїда A^* називається *біфіксною*, якщо вона одночасно є префіксною та суфіксною. Очевидно, що підмножина X вільного моноїда A^* є суфіксною тоді і лише тоді, коли її обернена множина $\widetilde{X}$ є префіксною.

Твердження 2.1.9. *Кожна префіксна (суфіксна, біфіксна) множина слів $X \neq \{1\}$ є кодом.*

Доведення. Позаяк $X \neq \{1\}$, то множина X не містить порожнього слова. Якщо множина X не є кодом, то існує слово w мінімальної довжини, яке має дві різні факторизації

$$w = x_1x_2\cdots x_n = x'_1x'_2\cdots x'_m \qquad (x_i, x'_j \in X).$$

Обідва слова x_1, x'_1 є непорожніми, і оскільки слово w має мінімальну довжину, то $x_1 \neq x'_1$. Але тоді виконується одна з умов: $x_1 < x'_1$ або $x'_1 < x_1$, що суперечить тому, що X є префіксною множиною. Отже X є кодом.

У випадку суфіксної множини доведення є аналогічним. □

Префіксним кодом (*суфіксним кодом*, *біфіксним кодом*) називається префіксна (суфіксна, біфіксна) множина слів, яка є кодом, тобто відрізняється від $\{1\}$.

Приклад 2.1.10. Однорідні коди є біфіксні. Множини $X = \{a, ba\}$ і $Y = \{a, ab\}$ над алфавітом $A = \{a, b\}$ з прикладу 2.1.8 є префіксним та суфіксним кодами, відповідно.

Приклад 2.1.11. Множини $X = a^*ba$ і $Y = \{a^nb^n : n > 0\}$ над алфавітом $A = \{a, b\}$ є префіксними, а отже є префіксним кодами. Множина Y є суфіксною, а отже є біфіксною, але множина X не є суфіксною. Цей приклад показує, що існують нескінченні (префіксні, суфіксні та біфіксні) коди над скінченним алфавітом.

Приклад 2.1.12. *Код Морзе* (*азбука Морзе*) ототожнює з кожним алфавітно-цифровим символом послідовність точок і тире. Наприклад, літера A кодується "·—", а P кодується "·——·". Якщо кожне кодове слово завершується додатковим символом (зазвичай пробілом, який називається "пауза'), код Морзе стає префіксним кодом.

Код X називається *максимальний* над алфавітом A, якщо X не міститься як власна підмножина в жодному іншому коді над A, тобто якщо

$$X \subseteq X' \quad \text{і} \quad X' - \text{код}, \quad \text{то} \qquad X = X'.$$

Максимальність коду залежить від алфавіту над яким він взятий. Справді, якщо $X \subset A^*$ і $A \subsetneq B$, то $X \subset B^*$ і X, безумовно, не є максимальним над алфавітом B, навіть якщо він є максимальним кодом над алфавітом A. Означення максимального коду не дає алгоритму, який дозволяє нам перевірити, що він виконується. Проте, максимальність є вирішальною, принаймні для розпізнаваних кодів (див. підрозділ 2.5).

Приклад 2.1.13. Однорідні коди A^n є максимальними над алфавітом A. Припустимо протилежне. Тоді існує слово $u \in A^+ \setminus A^n$ таке, що $Y = A^n \cup \{u\}$ є кодом. Слово $w = u^n$ належить вільному моноїдові Y^*, і воно також є елементом вільного моноїда $(A^n)^*$, оскільки його довжина є кратною натуральному числу n. Отже отримуємо, що $w = u^n = x_1x_2\cdots x_{|u|}$ для деяких $x_1, \ldots, x_{|u|} \in A^n$. Очевидно, що $u \notin A^n$. Таким чином, дві факторизації слова w є різними, а отже Y не є кодом над алфавітом A і A^n є максимальним кодом.

Твердження 2.1.14. *Кожен код X над алфавітом A міститься в максимальному коді над A.*

Доведення. Нехай $\mathcal{F}$ — множина усіх кодів над алфавітом A, які містять код X. Впорядкуємо множину $\mathcal{F}$ стосовно відношення включення. Для того, щоб показати, що $\mathcal{F}$ містить максимальний елемент, за лемою Цорна достатньо довести, що кожен ланцюг $\mathcal{C}$ в $\mathcal{F}$ містить точну верхню грань у $\mathcal{F}$.

Розглянемо довільний ланцюг $\mathcal{C}$ кодів, які містять код X. Тоді

$$\widehat{Y} = \bigcup_{Y \in \mathcal{C}} Y$$

є точкою верхньою гранню ланцюга $\mathcal{C}$. Залишилось довести, що множина $\widehat{Y}$ є кодом над алфавітом A. Нехай

$$y_1 \cdots y_n = y'_1 \cdots y'_m$$

для деяких $y_1, \ldots, y_n, y'_1, \ldots, y'_m \in \widehat{Y}$ і $n, m \geqslant 1$. Кожен з елементів y_i, y'_j належить до деякого коду з ланцюга $\mathcal{C}$ і це визначає $n + m$ елементів (не обов'язково різних) ланцюга $\mathcal{C}$. Один з них, позначимо його через Z, містить всі інші коди. Отже $y_1, \ldots, y_n, y'_1, \ldots, y'_m \in Z$, і оскільки Z є кодом, то отримуємо, що $n = m$ і $y_i = y'_i$ для $i = 1, \ldots, n$. Звідси випливає, що $\widehat{Y}$ є кодом над алфавітом A. □

Зауважимо, що твердження 2.1.14 не поширюється на скінченні коди. Існують скінченні коди, які не містяться в жодному максимальному скінченному коді. Приклад такого коду буде викладено в підрозділі 2.5 (приклад 2.5.7).

Той факт, що множина $X \subset A^*$ є кодом, допускає дуже просте вираження в термінології формальних степеневих рядів:

Твердження 2.1.15. *Нехай A — алфавіт, X — підмножина вільної напівгрупи A^+ і $M = X^*$ — підмоноїд в A^*, породжений множиною X. Тоді множина X є кодом тоді і лише тоді, коли $\underline{M} = (\underline{X})^*$, або еквівалентно $\underline{M} = (1 - \underline{X})^{-1}$.*

Доведення. За твердженням 1.7.4 коефіцієнт характеристичного ряду $((\underline{X})^*, w)$ слова w у вільному моноїді $(\underline{X})^*$ дорівнює кількості різних факторизацій слова w словами в множині X. За означенням множина X є кодом тоді і лише тоді, коли цей коефіцієнт набуває значення 0 і 1 для довільного слова в A^*. Але це еквівалентно тому, що $(\underline{X})^*$ є характеристичним рядом його носія, тобто, що $(\underline{X})^* = \underline{M}$. □

2.2 Коди та вільні підмоноїди

Підмоноїд X^*, породжений кодом X іноді простіше досліджувати, ніж сам код. Той факт, що множина X є кодом (префіксним кодом, біфіксним кодом) еквівалентний властивості, що X^* є вільним моноїдом (правоунітаним моноїдом, біунітарним моноїдом). Ці властивості можна перевірити безпосередньо на підмоноїді без будь-якого явного описання його бази. Таким чином, ми можемо довести, що множини є кодами, знаючи лише підмоноїди, які вони породжують.

Ми почнемо із загальної властивості. Надалі через A будемо позначати деякий непорожній алфавіт.

Твердження 2.2.1. *Кожен підмоноїд M вільного моноїда A^* має єдину мінімальну множину породжуючих елементів*

$$X = (M \setminus \{1\}) \setminus (M \setminus \{1\})^2.$$

Доведення. Нехай $Q = M \setminus \{1\}$. Спочатку перевіримо чи множина X породжує моноїд M, тобто доведемо, що виконується рівність $X^* = M$. Позаяк $X \subseteq M$, то $X^* \subseteq M$. Ми доведемо обернене включення за індукцією по довжині слів. Очевидно, що $1 \in X^*$. Нехай $m \in Q$. Якщо $m \notin Q^2$, то $m \in X$. У протилежному випадку маємо $m = m_1 m_2$ для $m_1, m_2 \in Q$ і обидва ці слова мають меншу довжину за довжину слова m. Отже слова m_1 і m_2 є елементами вільного моноїда X^* за припущенням індукції та $m \in X^*$.

Тепер нехай Y — множина породжуючих елементів моноїда M. Ми можемо припускати, що $1 \notin Y$. Тоді кожен елемент $x \in X$ є елементом вільного моноїда Y^* і таким чином його можна записати у вигляді $x = y_1 y_2 \cdots y_n$, де $y_i \in Y$ і $n \geqslant 0$. З того факту, що $x \neq 1$ і $x \notin Q^2$ випливає, що $n = 1$ і $x \in Y$. Це доводить, що $X \subseteq Y$. Таким чином X є мінімальною множиною породжуючих елементів моноїда M і ця множина єдина. □

Приклад 2.2.2. Нехай $A = \{a, b\}$ і $M = \{w \in A^* \colon |w|_a \equiv 0 \mod 2\}$. Тоді ми обчислимо

$$X = (M \setminus \{1\}) \setminus (M \setminus \{1\})^2 = b \cup ab^*a.$$

Ми тепер повернемося до вивчення підмоноїдів, породжених кодом. За означенням, підмоноїд M вільного моноїда A^* називається *вільним*, якщо існує ізоморфізм

$$\alpha \colon B^* \to M$$

вільного моноїда B^* на моноїд M.

Твердження 2.2.3. *Якщо M — вільний підмоноїд вільного моноїда A^*, то його мінімальна множина породжуючих елементів є кодом. Навпаки, якщо $X \subseteq A^*$ є кодом, то підмоноїд X^* вільного моноїда A^* є вільним і X є його мінімальною множиною породжуючих елементів.*

Доведення. Нехай $\alpha \colon B^* \to M$ — морфізм. Тоді відображення α, якщо на нього дивитися як на морфізм з B^* в A^*, є ін'єктивним. За твердженням 2.1.1, множина $X = \alpha(B)$ є кодом. Далі $M = \alpha(B^*) = (\alpha(B))^* = X^*$, а отже множина X породжує моноїд M. Більше того $B = B^+ \setminus B^+B^+$ і $\alpha(B^+) = M \setminus \{1\}$. Отож, $X = (M \setminus \{1\}) \setminus (M \setminus \{1\})^2$, а це доводить, що X є мінімальною множиною породжуючих елементів моноїда M.

Навпаки, припустимо, що $X \subseteq A^*$ є кодом. Розглянемо кодуючий морфізм $\alpha\colon B^* \to A^*$ для коду X. Тоді α — ін'єктивне відображення й α — бієктивне відображення з B на X. Отже α є бієкцією з B^* на $\alpha(B^*) = X^*$. Звідси випливає, що підмоноїд X^* вільного моноїда A^* є вільним. Тепер, оскільки α — бієкція, то з $B = B^+ \setminus B^+B^+$ випливає, що $X = X^+ \setminus X^+X^+$. За твердженням 2.2.1, X є мінімальною множиною породжуючих елементів моноїда M. □

Код X, який породжує вільний підмоноїд M вільного моноїда A^* називається *базою* моноїда M.

Наслідок 2.2.4. *Нехай X і Y — коди над алфавітом A. Якщо $X^* = Y^*$, то $X = Y$.*

Приклад 2.2.5. Множина

$$X = (M \setminus \{1\}) \setminus (M \setminus \{1\})^2 = b \cup ab^*a,$$

означена в прикладі 2.2.2 є (біфіксним) кодом, а отже M є вільним підмоноїдом вільного моноїда A^*.

За твердженням 2.2.3 можна виділити два випадки, коли множина X не є кодом. По-перше, коли X не є мінімальною породжуючою множиною моноїда $M = X^*$, тобто існує рівність

$$x = x_1x_2 \cdots x_n$$

з $x, x_1, \ldots, x_n \in X$ і $n \geqslant 2$. Зауважимо, що, незважаючи на цей факт, моноїд M може бути вільним. Інший випадок виконується, коли X є мінімальною множиною породжуючих елементів, але моноїд M не є вільним (це випадок, розглянутий у прикладі 2.1.5).

Тепер наведемо характеристику вільних підмоноїдів вільного моноїда A^*, яка є внутрішнім у тому сенсі, що він не спирається на бази. Інша незначна характеристика наведена у вправі 2.8.4.

Нехай M — моноїд. Підмоноїд N моноїда M називається *стійким* (в M), якщо

$$u, v, uw, wv \in N \qquad \Longrightarrow \qquad w \in N, \tag{2.5}$$

для всіх $u, v, w \in M$. Гіпотезу (2.5) можна записати так:

$$w \in N^{-1}N \cap NN^{-1},$$

таким чином умовою стабільності стає

$$N^{-1}N \cap NN^{-1} \subseteq N,$$

або просто

$$N^{-1}N \cap NN^{-1} = N, \tag{2.6}$$

оскільки $1 \in N$, а отже

$$N \subseteq N^{-1}N \cap NN^{-1}.$$

На рис. 2.2 наведено зображення гіпотези (2.5), коли елементи u, v і w є словами. Членство в моноїді N зображено дугою.

Стійкі підмоноїди появляються майже у всіх підрозділах цієї книги. Причиною цього є твердження 2.2.6, яке дає примітивну характеристику вільних підмоноїдів вільного моноїда. Як практичне застосування, це твердження використовується для того, щоб довести, що деякі підмоноїди є вільними, і тому їх базами є кодами.

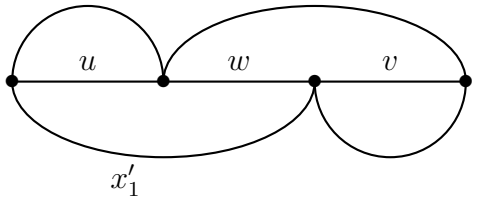


Рис. 2.2: Зображення стабільності

Твердження 2.2.6. *Підмоноїд N вільного моноїда A^* є стійким тоді і лише тоді, коли він вільний.*

Доведення. Припустимо спочатку, що підмоноїд N вільного моноїда A^* є стійким. Покладемо

$$X = (N \setminus \{1\}) \setminus (N \setminus \{1\})^2.$$

Припустимо протилежне, що X не є кодом. Тоді існує слово $z \in N$ мінімальної довжини, яке має дві різні факторизації в словах множини X:

$$z = x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m,$$

де $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m \in X$. Не зменшуючи загальності, можемо вважати, що $|x_1| < |y_1|$. Тоді $y_1 = x_1 w$ для деякого непорожнього слова w. Звідси випливає, що

$$x_1, \qquad y_2 \cdots y_m, \qquad x_1 w = y_1, \qquad w y_2 \cdots y_m = x_2 \cdots x_n$$

є всі елементами моноїда N. Позаяк моноїд N є стійким, то $w \in N$. Отож, отримуємо, що $y_1 = x_1 w \notin N$. Отримали протиріччя. Отже множина X кодом.

Навпаки, припустимо, що підмоноїд N є вільним і нехай X — його база. Нехай $u, v, w \in A^*$ і припустимо, що $u, v, uw, wv \in N$. Покладемо

$$u = x_1 \cdots x_k, \qquad wv = x_{k+1} \cdots x_r, \qquad uw = y_1 \cdots y_l, \qquad v = y_{l+1} \cdots y_s,$$

з $x_1, \ldots, x_r, y_1, \ldots, y_s \in X$. З рівності $u(wv) = (uw)v$ випливає, що

$$x_1 \cdots x_k x_{k+1} \cdots x_r = y_1 \cdots y_l y_{l+1} \cdots y_s.$$

Таким чином, $r = s$ і $x_i = y_i$ $(i = 1, \ldots, s)$, оскільки множина X є кодом. Більше того, $l \geqslant k$ оскільки $|uw| \geqslant |u|$, звідки випливає, що

$$uw = x_1 \cdots x_k x_{k+1} \cdots x_l = u x_{k+1} \cdots x_l,$$

а отже $w = x_{k+1} \cdots x_l$. Таким чином, підмоноїд N вільного моноїда A^* є стійким. □

Підмоноїди, які породжуються префіксними кодами, також можна охарактеризувати умовою, яка не залежить від бази. Нехай M — моноїд і N — підмоноїд моноїда M. Тоді N називається *унітарним справа* в M, якщо

$$u, uv \in N \qquad \Longrightarrow \qquad v \in N.$$

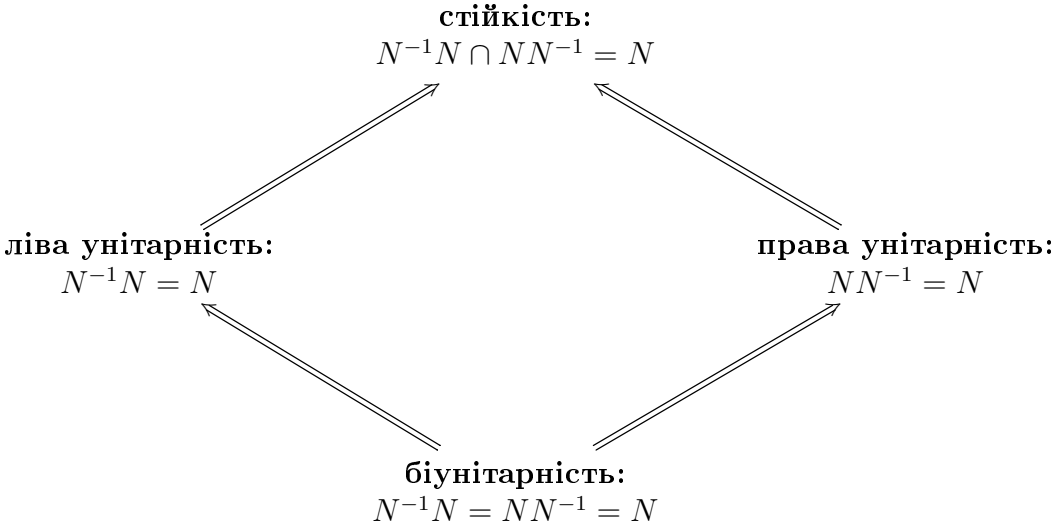
для всіх $u, v \in M$. Симетрично, підмоноїд N називається *унітарним зліва* в M, якщо

$$u, vu \in N \qquad \Longrightarrow \qquad v \in N.$$

для всіх $u, v \in M$. Ці умови можна переписати наступним чином: підмоноїд N є унітарним справа тоді і лише тоді, коли $N^{-1}N = N$, і N є унітарним зліва тоді і лише тоді, коли $NN^{-1} = N$.

Підмоноїд N моноїда M називається *біунітарним*, якщо він є одночасно унітарним справа й унітарним зліва.

Ці чотири властивості підмоноїда стійкість, унітарність зліва, унітарність справа та біунітарність мають однакову природу. Взаємовідношення між ними можна описати так:



Приклад 2.2.7. Підмоноїд M вільного моноїда A^*, означений в прикладі 2.2.2, є біунітарним. Справді, якщо $u, uv \in M$, то $|u|_a$ і $|uv|_a = |u|_a + |v|_a$ є парними числами. Звідки випливає, що $|v|_a$ – парне число та $v \in M$. Отже підмоноїд M є унітарним справа.

Приклад 2.2.8. У теорії груп поняття стійкого, унітарного та біунітарного виснажуються і збігаються з поняттям підгрупи. Справді, нехай H — стійкий підмоноїд групи G. Для всіх $h \in H$ обидва елементи hh^{-1} і $h^{-1}h$ є елементами підмоноїда H. Стійкість означає, що $h^{-1} \in H$. Отже, H є підгрупою групи G. Якщо H — підгрупа групи G, то, навпаки, отримуємо, що $HH^{-1} = H^{-1}H = H$, що показує, що H як підмоноїд є біунітарним.

Наступне твердження показує взаємозв'язок між підмоноїдами, які ми визначили, і кодами.

Твердження 2.2.9. *Підмоноїд M вільного моноїда A^* є унітарним справа (відп. унітарним зліва, біунітарним) тоді і лише тоді, коли мінімальна множина породжуючих елементів моноїда M є префіксним кодом (відп. суфіксним кодом, біфіксним кодом). Зокрема, а унітарний справа (відп. унітарний зліва, біунітарний) підмоноїд вільного моноїда A^* є вільним.*

Доведення. Нехай $M \subseteq A^*$ — підмоноїд, $Q = M \setminus \{1\}$ і нехай $X = Q \setminus Q^2$ — мінімальна породжуюча множина моноїда M. Припустимо, що підмоноїд M вільного моноїда A^* є унітарним справа.

Для доведення того, що множина X є префіксною, припустимо, що $x, xu \in X$ для деякого $u \in A^*$. Тоді $x, xu \in M$, а отже $u \in M$. Якщо $u \neq 1$, то $u \in Q$; але тоді висловлення $xu \in Q^2$ суперечить припущенню. Отож, $u = 1$ і множина X є префіксною.

Навпаки, припустимо, що множина X є префіксною. Нехай $u, v \in A^*$ — такі елементи, що $u, uv \in M = X^*$. Тоді

$$u = x_1 \cdots x_n, \qquad uv = y_1 \cdots y_m$$

для деяких $x_1, \ldots, x_n, y_1, \ldots, y_m \in X$. Внаслідок цього отримуємо, що

$$x_1 \cdots x_n v = y_1 \cdots y_m.$$

Позаяк множина X є префіксною, то жодне зі слів ні x_1, ні y_1 не є власним префіксом іншого. Звідси випливає, що $x_1 = y_1$, і з аналогічних міркувань отримуємо, що $x_2 = y_2, \ldots, x_n = y_n$. Це доводить, що $m \geqslant n$ і $v = y_{n+1} \cdots y_m \in M$. Отже підмоноїд M вільного моноїда A^* є унітарним справа. □

Нехай M — вільний підмоноїд вільного моноїда A^*. Тоді моноїд M називається *максимальним*, якщо $M \neq A^*$ і M не є власним вільним підмоноїдом іншого вільного підмоноїда відмінного від A^*.

Твердження 2.2.10. *Якщо моноїд M є максимальним вільним підмоноїдом вільного моноїда A^*, то його база X є максимальним кодом.*

Доведення. Нехай Y — код над алфавітом A з $X \subsetneq Y$. Тоді $X^* \subseteq Y^*$ і $X^* \neq Y^*$, оскільки в протилежному випадку $X = Y$ за наслідком 2.2.4. Отримали, що вільний підмоноїд X^* вільного моноїда A^* є максимальним. Отже $Y^* = A^*$ і $Y = A$. Отож, отримуємо, що $X \subsetneq A$. Нехай $b \in A \setminus X$. Множина $Z = X \cup b^2$ є кодом і $M \subsetneq Z^* \subsetneq A^*$. Обидва включення є строгими, оскільки $b^2 \notin M$ і $b \notin Z^*$. Це суперечить максимальності вільного підмоноїда M. □

Зауважимо, що обернене твердження до твердження 2.2.10 є хибним, оскільки однорідні коли A^n $(n \geqslant 1)$ є максимальними. Але якщо $k, n \geqslant 2$, то маємо $(A^{kn})^* \subsetneq (A^n)^* \subsetneq A^*$, і це доводить, що вільний підмоноїд $(A^{kn})^*$ вільного моноїда A^* не є максимальним.

Тепер ми введемо сім'ю біфіксних кодів, які називаються груповими кодами, які мають цікаві властивості. Перш ніж дати цк означення, розглянемо таку ситуацію.

Нехай G — група, H — підгрупа в G і

$$\varphi\colon A^* \to G \tag{2.7}$$

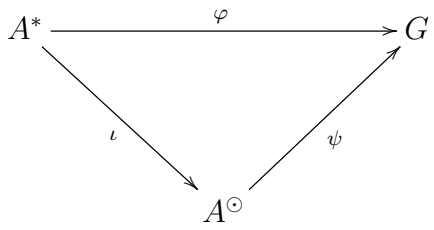
є морфізмом. Підмоноїд

$$M = \varphi^{-1}(H) \tag{2.8}$$

вільного моноїда A^* є біунітарним. Справді, якщо, наприклад, $p, pq \in M$, то $\varphi(p), \varphi(pq) \in H$, а тому $\varphi(p)^{-1}\varphi(pq) = \varphi(q) \in H$ і $q \in M$. Аналогічно доводиться,

що моноїд M унітарним зліва. Таким чином, база моноїда M, наприклад множина X, є біфіксним кодом.

Означення підмоноїда M у формулі (2.8) еквівалентно описанню як перетин вільного моноїда A^* з підгрупою вільної групи $A^\odot$ над алфавітом A. Справді, морфізм φ у формулі (2.7) факторизується єдиним чином в діаграмі



з канонічним ін'єктивним відображенням ι. Поклавши $Q = \psi^{-1}(H)$, отримуємо

$$M = Q \cap A^*.$$

Навпаки, якщо Q — підгрупа вільної групи $A^\odot$ і $M = Q \cap A^*$, то

$$M = \iota^{-1}(Q).$$

Груповим кодом називається база X підмоноїда $M = \varphi^{-1}(H)$, де φ — морфізм, який визначається за формулою (2.7) і крім того припускається, що він є сюр'єктивним. Тоді множина X є біфіксним кодом і X є максимальним кодом. Справді, якщо $M = A^*$, то код $X = A$ є максимальним. У протилежному випадку, візьмемо слово $w \in A^* \setminus M$ і покладемо $Y = X \cup w$. Перевіримо, що множина Y не є кодом. Покладемо $m = \varphi(w)$. Оскільки відображення φ є сюр'єктивним, то існує слово $\overline{w} \in A^*$ таке, що $\varphi(\overline{w}) = m^{-1}$. Обидва слова $u = w\overline{w}$ і $v = \overline{w}w$ є елементами моноїда M, і $w\overline{w}w = uw = wv \in Y^*$. Слово $w\overline{w}w$ має дві різні факторизації словами алфавіта Y, а саме слово uw утворюється з слів алфавіту X, за якими слідує слово з алфавіту Y, та слово wv, яке складається зі слів утворених оберненим порядком: спочатку йдуть слова алфавіту Y, а потім слова алфавіту X. Таким чином, множина Y не є кодом, а отже код X є максимальним.

Наведемо три приклади групових кодів.

Приклад 2.2.11. Нехай $A = \{a, b\}$ і розглянемо множину

$$M = \{w \in A^* \colon |w|_a \equiv 0 \mod 2\}$$

з прикладу 2.2.2. Маємо $M = \varphi^{-1}(0)$, де

$$\varphi \colon A^* \to \mathbb{Z}/2\mathbb{Z}$$

є морфізм, породжений відображенням $\varphi \colon A \to \mathbb{Z}/2\mathbb{Z}$, $\varphi(a) = 1$ і $\varphi(b) = 0$. Таким чином, база моноїда M, а саме множина $X = b \cup ab^*a$, є груповим кодом, а отже є максимальним кодом.

Приклад 2.2.12. Однорідний код A^m над алфавітом A є груповим кодом. Моноїд $(A^m)^*$ є насправді ядром морфізму вільного моноїда A^* на групу $\mathbb{Z}/m\mathbb{Z}$, який відображає всі літери алфавіту A на число 1.

Приклад 2.2.13. Нехай $A = \{a, b\}$ і розглянемо підмоноїд

$$\{w \in A^* \colon |w|_a = |w|_b\} \tag{2.9}$$

вільного моноїда A^*, який складається зі слів алфавіту A, що мають багато літер a і b. Нехай

$$\delta \colon A^* \to \mathbb{Z}$$

є морфізм, породжений відображенням $\delta \colon A \to \mathbb{Z}$, $\delta(a) = 1$ і $\delta(b) = -1$. Очевидно, що

$$\delta(w) = |w|_a - |w|_b$$

для довільного слова $w \in A^*$. Таким чином, множина (2.9) збігається з повним прообразом $\delta^{-1}(0)$. База моноїда $\delta^{-1}(0)$ позначається через D або через D_1, сам підмоноїд позначається через D^* або D_1^*. Слова над алфавітом D називаються "*Dyck-primes*" (*первинними числами за Диком*), множина D називається *кодом Дика* над алфавітом A, а множина D^* — *множиною Дика* над алфавітом A.

Приклад 2.2.14. Більш загально, нехай $A = B \cup \overline{B}$, де $B \cap \overline{B} = \varnothing$, є алфавіт, який складається з $2n$ літер, і нехай

$$\delta \colon A^* \to B^{\odot}$$

є морфізм вільного моноїда A^* у вільну групу $B^{\odot}$, породжений відображенням $\delta \colon A \to B^{\odot}$, $\delta(b) = b$ і $\delta(\bar{b}) = b^{-1}$, для $b \in B$ і $\bar{b} \in \overline{B}$. База підмоноїда $\delta^{-1}(1)$ вільного моноїда A^* позначається через D_n і називається *кодом Дика* над алфавітом A, або *кодом Дика над n-літерами*.

Перейдемо тепер до дещо іншої теми і розглянемо вільні підмоноїди A^*, що містять заданий підмоноїд. Почнемо з наступного спостереження, яке випливає з твердження 2.2.6.

Твердження 2.2.15. *Непорожній перетин довільної сім'ї вільних підмоноїдів вільного моноїда A^* є вільним підмоноїдом у A^*.*

Доведення. Нехай $(M_i)_{i \in \mathscr{I}}$ — сім'я вільних підмоноїдів вільного моноїда A^*. Покладемо $M = \bigcap_{i \in \mathscr{I}} M_i$ і припустимо, що $M \neq \varnothing$. Очевидно, що M підмоноїд у A^*, і достатньо довести, що M є стійким. Якщо

$$u, vw, uv, w \in M,$$

то ці чотири слова належать до кожного з моноїдів M_i. Оскільки кожен з моноїдів M_i є стійким, то $w \in M_i$ для кожного $i \in \mathscr{I}$. Отож, $w \in M$. □

Твердження 2.2.15 спонукає до наступних міркувань. Нехай X — підмножина вільного моноїда A^*. Як ми вже бачили, перетин усіх вільних підмоноїдів вільного моноїда A^*, які містить множину X, знову є вільним підмоноїдом. Це найменший вільний підмоноїд вільного моноїда A^*, який містить множину X. Ми називатимемо його *вільною оболонкою* множини X. Якщо X^* — вільний підмоноїд, то він, звичайно, збігається з його вільною оболонкою.

Нехай X — підмножина вільного моноїда A^*, N — вільна оболонка множини X і Y — база вільного підмоноїда N. Якщо X не є кодом, то $X \neq Y$. Наступний результат, який відомий, як *теорема про дефект* описує цікаве співвідношення між множинами X і Y.

Теорема 2.2.16 (теорема про дефект). *Нехай X — підмножина вільного моноїда A^* і Y — база вільної оболонки множини X. Якщо X не є кодом, то*

$$\operatorname{Card}(Y) \leqslant \operatorname{Card}(X) - 1.$$

Наступний результат є наслідком теореми 2.2.16, і він доводиться безпосередньо (див. вправу 2.8.2).

Наслідок 2.2.17. *Нехай $X = \{x_1, x_2\}$. Тоді X кодом тоді і лише тоді, коли x_1 і x_2 не є степенями деякого слова.*

Зауважимо, що наслідок 2.2.17 повністю описує коди з двома елементами. Випадок множини з трьома словами є вже набагато складнішим (див. вправи 2.8.20 і 2.8.21).

Для доведення теореми 2.2.16 нам буде потрібний такий результат:

Твердження 2.2.18. *Нехай X — підмножина вільного моноїда A^* і Y — база вільної оболонки множини X. Тоді*

$$Y \subseteq X(Y^*)^{-1} \cap (Y^*)^{-1}X,$$

тобто кожне слово в множині Y появляється як перший (відп. останній) множник у факторизації деякого слова $x \in X$ у словах, що належать базі Y.

Доведення. Припустимо, що слово $y \in Y$ не появляється в $(Y^*)^{-1}X$. Тоді

$$X \subseteq \{1\} \cup Y^*(Y \setminus \{y\}).$$

Взявши

$$Z = y^*(Y \setminus \{y\}),$$

маємо, що $Z^+ = Y^*(Y \setminus \{y\})$, а отже $X \subseteq Z^*$. Підмоноїд Z^* в A^* є вільним. Справді, кожне слово $z \in Z^*$ має єдину факторизацію

$$z = y_1 y_2 \cdots y_n, \qquad y_1, \ldots, y_n \in Y, \qquad y_n \neq y,$$

а отже може бути записане як

$$z = y^{p_1} z_1 y^{p_2} z_2 \cdots y^{p_r} z - r, \qquad z_1, \ldots, z_r \in Y \setminus \{y\}, \qquad p_1 \geqslant 0, \ldots, p_r \geqslant 0.$$

Отримуємо, що $X \subseteq Z^* \subsetneq Y^*$, звідки випливає, що Y^* не є вільною оболонкою множини X, а це суперечить припущенню. □

Доведення теореми 2.2.16. Якщо множина X містить порожнє слово, то X і $X' = X \setminus \{1\}$ мають одинакові вільні оболонки Y^*. Якщо твердження теореми виконується для множини X', то воно виконується і для множини X, оскільки якщо X' є кодом, то $Y = X'$ і $\operatorname{Card}(Y) = \operatorname{Card}(X) - 1$, а в іншому випадку

$$\operatorname{Card}(Y) \leqslant \operatorname{Card}(X') - 1 \leqslant \operatorname{Card}(X) - 2.$$

Таким чином, ми можемо припускати, що $1 \notin X$. Нехай $\alpha\colon X \to Y$ — відображення, означене за формулою

$$\alpha(x)y, \qquad \text{якщо} \quad x \in yY^*.$$

Це відображення визначається однозначно, оскільки множина Y є кодом. Це відображення також всюди визначене, оскільки $X \subseteq Y^*$. За твердженням 2.2.18 відображення α є сюр'єктивним. Якщо множина X не є кодом, то існує відношення

$$x_1 x_2 \cdots x_n = x'_1 x'_2 \cdots x'_m, \qquad x_1, x_2, \ldots, x_n, x'_1, x'_2, \ldots, x'_m \in X, \tag{2.10}$$

з $x_1 \neq x'_1$. Однак, Y є кодом, а також за (2.10) маємо, що

$$\alpha(x_1) = \alpha(x'_1).$$

Таким чином, відображення α не є ін'єктивним. Це доводить нашу нерівність. □

2.3 Тест для кодів

Не завжди вдається легко перевірити, що дана множина слів є кодом. Тест, описаний у цьому підрозділі, не ґрунтується на жодній новій властивості кодів, а складається лише з систематичної організації обчислень, необхідних для перевірки того, що множина слів задовольняє означення коду.

У випадку, коли множина X є скінченною, або, загалом, якщо множина X є розпізнуваною, то обчислення є скінченними. Іншими словами, ця задача ефективно розв'язується, коли є скінченна або розпізнувана множина є кодом.

Перш ніж почати описання алгоритму, розглянемо приклад.

Приклад 2.3.1. Нехай $A = \{a, b\}$ — алфавіт. Тоді підмножина

$$X = \{b, abb, abbba, bbba, baabb\}$$

в A^* не є кодом. Наприклад

$$(abb)(baabb) = (abbba)(abb).$$

Розглянемо слово

$$w = abbbabbbaabb,$$

яке має дві різні факторизації (див. рис. 2.3)

$$w = (abbba)(bbba)(abb) = (abb)(b)(abb)(baabb).$$

Ці дві факторизації визначають послідовність префіксів слова w, кожна з яких

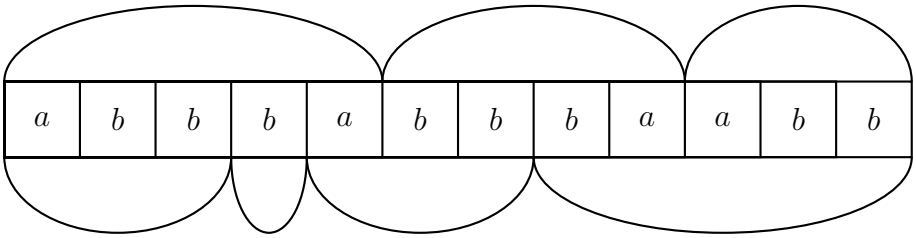


Рис. 2.3: Дві факторизації слова $abbbabbbaabb$

відповідає спробі подвійної факторизації. Ми надаємо цей список разом із спробою подвійної факторизації:

$$\begin{aligned}
(abbba) &= (abb)\underline{ba} \\
(abbba) &= (abb)(b)\underline{a} \\
(abbba)\underline{bb} &= (abb)(b)(abb) \\
(abbba)(bbba) &= (abb)(b)(abb)\underline{ba} \\
(abbba)(bbba)\underline{abb} &= (abb)(b)(abb)(baabb) \\
(abbba)(bbba)(abb) &= (abb)(b)(abb)(baabb).
\end{aligned}$$

Кожна, крім останньої з цих спроб, не спрацьовує через підкреслений суфікс, який залишається після факторизації.

Представлений тут алгоритм обчислює всі лишки у всіх спробах подвійної факторизації. Він виявляє подвійну факторизацію тим, що порожнє слово є одним із лишків.

Формально обчислення організовані наступним чином. Нехай X — підмножина вільної напівгрупи A^+ над множиною A, і нехай

$$\begin{aligned} U_1 &= X^{-1}X \setminus \{1\}, \\ U_{n+1} &= X^{-1}U_n \cup U_n^{-1}X \qquad (n \geqslant 1). \end{aligned} \tag{2.11}$$

Тоді отримуємо наступний результат:

Теорема 2.3.2. *Множина $X \subseteq A^+$ є кодом тоді і тільки тоді, коли жодна з множин U_n, визначених у формулі (2.11), не містить порожнього слова.*

Якщо $X \subseteq A^+$ префіксом (отож, кодом), то $U_1 = X^{-1}X \setminus \{1\} = \varnothing$. Таким чином, алгоритм негайно закінчується для таких кодів.

Приклад 2.3.3. Нехай X — множина, визначена в прикладі 2.3.1. Слово ba є в множині U_1, далі $a \in U_2$, тоді $bb \in U_3$ і $ba \in U_4$, на завершенні $abb \in U_5$ і оскільки $1 \in U_6$, то множина X не є кодом, за теоремою 2.3.2.

В основі доведення теореми 2.3.2 є лема 2.3.4.

Лема 2.3.4. *Нехай $X \subseteq A^+$ і $(U_n)_{n\geqslant 1}$ — сім'я, означена в (2.11). Для всіх $n \geqslant 1$ $w \in U_n$ тоді і лише тоді, коли існують натуральні числа $p, q \geqslant 1$ з $p + q = n + 1$ і слова $x_1, \ldots, x_p, y_1, \ldots, y_q \in X$ такі, що $x_1 \neq y_1$ і w є суфіксом слова y_q таким, що*

$$x_1 \cdots x_p w = y_1 \cdots y_q. \tag{2.12}$$

Доведення. Ми доведемо за індукцією по n, що для $w \in U_n$ слова, які задовольняють умову (2.12) існують. Спочатку, якщо $w \in U_1$, то за означенням множини U_1 маємо, що $xw = y$ для деяких $x, y \in X$ таких, що $x \neq y$, і слово w є суфіксом слова y, а отже твердження леми виконується для $n = 1$.

Нехай $w \in U_n$, для деякого $n > 1$. Тоді або $xw = v$, або $vw = x$ для деяких $x \in X$ і $v \in U_n^1$. За припущенням індукції

$$x_1 \cdots x_p v = y_1 \cdots y_q,$$

для натуральних чисел p і q таких, що $p + q = n$ і $x_1, \ldots, x_p, y_1, \ldots, y_q \in X$ з $x_1 \neq y_1$ і слово v є суфіксом слова y_q. Якщо $xw = v$, то рівність

$$x_1 \cdots x_p x w = y_1 \cdots y_q,$$

доводить, що ця умова задовольняється словами $x_1, \ldots, x_p, x_{p+1}, y_1, \ldots, y_q$ з $x_{p+1} = x$, оскільки слово w є суфіксом слова y_q. З іншого боку, якщо $vw = x$ то

$$x_1 \cdots x_p x = y_1 \cdots y_q w,$$

доводить, що ця умова задовольняється словами $y_1, \ldots, y_q, x_1, \ldots, x_p, x_{p+1}$ з $x_{p+1} = x$, оскільки слово w є суфіксом слова x.

Навпаки, доведемо за індукцією по n, що якщо, для натуральних p і q з $p+q=n+1$, існують слова $x_1,\dots,x_p,y_1,\dots,y_q\in X$ з $x_1\neq y_1$ і слово w є суфіксом слова y_q такі, що

$$x_1\cdots x_pw=y_1\cdots y_q,$$

тоді $w\in U_n$.

Властивість очевидно виконується для $n=1$. Припустимо, що $n>1$. Оскільки слово w є суфіксом слова y_q, то маємо, що $y_q=vw$ для деякого слова v, і рівність стає

$$x_1\cdots x_p=y_1\cdots y_{q-1}v.$$

Покладемо $v=v'x_{r+1}\cdots x_p$, де слово v' є суфіксом слова x_r для деякого натурального числа r такого, що $1\leqslant r\leqslant p$. Тоді $x_1\cdots x_r=y_1\cdots y_{q-1}v'$, а отже $v'\in U_{r+q-2}$ за припущенням індукції.

Позаяк $y_q=v'x_{r+1}\cdots x_pw$, то маємо, що $x_{r+1}\cdots x_pw\in U_{r+q-2}^{-1}X\subseteq U_{r+q-1}$. Далі за індукцією по i ми доведемо, що $x_{r+i}\cdots x_pw\in U_{r+q+i-2}$ для $1\leqslant i\leqslant p-r$.

Це виконується для $i=1$, і оскільки $x_{r+i}\in X$, то з умови $x_{r+i}\cdots x_pw\in U_{r+q+i-2}$ випливає, що $x_{r+i+1}\cdots x_pw\in U_{r+q+i-1}$. Отож, ми отримали, що $x_pw\in U_{p+q-2}$ і на завершенні, що $w\in U_{p+q-1}$. Це завершує доведення леми. □

Доведення теореми 2.3.2. Якщо множина X не є кодом, тоґ існує реалізація

$$x_1x_2\cdots x_p=y_1y_2\cdots y_q,\qquad x_1,x_2,\dots,x_p,y_1,y_2,\dots,y_q\in X,\qquad x_1\neq y_1. \tag{2.13}$$

За лемою 2.3.4, порожнє слово є елементом множини U_{p+q-1}. Навпаки, якщо $1\in U_n$, то існує факторизація (2.13) з $p+q-1=n$, а це доводить, що множина X не є кодом. Це завершує доведення теореми. □

Приклад 2.3.5. Нехай X — множина, визначена в прикладі 2.3.1. Для

$$X=\{b,abb,abbba,bbba,baabb\}$$

отримуємо

$$\begin{array}{lll} U_1=\{ba,bba,aabb\}, & X^{-1}U_1=\{a,ba\}, & U_1^{-1}X=\{abb\},\\ U_2=\{a,ba,abb\}, & X^{-1}U_2=\{a,1\}, & U_2^{-1}X=\{bb,bbba,abb,1,ba\}. \end{array}$$

отож, $1\in U_3$ і X не є кодом.

Приклад 2.3.6. Нехай $X=\{a,ab,ba\}$ і $A=\{a,b\}$. Ми маємо

$$U_1=\{b\},\qquad U_2=\{a\},\qquad U_3=\{1,b\},\qquad U_4=X,\qquad U_5=U_3.$$

Множина U_3 містить порожнє слово. Отож, X не є кодом.

Приклад 2.3.7. Нехай $X=\{aa,ba,bb,baa,bba\}$ і $A=\{a,b\}$. Ми отримуємо $U_1=\{a\}$, $U_2=U_1$. Отож, $U_n=\{a\}$ для всіх натуральних чисел $n\geqslant 1$, а отже X є кодом.

Наступне твердження показує, що теорема 2.3.2 надає алгоритм для перевірки того, чи розпізнувана множина є кодом, і воно є очевидним, якщо множина X є скінченною, оскільки кожна множина U_n складається з суфіксів слів у множині X.

Твердження 2.3.8. *Якщо $X \subset A^+$ — розпізнувана множина, то множина всіх U_n $(n \geqslant 1)$ є скінченною.*

Доведення. Нагадаємо, що через $\sim_X$ позначається синтаксична конгруенція на множині X.

Нехай μ — конгруенція на вільному моноїді A^* з двома класами $\{1\}$ і A^+. Нехай $\iota = \sim_X \cap \mu$. Ми використаємо наступний загальний факт.

Якщо $L \subseteq A^*$ — об'єднання класів еквівалентності конгруенції θ, тоді $Y^{-1}L$ є об'єднанням класів конгруенції $\mod \theta$, для довільної підмножини Y вільного моноїда A^*. (Справді, нехай $z \in Y^{-1}L$ і $z' \equiv z \mod \theta$. Тоді $yz \in L$ для деякого $y \in Y$, звідки отримуємо $yz' \in L$. Отож, $z' \in Y^{-1}L$.)

Доведемо, що кожна множина U_n є об'єднанням класів еквівалентності ι за індукцією по $n \geqslant 1$. Для $n = 1$ множина X є об'єднанням класів відношення $\sim_X$, таким чином множина $X^{-1}X$ також є об'єднанням класів для відношення $\sim_X$, і, нарешті, $X^{-1}X \setminus \{1\}$ — об'єднання класів відношення ι. Далі, якщо множина U_n є об'єднанням класів відношення ι, то за попереднім фактом обидві множини $U_n^{-1}X$ і $X^{-1}U_n$ — об'єднання класів еквівалентності ι. Таким чином, U_{n+1} є об'єднанням класів відношення ι. З того, що множина X розпізнувана, випливає, що ι має скінченний індекс. Звідси випливає твердження леми. □

Приклад 2.3.9. Нехай $A = \{a, b\}$ і $X = ba^*$. Тоді X є розпізнуваним суфіксним кодом. Справді, $U_1 = a^+$ і $U_2 = \varnothing$. Таким чином, послідовність (U_n) має два різних елементи.

2.4 Коди та розподіли Бернуллі

У цьому розділі ми розглянемо розподіли Бернуллі. Нагадаємо, що для розподілу Бернуллі π на A^* і підмножини $X \subseteq A^*$ ми визначаємо

$$\pi(X) = \sum_{x \in X} \pi(x).$$

Значення $\pi(X)$ є невід'ємним числом або дорівнює $+\infty$. Для будь-якої сімї $(X_i)_{i \geqslant 0}$, підмножин вільного моноїда A^*, маємо

$$\pi\left(\bigcup_{i \geqslant 0} X_i\right) \geqslant \sum_{i \geqslant 0} \pi(X_i), \tag{2.14}$$

з рівністю, якщо множини X_i є попарно неперетинними.

Приклад 2.4.1. Нехай $A = \{a, b\}$ і $X = \{a, ba, bb\}$. Нехай π — розподіл Бернуллі на вільному моноїді A^*. Поклавши $p = \pi(a)$ і $q = \pi(b)$, отримуємо

$$\pi(X) = p + pq + q^2 = p + pq + (1 - p)q = p + q = 1.$$

Для розподілу Бернуллі π і множини X, нагадаємо, що ймовірність породжена рядом над X дорівнює

$$F_X(t) = \sum_{n \geqslant 0} \pi(X \cap A^n) t^n.$$

Оскільки $\pi(X \cap A^n) \leqslant 1$, то радіус збіжності ряду $F_X(t)$ дорівнює щонайменше 1 і $\pi(X) = F_X(1)$.

Лема 2.4.2. *Нехай π — розподіл Бернуллі на вільному моноїді A^*. Тоді*

(*i*) $F_{X \cup Y}(t) = F_X(t) + F_Y(t)$, *якщо* $X \cap Y = \varnothing$,
(*ii*) $F_{XY}(t) = F_X(t) F_Y(t)$, *якщо добуток* XY *є однозначним,*

для підмножин $A, B \subseteq A^+$.

Доведення. Перша рівність є очевидною. Для доведення другої рівності зауважимо, що

$$XY \cap A^n = \bigcup_{i+j=n} (X \cap A^i)(Y \cap A^j),$$

для всіх натуральних n. Вищезгадане об'єднання є диз'юнктним у випадку, коли добуток XY є однозначним. Отже, з першої рівності випливає, що

$$\pi(XY \cap A^n) = \bigcup_{i+j=n} \pi((X \cap A^i)(Y \cap A^j)),$$

і оскільки виконується очевидна рівність

$$\pi((X \cap A^i)(Y \cap A^j)) = \pi((X \cap A^i))\pi((Y \cap A^j)),$$

то отримуємо твердження (*ii*). □

Зауважимо, що

$$F_{X_1\cdots X_m}(t) = F_{X_1}(t)\cdots F_{X_m}(t).$$

у випадку, коли кожне слово в добутку $X_1\cdots X_m$ має єдину факторизацію, як добуток слів у $X_1,\ldots,X_m$.

Твердження 2.4.3. *Нехай $X \subset A^+$ — код і π — розподіл Бернуллі на вільному моноїді A^*. Тоді*

$$F_{X^*}(t) = \frac{1}{1-F_X(t)}.$$

Доведення. Оскільки $F_X(0) = 0$, то

$$\frac{1}{1-F_X(t)} = \sum_{n\geqslant 0} F_X(t)^n.$$

Оскільки множина X є кодом, то добутки X^n є однозначними, тобто кожне слово в X^n має єдину факторизацію, як добуток n слів у множині X. За лемою 2.4.2 отримуємо, що $F_{X^n}(t) = F_X(t)^n$. Оскільки більше того множини X^n є попарно диз'юнктними, то маємо

$$F_{X^*}(t) = F_{\bigcup_{n\geqslant 0} X^n}(t) = \sum_{n\geqslant 0} F_{X^n}(t).$$

Отож, отримуємо

$$\frac{1}{1-F_X(t)} = \sum_{n\geqslant 0} F_X(t)^n = \sum_{n\geqslant 0} F_{X^n}(t) = F_{X^*}(t),$$

що і завершує доведення. □

У випадку однорідного розподілу Бернуллі отримаємо наступне наслідки, що відносяться до звичайних породжуючих функцій $f_X(t)$ і $f_{X^*}(t)$ множин X і X^*, відповідно.

Наслідок 2.4.4. *Нехай X — код над скінченним алфавітом A. Тоді*

$$f_{X^*}(t) = \frac{1}{1-f_X(t)}.$$

Доведення. Справді, за рівнянням (1.31) для однорідного розподілу Бернуллі отримуємо, що $f_X(t) = F_X(kt)$ і $f_{X^*}(t) = F_{X^*}(kt)$, де $k = \mathrm{Card}(A)$. Далі скористаємося твердженням 2.4.3. □

Теорема 2.4.5. *Якщо X є кодом над алфавітом A, то $\pi(X) \leqslant 1$ для всіх розподілів Бернуллі π на A^*.*

Доведення. Припустимо, що код X є скінченним. Тоді значення $\pi(X)$ є також скінченним. Припустимо протилежне, that $\pi(X) > 1$. Тоді $F_X(1) > 1$, а отже існує число $r < 1$ таке, що $F_X(r) = 1$. Оскільки множина X є кодом, то за твердженням 2.4.3 виконується рівність

$$F_{X^*}(t) = \frac{1}{1-F_X(t)}.$$

Тоді ряд $F_{X^*}(t)$ розбігається для $t = r$, а отже радіус збіжності ряду $F_{X^*}(t)$ є строго меншим за 1, що суперечить ймовірності породжуючого ряду.

Оскільки значення $\pi(X)$ є обмеженням зверху значень для скінченним підмножин з X, звідки випливає твердження теореми. □

У випадку, коли алфавіт A є скінченним і, коли розподіл π є рівномірним, отримуємо

Наслідок 2.4.6. *Нехай X — код над алфавітом з k літер. Тоді*

$$\sum_{x\in X} k^{-|x|} \leqslant 1.$$

Приклад 2.4.7. Нехай $A = \{a, b\}$ і $X = \{b, ab, ba\}$. Означимо розподіл Бернуллі π так: $\pi(a) = 1/3$, $\pi(b) = 2/3$. Тоді

$$\pi(X) = \frac{2}{3} + \frac{2}{9} + \frac{2}{9} = \frac{10}{9},$$

а отже множина X не є кодом. Зауважимо, що для $\pi(a) = \pi(b) = 1/2$ отримуємо $\pi(X) = 1$. Таким чином, не можна зробити висновок, що множина X не є кодом з іншим розподілом.

Наступний приклад показує, що твердження обернене до теореми 2.4.5 не виконується.

Приклад 2.4.8. Нехай $A = \{a, b\}$ і $X = \{ab, aba, aab\}$. Тоді множина X не є кодом, оскільки

$$(aba)(ab) = (ab)(aab).$$

Проте будь-який розподіл Бернуллі π дає $\pi(X) < 1$. Справді, покладемо $p = \pi(a)$ і $q = \pi(b)$. Тоді

$$\pi(X) = pq + 2p^2q.$$

Легко бачити, що ми завжди маємо $pq \leqslant \frac{1}{4}$ і також $p^2q \leqslant \frac{4}{27}$, оскільки $p + q = 1$. Внаслідок цього отримуємо

$$\pi(X) \leqslant \frac{1}{4} + \frac{8}{27} < 1.$$

Цей приклад дає хорошу ілюстрацію меж теореми 2.4.5 у її використанні для перевірки того, чи є множина кодом. Справді, множина X з прикладу 2.4.8, де тест є хибним, отримують з множини з прикладу 2.4.7, де тест є успішним, просто шляхом заміни b на ab. Це показує, що обчислений аргумент зображений розподілом Бернуллі враховує як довжини, так і кількість слів. Іншими словами, теорема 2.4.5 дозволяє зробити висновок, що множина X не є кодом, лише коли є "занадто багато коротких слів".

Твердження 2.4.9. *Нехай X — код над алфавітом A. Якщо існує додатній розподіл Бернуллі π на A^* такий, що $\pi(X) = 1$, то код X є максимальним.*

Доведення. Припустимо, що код X не є максимальний. Тоді існує деяке слово $y \notin X$ таке, що $Y = X \cup \{y\}$ є кодом. За теоремою 2.4.5 маємо, що $\pi(Y) \leqslant 1$. З іншого боку,

$$\pi(Y) = \pi(X) + \pi(y) = 1 + \pi(y).$$

Таким чином, отримуємо $\pi(y) = 0$, що є неможливим оскільки розподіл Бернуллі π є додатнім. □

Твердження 2.4.9 є дуже корисним для доведення максимальності коду. Прямий метод доведення максимальності, заснований на означенні, насправді зазвичай набагато є складнішим, ніж перевірка умов твердження. Більш чітке твердження, що виконується для великого класу кодів, буде викладено в наступному підрозділі (теорема 2.5.16).

Приклад 2.4.10. В умовах прикладу 2.4.1, оскільки $\pi(X) = 1$ і код X є префіксним, то X є максимальним кодом.

Приклад 2.4.11. Розглянемо знову код Дика D над алфавітом $A = \{a, b\}$, описаний в прикладі 2.2.13. Нехай π — розподіл Бернуллі на вільному моноїді A^*, і покладемо $p = \pi(a)$, $q = \pi(b)$.

Нехай $D_a = D \cap aA^*$ і $D_b = D \cap bA^*$. Зауважимо, що множина D_a утворюється зі слів x над алфавітом A таких, що $|u|_a - |u|_b > 0$ для кожного непорожнього власного префікса u слова x, або еквівалентно $|v|_a - |v|_b < 0$ для кожного непорожнього власного суфікса v слова x. Зокрема, $D_a = b\widetilde{D}_b$, оскільки таке ж саме твердження виконується для D_b, якщо замінити b на a. Покажемо це

$$D_a = aD_a^*b \qquad \text{і} \qquad D_b = bD_b^*a. \tag{2.15}$$

Нехай x — слово з множини D_a. Очевидно, що $x = ayb$ для деякого слова $y \in A^*$. Оскільки $|x|_a = |x|_b$, то маємо, що $|y|_a = |y|_b$, а отже $y \in D^*$. Покладемо $y = y_1y_2\cdots y_n$ з $y_i \in D$. Тоді кожен елемент y_i належить D_a. Справді, якщо $y_i \in D_b$, то $ay_1\cdots y_{i-1}b$ є префіксом слова x який належить множині D_a, а це суперечить том факту, що множина D є префіксним кодом. Навпаки, кожне слово з множини aD_a^*b, очевидно належить множині D_a. Це доводить рівність $D_a = aD_a^*b$. Друга рівність доводиться аналогічним чином.

Оскільки всі добутки в рівності (2.15) є однозначними, отримуємо

$$F_{D_a}(t) = F_a(t)F_{D_a^*}(t)F_b(t).$$

Оскільки множина D_a є кодом, то

$$F_{D_a^*}(t) = \frac{1}{1 - F_{D_a}(t)}.$$

Отже величина $F_{D_a}(t)$ є одним із розв'язків квадратного рівняння

$$Y(t)^2 - Y(t) + pqt^2 = 0.$$

Це рівняння має два розв'язки

$$\frac{1 + \sqrt{1 - 4pqt^2}}{2} \qquad \text{і} \qquad \frac{1 - \sqrt{1 - 4pqt^2}}{2}.$$

Оскільки $F_{D_a}(0) = 0$, то

$$F_{D_a}(t) = \frac{1 - \sqrt{1 - 4pqt^2}}{2}.$$

Позаяк $D_a = \widetilde{D}_b$, то маємо, що $F_{D_a}(t) = F_{D_b}(t)$. Отже $F_D(t) = 2F_{D_a}(t)$, звідки випливає, що

$$F_{D_a}(t) = 1 - \sqrt{1 - 4pqt^2}.$$

Отож, $\pi(D) = 1 - \sqrt{1-4pqt^2}$, або еквівалентно, що $\pi(D) = 1 - |p-q|$ оскільки

$$(p-q)^2 = (p+q)^2 - 4pq = 1 - 4pq.$$

Для $\pi(a) = \pi(b) = 1/2$ маємо, що $\pi(D) = 1$. Це дає інше доведення того, що множина D є максимальним кодом (приклад 2.2.13). Зауважимо, що $\pi(D) < 1$ для довільного іншого розподілу Бернуллі.

Приклад 2.4.12. Множина $X = \bigcup_{n\geqslant 0} a^n b A^n$ є префіксною, а отже вона є кодом над алфавітом $A = \{a, b\}$. Множина X є максимальним кодом. Справді, нехай π — додатній розподіл Бернуллі, і покладемо $p = \pi(a)$. Тоді

$$\pi(a^n b A^n) = p^n(1-p),$$

а отже отримуємо

$$\pi(X) = \sum_{n\geqslant 0} p^n(1-p) = (1/(1-p))(1-p) = 1.$$

Тепер сформулюємо твердження, яке доводить, що нерівність наслідка 2.4.6 є фактично жорсткою.

Теорема 2.4.13 (Крафта–Макміллана). *Для довільної послідовності $(u_n)_{n\geqslant 1}$ цілих чисел існує код X над алфавітом A з k символів такий, що $u_n = \mathrm{Card}(X \cap A_n)$ тоді і лише тоді, коли*

$$\sum_{n\geqslant 1} u_n k^{-n} \leqslant 1. \tag{2.16}$$

Більше того, код X можна вибрати так, щоб він був префіксним[1].

Доведення. Необхідність випливає з наслідку 2.4.6. Навпаки зауважимо спочатку, що за нерівністю маємо також $\sum_{1\leqslant i\leqslant n} u_i k^{-i} \leqslant 1$, або еквівалентно, помноживши обидві частини цієї нерівності на k^n, маємо $\sum_{1\leqslant i\leqslant n} u_i k^{n-i} \leqslant k^n$ для всіх натуральних чисел $n \geqslant 1$. Тепер доведемо за індукцією по $n \geqslant 1$, що існує префіксний код X_n на алфавіті A з k символів такий, що $\mathrm{Card}(X_n \cap A^i) = u_i$ для $1 \leqslant i \leqslant n$.

Це твердження є правильним для $n = 1$, оскільки $u_1 \leqslant k$. Далі, припустимо, що властивість виконується для n. Множина слів довжини $n+1$ з префіксом в X_n є

$$\bigcup_{1\leqslant i\leqslant n} \left(X_n \cap A^i\right) A^{n+1-i}.$$

Звідси отримуємо, що кількість слів довжини $n+1$ з префіксом в X_n дорівнює

$$s = \sum_{1\leqslant i\leqslant n} u_i k^{n+1-i}.$$

Оскільки $s + u_{n+1} \leqslant k^{n+1}$, то ми можемо вибрати множину Y слів u_{n+1} довжини $n+1$ без префіксів з X_n. У цьому випадку, множина $X_{n+1} = X_n \cup Y$ є префіксним кодом з розподілом довжини $(u_i)_{1\leqslant i\leqslant n+1}$. □

[1] Нерівність (2.16) називається *нерівністю Крафта*.

2.5 Повні множини

Будь-яка підмножина коду сама є кодом. Отже, важливо знати структуру максимальних кодів. Багато результатів, що містяться в цій книзі, стосуються максимальних кодів.

Поняття повних множин, введених у цьому підрозділі, в певному сенсі є дуальним до поняття коду. Наприклад, будь-яка множина, що містить повну множину, є повною. Навіть якщо дуальність не є досконало збалансованою, вона дозволяє сформулювати максимальність у термінах повноти, замінюючи таким чином екстремальну властивість комбінаторною.

Нехай M — моноїд і P — підмножина в M. Елемент $m \in M$ називається *поповнювальним* у множині P, якщо існують елементи $u, v \in M$ такі, що $umv \in P$. Це еквівалентно тому, що множина P перетинає двобічний ідеал MmM,

$$MmM \cap P \neq \varnothing,$$

або, іншими словами, що

$$m \in F(P) = M^{-1}PM^{-1}.$$

Під *поповнювальним словом* будемо розуміти поповнювальний елемент вільного моноїда. Слово (елемент), яке (який) не є поповнювальним в P називається *непоповнювальним*. Множина елементів, які є поповнювальними в P звичайно збігається з $F(P)$; множина $\overline{F}(P) = M \setminus F(P)$ непоповнювальних елементів є двобічним ідеалом у моноїді M, що не перетинає множину P.

Підмножина P моноїда M називається *щільною* в M, якщо всі елементи множини M є поповнювальними в P, тобто, якщо $F(P) = M$, або еквівалентно, якщо P перетинає всі (двобічні) ідеали в моноїді M. Очевидно, що кожна надмножина щільної множини є щільною.

Використання прикметника "щільний" мотивується тим, що щільні підмножини в моноїді M є щільними підмножинами в моноїді M стосовно деякої топології на M (див. вправу 2.8.16).

Приклад 2.5.1. Нехай $A = \{a\}$. Щільними підмножинами у вільному моноїді A^* є нескінченні підмножини.

Приклад 2.5.2. У групі G кожна непорожня підмножина є щільною, оскільки $GmG = G$ для довільного $m \in G$.

Приклад 2.5.3. Код Дика D над алфавітом $A = \{a, b\}$ є щільною підмножиною в A^*. Справді, якщо $w \in A^*$, то $v = a^{2|w|_b}wb^{|w|}$, очевидно, є елементом в D^*. Крім того, не має власного непорожнього префікса слова v, що є в D^*. Отож, v є елементом кода D, а це доводить, що слово w є поповнювальним в множині D.

Корисно мати спеціальний термін для кодів X таким, що підмоноїд X^* є щільним у вільному моноїді над деяким алфавітом. Підмножина P моноїда M називається *повною* в M, якщо підмоноїд, що породжується множиною P є щільним. Кожна щільна множина також є повною. Далі, підмножина X вільного моноїда A^* є повною тоді і тільки тоді, коли $F(X^*) = A^*$.

Приклад 2.5.4. Будь-яка непорожня підмножина вільної напівгрупи a^+ є повною, оскільки вона породжує нескінченний підмоноїд.

Теорема 2.5.5. *Кожен максимальний код є повною множиною.*

Теорема 2.5.5 є безпосереднім наслідком наступного твердження.

Твердження 2.5.6. *Нехай A — алфавіт і $X \subset A^+$ — максимальний код. Тоді*

$$X^*wA^* \cap X^* \neq \varnothing,$$

для довільного слова $w \in A^*$.

Доведення. Твердження є очевидним у випадку, коли $\mathrm{Card}(A) = 1$, або якщо w є порожнім словом. В іншому випадку, за твердженням 1.3.6 існує слово $w' \in A^+$ таке, що $y = ww'$ є необлямованим. Покладемо $Y = X \cup \{y\}$. Достатньо довести, що $X^*yA^* \cap X^* \neq \varnothing$. Позаяк множина Y не є кодом, то маємо $x_1 \cdots x_n = y_1 \cdots y_m$ з $n, m \geqslant 1$, $x_i, y_j \in Y$ і $x_1 \neq y_1$. Оскільки множина X є кодом, то хоча б одне зі слів x_i, y_j дорівнює слову y. Розглянемо крайнє зліва виникнення слова y серед слів x_i, y_j. Ми можемо припускати, що слово y виникає серед слів x_i, скажемо, наприклад, з індексом k. Отож, $x_1, \ldots, x_{k-1} \in X$ і $x_k = y$. Нехай l — найменший індекс такий, що слово $x_1 \cdots x_k$ є префіксом слова $y_1 \cdots y_l$. Покладемо

$$z = x_1 \cdots x_k u = y_1 \cdots y_l.$$

Очевидно, що $z \in X^*yA^*$ (див. рис. 2.4). Ми доведемо, що $z \in X^*$, показавши, що

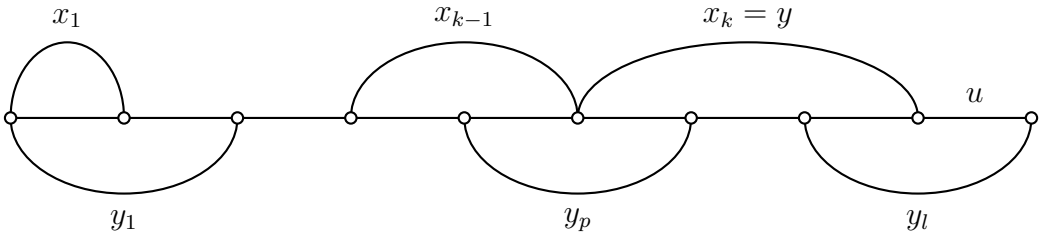


Рис. 2.4: Доведення того, що $z \in X^*yA^* \cap X^*$

$y_1, \cdots, y_l \in X$. Нехай p — найменший індекс такий, що слово $x_1 \cdots x_{k-1}$ є префіксом слова $y_1 \cdots y_p$. Покладемо $x_1 \cdots x_{k-1}v = y_1 \cdots y_p$, зі словом v, яке є непорожнім, оскільки множина X кодом. Отож, отримуємо, що $x_k u = vy_{p+1} \cdots y_l$. З мінімальності числа k випливає, що $y_1, \ldots, y_p \in X$. Далі, $y_{p+1}, \ldots, y_{l-1}$ є власними множниками слова $x_k = y$, а отже є також елементом множини X. На завершенні отримуємо, що $y_l \neq y$, оскільки слово y є необлямованим. Таким чином, $y_l \in X$ і $z \in X^*$. □

Приклад 2.5.7. Тепер ми можемо перевірити одну з вимог, наведених у підрозділі 2.1, а саме: існують скінченні коди, які не містяться в максимальному скінченному коді.

Нехай $X = \{a^5, ba^2, ab, b\}$. Множина X є кодом над алфавітом $A = \{a, b\}$. Довільний максимальний код, який чистить код X є нескінченним. Справді, нехай Y —

максимальний код над алфавітом A, який містить код X. Припустимо, що код Y є скінченним. Покладемо $m = \max\{|y| : y \in Y\}$ і нехай

$$u = b^m a^{4+5m} b^m.$$

Оскільки код Y є максимальним, то за теоремою 2.5.5 він є повною множиною. Отож, слово u є множником слова в Y^*. Ані слово b^m, ні слово a^{4+5m} не можуть бути власними множниками слова з коду Y. Отже існують слова $y, y' \in Y \cup \{1\}$ і цілі числа $p, q, r \geqslant 0$ такі, що

$$u = b^p y a^q y' b^r$$

з $a^q \in Y^*$ (див. рис. 2.5). Слово a^5 є єдиним словом у коді Y, що не містить літеру b.

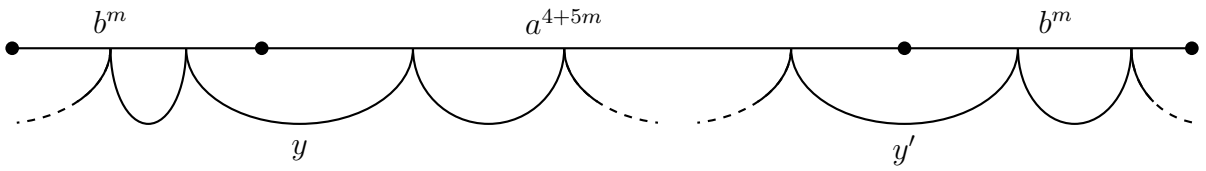


Рис. 2.5: Факторизація слова $b^m a^{4+5m} b^m$ словами з коду Y

Таким чином число q є кратним числу 5, а це означає, що $|y|_a + |y'|_a \equiv 4 \mod 5$.

Нехай $y = b^h a^{5s+i}$ і $y' = a^{j+5t} b^k$ з $0 \leqslant i, j \leqslant 4$. Маємо, що $i + j \equiv 4 \mod 5$, звідки випливає, що $i + j = 4$. Ми доведемо, що довільний вибір чисел i та j призводить до висновку, що множина Y не є кодом. Отримали протиріччя.

Якщо $i = 0$, $j = 4$, то $k \geqslant 1$ і ми отримуємо, що

$$ba^2 \cdot a^{5t+4} b^k = b \cdot a^{5(t+1)} \cdot ab \cdot b^{k-1}.$$

Якщо $i = 1$, $j = 3$, то

$$b^h a^{5s+1} \cdot b = b^h \cdot a^{5s} \cdot ab.$$

Якщо $i = 2$, $j = 2$, то

$$b \cdot a^{2+5t} b^k = ba^2 \cdot a^{5t} \cdot b^k.$$

Якщо $i = 3$, $j = 1$, то $h \geqslant 1$ і ми отримуємо, що

$$b^h a^{5s+3} \cdot b = b^{h-1} \cdot ba^2 \cdot a^{5s} \cdot ab.$$

Якщо $i = 4$, $j = 0$, то

$$b^h a^{5s+4} \cdot ab = b^h \cdot a^{5(s+1)} \cdot b.$$

Цей приклад є конкретним випадком більш загальної конструкції (див. твердження 12.3.1).

Обернене твердження до теореми 2.5.5 є неправильним (див. приклад 2.5.9). Однак, воно є правильним при додаткових припущеннях, які спираються на наступне означення.

Підмножина P моноїда M, яка не є щільною, називається *тонкою*. Якщо підмножина P є тонкою, то існує хоча б один елемент m у моноїді M, який є непоповнювальним у P, тобто виконується умова $MmM \cap P = \varnothing$, або їй еквівалентна умова $F(P) \neq M$.

Використання прикметника "тонкий" мотивується результатами, такими як твердження 2.5.8 або 2.5.12.

Твердження 2.5.8. *Нехай M — моноїд і $P, Q, R \subseteq M$. Тоді множина $P \cup Q$ є тонкою тоді і лише тоді, коли P і Q є тонкими. Якщо множина R є щільною і множина P є тонкою, то множина $R \setminus P$ є щільною.*

Доведення. Якщо підмножини P і Q моноїда M є тонкими, то існують елементи $m, n \in M$ такі, що

$$MmM \cap P = \varnothing \qquad \text{і} \qquad MnM \cap Q = \varnothing.$$

Позаяк $MnnM \subseteq MmM$ і $MnnM \subseteq MnM$, то

$$\begin{aligned} MmnM \cap (P \cup Q) &= (MmnM \cap P) \cup (MmnM \cap Q) \subseteq \\ &\subseteq (MmM \cap P) \cup (MnM \cap Q) = \\ &= \varnothing, \end{aligned}$$

а отже елемент mn є непоповнювальним в $P \cup Q$. Звідси випливає, що множина $P \cup Q$ є тонкою в M. Навпаки, якщо множина $P \cup Q$ є тонкою в M, то існує елемент $m \in M$, який є непоповнювальним в $P \cup Q$, а отже є непоповнювальним в кожній з множин P і Q. Отож, підмножини P і Q моноїда M є тонкими. Якщо множина R є щільною в моноїді M і множина P є тонкою в M, то множина $R \setminus P$ не може бути тонкою в M, оскільки в цьому випадку $R = (R \setminus P) \cup P$ мала б бути також тонкою в моноїді M за попереднім твердженням. □

Тонкі підмножини вільного моноїда мають додаткові властивості. Зокрема, будь-яка скінченна підмножина в A^* є очевидно тонкою. Більш того, якщо X і Y — тонкі підмножини у вільному моноїді A^*, то множина XY є також тонкою в A^*. Справді, якщо $u \notin F(X)$ і $v \notin F(Y)$, то $uv \notin F(XY)$.

Приклад 2.5.9. Код Дика D над алфавітом $A = \{a, b\}$ є щільним у вільному моноїді A^* (див. приклад 2.5.31). Також код Дика D є максимальним кодом, оскільки він є груповим (див. приклад 2.1.11). Для кожного слова $x \in D$ за твердженням 2.5.8 код $D \setminus \{x\}$ залишається щільним у вільному моноїді A^*, а отже код $D \setminus \{x\}$ є повним. Але звичайно код $D \setminus \{x\}$ не є більше максимальним. Цей приклад показує, що обернене твердження до теореми 2.5.5 не виконується в загальному випадку.

Обернене твердження до теореми 2.5.5 є істинним у випадку кодів, які є тонкими і повними. Перш ніж перейти до доведення цього факту, наведемо деякі корисні властивості тонких і повних множин.

Твердження 2.5.10. *Нехай A — алфавіт, $X \subset A^*$ — тонка та повна множина, і w — слово непоповняльне в X. Тоді*

$$A^* = \bigcup_{d \in D,\, g \in G} d^{-1} X^* g^{-1} = D^{-1} X^* G^{-1}, \tag{2.17}$$

де D і G — множини суфіксів (відп. префіксів) слова w.

Доведення. Нехай $z \in A^*$. Позаяк множина X^* є щільною у вільному моноїді A^*, то слово wzw є поповнювальним у X^*, а отже

$$uwzwv \in X^*,$$

для деяких слів $u, v \in A^*$. Тепер слово w не є множником слова в X. Таким чином, існують дві факторизації $w = g_1 d = g d_1$ такі, що

$$ug_1, dzg, d_1 v \in X^*.$$

Звідси випливає, що $z \in d^{-1} X^* g^{-1}$. □

Твердження 2.5.11. *Нехай A — алфавіт і X — тонка та повна множина у вільному моноїді A^*. Тоді $\pi(X) \geqslant 1$ для довільного додатнього розподілу Бернуллі π на A^*.*

Доведення. Маємо, що $\pi(A^*) = \infty$. Оскільки об'єднання в рівності (2.17) є скінченним, то існує пара $(d, g) \in D \times G$ така, що $\pi(d^{-1} X^* g^{-1}) = \infty$. Тепер

$$d(d^{-1} X^* g^{-1}) g \subset X^*.$$

Звідси випливає, що

$$\pi(d)\pi(d^{-1} X^* g^{-1})\pi(g) \leqslant \pi(X^*).$$

З додатної визначеності розподілу Бернуллі π випливає, що $\pi(dg) \neq 0$. Отож, $\pi(X^*) = \infty$. Тоді отримуємо, що

$$\pi(X^*) \leqslant \sum_{n \geqslant 0} \pi(X^n) \leqslant \sum_{n \geqslant 0} (\pi(X))^n.$$

Припустивши, що $\pi(X) < 1$, отримуємо, що $\pi(X^*) < \infty$. Отож, $\pi(X) \geqslant 1$. □

Звернемо увагу на наступну властивість, що показує, як вже стверджувалося раніше, що тонка множина має лише декілька слів.

Твердження 2.5.12. *Нехай A — алфавіт і X — тонка множина у вільному моноїді A^*. Тоді $\pi(X) < \infty$ для довільного додатнього розподілу Бернуллі π на A^*.*

Доведення. Нехай w — слово, яке не є множником жодного слова з множини X: $w \notin F(X)$. Покладемо $n = |w|$. Тоді маємо $n \geqslant 1$. Для $0 \leqslant i \leqslant n-1$ розглянемо

$$X_i = \{x \in X : |x| \equiv i \mod n\}.$$

Достатньо довести, що значення $\pi(X_i)$ є скінченним для $i = 0, \ldots, n-1$. Тоді отримуємо

$$X_i \subset A^i \left(A^n \setminus \{w\}\right)^*.$$

Оскільки множина $A^n \setminus \{w\}$ є кодом, то маємо, що

$$\pi\left(\left(A^n \setminus \{w\}\right)^*\right) = \sum_{k \geqslant 0} (\pi(A^n \setminus \{w\}))^k = \sum_{k \geqslant 0} (1 - \pi(w))^k.$$

З додатної визначеності розподілу Бернуллі π випливає, що $\pi(w) > 0$, а отже

$$\pi\left(\left(A^n \setminus \{w\}\right)^*\right) = \frac{1}{\pi(w)}.$$

Отож, $\pi(X_i) \leqslant \dfrac{1}{\pi(w)}$. □

Тепер ми готові довести таку теорему.

Теорема 2.5.13. *Кожен тонкий і повний код є максимальним.*

Доведення. Нехай X — тонкий і повний код над алфавітом A і нехай π — додатній розподіл Бернуллі на A^*. За твердженням 2.5.11, $\pi(X) \geqslant 1$, і за теоремою 2.4.5 маємо, що $\pi(X) \leqslant 1$. Отож, $\pi(X) = 1$. Тоді з твердження 2.4.9 випливає, що код X є максимальним. □

Теореми 2.5.5 і 2.5.13 можна згрупувати разом у такій теоремі:

Теорема 2.5.14. *Нехай X — код над алфавітом A. Тоді X є повним тоді і лише тоді, коли X є щільним або максимальним.*

Доведення. Нехай X — повний код над алфавітом A. Якщо код X не є щільним, то він тонкий, а отже X є максимальним за теоремою 2.5.13. Навпаки, щільна множина є повною, а максимальний код повний за теоремою 2.5.5. □

Перш ніж надати інші наслідки теореми 2.5.13 і 2.5.14, запропонуємо перше застосування комбінаторної характеристики максимальності.

Твердження 2.5.15. *Нехай A — непорожня множина й $X \subset A^*$ — скінченний максимальний код. Для довільної непорожньої підмножини $B \subseteq A$ код $X \cap B^*$ є максимальним над алфавітом B. Зокрема, для кожної літери $a \in A$ існує ціле число n таке, що $a^n \in X$.*

Доведення. Друге твердження випливає з першого, приймаючи $B = \{a\}$. Нехай $n = \max\{|x| \colon x \in X\}$ — максимальна довжина слів у коді X, $\varnothing \neq B \subseteq A$. Щоб показати, що $Y = X \cap B^*$ — максимальний код над алфавітом B, достатньо показати, з урахуванням теореми 2.5.13, що множина Y повна (у B^*). Нехай $w \in B^*$ і $b \in B$. Розглянемо слово

$$w' = b^{n+1} w b^{n+1}.$$

З повноти коду X випливає існування слів $u, v \in A^*$ таких, що

$$uw'v = x_1 x_2 \cdots x_k$$

для деяких $x_1, x_2, \ldots, x_k \in X$. Але за визначенням числа n, існують два цілих числа i та j $(1 \leqslant i < j \leqslant k)$ такі, що

$$x_i x_{i+1} \cdots x_j = b^r w b^s$$

для деяких $r, s \in \{1, \ldots, n\}$ (див. рис. 2.6). Але тоді $x_i, x_{i+1}, \ldots, x_j \in X \cap B^* = Y$. Це доводить, що слово w є поповнювальним у Y^*. □

Нехай $X \subset A^+$ — скінченний максимальний код і $a \in A$ — літера. (Єдине) ціле число n таке, що $a^n \in X$ називається *порядком* літери a стосовно коду X.

Теорема 2.5.16. *Нехай A — алфавіт і X — тонкий код над вільним моноїдом A^*. Тоді такі умови є еквівалентними:*

(*i*) *X — максимальний код над алфавітом A;*
(*ii*) *існує додатній розподіл Бернулля π вільного моноїда A^* з $\pi(X) = 1$;*

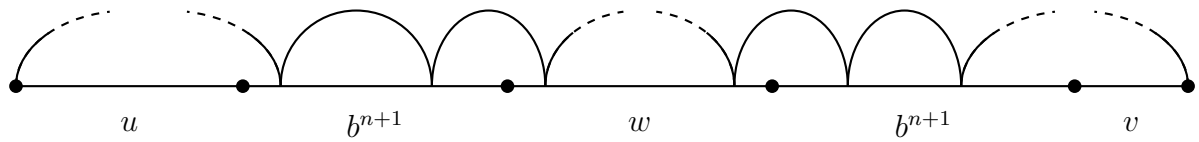


Рис. 2.6: Факторизація слова $ub^{n+1}wb^{n+1}v$

(*iii*) $\pi(X) = 1$ *для довільного додатнього розподілу Бернулля* π *вільного моноїда* A^*;
(*iv*) X — *повна підмножина вільного моноїда* A^*.

Доведення. Імплікація $(i) \Longrightarrow (iv)$ — це теорема 2.5.5.

Імплікація $(iv) \Longrightarrow (iii)$ випливає з теореми 2.4.5 і твердження 2.5.11.

Імплікація $(iii) \Longrightarrow (ii)$ є очевидною.

Імплікація $(ii) \Longrightarrow (i)$ — це твердження 2.4.9. □

Теорема 2.5.16 дає напрочуд простий метод для перевірки, коли тонкий код X є максимальним. Достатньо взяти будь-який додатній розподіл Бернуллі π і перевірити, чи $\pi(X) = 1$.

Приклад 2.5.17. Код Дика D над алфавітом $A = \{a, b\}$ є максимальним і повним, але задовольняє умову $\pi(D) = 1$ лише для одного розподілу Бернуллі (див. приклад 2.4.11). Отож, з того, якщо виконуються умови (i), (ii) і (iv) теореми 2.5.16, то з цього не випливає умова (iii) цієї теореми для щільних кодів.

Приклад 2.5.18. Префіксний код $X = \bigcup_{n\geqslant 0} a^n bA^n$ над алфавітом $A = \{a, b\}$ є щільним, оскільки $a^{|w|}bw \in X$ для всіх $w \in A^*$. Він задовольняє умову (iii) теореми 2.5.16, як це було доведено в прикладі 2.4.12. Отож, код X задовольняє чотири умови теореми 2.5.16, не будучи тонким.

Теорема 2.5.19. *Нехай* A — *алфавіт,* X — *тонка підмножина вільної напівгрупи* A^+ *і* π — *додатній розподіл Бернуллі. Тоді з будь-яких двох з трьох таких умов випливає третя:*

(*i*) X *є кодом;*
(*ii*) $\pi(X) = 1$;
(*iii*) *підмножина* X *є повною.*

Доведення. $(i) + (ii) \Longrightarrow (iii)$ З умови $\pi(X) = 1$ за твердженням 2.4.9 випливає, що X є максимальним кодом. Отож, за теоремою 2.5.5 код X є повним.

$(i) + (iii) \Longrightarrow (ii)$ З теореми 2.4.5 та умови (i) випливає, що $\pi(X) \leqslant 1$. Тепер, оскільки X — тонка підмножина вільної напівгрупи A^+ і є повною, то за твердженням 2.5.11 маємо, що $\pi(X) \geqslant 1$.

$(ii) + (iii) \Longrightarrow (i)$ Нехай $n \geqslant 1$ — ціле число. Спочатку перевіримо, що множина X^n є тонкою та повною. Для перевірки повноти, зафіксуємо $u \in A^*$ і $v, w \in A^*$ такі, що $vuw \in X^*$. Тоді $vuw \in X^k$ для деякого цілого $k \geqslant 0$. Таким чином, $(vuw)^n \in (X^n)^k \subset (X^n)^*$. Це доводить, що елемент u є поповнювальним у моноїді $(X^n)^*$. Далі,

оскільки множина X є тонкою, і оскільки добуток двох тонких множин є знову тонкою множиною, то множина X^n є тонкою.

Таким чином, множина X^n є тонкою та повною. Отже, $\pi(X^n) \geqslant 1$ за твердженням 2.5.11. З іншого боку, маємо $\pi(X^n) \leqslant \pi(X)^n$, а отже, $\pi(X^n) \leqslant 1$. Отже, $\pi(X^n) = 1$. Отож,

$$\pi(X^n) = \pi(X)^n$$

для всіх цілих $n \geqslant 1$. З твердження 2.4.3 випливає, що множина X є кодом. □

Тонкі коди складають дуже важливий клас кодів. Вони будуть охарактеризовані деякою умовою скінченності в розділі 11. Ми очікуємо ці результати, доводячи конкретний випадок, який показує, що клас тонких кодів є досить великим.

Твердження 2.5.20. *Кожен розпізнуваний код є тонким.*

Доведення. Нехай A — непорожня множина, $X \subset A^*$ — розпізнуваний код і $\mathcal{A} = (Q, i, T)$ — детерміністичний повний автомат, який розпізнає множину X. Поставимо у відповідність слову w число

$$\rho(w) = \operatorname{Card}(Q \cdot w) = \operatorname{Card}\{q \cdot w \colon q \in Q\}.$$

Маємо, що $\rho(w) \leqslant \operatorname{Card}(Q)$ і $\rho(uwv) \leqslant \rho(w)$ для всіх слів u, v.

Нехай J — множина слів $w \in A^*$ з мінімальним $\rho(w)$. З попередньої нерівності випливає, що J є двобічним ідеалом вільного моноїда A^*.

Нехай $w \in J$ і $P = Q \cdot w$. Тоді $P \cdot w = P$. Справді, $P \cdot w \in Q \cdot w = P$, і з іншого боку $P \cdot w = Q \cdot w^2$. Отож, $\operatorname{Card}(P \cdot w) = \rho(w^2)$. Оскільки значення $\rho(w)$ є мінімальним, то звідки отримуємо рівність $\rho(w^2) = \rho(w)$. Це доводить, що відображення $p \mapsto p \cdot w$ з P на P є бієктивним. Звідси випливає, що існує деяке ціле число n таке, що $p \mapsto p \cdot w^n$ є тотожнім відображенням на P.

Оскільки $P = Q \cdot w$, то маємо $q \cdot w = q \cdot w^{n+1}$ для всіх $q \in Q$. Для доведення того факту, що код X є тонким, достатньо показати, що X не перетинає двобічний ідеал J. Припустимо, що $J \cap X \neq \varnothing$ і нехай $x \in X \cap J$. Тоді $i \cdot x = t \in T$. Нехай $x \in J$ і за попередньо доведеним існує деяке ціле число $n \geqslant 1$ таке, що $i \cdot x^{n+1} = t$. Звідси випливає, що $x^{n+1} \in X$. Але це неможливо, оскільки множина X є кодом. □

Обернене твердження до твердження 2.5.20 є хибним, як це випливає з наступного прикладу.

Приклад 2.5.21. Код $X = \{a^n b^n \colon n \geqslant 1\}$ є тонким (для прикладу, елемент ba не є множником коду X), але код X не є розпізнуваним.

Приклад 2.5.22. В одному цікавому випадку виконується обернене твердження до твердження 2.5.20: будь-який тонкий груповий код є розпізнуваним. Справді, нехай $X \subset A^*$ — груповий код і $\varphi \colon A^* \to G$ — сюр'єктивний на групу G, і H — підгрупа групи G така, що $X^* = \varphi^{-1}(H)$. За припущенням, множина X є тонкою. Нехай m — слово, що є непоповнювальним у X. Ми доведемо, що підгрупа H має скінченний індекс у групі G, а точніше

$$G = \bigcup_{p \leqslant m} H\varphi(p)^{-1},$$

де слово p проходить через всі префікси слова m. Справді, нехай $g \in G$ і $w \in \varphi^{-1}(g)$. Нехай $u \in A^*$ — такий елемент, що $\varphi(u)$ — груповий обернений елемент до елемента $g\varphi(m)$. Тоді $\varphi(wmu) = g\varphi(m)\varphi(u) = 1$, звідки випливає, що $wmu \in X^*$. Далі, слово m є непоповнювальним в X. Таким чином, слово m не множником слова в X, а отже існує факторизація $m = pq$ така, що $wp, qu \in X^*$. Але тоді $h = \varphi(wp) \in H$. Оскільки $h = g\varphi(p)$, то маємо, що $g \in H\varphi(p)^{-1}$. Це завершує доведення формули.

Формула показує, що існує скінченна кількість правих суміжних класів підгрупи H у групі G. Отже, зображення групи G підстановками на правих суміжних класах підгрупи H є також скінченним. Позначимо її через K. Нехай $\alpha\colon G \to K$ — канонічний морфізм, який визначається за формулою $Hr\alpha(g) = Hrg$ (див. підрозділ 1.13). Тоді, поклавши

$$N = \{\sigma \in K\colon H\sigma = H\},$$

отримуємо, що

$$H = \alpha^{-1}(N) = \alpha^{-1}(\alpha(H)).$$

Отже, $X^* = \psi^{-1}\psi(X^*)$, де $\psi = \alpha \cdot \varphi$. Оскільки множина K скінчена, це показує, що моноїд X^* є розпізнуваним. Отже, множина X також розпізнається (див. вправа 2.8.8).

Зауваження 2.5.23. Ми використали в попередніх підрозділах аргументи, які спираються в основному на дві методики: імовірність, з одного боку, яка дозволила нам довести головним чином теорему 2.5.13, і прямі комбінаторні аргументи на словах з іншого боку (як у доведенні теореми 2.5.5).

Цікаво буде відзначити, що деякі з доведень можна завершити, використовуючи тільки одну з двох методик. Ретельний аналіз показує, що попередні твердження, за винятком тих, що пов'язані з максимальністю, можуть бути встановлені, використовуючи лише аргументи щодо ймовірностей. Наприклад, імплікація $(ii) \Longrightarrow (iv)$ в теоремі 2.5.16 може бути доведена наступним чином без використання максимальності кода X. Якщо код X не є повним, то моноїд X^* є тонким. Отже, за твердженням 2.5.12, $\pi(X^*) < \infty$, звідки за твердженням 2.4.3 отримуємо нерівність $\pi(X) < 1$.

І навпаки, для деяких з наведених тут результатів існують комбінаторні доведення, які не спираються на ймовірності. Це стосується теореми 2.5.13, де наведене доведення в значній мірі спирається на аргументи про ймовірності. Ще одне підтвердження цього результату буде наведено в розділі 9 (наслідок 9.4.6). Це доведення базується на тому, що якщо $X \subset A^+$ — тонкий повний код, то всі слова $w \in A^*$ задовольняють умову

$$(X^*wX^*)^+ \cap X^* \neq \varnothing.$$

Звідси випливає теорема 2.5.13, оскільки за цією формулою множина $X \cup \{w\}$ не є кодом для $w \notin X$, а отже X є максимальним кодом.

Приклад 2.5.7 показує, що скінченний код не завжди міститься в скінченному максимальному коді. *Проблема про вкладення* для скінченного коду X — це існування скінченного максимального коду, що містить код X. *Гіпотеза про вкладення* стверджує, що проблема вкладення є розв'язною.

Доведемо наступну чудову властивість.

Теорема 2.5.24 (Еренфойхта-Розенберга). *Кожен раціональний код міститься в максимальному раціональному коді.*

Доведення теореми 2.5.24 спирається на такий результат.

Твердження 2.5.25. *Нехай A — непорожня множина, $X \subset A^+$ — код і $y \in A^*$ — необлямоване слово таке, що $A^*yA^* \cap X^* = \varnothing$. Нехай*

$$U = A^* \setminus (X^* \cup A^*yA^*). \tag{2.18}$$

Тоді множина

$$Y = X \cup y(Uy)^* \tag{2.19}$$

є повним кодом.

Доведення. Покладемо $V = A^* \setminus A^*yA^*$. Тоді за припущенням $X^* \subset V$ і $U = V \setminus X^*$. Спочатку зауважимо, що множина $Z = Vy$ є префіксним кодом.

Припустимо справді, що $vy < v'y$ для двох слів v і v' у V. Оскільки слово y є необлямованим, то слово vy має бути префіксом слова v'. Але тоді слово v' є в A^*yA^*, отримали протиріччя. Отож. код Z є префіксом.

Тепер ми покажемо, що множина Y є кодом. Припустимо протилежне та розглянемо відношення

$$y_1y_2 \cdots y_n = y'_1y'_2 \cdots y'_m$$

з $y_1, y_2, \ldots, y_n, y'_1, y'_2, \ldots, y'_m \in Z$ і $y_1 \neq y'_1$. Оскільки множина X є кодом, одне з цих слів має бути в $Y \setminus X$. Припустимо, що одне зі слів $y_1, y_2, \ldots, y_n$ є в $Y \setminus X$, і нехай p — найменший індекс такий, що $y_p \in y(Uy)^*$. З умови $y \notin F(X^*)$ також випливає, що $y_p \notin F(X^*)$. Отже, одне зі слів $y'_1, y'_2, \ldots, y'_m$ є в $y(Uy)^*$. Нехай q — найменший індекс такий, що $y'_q \in y(Uy)^*$. Тоді

$$y_1y_2 \cdots y_{p-1}y,\ y'_1y'_2 \cdots y'_{q-1}y \in Z$$

звідки отримуємо рівність

$$y_1y_2 \cdots y_{p-1} = y'_1y'_2 \cdots y'_{q-1},$$

оскільки код Z є префіксним. Множина X є кодом, а отже з $y_1 \neq y'_1$ випливає, що $p = q = 1$. Покладемо

$$y_1 = yu_1y \cdots yu_ky \qquad \text{і} \qquad y'_1 = yu'_1y \cdots yu'_ly,$$

з $u_1, \ldots, u_k, u'_1, \ldots, u'_l \in U$. Припустимо, що $y_1 < y'_1$. Позаяк код Z є префіксним, то множина Z^* є унітарною справа. З $U \subseteq V$ випливає, що кожне зі слів u_iy і u'_iy є в Z. Внаслідок цього отримуємо, що

$$u_1 = u'_1, \ldots, u_k = u'_k.$$

Нехай $t = u'_{k+1}y \cdots yu'_ly$. Маємо

$$y_2 \cdots y_n = ty'_2 \cdots y'_m.$$

Слово y є множником слова t, а отже також зустрічається в слові $y_2 \cdots y_n$. Це доводить, що одне зі слів $y_2, \ldots, y_n$, скажемо y_r, є в $y(Uy)^*$. Припустимо, що вибраний

індекс r є мінімальним. Тоді $y_2 \cdots y_{r-1}y \in Z$ і $u'_{k+1}y \in Z$ є префіксами деякого слова. З множини Z, яка є префіксною, маємо

$$u'_{k+1} = y_2 \cdots y_{r-1}.$$

Отже $u'_{k+1} \in X^*$, а це суперечить припущенню $u'_{k+1} \in U$. Це доводить, що множина Y є кодом.

На завершенні ми доведемо, що код Y кодом. Нехай $w \in A^*$ і покладемо

$$w = v_1yv_2y \cdots yv_{n-1}yv_n$$

з $n \geqslant 1$ і $v_i \in A^* \setminus A^*yA^*$. Тоді $ywy \in Y^*$. Справді нехай $v_{i_1}, v_{i_2}, \ldots, v_{i_k}$ є такі елементи v_i, що є в X^*. Тоді

$$ywy = (yv_1y \cdots yv_{i_1-1}y)v_{i_1}(yv_{i_1+1}y \cdots yv_{i_2-1}y) \cdots v_{i_k}(yv_{i_k+1}y \cdots yv_ny).$$

Кожне зі слів у дужках є в Y. Таким чином, все слово є в Y^*. □

Доведення теореми 2.5.24. Нехай X — раціональний код. Тоді множина U, означена в рівності (2.18) є раціональною. Отже Y є раціональним кодом. За твердженням 2.5.20 множина Y є тонкою. З теореми 2.5.13 випливає, що Y є максимальним кодом. □

Приклад 2.5.26. Нехай $A = \{a, b\}$ і $X = \{a, ab\}$. Слово $y = bba$ є необлямованим і є непоповнювальним у X^*. Детерміністичний автомат, який розпізнає множину

$$U = A^* \setminus (X^* \cup A^*yA^*)$$

зображено на рис. 2.7. Відповідно, отримаємо, після деяких переписувань вираз

$$U = b^+ \cup X^*abb^+ \cup bX^*ab^*.$$

Розглянемо розподіл Бернуллі π на вільному моноїді A^* і покладемо $p = \pi(a)$ і $q = \pi(b)$. Тоді з очевидних обчислень випливає, що $\pi(U) = 1/pq$, а отже $\pi(Y) = 1$ для множини Y, визначеної за формулою (2.18), звідки випливає, що множина Y є максимальною.

Приклад 2.5.27. Нехай $A = \{a, b\}$ і $X = \{bb, bbab, babb\}$. Слово $y = aba$ є непоповнювальним у моноїді X^*. Однак, множина $X \cup \{y\}$ не є кодом, оскільки

$$(bb)(aba)(babb) = (bbab)(aba)(bb).$$

Цей приклад показує, що твердження 2.5.25 є хибним без припущення, що слово y є необлямованим.

Наступне твердження показує, як властивість бути повним кодом відображається в автоматі.

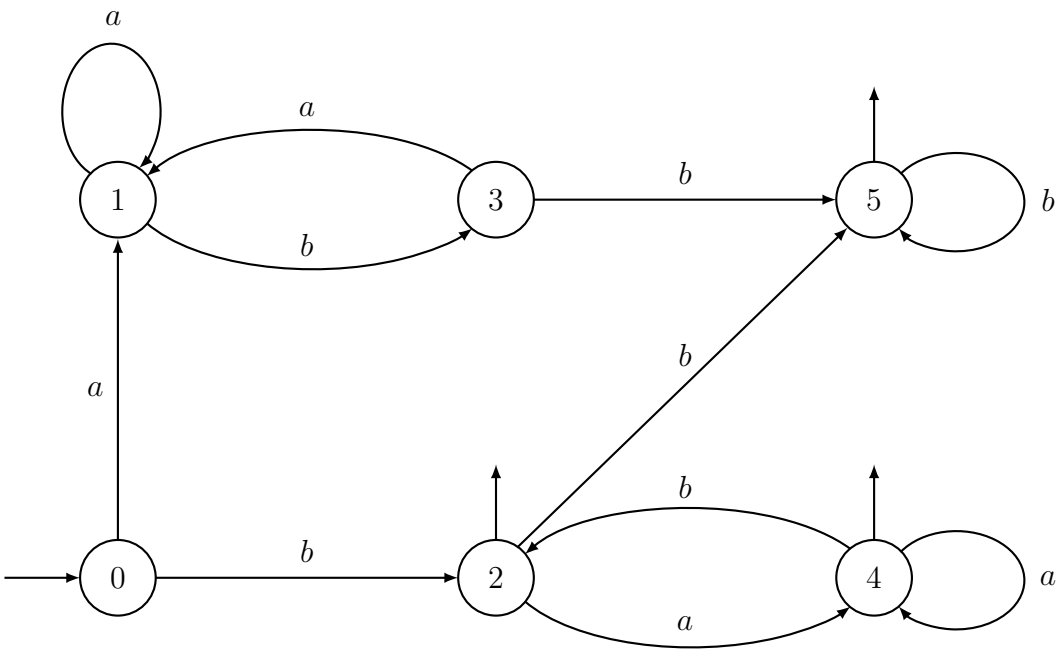


Рис. 2.7: Автомат, який розпізнає множину U

Твердження 2.5.28. *Нехай $A \neq \varnothing$, $X \subset A^+$ і $\mathcal{A} = (Q, 1, 1)$ — впорядкований автомат, який розпізнає моноїд X^*. Тоді множина X є повною тоді і лише тоді, коли моноїд переходів автомата $\mathcal{A}$ не містить порожнього відношення.*

Доведення. Якщо множини X є повною, то для довільного слова $w \in A^*$ існують два слова $u, v \in A^*$ такі, що $uwv \in X^*$. Тоді існує шлях

$$1 \xrightarrow{u} p \xrightarrow{w} q \xrightarrow{v} 1.$$

Звідси випливає, що (p, q) є в $\varphi(w)$, а отже $\varphi_{\mathcal{A}}(w)$ не є порожнім відношенням.

Навпаки, якщо $\varphi_{\mathcal{A}}(A^*)$ не містить порожнього відношення, то для кожного слова $w \in A^*$ існує хоча б один шлях $p \xrightarrow{w} q$. Позаяк автомат $\mathcal{A}$ є впорядкованим, то існують два шляхи $1 \xrightarrow{u} p$ і $q \xrightarrow{v} 1$. Тоді $uwv \in X^*$. Отже множина X є повною. □

Для (комутативного) полінома $p \in Q[A]$ та розподілу Бернуллі π на алфавіті A через $\pi(p)$ позначимо кількість число, отримане підстановкою $\pi(a)$ на літеру a, для всіх $a \in A$. Більш точно, поклавши $A = \{a_1, \ldots, a_n\}$ і $p = p(a_1, \ldots, a_n)$, число $\pi(p)$ дорівнює $\pi(p) = p(\pi(a_1), \ldots, \pi(a_n))$.

Твердження 2.5.29. *Нехай $A \neq \varnothing$, $p \in Q[A]$ — поліном і $a \in A$ — літера. Тоді такі умови є еквівалентними:*

(i) p ділиться на многочлен $1 - \sum_{a \in A} a$;

(ii) $\pi(p) = 0$ для кожного додатнього розподілу Бернуллі.

Доведення. Імплікація $(i) \Longrightarrow (ii)$ є очевидною.

Для доведення імплікації $(ii) \Longrightarrow (i)$ зафіксуємо літеру $a \in A$, ы покладемо $B = A \setminus \{a\}$. Розглянемо поліном зі змінною a з коефіцієнтами в $Q[B]$. Аналогічно, розглянемо $\sum_{a\in A} -1 = a + u$, як лінійний поліном зі змінною a та з постіним коефіцієнтом u, де $u = \sum_{b\in B} b - 1$.

Евклідове ділення полінома p поліномом $a + u$ дає $p = q(a + u) + r$, де $q \in Q[A]$ і $r \in Q[B]$. Оскільки $\pi(p) = 0$ і $\pi(a + u) = 0$ для кожного додатнього розподілу Бернуллі π, то поліном r занульовується в усіх точках $z = (z_1, \ldots, z_{n-1}) \in Q^{n-1}$ таких, що $z_i > 0$ і $z_1 + \cdots + z_{n-1} \leqslant 1$. Звідси випливає, що поліном r тако занульовується, а отже многочлен $1 - \sum_{a\in A} a$ ділить многочлен p. □

Нагадаємо, що через α позначається канонічний морфізм з $Q\langle\langle A\rangle\rangle$ на $Q[[A]]$.

Теорема 2.5.30. *Нехай $A \neq \varnothing$ і X — скінченний максимальний код на алфавіті A. Тоді $\alpha(\underline{X}) - 1$ ділиться на многочлен $\alpha(\underline{A}) - 1$.*

Доведення. Нехай π – додатній розподіл Бернуллі на вільному моноїді A^*. За теоремою 2.5.16, $\pi(X) = 1$. Далі скористаємося твердженням 2.5.29. □

Приклад 2.5.31. Для коду $X = \{aa, ba, bb, baa, bba\}$ з прикладу 4.1.7 виконується рівність

$$\alpha(\underline{X}) - 1 = (b + 1)(a + b - 1)(a + 1).$$

2.6 Композиція кодів

Введемо часткову бінарну операцію на кодах, що називаються *композицією*. Ця операція пов'язує два коди Y і Z, та задовольняє певним умовам сумісності, та третій код, який позначається через $Y \circ Z$.

Існує подвійний інтерес до цієї операції. По-перше, він дає корисний метод побудови більш складних кодів з простих. Наприклад, ми побачимо, що композиція префіксного та суфіксного кодів може бути кодом, який не є ні префіксним, ні суфіксним.

По-друге, і це становить головний інтерес для композиції, оберене поняття композиції дозволяє досліджувати структуру кодів. Якщо код X розкладається на два коди Y і Z, то ці коди, як правило, є простішими.

Нехай $Z \subset A^*$ і $Y \subset B^*$ — коди з $B = \mathrm{alph}(Y)$. Тоді коди Y і Z називається *композиційовними*, якщо існує бієкція з B на Z. Якщо відображення β є такою бієкцією, то коди Y і Z називаються *композиційовними* через β. Тоді відображення β визначає морфізм з вільного моноїда B^* у вільний моноїд A^*, який є ін'єктивним, оскільки множина Z є кодом (див. твердження 2.1.1). Множина

$$X = \beta(Y) \subseteq Z^* \subseteq A^* \tag{2.20}$$

отримується композицією Y і Z (за допомогою відображення β). Позначимо її через

$$X = Y \circ_\beta Z,$$

або просто $Y \circ Z$, коли контекст дозволяє це. Оскільки відображення β є ін'єктивним, то X і Y пов'язані між собою бієкцією, і зокрема $\mathrm{Card}(X) = \mathrm{Card}(Y)$. Слова у коді X отримуються просто заміною, у словах коду Y, кожної літери b на слово $\beta(b) \in Z$. З ін'єктивності відображення β, наслідку 2.1.6 та формули (2.20) випливає такий результат.

Твердження 2.6.1. *Якщо Y і Z — два композиційовні коди, то $X = Y \circ Z$ є кодом.*

Приклад 2.6.2. Нехай $A = \{a, b\}$, $B = \{c, d, e\}$ і

$$Z = \{a, ba, bb\} \subset A^*, \qquad Y = \{cc, d, dc, e, ec\} \subset B^*.$$

Код Z є префіксним, а код Y є суфіксним. Далі $\mathrm{Card}(B) = \mathrm{Card}(Z)$. Отже коди Y і Z є композиційовними, зокрема за допомогою морфізму $\beta\colon B^* \to A^*$, визначеного

$$\beta(c) = a, \qquad \beta(d) = ba, \qquad \beta(e) = bb.$$

Тоді

$$X = Y \circ Z = \{aa, ba, baa, bb, bba\}.$$

Код X не є ні префіксним, ні суфіксним. Означимо морфізм $\beta'\colon B^* \to A^*$ наступним чином:

$$\beta'(c) = ba, \qquad \beta'(d) = a, \qquad \beta'(e) = bb.$$

Тоді $X' = Y \circ_{\beta'} Z = \{baba, a, aba, bb, bbba\}$. Цей приклад показує, що код $Y \circ_\beta Z$ істотно залежить від відображення β.

Два вирази $X = X \circ A$ і $X = B \circ X$ — це саме ті випадки, які отримані шляхом заміни одного з двох кодів на алфавіт у виразі

$$X = Y \circ Z.$$

Справді, якщо $Y = B$, то $Z = \beta(B) = X$; а якщо тепер $Z = A$, то B можна ідентифікувати з A, а Y можна ідентифікувати з X. Ці приклади показують, що кожен код отримується принаймні двома способами як композиція кодів.

Зауважимо, також, що

$$X = Y \circ_\beta Z \qquad \Longrightarrow \qquad X^n = Y^n \circ_\beta Z, \qquad n \geqslant 2.$$

Справді, множина Y^n є колом за наслідком 2.1.7 і

$$Y^n \circ Z = \beta(Y^n) = X^n.$$

Твердження 2.6.3. *Нехай $X \subset C^*$, $Y \subset B^*$ і $Z \subset A^*$ — три коди, і припустимо, що X і Y — композиційовні коди через відображення γ, і такі, що Y і Z – композиційовні коди через відображення β. Тоді*

$$(X \circ_\gamma Y) \circ_\beta Z = X \circ_{\beta\gamma} (Y \circ_\beta Z).$$

Доведення. Ми можемо припускати, що $C = \mathrm{alph}(X)$ і $B = \mathrm{alph}(Y)$. За припущенням ін'єктивні морфізми $\gamma\colon C^* \to B^*$ і $\beta\colon B^* \to A^*$ задовольняють умови

$$\gamma(C) = Y \qquad \text{і} \qquad \beta(B) = Z,$$

відповідно. Нехай $\delta\colon D^* \to C^*$ — морфізм кодування для коду X, а отже $\delta(D)$. Тоді

$$D^* \xrightarrow{\delta} C^* \xrightarrow{\gamma} B^* \xrightarrow{\beta} A,$$

і

$$\beta\gamma\delta(D) = \beta\gamma(X) = X \circ_{\beta\gamma} \beta\gamma(C) = X \circ_{\beta\gamma} (Y \circ \beta Z),$$

а отже

$$\beta\gamma\delta(D) = \beta(\gamma\delta(D)) = \gamma\delta(D) \circ_\beta \beta(B) = (X \circ_\gamma Y) \circ_\beta Z,$$

що і завершує доведення твердження. □

Деякі властивості кодів зберігаються операцією композиція кодів.

Твердження 2.6.4. *Нехай Y і Z — композиційовні коди й $X = Y \circ Z$. Тоді:*

(1) *якщо Y і Z — префіксні (суфіксні) коди, то X — префіксний (суфіксний) код;*
(2) *якщо Y і Z — повні коди, то X — повний код;*
(3) *якщо Y і Z — тонкі коди, то X — тонкий код.*

Доведення пункту 3 твердження 2.6.4 використовує лему 2.6.5, яка не може бути доведена до викладень розділу 9 (лема 9.4.8), де будуть доступні більш потужні інструменти.

Лема 2.6.5. *Нехай $A \neq \varnothing$ і Z — тонкий код над A. Для довільного слова $u \in Z^*$ існує слово $w \in Z^*uZ^*$, яке задовольняє таку властивість: якщо $twn \in Z^*$, то існує факторизація $w = sut$ з $ms, tn \in Z^*$.*

Доведення твердження 2.6.4. Нехай $Y \subset B^*$, $Z \subset A^*$ і $\beta\colon B^* \to A^*$ — ін'єктивний морфізм з $\beta(B) = Z$. Отож, $X = \beta(Y) = Y \circ_\beta Z$.

(1) Припустимо, що Y і Z — префіксні коди. Розглянемо $x, xu \in X$ з $u \in A^*$. Позаяк $X \subset Z^*$, то $x, xu \in Z^*$, і оскільки Z^* — унітарний справа моноїд, то $u \in Z^*$. Нехай $y = \beta^{-1}(x)$, $v = \beta^{-1}(u) \in B^*$. Тоді множини $y, yv \in Y$ і Y є префіксними. Отож, $v = 1$, а отже $u = 1$. Звідси випливає, що код X є префіксним. Доведення у випадку суфіксних кодів є аналогічним.

(2) Let $w \in A^*$. Код Z є повним, а отже $uwv \in Z^*$ для деяких слів $u, v \in A^*$. Нехай $h = \beta{-}1(uwv) \in B^*$. З повноти коду Y випливає існування двох слів $\overline{u}, \overline{v} \in B^*$ таких, що $\overline{u}h\overline{v} \in Y^*$. Але тоді $\beta(\overline{u})uwv\beta(\overline{v}) \in X^*$. Звідси випливає повнота коду X.

(3) Якщо код Z не є повним, то $F(X) \subset F(Z^*) \neq A^*$ і код X є тонким. Припустимо, що код Z є повним. Код Y є тонким. Отже, отримуємо $F(Y) \neq B^*$. Нехай $\overline{u} \in B^* \setminus F(Y)$ і $u = \beta(\overline{u})$. Нехай w — слово, яке ставиться у відповідність слову u в лемі 2.6.5. Тоді $w \notin F(X)$. Справді, припустивши протилежне отримуємо, що існують слова $m, n \in A^*$ такі, що

$$x = mwn \in X \subset Z^*.$$

З огляду на лему 2.6.5,

$$x = msutn, \qquad \text{з} \quad ms, tn \in Z^* = \beta(B^*).$$

Поклавши $p = \beta^{-1}(ms)$, $q = \beta^{-1}(tn)$, отримуємо $p\overline{u}q \in Y$. Отож, $\overline{u} \in F(Y)$, а це суперечить припущенню. З отриманого протиріччя випливає, що слово w не э елементом коду X, а отже код X є тонким. □

Розглянемо тепер другий аспект операції композиції кодів, а саме розклад коду на більш прості. Для цього зручно поширити позначення alph наступним чином: нехай $Z \subset A^*$ — код і $X \subset A^*$. Тоді

$$\mathrm{alph}_Z(X) = \{z \in Z\colon \text{існують} \quad u, v \in Z^* \quad \text{такі, що} \quad uzv \in X\}.$$

Іншими словами, $\mathrm{alph}_Z(X)$ — це множина слів у Z, які з'являються принаймні один раз у факторизації слова у X, як добуток слів у Z. Звичайно, $\mathrm{alph}_A = \mathrm{alph}$. Наступне твердження описує умову існування розкладу.

Твердження 2.6.6. *Нехай $A \neq \varnothing$ і $X, Z \subset A^*$ — коди. Тоді існує код Y такий, що $X = Y \circ Z$ тоді і лише тоді, коли*

$$X \subset Z^* \qquad i \qquad \mathrm{alph}_Z(X) = Z. \tag{2.21}$$

Доведення. Нехай $X = Y \circ_\beta Z$, де $\beta\colon B^* \to A^*$ — ін'єктивний морфізм, $Y \subset B^*$ і $B = \mathrm{alph}(Y)$. Тоді $X = \beta(Y) \subset \beta(B^*) = Z^*$, і далі $\beta(B) = \mathrm{alph}_{\beta(B)}(\beta(Y))$, тобто маємо $Z = \mathrm{alph}_Z(X)$.

Навпаки, нехай $\beta\colon B^* \to A^*$ — морфізм кодування для коду Z, і множина $Y = \beta^{-1}(X)$. Тоді $X \subset \beta(B^*) = Z^*$ s $\beta(Y) = X$. З наслідку 2.1.6 випливає, що множина Y є кодом. Далі $\mathrm{alph}(Y) = B$, оскільки $Z = \mathrm{alph}_Z(X)$. Отож, коди Y і Z є композиційовними та $X = Y \circ_\beta Z$. □

Друге твердження в умові (2.21) означає, що всі слова в коді Z з'являються принаймні в одній факторизації слова в коді X, як добутку слів у коді Z.

Ми вже бачили, що існують два очевидні розкладу коду $X \subset A^*$, як $X = Y \circ Z$, а саме $X = B \circ X$ і $X = X \circ A$. Вони отримані, взявши $Z = X$ і $Z = A$ в твердженні 2.6.6 і припустивши $A = \mathrm{alph}(X)$. Ці розклади не є цікавими. Ми будемо називати *нерозкладним* код, який не має інших розкладів. Формально код $X \subset A^*$ з $A = \mathrm{alph}(X)$ називається *нерозкладним*, якщо з $X = Y \circ Z$ і $B = \mathrm{alph}(Y)$ випливає, що $Y = B$ або $Z = A$. Якщо код X є розкладним, і якщо Z є таким кодом, що $X = Y \circ Z$, і $Z \neq X$, $Z \neq A$, то ми говоримо, що *код X розкладається над Z*.

Приклад 2.6.7. Нехай X — код, означений у прикладі 2.6.2. Код X розкладається над Z. Навпаки, код $Z = \{a, ba, bb\}$ є нерозкладним. Справді, нехай T — код такий, що $Z \subset T^*$, і припустимо, що $T \neq A$. Обов'язково, $a \in T$. Отож, $b \notin T$. Але тоді $ba, bb \in T$, звідки випливає, що $Z \subset T$. Отже, Z є максимальним колом (приклад 2.4.1), а отже $Z = T$.

Твердження 2.6.8. *Для довільного скінченного коду X існують нерозкладні коди $Z_1, \ldots, Z_n$ такі, що*

$$X = Z_1 \circ \cdots \circ Z_n.$$

Для доведення твердження 2.6.8 введемо нове поняття. Нехай X — скінченний код і

$$\ell(X) = \sum_{x\in X}(|x| - 1) = \sum_{x\in X}|x| - \mathrm{Card}(X).$$

Для кожного $x \in X$, маємо $|x| \geqslant 1$. Отож, $\ell(X) \geqslant 0$, і більше того $\ell(X) = 0$ тоді і тільки тоді, коли код X є підмножиною алфавіта.

Твердження 2.6.9. *Нехай $A \neq \varnothing$ і $B \neq \varnothing$. Якщо $X, Z \subseteq A^*$ і $Y \subset B^*$ — скінченні коди такі, що $X = Y \circ Z$, то*

$$\ell(X) \geqslant \ell(Y) + \ell(Z).$$

Доведення. Нехай $\beta\colon B^* \to A^*$ — ін'єктивний морфізм такий, що $X = Y \circ_\beta Z$. З рівності $\mathrm{Card}(X) = \mathrm{Card}(Y)$ випливає, що

$$\ell(X) - \ell(Y) = \sum_{x\in X}|x| - \sum_{y\in Y}|y| = \sum_{y\in Y}(|\beta(y)| - |y|).$$

А отже $|\beta(y)| = \sum\limits_{b\in B}|\beta(b)||y|_b$. Таким чином, отримуємо, що

$$\begin{aligned}\ell(X) - \ell(Y) &= \sum_{y\in Y}\left(\sum_{b\in B}|\beta(b)||y|_b - |y|_b\right) = \\ &= \sum_{y\in Y}\left(\sum_{b\in B}(|\beta(b)| - 1)|y|_b\right) = \\ &= \sum_{b\in B}(|\beta(b)| - 1)\left(\sum_{y\in Y}|y|_b\right).\end{aligned}$$

За припущенням маємо $B = \mathrm{alph}(Y)$, звідки випливає, що $\sum\limits_{y\in Y}|y|_b \geqslant 1$ для всіх $b \in B$. З ін'єктивності відображення β випливає, що $|\beta(b)| \geqslant 1$ для $b \in B$. Отож,

$$\ell(X) - \ell(Y) \geqslant \sum_{b\in B}(|\beta(b)| - 1) = \sum_{z\in Z}(|z| - 1) = \ell(Z),$$

що і завершує доведення твердження. □

Доведення твердження 2.6.8. Доведення проведемо індукцією по $\ell(X)$. Якщо $\ell(X) = 0$, то X складається з букв, які є очевидно нерозкладними. Якщо $\ell(X) > 0$ і X є розкладним, то $X = Y \circ Z$ для деяких кодів Y, Z. Далі Y і Z не утворюються лише з літер, а отже $\ell(Y) > 0$, $\ell(Z) > 0$. За твердженням 2.6.9 маємо, що $\ell(Y) < \ell(X)$ і $\ell(Z) < \ell(X)$. Таким чином, коди Y і Z є композицією нерозкладних кодів, а звідси випливає, що X є також такою композицією. □

Твердження 2.6.8 доводить існування розкладу кодів. Цей розклад не є єдиним, і це випливає з наступного прикладу.

Приклад 2.6.10. Розглянемо коди

$$X = \{aa, ba, baa, bb, bba\}, \qquad Y = \{cc, d, dc, e, ec\}, \qquad Z = \{a, ba, bb\}$$

з прикладу 2.6.2. Легко бачити, що $X = Y \circ Z$. Також існує розклад $X = Y' \circ_\gamma Z'$ з

$$Y' = \{cc, d, cd, e, ce\}, \qquad Z' = \{aa, b, ba\}$$

та ін'єктивним морфізмом $\gamma\colon B^* \to A^*$, який визначається

$$\gamma(c) = b, \qquad \gamma(d) = aa \qquad \text{і} \qquad \gamma(e) = ba.$$

Код Z є нерозкладним, код Z' утворюється заміною літер a та b, і беручи тоді обернене. Ці операції не змінюють нерозкладність коду.

Приклад 2.6.11. Цей приклад показує, що в розкладі коду на нерозкладні коди навіть кількість компонент не повинна бути єдиною. Для $X = \{a^3b\}$ маємо

$$X = \{cd\} \circ \{a^2, ab\} = \{cd\} \circ \{u^2, v\} \circ \{a, ab\}$$

і також

$$X = \{cd\} \circ \{a^3, b\}.$$

Це дає два розклади коду X довжини 3 і 2, відповідно.

Код X з прикладу 2.6.10 не є префіксним, ні суфіксним, але розкладається на такі коди. Ми можемо запитати: коли довільний (скінченний) код отримується як композиція префіксних і суфіксних кодів. Це не завжди так, як показано в наступному прикладі, див. також вправу 2.8.21.

Приклад 2.6.12. Код $X = \{b, ba, a^2b, a^3ba^4\}$ не є композицією префіксних і суфіксних кодів.

Припустимо протилежне. Тоді $X \subset Z^*$ для деякого префіксного (або суфіксного) коду $Z \neq A$. Отож, моноїд Z^* є унітарним справа (відп. унітарним зліва). Оскільки $b, ba \in Z^*$, то $a \in Z^*$, звідки випливає, що $A = \{a, b\} \subset Z^*$ й $A = Z$. Припустивши, що моноїд Z^* є унітарним зліва, отримуємо, що з $b, a^2b \in Z^*$ випливає $a^2 \in Z^*$. Нслідком цього є $a^3b \in Z^*$, а отже $a^3 \in Z^*$ і на завершенні отримуємо, що$a \in Z^*$. Отож, знову отримуємо $Z = A$.

Наведемо перелік властивостей кодів, які успадковуються множниками розкладу. Твердження 2.6.13 в певному сенсі є дуальним до твердження 2.6.4.

Твердження 2.6.13. *Нехай X, Y і Z — коди такі, що $X = Y \circ Z$. Тоді:*

(1) *якщо X — префіксний (суфіксний) код, то Y — префіксний (суфіксний) код;*
(2) *якщо X — максимальний код, то Y і Z — максимальні коди;*
(3) *якщо X — повний код, то Z — повний код;*
(4) *якщо X — тонкий код, то Z — тонкий код.*

Доведення. Припустимо, що $X, Z \subset A^*$, $Y \subset B^*$ і $\beta\colon B^* \to A^*$ — ін'єктивний морфізм такий, що $\beta(B) = Z$ і $\beta(Y) = X$.

(1) Нехай $y, yu \in Y$. Тоді $\beta(y), \beta(y)\beta(u) \in X$, і оскільки код X є префіксним, то $\beta(u) = 1$. З того, що $\beta\colon B^* \to A^*$ — ін'єктивний морфізм отримуємо рівність $u = 1$.

(2) Якщо код Y не є максимальним, то покладемо $Y' = Y \cup \{y\}$ — код для деякого $y \notin Y$. Тоді $\beta(Y') = \beta(Y) \cup \beta(y)$ є кодом, який відмінний від коду X з ін'єктивністю морфізму β. Отож, код X не є максимальним.

Тепер припустимо, що код Z не є максимальним. Покладемо $Z' = Z \cup \{z\}$ для деякого слова $z \notin Z$ такого, що Z' є кодом. Розширимо алфавіт B до алфавіту $B' = B \cup \{\}b$ (де $b \notin B$) та означимо морфізм β над B'^* за формулою $\beta(b) = z$. Тоді $\beta\colon B'^* \to A^*$ — ін'єктивний морфізм за твердженням 2.1.1 оскільки множина Z' є кодом. Множина $Y' = Y \cup \{b\}$ є кодом, а отже множина $\beta(Y') = X \cup \{z\}$ також є кодом, звідки випливає, що X не є максимальним кодом.

Твердження (3) випливає з включення $X^* \subset Z^*$.

(4) Кожне слово в коді Z є множником слова в коді X. Звідси випливає, що $F(Z) \subseteq F(X)$. За припущенням, $F(X) \neq A^*$. Отож, $F(Z) \neq A^*$, а отже код Z є тонким. □

Твердження 2.6.14. *Нехай X, Y і Z — три коди такі, що $X = Y \circ Z$. Тоді код X є тонким і повним тоді і тільки тоді, коли коди Y і Z є тонкими і повними.*

Доведення. За твердженням 2.6.4 з того, що коди Y і Z є тонкими і повними випливає, що код X є тонким і повним. Навпаки, припустимо, що код X є тонким і повним. З твердження 2.6.13 випливає, що код Z є тонким і повним. За теоремою 2.5.14 код X є максимальним. За твердженням 2.6.13 код Y є максимальним, а отже за теоремою 2.5.5, Y є повним кодом. Залишилось довести, що код Y є тонким. З позначеннями доведення твердження 2.6.13 розглянемо слово $u \notin F(X)$. Оскільки моноїд Z^* є щільним, то $sut \in Z^*$ для деяких слів $s, t \in A^*$. Отож, $sut = \beta(w)$ для деякого слова $w \in B^*$. Але тепер слово w не є поповнювальним в коді Y, інакше $hwk \in Y$ для деяких слів $h, k \in B^*$. Звідси випливає, що $\beta(h)sut\beta(k) \in X$, а отже $u \in F(X)$. Таким чином, код Y є тонким. □

За твердженням 2.6.14 для тонких кодів Y і Z код $Y \circ Z$ є максимальним тоді і тільки тоді, коли коди Y і Z є максимальними. Ми не знаємо прикладу, який показує, що це твердження є хибним без додаткового припущення, що коди Y і Z є тонкими.

Твердження 2.6.15. *Нехай $A \neq \varnothing$ і X — максимальний код над алфавітом A. Для довільного коду $Z \subset A^*$ код X розкладається над Z тоді і тільки тоді, коли $X^* \subseteq Z^*$. Зокрема, код X є нерозкладним тоді і лише тоді, коли X^* є максимальним вільним підмоноїдом вільного моноїда A^*.*

Доведення. Якщо код X розкладається над кодом Z, то $X^* \subseteq Z^*$. Навпаки, якщо $X^* \subseteq Z^*$, то покладемо $\overline{Z} = \mathrm{alph}_Z(X)$. Тоді $X \subset \overline{Z}^*$, і звичайно $\overline{Z} = \mathrm{alph}_{\overline{Z}}(X)$. За твердженням 2.6.6 код X розкладається над кодом $\overline{Z}$. З твердження 2.6.13 випливає, що код $\overline{Z}$ є максимальним. З включення $\overline{Z} \subseteq Z$ отримуємо рівність $\overline{Z} = Z$. □

Приклад 2.6.16. Нехай A — алфавіт. Ми доведемо, що однорідний код A^n розкладається над кодом Z тоді і тільки тоді, коли $Z = A^m$ і число m ділить число n. Зокрема, код A^n є нерозкладним для первинного числа n і для $n = 1$.

Справді, нехай $A^n = X = Y \circ_\beta Z$, де $Y \subset B^*$ і $\beta\colon B^* \to A^*$. Код X є максимальним і біфіксним, а отже код Y також є максимальним і біфіксним і код Z є максимальним. Нехай $y \in Y$ — слово максимальної довжини, і покладемо $y = ub$ з $b \in B$. Тоді $Y \cup uB$ є префіксом. Нехай справді $y' = ub'$, $b' \in B$. Кожен власний префікс слова y' є також власним префіксом слова y, а отже не є елементом у $Y \cup uB$. Далі, якщо y' є префіксом деякого слова y'' в $Y \cup uB$, то за максимальністю довжини слова y маємо, що $|y'| = |y''|$ і $y' = y''$. Отож, множина $Y \cup uB$ є кодом. Звідси отримуємо рівність $Y \cup uB = Y$, оскільки код Y є максимальним. Звідси випливає, що $\beta(uB) = \beta(u)Z \subseteq X$. Тепер, оскільки код X є максимальним, то всі слова в коді Z мають однакову довжину, і нехай вона дорівнює m. Позаяк код Z є максимальним, то $Z = A^m$. Звідси випливає, $n = m|y|$.

2.7 Префіксний граф кода

Префіксний граф використовується для того, щоб дати ефективну перевірку того, чи є множина X кодом. Граф також може відповісти на деякі інші питання про множину X, застосовуючи стандартну техніку для трансверсалі графа. Це буде детально описано в наступних розділах (див. вправи 5.4.1 і 5.4.2).

Нехай X — скінченна множина слів над деяким алфавітом A. Означимо граф G_X для X, який називається *префіксним графом множини* X, наступним чином. Вершинами графа G_X є непорожні префікси слів множини X, та існує ребро з вершини s у вершину t, тоді і тільки тоді, коли виконується одна з двох умов: або $st \in X$, або $sx = t$ для деякого слова $x \in X$ (див. рис. 2.8).

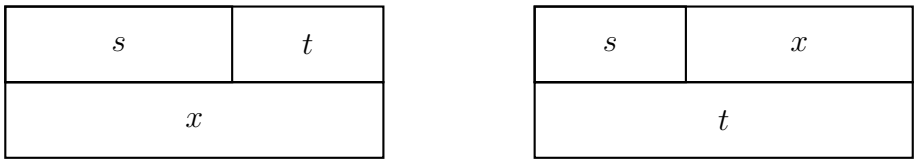


Рис. 2.8: Два типи вершин префіксного графа

Ребра першого типу називаються *схрещуваннями*, а ті, що є другого типу *розширеннями*. Ребро схрещування (s,t) позначене словом t, ребро розширення (s,t) з $sx = t$ позначене x. Як завжди, мітка шляху є добутком міток її ребер. У випадку, коли $sx = t$ і x, t є в X, то (s,t) є ребро розширення, позначене x, а (s,x) — ребро схрещування, також позначене через x.

Вершина s призначена для зображення префікса, який був побудований в процесі побудови подвійної факторизації, скажемо $ys = z$, для $y, z \in X^*$. Ребро схрещування (s,t) з $st = x \in X$, дає факторизацію $yx = zt$, а префікс t переставляється на інший бік рівняння, тоді як ребро розширення (s,t) з $sx = t$ замінює факторизацію на $yt = zx$, розширюючи поточний префікс з s до t (див. рис. 2.9).

Приклад 2.7.1. Нехай $X = \{a, bb, abbba, babab\}$ над алфавітом $A = \{a, b\}$. Непорожніми префіксами, крім слів множини X, є слова

$$b, ab, ba, abb, bab, abbb \qquad \text{і} \qquad baba,$$

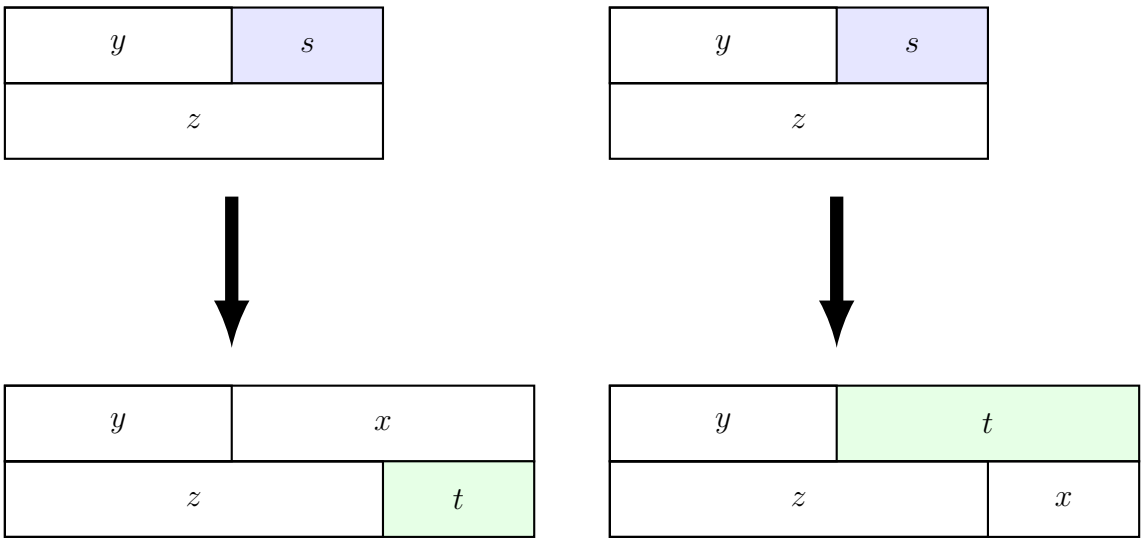


Рис. 2.9: Два способи продовження подвійної факторизації $ys = z$. Зліва вона поширюється на $yx = zt$, а справа на $yt = zx$

а отже граф має 11 вершин. Префіксний граф G_X зображено на рис. 2.10. Ребро схрещування зображено штрихованим і ребро розширення зображено суцільним. Міткою ребра схрещування є назва його кінця. Міткою ребра розширення (s, t) є слово $x \in X$ для якого $sx = t$.

Ми доведемо, що множина X є кодом тоді і тільки тоді, коли не існує шляху в префіксному графі G_X від вершини в X до вершини в X. У наведеному прикладі 2.7.1 є шлях від a до a, або до $abbba$, а тому множина X не є кодом.

Почнемо з леми, яка описує шляхи в префіксному графі G_X. По-перше, нам потрібне означення. Дві факторизації $(x_1, \ldots, x_n)$ і $(y_1, \ldots, y_m)$ слова w називаються *диз'юнктними*, якщо $x_1 \cdots x_n \neq y_1 \cdots y_j$ для $1 \leqslant i < n$, $1 \leqslant j < m$. Ми просто кажемо, що

$$x_1 \cdot x_n = y_1 \cdot y_m$$

є *диз'юнктною подвійною факторизацією*, коли дві факторизації $(x_1, \ldots, x_n)$ і $(y_1, \ldots, y_m)$ деякого одного й того ж слова є диз'юнктними.

Лема 2.7.2. *Існує шлях довжини $n \geqslant 1$ з вершини s у вершину t у префіксному графі X тоді і тільки тоді, коли існують слова $x_1, \ldots, x_k, y_1, \ldots, y_l \in X$ такі, що*

$$sy_1 \cdots y_l t = x_1 \cdots x_k \qquad \text{або} \qquad sy_1 \cdots y_l = x_1 \cdots x_k t$$

є диз'юнктними факторизаціями з $k + l = n$, і більше того, слово s префіксом слова x_1 (відп. префіксом слова t у випадку $k = 0$). Міткою шляху є слово $y_1 \cdots y_l t$ у першому випадку, і слово $y_1 \cdots y_l$ у другому випадку. Перший (другий) випадок відбувається тоді і тільки тоді, коли шлях містить непарну (парну) кількість ребер схрещування.

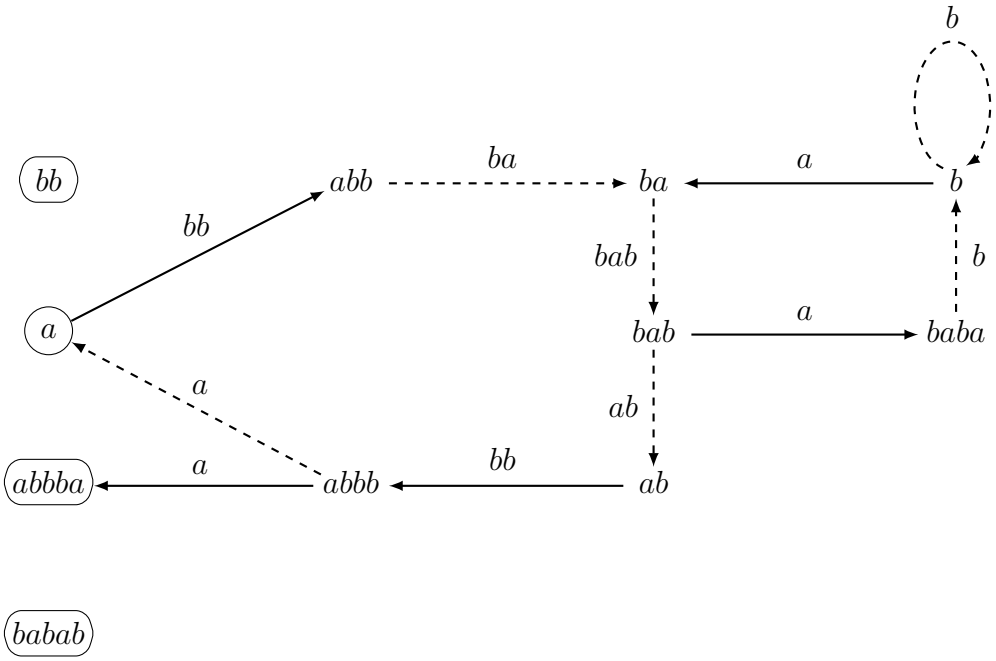


Рис. 2.10: Префіксний граф G_X для множини $X = \{a, bb, abbba, babab\}$

Приклад 2.7.3. Розглянемо приклад шляху

$$abb \xrightarrow{ba} ba \xrightarrow{bab} bab \xrightarrow{ab} ab \xrightarrow{bb} abbb$$

у графі з прикладу 2.7.1. Його можна зобразити так:

				b	a	b	a	b			
a	b	b	b	a	b	a	b	a	b	b	b

Цей шлях має довжину 4, перші 3 ребра є ребрами схрещування, останнє є ребром розширення. Цьому шляхові відповідає диз'юнктна факторизація

$$abb|babab|abbb = abbba|babab|bb.$$

Тут $l = 1$, $k = 3$, і добуток міток дорівнює $bababbbb$. Шлях

$$a \xrightarrow{bb} abb \xrightarrow{ba} ba \xrightarrow{bab} bab \xrightarrow{ab} ab \xrightarrow{bb} abbb \xrightarrow{a} a$$

має ще два ребра.

a	b	b	b	a	b	a	b	a	b	b	b
a	b	b	b	a	b	a	b	a	b	b	b

Цьому шляху відповідають диз'юнктні факторизації

$$a|bb|babab|abbba = abbba|babab|bb|a,$$

звідки випливає, що множина X не є кодом.

Доведення леми 2.7.2. Припустимо спочатку, що існує шлях довжини $n \geqslant 1$ з вершини s у вершину t. Якщо $n = 1$, то або $st = x$, або $sx = t$ з $x \in X$. Таким чином, існує подвійна факторизація необхідної форми для $n = 1$.

Припустимо тепер, що $n \geqslant 1$ та існує ребро з вершини t у вершину u. За припущенням,

$$sy_1 \cdots y_l t = x_1 \cdots x_k \qquad \text{або} \qquad sy_1 \cdots y_l = x_1 \cdots x_k t,$$

і або $tu = x \in X$ або $tx = u$ для деякого слова $x \in X$, $u \notin X$. Отже, необхідно перевірити чотири випадки.

1. Якщо $sy_1 \cdots y_l t = x_1 \cdots x_k$ і $tu = x \in X$, то

   $$sy_1 \cdots y_l x = x_1 \cdots x_k u,$$

   і ці факторизації знову є диз'юнктними, оскільки слово u є власним суфіксом слова x.

2. Якщо $sy_1 \cdots y_l t = x_1 \cdots x_k$ і $tx = u$ для деякого слова $x \in X$, то

   $$sy_1 \cdots y_l u = x_1 \cdots x_k x,$$

   а отже факторизації знову є диз'юнктними, оскільки слово u є власним суфіксом слова t, а тому воно є власним суфіксом слова x_k.

3. Якщо $sy_1 \cdots y_l = x_1 \cdots x_k t$ і $tu = x \in X$, то

   $$sy_1 \cdots y_l u = x_1 \cdots x_k x,$$

   і ці факторизації знову є диз'юнктними, оскільки слово u є власним суфіксом слова x. Більше того, якщо $k = 0$, то слово s є префіксом слова x, оскільки s є префіксом слова t і t є префіксом слова x.

4. Якщо $sy_1 \cdots y_l = x_1 \cdots x_k t$ і $tx = u$ для деякого слова $x \in X$, то

   $$sy_1 \cdots y_l x = x_1 \cdots x_k u,$$

   і ці факторизації знову є диз'юнктними, оскільки слово u є власним суфіксом слова x. Якщо $k = 0$, то слово s префіксом слова t і t є префіксом слова u, а отже s є префіксом слова u.

Навпаки, припустимо, що існує подвійна факторизація $sy_1 \cdots y_l t = x_1 \cdots x_k$ або подвійна факторизація $sy_1 \cdots y_l = x_1 \cdots x_k t$, з $k + l = n$. Якщо $n = 1$, то $k = 1$, $l = 0$ у першому випадку, і $k = 0$, $l = 1$ у другому випадку. Справді, значення $k = 1$, $l = 0$ у другому випадку виключається умовою, що слово s є префіксом слова x_1.

Таким чином, у першому випадку існує ребро схрещування (s,t), а у другому — ребро розширення (s,t).

Припустимо, що $n>1$ і $sy_1\cdots y_lt = x_1\cdots x_k$. Позаяк $t\neq x_k$, то одне з цих слів є власним суфіксом іншого. Припустимо спочатку, що слово t є власним суфіксом слова x_k, і покладемо $x_k = ut$. Тоді існує ребро з u до t у графі G_X, і більше того

$$sy_1\cdots y_l = x_1\cdots x_{k-1}u.$$

Якщо $k=1$, тоді слово s є власним префіксом слова u, інакше слово s залишається власним префіксом слова x_1. Застосувавши індукцію, отримуємо, що існує шлях з вершини s до вершини u довжини $n-1$, а отже існує шлях довжини n з вершини s до вершини t. Припустимо далі, що слово x_k є суфіксом слова t і покладемо $t = ux_k$. Це визначає ребро розширення (u,t). Отож,

$$sy_1\cdots y_lu = x_1\cdots x_{k-1}.$$

Позаяк лівий бік рівності є непорожнім, то слово s є префіксом слова x_1. Висновок знову випливає з припущення індукції.

Якщо подвійною факторизацією є

$$sy_1\cdots y_l = x_1\cdots x_kt,$$

то оскільки слово s є власним префіксом правого боку рівності, отримуємо $l>0$.

Якщо слово y_l є власним суфіксом слова t, то $t = uy_l$ для деякого слова u та існує ребро розширення (u,t). Замінивши слово t на uy_l, отримуємо

$$sy_1\cdots y_{l-1} = x_1\cdots x_ku.$$

Звідси випливає, що слово s є префіксом слова x_1, або $k=0$, а тоді слово s є власним префіксом слово u якщо $l>1$ або $s=u$ якщо $l=1$. У першому випадку, існує шлях з вершини s до вершини u, а в другому випадку існує саме ребро (s,t).

На завершенні, припустимо, що слово t є власним суфіксом слова y_l. Тоді $y_l = ut$, а отже існує ребро схрещення (u,t). Далі,

$$sy_1\cdots y_{l-1}u = x_1\cdots x_k,$$

а отже $k\geqslant 1$ і слово s залишається префіксом слова x_1. Існує знову шлях з вершини s до вершини u довжини $n-1$ з припущенням індукції. Це завершує доведення леми. □

Теорема 2.7.4. *Множина X непорожніх слів є кодом тоді і тільки тоді, коли не існує шляху в її префіксному графі G_X з вершини в X до вершини в X.*

Доведення. Припустимо, що існує шлях з вершини в X до вершини в X у префіксному графі G_X. Тоді існує диз'юнктна подвійна факторизація одного з випадків, описаних в доведенні леми 2.7.2. У кожному з цих випадків отримуємо подвійну факторизацію слова, як добуток слів у множині X.

Навпаки, припустимо, що множина X не є кодом, і розглянемо найкоротше слово w у вільній напівгрупі X^+, яке має дві різні факторизації

$$w = x_1\cdots x_n = y_1\cdots y_m,$$

з $x_1,\ldots,x_n,y_1,\ldots,y_m\in X$. Можемо вважати, що x_1 є власним префіксом слова y_1. Тоді існує шлях з вершини x_1 до вершини y_m довжини $m+n-2$ у графі G_X. □

З огляду на скінченний граф G, багато властивостей графа G можна перевірити в лінійному часі щодо розміру графа G, де розміром є загальна кількість вершин і ребер у G. Серед цих властивостей є існування циклів, існування шляхів між виділеними множинами вершин, та інше. Усі властивості, описані в попередньому розділі, є такого ж типу. Для цього необхідно оцінити розмір графа G_X множини X.

Твердження 2.7.5. *Нехай X — скінченна множина слів з n елементами та $N = \sum_{x\in X} |x|$ — сума довжин слів у множині X. Тоді префіксний граф G_X має щонайбільше N вершин і щонайбільше nN ребер.*

Доведення. Вершини графа G_X — це непорожні префікси слів у множині X і їх є не більше, чим $N-1$. Далі розглянемо вершину t і ребро (s,t), що входить в t. Якщо (s,t) є ребром схрещення, то слово $st \in X$ довше, ніж слово t, а якщо $t = sx$ для деякого слова $x \in X$, то слово x коротше, ніж слово t. Таким чином, слово x у множині X або породжує максимум одне ребро схрещення, або воно генерує не більше одного ребра розширення. Отже, загальна кількість ребер, які входять у вершину t, не перевищує xbckf n, а загальна кількість ребер у графі G_X не є більшою за nN. □

З вище викладених міркувань випливає такий наслідок:[2]

Наслідок 2.7.6. *Префіксний граф G_X множини X з n слів загальної довжини N, можна перевірити за час $O(nN)$, на те чи X є кодом.*

Залишається показати, як побудувати префіксний граф G_X скінченної множини X у лінійному часі по його розмірі, тобто по nN, де n – кількість слів у множині X, а N — сума довжин слів у X.

Побудова здійснюється в три етапи. Спочатку будується простий автомат, що розпізнає множину X. Цей автомат є детерміновним, але не повним і має форму дерева. Такий автомат зазвичай називають *навантаженим деревом* (англ. *trie*). Вершини графа G_X є серед станів цього автомата. Потім автомат перетворюється в так звану *машину, яка розпізнає шаблони* (англ. *pattern matching machine*). Це робиться в обладнанні навантаженого дерева *функцією відмови* (англ. *failure function*). Роль цієї функції полягає в тому, щоб забезпечити, у випадку, якщо перехід не існує для деякої літери в якийсь стан, то можна шукати можливий перехід у інший стан. В результаті машина, яка розпізнає шаблони, розпізнає за допомогою функції відмови множину A^*X слів, що закінчуються словами з множини X.

Ці два попередні кроки використовуються на останньому етапі для ефективного обчислення ребер графа G_X.

Для скінченної множини X слів над алфавітом A *навантаженого дерева* множини X є автомат, чий набір станів є множиною P префіксів слів множини X. Початковим станом тут є порожнє слово, кінцевими станами є слова з множини X. Функція станів визначена для $p \in P$ і $a \in A$ тоді і тільки тоді, коли pa в P, і тоді $p \cdot a = pa$.

[2]Кажуть, що алгоритм виконується за лінійний час або час $O(n)$, коли його складність дорівнює $O(n)$. По простому, це означає, що час виконання зростає щонайбільше лінійно від кількості вхідних даних. Більш точно, це означає, що існує константа c, така, що час виконання буде щонайбільше cn, коли розмір вхідних даних n. Наприклад, час виконання процедури, яка знаходить суму всіх елементів списку, буде пропорційною довжині списку за умови, що час виконання операції додавання є сталим, або, принаймні, обмежений сталою.

Навантажене дерево множини X можна побудована дуже просто, вставивши слова множини X у дерево, яке спочатку зводиться до порожнього слова.

TRIE(X)

```
1   T ← New Automaton()
2   for x ∈ X do
3       p ← ε
4       for i ← 1 to |x| do
5           a ← x[i]
6           if p · a exists then
7               p ← p · a
8           else q ← New State()
9               p · a ← q
10              p ← q
11      SetTerminal(p)
12  return T
```

Цей алгоритм чітко обчислює навантажене дерево множини X за час $O(N)$, де N — сума довжин слів у X.

Приклад 2.7.7. Навантажене дерево множини $X = \{a, bb, abbbba, babab\}$ зображено на рис. 2.11. Воно розглядається як автомат, що приймає слова в множині X.

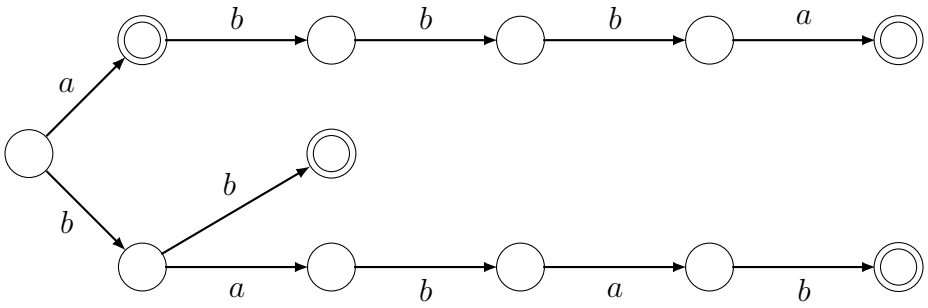


Рис. 2.11: Навантажене дерево множини $X = \{a, bb, abbbba, babab\}$

Для скінченної множини X слів над алфавітом A, функція відмови призначена для використання, коли функція наступного стану $p \cdot a$ є невизначеною в навантаженому дереві множини X. Вона дає стан q, де необхідно запустити нове навантажене дерево для обчислення наступного стану.

Функція відмови f множини X визначається на множині непорожніх префіксів слів множини X. Для $p \in P$, $p \neq \varepsilon$, $f(p)$ — найдовший власний суфікс слова p, який є в P. Для порожнього слова покладемо $f(\varepsilon) = \varepsilon$.

Машина, яка розпізнає шаблони множини X є автоматом, отриманим з навантаженого дерева множини X шляхом розширення функції наступного стану на P так:

$$p \cdot a = \begin{cases} pa, & \text{якщо } pa \in P; \\ f(p) \cdot a, & \text{в інших випадках.} \end{cases}$$

Більш того, зауважимо, що стан p є кінцевим, якщо $f(p)$ є кінцевим станом. Функція ComputeFailure(T) обчислює функцію відмови для навантаженого дерева T.

ComputeFailure(T)

```
1   f(ε) ← ε
2   F ← New Queue()
3   for a ∈ A such that ε · a is defined do
4       f(ε · a) ← ε
5       Add(F, ε · a)
6   while F ≠ ∅ do
7       p ← Get(F)
8       if IsTerminal(f(p)) then
9           SetTerminal(p)
10      for a ∈ A such that p · a is defined do
11          q ← f(p)
12          while q · a is undefined do
13              q ← f(p)
14          f(p · a) ← q · a
15      Add(F, p · a)
```

Машина, яка розпізнає шаблони отримується шляхом побудови спочатку навантаженого дерева, а потім функції відмови.

Приклад 2.7.8. Машина, яка розпізнає шаблони множини $X = \{a, bb, abbbba, babab\}$ зображена на рис. 2.12. Вона розглядається як автомат, вона приймає слова в A^*X.

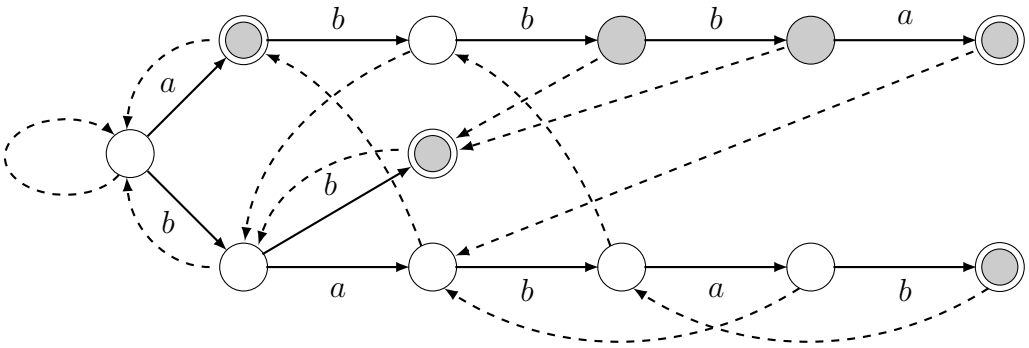


Рис. 2.12: Машина, яка розпізнає шаблони множини $X = \{a, bb, abbbba, babab\}$

Її приймаючі стани є сірими. Функція відмови зображається штрихованими ребрами.

Стан p є кінцевим для машини, яка розпізнає шаблони, якщо він є словом в A^*X. Виявляється корисним знати найдовший суфікс стану p, який є в X. Назвемо його $\sigma(p)$. Функція σ невизначена на некінцевих станах, а для кінцевих станів визначається так:

$$\sigma(p) = \begin{cases} f(p), & \text{якщо } f(p) \text{ є в } X; \\ \sigma(f(p)), & \text{в інших випадках.} \end{cases}$$

Це показує, що ми пам'ятаємо які стани є в X, і це досить легко і лінійно по кількості станів, щоб обчислити функцію σ.

Тепер ми готові обчислити ребра графа G_X. Кожне слово x в X може виробляти декілька ребер схрещування (s, t). Ребро є ребром схрещування, якщо суфікс t також є префіксом слова в X. Всі ці суфікси перенумеровані функцією відмови. Таким чином, ми отримали функцію для обчислення ребер схрещування:

CrossingEdges(X)

```
1   for x ∈ X do
2       t ← f(x)
3       while t ≠ ε do
4           s ← xt^{-1}
5           AddCrossingEdge(s, t)
6           t ← f(t)
```

Єдиним непростим напрямком є обчислення вершини, яка відповідає слову xt^{-1}. Це можна зробити, підтримуючи для кожного слова x в X масив покажчиків на вершини його префіксів, індексованих їх довжиною. Отже, з довжини слова x і довжини слова t отримуємо довжину слова s, тобто s сталим часом.

Обчислення ребер розширення дуже схожі. Враховуючи суфікс t, шукаємо всі суфікси x слова t. Кожен з цих суфіксів дає ребро розширення (s, t), причому $sx = t$. Щоб прокрутити суфікси t, які є в X, можна повторити функцію σ. Таким чином функцією є:

ExtendingEdges(X)

```
1  for t terminal states do
2      x ← σ(t)
3      while t ≠ ε do
4          s ← tx^{-1}
5          AddExtendingEdges(s, t)
6          t ← σ(x)
```

Знову ж таки, хитрою точкою є обчислення вершини $s = tx^{-1}$. Для цього для кожної вершини p зберігається покажчик на найдовше слово в X, для якого p є префіксом. У даному випадку слово s є префіксом слова t, тому вони поділяють одне і те ж найдовше слово в X, і знову застосовується трюк використовуваного раніше масиву для того, щоб дати вершину s в сталий час.

Загалом, наступна функція обчислює префіксний граф множини X.

ExtendingEdges(X)

```
1  T ← Trie(X)
2  ComputeFailure(T)
3  CrossingEdges(X)
4  ExtendingEdges(X)
```

Нарешті, можна викласти наступний результат, як наслідок попередніх конструкцій.

Твердження 2.7.9. *Для множини X, яка складається з n слів над деяким алфавітом A, загальної довжини $N = \sum_{x \in X} |x|$, префіксний граф G_X можна побудувати в часі та просторі $O(nN)$.*

2.8 Вправи до розділу 2

Підрозділ 2.1

В. 2.8.1. Нехай $n \geqslant 1$ — натуральне число. Нехай I і J — дві множини невід'ємних цілих чисел такі, що для $i, i' \in I$ та $j, j' \in J$, з умови

$$i + j \equiv i' + j' \mod n$$

випливає, що

$$i = i' \qquad \text{та} \qquad j = j'.$$

Нехай $Y = \{a^i b a^j : i \in I, j \in J\}$ і $X = Y \cup \{a^n\}$. Довести, що X є кодом над алфавітом $A = \{a, b\}$.

Підрозділ 2.2

В. 2.8.2. Довести безпосередньо (тобто не використовуючи теорему 2.2.16), що множина $X = \{x, y\}$ є кодом тоді і лише тоді, коли x та y не є степенями одноелементного слова.

(*Підказка*: використати індукцію по $|x| + |y|$.)

В. 2.8.3. Нехай K — поле й A — непорожня множина. Нехай $X \subset A^+$ — код і $K\langle X\rangle$ — піднапівкільце напівкільця $K\langle A\rangle$, породжене елементами множини X. Довести, що напівкільце $K\langle X\rangle$ є вільним в такому сенсі: нехай $\beta\colon B^* \to A^*$ — кодуючий морфізм для X. Продовжимо відображення β лінійно до морфізму з напівкільця $K\langle B\rangle$ в напівкільце $K\langle A\rangle$. Довести, що відображення β є ізоморфізмом між напівкільцями $K\langle B\rangle$ і $K\langle X\rangle$.

В. 2.8.4. Довести, що підмоноїд N моноїда M є стійким тоді і лише тоді, коли для всіх $m, n \in M$ виконується умова:

$$nm, n, mn \in N \qquad \Longrightarrow \qquad m \in N.$$

В. 2.8.5. Нехай M — комутативний моноїд. Довести, що підмоноїд моноїда M є стійким тоді і лише тоді, коли він є біунітарним.

В. 2.8.6. Нехай A — непорожня множина. Для $X \subset A^+$ нехай Y — база найменшого унітарного справа підмоноїда, який містить множину X.

(*a*) Довести, що $Y \subseteq (Y^*)^{-1}X$.
(*b*) Вивести звідси, що $\mathrm{Card}(Y) \leqslant \mathrm{Card}(X)$, і наведіть приклад, який показує, що ця нерівність може перетворитися в рівність.

В. 2.8.7. Нехай A — непорожня множина й X — підмножина вільної напівгрупи A^+. Означимо послідовність $(S_n)_{n\geqslant 0}$ підмножин вільного моноїда A^*, поклавши:

$$S_0 = X^*, \qquad S_{n+1} = \left(S_n^{-1} S_n \cap S_n S_n^{-1}\right)^*.$$

Означимо $S(X) = \bigcup_{n\leqslant 0} S_n$. Довести, що $S(X)$ вільною оболонкою множини X, а у випадку коли множина X є розпізнуваною, то і її вільна оболонка також є розпізнуваною.

В. 2.8.8. Нехай A — непорожня множина, M — підмоноїд вільного моноїда A^* й $X = (M \setminus \{1\}) \setminus (M \setminus \{1\})^2$ — мінімальна породжуюча множина в M. Довести, що множина X є розпізнуваною тоді і тільки тоді, коли моноїд M є розпізнуваний.

В. 2.8.9. Довести, що моноїд M є вільним тоді і лише тоді, коли він задовольняє такі умови:

(*i*) існує морфізм $\lambda\colon M \to \mathbb{N}$ в адитивний моноїд $\mathbb{N}$ такий, що $\lambda^{-1}(0) = 1_M$;
(*ii*) для всіх $x, y, z, t \in M$, виконується рівність $xy = zt$ тоді і тільки тоді, коли існує елемент $u \in M$ такий, що $xu = z$ і $y = ut$, або $x = zu$ і $uy = t$.

Підрозділ 2.3

В. 2.8.10. Нехай A — непорожня множина й X — підмножина вільної напівгрупи A^+ така, що $X \cap XX^+ = \varnothing$. Означимо відношення $\rho \subseteq A^* \times A^*$ так: $(u, v) \in \rho$ тоді і тільки тоді, коли існує слово $x \in X^*$ таке, що

$$uxv \in X, \qquad ux \neq 1, \qquad uv \neq 1 \qquad \text{і} \qquad xv \neq 1.$$

Довести, що множина X є кодом тоді і тільки тоді, коли $(1, 1) \notin \rho^+$, де через ρ^+ позначається транзитивне замикання відношення ρ.

Підрозділ 2.4

В. 2.8.11. Нехай $n \geqslant 1$ — натуральне число. Нехай I і J — дві підмножини множини $\{0, 1, \ldots, n-1\}$ такі, що для кожного числа $p \in \{0, 1, \ldots, n-1\}$ існує єдина впорядкована пара $(i, j) \in I \times J$ така, що

$$p \equiv i + j \mod n.$$

Нехай

$$V = \{i + j - n\colon i \in I, j \in J, i + j \geqslant n\}.$$

Для множини K цілих чисел означимо

$$a^K = \left\{a^k\colon k \in K\right\}.$$

Довести, що підмножина $X \subset \{a, b\}^*$, означена

$$X = a^I \left(ba^V\right)^* ba^J \cup a^n,$$

є кодом.

В. 2.8.12. *Код Моцкіна* (*the Motzkin code*) — це префіксний код M над алфавітом $A = \{a, b, c\}$, утворений словами $w \in A^*$ такими, що $|w|_a - |w|_b = 0$, але $|u|_a - |u|_b > 0$ для довільного власного непорожнього префікса слова w. Довести, що породжуючими рядами коду M і моноїда M^* є

$$f_M(t) = \frac{1 + t - \sqrt{1 - 2t - 3t^2}}{2} \qquad \text{і} \qquad f_{M^*}(t) = \frac{1 - t - \sqrt{1 - 2t - 3t^2}}{2t^2},$$

відповідно.

(*Підказка*: використайте той факт, що $M = \{c\} \cup P$, де $P = M \cap aA^*$ і $P = aM^*b$.)

В. 2.8.13. Нехай $A = \{a_1, \overline{a}_1, \ldots, a_n, \overline{a}_n\}$ і D — код Дика над алфавітом A. Довести, що

$$\pi(D) = \frac{1}{2n-1},$$

для однорідного розподілу Бернуллі на вільному моноїді A^*.

(*Підказка*: означимо $D_a = D \cap aA^*$ для $a \in A$ і доведемо, що $\underline{D_a} = a\left(\underline{D} - \underline{D_{\overline{a}}}\right)^* \overline{a}$.)

В. 2.8.14. Нехай $A = \{a, b, c\}$, $B = A \times A$ й $X = \{a, b^2\}$. Ототожнимо множину пар слів (x, y) квадрата вільного моноїда $A^* \times A^*$ однакових довжин з їх зображенням, як словом над B, тобто ототожнимо $(a_1a_2\cdots a_n, b_1b_2\cdots b_n)$ з $(a_1, b_1)(a_2, b_2)\cdots(a_n, b_n)$. Тут $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$. Довести, що множина

$$U = \{(x, y) \in X^* \times X^* \colon |x| = |y|\}$$

є вільним підмоноїдом вільного моноїда B^*, породженим біфіксним кодом Y (див. наприклад рис. 2.13). Використавши це, довести рівність

$$\sum_{n \geqslant 0} f_{n+1}^2 t^n = \frac{1-t}{(1+t)(1-3t+t^2)},$$

де f_n n-е *число Фібоначчі*, означене рекурентно $f_0 = 0$, $f_1 = 1$ і $f_{n+1} = f_n + f_{n-1}$ для натуральних чисел $n \geqslant 1$.

a	b	b	a	b	b	b	b	b	b	b	b	a							
b	b	b	b	a	b	b	b	b	a	a	b	b							

Рис. 2.13: Ця пара слів у множині U є добутком трьох слів з коду Y: $(a, b)(b^2, b^2)(a, b)$, $(b, a)(b^2, b^2)^2(b, a)$ і $(ba)(b, b)(a, b)$.

(*Підказка*: покажіть, що множина U породжується множиною $Y = (a, a) \cup (b^2, b^2) \cup (a, b)(b^2, b^2)^*(a, b) \cup (a, b)(b^2, b^2)^*(b^2, ba) \cup (b, a)(b^2, b^2)^*(b, a) \cup (b, a)(b^2, b^2)^*(ba, b^2)$.)

Підрозділ 2.5

В. 2.8.15. Нехай $A = \{a, b\}$. Довести, що підмножина $X = \{a^3, b, ab, ba^2, aba^2\}$ є повною у вільному моноїді A^* і, що X не мстить власної повної підмножини в A^*. Довести, що X не є кодом.

В. 2.8.16. Нехай M — моноїд і $\mathscr{F}$ — сім'я підмножин моноїда M, які є двобічними ідеалами в M або є порожньою.

(a) Довести, що існує топологія на моноїді M для якої $\mathscr{F}$ є сім'єю відкритих множин.

(b) Довести, що підмножина P з M щільна в M відносно цієї топології тоді і тільки тоді, коли $F(P) = M$, тобто якщо множина P є щільною у сенсі означення, наведеного в підрозділі 2.5.

В. 2.8.17. З позначеннями з твердження 2.5.25 і $V = A^* \setminus A^* y A^*$ довести послідовно, що

$$\begin{aligned}\underline{A}^* &= (\underline{V}y)^*\underline{V} = \\ &= (\underline{U}y)^*(\underline{X}^* y(\underline{U}y)^*)^*\underline{V}) = \\ &= (\underline{U}y)^*\underline{V} + (\underline{U}y)^*(\underline{Y})^* y(\underline{U}y)^*\underline{V}.\end{aligned}$$

(Використайте рівність $(\sigma+\tau)^* = \tau^*(\sigma\tau^*)^* = (\sigma^*\tau)^*\sigma^*$ для двох степеневих рядів σ і τ, що не мають постійних коефіцієнтів. Вивести безпосередньо з цих рівностей те, що Y є кодом і, що Y є повним кодом.

В. 2.8.18. Довести, що кожен худий код міститься в максимальному худому коді.

Підрозділ 2.6

В. 2.8.19. Нехай $\psi\colon A^* \to G$ — морфізм з вільного моноїда A^* на групу G, H — підгрупа в G та X – груповий код, визначений $X^* = \psi^{-1}(H)$. Доведіть, що код X нерозкладний тоді і тільки тоді, коли H — максимальна підгрупа в G.

В. 2.8.20. Доведіть, що будь-який код $X = \{x, y\}$ з двома елементами є композицією префіксного та суфіксного кодів.

В. 2.8.21. Доведіть, що код $X = \{a, aba, babaab\}$ не можна отримати як композицію префіксного та суфіксного кодів. Покажіть, що він міститься в скінченному максимальному коді Y, який визначається так:

$$\underline{Y} - 1 = (1 + b + baba(1 + a + b))(a + b - 1)(1 + ba).$$

Доведіть, що код Y належить до сім'ї скінченних максимальних кодів, визначених у вправі 14.8.7.

Нотатки до розділу 2

Коди часто називаються єдино розшифрованими кодами (англ. *uniquely decipherable codes*) або *UD-кодами*. Поняття коду виникло в теорії комунікацій, ініційованої Клодом Шенноном (Claude Elwood Shannon) наприкінці 1940-х років [189, 190]. Робота Шеннона представила нову наукову область з багатьма галузями та областями застосування. До них відносяться стиснення даних, виправлення помилок і криптографія. Можна знайти вичерпне описання цих тем в монографії [161]. Розробка теорії кодування призводить до детального вивчення кодів постійної довжини у зв'язку з проблемами виявлення та корекції помилок. Описання цих досліджень можна знайти в [142] або [129]. Спеціальний клас згорткових кодів, які мають тісний зв'язок зі скінченними автоматами, як представлено тут, розглядається детально в монографії [150]. Ранньою стандартною книгою з теорії інформації та комунікацій є монографія Еша [18–20].

Коди змінної довжини вперше глибоко досліджували Шютценбергер [178], а також Гілберт і Мур [76]. Напрям, що наслідує Шютценбергера, полягає в поєднанні теорії кодів з класичною некоммутативною алгеброю. Результати, представлені в цьому курсі, представляють цю точку зору. Раннюю оцінку про це можна знайти в статті

Ніва [154]. Оскільки коди є основою вільних підмоноїдів вільного моноїда, коди також пов'язані з основами вільних алгебр або вільних груп, оскільки вільна напівгрупа може бути вбудована в обидві структури. Для викладу вільних алгебр див. монографії Кона [54, 55]. Для введення в теорію вільних груп, див. монографію [7, 143, 144].

Взаємозв'язок між кодами змінної довжини і автоматами, а також декілька згаданих застосувань представлені в працях [25] і [26].

Поняття стійкого підмоноїда вперше з'являється в праці Шютценбергера [178], яка містить твердження 2.2.6. Аналогічний результат наводиться також у статтях Шевріна [12, 192], Кона [53] і Блюма [37]. Твердження 2.2.15 появляється в праці [201]. Теорема про дефект (теорема 2.2.16) доведена в декількох формулюваннях у працях [8, 60, 123, 145]. Деякі узагальнення цієї теореми обговорюються в [33] (див. також [134]). Подібні задачі розв'язувалися в [195].

Тест для кодів, наведений у підрозділі 2.3, опубліковано в [176], і він фактично відомий як *алгоритм Сардінаса і Паттерсона*. Доведення коректності цього мотивувало ряд статей: [6, 22, 137, 170]. Дизайн ефективного алгоритму описаний у [195] (див. також [17, 171]). Проблема перевірки того, чи є розпізнавана множина кодом, є особливим випадком відомої проблеми в теорії автоматів, а саме перевірка того, чи є раціональне вираз однозначним. Для цього питання існують стандартні процедури прийняття рішень (див. [15, 62]). Ці методи будуть використовуватися в розділі 4. Зв'язок між кодами та раціональними виразами було вказано в [45]. Характеристика таких кодів, кодування морфізму яких зберігає зіркову висоту раціональних виразів викладена в [88].

Результати підрозділу 2.4 добре відомі в теорії інформації. Наслідок 2.4.6 з його оберненим твердженням у теоремі 2.4.13 відомий як теорема Крафта-Макміллана (див. [151]).

Основні результати підрозділу 2.5 належать Шютценбергеру [178]. Наше викладення цього розділу є трохи більш загальним. Твердження 2.5.25 і теорема 2.5.24 взяті зі статті [61]. Вони відповіли на питання Рестіво зі статті [163]. Теорема 2.5.19 з'явилася в [38]. Приклад 2.5.7 — це особливий випадок конструкції, викладеної в статті [163], вправа 2.8.7 взята з [33], вправа 2.8.9 відома як лема Леві (див. [126]), вправа 2.8.10 взята зі статті [194].

Ми слідуємо праці [14] для побудови навантаженого дерева, оснащеного функцією відмови. Отримана структура називається машиною, яка розпізнає шаблони. Представлення алгоритму слідує опису, наведеним у праці [92] (див. також [47]). Ці документи містять транскрипцію до префіксів реалізації [17]. Аналогічна реалізація для статті [92] наведена в статтях [90, 91]. Реалізація, запропонована в статті Роде [171], дає ті ж межі, але й більше залучена. Вона заснована на дереві суфіксів, тобто на компактному дереві, що представляє всі суфікси скінченної множини слів.

Точна складність перевірки єдиного розшифрування покищо невідома, див. статті [69, 92] для обговорення та часткових результатів.

Основні властивості кодів також досліджені в структурах, які є більш загальними, ніж вільні моноїди, а саме *вільні частково комутативні моноїди*. Розглянемо симетричне відношення $I \subseteq A \times A$ над алфавітом A, вільний частково комутативний моноїд $M(A, I)$ є моноїд, породжений множиною A, стосовно тотожності $ab = ba$ для всіх пар $a, b \in I$. Дві задачі мають були досліджені. Перша, розглянемо гомоморфізм

$f\colon M \to N$ між вільними частково комутативними моноїдами M і N, чи можна визначити, чи морфізм f є ін'єкційним? Це виявилося нездійсненним навіть тоді, коли моноїд є вільним (див. огляд Діккерта та Мушолла [58] для деталей та посилань). Далі, коли для частково комутативних моноїдів M і N існує ін'єкційний морфізм з M в N? Ця проблема, відома як проблема кодування слідів, також виявилася нерозв'язаною в цілому [115]. Було також описано декілька конкретних випадків, коли ці проблеми розв'язуються.

Поняття коду також було узагальнене до кодів у символічних динамічних системах Ройтенауером [166], а потім Рестіво [164]. Нехай G — скінченний напрямлений мультиграф з ребрами, позначеними буквами з алфавіту A (множина міток бі-нескінченних шляхів утворює те, що називається *софічною системою, визначеною* графом G). Нехай $S(G)$ — множина скінченних слів, які є міткою шляху в графі G. Підмножина X з $S(G)$ є кодом над мультиграфом G, якщо будь-який елемент множини $S(G)$ має не більше однієї факторизації в елементах множини X. Таким чином, код у звичайному розумінні відповідає випадку, коли $S(G) = A^*$. Множина $X \subseteq S(G)$ є повною над мультиграфом G, якщо будь-який елемент $S(G)$ є фактором слова вільного моноїда X^*. У статті [30] показано, що будь-який максимальний код над мультиграфом G є повним над G. Це узагальнює теорему 2.5.5. Обернене твердження не вірно, навіть для скінченних кодів, а, отже, немає узагальнення теореми 2.5.13. Інші результати для кодів над графами наведені в працях [29, 166].

Інші структури, для яких розглядалося поняття кодів, включають дерева. Помічені дерева є природним узагальненням слів, для яких поняття автомата було введено набагато раніше. Коди дерев були введені Ніва в [155] і його дослідження було розвинуто, наприклад, у праці [147].

Коди Дика названі на честь німецького математика Вальтера фон Дика (Walther von Dyck) (див. також [32]). Коди Моцкіна вправи 2.8.12 названі на честь шляхів Моцкіна (див., наприклад, [83, 84]).

Комбінаторні доведення для вираження породжуючого ряду квадратів чисел Фібоначчі, наведених у вправі 2.8.14, наведено з праці Шапіро [191], див. також [196,197, приклад 4.7.14], і [67].

Вправа 2.8.21 взята з праці [59]. Вона є контрприкладом до гіпотези в [165], стверджуючи, що кожен трьох-словесний код складається з префіксних і суфіксних кодів. Невідомо, чи міститься в скінченному максимальному коді код з трьох слів.

Розділ 3

Префіксні коди

Безсумнівно, префіксні коди є найпростішими для побудови. Перевірка того, що дана множина слів є префіксним кодом є простою. Однак більшість цікавих проблем про коди можна звести до префіксних кодів. У цьому сенсі ці коди формують сім'ю моделей кодів: найчастіше простіше набувати інтуїцію про префіксні коди, ніж загальні коди. Проте ми можемо помітити, що міркування про префіксні коди часто працюють у загальному випадку.

З цієї причини ми тепер пропонуємо розділ про префіксні коди. У першому підрозділі ми коментуємо їх означення та даємо деякі елементарні властивості. Ми також показуємо, як намалювати зображення префіксного коду як дерева (буквальне зображення префіксних кодів).

У підрозділі 3.2 представлена конструкція автоматів, пов'язаних з префіксними кодами. Ці автомати є детермінованими, і ми побачимо в розділі 9, як поширити цю конструкцію на більш загальні коди.

Третій розділ стосується максимальних префіксних кодів. Наведено характеристики в термінах повноти. У підрозділі 3.4 представлені звичайні операції з префіксними кодами. Більшість з них легко інтерпретувати як операції на деревах.

Важлива сім'я префіксних кодів введена в підрозділі 3.5. Вони мають багато комбінаторних властивостей, які ілюструють раніше введені поняття. Синхронізація префіксних кодів визначена в підрозділі 3.6. Насправді, це поняття буде узагальнене для довільних кодів у розділі 9, де буде встановлено їх зв'язок з групами. Це робиться в підрозділі 3.7, де вводено поняття рекурентної події. Породжуючий ряд раціонального префіксного коду є $\mathbb{N}$-раціональним і задовольняє нерівність Крафта. Ми доводимо в підрозділі 3.8 обернене твердження.

3.1 Префіксні коди

Цей вступний розділ містить еквівалентні формулювання означення префіксного коду разом з описанням дерева, пов'язаного з префіксним кодом. Потім ми покажемо, як будь-який префіксний код індукує природним чином факторизацію вільного моноїда. Звичайно, всі результати в цьому розділі переносяться на суфіксні коди за допомогою операції взяття оберненого слова.

Нагадаємо, що для слів x і y позначимо через $x \leqslant y$ (відповідно $x < y$) те, що x — префікс (відповідно, власний префікс) слова y. Частковий порядок, який

визначається за відношенням $\leqslant$, називається *префіксним порядком*. Ми писатимемо, що $x \geqslant y$ (відп. $x > y$), якщо $y \leqslant x$ (відп. $y < x$). Два слова x і y є *непорівняльними* стосовно префіксного порядку, і будемо це записувати $x \bowtie y$, якщо слово x не є префіксом слова y, а також y не є префіксом слова x.

Підмножина X вільного моноїда A^* називається *префіксною*, якщо будь-яких дві різні слова в X є непорівняльними стосовно префіксного порядку. Якщо префіксна підмножина X містить порожнє слово 1, то $X = \{1\}$. В інших випадках множина X є кодом (твердження 2.1.9).

Приклад 3.1.1. Звичайне двійкове зображення натуральних чисел експоненціально більш лаконічне, ніж одинарне зображення, і тому краще для ефективності. Однак він не пристосований до подання послідовностей цілих чисел, оскільки він не є однозначно розшифрованим: наприклад, 11010 може представляти число 26, для послідовності 6,2 або послідовності $1, 2, 2$. *Код Еліа* (*Elias code*) додатнього цілого числа, що складається з його двійкового зображення, передує кількості нулів, рівних довжині цього представлення мінус один. Наприклад, код Еліа числа 26 дорівнює 000011010. Легко бачити, що множина кодувань Еліа додатних цілих чисел є префіксним кодом. Насправді, це те ж саме, як і код з прикладу 2.4.12, при цьому символ a замінений на 0 і символ b замінений на 1.

Зручно мати скорочення для власних префіксів (відповідно, власних суфіксів) слів множини X. Для цього ми використовуємо

$$XA^- = X(A^+)^{-1} \qquad \text{і} \qquad A^-X = (A^+)^{-1}X.$$

Отже, $u \in XA^-$ тоді і тільки тоді, коли $u < x$ для деякого $x \in X$. Симетрично $u \in XA^+$ тоді і тільки тоді, коли $u > x$ для деякого $x \in X$.

Існує ряд еквівалентних означень для множини бути префіксною, і всі вони будуть корисними. Множина X є префіксною тоді і тільки тоді, коли виконується одна з нижче перелічених умов:

(*i*) $X \cap XA^+ = \varnothing$;
(*ii*) $X \cap XA^- = \varnothing$;
(*iii*) множини XA^+, X і XA^- є попарно диз'юнктними;
(*iv*) якщо $x, xu \in X$, то $u = 1$;
(*v*) якщо $xu = x'u'$ з $x, x' \in X$, то $x = x'$ і $u = u'$.

Наступне твердження можна розглядати як описання способу побудови префіксних кодів. Воно також показує корисний взаємозв'язок між префіксними кодами та правими ідеалами вільного моноїда.

Твердження 3.1.2. *Для довільної підмножини Y вільного моноїда A^* множина $X = Y \setminus YA^+$ є префіксною. Більше того, $XA^* = YA^*$, тобто множини X і Y є одночасно порожніми або породжують один і той же правий ідеал, та X є мінімальною множиною з цією властивістю.*

Доведення. Нехай $X = Y \setminus YA^+$. З $X \subseteq Y$ випливає, що $XA^+ \subseteq YA^+$, а отже

$$X \cap XA^+ \subseteq X \cap YA^+ = \varnothing.$$

Звідси випливає, що множини X є префіксною. Далі, $XA^* \subseteq YA^*$. Для доведення оберненого включення припустимо, що $u \in Y$ нехай слово v є найкоротшим суфіксом слова u в Y. Тоді $v \in X$, а отже $u \in XA^*$. Отож, $Y \subseteq XA^*$ і $YA^* = XA^*$.

Нехай Z — мінімальна множина породжуючих елементів множини YA^*, тобто $ZA^* = YA^*$. Ми покажемо, що $X \subseteq Z$. Нехай справді x — слово в X. Тоді $x = zu$ для деяких $u \in A^*$ і $z \in Z$. Позаяк множина X також породжує множину YA^*, то $z = x'u'$ для деяких $x' \in X$, $u' \in A^*$. Таким чином, $x = zu = x'u'u$, і оскільки множина X є префіксною, то $uu' = 1$. Звідси випливає включення $X \subseteq Z$, а отже $X = Z$. □

Множина $X = Y \backslash YA^+$ називається *початковою частиною* множини Y, або також *базою правого ідеала* YA^*.

Наступні твердження описують природні бієкції між таким сім'ями підмножин вільного моноїда A^*:

(1) сім'я $\mathfrak{X}$ префіксних підмножин;
(2) сім'я $\mathfrak{I}$ складається з правих ідеалів вільного моноїда A^* разом з порожньою множиною;
(3) сім'я $\mathfrak{R}$ префіксно замкнених підмножин.

Ми описуємо тут ці три бієкції (див. рис. 3.1).

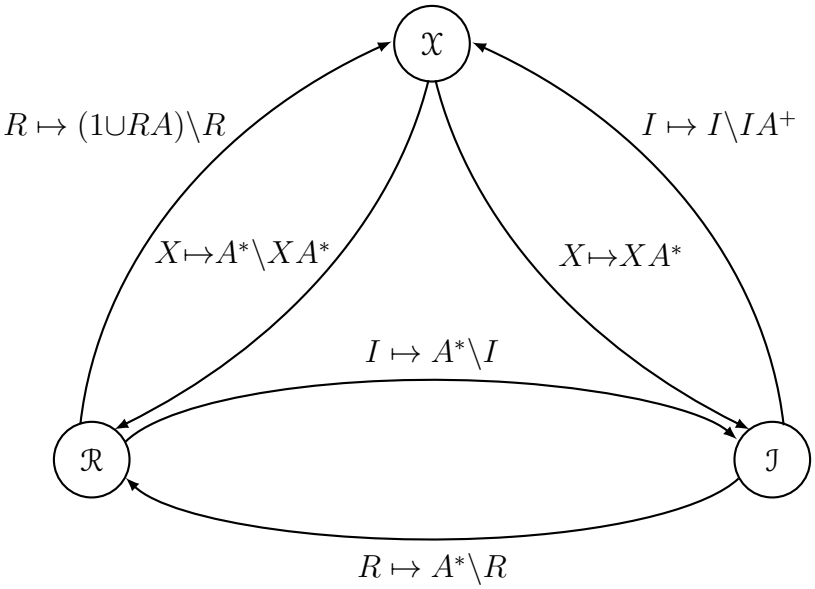


Рис. 3.1: Бієкції між трьома сім'ями $\mathfrak{X}$, $\mathfrak{I}$ і $\mathfrak{R}$

Твердження 3.1.3. *Справджуються такі бієкції.*

(*i*) *Відображення* $X \mapsto XA^*$ *є бієкцією зі сім'ї* $\mathfrak{X}$ *на* $\mathfrak{I}$, *а відображення*

$$I \mapsto I \setminus IA^+$$

є до нього оберненою бієкцією з $\mathfrak{I}$ *на* $\mathfrak{X}$.

(*ii*) *Операція теоретико множинного доповнення відображає бієктивно сім'ю* $\mathcal{R}$ *на* $\mathcal{I}$.

(*iii*) *Відображення*

$$X \mapsto A^* \setminus XA^*$$

є бієкцією зі сім'ї $\mathcal{X}$ *на* $\mathcal{R}$, *а відображення*

$$R \mapsto (\{1\} \cup RA) \setminus R$$

є до нього оберненою бієкцією з $\mathcal{R}$ *на* $\mathcal{X}$.

Доведення. (*i*) Для довільної непорожньої підмножини X вільного моноїда A^*, множина XA^* є правим ідеалом в A^*. Навпаки, для довільної підмножини I вільного моноїда A^*, множина $X = I \setminus IA^+$ є префіксною. Справді, власний префікс елемента множини X не є елементом множини I, а отже не є елементом множини X. Отож, два означені вище відображення є коректно визначеними. Тепер ми покажемо, що вони є взаємно оберненими.

Нехай X — префіксна підмножина вільного моноїда A^* і нехай $I = XA^*$. Тоді $X = I \setminus IA^+$. Справді

$$I \setminus IA^+ = XA^* \setminus XA^+ = (X \cup XA^+) \setminus XA^+ = X \setminus XA^+ = X,$$

оскільки $X \cap XA^+ = \varnothing$.

На завершенні, нехай I — правий ідеал вільного моноїда A^* та $X = I \setminus IA^+$. За твердженням 3.1.2 отримуємо, що $XA^* = IA^* = I$.

(*ii*) Якщо слово w не є елементом правого ідеала I, то жоден його префікс не є елементом в I, також. Отож, множина $R = A^* \setminus I$ є префіксно замкненою. Навпаки, доповнення до префіксно замкненої множини є правим ідеалом вільного моноїда A^*, або є порожньою.

(*iii*) Наше відображення відображає $\varnothing$ в A^*. Для непорожнього префіксного кода X бієкція з п. (*i*) відображає його в правий ідеал $I = XA^* \neq A^*$. Операція теоретико множинного доповнення відображає код X в непорожню префіксно замкнену множину $R = A^* \setminus I = A^* \setminus XA^*$ за твердженням (*ii*). Звідси випливає перше твердження.

За твердженнями (*i*) і (*ii*) обернене до цього відображення відображає правий ідеал R на множину $X = I \setminus IA^+$ з $I = A^* \setminus R = XA^*$. Нехай $Y = RA \setminus R$. Слово x множини X не є елементом в R. Покладемо $x = ua$ з $u \in A^*$ і $a \in A$. Оскільки слово u не є елементом в I, то воно є R. Отож, слово x є елементом в Y. Навпаки, нехай y — слово в Y. Тоді y не є елементом в R, а отже y є елементом в I. Позаяк $y \in RA$, то кожен власний префікс слова y є в R. Отож, слово y не має власного префікса в I, тобто маємо $y \notin IA^+$. Звідси випливає, що $y \in X$. □

Зауважимо, що ці бієкції, що мають майже ті ж доведення, виконується в будь-якій впорядкованій множині.

Приклад 3.1.4. Нехай $A = \{a, b\}$ і $Y = A^*aA^*$ — множина слів, які містять щонайменше одну літеру a. Тоді

$$X = Y \setminus YA^+ = b^*a.$$

Приклад 3.1.5. Нехай $A = \{a, b\}$. Множина $I = A^*abA^*$ — множина слів, які містять множник ab, є правим ідеалом. Доповнення до I є префіксно замкненою множиною $R = b^*a^*$. Префіксний код $X = I \setminus IA^+$ збігається з $X = b^*a^*ab$. Цей код, як і попередній належить до сім'ї семафорних кодів, які вивчаються в підрозділі 3.5.

Вище згадані бієкції мають наступний аналог як відношення між формальними рядами.

Твердження 3.1.6. *Нехай X — префіксний код над алфавітом A і $R = A^* \setminus XA^*$. Тоді*

$$\underline{X} - 1 = \underline{R}(\underline{A} - 1) \qquad і \qquad \underline{A}^* = \underline{X}^*\underline{R}. \tag{3.1}$$

Доведення. Ми спочатку покажемо, що ці два рівності є еквівалентними. За твердженням 2.6.1 маємо, що $\underline{X}^* = (1 - \underline{X})^{-1}$. З цієї рівності та з рівності $(1 - \underline{A})^{-1} = \underline{A}^*$ отримуємо, домноживши рівність $1 - \underline{X} = \underline{R}(1 - \underline{A})$ справа на $\underline{X}^*$ і зліва на $\underline{A}^*$, рівність $\underline{A}^* = \underline{X}^*\underline{R}$. Обернені операції, що домноживши зліва на $1 - \underline{X}$ і справа на $1 - \underline{A}$, отримуємо знову перше рівняння.

Добуток X і A^* є однозначним за властивістю (v) префіксних кодів, яка перелічена вище. Таким чином, $\underline{XA^*} = \underline{X}\ \underline{A}^*$, і

$$\underline{R} = \underline{A^* \setminus XA^*} = \underline{A}^* - \underline{X}\ \underline{A}^* = (1 - \underline{X})\underline{A}^*.$$

Домноживши обидві сторони даної рівності на $1 - \underline{A}$ справа, отримуємо

$$\underline{R}(1 - \underline{A}) = 1 - \underline{X},$$

що завершує доведення формули. □

Звернемо увагу на наступні комбінаторні інтерпретації формул (3.1). Перша з них може бути переписана як

$$\underline{R}\ \underline{A} + 1 = \underline{X} + \underline{R}$$

і стверджує, що слово в R, за яким слідує буква, або в R, або в X, і що кожне слово в X складається зі слова в R, за яким йде буква. Друга формула стверджує, що кожне слово $w \in A^*$ допускає єдину факторизацію

$$w = x_1x_2 \cdots x_nu, \qquad x_1, \ldots, x_n \in X, \quad u \in R.$$

Приклад 3.1.7. Нехай $A = \{a, b\}$ і $X = a^*b$ як в прикладі 3.1.4. Тоді $R = a^*$. З твердження 3.1.6 випливає, що

$$\underline{X} - 1 = \underline{R}(\underline{A} - 1) = a^*(a + b - 1) = a^*b - 1.$$

Ми виокремлюємо наступний наслідок, який також міститься в твердженні 3.1.3 для зручності посилання.

Наслідок 3.1.8. *Нехай X і Y — префіксні підмножини вільного моноїда A^*. Якщо $XA^* = YA^*$, то $X = Y$.*

Зауважимо, що існує пряме доведення рядами, оскільки з $XA^* = YA^*$ випливає рівність $\underline{X}\,\underline{A}^* = \underline{Y}\,\underline{A}^*$, з якої випливає рівність, спрощуванням вільного моноїда $\underline{A}^*$.

Тепер наведемо корисне графічне представлення префіксних кодів. Вона полягає в співставленні дерева з кожним префіксним кодом так, що листя[1] дерева представляють слова в коді.

Спочатку, ми пов'язуємо нескінченне дерево з множиною A^* всіх слів над алфавітом A наступним чином. Алфавіт є лінійно впорядкованою множиною, а слова однакової довжини впорядковуються лексикографічно. Кожна вершина дерева представляє слово в A^*. Слова меншої довжини розташовані зліва від слів більшої довжини, а слова рівної довжини розташовані вертикально відповідно до лексичного впорядкування. Існує ребро від слова u до слова v тоді і тільки тоді, коли $v = ua$ для деякої літери $a \in A$. Дерево, отримане таким чином, є *літерним зображенням* вільного моноїда A^*, який також називається *графом Келі* вільного моноїда A^* (див. рис. 3.2).

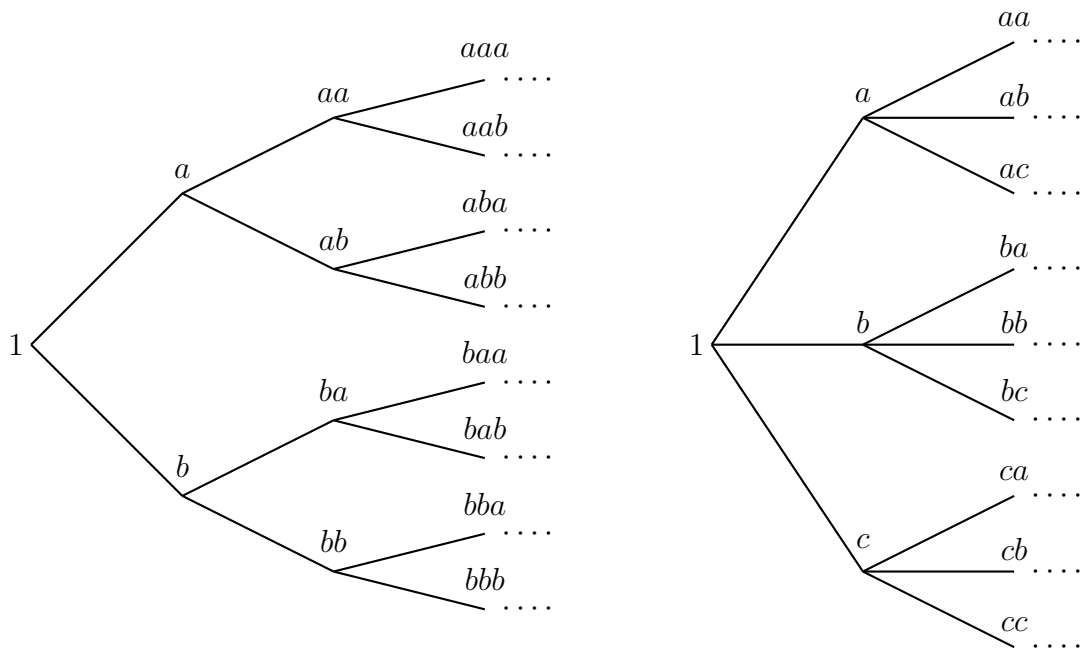


Рис. 3.2: Літерні зображення вільних моноїдів $\{a, b\}^*$ і $\{a, b, c\}^*$

До даної підмножини X вільного моноїда A^* ми пов'язуємо піддерево літерального зображення вільного моноїда A^* наступним чином. Ми зберігаємо тільки вузли, які відповідають словам в множині X і всі вузли на шляхах від кореня до цих вузлів. Вузли, що відповідають словам у множині X, позначаються при необхідності. Дерево, отримане таким чином називається *літерним зображенням* множини X. Рис. 3.3 і 3.4 дають декілька прикладів літерних зображень множин.

[1] *Листком* некореневого дерева називається його вершина степеня 1.

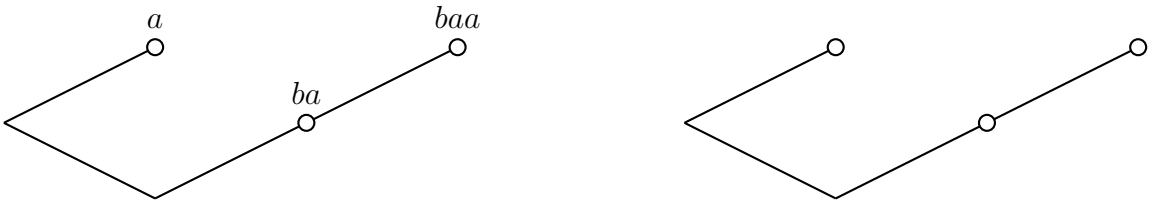


Рис. 3.3: Літерні зображення множини $X = \{a, ba, baa\}$ з явним маркуванням і з неявним маркуванням

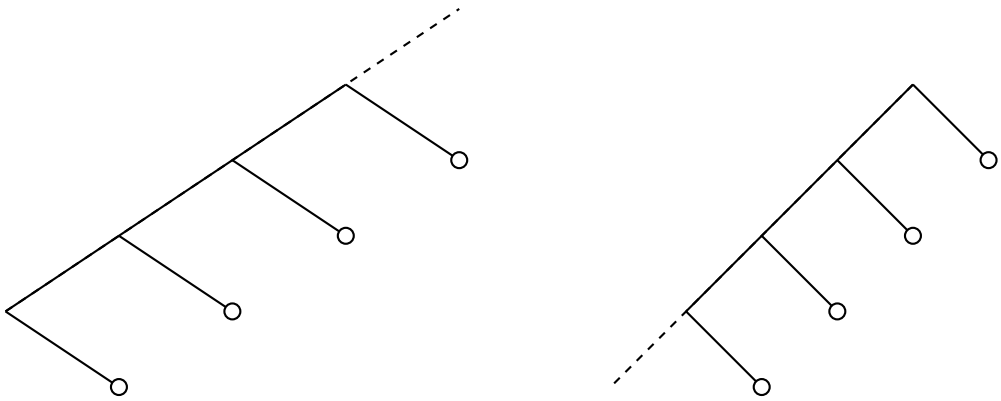


Рис. 3.4: Літерні зображення множини $X = a^*b$. Ліворуч подання зліва направо, а праворуч малюнок зверху вниз.

Альтернативне графічне зображення малює дерево зверху вниз, а не зліва направо. У цьому випадку слова рівної довжини розташовуються горизонтально зліва направо відповідно до їх лексикографічного порядку. Див. рис. 3.4 для прикладу.

Легко бачити, що код X є префіксним тоді і тільки тоді, коли в літерному зображенні множини X, вузли, які відповідають словам в коді X, є всі листками дерева.

Приклад 3.1.9. Код Еліа означено в прикладі 3.1.1, а його графічне зображення на рис. 3.5.

Перевага літерного зображення, порівняно з простим перерахуванням, полягає в легкому зчитуванні. На відміну від того, що може здатися, воно дозволяє компактне зображення достатньо великих кодів (див. рис. 3.6).

Приклад 3.1.10. Нехай $X = \{a, baa, bab, bb\}$ — код над алфавітом $A = \{a, b\}$ зображено на рис. 3.7. Тут

$$R = \{1, b, ba\} = XA^- \qquad \text{і} \qquad \underline{X} - 1 = (1 + b + ba)(\underline{A} - 1).$$

Рівність між R і XA^- описує максимальні префіксні коди, як це буде показано в підрозділі 3.3.

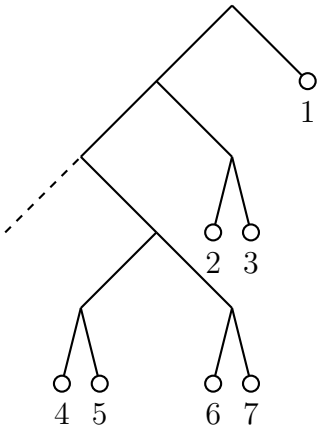


Рис. 3.5: Код Еліа

Приклад 3.1.11. Нехай $X = (b^2)^*\{a^2b, ba\}$ — код над алфавітом $A = \{a, b\}$ зображено на рис. 3.8. Тут $R = R_1 \cup R_2$, де

$$R_1 = XA^- = (b^2)^*(\{1\} \cup \{a\} \cup \{b\} \cup \{a^2\})$$

— множина власних префіксів множини X і

$$R_2 = XA^+ - X - XA^- = (b^2)^*(abA^* \cup a^3A^*).$$

Отож, з (3.1) випливає, що

$$\underline{X} - 1 = (b^2)^*(1 + a + b + a^2 + ab\underline{A}^* + a^3\underline{A}^*)(\underline{A} - 1).$$

3.2 Автомати префіксних кодів

Літерне зображення дає простий метод для перевірки того, чи є слово w елементом моноїда X^* для деякого фіксованого префікса коду X. Достатньо рухатися по шляху, що починається від кореня дерева через послідовні літери слова w. Кожен раз, коли досягається листок, то відповідний множник слова w розпадається і процедура перезапускається, тобто починається з початку.

Ми розглядатимемо декілька автоматів, отриманих з літерного зображення, і поставимо їм у відповідність мінімальні автомати. Окремий випадок префіксних кодів цікавий сам по собі, оскільки він є джерелом більшості загальних результатів розділу 9.

Нагадаємо (див. розділ 1), що для будь-якої підмножини $X \subseteq A^*$ через $\mathcal{A}(X)$ позначається мінімальний детермінований автомат, що розпізнає множину X.

Твердження 3.2.1. *Нехай $A \neq \varnothing$ і X — підмножина вільного моноїда A^*. Тоді такі умови є еквівалентними:*

(*i*) *множина X є префіксною;*

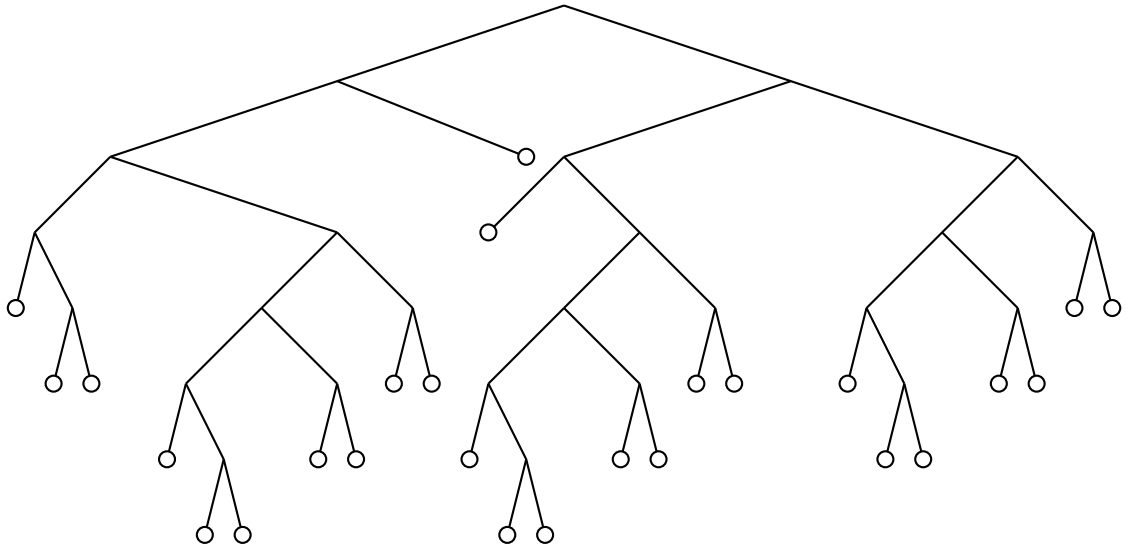


Рис. 3.6: Код з 26 елементами

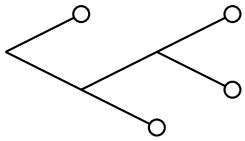


Рис. 3.7: Префіксний код $\{a, baa, bab, bb\}$

(*ii*) *мінімальний автомат* $\mathcal{A}(X)$ *є порожнім, або має єдиний кінцевий стан* t *і* $t \cdot A = \varnothing$*;*

(*iii*) *існує детермінований автомат* $\mathcal{A} = (Q, i, T)$*, який розпізнає множину* X *такий, що* $T \cdot A = \varnothing$*.*

Доведення. $(i) \Longrightarrow (ii)$ Припустимо, що множина X є непорожньою. Покладемо $\mathcal{A}(X) = (Q, i, T)$. Спочатку, ми стверджуємо, що

$$\{w \in A^* \colon q \cdot w \in T\} = \{1\}$$

для $q \in T$. Справді, нехай $x \in X$ і $w \in A^*$ — слова такі, що $i \cdot x = q$ (пам'ятаємо, що $q \in T$) і $q \cdot w \in T$. Тоді $xw \in X$, звідки випливає, що $w = 1$. Це завершує доведення нашого твердження.

Таким чином, два кінцевих стани не є розділеними, і з мінімальності автомата $\mathcal{A}(X)$ випливає, що $\mathcal{A}(X)$ має тільки один кінцевий стан, скажімо t. Припустимо, що $t \cdot A \neq \varnothing$, і $t \cdot a = p$ для деякої літери $a \in A$ та деякого стану p. Оскільки стан p є кодоступним, то $p \cdot v = t$ для деякого слова $v \in A^*$. Отож, $t \cdot av = t$, звідки випливає, що $av = 1$, протиріччя.

Імплікація $(ii) \Longrightarrow (iii)$ очевидна.

$(iii) \Longrightarrow (i)$ З $T \cdot A = \varnothing$ випливає, що $T \cdot A^+ = \varnothing$. Отож, якщо $x \in X$ і $w \in A^+$, то $i \cdot xw = \varnothing$ і $xw \notin X$. Таким чином, отримуємо, що $X \cap XA^+ = \varnothing$. □

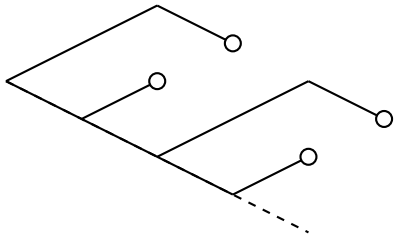


Рис. 3.8: Префіксний код $(b^2)^*\{a^2b, ba\}$

Легко побудувати автомат для префіксного коду, починаючи з літерного зображення. Цей автомат, який називають *літерним автоматом* префіксного коду X, є детермінований автомат

$$\mathcal{A} = (XA^- \cup X, 1, X)$$

і визначається за формулою

$$u \cdot a = \begin{cases} ua, & \text{якщо } ua \in XA^- \cup X; \\ \varnothing, & \text{в протилежному випадку.} \end{cases}$$

Позаяк множина $XA^- \cup X$ є префіксно замкненою, то відразу бачимо, що $1 \cdot u \in X$ тоді і тільки тоді, коли $u \in X$, тобто $L(\mathcal{A}) = X$. Наочне зображення літерного автомата відповідає, звичайно, літерному зображенню кода.

Приклад 3.2.2. Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$. Код X має літерне зображення, яке зображене на рис. 3.9 і літерний автомат, який зображений

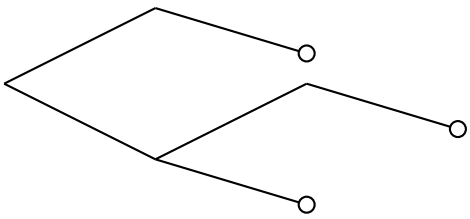


Рис. 3.9: Літерне зображення кода $\{ab, bab, bb\}$

на рис. 3.10.

Літерний автомат $\mathcal{A}$ префіксного коду X є впорядкованим автоматом, але не є мінімальним в цілому. Для нескінченних кодів він завжди є нескінченним. Розглянемо два стани автомата $\mathcal{A}$. Еквівалентно розглянути два префікси слів з множини X, скажемо u і v, що входять в ці стани. Ці два стани є невідокремлюваними тоді і тільки тоді, коли

$$u^{-1}X = v^{-1}X.$$

Зауважимо, що ця рівність означає на літерному зображенні множини X маємо, що два піддерева з коренями u і v, відповідно, є однаковими. Це забезпечує легку процедуру для обчислення мінімального автомата: по-перше, всі кінцеві стани помічені,

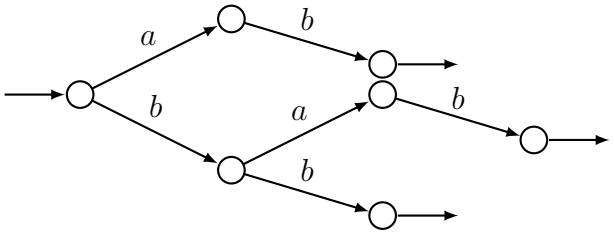


Рис. 3.10: Літерний автомат кода $\{ab, bab, bb\}$

скажімо, за допомогою мітки 0. Якщо всі мітки до i визначені, ми розглядаємо такі піддерева такі, що всі вузли, крім коренів, позначені. Тоді корені помічені однаково, якщо (помічені) піддерева є ізоморфними. Взявши як мітки як стани, отримуємо мінімальний автомат. Процедура описана в прикладах 3.2.2, 3.2.3, 3.2.4 і 3.2.5.

Приклад 3.2.3. Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$ (див. приклад 3.2.2). Зважаючи на твердження 3.2.1, кінцеві стани дерева є невідокремлюваними. Стани a та ba є невідокремлюваними, оскільки $a^{-1}X = (ba)^{-1}X = b$. Інших відношень не існує. Таким чином, мінімальний автомат наведено на рис. 3.11.

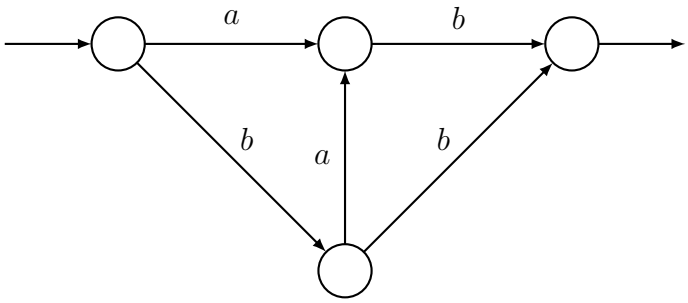


Рис. 3.11: Мінімальний автомат кода $X = \{ab, bab, bb\}$

Приклад 3.2.4. Літерний автомат множини $X = (b^2)^*(a^2b \cup ba)$ зображено на рис. 3.12. Очевидно, що кінцеві стани є еквівалентними, а також такими є попередники кінцевих станів і їх попередників. На головній діагоналі, однак, стани є еквівалентними лише з кроком 2. Це дає мінімальний автомат з рис. 3.13.

Приклад 3.2.5. На рис. 3.14 процедура маркування була проведена для 26 елементного кода на рис. 3.6. Це дає наступний мінімальний автомат з рис. 3.15.

Розглянемо тепер автомати, що розпізнають підмоноїд X^* породжений префіксним кодом X. Нагадаємо, що моноїд X^* є унітарним справа (див. твердження 2.2.9). Твердження 3.2.6 є аналогом твердження 3.2.1.

Твердження 3.2.6. *Нехай $A \neq \varnothing$ і P — підмножина вільного моноїда A^*. Такі умови є еквівалентними:*

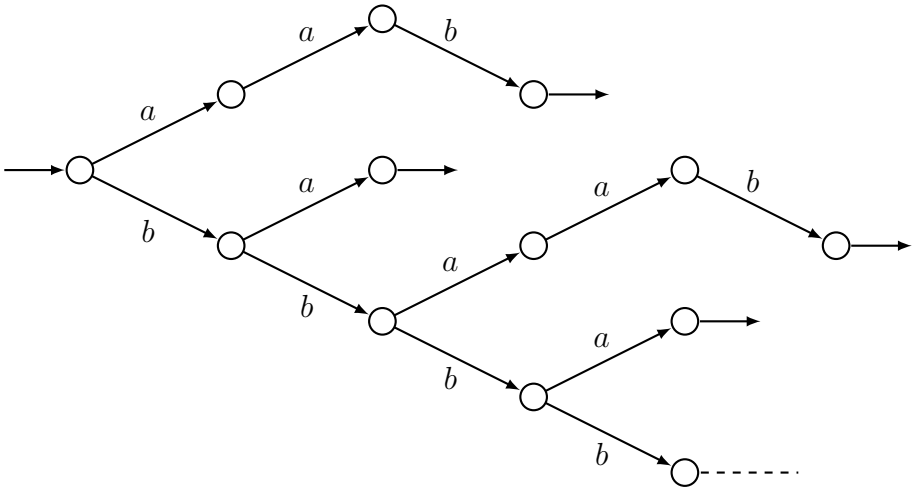


Рис. 3.12: Літерний автомат префіксного кода $X = (b^2)^*(a^2b \cup ba)$

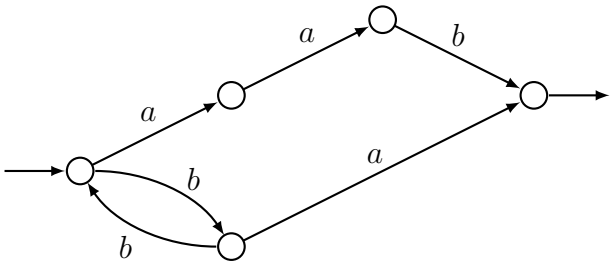


Рис. 3.13: Мінімальний автомат до рис. 3.12

(*i*) P — *унітарний справа підмоноїд;*

(*ii*) *мінімальний автомат* $\mathcal{A}(P)$ *має єдиний кінцевий стан, а саме початковий стан;*

(*iii*) *існує детермінований автомат, що розпізнає моноїд , маючи початковий стан як єдиний кінцевий стан.*

Доведення. $(i) \Longrightarrow (ii)$ Стани в автоматі $\mathcal{A}(P)$ є непорожніми множинами $u^{-1}P$, для $u \in A^*$. Далі, якщо $u \in P$, то $u^{-1}P = P$, оскільки $uv \in P$ тоді і лише тоді, коли $v \in P$. Таким чином, існує лише один кінцевий стан в автоматі $\mathcal{A}(P)$, а саме моноїд P, який також є початковим станом.

Імплікація $(ii) \Longrightarrow (iii)$ є очевидною.

$(iii) \Longrightarrow (i)$ Нехай $\mathcal{A} = (Q, i, i)$ — автомат, що розпізнає множину P. Тоді множина P є підмоноїдом, оскільки кінцевий стан і початковий стан збігаються. Далі, нехай $u, uv \in P$. Тоді $i \cdot u = i$ та $i \cdot uv = i$. Звідси випливає, що $i \cdot v = i$, оскільки автомат $\mathcal{A} = (Q, i, i)$ є детермінованим. Таким чином, отримуємо $v \in P$, звідки випливає, що моноїд P є унітарним справа. □

Нехай $\mathcal{A} = (Q, i, T)$ — довільний детермінований автомат над непорожнім алфа-

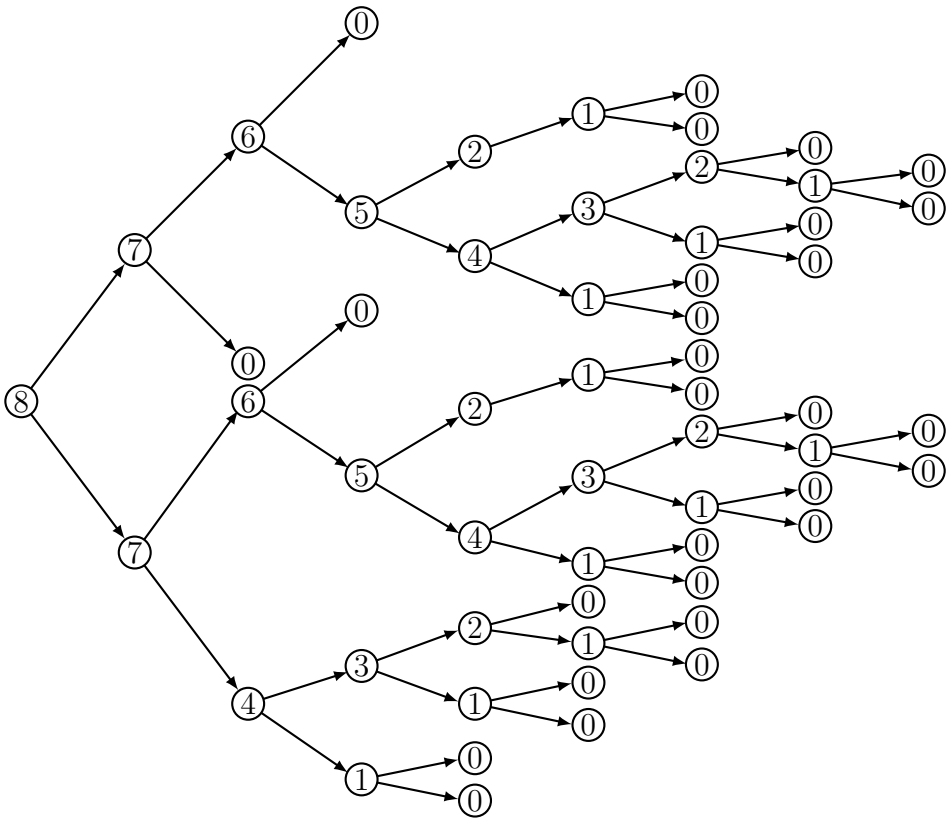


Рис. 3.14: Обчислення мінімального автомата

вітом A. *Стабілізатором* стану q автомата $\mathcal{A}$ називається підмоноїд

$$\mathrm{Stab}(q) = \{w \in A^* \colon q \cdot w = q\}$$

вільного моноїда A^*.

Безпосередньо з доведення твердження 3.2.6 випливає

Твердження 3.2.7. *Стабілізатор стану детермінованого автомату $\mathcal{A} = (Q, i, T)$ над непорожнім алфавітом A є унітарним справа деякого підмоноїда вільного моноїда A^*. Кожен унітарний справа деякого підмоноїд є стабілізатором стану деякого детермінованого автомата.*

Це твердження показує важливість унітарних справа підмоноїдів і префіксних кодів в теорії автоматів. Твердження 3.2.8 представляє метод виведення мінімального автомата $\mathcal{A}(X^*)$ вільного моноїда X^* з мінімального автомата $\mathcal{A}(X)$ префіксного коду X.

Твердження 3.2.8. *Нехай $A \neq \varnothing$, X — непорожній префіксний код над алфавітом A і $\mathcal{A}(X) = (Q, i, t)$ — мінімальний автомат коду X. Тоді мінімальним автоматом вільного моноїда X^* є автомат $\mathcal{A}(X^*)$, який визначається так:*

$$(Q, t, t), \qquad \textit{якщо } \mathrm{Stab}(i) \neq 1; \tag{3.2}$$

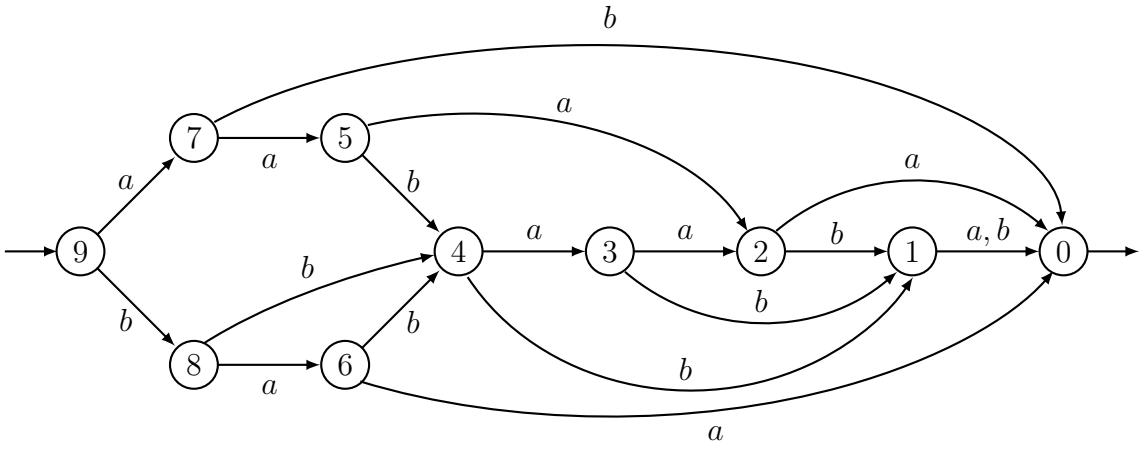


Рис. 3.15: Мінімальний автомат

$$(Q\backslash\{i\}, t, t), \quad \textit{якщо } \mathrm{Stab}(i) = 1, \tag{3.3}$$

і дія автомата $\mathcal{A}(X^*)$*, яка позначається* $\circ$*, визначається так:*

$$q \circ a = q \cdot a, \qquad \textit{для } q \neq t; \tag{3.4}$$

$$t \circ a = i \cdot a. \tag{3.5}$$

Доведення. Нехай $\mathcal{B} = (Q, t, t)$ — автомат отриманий за автомату $\mathcal{A}(X)$, в якому визначена дія $\circ$ за формулами (3.4) і (3.5). Тоді очевидно, що

$$L(\mathcal{B}) = \{w \colon t \circ w = t\} = X^*.$$

Перевіримо, що автомат $\mathcal{B}$ є зведеним. Для цього розглянемо два різні стани p і q. Оскільки автомат $\mathcal{A}(X)$ — зведений, то існує слово u у вільному моноїді A^*, що розділяє стани p і q, тобто таке, що, скажімо

$$p \cdot u = t \qquad \text{і} \qquad q \cdot u \neq t. \tag{3.6}$$

Звідси випливає, що $p \circ u = t$, а також $p \circ v \neq t$ для всіх слів $v < u$. Якщо $q \circ u \neq t$, то слово u відокремлює слова p і q також автоматом $\mathcal{B}$. В іншому випадку існує найменший префікс v слова u такий, що $q \circ v = t$. Для цього слова v маємо, що $q \circ v = t$. Врахувавши (3.6), отримуємо $v \neq U$, а отже $v < u$. Але тоді $q \circ u = t$ і $p \circ v \neq t$, і це доводить, що слова p і q відокремлюються словом v.

Кожне стан в автоматі $\mathcal{B}$ є доступним, оскільки він є випадком в автоматі $\mathcal{A}(X)$. З того, що $1 \neq X$ отримуємо $i \neq t$. Стан i є доступним в автоматі $\mathcal{B}$ тоді і тільки тоді, коли множина $\{w \colon t \circ w = i\}$ є непорожньою, отже, тоді і тільки тоді, коли $\mathrm{Stab}(i) \neq 1$. В іншому випадку доступною частиною автомата $\mathcal{B}$ є його звуження на множину $Q \setminus \{i\}$. □

Автомат $\mathcal{A}(X^*)$ завжди має вигляд зображений формулою (3.3), якщо префіксний код X є скінченним. У цьому випадку автомат $\mathcal{A}(X^*)$ отриманий шляхом ототожнення початкового та кінцевого станів. Для описання загального випадку див. вправу 3.10.4.

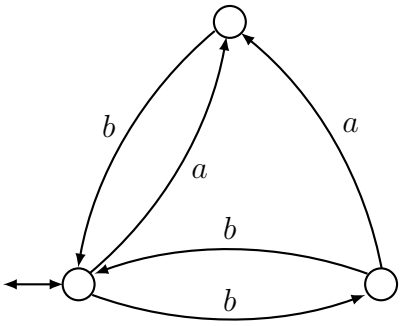


Рис. 3.16: Мінімальний автомат вільного моноїда X^*, для $X = \{ab, bab, bb\}$

Приклад 3.2.9. Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$ (див. приклад 3.2.2). Мінімальний автомат вільного моноїда X^* зображено на рис. 3.16. Код X є скінченним і автомат $\mathcal{A}(X^*)$ визначається формулою (3.3).

Приклад 3.2.10. Нехай $X = (b^2)^*(a^2b \cup ba)$ (див. приклад 3.2.4). Автомат $\mathcal{A}(X^*)$ отримується без видалення початковий стану автомата $\mathcal{A}(X)$ і задається формулою (3.2) (див. рис. 3.17).

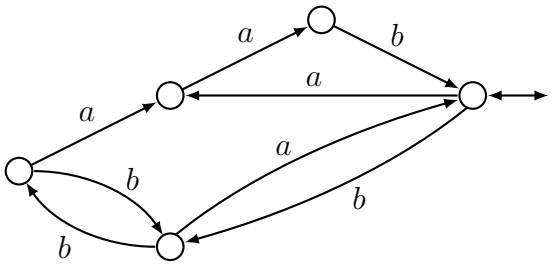


Рис. 3.17: Мінімальний автомат вільного моноїда X^*, для $X = (b^2)^*(a^2b \cup ba)$

Приклад 3.2.11. Розглянемо код $X = ba^*b$ над алфавітом $A = \{a, b\}$. Його мінімальний автомат зображено на рис. 3.18. Стабілізатор початкового стану – це тільки

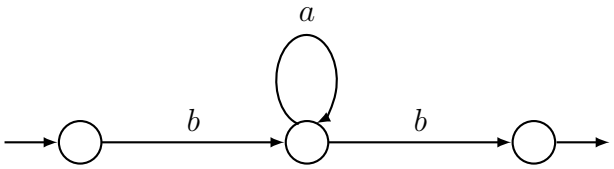


Рис. 3.18: Мінімальний автомат коду $X = ba^*b$

порожнє слово 1. Мінімальний автомат $\mathcal{A}(X^*)$, наведений на рис. 3.19, і він отримується з формули (3.3).

Конструкція, аналогічна конструкції твердження 3.2.8, дозволяє визначити *літерний автомат* вільного моноїда X^* для префіксного коду X. Це є автомат

$$\mathcal{A} = (XA^-, 1, 1),$$

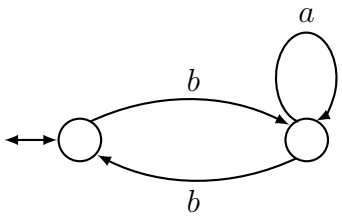


Рис. 3.19: Мінімальний автомат вільного моноїда X^*, для $X = ba^*b$

станами якого є власні префікси слів коду X, і з дією, яка визначається так:

$$u \cdot a = \begin{cases} ua, & \text{якщо } ua \in XA^-; \\ 1, & \text{якщо } ua \in X; \\ \varnothing, & \text{в інших випадках.} \end{cases} \tag{3.7}$$

Цей автомат отримують з літерного автомата коду X, ототожнюючи всі кінцеві стани літерного автомата коду X з початковим станом 1. З побудови безпосередньо випливає, що цей автомат розпізнає вільний моноїд X^*.

Наступною властивістю раціональних префіксних кодів ми скористаємося пізніше (див. розділ 6.6).

Твердження 3.2.12. *Для кожного раціонального префіксного коду X над алфавітом A існує ціле число N таке, що довжина довільної строго зростаючої послідовності суфіксів слів з коду X стосовно префіксного порядку обмежена числом N.*

Доведення. Нехай $\mathcal{A} = (Q, i, T)$ — скінченний автомат з N станами, що розпізнає код X, і припускаємо, що існує послідовність $N+1$ суфіксів $s_0, \ldots, s_N$ слів множини X таких, що кожне слово s_j є власним префіксом слова s_{j+1}. Кожне слово s_j — це мітка шляху від деякого стану q_j до кінцевого стану t_j в автоматі $\mathcal{A}$. Більше того, для кожного індексу j існує слово p_j, яке є міткою шляху від початкового стану i до стану q_j. Зауважимо, що слово $p_j s_j$ є елементом коду X для кожного індексу j. За означенням числа N існують числа j, k з $0 \leqslant j < k \leqslant N$ такі, що $q_j = q_k$. Таким чином, отримуємо, що слова $p_j s_j$ і $p_j s_k$ є елементами коду X, слово $p_j s_j$ є власним префіксом слова $p_j s_k$, а це суперечить тому, що множина X є префіксною. □

Приклад 3.2.13. Розглянемо префіксний код $X = A^*aba \setminus A^+aba$ над алфавітом $A = \{a, b\}$. Послідовностями максимальної довжини строго зростаючих послідовностей суфіксів, стосовно префіксного порядку, є $\varepsilon, a, a^n aba$ з $n \geqslant 1$. Іншою послідовністю є ε, ba.

3.3 Максимальні префіксні коди

Префіксна підмножина X вільного моноїда A^* називається *максимальною*, якщо вона не є власною підмножиною будь-якої іншої префіксної підмножини в A^*, тобто якщо $X \subset Y \subset A^*$ і Y — префіксна підмножина, то $X = Y$.

Що стосується максимальних кодів, посилання на основний алфавіт необхідно для того, щоб означення було коректним.

Множина $\{1\}$ є максимальною префіксною множиною. Кожна інша максимальна префіксна множина — це код. Максимальний префіксний код є завжди максимальним префіксним. Обренене твердження не виконується: існують максимальні префіксні коди, які не є максимальними як коди. Проте, за слабких припущень, а саме для тонких кодів, ми покажемо, що максимальні префіксні коди є максимальними кодами.

Дослідження максимальних префіксних кодів використовує зліва-на-право орієнтовану версію щільних і повних кодів.

Нехай M — моноїд і N — підмножина в M. Елемент $m \in M$ називається *поповнювальним справа* в N, якщо $mw \in N$ для деякого елемента w з M. Це еквівалентно тому, що множина N перетинає правий ідеал mM. Підмножина N називається *щільною справа*, якщо кожен елемент $m \in M$ є поповнювальним справа в N тобто, якщо N перетинає всі праві ідеали моноїда M. Множина N є *повною справа*, якщо підмоноїд породжений множиною N є щільним справа. Множина N називається *худою справа*, якщо вона не є щільною справа. Звичайно, всі ці означення мають зміст, якщо в них "правий" замінити "лівим".

Наступі імплікації виконуються для довільної непорожньої підмножини N моноїда M:

$$\begin{aligned} N\text{-щільна справа} &\implies N\text{-щільна;} \\ N\text{-повна справа} &\implies N\text{-повна;} \\ N\text{-тонка} &\implies N\text{-тонка справа.} \end{aligned}$$

У випадку вільного моноїда A^*, підмножина N в A^* щільною справа тоді і тільки тоді, коли кожне слово вільного моноїда A^* є префіксом деякого слова з множини N. Таким чином, (непорожній) лівий ідеал є щільним справа. Аналогічно, підмножина N є повною справа, якщо кожне слово w вільного моноїда A^* можна записати як

$$w = m_1 m_2 \cdots m_r p,$$

для деяких $r \geqslant 0$, $m_1, \ldots, m_r \in N$, і префікса p деякого слова в N.

Твердження 3.3.1. *Нехай $A \neq \varnothing$. Тоді для довільної підмножини $X \subset A^*$ такі умови є еквівалентними:*

(*i*) *множина XA^* є щільною справа;*
(*ii*) $A^* = XA^- \cup X \cup XA^+$;
(*iii*) *для довільного слова $w \in A^*$ існують слова $u, v \in A^*$, $x \in X$ такі, що $wu = xv$.*

Доведення. (*i*) $\Longrightarrow$ (*iii*) Нехай $w \in A^*$. Оскільки підмножина XA^* є щільною справа, то вона перетинає правий ідеал wA^*. Отож $wu = xv$ для деяких слів $u, v \in A^*$ та $x \in X$.

(*iii*) $\Longrightarrow$ (*ii*) Якщо $wu = xv$, то $w \in XA^-$, $w \in X$ або $w \in XA^+$ згідно до того, що $w < x$, $w = x$, або $w > x$.

(*ii*) $\Longrightarrow$ (*i*) Множиною префіксів множини XA^* є $XA^- \cup X \cup XA^+$. □

Твердження 3.3.2. *Нехай $A \neq \varnothing$ і $X \subset A^+$. Тоді підмножина XA^* є щільною справа тоді і тільки тоді, коли множина X повною справа.*

Доведення. Припустимо спочатку, що XA^* є щільною справа та розглянемо слово $w \in A^*$. Якщо $w \in XA^- \cup X$, то $wu \in X$ для деякого слова $u \in A^*$. В протилежному випадку $w \in XA^+$ за твердженням 3.3.1. Отож, $w = xw'$ для деякого слів $x \in X$, $w' \in A^+$. Оскільки $x \neq 1$, то $|w'| < |w|$. Тоді за індукцією маємо, що $w'u \in X^*$ для деякого слова $u \in A^*$. Таким чином, слово w є префіксом деякого слова множини X^*.

Навпаки, нехай $w \in A^*$, і припустимо, що $wu \in X^*$ для деякого слова $u \in A^*$. Домноживши, якщо необхідно на деяке слово з множини X, ми можемо вважати, що $wu \neq 1$. тоді $wu \in X^+ \subset XA^*$. □

Зауважимо, що твердження 3.3.2 не виконується у випадку $X = \{1\}$. У цьому випадку множина $XA^* = A^*$ є щільною справа, але $X^* = \{1\}$ не є, очевидно, повною справа.

Наступне твердження описує природні бієкції між такими сім'ями підмножин вільного моноїда A^*:

(*i*) сім'я $\mathcal{M}$ максимальних префіксних множин;
(*ii*) сім'я $\mathcal{D}$ правих ідеалів, які є щільними справа;
(*iii*) сім'я $\mathcal{P}$ префіксно замкнених підмножин, які не містять правий ідеал.

Ці бієкції фактично є обмеженнями бієкції з твердження 3.1.2.

Твердження 3.3.3. *Виконуються такі умови:*

(*i*) *відображення $X \mapsto XA^*$ є бієкцією з $\mathcal{M}$ на $\mathcal{D}$, і відображення $I \mapsto I \setminus IA^+$ є до нього оберненим;*
(*ii*) *операція теоретико множинного доповнення бієктивно відображає $\mathcal{P}$ на $\mathcal{D}$;*
(*iii*) *відображення $X \mapsto XA^-$ є бієкцією з $\mathcal{M}$ на $\mathcal{P}$, і відображення $P \mapsto PA \setminus P$ є до нього оберненим.*

Доведення. (*i*) Нехай X — максимальна префіксна множина. Кожне слово $u \in A^*$ є сумісним зі словом множини X, оскільки в іншому випадку множина $X \cup \{u\}$ буде префіксною, що суперечить максимальності множини X. Отож, правий ідеал XA^* є щільним справа. Доведення того, що відображення $I \mapsto I \setminus IA^+$ є до нього оберненим доводиться аналогічно.

Твердження (*ii*) є наслідком того факту, що множина щільною справа тоді і тільки тоді, коли її доповнення не містить правий ідеал.

(*iii*) Якщо X — максимальна префіксна підмножина вільного моноїда A^*, то правий ідеал XA^* є щільним справа. Отож, за твердженням 3.3.1 отримуємо, що $A^* \setminus XA^* = XA^-$. □

Наступний наслідок видається корисним.

Наслідок 3.3.4. *Нехай $A \neq \varnothing$, $L \subset A^+$ і $X = L \setminus LA^+$. Тоді множина L є повною справа тоді і тільки тоді, коли X є максимальним префіксним кодом.*

Доведення. За твердженням 3.3.2 множина L є повною справа тоді і тільки тоді, коли правий ідеал LA^* є щільним справа. З твердження 3.1.2 випливає, що $XA^* = LA^*$. Далі застосуємо твердження 3.3.3. □

Особливим випадком наслідку 3.3.4 є наступна важлива теорема, яка випливає з нього, взявши за множину L префіксний код X.

Теорема 3.3.5. *Нехай $A \neq \varnothing$ і $X \subset A^+$ — префіксний код. Тоді код X є повним справа тоді і тільки тоді, коли X є максимальним префіксним кодом.*

Тепер ми доведемо твердження, яке відповідає твердженню 3.1.6 для максимальних префіксних кодів.

Теорема 3.3.6. *Нехай $A \neq \varnothing$, $X \subset A^+$ — префіксний код і $P = XA^-$ — множина власних префіксів слів коду X. Тоді код X є максимальним префіксним тоді і тільки тоді, коли виконується одна з двох наступних еквівалентних умов*

$$\underline{X} - 1 = \underline{P}(\underline{A} - 1) \qquad \textit{або} \qquad \underline{A}^* = \underline{X}^*\underline{P}. \tag{3.8}$$

Доведення. Покладемо $R = A^* \setminus XA^*$. Якщо код X є максимальним префіксним, то за твердженням 3.3.1 правий ідеал XA^* є щільним справа і $R = P$. Далі застосуємо твердження 3.1.6.

Навпаки, якщо $\underline{X} - 1 = \underline{P}(\underline{A} - 1)$, то за рівністю (3.1) маємо, що

$$\underline{P}(\underline{A} - 1) = \underline{R}(\underline{A} - 1).$$

Оскільки ряд $\underline{A} - 1$ є оборотним, то отримуємо, що $P = R$, а звідси випливає, що правий ідеал XA^* є щільним справа. □

Наслідок 3.3.7. *Нехай X — скінченний n елементний максимальний префіксний код над k-елементним алфавітом і $p = \mathrm{Card}(XA^-)$ — кількість власних префіксів слів з коду X. Тоді $n - 1 = p(k - 1)$.*

У випадку скінченного максимального префіксного коду рівності теореми 3.3.6 дають факторизацію ряду $\underline{X} - 1$ на два поліноми. Знову ж таки, існує формула, отримана з формули (3.8), а саме: $1 + \underline{P}\,\underline{A} = \underline{P} + \underline{X}$, яка має інтерпретацію літерного зображення коду X, що робить перевірку максимальності дуже легкою: якщо p є вузлом, який є не в коді X, то для кожного $a \in A$ має існувати вузол pa в літерному зображенні коду X.

Тепер доведемо, що для тонких множин максимальний префіксний код також є максимальним кодом.

Теорема 3.3.8. *Нехай $A \neq \varnothing$ і X — худа підмножина в A^+. Тоді наступні умови є еквівалентними:*

(*i*) *X є максимальним префіксним кодом;*
(*ii*) *X є префіксним і максимальним кодом;*
(*iii*) *множина X є повною справа і є кодом.*

Доведення. Імплікація $(ii) \Longrightarrow (i)$ є очевидною.

Імплікація $(i) \Longrightarrow (iii)$ випливає з твердження 3.3.3(i) і твердження 3.3.2.

$(iii) \Longrightarrow (ii)$ Нехай $Y = X \setminus XA^+$. За твердженням 3.1.2, $YA^* = XA^*$. Отож множина Y є повною справа. Звідси випливає, що множина Y є повною. Множина Y є також тонкою, оскільки $Y \subseteq X$. За теоремою 2.5.13, Y є максимальним кодом. З включення $Y \subseteq X$ отримуємо рівність $X = Y$. □

З наступного прикладу випливає, що твердження теореми 3.3.8 не виконуються без припущення, що код є тонким.

Приклад 3.3.9. Нехай $X = \{uba^{|u|} : u \in A^*\}$, з $A = \{a, b\}$. Цей код є оберненим до коду, означеного а прикладі 2.4.12. X є максимальним кодом, а отже є повним справа. Однак, X не є префіксним кодом. З наслідку 3.3.4 випливає, що множина $Y = X \setminus XA^+$ є максимальним префіксним кодом. Звичайно, $Y \neq X$, а отже Y не є максимальним кодом.

Твердження 3.3.10 безпосередньо випливає з теорем 2.5.16 і 3.3.8.

Твердження 3.3.10. *Нехай $A \neq \varnothing$ і X — худа підмножина в A^+. Тоді наступні умови є еквівалентними:*

(*i*) *X є максимальним префіксним кодом;*
(*ii*) *множина X є префіксною й існує додатній розподіл Бернуллі π з $\pi(X) = 1$;*
(*iii*) *множина X є префіксною та $\pi(X) = 1$ для довільного додатнього розподілу Бернуллі π.*

У попередньому підрозділі ми виклали описання префіксних кодів за допомогою базисів стабілізаторів в детермінованому автоматі. Тепер розглянемо максимальні префіксні коди. Означимо наступне поняття. Стан q детермінованого автомата $\mathcal{A} = (Q, i, T)$ над алфавітом A називається *зворотним*, якщо для всіх слів $u \in A^*$, існує слово $v \in A^*$ таке, що $q \cdot uv = q$. Звідси випливає, зокрема, що $q \cdot u \neq \varnothing$ для всіх $u \in A^*$.

Твердження 3.3.11. *Нехай $A \neq \varnothing$ і X — префіксний код над алфавітом A. Тоді наступні умови є еквівалентними:*

(*i*) *X — максимальний префіксний код;*
(*ii*) *мінімальний автомат вільного моноїда X^* є повним;*
(*iii*) *усі стани мінімального автомата вільного моноїда X^* є зворотними;*
(*iv*) *початковий стан мінімального автомата вільного моноїда X^* є зворотним;*
(*v*) *вільний моноїд X^* є стабілізатором зворотного стану в деякому детермінованому автоматі.*

Доведення. (*i*) $\Longrightarrow$ (*ii*) Нехай $\mathcal{A}(X^*) = (Q, i, i)$ — мінімальний автомат вільного моноїда X^*. Розглянемо довільні $q \in Q$ і $a \in A$. Існує деяке слово $u \in A^*$ таке, що $i \cdot u = q$. Оскільки код X є повним справа, то $uav \in X^*$ для деякого слова $v \in A^*$. Отож, отримуємо

$$i = i \cdot uav = (q \cdot a) \cdot v,$$

звідки випливає, що $q \cdot a \neq \varnothing$. Таким чином, $\mathcal{A}(X^*)$ — повний автомат.

(*ii*) $\Longrightarrow$ (*iii*) Нехай $q \in Q$ і $u \in A^*$. Оскільки $\mathcal{A}(X^*)$ — повний автомат, то $q' = q \cdot u \neq \varnothing$. З того, що автомат $\mathcal{A}(X^*)$ є мінімальний випливає, що стан q' є кодоступним, а стан q є доступним. Отож, $q' \cdot v = q$ для деякого слова $v \in A^*$, а звідси випливає, що стан q є зворотним.

Імплікації (*iii*) $\Longrightarrow$ (*iv*) і (*iv*) $\Longrightarrow$ (*v*) є очевидними.

(*v*) $\Longrightarrow$ (*i*) Нехай $\mathcal{A} = (Q, i, i)$ — детермінований автомат і $q \in Q$ — зворотний стан такий, що $X^* = \mathrm{Stab}(q)$. Для всіх слів $u \in A^*$ існує слово $v \in A^*$ таке, що $q \cdot uv = q$, а отже $uv \in X^*$. Звідси випливає, що код X є повним справа. Оскільки множина X є префіксною, то залишилося застосувати теорему 3.3.8. □

3.4 Операції на префіксних кодах

Префіксні коди замкнені стосовно деяких простих операцій. Почнемо із загального результату, який буде неодноразово використовуватися.

Твердження 3.4.1. *Нехай $A \neq \varnothing$, X і $(Y_i)_{i\in\mathcal{I}}$ — непорожні підмножини вільного моноїда A^*, і $(X_i)_{i\in\mathcal{I}}$ — розбиття множини X. Означимо*

$$Z = \bigcup_{i\in\mathcal{I}} X_i Y_i.$$

Тоді виконуються такі умови:

(*i*) *якщо X і Y_i — префіксні (максимальні префіксні) множини, то Z — префіксна (максимальна префіксна) множина;*

(*ii*) *якщо Z — префіксна множина, то всі Y_i ($i \in \mathcal{I}$) є префіксним множинами;*

(*iii*) *якщо X — префіксна множина та Z — максимальна префіксна множина, то X і Y_i — максимальні префіксні множини.*

Доведення. (*i*) Припустимо, що $z, zu \in Z$. Тоді $z = xy$, $zu = x'y'$ для деяких $i, j \in \mathcal{I}$, $x \in X_i$, $y \in Y_i$, $x' \in X_j$, $y' \in Y_j$. З відношення $xyu = x'y'$ випливає, що $x = x'$, оскільки множина X є префіксною, звідки випливає, що $i = j$ і $y = y'$. Отож, $u = 1$ і множина Z є префіксною. Припустимо, що ліві ідеали XA^* і Y_iA^* є щільними справа. Нехай $w \in A^*$. Тоді $ww' = xv$ для деяких $w', v \in A^*$, $x \in X$. Нехай x належить множині X_i. Оскільки лівий ідеал Y_iA^* щільним справа, то $vv' \in Y_iA^*$ для деякого слова $v' \in A^*$. Отож, $ww'v' \in X_iY_iA^*$, звідки випливає, що $ww'v' \in ZA^*$. Таким чином, Z — максимальна префіксна множина.

(*ii*) Нехай $y, yu \in Y_i$ та $x \in X_i$. Тоді $xy, xyu \in Z$, звідки випливає, що $u = 1$.

(*iii*) З включення $ZA^* \subseteq XA^*$ отримуємо, що правий ідеал XA^* є щільним справа. Звідси випливає, що множини X є максимальною префіксною. Для доведення того, що правий ідеал Y_iA^* є щільним справа, зафіксуємо довільне слово $w \in A^*$. Для довільного елемента $x \in X_i$ слово xw є поповнювальним справа в ZA^*. Отож, $xw = zw'$ для деякого $z \in Z$. Поклавши $z = x'y'$ з $x' \in X_j$, $y' \in Y_j$, отримуємо $xw = x'y'w'$. Оскільки код X — префіксний, то $x = x'$, а отже $w = y'w'$, звідки випливає, що слово w міститься в правому ідеалі Y_iA^*. □

Для $\mathrm{Card}(\mathcal{I}) = 1$, ми отримуємо, зокрема,

Наслідок 3.4.2. *Якщо X і Y — префіксні коди (максимальні префіксні множини), то XY — префіксний код (максимальна префіксна множина).*

Обернене твердження до наслідка 3.4.2 виконується лише при виконанні обмежуючих умов і буде викладено в твердженні 3.4.13.

Приклад 3.4.3. *Код Ґоломба* (*the Golomb code*) порядку $m \geqslant 1$ над алфавітом $\{0, 1\}$ є максимальний нескінченний префіксний код

$$G_m = 1^*0R_m,$$

де $R_1 = \{\varepsilon\}$ і для $m \geqslant 2$ множина R_m є нескінченним префіксним кодом, який визначається нижче. Таким чином, кожен код G_m є добутком максимальних префіксних кодів 1^*0 і R_m.

Якщо $m = 2^k$ для деякого цілого числа k, то R_m є множиною усіх бінарних слів довжини k. В іншому випадку правило більш складним. Покладемо $m = 2^k + l$, з $0 < l < 2^k$. Поклавши $n = 2^k - 1$, означимо

$$R_m = \begin{cases} 0R_l \cup 1R_{2n}, & \text{якщо } l \geqslant n; \\ 0R_l \cup 1R_{n+l}, & \text{в іншому випадку.} \end{cases}$$

Множинв R_1 і коди R_m для $m = 2, \ldots, 7$ зображено на рис. 3.20. Зауважимо, зокрема,

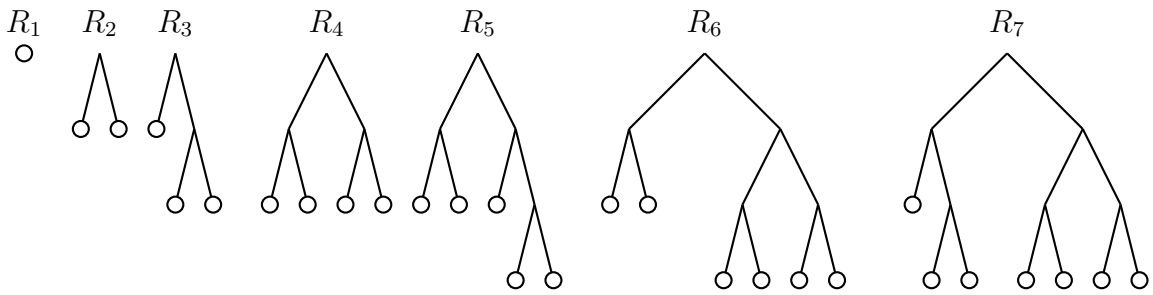


Рис. 3.20: Множини коду Ґоломба з R_1 до R_7

що довжини кодових-слів різняться щонайбільше на одиницю.

Коди Ґоломба порядків $1, 2, 3$ зображені на рис. 3.21. Звернемо увагу, що, за

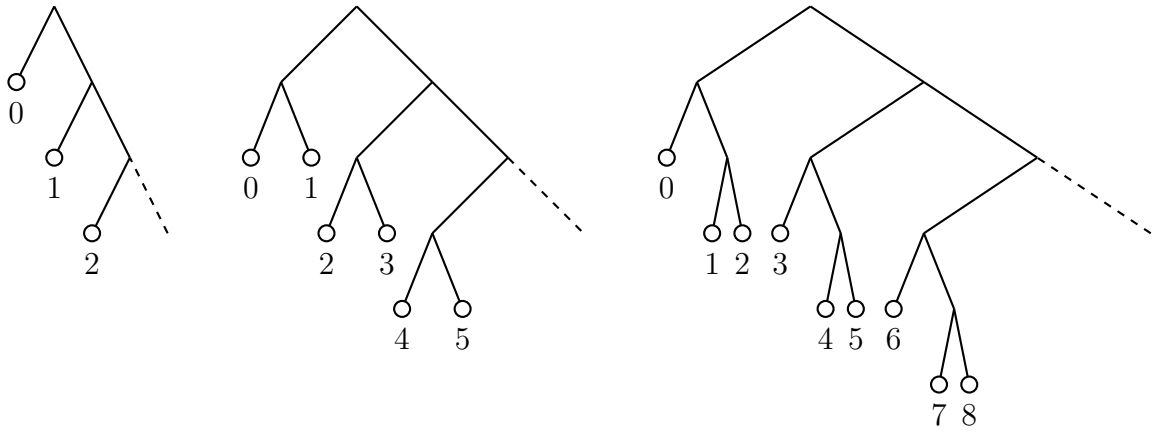


Рис. 3.21: Коди Ґоломба порядків $1, 2, 3$

вийнятком, можливо, для першого рівня, є рівно m слів кожної довжини. Коди Ґоломба використовуються для зображення цілих чисел, як показано на рис. 3.21. Можна довести, що вони є оптимальними для деяких імовірністних розподілів (див. вправу 3.10.20).

Приклад 3.4.4. *Код Ґоломба-Райса* (*the Golomb–Rice code*) порядку k є частковим випадком коду Ґоломба для $m = 2^k$. Його структура особливо проста і дозволяє легко виразити описання кодування цілого числа: кодування присвоює цілому числу $n \geqslant 0$

два слова е двійковій системі числення, *базове слово* і *зміщення*. Базовим словом є унарне розширення значення $\lfloor n/2^k \rfloor$, яке слідує за 0. Таким чином, для $k = 2$ ціле число $n = 9$ кодується 110|01. Бінарні дерева, які зображають код Ґоломба-Райса порядків $0, 1, 2$ представлені на рис. 3.22. Інше зображення коду Ґоломба–Райса

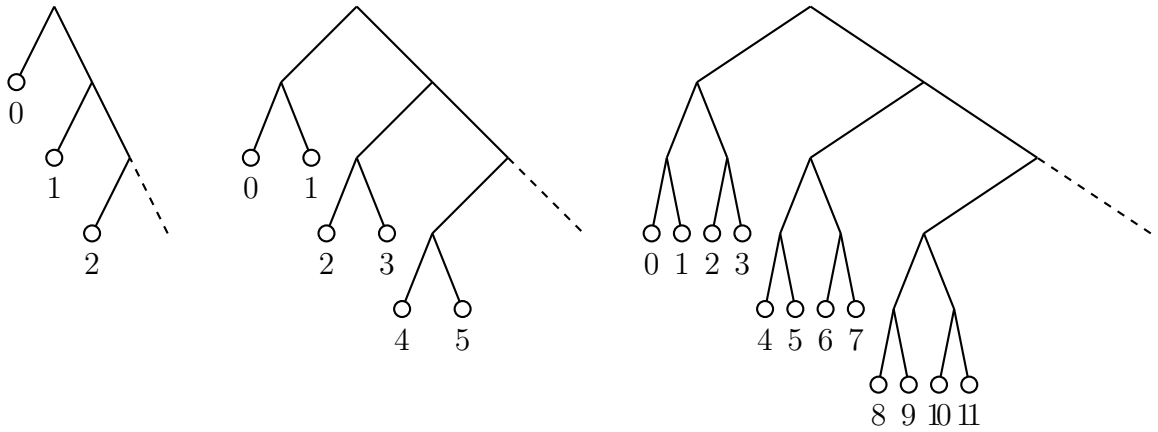


Рис. 3.22: Коди Ґоломба–Райса порядків $0, 1, 2$

порядку k визначається регулярним виразом

$$GR_k = 1^*0(0+1)^k. \tag{3.9}$$

Цей вираз виражає той факт, що бінарні слова, що формують код, складаються з базового слова вигляду 1^i0 для деякого цілого числа $i \geqslant 0$ і зміщення, яке є довільною бінарною послідовністю довжини k.

Приклад 3.4.5. *Експоненціальні коди Ґоломба* утворюють сім'ю, яка залежить від цілого числа k з розподілом довжини, більш придатним для деяких розподілів ймовірностей, ніж коди Ґоломба–Райса. Випадок $k = 0$ тісно пов'язаний з кодом Еліа, вже згаданим у прикладі 3.1.1.

Базисне слово слова-кода для цілого числа n утворюється наступним чином. Нехай x — зображення в двійковій системі числення числа $1+\lfloor n/2^k \rfloor$ й i — його довжина. Базисне слово робиться з унарного зображення значення $i-1$, за яким слідує x з його початковим символом 1 заміненим на символ 0. Зміщення, як і раніше, є двійковим зображеенням решти ділення n на 2^k, записаним на k бітах. Таким чином, для $k = 1$, кодове слово для 9 дорівнює 11001|1. Експоненціальні коди Ґоломба порядків 1, 2 і 3 зображено на рис. 3.23.

Вираз, який описує експоненціальний код Ґоломба, має вигляд

$$EG_k = \bigcup_{i \geqslant 0} 1^i0(0+1)^{i+k},$$

і ми отримуємо просте відношення

$$EG_k = EG_0(0+1)^k.$$

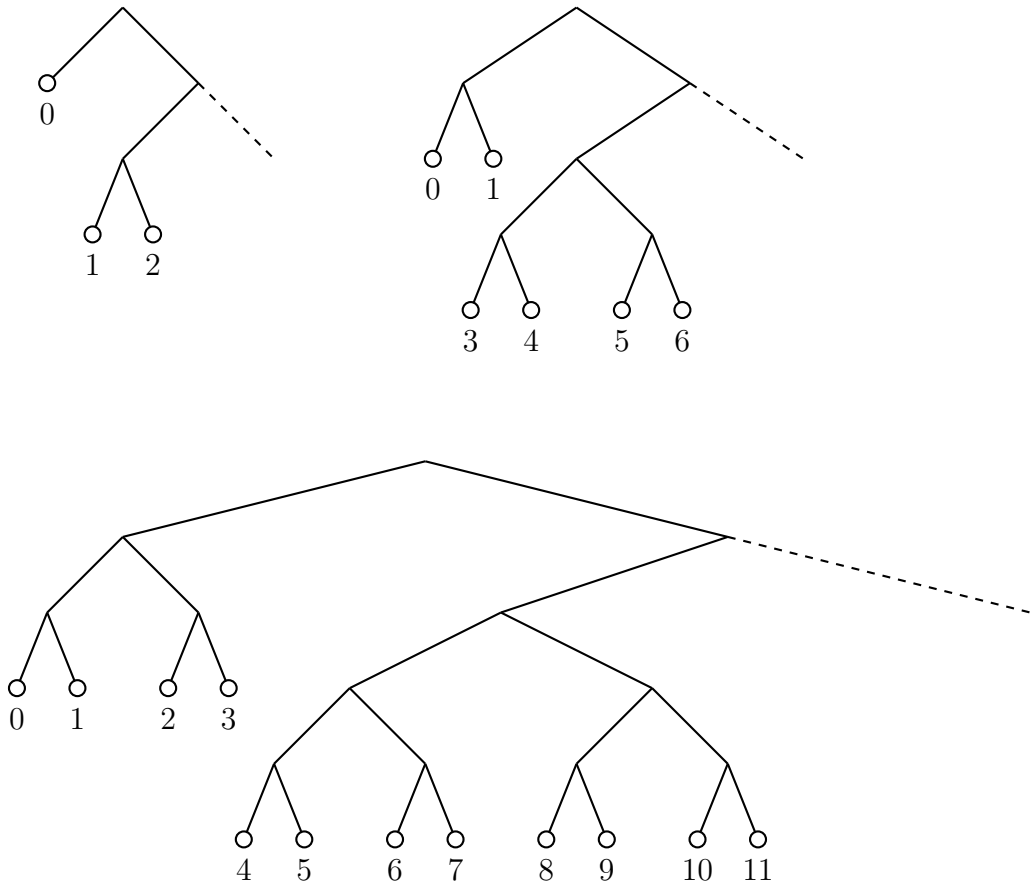


Рис. 3.23: Експоненціальні коди Ґоломба порядків 1, 2 і 3

Наслідок 3.4.6. *Нехай $A \neq \varnothing$, $X \subset A^+$ і $n \geqslant 1$. Тоді множина X є (максимальною) префіксною тоді і тільки тоді, коли множина X^n є (максимальною) префіксною.*

Доведення. За наслідком 3.4.2, множина X^n є максимальною префіксною для максимального префіксного коду X.

Навпаки, поклавши $Z = X^n = X^{n-1}X$, то з твердження 3.4.1(*ii*) випливає, що множина X є префіксною. Записавши $Z = XX^{n-1}$, то за твердженням 3.4.1(*iii*), з того, що множина Z є максимальною префіксною випливає, що множини X і X^{n-1} є також максимальними префіксними. □

Наслідок 3.4.6 спеціальним випадком твердження 3.4.11, яке ми доведемо пізніше.

Наслідок 3.4.7. *Нехай X і Y — префіксні коди та $X = X_1 \cup X_2$ — розбиття. Тоді $Z = X_1 \cup X_2Y$ є префіксним кодом і Z є максимальним префіксним кодом тоді і лише тоді, коли X і Y є максимальними префіксними кодами.*

Доведення. З $Y' = \{1\}$ маємо, що $Z = X_1Y' \cup X_2Y$. Залишилося використати твердження 3.4.1, оскільки Y' є максимальною префіксною множиною. □

Є особливий випадок цього наслідку, який заслуговує на увагу. Він представляє цікаву операцію на кодах, що розглядаються як дерева.

Наслідок 3.4.8. *Нехай X і Y — префіксні коди й $x \in X$. Тоді код*

$$Z = (X \setminus \{x\}) \cup xY$$

є префіксним і Z є максимальним префіксним кодом тоді і тільки тоді, коли X і Y є максимальними префіксними кодами.

Операція, виконана на префіксних кодах X і Y, наведена на рис. 3.24. Ми тепер

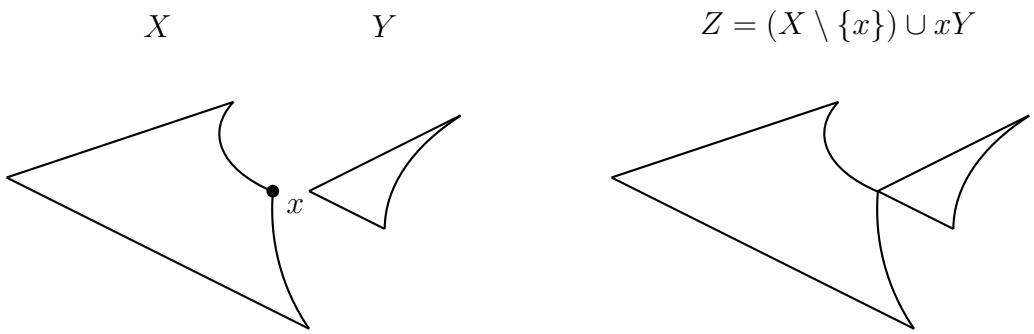


Рис. 3.24: Поєднання кодів X і Y

повернемося до оберненої операції.

Твердження 3.4.9. *Нехай $A \neq \varnothing$, Z — префіксний код і $p \in ZA^-$. Тоді*

$$Y_p = p^{-1}Z \qquad і \qquad X = Z \setminus pY_p \cup \{p\} \tag{3.10}$$

є префіксними множинами. Більше того, якщо Z — максимальна префіксна множина, то Y_p і X також є максимальними префіксними множинами.

Операцію описану в формулі (3.10) можна зобразити, як це показано на рис. 3.25. Твердження 3.4.9 є частковим випадком твердження 3.4.10.

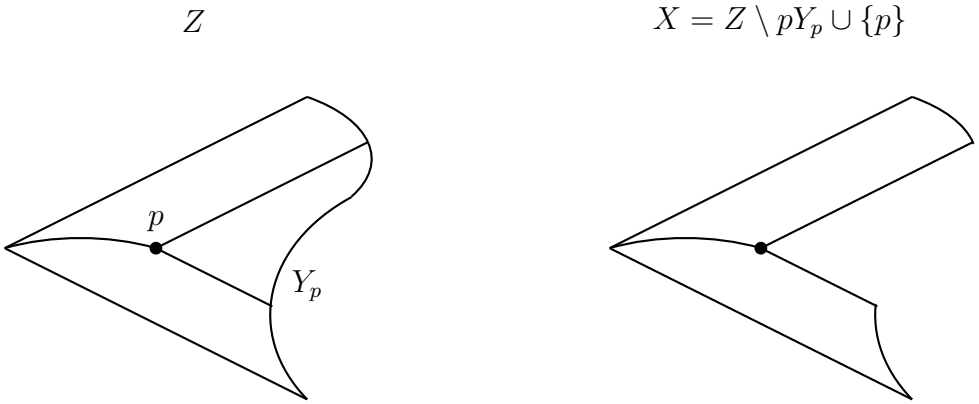


Рис. 3.25: Відокремлення Z і Y_p

Твердження 3.4.10. *Нехай $A \neq \varnothing$, Z — префіксний код і Q — префіксна підмножина в ZA^-. Для кожного елемента $p \in ZA^-$ множина $Y_p = p^{-1}Z$ є префіксним кодом; крім того*

$$X = Q \cup \left(Z \setminus \bigcup_{p \in Q} pY_p \right)$$

є префіксною множиною. Якщо Z максимальною префіксною множиною, то X і Y_p $(p \in Q)$ є максимальними префіксними множинами.

Доведення. Покладемо $X_0 = Z \setminus \bigcup_{p \in Q} pY_p$, $Y_0 = \{1\}$, $X_p = \{p\}$. Тоді

$$Z = X_0 Y_0 \cup \bigcup_{p \in Q} X_p Y_p.$$

Таким чином, для виведення результату з твердження 3.4.1 достатньо довести, що множина X є префіксною.

Нехай $x, xu \in X$ з $u \in A^+$. Ці два слова не можуть бути одночасно належати ні префіксній множині Z, ні префіксній множині Q. Оскільки $Q \subseteq ZA^-$, маємо, що $x \in Q, xu \in Z$. Таким чином, отримуємо, що $u \in Y_x$ і xu не міститься в множині X. □

Твердження 3.4.1 і 3.4.10 можна використати для переліку максимальних префіксних кодів. Це дозволяє проілюструвати обчислення у випадку, коли $A = \{a, b\}$. Якщо множина Z максимальною префіксною та $Z \neq 1$, то обидві множини

$$X = a^{-1}Z, \qquad Y = b^{-1}Z$$

є максимальними префіксними та

$$Z = aX \cup bY. \tag{3.11}$$

Навпаки, якщо X і Y — максимальні префіксні множини, то множина Z також є максимальною префіксною. Таким чином, рівність (3.11) визначає бієктивне відображення з множини максимальних префіксних кодів у множину пар максимальних префіксних множин. Більше того

$$\mathrm{Card}(Z) = \mathrm{Card}(X) + \mathrm{Card}(Y).$$

Нехай α_n – кількість максимальних префіксних множин з n елементами. Тоді за рівністю (3.11) маємо

$$\alpha_n = \sum_{k+l=n} \alpha_k \alpha_l. \tag{3.12}$$

для $n \geqslant 2$. Нехай $\alpha(t) = \sum_{n \geqslant 0} \alpha_n t^n$. Тоді з рівності (3.12) випливає, що

$$\alpha(t)^2 - \alpha(t) + t = 0.$$

Це рівняння має розв'язки

$$\frac{1 \pm \sqrt{1 - 4t}}{2}.$$

Позаяк $\alpha(0) = 0$, то отримуємо

$$\alpha(t) = \frac{1 - \sqrt{1-4t}}{2}.$$

Використавши біноміальні формули, для $n \geqslant 1$ маємо, що

$$\begin{aligned}
\alpha_n &= -\frac{1}{2} \cdot (-4)^n \cdot \binom{1/2}{n} = \\
&= -\frac{1}{2} \cdot (-4)^n \cdot \frac{1/2(1/2-1) \cdot \ldots \cdot (1/2-n+1)}{n!} = \\
&= -\frac{1}{2} \cdot (-4)^n \cdot \frac{1}{2^n} \cdot \frac{1(1-2) \cdot \ldots \cdot (1-2n+2)}{n!} = \\
&= -\frac{1}{2} \cdot (-1)^n \cdot 2^n \cdot (-1)^{n-1} \cdot \frac{1 \cdot 3 \cdot \ldots \cdot (2n-3)}{n!} = \\
&= 2^{n-1} \cdot \frac{(2n-2)!}{n!(n-1)!2^{n-1}} = \\
&= \frac{1}{n} \cdot \binom{2n-2}{n-1}.
\end{aligned}$$

Таким чином, отримуємо

$$\alpha_{n+1} = \frac{1}{n+1} \cdot \binom{2n}{n}. \tag{3.13}$$

Ці числа називаються *числами Каталана* (*the Catalan numbers*). Див. вправу 3.10.6 для іншого доведення та для випадку більше двох літер. Такого близького виразу не відомо для кількості скінченних максимальних кодів. У таблиці 3.1 наведено перші числа Каталана.

n	1	2	3	4	5	6	7	8
α_n	1	1	2	5	14	42	132	429

Табл. 3.1: Перші числа Каталана

Твердження 3.4.11. *Нехай Y і Z — композиційовні коди й $X = Y \circ Z$. Тоді X є максимальним префіксним і тонким кодом тоді і тільки тоді, коли Y і Z є максимальними префіксними та тонкими кодами.*

Доведення. Припустимо спочатку, що X є максимальним префіксним і тонким кодом. Тоді код X є повним справа за теоремою 3.3.8. Отже, код X є тонким і повним. За твердженням 2.6.14 обидва коди Y і Z є тонкими та повними. Далі за твердженням 2.6.13(i) код Y є префіксним. Отже код Y, будучи тонким, префіксним і повним, є максимальним префіксним кодом. Далі множина X щільною справа, а отже $X \subset Z^*$. Таким чином, код Z є щільним справа. Звідси випливає, що код Z є повним справа, і використавши теорему 3.3.8, отримуємо, що код Z є максимальним префіксним.

Навпаки, оскільки коди Y і Z є префіксними, то за твердженням 2.6.4 код X є префіксним, а з того що коди Y і Z є одночасно тонкими і повними, то з твердження 2.6.14 випливає, що код X є тонким і повним. Таким чином, X — максимальний префіксний код. □

Твердження 3.4.12. *Нехай $A \neq \varnothing$, Z — префіксний код над алфавітом A та $Z = X \cup Y$ — розбиття. Тоді $T = X^{\circledS}Y$ є префіксним кодом, і більше того T є максимальним префіксним кодом тоді і тільки тоді, коли Z є максимальним префіксним кодом.*

Доведення. Нехай B — алфавіт, який бієктивно співставлений з кодом Z і $B = C \cup D$ — розбиття алфавіту B, яке індукується розбиттям $Z = X \cup Y$. Тоді

$$T = C^*D \circ Z.$$

Код C^*D очевидно є префіксним. Отож, код T є префіксним за твердженням 2.6.4. Далі, з $T^* = \{1\} \cup Z^*Y$ випливає, що код T є повним справа тоді і тільки тоді, коли код Z є повним справа. Друга частина твердження випливає з твердження 3.3.3. □

Ми завершуємо цей підрозділ доведенням оберненого твердження до наслідку 3.4.2.

Твердження 3.4.13. *Нехай $A \neq \varnothing$, X і Y — скінченні непорожні підмножини вільного моноїда A^* такі, що добуток XY є однозначним. Якщо XY є максимальним префіксним кодом, то X і Y є максимальними префіксними кодами.*

Доведення. Нехай $Z = XY$ і $n = \max\{|y| \colon y \in Y\}$. Доведення проведемо індукцією по n. Для $n = 0$, маємо $Y = \{1\}$ і $Z = X$. Отож, у цьому випадку висловлення твердження є, очевидно, істинним. Припустимо, що $n \geqslant 1$ і нехай

$$T = \{y \in Y \colon |y| = n\} \qquad \text{і} \qquad Q = \{q \in YA^- \colon qA \cap T \neq \varnothing\}.$$

За побудовою маємо, що $T \subseteq QA$. Насправді виконується рівність $T = QA$. Справді, нехай $q \in Q$, $a \in A$ й $x \in X$ — слово максимальної довжини. Тоді слово xq є префіксом деякого слова з Z, і слово xqa є поповнювальним справа в правому ідеалі ZA^*. Оскільки код Z є префіксним, то жоден префікс слова xqa не є елементом коду Z. Звідси отримуємо, що

$$xqav = x'y',$$

для деяких $x' \in X$, $y' \in Y$ і $v \in A^*$.

Тепер маємо $n = |qa| \geqslant |y'|$ і $|x| \geqslant |x'|$. Отож, $x = x'$, $y' = qa$ і $v = 1$. Звідси випливає, що $qa \in Y$ і $T = QA$. Тепер нехай

$$Y' = (Y \setminus T) \cup Q \qquad \text{і} \qquad Z' = XY'.$$

Перевіримо, що множина Z' є префіксною. Припустимо, що це не так. Тоді

$$xy'u = x'y''$$

для деяких $x, x' \in X$, $y', y'' \in Y'$ і $u \neq 1$. Нехай a — перша літера слова u. Тоді або y', або $y'a$ є елементом множини Y. Аналогічно, якщо b — перша літера слова u, то або y'' або $y''b$ є елементом множини Y, для довільної літери $b \in A$. припустимо, що $y' \in Y$. Тоді слово $xy' \in Z$ є власним префіксом слова $x'y''$, або слова $x'y''b$, одне з них міститься в множині Z. Це суперечить тому, що множина Z є префіксною. Отож, отримуємо $y'a \in Y$. Як у попередньому випадку маємо, що слово xy' не є власним префіксом слова $x'y''$ або слова $x'y''b$. При цьому обов'язково $u = a$ і $y'' \in Y$, а отже маємо, що

$$xy'a = x'y''$$

з $y'a, y'' \in Y$. З однозначності добутку XY випливає, що $x = x'$ і $y'a = y''$. Але тоді $y'' \notin Y'$. Отримали протиріччя.

Для доведення того, що множина Z' є максимальною префіксною, зауважимо, що $Z \subseteq Z' \cup Z'A$. Отож, $ZA^* \subseteq Z'A^*$ і з твердження 3.3.3 випливає, що множина Z' є максимальною префіксною. На завершенні, легко бачити, що добуток XY' є однозначним: якщо $xy' = x'y''$ з $x, x' \in X$, $y', y''Y'$, то або $y', y'' \in Y \setminus T$, або $y', y'' \in Q$, а третій випадок виключається за рахунок префіксності множини Z.

Звичайно, $\max\{|y| \colon y \in Y'\} = n-1$. За припущенням індукції маємо, що X і Y' — максимальні префіксні множини. Оскільки

$$Y = (Y' \setminus Q) \cup QA,$$

то за наслідком 3.4.7 множина Y максимальною префіксною. □

Можна також дати зовсім інше доведення твердження 3.4.13, використовуючи той факт, що в припущеннях цього твердження виконується умова $\pi(X)\pi(Y) = 1$ для всіх розподілів Бернулі π (див. вправу 3.10.7).

Наступний приклад показує, що твердження 3.4.13 не виконується у випадку нескінченних кодів.

Приклад 3.4.14. Розглянемо $X = \{1, a\}$ і $Y = (a^2)^*b$ над алфавітом $A = \{a, b\}$. У цьому випадку множина X не є префіксною, а множина Y не є максимальною префіксною. Однак, $XY = a^*b$ є максимальним префіксним кодом і цей добуток є однозначним.

3.5 Семафорні коди

Цей підрозділ містить детальне вивчення семафорних кодів, які представляють цікавий підклас префіксних кодів. Ці дослідження також ілюструють методи, представлені в попередніх підрозділах.

Твердження 3.5.1. *Нехай $A \neq \varnothing$. Для довільної непорожньої підмножини S вільної напівгрупи A^+ множина*

$$X = A^*S \setminus A^*SA^+ \tag{3.14}$$

є максимальним префіксним кодом.

Доведення. Множина $L = A^*S$ є лівим ідеалом у вільному моноїді A^*, а отже є щільною справа. Звідси випливає, що множина L є повною справа, і за наслідком 3.3.4, множина $X = L \setminus LA^+$ є максимальним префіксним кодом. □

Код X форми рівності (3.13) називається *семафорним кодом* (а *semaphore code*), множина S — це множина *семафорів* для коду X. Термінологія випливає з наступного спостереження: *слово є в коді X тоді і тільки тоді, коли воно закінчується семафором, але жоден з його власних префіксів не закінчується семафором.* Таким чином, читання слова зліва направо, перший вигляд семафора дає "сигнал", який вказує, що прочитане до тепер розташоване в коді X.

Приклад 3.5.2. Нехай $A = \{a, b\}$ і $S = \{a\}$. Тоді $X = A^*a \setminus A^*aA^+$, звідки отримуємо $X = b^*a$.

Приклад 3.5.3. Для $A = \{a, b\}$ і $S = \{aa, ab\}$ маємо $A^*S = A^*aA$. Таким чином $A^* \setminus SA^*SA^+ = b^*aA$.

Наступне твердження охарактеризовує семафорні коди серед префіксних кодів.

Твердження 3.5.4. *Нехай $A \neq \varnothing$ і $X \subset A^+$. Тоді X є семафорним кодом тоді і тільки тоді, коли X є префіксним і*

$$A^*X \subseteq XA^*. \tag{3.15}$$

Доведення. Нехай $X = A^*S \setminus A^*SA^+$ — семафорний код. Тоді код X є префіксним і залишилось довести, що виконується рівність (3.15). Нехай $w \in A^*X$. Оскільки $w \in A^*S$, то слово w має множник з множини S. Нехай w' — найкоротший префікс слова w, який міститься в A^*S. Тоді слово w' міститься в коді X, а отже $w \in XA^*$.

Навпаки, припустимо, що префіксний код X задовольняє умову (3.15). Покладемо $M = XA^*$. З твердження 3.1.2 і з того факту, що код X є префіксним випливає, що $X = M \setminus MA^+$. З рівності (3.15) випливає, що

$$A^*M = A^*XA^* \subseteq XA^* = M,$$

а отже, $M = A^*M$ і $X = A^*M \setminus A^*MA^+$. □

Приклад 3.5.5. Нехай $A = \{a, b\}$. Код $Y = \{a^2, aba, ab^2, b\}$ є максимальним префіксним кодом над алфавітом A. Однак, Y не є семафорним кодом, оскільки $ab \in A^*Y$, але $ab \notin YA^*$.

Семафорний код є максимальним префіксним, а отже є повними справа. Наступне твердження описує такі повні справа множини, які є семафорними кодами.

Твердження 3.5.6. *Нехай $A \neq \varnothing$ і $X \subset A^+$. Тоді X є семафорним кодом тоді і тільки тоді, коли множина X є повною справа й*

$$X \cap A^*XA^+ = \varnothing. \tag{3.16}$$

Доведення. Семафорний код є максимальним префіксним, а отже є повним справа. Далі з умови (3.15) випливає, що

$$A^*XA^+ \subseteq XA^+,$$

а отже

$$X \cap A^*XA^+ \subseteq X \cap XA^+ = \varnothing,$$

звідки випливає рівність (3.16).

Навпаки, якщо множина X задовольняє умову (3.16), то вона є префіксною. Для доведення того, що X є семафорним кодом, перевіримо чи виконується умова (3.15). Нехай $w = ux \in A^*X$ з $u \in A^*$, $x \in X$. Оскільки код X є префіксним, то маємо, що $uxv = x'y$ для деяких $x' \in X$, $y \in X^*$ і $v \in A^*$. З умови (3.16) випливає, що слово ux не є власним префіксом слова x', а отже $ux \in x'A^*$. □

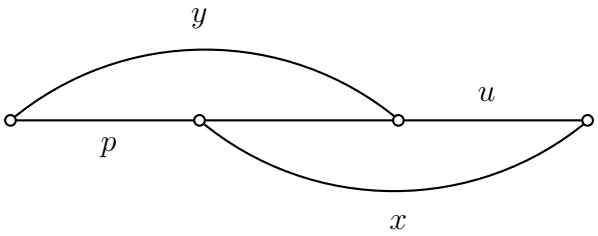


Рис. 3.26: Доведення наслідку 3.5.7

Наслідок 3.5.7. *Нехай $A \neq \varnothing$ і $X \subset A^+$ — семафорний код і $P = XA^-$. Тоді*

$$PX \subseteq XP \cup X^2.$$

Доведення. Нехай $p \in P$, $x \in X$ (див. рис. 3.26). За рівністю (3.15), $px = yu$ для деяких $y \in X$, $u \in A^*$. Код X є префіксним, а отже $|p| < |y|$. Звідси випливає, що слово u є суфіксом слова x, і тоді з умови (3.16) випливає, що $u \notin XA^+$. Код X є максимальним префіксним, а отже $u \in XA^- \cup X$. □

Формула (3.16) виражає властивість семафорних кодів, яка є більш сильнішою, ніж префіксна умова: *для семафорного кода X і двох елементів $x, x' \in X$, єдиний можливий шлях для слова x з'явитись як множник у слові x' означає бути суфіксом слово x'*. Тепер ми використаємо цей факт для того, щоб охарактеризувати семафорні коди серед максимальних префіксних кодів.

Твердження 3.5.8. *Нехай $A \neq \varnothing$, $X \subset A^+$ і $P = XA^-$ — множина власних префіксів слів з множини X. Тоді X є семафорним кодом тоді і тільки тоді, коли X є максимальним префіксним кодом і множина P є префіксно замкненою.*

Доведення. Нехай X — семафорний код. Тоді X є максимальним префіксним кодом за твердженням 3.5.1. Далі, нехай $p = uq \in P$ з $u, q \in A^*$. Нехай $v \in A^+$ — слово таке, що $pv \in X$. Тоді $q \notin XA^*$, оскільки в протилежному випадку $v = uqv \in X \cap A^*XA^+$, а це суперечить твердженню 3.5.6. Отож, отримуємо $q \in XA^- = P$.

Навпаки, припустимо, що X є максимальним префіксним кодом і множина P є префіксно замкненою. Припустимо, що $X \cap A^*XA^+ \neq \varnothing$. Нехай $x \in X \cap A^*XA^+$. Тоді $x = ux'v$ для деяких $u \in A^*$, $x' \in X$ і $v \in A^+$. Звідси випливає, що $ux' \in P$, і оскільки множина P є суфіксно замкненою, то також маємо, що $x' \in P$, що є неможливим. Таким чином, за твердженням 3.5.6 множина X є семафорним кодом. □

Зауважимо, що звичайно множина P з твердження 3.5.8 є префіксно замкненою. Отож, множина P є суфіксно замкненою тоді і тільки тоді, коли вона містить множники її елементів.

Іншим наслідком твердження 3.5.6 є наступний результат.

Твердження 3.5.9. *Кожен семафорний код є тонким.*

Доведення. За формулою (3.16) жодне зі слів з множини XA^+ не є множником слова з множини X. □

Наслідок 3.5.10. *Кожен семафорний код є максимальним кодом.*

Доведення. Семафорний код є максимальним префіксним кодом і тонкою множиною за твердженнями 3.5.1 і 3.5.9. Отож, за теоремою 3.3.8 такий код є максимальним кодом. □

Тепер ми визначимо множини семафорів, що дають один і той же семафорний код.

Твердження 3.5.11. *Нехай $A \neq \varnothing$. Дві непорожні множини S і T вільної напівгрупи A^+ визначають один і той же семафорний код тоді і тільки тоді, коли $A^*SA^* = A^*TA^*$. Для кожного семафорного коду X існує єдина мінімальна множина семафорів, а саме $T = X \setminus A^+X$.*

Доведення. Нехай $X = A^*S \setminus A^*SA^+$ і $Y = A^*T \setminus A^*TA^+$. За твердженням 3.1.2 маємо, що $XA^* = A^*SA^*$ і $YA^* = A^*TA^*$, і тоді з наслідку 3.1.8 випливає, що $X = Y$ тоді і тільки тоді, коли $A^*SA^* = A^*TA^*$.

Далі, нехай $X = A^*S \setminus A^*SA^+$ — семафорний код. За означенням множини $T = X \setminus A^+X$, ми можемо застосувати до T дуальне твердження до твердження 3.1.2. Таким чином, $A^*T = A^*X$. Позаяк $A^*TA^* = A^*XA^* = A^*SA^*$, то множини S і T визначають однаковий семафорний код. Таким чином, отримуємо, що $X = A^*T \setminus A^*TA^+$.

На завершенні перевіримо, що $T \subseteq S$. Нехай $t \in T$. Позаяк $A^*TA^* = A^*SA^*$, то $t = usv$ для деяких $u, v \in A^*$, $s \in S$ і $s = u't'v'$ для деяких $u', v' \in A^*$, $t' \in T$. Отож, $t = uu't'v'v$. Зауважимо, що $T \subseteq X$. Таким чином, застосувавши формулу (3.16), отримуємо рівність $v'v = 1$. Позаяк T є суфіксним кодом, то $uu' = 1$. Отож, отримуємо, що $t = s$ і $t \in S$. □

Розглянемо тепер деякі операції на семафорних кодах.

Твердження 3.5.12. *Якщо X і Y — семафорні коди, то XY є семафорним кодом. Навпаки, якщо XY — семафорний код і X — префіксний код, то X є семафонним кодом.*

Доведення. Якщо X і Y — семафорні коди, то за наслідком 3.4.2 множина XY є префіксним кодом. Далі за твердженням 3.5.4 маємо, що

$$A^*XY \subseteq XA^*Y \subseteq XYA^*,$$

а отже XY є семафорним кодом.

Припустимо, що XY є семафорним кодом і X є префіксним кодом. Ми покажемо, що $A^*X \subseteq XA^*$. Для цього припустимо, що $w = ux \in A^*X$, для $u \in A^*$, $x \in X$, і нехай y — слово в множині Y мінімальної довжини. Тоді

$$wy = uxy = x'y'u',$$

для деяких $x' \in X$, $y' \in Y$, $u' \in A^*$ (див. рис. 3.27). За вибором слова y маємо, що $|y| \leqslant |y'| \leqslant |y'u'|$, а отже $|ux| \geqslant |x'|$, звідки випливає, що $ux \in XA^*$. □

З наступного прикладу випливає, якщо XY — семафорний код, то код Y не обов'язково повинен бути семафоруним, навіть якщо він є максимальним префіксним.

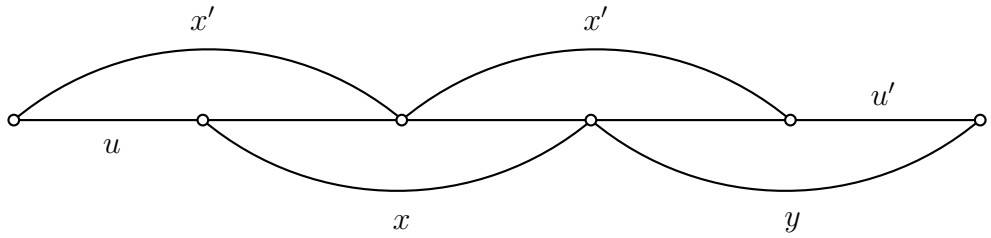


Рис. 3.27: Доведення твердження 3.5.12

Приклад 3.5.13. Означимо множини $X = a^*b$ та $Y = \{a^2, aba, ab^2, b\}$ над алфавітом $A = \{a, b\}$. Тоді X є семафорним кодом, а Y є максимальним префіксним кодом. Однак Y не є семафорним кодом (див. приклад 3.5.5). З іншого боку код $Z = XY$ є семафорним. Справді, множина Z є максимальним префіксним кодом, а множина

$$P = ZA^- = a^*\{1, b, ba, bab\}$$

є суфіксно-замкненою. Висновок випливає з наслідка 3.5.7 (див. рис. 3.28).

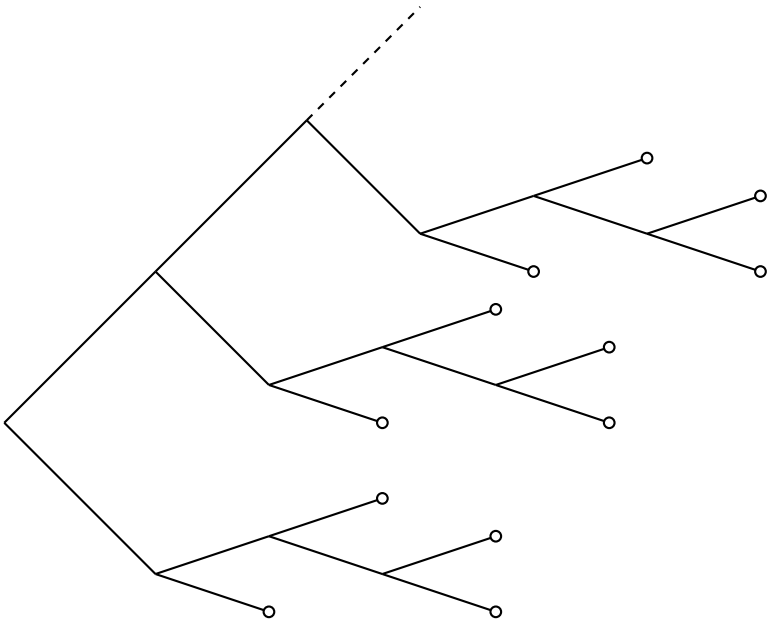


Рис. 3.28: Код $a^*b\,\{a^2, aba, ab^2, b\}$

Наслідок 3.5.14. *Нехай $A \neq \varnothing$. Для довільних підмножини X вільної напівгрупи A^+ and натурального числа $n \geqslant 1$, множина X є семафорним кодом тоді і тільки тоді, коли X^n є семафорним кодом.*

Доведення. Якщо X^n є семафорним кодом, то множина X є префіксною за наслідком 3.4.6, і X є семафорним кодом за твердженням 3.5.12.

Обернене твердження є безпосереднім наслідком твердження 3.5.12. □

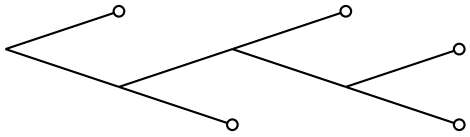


Рис. 3.29: Код $X = \{a, baa, baba, bab^2, b^2\}$

Приклад 3.5.15. Код $X = \{a, baa, baba, bab^2, b^2\}$ над алфавітом $A = \{a, b\}$, який зображено на рис. 3.29, є максимальним префіксним кодом, але не є семафорним. Справді, слово має внутрішню появу в слові bab^2, що суперечить формулі (3.16). Однак, код X розкладається на композицію двох семафорних кодів

$$X = Y \circ Z,$$

де $Y = \{c, dc, d^2, de, e\}$ і $Z = \{a, ba, b^2\}$.

Для семафорного коду

$$X = A^*S \setminus A^*SA^+$$

природно розглянути код

$$Y = SA^* \setminus A^+SA^*,$$

який є максимальним суфіксним кодом. Його обернений

$$\widetilde{Y} = A^*\widetilde{S} \setminus A^*\widetilde{S}A^+$$

є семафорним кодом з семафором $\widetilde{S}$. Наступний результат показує сильне співвідношення між X і Y.

Твердження 3.5.16. *Нехай $A \neq \varnothing$ і $S \subseteq A^+$. Тоді існує бієктивне відображення*

$$\beta\colon X = A^*S \setminus A^*SA^+ \to Y = SA^* \setminus A^+SA^*$$

таке, що $\beta(x)$ є спряженим словом до x для кожного слова $x \in X$.

Доведення. Спочатку розглянемо двобічний ідеал $J = A^*SA^*$. Виконуються рівності

$$X = J \setminus JA^+ \qquad \text{і} \qquad Y = J \setminus A^+J.$$

Справді, $A^*JA^* = A^*SA^*$ і з твердження 3.5.11 випливає, що $X = A^*J \setminus JA^+$. Рівність $X = J \setminus JA^+$ виконується, оскільки $A^*J = J$. З симетричних аргументів випливає, що виконується рівність $Y = J \setminus A^+J$.

Далі, означимо множину

$$D(x) = \big\{d \in A^+\colon \text{існує слово } g \in A^* \text{ таке, що } x = gd \text{ і } dg \in J\big\}$$

для кожного слова $x \in X$. Таким чином, множина $D(x)$ складається з непорожніх суфіксів слова x. Більше того, множина $D(x)$ є непорожньою,оскільки $x \in D(x)$. Отож, для кожного слова $x \in X$ множина $D(x)$ містить деяке найкоротше слово. Це

ми використаємо для означення відображення відображення $\beta\colon X \to Y$ наступним чином. Для кожного слова $x \in X$ покладемо

$$\beta(x) = dg, \tag{3.17}$$

де d — найкоротше слово в $D(x)$, і слово g задовольняє умову

$$x = gd. \tag{3.18}$$

Отож, слово $\beta(x)$ є спряженим до слова x і $\beta(x) \in J$. Ми покажемо, що

$$\beta(x) \in J \setminus A^+J = Y.$$

Припустимо протилежне. Тоді

$$\beta(x) = dg = uj, \tag{3.19}$$

для деяких слів $u \in A^+$, $j \in J$.

Далі, нехай слово g є власним префіксом слова x. Тоді $g \notin J$. Справді, якщо $g \in J$, то слово g має мати префікс з множини X, а це суперечить тому, що множина X є префіксною. Звідси випливає, що $|g| < |j|$, оскільки в протилежному випадку слово g має належати до ідеала, породженого словом j, а отже отримуємо знову, що $g \in J$.

Звідси та з формули (3.19) випливає, що $|d| > |u|$, а отже $d = ud'$ для деякого слова $d' \in A^+$. Більше того, отримуємо $d' \in D(x)$, оскільки $d'(gu) = ju \in J$ і $(gu)d' = gd = x \in X$. Звідси отримуємо протиріччя, оскільки довжина слова d' є строго меншою за довжину слова d. Отож, $\beta(x) \in Y$.

Розглянемо обернене відображення $\gamma\colon Y \to X$, означене з урахуванням, для y в Y, множини

$$G(y) = \left\{e \in A^+ \colon y = eh \text{ і } he \in J\right\},$$

і поклавши $\gamma(y) = he$, зі словом $e \in G(y)$ мінімальної довжини.

Якщо $y = \beta(x) = dg$ визначається за формулами (3.17) і (3.18), і якщо $\gamma(y) = he$ з $e \in G(y)$, $eh = y$, то

$$dg = \beta(x) = eh. \tag{3.20}$$

Зауважимо, що $gd \in J$. Отож, $d \in G(y)$. Тому отримуємо, що $|d| \geqslant |e|$. Далі слово e не є власним префіксом слова d. Інакше поклавши $d = eu$, $ug = h$ у формулі (3.20) з $u \in A^+$, отримуємо

$$geu = gd = x \qquad \text{і} \qquad uge = he \in J,$$

стверджуючи, що $u \in D(x)$, а це суперечить мінімальності величини $|d|$. Отож, $d = e$, $g = h$ і $\gamma(\beta(x)) = x$. Аналогічне доведення показує, що $\beta(\gamma(y)) = y$ для $y \in Y$. Таким чином, β і γ є взаємно оберненими бієкціями. □

Приклад 3.5.17. Тепер проілюструємо конструкцію твердження 3.5.16 розглянувши, над алфавітом $A = \{a, b\}$, множину семафорів $S = \{a^2, ba, b^2\}$. Тоді

$$X = A^*S \setminus A^*SA^+ = \left\{a^2, ba, b^2, aba, ab^2\right\},$$
$$Y = SA^* \setminus A^+SA^* = \left\{a^2, a^2b, ba, bab, b^2\right\}.$$

У таблиці 3.2 наведено у кожному рядку елемент $x \in X$, відповідну множину $D(x)$ і елемент $\beta(x) \in Y$.

X	D	Y
aa	a, aa	aa
aba	a, ba, aba	aab
abb	b, bb, abb	bab
ba	ba	ba
bb	b, bb	bb

Табл. 3.2: Відповідність між множинами X і Y

Твердження 3.5.16 показує, що будь-який семафорний код може бути перетворений у суфіксний код за допомогою біекції, яка обмінюється спряженими словами. Ця властивість не виконується для довільних префіксних кодів, як викладено в наступному прикладі.

Приклад 3.5.18. Нехай $A = \{a, b, c\}$ і $X = \{ab, ba, c, ac, bca\}$. Припустимо, що існує спряження, яке зберігає бієкцію β, що відображає код X на суфіксний код Y. Тоді код Y обов'язково містить c, ab і ba. Далі код Y містить ca (з c і ac код Y не буде суфіксом). Усі слова, спряжені зі словом bca, тепер мають суфікси, які збігаються з одним зі слів c, ab, ba, чи ca. Таким чином, код Y не є суфіксним.

Фактично, код X не може бути поповненим у семафорному коді, оскільки літера c є множником слова bca.

Ми завершуємо цей підрозділ наступним результатом, який показує, що біфіксні коди зазвичай не є семафорними кодами.

Твердження 3.5.19. *Нехай $A \neq \varnothing$ і X — біфіксний семафорний код над алфавітом A. Тоді $X = A^n$ для деякого натурального числа $n \geqslant 1$.*

Доведення. Достатньо довести, що $X \subseteq A^n$ для деякого натурального числа $n \geqslant 1$. Нехай $x, y \in X$. Для кожного суфікса q слова x, маємо $qy \in A^*X \subseteq XA^*$. Отож, за твердженнями 3.5.4 і 3.5.6 існує префікс p слова y такий, що $qp \in X$.

Таким чином, ми означили відображення з множини суфіксів коду X у множину префіксів слова y. Оскільки множина X є суфіксною, то це відображення є ін'єктивним. Справді, якщо qp і $q'p$ є елементами коду X для двох суфіксів q, q' слова x, то $q = q'$. Звідси випливає, що $|x| \leqslant |y|$. Помінявши місцями слова x і y, отримуємо, що $|y| \leqslant |x|$. Таким чином, усі слова в коді X мають однакову довжину. □

3.6 Синхронізовані коди

Нехай $A \neq \varnothing$ і X — префіксний код над алфавітом A. Слово $w \in A^*$ називається *синхронізацією* коду X, якщо довільних слів $u, v \in A^*$ виконується умова

$$uwv \in X^* \quad \Longrightarrow \quad uw, wv \in X^*.$$

Зауважимо, якщо це виконується то слово v також міститься у вільному моноїді X^*, оскільки моноїд X^* є унітарним справа. Якщо слово w є синхронізацією коду X, то слово xwy є синхронізацією коду X для довільних слів $x, y \in X^*$.

Дане означення дає просту форму для слова-синхроізації коду X, яке є елементом вільного моноїда X^*. Це саме є той випадок, яким ми будемо цікавитися та вивчати. Слово w вільного моноїда X^* є його синхронізацією тоді і тільки тоді, коли для всіх слів $u, v \in A$ виконується умова

$$uwv \in X^* \quad \Longrightarrow \quad uw \in X^*.$$

Префіксний код X називається *синхронізованим*, якщо існує слово у вільному моноїді X^*, яке є синхронізацією коду X. Далі (див. розділ 10) ми означимо поняття синхронізованого коду для довільного коду.

Приклад 3.6.1. Нехай $A = \{a, b\}$. Префіксний код $X = \{ab, ba\}$ є синхронізованим. Справді, слово $abba$ є синхронізацією коду X, оскільки з $uabbav \in X^*$ випливає, що $uab, bav \in X^*$, а отже $uabba \in X^*$.

Якщо X — максимальний префіксний код, то слово w є синхронізацією коду X тоді і тільки тоді, коли

$$A^*w \subseteq X^*. \tag{3.21}$$

Справді, нехай слово w є синхронізацією коду X. Для довільного слова $u \in A^*$, оскільки моноїд X^* є щільним справа, то існує слово v таке, що $uwv \in X^*$. Тоді $uw \in X^*$. Таким чином, виконується умова (3.21). Навпаки, якщо виконується умова (3.21), то $uw \in X^*$ для всіх слів $u \in A^*$, а отже слово w є синхронізацією коду X.

Зауважимо, якщо X є максимальним префіксним кодом, то за умовою (3.21) кожне слово-синхронізація коду X є елементом вільного моноїда X^*.

Приклад 3.6.2. Нехай $A = \{a, b\}$. Код $X = b^*a$ є синхронізованим. Справді, слово a є синхронізацією коду X, оскільки $A^*a \subseteq X^*$.

Приклад 3.6.3. Максимальний біфіксний код X над над алфавітом A ніколи не є синхронізованим у випадку $X = A$. Припустимо, що слово $w \in A^*$ є синхронізацією. Для будь-якого слова $u \in A^*$ маємо, що $uw \in X^*$. Оскільки моноїд X^* є унітарним зліва, то $u \in X$. Отож, отримуємо рівність $A^* = X^*$.

Термінологія випливає з наступного спостереження: нехай w — слово, яке може бути розкладене в добуток в словах деякого префіксного коду X. З появи, в середині слова w, деякого слова синхронізації $x \in X^*$, тобто з існування факторизації

$$w = uxv$$

випливає, що $ux \in X^*$. Таким чином, ми можемо розпочати декодування з початку слова v. Оскільки множина X є унітарною справа, то насправді $w \in X^*$ тоді і тільки тоді, коли $v \in X^*$. Це означає, що це слово повністю знаходиться в множині X^* тоді і тільки тоді, коли його кінцеву частину можна декодувати.

Зауважимо, що довільний код X над алфавітом A, який задовольняє умову (3.21) є максимальним префіксним. Справді, нехай $y, yu \in X$. Тоді $uw \in X^*$, і $y(uw)$ та $(yu)w$ — дві X-факторизації, які є різними у випадку $u \neq 1$. Таким чином, отримуємо, що $u = 1$. Next, з умови (3.21)(3.21) випливає, що код X є повною справа множиною.

Довільний синхронізований префіксний код є тонким. Справді, якщо слово x є непорожньою синхронізацією префіксного коду X, то слово x^2 не є множником слова

з коду X, оскільки в цьому випадку $uxxv \in X$ для деяких слів $u, v \in A^*$. Тоді з умови $ux \in X^+$ випливало би, що множина X не є префіксною.

Той факт, що префіксний код X синхронізованим, добре зображається автоматами, що розпізнають моноїд X^*. Сформулюємо означення. Нехай $\mathcal{A} = (Q, i, T)$ — детермінований автомат на алфавіті A. *Ранг* слова $x \in A^*$ в автоматі $\mathcal{A}$ позначається через $\mathrm{rank}_{\mathcal{A}}(x)$ і визначається за формулою

$$\mathrm{rank}_{\mathcal{A}}(x) = \mathrm{Card}(Q \cdot x).$$

Очевидно, що $\mathrm{rank}_{\mathcal{A}}(x)$ є невід'ємним цілим числом, або дорівнює $+\infty$, і крім того виконується нерівність

$$\mathrm{rank}_{\mathcal{A}}(uxv) \leqslant \mathrm{rank}_{\mathcal{A}}(x),$$

для довільних слів $x, u, v \in A^*$.

Слово $w \in A^*$ називається *синхронізацією* в автоматі $\mathcal{A}$ над алфавітом A, якщо $\mathrm{rank}_{\mathcal{A}}(w) = 1$. Автомат $\mathcal{A}$ називається *синхронізованим*, якщо існує слово, яке є синхронізацією в $\mathcal{A}$.

Твердження 3.6.4. *Нехай X — префіксний код над непорожнім алфавітом A. Тоді наступні умови є еквівалентними:*

- (i) *X — синхронізований;*
- (ii) *літеральний автомат вільного моноїда X^* є синхронізованим;*
- (iii) *мінімальний автомат $\mathcal{A}(X^*)$ вільного моноїда X^* є синхронізованим;*
- (iv) *існує впорядкований синхронізований детермінований автомат, який розпізнає вільний моноїд X^*.*

Доведення. $(i) \Longrightarrow (ii)$ Нехай P — множина префіксів коду X і $\mathcal{A} = (P, 1, 1)$ — літерний автомат вільного моноїда X^*. Нехай Let $x \in X^*$ — синхронізація для коду X. Тоді стан 1 належить множині $P \cdot x$, а отже слово x має додатній ранг. Далі, нехай $p \in P$. Якщо $p \cdot x$ існує, то існує слово s таке, що $p \cdot xs = 1$. Тоді $pxs \in X^*$ і $px \in X^*$, оскільки слово x є сихронізацією, звідки випливає, що $p \cdot x = 1$. Таким чином, отримуємо, що $\mathrm{rank}_{\mathcal{A}}(x) = 1$.

$(ii) \Longrightarrow (iii)$ Слово синхронізація в літерному автоматі вільного моноїда X^* є також синхронізацією в автоматі $\mathcal{A}(X^*)$. Фактично будь-який фактор-автомат синхронізованого автомата є синхронізованим.

Імплікація $(iii) \Longrightarrow (iv)$ є очевидною.

$(vi) \Longrightarrow (i)$ Нехай $\mathcal{A} = (Q, i, T)$ — впорядкований автомат і $w \in A^*$ — таке слово, що $\mathrm{rank}_{\mathcal{A}}(w) = 1$. Існує шлях $p \xrightarrow{w} q$ в автоматі $\mathcal{A}$, і скільки автомат $\mathcal{A}$ є впорядкованим, то стан p є доступним, а стан q є кодоступним. Таким чином, існують слова z, y такі, що $x = zwy \in X^*$. Ми доведемо, що слово x є синхронізацією для кода X.

Нехай справді u, v — слова такі, що $uxv \in X^*$. Тоді стан $i \cdot ux$ є визначано, і оскільки $\mathrm{rank}_{\mathcal{A}}(x) = 1$, то $i \cdot ux = i \cdot x$. Отож, отримуємо, що $i \cdot ux \in T$ і $ux \in X^*$. □

Два стани p і q автомата $\mathcal{A}$ називаються *синхроїзовними*, якщо існує слово w таке, що

$$\mathrm{Card}\, p \cdot w, q \cdot w = 1.$$

Наступний результат складає основу алгоритму для обчислення синхроїзованого слова (див. вправу 3.10.13).

Твердження 3.6.5. *Нехай $\mathcal{A}$ — сильно зв'язний детермінований автомат, для якого існує слово зі скінченним ненульовим рангом. Тоді $\mathcal{A}$ є синхронізованим тоді і тільки тоді, коли довільні два стани автомата $\mathcal{A}$ є синхронізовними.*

Доведення. Нехай Q — множина станів автомата $\mathcal{A}$. Припустимо спочатку, що автомат $\mathcal{A}$ є синхронізованим. Нехай x — слово рангу 1 і r, s — два стани в Q такі, що $r \cdot x = s$. Нехай p, q — пара станів з Q. Оскільки автомат $\mathcal{A}$ є сильно зв'язним, то існує слово y таке, що $p \cdot y = r$, кожен раз, коли $p \cdot yx = s$. Якщо $q \cdot yx$ визначено, то $q \cdot yx = s$, а отже стани p і q є синхронізовними.

Навпаки, нехай x — слово мінімального ненульового рангу в автоматі $\mathcal{A}$. За припущенням, цей ранг є нескінченним. Ми доведемо, що $\mathrm{Card}(Q \cdot x) = 1$. Припустимо, що існують стани $p, q \in Q \cdot x$ таке, що $p \neq q$. Оскільки стати p і q є синхронізовними, то існує слово y таке, що $\mathrm{Card}\{p \cdot y, q \cdot y\} = 1$. Тоді $0 < \mathrm{rank}_{\mathcal{A}}(xy)$, оскільки $p \cdot y$ або $q \cdot y$ є непорожнім. Нехай $\mathrm{rank}_{\mathcal{A}}(xy) < \mathrm{rank}_{\mathcal{A}}(x)$, оскільки $p \neq q$, що суперечить мінімальності рангу слова x. Це доводить, що $\mathrm{Card}(Q \cdot x) = 1$, а отже автомат $\mathcal{A}$ є синхронізованим. □

Твердження 3.6.6. *Нехай X — тонкий максимальний префіксний код над алфавітом A та $P = XA^-$. Тоді код X є синхронізованим тоді і тільки тоді, коли для всіх $p \in P$ існує слово $x \in X^*$ таке, що $px \in X^*$.*

Доведення. Умова є необхідною. Справді, нехай $x \in X^*$ — синхронізація для коду X. Тоді з рівності (3.21) випливає, що $Px \subseteq X^*$.

Умова є також достатньою. Нехай $\mathcal{A} = (P, 1, 1)$ — літеральний автомат вільного моноїда X^*. Автомат $\mathcal{A}$ є повним, оскільки код X є максимальним. Оскільки код X є тонким і максимальним, то множина $\overline{F}(X) \cap X^*$ є непорожньою. Нехай $w \in \overline{F}(X) \cap X^*$. Ми доведемо, що слово w має скінченний додатній ранг. Очевидно, що $1 \in P \cdot w$, а отже множина $\overline{F}(X) \cap X^*$ є непорожньою. Далі, множина $P \cdot w$ складається з суфіксів слова w. Таким чином, вона є скінченною та слово w має скінченний ранг.

З огляду на твердження 3.6.5, нехай p, q — два стани в P. Існує слово u таке, що $pu \in X$. Нехай $r = q \cdot u$. За припущенням, існує слово $x \in X^*$ таке, що $rx \in X^*$. Таким чином, $p \cdot ux = 1$ і $q \cdot ux = r \cdot x = 1$, звідки випливає, що стани p і q є синхронізовними. □

Твердження 3.6.7. *Нехай X, Y і Z — максимальні префіксні коди такі, що $X = Y \circ Z$. Тоді код X є синхронізованим тоді і тільки тоді, коли коди Y і Z є синхронізованими.*

Доведення. Нехай $Y \subset B^*$, $X, Z \subset A^*$ і $\beta\colon B^* \to A^*$ — морфізм такі, що

$$X = Y \circ_\beta Z.$$

Спочатку припустимо, що Y і Z — синхронізовані коди і $y \in Y^*$, $z \in Z^*$ — синхронізації. Тоді $B^*y \subseteq Y^*$ і $A^*z \subseteq Z^*$, звідки отримуємо, що

$$A^*z\beta(y) \subseteq Z^*\beta(y) = \beta(B^*y) \subseteq \beta(Y^*) = X^*,$$

а це доводить, що слово $z\beta(y)$ є синхронізацією кода X. Навпаки, припустимо, що $A^*x \subseteq X^*$ для деякого слова $x \in X^*$. Тоді $x \in Z^*$ і $X^* \subseteq Z^*$, а отже слово x є синхронізацією коду Z. Далі, нехай $y = \beta^{-1}(x) \in Y^*$. Тоді

$$\beta(B^*y) = Z^*x \subseteq A^*x \subseteq X^* = \beta(Y^*).$$

Оскільки відображення $\beta\colon B^* \to A^*$ є ін'єктивним, то звідси випливає, що $B^*y \subseteq Y^*$. Звідси випливає, що код Y є синхронізованим. □

Приклад 3.6.8. Код $X = (A^2 \setminus b^2) \cup b^2A^2$ не є синхронізованим, оскільки він розкладається на кодом A^2, який не є синхронізованим (приклад 3.6.3). Також, безпосередньо легко побачити, що слово $x \in X^*$ не може нікоди синхронізувати слова непарної довжини.

Приклад 3.6.9. Для довільних максимального префіксного коду Z і натурального числа $n \geqslant 2$, код $X = Z^n$ не є синхронізованим. Справді, такий код має вигляд $X = B^n \circ Z$ для деякого алфавіта B, і код B^n є синхронізованим лише для $n = 1$ (приклад 3.6.3).

Тепер наведемо результат про префіксні коди, який буде узагальнено, коли будуть доступні інші методи (теорема **??**). Доведення цього факту є елементарним. Нагадаємо з розділу 2, що для скінченного коду X *порядком* літери a називається таке ціле число n, що $x^n \in X$.

Існування порядку елемента x випливає з твердження 2.5.15. Зауважимо, що для скінченного максимального префіксного коду це є безпосереднім наслідком включення $a^+ \subseteq X^*P$, з $P = XA^-$.

Теорема 3.6.10. *Нехай $X \subseteq A^+$ — скінченний максимальний префіксний код. Якщо порядки літер $a \in A$ є взаємно первинними числами*[2] *, то код X є синхронізованим.*

Доведення. Нехай $P = XA^-$ і $\mathcal{A} = (P, 1, 1)$ — літерний автомат вільного моноїда X^*. Цей автомат є повним, оскільки код X є максимальним префіксним. Нагадаємо, що його дія визначається за формулою

$$p \cdot a = \begin{cases} pa, & \text{якщо } pa \in P; \\ 1, & \text{якщо } pa \in X. \end{cases}$$

Покладемо $Q(w) = P \cdot w$ для всіх $w \in A^*$. Тоді

$$Q(w'w) \subseteq Q(w) \qquad \text{і} \qquad \operatorname{Card} Q(w'w) \leqslant \operatorname{Card} Q(w'), \tag{3.22}$$

для $w, w' \in A^*$. Зауважимо, що $\operatorname{Card}(Q(w)) = \operatorname{rank}_{\mathcal{A}}(w)$ для всіх $w \in A^*$.

Нехай $u \in A^*$ — слово таке, що величина $\operatorname{Card}(Q(u))$ є мінімальною. З того, що код X повною справа множиною випливає, що існує слово $v \in A^*$ таке, що $w = uv \in X^+$. За умовою (3.22) величина $\operatorname{Card}(Q(w))$ є мінімальною. Далі з $w \in X^+$ випливає, що

$$1 \in Q(w). \tag{3.23}$$

Ми доведемо, що $\operatorname{Card}(Q(w)) = 1$. Це доводить теорему з огляду на твердження 3.6.4.

Нехай $a \in A$ фіксована літера та n — додатне ціле число таке, що $a^n \in X$. Ми означимо дві множини цілих чисел I та K так:

$$I = \left\{ i \in \mathbb{N} \colon Q(w)a^i \cap X \neq \varnothing \right\},$$
$$K = \left\{ k \in \{0, \ldots, n-1\} \colon a^k w \in X^* \right\}.$$

[2] Взаємно первинні числа — натуральні або цілі числа, які не мають спільних дільників більших за 1, або, інакше кажучи, якщо їх найбільший спільний дільник дорівнює 1.

Спочатку ми покажемо, що

$$\operatorname{Card} I = \operatorname{Card}(Q(w)). \tag{3.24}$$

Справді, розглянемо слово $p \in Q(w) \subseteq P$. Існує ціле число i таке, що $pa^i \in X$, оскільки код X є скінченним і максимальним. Це ціле число є однозначно визначеним, оскільки в протилежному випадку код X не буде префіксним. Таким чином, існує відображення, яке ставить у відповідність кожній літері $p \in Q(w)$ ціле число i таке, що $pa^i \in X$. Це відображення є очевидно сюр'єктивним на множину I. Ми перевіримо, що це відображення є також ін'єктивним. Припустимо протилежне. Тоді $pa^i \in X$ і $p'a^i \in X$ для деяких слів $p, p' \in Q(w)$ таких, що $p \neq p'$. Звідси випливає, що $\operatorname{Card}(Q(wa^i)) < \operatorname{Card}(Q(w))$, що суперечить мінімальності значення $\operatorname{Card}(Q(w))$. Таким чином, так визначене відображення є бієктивним. Це доводить рівність (3.24). Далі, покладемо

$$m = \max\{i + k \colon i \in I, k \in K\}.$$

Очевидно, що

$$m = \max I + \max K \leqslant \max I + n - 1.$$

Нехай

$$R = \{m, m+1, \ldots, m+n-1\}.$$

Ми знайдемо бієкцію з $I \times K$ на R. Для цього, нехай $r \in R$ і для кожного слова $p \in Q(w)$, нехай

$$\nu(p) = p \cdot a^r w.$$

Тоді

$$\nu(p) = (p \cdot a^r) \cdot w \in P \cdot w = Q(w).$$

Таким чином, $\nu(Q(w)) \subseteq Q(w)$ і

$$\nu(Q(w)) = (P \cdot w) \cdot a^r w = P \cdot wa^r w = Q(wa^r w),$$

а отже з мінімальності множини $Q(w)$ випливає рівність $\nu(Q(w)) = Q(w)$. Отож, відображення ν є бієктивним відображенням множини $Q(w)$ на себе. З умови (3.23) випливає, що існує єдине слово $p_r \in Q(w)$ таке, що $p_r a^r w \in X^*$. Нехай i_r — єдине ціле число таке, що $p_r a^{i_r} \in X$. Таке ціле число існує, оскільки X є скінченним максимальним префіксним кодом. Тоді $i_r \in I$, звідки випливає, що $i_r \leqslant m \leqslant r$. Покладемо

$$r = i_r + \lambda n + k_r, \tag{3.25}$$

з $\lambda \in \mathbb{N}$ і $0 \leqslant k_r < n$. Це однозначно визначає величину k_r і ми маємо

$$p_r a_r w = \left(p_r a^{i_r}\right) (a^n)^\lambda \left(a^{k_r} w\right).$$

Оскільки $p_r a^{i_r} \in X$ і моноїд X^* є унітарним справа, то маємо $(a^n)^\lambda \left(a^{k_r} w\right) \in X^*$ і також $a^{k_r} w \in X^*$. Отож, $k_r \in K$. Попередня конструкція визначає відображення

$$R \longrightarrow I \times K, \quad r \mapsto (i_r, k_r) \tag{3.26}$$

спочатку визначенням значення i_r, а потім обчисленням значення k_r за допомогою формули (3.25). Це відображення є ін'єктивним. Справді, якщо $r \neq r'$, то або $i_r \neq i_{r'}$, або з формули (3.25) і з $r \not\equiv r' \mod n$ випливає, що $k_r \neq k_{r'}$.

Тепер ми покажемо, що відображення (3.26) є сюр'єктивним. Нехай $(i,k) \in I \times K$ і $\lambda \in \mathbb{N}$ — такі, що

$$r = i + \lambda n + k \in R.$$

За означенням множини I існує єдине слово $q \in Q(w)$ таке, що $qa^i \in X$, і за означенням множини K, маємо

$$qa^r w \in X^*.$$

отож, $q = p_r$, $i = i_r$, $k = k_r$, що доводить об'єктивність даного відображення.

З бієктивності випливає, що

$$n = \operatorname{Card}(R) = \operatorname{Card}(I) \operatorname{Card}(K).$$

Це, у свою чергу, передбачає рівність (3.24), що $\operatorname{Card} Q(w)$ ділить ціле число n. Таким чином $\operatorname{Card} Q(w)$ ділить порядок кожної літери в алфавіті. Оскільки ці порядки взаємно первинними, то $\operatorname{Card} Q(w) = 1$. □

Приклад 3.6.11. Нехай $A = \{a, b\}$ і $X = (A^2 \setminus b^2) \cup b^2 A$. Порядок алфавіта A дорівнює 2, а порядок літери b дорівнює 3. Таким чином, код X є синхронізованим за теоремою 3.6.10 і справді слово $abba$ є синхронізацією.

Пізніше (підрозділ 11.2) ми доведемо таку важливу теорему.

Теорема 3.6.12 (Шютценбергер). *Нехай X — семафорний код. Тоді існує синхронізований семафорний код Z і ціле число d такі, що*

$$X = Z^d.$$

З цього результату випливає твердження 3.5.19 як особливий випадок. Розглянемо справді біфіксний семафорний код $X \subseteq A^+$. Тоді за теоремою 3.6.12 маємо $X = Z^d$ зі синхронізованим кодом Z. Оскільки код X є біфіксним, то код Z є також біфіксним (твердження 3.4.12), але біфіксний синхронізований код є тривіальним за прикладом 3.6.3. Таким чином, $Z = A$ і $X = A^d$.

Теорема 3.6.12 простим чином описує структуру семафорних кодів, які не є синхронізованими.

Ми можемо запитати, чи існує таке описання для загальних префіксних максимальних кодів: *чи правда, що нерозкладний максимальний префіксний код X є біфіксним або синхронізованим?* На жаль, це не так, навіть коли код X є скінченним, як це показано в наступному прикладі.

Приклад 3.6.13. Нехай $A = \{a, b\}$ і X — префіксний код з автоматом $\mathcal{A}(X) = (Q, 1, 1)$, чиї переходи наведені в таблиці 3.3.

Q	1	2	3	4	5	6	7	8	9
a	2	3	1	1	3	8	9	3	1
b	4	6	7	5	1	4	1	5	1

Табл. 3.3: Переходи автомата $\mathcal{A}(X^*)$

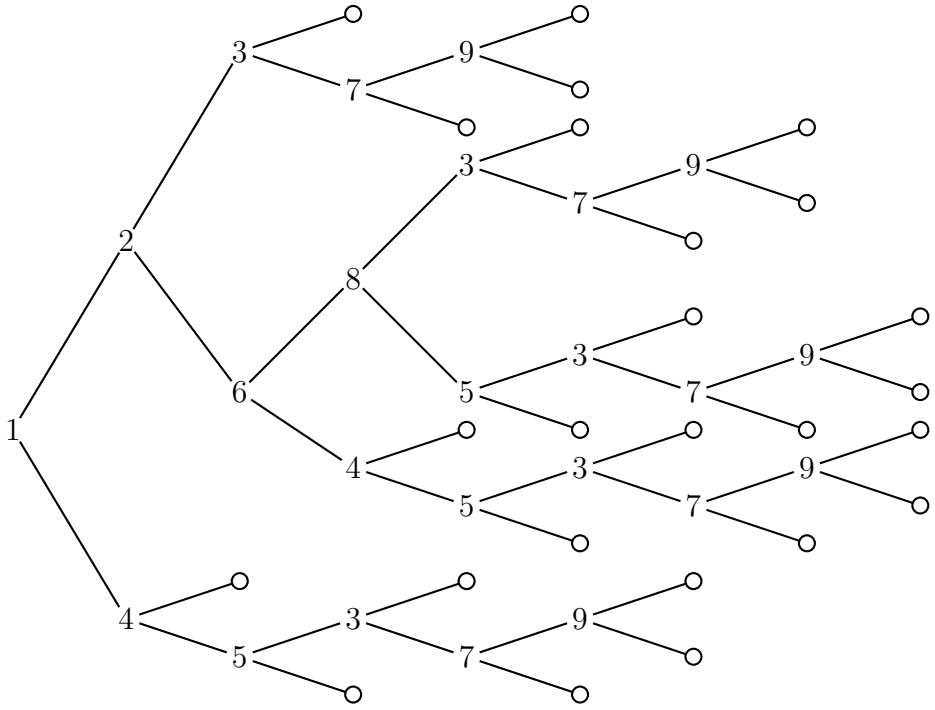


Рис. 3.30: Нерозкладний код, який не є синхронізованим

Автомат $\mathcal{A}(X^*)$ є повним, а отже код X є максимальним префіксним. Насправді, код X є скінченним і його зображено на рис. 3.30,

Для доведення того факту, що код X не є синхронізованим, зауважимо, що дія літер a та b зберігає глобально множини станів

$$\{1,2,3\}, \qquad \{1,4,5\}, \qquad \{4,6,7\}, \qquad \{1,8,9\}$$

як це показано на рис. 3.31, Звідси випливає, що код X не є синхронізованим. Справді,

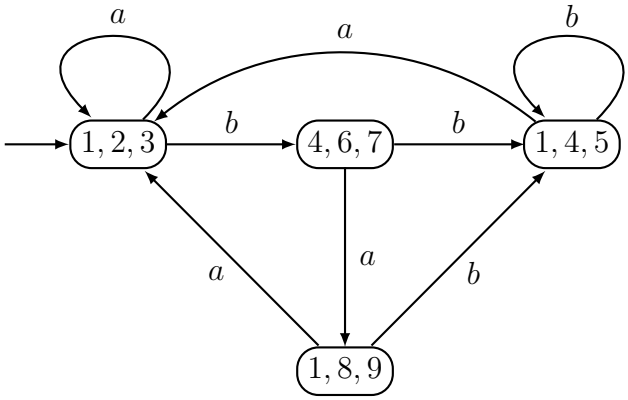


Рис. 3.31: Дія літер a та b

припустимо, що слово $x \in X^*$ є синхронізацією. Тоді за означенням $A^*x \subseteq X^*$, звідки

випливає, що $q \cdot x = 1$ для всіх станів $q \in Q$. Таким чином, для кожного з трьох елементів підмножини I будемо мати $I \cdot x = \{1\}$.

Далі код X не є біфіксним, оскільки $b3, ab^4 \in X$. Нарешті, перевірка на рис. 3.30 показує, що код X є нерозкладним.

Означимо канонічний розклад префіксного коду, що називається його *максимальним розкладом*. Це використовується для того, щоб показати в главі 11, що лише максимальні префіксні коди можуть створювати нетривіальні групи композицією.

Твердження 3.6.14. *Нехай $X \subseteq A^+$ — префіксний код. Нехай $D = X^*(A^*)^{-1}$ — множина префіксів вільного моноїда X^*. Множина*

$$U = \left\{u \in A^* \colon u^{-1}D = D\right\}$$

є унітарним справа підмоноїдом вільного моноїда A^*. Нехай Z — префіксний код, породжуючий моноїд U. Код X розкладається як

$$X = Y \circ Z, \tag{3.27}$$

де Y — максимальний префіксний код.

Доведення. Зауважимо спочатку, що $U \subseteq D$. Нехай $u \in U$. Оскільки $1 \in D$, то $1 \in u^{-1}D$, звідки випливає, що $u \in D$.

Множина U є підмоноїдом вільного моноїда A^*. Справді, нехай $u, v \in U$. Тоді з

$$(uv)^{-1}D = v^{-1}u^{-1}D = v^{-1}D = D$$

випливає, що $uv \in U$. Припустимо далі, що $u, uv \in U$. Тоді $u^{-1}D = D$ і

$$v^{-1}D = v^{-1}u^{-1}D = (uv)^{-1}D = D.$$

Таким чином, моноїд U є унітарним справа.

Ми маємо, що $X^* \subseteq Z^* = U$. Справді, моноїд X^* є унітарним справа. Таким чином, $x^{-1}X^* = X^*$ для всіх $x \in X^*$. Звідси випливає, що

$$x^{-1}D = x^{-1}\left(X^*(A^*)^{-1}\right) = \left(x^{-1}X^*\right)(A^*)^{-1} = X^*(A^*)^{-1} = D.$$

Ми перевіримо, що для слова $u \in U$ існує слово $v \in U$ таке, що $uv \in X^*$. Справді, нехай $u \in U$. Тоді $u \in D$, а отже $uv \in X^*$ для деякого слова $v \in A^*$. Позаяк $X^* \subseteq U$ то маємо $u, uv \in U$, і використавши той факт, що моноїд U є унітарним справа, отримуємо, що $v \in U$. Випадок доводить, що код X розкладається над кодом Z. Нехай код Y є таким, що $X = Y \circ Z$. Тоді за твердженням 2.6.13 код Y є префіксним. Твердження також доводить, що код Y є повним справа, а отже Y є префіксним максимальним кодом. □

Можна довести (див. вправу 3.10.16), що для довільного іншого розкладу $X = Y' \circ Z'$ з префіксним кодом Z' і максимальним префіксним кодом Y', маємо, що $Z'^* \subseteq Z^*$. Це обґрунтовує назву *максимальний розклад* префіксного коду X, наданого розкладом (3.27).

У випадку, коли X є максимальним префіксним кодом, множина D визначена вище, збігається з вільним моноїдом A^*. Отож, $U = A^*$ і $Z = A$ в (3.27). Таким чином, максимальний розклад, у цьому випадку є тривіальним.

Приклад 3.6.15. Нехай $A = \{a, b\}$ і $X = \{aa, aba, ba\}$. Максимальним розкладом коду X є $X = Y \circ Z$, з $Y = \{uu, uv, v\} \subseteq B^+$, $B = \{u, v\}$ і $Z = \{a, ba\}$.

3.7 Рекурентні події

Результати розділу 2 щодо розподілів Бернуллі застосовуються, звичайно, до префіксних кодів. Однак для цих кодів існують важливі розширення в двох напрямках. По-перше, властивості доведені в розділі 2 виконується і для розподілів ймовірностей, які є набагато більш загальними, ніж розподіли Бернуллі. По-друге, існує чудова комбінаторна інтерпретація середньої довжини префіксного коду за допомогою суми ймовірностей його власних префіксів (твердження 3.7.12).

Наступний результат показує, що для префіксного коду теорема 2.4.5 виконується для довільного розподілу імовірностей.

Твердження 3.7.1. *Нехай $A \neq \varnothing$ і π — розподіл імовірностей на вільному моноїді A^*. Тоді $\pi(X) \leqslant 1$ для довільного префіксного коду X на A^*.*

Доведення. Нагадаємо, що через $A^{[n]}$ позначається множина слів довжини не більше за натуральне число n. Для $x \in X \cap A^{[n]}$ маємо $\pi(x) = \pi(xA^{n-|x|})$ за умовою когерентності. Далі, множини $xA^{n-|x|}$ для $x \in X \cap A^{[n]}$ є попарно диз'юнктними, оскільки код X є префіксним. Отже

$$\sum_{x \in X \cap A^{[n]}} \pi\left(xA^{n-|x|}\right) = \pi\left(\bigcup_{x \in X \cap A^{[n]}} xA^{n-|x|}\right) \leqslant \pi(A^n) = 1.$$

Звідси випливає, що для довільного натурального числа n маємо, що

$$\pi\left(X \cap A^{[n]}\right) = \sum_{x \in X \cap A^{[n]}} \pi(x) = \sum_{x \in X \cap A^{[n]}} \pi\left(xA^{n-|x|}\right) \leqslant \pi(A^n) = 1.$$

Таким чином, отримуємо, що $\pi\left(X \cap A^{[n]}\right) \leqslant 1$ натурального числа n. Взявши границю для $n \to \infty$, отримуємо, що $\pi(X) \leqslant 1$. □

Твердження 3.7.2. *Нехай π — розподіл імовірностей на вільному моноїді A^*. Тоді $\pi(X) = 1$ для довільного скінченного максимального префіксного коду X.*

Доведення. Нехай n — натуральне число, яке більше за максимальну довжину слів у коді X. Оскільки префіксний код X є максимальним, то X — повна справа множина, а отже кожне слово довжини n має єдиний префікс в X. Звідси випливає, що

$$\pi(X) = \sum_{x \in X} \pi(x) = \sum_{x \in X} \pi\left(xA^{n-|x|}\right) = \pi(A^n) = 1.$$

Твердження доведено. □

Наступне правило обчислення буде корисним.

Лема 3.7.3. *Нехай $X \subset A^+$ — префіксний код. Тоді $\pi(p) = \pi(pA^* \cap X)$ для кожного імовірнісного розподілу π на вільному моноїді такого, що $\sum_{x \in X} \pi(x) = 1$ і для кожного префікса p слова коду X.*

Доведення. Спочатку припустимо, що $\pi(p) = 0$. Тоді, використавши умову когерентності, отримуємо, що $\pi(x) = 0$ для кожного слова $x \in pA^* \cap X$. Таким чином виконується висновок. В іншому випадку покладемо $Y = p^{-1}X$ і $Z = X \setminus pY$. Легко перевірити, що функція ρ, визначена на вільному моноїді A^* за формулою $\rho(u) = \pi(pu)/\pi(p)$ є розподілом ймовірностей. Позаяк Y і $Z \cup p$ є префіксними кодами, то маємо $\rho(Y) \leqslant 1$ і $\pi(p) + \pi(Z) \leqslant 1$, за твердженням 3.7.1. Оскільки $X = pY \cup Z$, то маємо

$$1 = \pi(pY) + \pi(Z) \leqslant \pi(p) + \pi(Z) \leqslant 1.$$

Отож, отримуємо рівність $\pi(pY) = \pi(p)$. □

Рекурентна подія на алфавіті A — це пара, яка складається з префіксного коду X на алфавіті A і розподілу ймовірностей π на A^*, що є мультиплікативний на X^*, тобто таким, що $\pi(xy) = \pi(x)\pi(y)$ для всіх $x, y \in X^*$. Наприклад, пара префіксного коду та розподілу Бернуллі є рекурентною подією.

Термінологія позичена з теорії ймовірностей. Розглянута подія — це членство в X^* префіксів слова, отриманого послідовністю випробувань, що визначають його літери зліва направо відповідно до ймовірності π. Більш точне формулювання буде викладено в розділі 13.

Рекурентна подія (X, π) називається *постійною*, якщо $\pi(X) = 1$ і *перехідною* в іншому випадку. У термінах теорії ймовірностей, подія є стійкою, якщо вона відбувається хоча б один раз з ймовірністю 1.

Твердження 3.7.2 показує, що рекурентна подія (X, π) є постійною, якщо X є скінченним максимальним префіксним кодом.

Приклад 3.7.4. Нехай π — додатній розподіл Бернуллі на вільному моноїді A^* і X — тонкий максимальний префіксний код. Тоді рекурентна подія (X, π) є постійною за теоремою 2.5.16.

Приклад 3.7.5. Нехай D — код Дика з прикладу 2.4.11 і π — розподіл Бернуллі на вільному моноїді $\{a, b\}^*$. Покладемо $p = \pi(a)$ і $q = \pi(b)$. Тоді $\pi(X) = 1 - |p - q|$. Отже рекурентна подія (D, π) є перехідною, коли $p \neq q$, і є постійною для $p = q$.

Нехай $\beta\colon B \to X$ — кодовий морфізм з префіксного коду X, що є бієкцією між вихідним алфавітом B і кодом X і продовжений до ін'єктивного морфізму з B^* в A^*. Постійна рекурентна подія (X, π) визначає розподіл Бернуллі μ на B^* так:

$$\mu(b) = \pi(\beta(b)), \qquad \text{для всіх літер} \quad b \in B.$$

Оскільки розподіл імовірностей π є мультиплікативною функцією на коді X^*, тоді маємо

$$\mu(w) = \pi(\beta(w)), \qquad \text{для всіх слів} \quad w \in B^*.$$

Наступний результат показує, що навпаки розподіл Бернуллі на вихідному алфавіті визначає єдиним чином рекурентну подію.

Твердження 3.7.6. *Нехай A — непорожній алфавіт, X — префіксний код над A і $\sigma\colon X \to [0, 1]$ — відображення таке, що $\sum_{x \in X} \sigma(x) = 1$. Тоді існує єдиний розподіл імовірностей π на A^*, який збігається з відображенням σ на X і пара (X, π) є рекурентною подією. Більше того,*

$$\pi(xw) = \pi(x)\pi(w) \qquad \textit{для всіх} \quad x \in X^* \quad \textit{і} \quad w \in A^*.$$

Доведення. Нехай $P = A^* \setminus XA^*$. Ми спочатку доведемо існування розподілу ймовірностей π. Для $x_1, \ldots, x_n \in X$ і $p \in P$ покладемо

$$\pi(x_1 \cdots x_n p) = \sigma(x_1) \cdots \sigma(x_n)\sigma(pA^* \cap X).$$

Оскільки $A^* = X^*P$ і факторизація є необлямованою, це визначає функцію π на вільному моноїді A^*. Останні дві формули є безпосереднім наслідком означення, оскільки для $w = yp$ з $y \in X^*$ і $p \in P$, маємо

$$\pi(xw) = \pi(xyp) = \pi(x)\pi(y)\pi(p) = \pi(x)\pi(w).$$

Тоді за означенням розподіл імовірностей π є мультиплікативною функцією на вільному моноїді X^* і збігається з відображенням σ на X. Ми тепер доведемо, що розподіл імовірностей π задовольняє умову когерентності. Маємо

$$pA^* \cap X = pAA^* \cap X = \bigcup_{a \in A} paA^* \cap X,$$

для довільного слова $p \in P$, оскільки $p \notin X$, а отже

$$\pi(p) = \sigma(pA^* \cap X) = \sum_{a \in A} \sigma(paA^* \cap X) = \sum_{a \in A} \pi(pa).$$

це доводить, що $\pi(w) = \sum_{a \in A} \pi(wa)$ для довільного слова $w \in A^*$. Це доводить те, що функція π є розподілом імовірностей.

Для доведення єдиності, припустимо, що функція π' — є розподілом імовірностей таким, що $\pi'(x) = \sigma(x)$ для всіх слів $x \in X$ і сама функція π' є мультиплікативною на вільному моноїді X^*. Зауважимо спочатку, що функції π і π' збігаються на X^*, оскільки обидві є мультиплікативними на X^* і збігаються на X.

Розглянемо слово $w \in A^*$ і нехай $w = xp$ з $x \in X^*$ і $p \in P$. Нехай n — натуральне число таке, що $x \in X^n$. Тоді, використавши лему 3.7.3 до префіксного коду X^{n+1} і до розподілу ймовірностей π', ми отримуємо $\pi'(wA^* \cap X^{n+1}) = \pi'(w)$. Позаяк $\pi'(wA^* \cap X^{n+1}) = \pi(wA^* \cap X^{n+1}) = \pi(w)$, то отримуємо, що $\pi(w) = \pi'(w)$. □

Приклад 3.7.7. Нехай $A = \{a, b\}$ і $X = \{a, ba\}$. Нехай $p, q \geqslant 0$ — такі, що $p + q = 1$ і відображення σ визначено наступним чином $\sigma(a) = p$ і $\sigma(ba) = q$. Єдиний розподіл імовірностей, який є мультиплікативною функцією на вільному моноїді X^* і збігається з σ на X задовольняє умови

$$\pi(aw) = p\pi(w), \qquad \pi(baw) = q\pi(w) \qquad \text{і} \qquad \pi(b^2w) = 0,$$

для всіх $w \in A^*$. Зауважимо, що $\pi(b) = q$, оскільки $\pi(bA^* \cap X) = \pi(ba)$.

Твердження 3.7.8. *Нехай $A \neq \varnothing$ і X — код над алфавітом A. Тоді для довільної постійної рекурентної події (X, π) над алфавітом A такої, що $\pi(x) > 0$ для $x \in X$, існує стохастичний автомат множина станів, якого є множиною префіксів коду X, що визначає розподіл імовірностей π.*

Доведення. Нехай Q — множина префіксів коду X і $A = (Q, 1, 1)$ — літерний автомат вільного моноїда X^*. Ми конвертуємо цей автомат у ваговий автомат (Q, I, T), поклавши

$$I(1) = 1 \quad \text{і} \quad I(q) = 0 \quad \text{для} \quad q \neq 1 \qquad \text{і} \qquad T(q) = 1 \quad \text{для всіх} \quad q \in Q.$$

Асоційована матриця зображення визначається так:

$$\mu(a)_{p,q} = \begin{cases} \pi(pa)/\pi(p), & \text{якщо } p \cdot a = q; \\ 0, & \text{в іншому випадку.} \end{cases}$$

З умови когерентності випливає, що

$$\sum_{a \in A} \mu(a)_{p,q} = \frac{1}{\pi(p)} \sum_{a \in A} \pi(pa) = 1.$$

Таким чином, автомат (Q, I, T) є стохастичним. Ми доведемо, що

$$\mu(w)_{p,q} = \begin{cases} \pi(pw)/\pi(p), & \text{якщо } p \cdot w = q; \\ 0, & \text{в іншому випадку,} \end{cases}$$

індукцією по довжині слова w. Випадок $|w| = 0$ є очевидним. Далі, нехай $a \in A$ і $w \in A^*$. Для стану $p \in Q$ такого, що значення $p \cdot aw$ визначено, покладемо $r = p \cdot a$ та $q = r \cdot w$. Тоді

$$\mu(aw)_{p,q} = \mu(a)_{p,r} \mu(w)_{r,q}.$$

Отже, отримуємо, що

$$\mu(aw)_{p,q} = \frac{\pi(pa)}{\pi(p)} \cdot \frac{\pi(rw)}{\pi(r)}.$$

Якщо $r \neq 1$, то маємо, що $r = pa$ і

$$\mu(aw)_{p,q} = \frac{\pi(paw)}{\pi(p)}.$$

Якщо $r = 1$, то $pa \in X$ і

$$\mu(aw)_{p,q} = \frac{\pi(pa)\pi(w)}{\pi(p)}.$$

Оскільки $\pi(pa)\pi(w) = \pi(paw)$ за твердженням 3.7.6, то формула

$$\mu(aw)_{p,q} = \frac{\pi(paw)}{\pi(p)}.$$

виконується і в цьому випадку. Звідси випливає, що

$$(|A|, w) = I\mu(w)T = \sum_{q \in Q} \mu(w)_{1,q} = \mu(w)_{1,1 \cdot w} = \pi(w).$$

Твердження доведено. □

Приклад 3.7.9. Нехай $A = \{a, b\}$ і $X = \{a, ba\}$ (див. приклад 3.7.7). Розподіл імовірностей π визначається матрицями

$$\mu(a) = \begin{bmatrix} p & q \\ 1 & 0 \end{bmatrix} \qquad \text{і} \qquad \mu(b) = \begin{bmatrix} 0 & q \\ 0 & 0 \end{bmatrix}.$$

Нехай (X, π) — рекурентна подія на алфавіті A. Нагадаємо з розділу 1, що

$$F_X(t) = \sum_{n \geqslant 0} \pi(X \cap A^n) t^n \qquad \text{і} \qquad F_{X^*}(t) = \sum_{n \geqslant 0} \pi(X^* \cap A^n) t^n$$

є ймовірністю породжуючого ряду коду X і вільного моноїда X^*. Наступний результат було доведено для довільних кодів у розділі 1 (твердження 2.4.3) у випадку розподілів Бернуллі.

Твердження 3.7.10. *Для кожної рекурентної події (X, π) виконується рівність*

$$F_{X^*}(t) = \frac{1}{1 - F_X(t)}.$$

Доведення. Оскільки множини X^k для натуральних k є попарно диз'юнктними, то

$$F_{X^*}(t) = \sum_{n \geqslant 0} \pi(X^* \cap A^n) t^n = \sum_{n \geqslant 0} \sum_{k \geqslant 0} \pi(X^k \cap A^n) t^n.$$

Звідси випливає, що

$$F_{X^*}(t) = \sum_{n \geqslant 0} \sum_{k \geqslant 0} \pi(X^k \cap A^n) t^n = \sum_{k \geqslant 0} F_{X^k}(t).$$

Оскільки відображення π є мультиплікативним на X^*, то маємо, що $\pi(X^n) = \pi(X)^n$, і звідси випливає, що $F_{X^n}(t) = F_X(t)^n$, за тими ж самими аргументами, як і в доведенні твердження 2.4.3. Таким чином, отримуємо

$$F_{X^*}(t) = \sum_{n \geqslant 0} F_X(t)^n.$$

Звідси випливає формула. □

Для множини K слів і розподілу ймовірностей π таких, що $\pi(K) = 1$, *середня довжина* множини K стосовно до розподілу π визначається за формулою

$$\lambda(K) = \sum_{x \in K} |x| \pi(x).$$

Середня довжина є невід'ємним дійсним числом або є нескінченною. Контекст завжди вказує, що є основним розподілом ймовірностей. Тому ми опускаємо посилання на нього в позначеннях.

Величина $\lambda(K)$ є фактично середньою випадковою величиною, що присвоює кожному слову $x \in K$ його довжину $|x|$.

Оскільки Since $\lambda(K) = \sum_{n \geqslant 0} n\pi(K \cap A^n)$, то ми маємо наступну корисну формулу для постійних подій.

Твердження 3.7.11. *Якщо (X, π) — постійна рекурентна подія, то*

$$\lambda(X) = F'_X(1).$$

Твердження 3.7.12. *Нехай (X, π) — постійна рекурентна подія та $P = XA^- -$ множина власних префіксів елементів множини X. Тоді $\lambda(X) = \pi(P)$.*

Доведення. За твердженням 3.7.6, для кожного слова $p \in P$ маємо $\pi(pA^* \cap X) = \pi(p)$. Тоді

$$\pi(P) = \sum_{p \in P} \pi(pA^* \cap X) = \sum_{x \in X} \sum_{p < x} \pi(x) = \sum_{x \in X} \pi(x)|x|,$$

остання рівність, що випливає з того, що кожен член $\pi(x)$ появляється рівно $|x|$ разів у сумі. □

З тверджень 3.7.2 і 3.7.12 випливає

Наслідок 3.7.13. *Нехай X — скінченний максимальний префіксний код над алфавітом A і $P = XA^-$. Тоді $\lambda(X) = \pi(P)$ для довільного розподілу ймовірностей π на вільному моноїді A^*.*

Для розподілу Бернуллі умова скінченності коду може бути замінена умовою, бути тонким.

Наслідок 3.7.14. *Нехай X — тонкий максимальний префіксний код над алфавітом A і $P = XA^-$. Тоді для довільного додатнього розподілу Бернуллі π на вільному моноїді A^* рекурентна подія (X, π) є постійною і виконується рівність $\lambda(X) = \pi(P)$. Більше того, середня довжина $\lambda(X)$ є скінченною.*

Доведення. Позаяк код X є максимальним, то з теореми 2.5.16 випливає рівність $\pi(X) = 1$. Отож, рекурентна подія (X, π) є постійною та рівність $\lambda(X) = \pi(P)$ випливає з твердження 3.7.12. Більше того, множина P є тонкою, оскільки кожен множник слова в множині P є також множником слова в коді X. За твердженням 2.5.12 образ $\pi(P)$ є скінченним. □

У розділі 13 ми побачимо, що середня довжина все ще є скінченною в більш загальному випадку тонких максимальних кодів.

Приклад 3.7.15. Нехай $A = \{a, b\}$ і $X = a^*b$ і π — додатній розподіл Бернуллі. Тоді

$$\lambda(X) = \pi(a^*) = \frac{1}{\pi(b)}.$$

Приклад 3.7.16. Нехай D — код Дика над алфавітом $A = \{a, b\}$ (див. приклад 2.4.11). Для однорідного розподілу Бернуллі виконується рівність

$$F_D(t) = 1 - \sqrt{1 - t^2}.$$

Тоді маємо, що

$$F'_D(t) = \frac{2t}{\sqrt{1 - t^2}}.$$

Таким чином, для рівномірного розподілу Бернуллі код Дика визначає постійну рекурентну подію, але середня довжина його є нескінченною.

Приклад 3.7.17. Нагадаємо з прикладу 3.4.4, що код Ґоломба-Райса порядку k визначається регулярним виразом

$$GR_k = 1^*0(0+1)^k. \tag{3.28}$$

Для розподілу Бернуллі π з $\pi(0) = p$ і $\pi(1) = q$, відповідним імовірнісним породжуючим рядом є

$$F_{GR_k}(t) = \sum_{n\geqslant 0} \frac{pt^{k+1}}{1-qt}.$$

Отож,

$$\pi(GR_k) = F_{GR_k}(1) = 1.$$

Середню довжину можна обчислити безпосередньо, як

$$F'_{GR_k}(1) = k + 1/p.$$

Ми можемо також обчислити це значення обчисленням значення $\pi(P)$, де P — множина власних префіксів множини GR_k. Звідси отримуємо, що

$$P = 1^* \cup 1^*0 \left(\bigcup_{0\leqslant i<k} \{0,1\}^i \right).$$

Позаяк $\pi(1^*) = 1/p$ і $\pi(1^*0) = 1$, то маємо

$$\pi(P) = 1/p + \sum_{0\leqslant i<k} \pi(1^*0)\pi(\{0,1\}^i) = 1/p + k.$$

Тепер розглянемо обчислення середньої довжини семафорних кодів. Почнемо з цікавої тотожності.

Твердження 3.7.18. *Нехай $X \subset A^+$ — семафорний код, $P = XA^-$ і S — мінімальна множина, для якої $X = A^*S \setminus A^*SA^+$. Нехай*

$$X_s = X \cap A^*s \qquad і \qquad R_{s,t} = \{w \in A^* \colon sw \in A^*t \text{ і } |w| < |t|\}.$$

для $s, t \in S$. Тоді

$$\underline{Pt} = \sum_{s\in S} \underline{X_s}\ \underline{R_{s,t}}. \tag{3.29}$$

для всіх $t \in S$.

Доведення. Спочатку ми зауважимо, що кожен добуток $X_sR_{s,t}$ є однозначним, оскільки код X_s є префіксним. Далі довільні два доданки суми є диз'юнктними, оскільки множина $X = \bigcup X_s$ є префіксною. Таким чином, достатньо довести, що

$$Pt = \bigcup_{s\in S} X_sR_{s,t}.$$

Спочатку нехай $p \in P$ та x — найкоротший префікс слова pt, який міститься в A^*S. Тоді $x \in X$ і

$$pt = xw$$

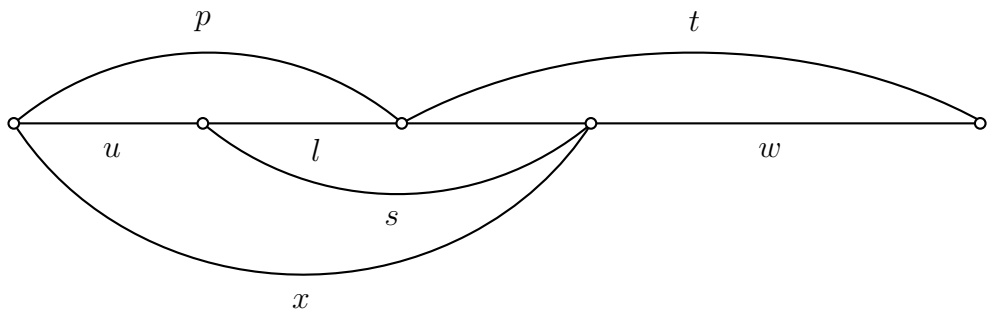


Рис. 3.32: Факторизація слова pt

для деякого слова $w \in A^*$. Далі $x \in X_s$ для деякого $s \in S$. Покладемо $x = us$. Оскільки слово $p \in P$, то маємо $|p| < |x|$, звідки отримуємо, що $|w| < |t|$ (див. рис. 3.32). Тепер слово p не може бути власним префіксом слова u, оскільки в протилежному випадку слово s мало б бути власним множником слова t, а це суперечить твердженню 3.5.11 і мінімальності множини S. Таким чином, слово u є префіксом слова p і $sw \in A^*t$, а це доводить, що $w \in R_{s,t}$.

Навпаки, нехай $x \in X_s$ і $w \in R_{s,t}$ для деяких $s, t \in S$. Тоді $x = us$ і $sw = lt$ для власного префікса l слова s. Тоді слово ul э власним префіксом слова $us = x$, а отже $ul \in P$ і $xw = ult \in Pt$. □

Наслідок 3.7.19. *Нехай $X \subset A^+$ — семафорний код, $P = XA^-$ і S — мінімальна множина, для якої $X = A^*S \setminus A^*SA^+$. Нехай*

$$X_s = X \cap A^*s \qquad і \qquad R_{s,t} = \{w \in A^* \colon sw \in A^*t \text{ і } |w| < |t|\}.$$

для $s, t \in S$. Тоді для довільного розподілу Бернуллі π виконується наступна система рівнянь:

$$\lambda(X)\pi(t) = \sum_{s \in S} \pi(X_s)\pi(R_{s,t}), \qquad (t \in S), \tag{3.30}$$

$$\sum_{s \in S} \pi(X_s) = 1. \tag{3.31}$$

Доведення. Рівняння (3.30) випливає з рівняння (3.29) застосуванням розподілу Бернуллі π до двох боків і зауваживши, що $\lambda(X) = \pi(P)$. Рівняння (3.31) випливає з того, що X є диз'юнктним об'єднання кодів X_s і сам X є тонким максимальним кодом. □

У випадку скінченної множини S система (3.30)–(3.30) складається з $1 + \mathrm{Card}(S)$ лінійних рівнянь і з $1 + \mathrm{Card}(S)$ невідомих змінних $\pi(X_s)$ і $\lambda(X)$. Це дає метод для обчислення значення $\lambda(X)$. У окремому випадку, коли множина S є одноточковою, то виконується таке твердження:

Наслідок 3.7.20. *Нехай $s \in A^+$, $X = A^*s \setminus A^*sA^+$ і*

$$R = \{w \in A^* \colon sw \in A^*s \quad і \quad |w| < |s|\}.$$

Тоді

$$\lambda(X) = \frac{\pi(R)}{\pi(s)},$$

для довільного розподілу Бернуллі π.

Приклад 3.7.21. Нехай $A = \{a, b\}$ і $s = aba$. Відповідна множина R має вигляд $R = \{1, ba\}$. Поклавши $p = \pi(a)$ і $q = \pi(b) = 1 - p$, отримуємо

$$\lambda(X) = \frac{1 + pq}{p^2 q}$$

для $X = A^*aba \setminus A^*abaA^+$. Тепер, виберемо $s' = baa$. Відповідна множина R' має вигляд $R' = \{1\}$. Таким чином, маємо

$$\lambda(X) = \frac{1}{pq^2}$$

для $X' = A^*baa \setminus A^*baaA^+$. Для $p = q = 1/2$, це дає

$$\lambda(X) = 10 \qquad \text{і} \qquad \lambda(X') = 8.$$

Це цікавий парадокс: ми повинні довше чекати першої появи слова aba, ніж на першу появу слова baa!

3.8 Розподіли довжин

Нехай X — префіксний код на алфавіті A з k літерами. Нехай $f_X(z) = \sum_{n\geqslant 0} u_n z^n$ з $u_n = \mathrm{Card}(X \cap A^n)$. Нагадаємо, що послідовність (u_n) є *розподілом довжини* коду X і f_X є породжуючим рядом кода X.

За теоремою 2.4.13 маємо, що $f_X(1/k) = \sum_{n\geqslant 0} u_n k^{-n} \leqslant 1$. Навпаки, якщо $u(z) = \sum_{n\geqslant 0} u_n z^n$ — ряд з невід'ємними коефіцієнтами то, з точки зору теореми 2.4.13, якщо $u(1/k) \leqslant 1$, то існує префіксний код X на k літерах такий, що $u(z) = f_X(z)$.

Якщо X — тонкий максимальним префіксним кодом, тоді $f_X(1/k) = 1$ за теоремою 2.5.16. І навпаки, якщо $u(z) = \sum_{n\geqslant 0} u_n z^n$ є рядом з невід'ємними коефіцієнтами, і якщо $u(1/k) = 1$, то існує префіксний код X на k літерах такий, що $f_X(z) = u(z)$. Цей код є, очевидно, максимальним кодом, а отже є максимальним префіксним кодом.

Приклад 3.8.1. З формули (3.9) випливає, що породжуючий ряд коду Ґоломба-Райса порядку k є

$$f_{GR_k}(z) = \frac{2^k z^{k+1}}{1 - z} = \sum_{i\geqslant k+1} 2^k z^i.$$

Нехай X — раціональний префіксний код. Породжуючий ряд $f_X(z)$ є $\mathbb{N}$-раціональним за твердженням 1.10.11. Наступна теорема доводить обернене.

Теорема 3.8.2. *Ряд $u(z) = \sum_{n\geqslant 0} u_n z^n$ є породжуючим рядом раціонального префіксного коду на k літерах тоді і тільки тоді, коли він є $\mathbb{N}$-раціональним, $u_0 = 0$ і він задовольняє нерівність $u(1/k) \leqslant 1$.*

Очевидно, що ці умови є необхідними. Щоб довести, що вони є достатніми, ми доводимо декілька проміжних результатів. Ми припустимо, що u є $\mathbb{N}$-раціональним рядом і, що $u(1/k) \leqslant 1$. Оскільки $u_0 = 0$, то існує номалізовний ваговий автомат, який розпізнає u за твердженням 1.10.10. Ми припускаємо, що u не є нуль-рядом.

Наступна лема є першим кроком доведення.

Лема 3.8.3. *Якщо $\mathcal{A} = (Q, i, t)$ — нормалізовний ваговий автомат, який розпізнає ряд u, матриця суміжності автомата $\mathcal{A}$ має k-наближений власний вектор w, який є додатній і таким, що $w_i = w_t$.*

Доведення. Нехай $\mathcal{A} = (Q, i, t)$ — нормалізовний ваговий автомат, який розпізнає ряд u. Нехай Нехай $\overline{\mathcal{A}}$ — ваговий автомат на множині станів $\overline{Q} = Q \setminus \{t\}$, отриманих шляхом злиття станів i та t. Нехай M — матриця переходів автомата $\mathcal{A}$ та $\overline{M}$ — матриця переходів автомата $\overline{\mathcal{A}}$. Оскільки автомат $\mathcal{A}$ є впорядкованим, то матриця $\overline{M}$ є незвідною. За твердженням 1.10.12, автомат $(\overline{Q}, i, i)$ розпізнає ряд $u^*(z) = \dfrac{1}{1 - u(z)}$. Оскільки $u(1/k) \leqslant 1$, то радіус збіжності ρ ряду u^* задовольняє умову $\rho \geqslant 1/k$. За твердженням 1.10.14 спектральний радіус λ матриці $\overline{M}$ дорівнює $1/\rho$. Таким чином, $\lambda \leqslant k$ і за твердженням 1.9.6 існує додатній k-наближений власний вектор $\overline{w}$ матриці $\overline{M}$. Нехай w — Q-вектор, визначений наступним чином $w_q = \overline{w}_q$ для кожного $q \neq t$ і $w_t = \overline{w}_i$. За означенням маємо $w_i = \overline{w}_i = w_t$. Ми доведемо, що w є додатнім k-наближеним власним вектором матриці M. Ми доведемо, що $\sum\limits_{q \in Q} M_{pq} w_q \leqslant k w_p$ для всіх $p \in Q$. Позаяк автомат $\mathcal{A}$ є нормалізовним, то $M_{p,i} = 0$ для всіх $p \in Q$. Далі, для $p \in \overline{Q}$, маємо

$$\begin{aligned}
\sum_{q \in Q} M_{pq} w_q &= \sum_{q \in Q \setminus \{i,t\}} M_{pq} w_q + M_{pt} w_t = \\
&= \sum_{q \in \overline{Q} \setminus \{i\}} \overline{M}_{pq} \overline{w}_q + \overline{M}_{pt} \overline{w}_t = \\
&= \sum_{q \in \overline{Q}} \overline{M}_{pq} \overline{w}_q \leqslant \\
&\leqslant k \overline{w}_p = \\
&= k w_p.
\end{aligned}$$

Більше того, позаяк $M_{tq} = 0$ для всіх $q \in Q$, нерівність виконується тривіально для $p = t$, оскільки $w_t \geqslant 0$. □

Ми будемо використовувати наступні дві комбінаторні леми деякого незалежного інтересу. Вони будуть використані при доведенні леми 3.8.6. Для Q-вектора $x = (x_q)_{q \in Q}$, через $d(x)$ позначатимемо суму його коефіцієнтів $d(x) = \sum\limits_{q \in Q} x_q$ і для двох Q-векторів $x = (x_q)_{q \in Q}$ і $y = (y_q)_{q \in Q}$ позначимо через $x \cdot y$ їх скалярний добуток, який визначається за формулою

$$x \cdot y = \sum_{q \in Q} x_q y_q.$$

Перша комбінаторна лема є варіацією принципу Діріхле.

Лема 3.8.4. *Для довільного цілого числа $m \geqslant 1$ і довільних Q-векторів z, $w \in \mathbb{N}^Q$ таких, що $d(z) = m$, існує Q-вектор z' такий, що $0 < z' \leqslant z$ і $z' \cdot w \equiv 0 \mod m$.*

Доведення. Позаяк $d(z) = m$, то існує послідовність $x^{(1)}, x^{(2)}, \ldots, x^{(m)}$ Q-векторів таких, що

$$0 < x^{(1)} < x^{(2)} < \cdots < x^{(m)} = z.$$

Справді, це є очевидним якщо $m = 1$. Припустимо, що $m > 1$. Існує індекс k такий, що $z_k > 0$. Означимо Q-вектор u, поклавши $u_i = z_i$ для $i \neq k$ та $u_k = z_k - 1$. Тоді $d(u) = m - 1 \geqslant 1$, і за індукцією існує послідовність $x^{(1)}, x^{(2)}, \ldots, x^{(m-1)}$ Q-векторів таких, що

$$0 < x^{(1)} < x^{(2)} < \cdots < x^{(m-1)} = u.$$

Встановлюючи $x^{(m)} = z$, отримуємо потрібну послідовність, оскільки $u < z$.

Розглянемо послідовність $x^{(1)}, x^{(2)}, \ldots, x^{(m)}$. Якщо всі лишки $x^{(i)} \cdot w$ по модулю m різні, то існує індекс i з $1 \leqslant i \leqslant m$ такий, що $x^{(i)} \cdot w \equiv 0 \mod m$. У цьому випадку встановлюємо $z' = x^{(i)}$. В іншому випадку існують індекси i, j з $1 \leqslant i < j \leqslant m$ такі, що $x^{(i)} \cdot w \equiv x^{(j)} \cdot w \mod m$. У цьому випадку встановлюємо $z' = x^{(j)} - x^{(i)}$. Зауважимо, що $0 < z' < x^{(j)} \leqslant z$. Отже, в обидвох випадках отримуємо $z \geqslant z' > 0$ і $z' \cdot w \equiv 0 \mod m$. □

Лема 3.8.5. *Для довільного цілого числа $m \geqslant 1$ і $y, w \in \mathbb{N}^Q$, існують натуральне число n і $n+1$ векторів $v^{(0)}, v^{(1)}, \cdots, v^{(n)} \in \mathbb{N}^Q$ такі, що $y = \sum_{j=0}^{n} v^{(j)}$, з*

(i) $d(v^{(j)}) \leqslant m$ *для* $0 \leqslant j \leqslant n$;
(ii) $v^{(j)} \cdot w \equiv 0 \mod m$ *для* $1 \leqslant j \leqslant n$.

Доведення. Ми проведемо індукцію по $d(y)$. Якщо $d(y) \leqslant m$, то властивості виконуються для $n = 0$ і $v^{(0)} = y$. Справді, умова (ii) є порожньою для $n = 0$. В іншому випадку, ми пишемо $y = z + y'$ для $d(z) = m$. За лемою 3.8.4 існує Q-вектор z' такий, що $0 < z' \leqslant z$ і $z' \cdot w \equiv 0 \mod m$. Ми пишемо $z = z' + s$. Тоді $y = z' + y''$ для $y'' = s + y'$. Позаяк $z' > 0$, то маємо $d(y'') < d(y)$ і ми можемо застосувати припущення індукції до y''. Множина векторів для y'' разом з z' дає бажаний результат для y, оскільки $d(z') \leqslant d(z) \leqslant m$. □

Лема 3.8.6. *Існує нормалізовний ваговий автомат $\mathcal{A} = (Q, i, t)$, який розпізнає ряд u такий, що матриця переходів автомата $\mathcal{A}$ має додатній k-наближений власний вектор w, який задовольняє умову $w_i = w_t = 1$.*

Доведення. Ми розпочнемо з нормалізовного вагового автомата $\mathcal{A} = (Q, i, t)$, який розпізнає ряд u. Нехай M — матриця переходів автомата $\mathcal{A}$. За лемою 3.8.3 існує додатній k-наближений власний вектор w матриці M такий, що $w_i = w_t$. Покладемо $m = w_i = w_t$. Нехай I — характеристичний Q-вектор стану i визначений наступним чином $I_i = 1$ і $I_q = 0$ для $q \neq i$, і нехай T — характеристичний Q-вектор стану t визначений подібно. Нехай

$$K = \left\{ r \in \mathbb{N}^Q \colon d(r) \leqslant m,\ r_t = 0 \right\},$$

і $R = K \cup \{T\}$. Оскільки $i \neq t$ і $d(I) = 1$, то вектор I міститься в K.

Ми означимо ваговий автомат $\mathcal{B} = (R, I, T)$, визначивши його матрицю переходів N наступним чином.

Розглянемо $r \in R$ і покладемо $z = rM$ і $y = z - z_t T$. Отож, $y_t = 0$. Ми застосуємо лему 3.8.5 до пари векторів y, w, де w і $m = w_i = w_t$ є, як визначено попередньо. Лема дає розклад $y = \sum_{j=0}^{n} v^{(j)}$, де кожен доданок $v^{(j)}$ є елементом множини K, оскільки $y_t = 0$. Ми покладемо

$$N_{r,s} = \begin{cases} \operatorname{Card}\left(\left\{j \cdot 0 \leqslant j \leqslant n \text{ і } v^{(j)} = s\right\}\right), & \text{якщо } s \neq T; \\ z_t, & \text{в іншому випадку.} \end{cases}$$

Позаяк $rM = y + z_t T$, то маємо

$$rM = \sum_{s \in R} N_{r,s} s. \tag{3.32}$$

Зауважимо, що коли $N_{r,s} \neq 0$ у правій частині, то $s \cdot w \equiv 0 \mod m$, за винятком одного значення s, для якого $N_{r,s} = 1$, що відповідає вектору $v^{(0)}$. Справді, це істинним для $s \neq T$ за умовою (ii) леми 3.8.5, і воно виконується також для $s = T$, оскільки $T \cdot w = w_t = m$.

Ми перевіримо, що автомат $\mathcal{B}$ розпізнає ряд u і, що його матриця переходів N має додатній власний k-вектор w', який задовольняє умову $w'I = w'T = 1$.

Нехай U — $R \times Q$-матриця, яка визначається так: $U_{r,q} = r_q$ для $q \in Q$. Таким чином, рядок з індексом r матриці U є сам Q-вектор r. Звідси випливає, що для кожного Q-вектора z маємо, що

$$(Uz)_r = \sum_{q \in Q} U_{r,q} z_q = r \cdot z.$$

Зауважимо також, що з конструкції випливає рівність $UM = NU$, оскільки рядок індексу r у матриці UM дорівнює rM, і

$$(NU)_{r,p} = \sum_{s \in R} N_{r,s} U_{s,p} = \sum_{s \in R} N_{r,s} s_p = (rM)_p$$

за формулою (3.32), доводить, що рядок індексу r в матриці NU дорівнює rM.

Нехай I' (від. T') — характеристичний R-вектор стану I (відп. стану T). Ми отримуємо, розглядаючи I, I' як вектори-рядки і T, T' як вектор-стовпчики рівності $I'U = I$ та $UT = T'$. Справді,

$$(I'U)_p = \sum_{r \in R} I'_r U_{r,p} = I'_I U_{I,p} = U_{I,p} = I_p,$$

і

$$(UT)_r = \sum_{p \in Q} U_{r,p} T_p = U_{r,t} = r_t,$$

для $r \in R$. Це доводить, що $UT = T'$ з $r_t = 0$ для всіх $r \in R$, за винятком $r = T$.

Оскільки $UM^n = N^n U$ для всіх натуральних чисел n, то маємо

$$u_n = IM^n T = I'UM^n T = I'N^n UT = I'N^n T'.$$

Це доводить, що ряд u розпізнається автоматом $\mathcal{B}$. Також маємо, що

$$NUw = UMw \leqslant kUw,$$

а отже $w' = Uw$ є k-наближеним власним вектором матриці N. Зауважимо, що $w'_I = w'_T = m$. Справді,

$$w'_I = I' \cdot w' = I' \cdot Uw = I'U \cdot w = I \cdot w = w_i,$$

і, оскільки рядок з індексом T матриці U є Q-вектор T, то

$$w'_T = (Uw)_T = T \cdot w = w_t.$$

Для кожного індексу $r \in R$ маємо, що

$$\sum_{s \in R} N_{r,s} w'_s \leqslant k w'_r.$$

Оскільки $w'_s = (Uw)_s = s \cdot w$, то маємо $w'_s \equiv 0 \mod m$ для всіх s за винятком, можливо, для одного індексу s_0, для якого $N_{r,s_0} = 1$. Ми перепишемо цю нерівність так:

$$\sum_{s \in R \setminus \{s_0\}} N_{r,s} w'_s + N_{r,s_0} w'_{s_0} \leqslant k w'_r.$$

Поділивши обидві частини останньої нерівності на m отримуємо

$$\sum_{s \in R \setminus \{s_0\}} \frac{N_{r,s} w'_s}{m} + \frac{N_{r,s_0} w'_{s_0}}{m} \leqslant \frac{k w'_r}{m}.$$

Взяття цілої частини від обох частин нерівності дає

$$\left\lceil \sum_{s \in R \setminus \{s_0\}} \frac{N_{r,s} w'_s}{m} + \frac{N_{r,s_0} w'_{s_0}}{m} \right\rceil \leqslant \left\lceil \frac{k w'_r}{m} \right\rceil.$$

Оскільки з лівого боку всі доданки є цілими числами, за винятком можливо останнього, і $N_{r,s_0} = 1$, то з останньої нерівності випливає, що

$$\sum_{s \in R \setminus \{s_0\}} \frac{N_{r,s} w'_s}{m} + N_{r,s_0} \left\lceil \frac{w'_{s_0}}{m} \right\rceil \leqslant \left\lceil \frac{k w'_r}{m} \right\rceil \leqslant k \left\lceil \frac{w'_r}{m} \right\rceil.$$

Це доводить, що вектор w'', визначений $w''_r = \left\lceil \frac{w'_r}{m} \right\rceil$ додатнім k-наближеним власним вектором таким, що $w''_{i'} = w''_{t'} = 1$. □

Доведення теореми 3.8.2. Спочатку доведемо, що існує нормалізовний ваговий автомат, який розпізнає ряд u такий, що кожен стан цього автомата має не більше k вихідних ребер.

За лемою 3.8.6 ми починаємо з нормалізовного вагового автомата $\mathcal{A} = (Q, i, t)$, який розпізнає ряд u з множиною станів Q таким чином, що матриця переходів M автомата $\mathcal{A}$ має додатній k-наближений власний вектор w з $w_i = w_t = 1$. Ми будемо

визначати ваговий автомат $\mathcal{A}' = (R, i', t')$ його матрицею переходів N. Ця матриця буде мати властивість, що існує невід'ємна матриця U така, що

$$MU = UN.$$

По побудові сума кожного рядка матриці N буде не більше за k.

Множина R містить w_q копій кожного стану q в Q. Позаяк $w_i = 1$, то множина R містить тільки одну копію початкового стану i. Формально, R є множиною пар (q, j) для $q \in Q$ і $1 \leqslant j \leqslant w_q$. Для фіксованих станів $p, q \in Q$, означимо матрицю $N_{(p,i),(q,j)}$ для $1 \leqslant i \leqslant w_p$ і $1 \leqslant j \leqslant w_q$ наступним чином.

Для стану $p \in Q$ покладемо

$$X(p) = \{(q, j, m) \colon q \in Q,\ 1 \leqslant j \leqslant w_q,\ 1 \leqslant m \leqslant M_{p,q}\}.$$

Таким чином, множина $X(p)$ містить $M_{p,q}$ копій кожного стану $(q, j) \in R$. Множина $X(p)$ має за означенням $\sum_{q \in Q} M_{p,q} w_q$ елементів. Оскільки $\sum_{q \in Q} M_{p,q} w_q \leqslant w_q$, то ми можемо розбити множину $X(p)$ на w_p множин $X_{p,1}, \ldots, X_{p,w_p}$, які мають щонайбільше k елементів. Позначимо через $X_{p,l,q,j}$ підмножину множини $X_{p,l}$, яка складається з елементів вигляду (q, j, m) для деякого m. Тоді означимо $N_{(p,l),(q,j)} = \mathrm{Card}(X_{p,l,q,j})$. Оскільки N — матриця переходів автомата згідно побудови, то $N_{(p,l),(q,j)}$ є вагою ребра зі стану (p, l) в стан (q, j). Сума ваг ребер, що виходять з кожного стану (p, l) є потужністю множини $X_{p,l}$ і, таким чином, не перевищує числа k. Зауважимо також, що $\sum_{1 \leqslant l \leqslant w_p} N_{(p,l),(q,j)} = M_{p,q}$, оскільки сума дорівнює кількості елементів множини $X(p)$ вигляду (q, j, m) для деякого m, тобто дорівнює точно $M_{p,q}$.

Означимо $Q \times R$-матрицю U так: $U_{q,(q,j)} = 1$ для $1 \leqslant j \leqslant w_q$, а всі інші її елементи дорівнюють 0. Тоді маємо, що $MU = UN$. Справді,

$$MU_{p,(q,j)} = \sum_{s \in Q} M_{p,s} U_{s,(q,j)} = M_{p,q} U_{q,(q,j)} M_{p,q}$$

та

$$UN_{p,(q,j)} = \sum_{r \in R} U_{p,r} N_{r,(q,j)} = \sum_{1 \leqslant l \leqslant w_p} U_{p,(p,l)} N_{(p,l),(q,j)} = M_{p,q}.$$

Нехай $\mathcal{A}' = (R, i', t')$ — ваговий автомат з матрицею переходів N і $i' = (i, 1)$ і $t' = (t, 1)$. За побудовою цей автомат є нормалізовним. Тоді автомат $\mathcal{A}'$ розпізнає ряд u. Справді, нехай I (відп. T) — характеристичний Q-вектор стану i (відп. стану t). Оскільки автомат $\mathcal{A}$ розпізнає ряд u, то $u_n = IM^nT$ для натурального числа n. Нехай подібно I' (відп. T') — харктеристичний R-вектор стану i' (відп. стану t'). За означенням станів i' та t' маємо, що $IU = I'$ і $T = UT'$. Позаяк $MU = UN$, то маємо також $M^nU = UN^n$ для всіх натуральних чисел n, а отже

$$I'N^nT' = IUN^nT' = IM^nUT' = IM^nT = u_n.$$

За побудовою, сума елементів кожного рядка матриці N не є більшою за k і, таким чином, автомат $\mathcal{A}'$ задовольняє необхідну власність.

Тепер ми помітимо ребра, що виходять з кожного стану, різними літерами. Оскільки існує тільки один початковий стан і відсутнє ребро з кінцевого стану, то отриманий автомат розпізнає префіксний код з генеруючим рядом u. □

Приклад 3.8.7. Нехай $u(z) = \dfrac{3z^2}{1-z^2}$. маємо, що $u(1/2) = 1$. Ряд u розпізнається впорядкованим нормалізовним ваговим автоматом, зображеним на рис. 3.33. Резуль-

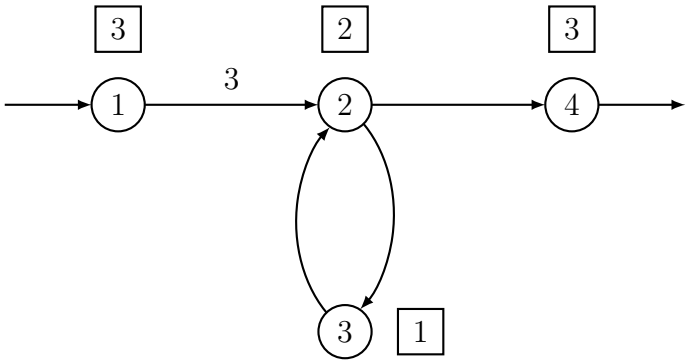


Рис. 3.33: Впорядкований нормалізовний ваговий автомат ряду u

тат перетворення, що реалізується в доведенні леми 3.8.6, представлений на рис. 3.34. Координати 2-наближеного власного вектора в обох випадках вказані в квадраті.

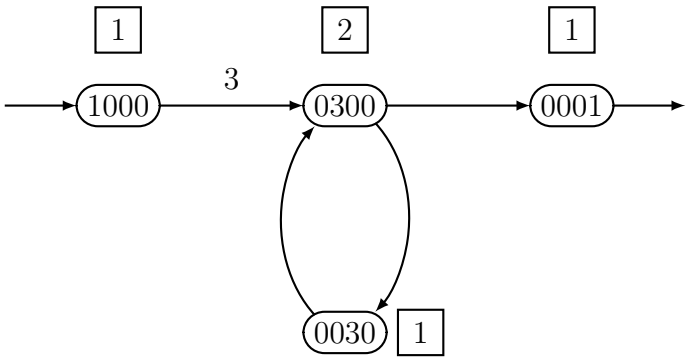


Рис. 3.34: Перше перетворення автомата з рис. 3.33

Ми обчислимо тільки доступну частину автомата $\mathcal{B}$. Це дає чотири вектори, зображені в станах автомата на рис. 3.34. Матрицями M, N і U з доведення леми 3.8.6 є

$$M = \begin{bmatrix} 0 & 3 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \qquad N = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad \text{і} \qquad U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Друге перетворення (доведення теореми 3.8.2) дає зважений автомат, зображеним на рис. 3.35. Зауважимо, що стан з вагою 2 є розщепленням на два стани $(2,1)$ і (2.2), і,

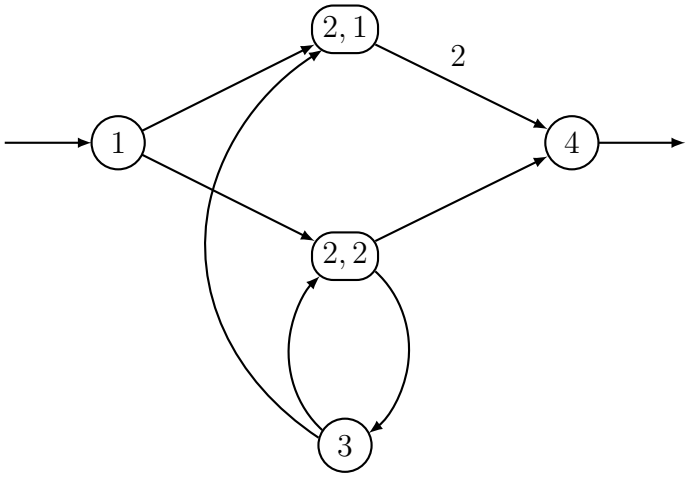


Рис. 3.35: Друге перетворення автомата з рис. 3.33

що його вихід розподіляється між ними. Матрицями M, N і U з доведення є

$$M = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \qquad N = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{і} \quad U = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Детерміністичне маркування дає автомат, представлений на рис. 3.36. Він розпізнає

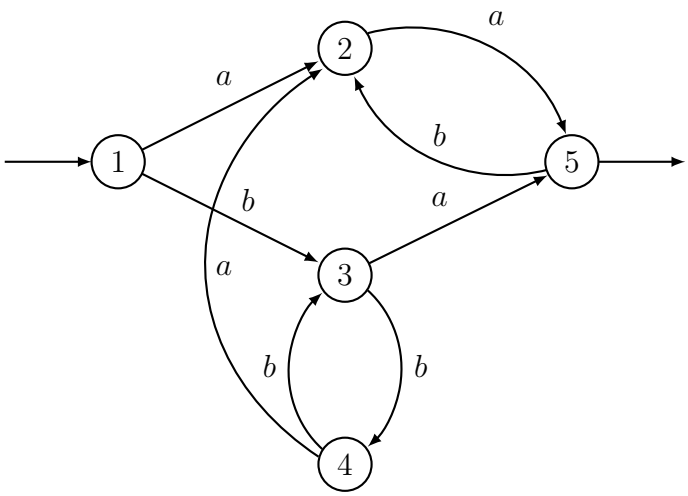


Рис. 3.36: Детерміністичне маркування автомата з рис. 3.33

регулярний префіксний код $X = (b^2)^*\{aa, ab, ba\}$. Остаточна мінімізація об'єднала б 1 і 4. Код X є максимальним, що не дивно, оскільки $u(1/2) = 1$.

3.9 Оптимальні префіксні коди

Нехай X — код над деяким алфавітом A, і припустимо, що кожна літера $a \in A$ має *вартість* $c(a)$, пов'язану з нею. Вартість слова w дорівнює за означенням сумі вартостей його літер.

Припустимо далі, що кожне кодове слово $x \in X$ має *вагу* $p(x)$, асоційовану з ним. *Ваговою вартістю* коду X називається величина

$$C_X = \sum_{x \in X} p(x)c(x).$$

Задача префіксного кодування полягає в тому, щоб знайти префіксний код X з мінімальною ваговою вартістю для заданих ваг. Далі ваги та вартість є додатніми числами.

Зазвичай, код X можна розглядати через морфізм кодування, тобто взаємно однозначної відповідності $\beta\colon B \to X$, для деякого алфавіту B, який продовжується до ін'єктивного морфізму з B^* в A^*. З огляду на це, вага слова $x \in X$ є насправді вагою літери $b \in B$ такою, що $x = \beta(b)$. Отже ваговою вартістю коду X є також

$$C_X = \sum_{b \in B} p(b)c(\beta(b)).$$

У випадку, коли всі літери $a \in A$ мають однакову вартість, вартість слова над алфавітом A є лише його довжиною. У цьому випадку задача префіксного кодування зводиться до побудови префіксного коду, який мінімізує рівність

$$C_X = \sum_{x \in X} p(x)|x|.$$

У випадку $\sum_{x \in X} p(x) = 1$ число C_X дорівнює просто середній довжині слів алфавіту X.

Кодування β, яке розв'язує задачу оптимального префіксного коду для рівних вартостей літер, називається *кодуванням Гаффмана* (*Huffman encoding*). Наступний жадібний алгоритм обчислює разв'язок в двійковому випадку за час $O(n \log n)$, а за час $O(n)$, якщо ваги доступні в зростаючому порядку. Нехай $A = \{0, 1\}$ і $p\colon B \to \mathbb{R}$ — функція ваги.

Якщо алфавіт B містить рівно один елемент c, то покладемо $\beta(c) = 1$. В іншому випадку виберемо два елементи $c_1, c_2 \in B$ мінімальної ваги такі, що

$$p(c_1), p(c_2) \leqslant p(c) \qquad \text{для всіх} \qquad c \in B \setminus \{c_1, c_2\}.$$

Нехай

$$B' = (B \setminus \{c_1, c_2\}) \cup \{d\},$$

де d — новий символ, який не міститься в B, і означимо $p'\colon B' \to \mathbb{R}_+$ наступним чином:

$$p'(c) = p(c) \quad \text{для всіх} \quad c \neq d \qquad \text{і} \qquad p'(d) = p(c_1) + p(c_2).$$

Нехай β' — кодування Гаффмана пари (B', p') і визначимо відображення $\beta\colon B \to A^*$ наступним чином:

$$\begin{aligned}
&\beta(c) = \beta'(c) \qquad \text{для} \quad c \in B \setminus \{c_1, c_2\},\\
&\beta(c_1) = \beta'(d)0,\\
&\beta(c_2) = \beta'(d)1.
\end{aligned}$$

Перевіримо, що β є кодуванням Гаффмана пари (B, p). Для цього ми доведемо, що існує оптимальне кодування β таке, що $\beta(c_1)$, $\beta(c_2)$ є словами максимальної довжини, які відрізняються лише останньою літерою.

Розглянемо префіксний код $X = \beta(B)$ такий, що вагова вартість C_X є мінімальною. Нехай $c_1, c_2 \in B$ — літери з найменшими вагами $p(c_1)$ і $p(c_2)$. Нехай $x, y \in X$ — два слова максимальної довжини, які відрізняються лише їх останньою літерою. Нехай $c, d \in B$ — літери такі, що $\beta(c) = x$ і $\beta(d) = y$. Визначимо кодування β' отримане з β заміною значень c_1 і c_2 на значення c і d, відповідно, і покладемо $X' = \beta'(B)$. Отримуємо, що $C_{X'} \leqslant C_X$, а отже $C_{X'} = C_X$.

Приклад 3.9.1. Розглянемо алфавіти

$$B = \{a, b, c, d, e, f\} \qquad \text{і} \qquad A = \{0, 1\},$$

і нехай ваги викладено в таблиці

	a	b	c	d	e	f
p	2	2	3	3	3	5

Кроки алгоритму представлені в послідовності дерев, наведеної на рис. 3.37.

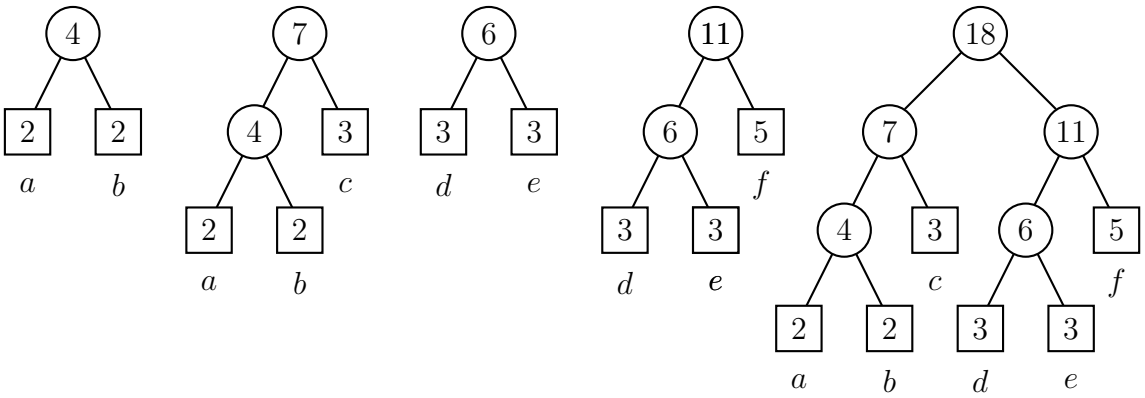


Рис. 3.37: Обчислення оптимального кодування Гаффмана шляхом поєднання дерев

У випадку, коли літери, що використовуються для кодування, мають нерівні вартості, менше відомо про задачу префіксного кодування. Задача мотивується морфізмами кодуванням, де різні символи можуть мати різний час передачі (проходження). Одним з прикладів є *телеграфний канал*, в якому тире "—" має в два рази більшу

вартість за точку "·". Іншим прикладом є сім'я бінарних *кодів з обмеженням довжини запису* (*run-length limited code* або *RLL-code*), де два послідовних символи 1 повинні бути розділені щонайменше a і не більше b суміжних нулів 0. У цій моделі кожне слово 0^k1 з $a \leqslant k \leqslant b$ може бути заміненим одноелементним символом в новому алфавіті, і вартість цього символу дорівнює $k+1$.

Задача префіксного кодування з нерівними літерними вартостями розглядалася в основному у випадку, коли вартості є цілими числами. Спеціалний випадок відомий, як *задача кодування Варна* (the *Varn coding problem*). Це є задачею префіксного кодування, коли всі ваги кодових слів рівні. Ця задача має дивовижно простий $O(n \log n)$ час розв'язання.

Припустимо, що всі n кодів-слів мають однакову вагу, яка дорівнює 1. Оптимальний код мінімізує вартість

$$C_X = \sum_{x \in X} c(x),$$

де вартість $c(x)$ дорівнює сумі вартостей її літер, тобто дорівнює

$$c(x) = \sum_{a \in A} c(a)|x|_a.$$

Ми будуємо оптимальний код над алфавітом A з k літер, припускаючи, що

$$n = q(k-1)+1 \qquad \text{для деякого цілого числа} \qquad q.$$

Так отриманий префіксний код є повним, а його дерево є повним з q внутрішніми вузлами і n листками. Алгоритм починається з дерева, що складається виключно з його кореня, і ітеративно замінює аркуш мінімальної вартості внутрішнім вузлом, який має k листків, по одному для кожної літери. Кількість листків збільшується на $k-1$, тому в q кроках виходить дерево з n листками.

Приклад 3.9.2. Припустимо, що ми шукаємо код із семи слів над тернарним алфавітом $\{a, b, c\}$, і що вартість літери a дорівнює 2, літери b дорівнює 4, а літери c дорівнює 5.

Ми починаємо з дерева, що складається з одного листка, а потім будуємо дерево, застосовуючи алгоритм. Існує два розв'язки, обидва з вартістю 45 наведені на рис. 3.38. Ліве дерево визначає префіксний код

$$\{aa, ab, ac, ba, bb, bc, c\},$$

а праве дерево визначає код

$$\{aaa, aab, aac, ab, ac, b, c\}.$$

На кожному кроці аркуш мінімальної вартості замінюється вузлом з 3 листками. Існує два варіанти для останнього кроку. Обидва дають оптимальне дерево.

В порядку отримання складності $O(n \log n)$ для конструкції, листя дерева керуються в черзі пріоритетів: тоді вставка листка виконується за $O(n \log n)$ операцій, і такий самий час складності виконується для вилучення листка з мінімальними вартостями. Для підтвердження правильності див. вправу 3.10.21.

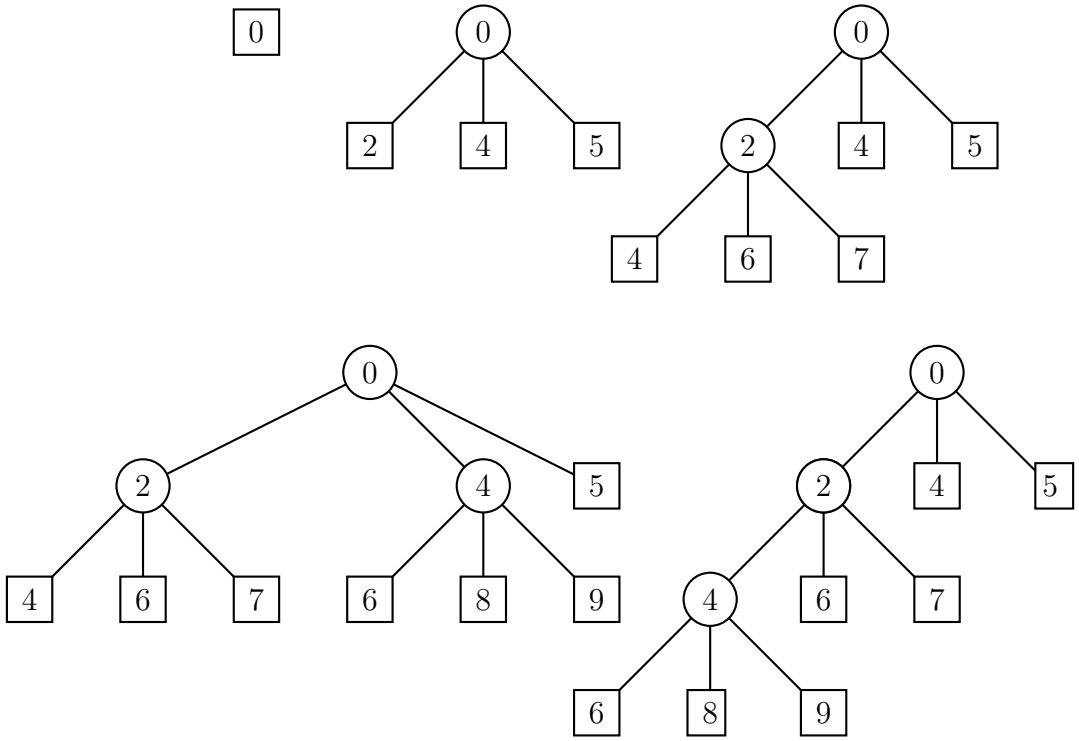


Рис. 3.38: Алгоритм Варна для 7 слів і алфавіт каналу з трьох літер.

VarnCoding()

```
1   T ← root
2   (By definition, the cost of the root is 0)
3   Q ← PriorityQueue()
4   Add(Q, root)
5   while the number of leaves is ≠ n do
6       f ← ExtractMin(Q)
7       for each a ∈ A do
8           c ← makeChild(f)
9           cost(c) ← cost(f) + cost(a)
10          Add(Q, c)
11  return T
```

Особливим випадком префіксного кодування є кодування, яке сумісне з даним порядком вхідного алфавіту. Розглянемо морфізм кодування $\beta\colon B^* \to A^*$, де A та B є алфавітами, які наділені порядком. Тоді морфізм β називається *порядковим кодуванням* або *алфавітним кодуванням*, якщо

$$b < b' \qquad \Longrightarrow \qquad \beta(b) < \beta(b'),$$

де порядок на A^* є лексикографічним порядком, індукованим порядком на алфавіті A. Якщо β — префіксне кодування, і якщо префіксний код $X = \beta(B)$ виглядає, як

дерево, це означає, що листки дерева, які читаються з ліва на право відповідають кодуванню вхідних літер в алфавіті B, читаються в алфавітному порядку. Таке дерево називається *впорядкованим*, або алфавітним. *Задача про впорядкований префіксний код* полягає в знаходженні впорядкованого кодування з мінімальною ваговою вартістю

$$C_X = \sum_{b \in B} p(b)|\beta(b)|,$$

де $p(b)$ — вага літери b.

Приклад 3.9.3. Розглянемо алфавіт $B = \{a, b, c\}$ з вагами $p(a) = p(c) = 1$ і $p(b) = 4$. Рис. 3.39 показує оптимальне дерево для цих ваг, а на рис. 3.40 ці ваги зображені

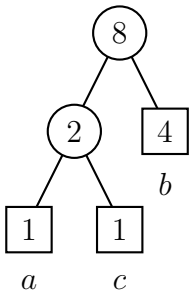


Рис. 3.39: Оптимальне дерево для ваг прикладу 3.9.3

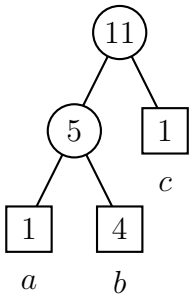


Рис. 3.40: Оптимальне впорядковане дерево для ваг прикладу 3.9.3

оптимальним впорядкованим деревом. Дерево на рис. 3.39 має вагову вартість 8, ы воно э оптимальним, але не є впорядкованим. Дерево на рис. 3.40 є впорядкованим і має вагову вартість 11. Цей приклад також показує, що алгоритм Гаффмана не дає оптимальне префіксне дерево.

Приклад 3.9.4. Розглянемо послідовність ваг $(4, 3, 3, 4)$. Оптимальне впорядковане дерево зображено на рис. 3.41. Це показує, що в оптимальному впорядкованому дереві листки з мінімальними вагами не обов'язково є суміжними.

Нехай $B = \{b_1, \ldots, b_n\}$ — впорядкований алфавіт з n літер і p_i — вага літери b_i. Ми представляємо алгоритм для обчислення оптимального впорядкованого дерева, який

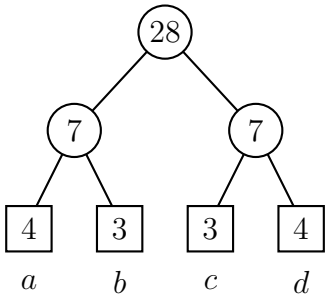


Рис. 3.41: Оптимальне впорядковане дерево для ваг $(4, 3, 3, 4)$

належить Гарсія та Вахсу. Ідея цього алгоритму полягає у використанні варіанту алгоритму Гаффмана групування разом пар елементів з мінімальними вагами, які є послідовними у впорядкуванні. Алгоритм може бути реалізованим до виконання за час $O(n \log n)$.

Алгоритм складається з трьох частин. У першій частині, яка називається *комбінуючою частиною*, починаємо з послідовності ваг

$$p = (p_1, \ldots, p_n)$$

і будуємо оптимальне бінарне дерево T' для підстановки

$$b_{\sigma(1)}, \ldots, b_{\sigma(n)}$$

алфавіту. Листки, зліва на право, мають ваги

$$p_{\sigma(1)}, \ldots, p_{\sigma(n)}.$$

У загальному випадку ця підстановка не є тотожньою, а отже само дерево не є впорядкованим, див. рис. 3.42. Тут число в коді є його вагою, що є сумою ваг листків

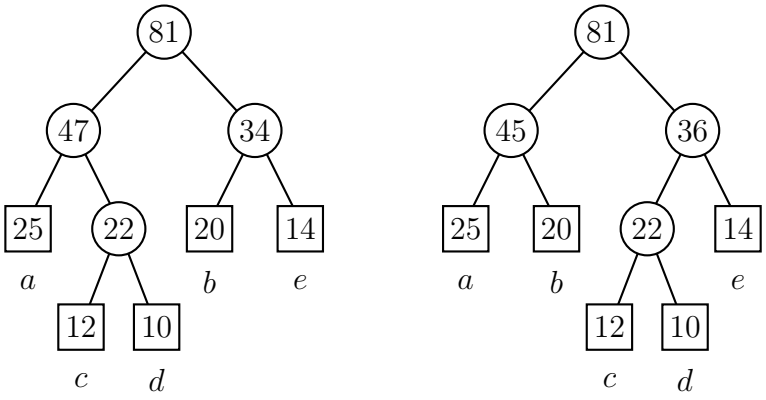


Рис. 3.42: Оптимальне впорядковане дерево для ваг $(4, 3, 3, 4)$

його піддерева. У другій частині, яка називається *присвоєння рівня*, обчислюються

рівні листків. В останні частині, яка називається *рекомбінуючою частиною*, будується дерево T, яке має ваги $p_1, \ldots, p_n$, пов'язані до їх листків з ліва на право, і де кожен листок з вагою p_i зустрічається на тому ж рівні, як і в дереві T'. Це дерево є впорядкованим за нашою побудовою (див. рис. 3.42). Оскільки листки мають той ж самий рівень у дереві T і в дереві T', відповідні кодові слова мають однакові довжини, а отже дерева T і T' мають однакову вартість. Таким чином, T є оптимальним впорядкованим деревом.

Тепер опишемо деталі алгоритму. Для зручності описання введемо наступну термінологію. Послідовність $(p_1, \ldots, p_k)$ чисел називається 2-*низхідною*, якщо $p_i > p_{i+2}$ для $1 \leqslant i \leqslant k-2$. Очевидно, що послідовність $(p_1, \ldots, p_k)$ є 2-низхідною тоді і тільки тоді, коли послідовність "сум сусідніх двох членів"

$$(p_1 + p_2, \ldots, p_{k-1} + p_k)$$

строго спадає.

Нехай $p = (p_1, \ldots, p_k)$ — послідовність (додатних) ваг. Продовжимо її поклавши: $p_0 = p_{n+1} = \infty$. *Лівою мінімальною парою* або просто *мінімальною парою* послідовності p називається пара (p_{k-1}, p_k), де $(p_1, \ldots, p_k)$ — найдовша 2-низхідний ланцюг, що є префіксом послідовності p. Індекс k називається *позицією* мінімальної пари послідовності. Іншими словами, k є ціле число таке, що

$$p_{i-1} > p_{i+1} \quad (1 < i < k) \qquad \text{і} \qquad p_{k-1} \leqslant p_{k+1}.$$

Зауважимо, що ліву мінімальну пару можна визначити еквівалентно умовами

$$p_{i-1} + p_i > p_i + p_{i+1} \quad (1 < i < k) \qquad \text{і} \qquad p_{k-1} + p_k \leqslant p_k + p_{k+1}.$$

Мета — це індекс j з $1 \leqslant j < k$ такий, що

$$p_{j-1} \geqslant p_{k-1} + p_k > p_j, \cdots, p_k.$$

Приклад 3.9.5. Для послідовності $(14, 15, 10, 11, 12, 6, 8, 4)$ лівою мінімальною парою є $(10, 11)$ і мета дорівнює 1, тоді як для послідовності $(28, 8, 15, 20, 7, 5)$ лівою мінімальною парою є $(15, 20)$ і мета дорівнює 2.

Пара (j, k), яка складається з розташування лівої мінімальної пари та її мети, називається *областю дії* послідовності p. Зауважимо, що послідовність

$$(p_{j-1}, p_{k-1} + p_k, p_j, \ldots, p_{k-2})$$

є 2-низхідною, оскільки $p_{j-1} \geqslant p_{k-1} + p_k > p_j, p_{j+1}$.

Три фази алгоритму працюють наступним чином.

Комбінація Приєднаємо одноелментне дерево до кожної ваги. Повторимо наступні кроки настільки довго, як послідовність ваг має більше одного елемента.

(*i*) Обчислюємо *ліву мінімальну пару* (p_{k-1}, p_k).
(*ii*) Обчислюємо *мету* j.
(*iii*) Видаляємо ваги p_{k-1} і p_k.
(*iv*) Вставляємо $p_{k-1} + p_k$ між p_{j-1} і p_j.

(*v*) Пов'язуємо з $p_{k-1}+p_k$ нове дерево з вагою $p_{k-1}-p_k$, яке має, як ліве, так і праве піддерева, дерево для p_{k-1} і для p_k, відповідно.

Присвоєння рівня Обчислюємо для кожної літери b з алфавіту B рівня її листка на дереві T'.

Рекомбінація Будуэмо впорядковане дерево T у якому листки літер мають рівні обчислені присвоєнням рівня.

Приклад 3.9.6. Розглянемо наступні ваги для алфавіту з п'яти літер:

	a	b	c	d	e
p	25	20	12	10	14

Початкова послідовність дерев зображена на рис. 3.43. Лівою мінімальною парою є

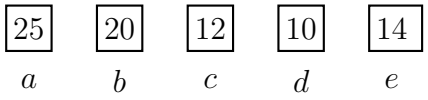


Рис. 3.43: Початкова послідовність дерев

12, 10, її мета дорівнює 2 так, що листки для c і d об'єднуються в дерево, яке вставляється праворуч від першого дерева. Тепер мінімальна пара (20, 14) (тут є нескінченна вага в правому кінці), тому лиски для літер b і e об'єднуються, і вставляються на початку. Це зображено на двох послідовностях рис. 3.44. Далі два останні дерева

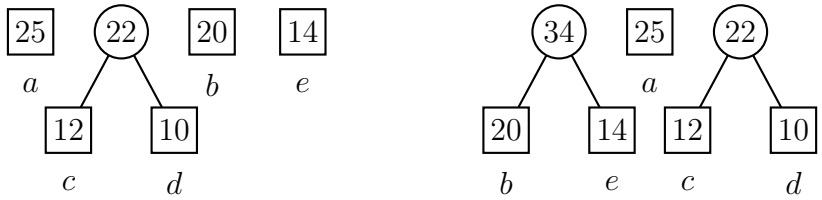


Рис. 3.44: Наступні два кроки

поєднуються і вставляються на початку, як показано зліва на рис. 3.45, і, нарешті, дві залишені дерева поєднуються, як показано справа на рис. 3.45.

Дерево $'$, отримане в кінці першої фази не є впорядкованим. Приписаними рівнями для літер прикладу є:

	a	b	c	d	e
рівень	2	2	3	3	2

Оптимальне впорядковане дерево з цими рівнями визнається рекомбінацією. Це є дерево, яке зображено справа на рис. 3.42. Вагова вартість цього дерева дорівнює 184.

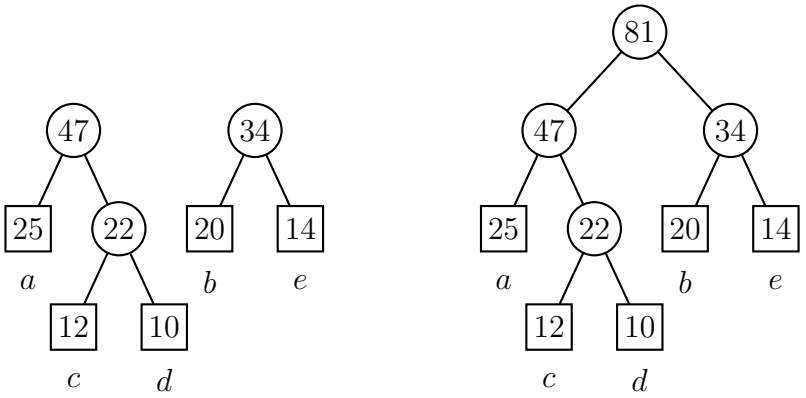


Рис. 3.45: Наступні два кроки

Ми тепер наведемо доведення алгоритму. Нехай T — деяке бінарне дерево з n листками, позначеними літерами $b_1, \ldots, b_n$ алфавіту B, з вагами $p_1, \ldots, p_n$, відповідно. Позначимо через l_i^T (або просто l_i) рівень аркуша b_i на дереві T, тобто довжині кодового слова, що кодує літеру b_i. Кожне з часткових дерев, побудованих в алгоритмі, буде ідентифіковано з його коренем, що розглядається як листок. Листок, який відповідний літері b_i, будемо позначати через λ_i.

Спочатку викладено дві прості леми.

Лема 3.9.7. *Нехай T — деяке бінарне дерево. Якщо $l_i > l_{i+1}$, то λ_i є правим листком. Симетрично, якщо $l_i < l_{i+1}$, то λ_i є лівим листком.*

Доведення. Припустимо, що λ_i є лівим листком. Тоді його правий брат є деревом, що містить листок λ_{i+1}. Таким чином, отримуємо, що $l_i \leqslant l_{i+1}$. □

Наступне твердження є першим кроком до доведення правильності алгоритму.

Лема 3.9.8. *Якщо $p_{i-1} > p_{i+1}$, то $l_i \leqslant l_{i+1}$ у кожному оптимальному впорядкованому дереві. Якщо $p_{i-1} = p_{i+1}$, то $l_i \leqslant l_{i+1}$ в деякому оптимальному впорядкованому дереві.*

Доведення. Припустимо, що $p_{i-1} \geqslant p_{i+1}$ і розглянемо дерево T з $l_i > l_{i+1}$. У цьому дереві правий листок λ_i є правою дитиною за лемою 3.9.8, і його лівими елементами одного рівня є дерево L з вагою $p(L) \geqslant p_{i-1}$, див. рис. 3.46. Будуємо нове дерево T' наступним чином: замінимо батьківське дерево L на самого себе L, замінюючи листок λ_{i+1} на вузол, що має як дітей листки λ_i і λ_{i+1}. Різниця вартостей дорівнює

$$C_{T'} - C_T = -p(L) + p_{i+1} - p_i(l_i - l_{i+1} - 1) \leqslant p_{i+1} - p_{i-1},$$

оскільки $l_i \geqslant l_{i+1} + 1$. Якщо $p_{i-1} > p_{i+1}$, то $C_{T'} - C_T < 0$ і дерево T не є оптимальним. Якщо $p_{i-1} = p_{i+1}$ ы якщо дерево T є оптимальним, то дерево T' також є оптимальним, і $l_i^{T'} = l_i^T$. □

Зауважимо також, що виконується симетричне твердження.

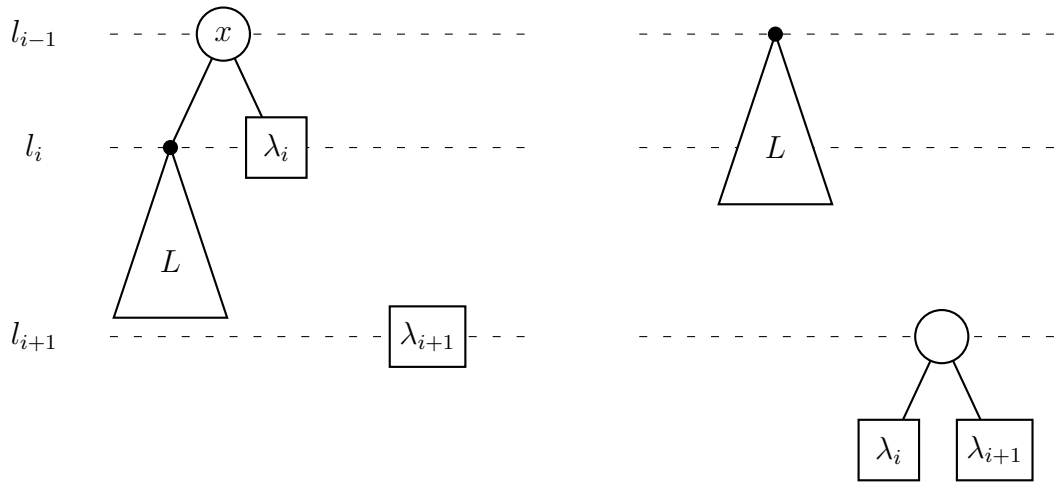


Рис. 3.46: Реорганізація листків в лемі 3.9.8

Наслідок 3.9.9. *Якщо $p_{i-1} < p_{i+1}$, то $l_{i-1} \leqslant l_i$ у кожному оптимальному впорядкованому дереві. Якщо $p_{i-1} = p_{i+1}$, то $l_{i-1} \geqslant l_i$ в деякому оптимальному впорядкованому дереві.*

Ми використаємо лему 3.9.8 у такому вигляді.

Наслідок 3.9.10. *Якщо підпослідовність $(p_{j-1}, \dots, p_k)$ є 2-низхідною, то*

$$l_j \leqslant \cdots \leqslant l_k$$

у кожному оптимальному впорядкованому дереві.

Тепер покажемо, що ми завжди можемо вважати, що мінімальне дерево для послідовності p має якийсь особливий вигляд. Таке дерево ми будемо називати *плоским*.

Твердження 3.9.11. *Нехай (j, k) — область дії послідовності $p = (p_1, \dots, p_n)$. Існує мінімальне дерево для послідовності p, для якої $l_{k-1} = l_k$ і виконується одна з двох умов:*

(a) $l_k = l_j + 1$, *або*
(b) $l_k = l_j$ *і* λ_j *є лівим листком.*

Доведення. Оскільки послідовність $p = (p_1, \dots, p_n)$ є 2-низхідною ш $p_0 = +\infty$, то за наслідком 3.9.10 маємо, що $l_1 \leqslant l_2 \leqslant \cdots \leqslant l_k$ в кожному мінімальному дереві. Далі $p_{k-1} \leqslant p_{k+1}$. Якщо $p_{k-1} < p_{k+1}$, то $l_{k-1} \geqslant l_k$ в кожному мінімальному дереві, а якщо $p_{k-1} = p_{k+1}$, то $l_{k-1} \geqslant l_k$ в деякому мінімальному дереві. Отож, отримуємо, що $l_{k-1} = l_k$ в деякому мінімальному дереві.

Розглянемо це дерево. Ми доведемо, що $l_j = l_k$ або $l_j = l_{k-1}$. Припустимо протилежне. Тоді $l_j \leqslant l_{k-2}$. Нехай s — найбільший індекс такий, що $l_s \leqslant l_{k-2}$. Тоді $s < k-1$, оскільки $l_{k-1} = l_k$. Нехай t — найменший індекс такий, що $l_t = l_k$. Тоді

$$l_j \leqslant \cdots \leqslant l_s < l_{s+1} \leqslant \cdots \leqslant l_{t-1} < l_t = \cdots = l_k.$$

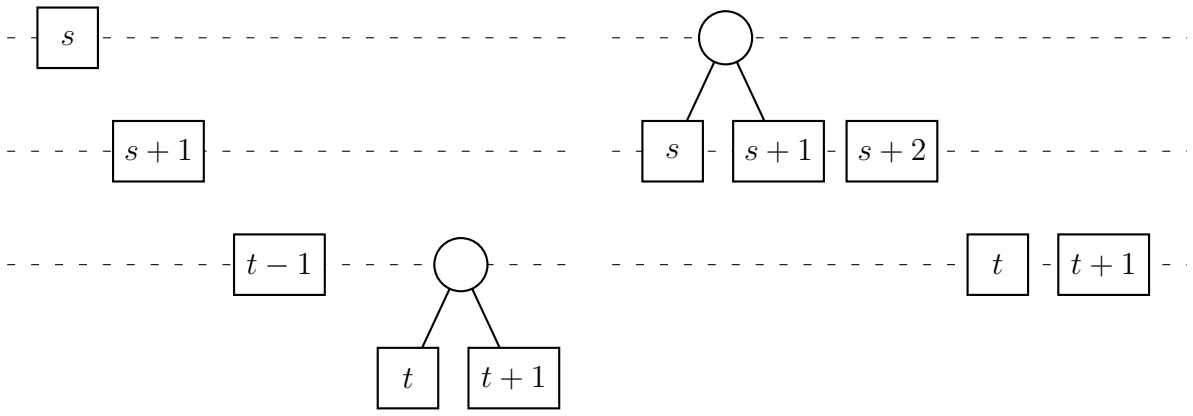


Рис. 3.47: Доведення твердження 3.9.11

Цілком можливо, що $s+1=t$. Зауважимо, що λ_{s+1} лівим листком за лемою 3.9.8, оскільки $l_s < l_{s+1}$. Аналогічно маємо, що λ_t є лівим листком, а λ_t і λ_{t+1} є одного рівня. Ми тепер зробимо таке перетворення, див. рис. 3.47, де ліва частина рисунку є перед зсувом, а права — після зсуву. Листок λ_s заміняється вузлом з двома елементами одного рівня λ_s і λ_{s+1}. Кожен з листків $\lambda_{s+2},\dots,\lambda_{t-1}$ посуваємо ліворуч. Листок λ_t заміняється листком λ_{t-1}, а батько листка λ_{t+1} заміняємо самим листком λ_{t+1}. Додаткові вартості на це перетворення не перевищують $p_s-p_t-p_{t+1}$, оскільки рівень листка λ_s збільшується на 1, рівень листка λ_{s+1} не збільшується, рівні листків λ_t і λ_{t+1} зменшується на 1. Тепер

$$p_s - p_t - p_{t+1} \leqslant p_s - p_{k-1} - p_k,$$

оскільки

$$p_t + p_{t+1} \geqslant p_{k-1} + p_k$$

(рівність можлива тому, що може бути $t=k-1$, а додаткові вартості менші за 0, оскільки $j>s$, і тому $p_s < p_{k-1}+p_k$). Це дає протиріччя, з якого випливає, що $l_j \geqslant l_{k-1}$.

Залишилось розглянути випадок, коли $l_j = l_k$. Стверджуючи протиріччя, припустимо, що λ_j — правий листок. Оскільки $l_{j-1} \leqslant l_j$, то листок λ_{j-1} є лівим листком і є однакового рівня з листком λ_j. Тоді зробимо наступні перетворення, зображені на рис. 3.48, де ліва частина рисунку відповідає ситуації перед перетворенням, а права — після перетворення. Замінимо спільного батька листків λ_{j-1} і λ_j на листок λ_{j-1}, посунемо $\lambda_j,\dots,\lambda_{k-2}$ на одну позицію праворуч, і замінимо листок λ_k вузлом з дітьми λ_{k-1} і λ_k. Оскільки листки $\lambda_{j-1},\dots,\lambda_k$ мають однаковий рівень перед перетворенням, то додаткова вартість дорівнює $-p_{j-1}+p_{k-1}+p_k$. Це значення не перевищує 0 за означенням мети. Оскільки дерево було мінімальним перед перетворенням, то дерево після перетворення має туж саму вартість. У цьому новому дереві, маємо справді $l_k = 1+l_j$. □

Дерево T для послідовності $p=(p_1,\dots,p_n)$ називається k-мінімальним, якщо воно є мінімальним серед усіх дерев, де листки p_{k-1} і p_k є однакового рівня.

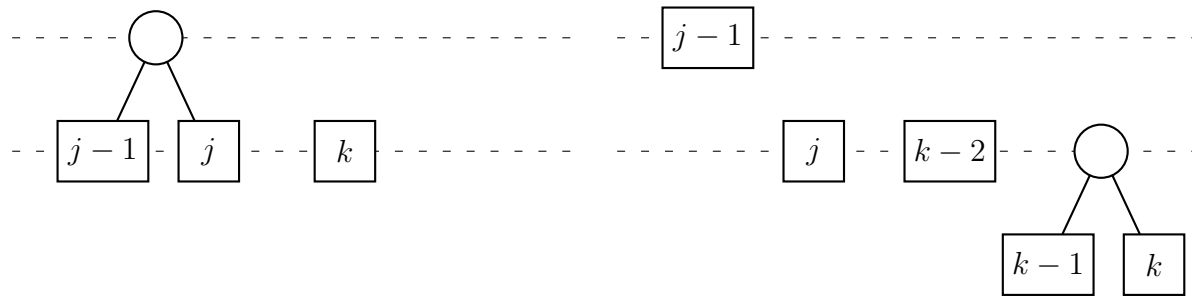


Рис. 3.48: Друге перетворення у твердженні 3.9.11

Перетворення, яке зберігає рівень σ дерева T є дерево T^σ, що має ті ж листки, як дерево T на тих же рівнях. За означенням, вартість дерева T^σ дорівнює вартості дерева T.

Лема 3.9.12. *Нехай* $p = (p_1, \ldots, p_n)$ *— послідовність ваг з областю дії* (j, k) *і нехай* T *— оптимальне плоске дерево для послідовності* p*. Нехай*

$$p' = (p_1, \ldots, p_{j-1}, p_{k-1}, p_k, p_j, p_{j+1}, \ldots, p_{k-2}, p_{k+1}, \ldots, p_n).$$

Існує перетворення, яке зберігає рівень, яке відображає дерево T *в дерево* T' *для* p' *таке, що листки для членів* p_{k-1} *і* p_k *є одного рівня.*

Доведення. Оскільки дерево T є плоским, то $l_j = l_k$ або $l_j = l_k - 1$. Якщо $l_j = l_k$, то виконується циклічний зсув листків $\lambda_j, \ldots, \lambda_k$ на дві позиції праворуч. Оскільки листок λ_j був лівою дитиною перед зсувом, то листки the leaves λ_{k-1} і λ_k є однакового рівня після зсуву, див. рис. 3.49.

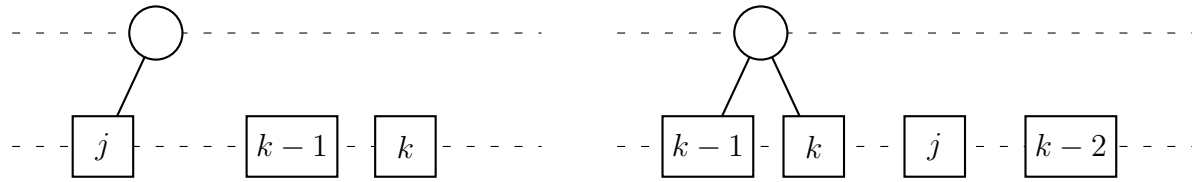


Рис. 3.49: Випадок $l_j = l_k$. До і після кругового зсуву

Якщо $l_j = l_k - 1$, то нехай s – такий індекс, що $l_s = l_j$ і $l_{s+1} = l_k$. Тоді виконується циклічний зсув листків $\lambda_{s+1}, \ldots, \lambda_k$ на дві позиції праворуч, як було попередньо, див. рис. 3.50.

Тоді застосуємо циклічний зсув на одну позицію праворуч послідовності $\lambda_j, \ldots, \lambda_s, x$, де x — батьківський вузол листків λ_{k-1} і λ_k, див. рис. 3.51. Це є таким перетворенням, що зберігає рівні листків, а отже отримане дерево має ту ж саму вартість, як і дерево T з якого ми починали. □

Теорема 3.9.13. *Нехай* $p = (p_1, \ldots, p_n)$ *— послідовність ваг з областю дії* (j, k) *і нехай*

$$\widehat{p} = (p_1, \ldots, p_{j-1}, p_{k-1} + p_k, p_j, p_{j+1}, \ldots, p_{k-2}, p_{k+1}, \ldots, p_n).$$

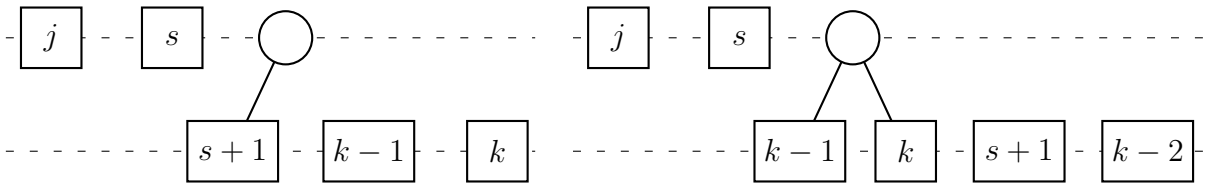


Рис. 3.50: Випадок $l_j = l_k - 1$: циклічний зсув. До і після кругового зсуву

Рис. 3.51: Випадок $l_j = l_k - 1$: до і після кругового зсуву

Нехай $\widehat{T}$ — мінімальне дерево для послідовності $\widehat{p}$, і нехай T' — дерево, отримане заміною дерева з двома листками λ_{k-1} і λ_k на листок, який відповідає елементам $p_{k-1} + p_k$ в дереві $\widehat{T}$. Тоді існує мінімальне дерево T для послідовності p вартості $c(T) = c(T')$, яке отримується підстановкою, що зберігає рівні дерева T'.

Доведення. Нехай $\widehat{T}$ — оптимальне дерево для послідовності $\widehat{p}$. Позаяк

$$c(T) = c(\widehat{T}) + p_{k-1} + p_k,$$

то дерево T' є k-мінімальним для послідовності

$$p' = (p_1, \ldots, p_{j-1}, p_{k-1}, p_k, p_j, p_{j+1}, \ldots, p_{k-2}, p_{k+1}, \ldots, p_n).$$

Якщо $j-1 = k-2$, то $p' = p$ і тут немає, що доводити. В іншому випадку, зауважимо, що послідовність

$$p_{j-1}, p_{k-1}, p_k, p_j, p_{j+1}, \ldots, p_{k-2}$$

є 2-низхідним множником послідовності $\widehat{p}$, оскільки

$$p_{j-1} \geqslant p_{k-1} + p_k > p_j \qquad \text{і} \qquad p_{k-1} + p_k > p_{j+1}.$$

Таким чином, позначивши через x листок в дереві $\widehat{T}$ з вагою $p_{k-1}+p_k$ наслідком 3.9.10 маємо, що

$$l_x^{\widehat{T}} \leqslant l_j^{\widehat{T}} \leqslant \cdots \leqslant l_{k-2}^{\widehat{T}}.$$

Вузол x є також батьком вузла листків для p_{k-1} і p_k в дереві T', і оскільки $l^{\widehat{T}} = l^{T'}$ для всіх вузлів дерева $\widehat{T}$, то отримуємо

$$l_x \leqslant l_j \leqslant \cdots \leqslant l_{k-2}$$

в дереві T'.

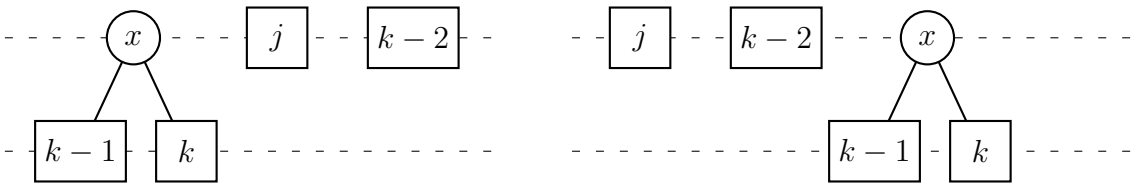


Рис. 3.52: Випадок $l_x = l_{k-2}$ в доведенні теореми 3.9.13: до і після кругового зсуву

Ми розрізняємо два випадки. Якщо $l_x = l_{k-2}$, то виконаємо таке перетворення: вузли $x, \lambda_j, \ldots, \lambda_{k-2}$ циклічно переставляються на одну позицію ліворуч, взявши вузли $\lambda_j, \ldots, \lambda_{k-2}, x$, і таким чином листки $\lambda_j, \ldots, \lambda_{k-2}, \lambda_{k-1}, \lambda_k$, див. рис. 3.52. Отримане дерево S перевіряє рівність $c(T) = c(T')$, а підстановка зберігає рівні.

Якщо $l_x < l_{k-2}$, то нехай s — такий індекс, що $l_x = l_s < l_{s+1}$. Тоді перше перетворення (див. рис. 3.53, де зображено стан до і після першого зсуву, післяцього зсуву праворуч) схоже до попереднього, але на $x, \lambda_j, \ldots, \lambda_s$ дає дерево, де послідовністю

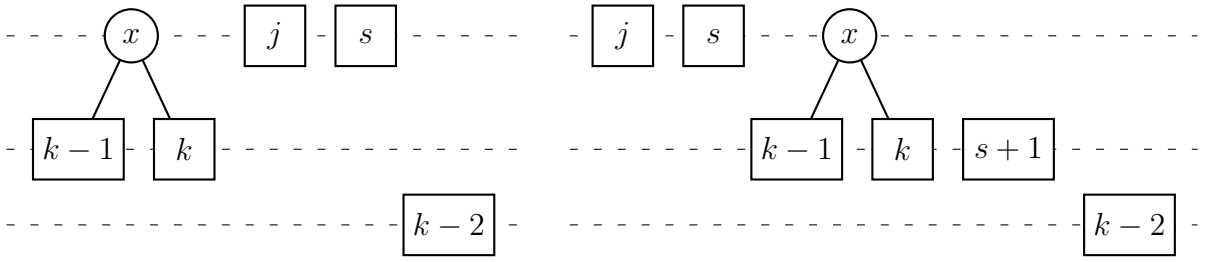


Рис. 3.53: Випадок $l_x < l_{k-2}$: перше перетворення

листків є

$$\lambda_j, \ldots, \lambda_{s-1}, \lambda_{k-1}, \lambda_k, \lambda_{s+1}, \ldots, \lambda_{k-2}.$$

Отже, маємо $l_{k-1} = l_k \leqslant l_{s+1} \leqslant \cdots \leqslant l_{k-2}$. Циклічна підстановка на дві позиції ліворуч листків $\lambda_{k-1}, \lambda_k, \lambda_{s+1}, \ldots, \lambda_{k-2}$ дає послідовність $\lambda_{s+1}, \ldots, \lambda_{k-2}\lambda_{k-1}, \lambda_k$, див. рис. 3.54, де зображено стан перед першим зсувом ліворуч, і після цього зсув праворуч.

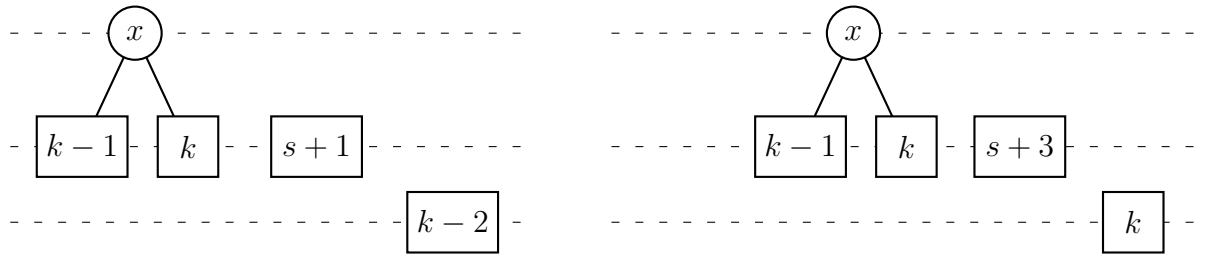


Рис. 3.54: Випадок $l_x < l_{k-2}$: друге перетворення

За лемою 3.9.14, яка доведена нижче, вартість отриманого дерева S є меншою за

вартість дерева T', хіба тільки $l_x = l_{k-2}$. Але за лемою 3.9.12, значення вартості $c(S)$ не може бути меншим за значення вартості $c(T')$. □

Лема 3.9.14. *Нехай $m \geqslant 3$ і $l_1 = l_2 \leqslant \cdots \leqslant l_m$ — натуральні числа і $(p_1, p_2, \ldots, p_m)$ — 2-низхідний ланцюг. Означимо*

$$c = p_{m-1}l_1 + p_m l_2 + p_1 l_3 + \cdots + p_{m-2}l_m,$$
$$c' = p_1 l_1 + p_2 l_2 + \cdot + p_m l_m.$$

Тоді $c' \leqslant c$, і рівність справджується лише у випадку $l_m = l_1$.

Доведення. Якщо $m = 3$, то $c' - c = (p_1 - p_3)(l_1 - l_3) \leqslant 0$, а отже $c' = c$ лише у випадку $l_1 = l_3$.

Якщо $m \geqslant 4$, то

$$c' - c = p_1(l_1 - l_3) + p_2(l_2 - l_4) + \cdots + p_{m-2}(l_{m-2} - l_m) + \\ + p_{m-1}(l_{m-1} - l_1) + p_m(l_m - l_2).$$

Оскільки ланцюг $(p_1, p_2, \ldots, p_m)$ є 2-низхідним, то $m-2$ перші члени цієї суми можна погрупувати і обмежити. Якщо число m є парним, то

$$c' - c \leqslant p_{m-3}(l_1 - l_{m-1}) + p_{m-2}(l_2 - l_m) + p_{m-1}(l_{m-1} - l_1) + p_m(l_m - l_2) = \\ = (p_{m-3} - p_{m-1})(l_{m-1} - l_1) + (p_{m-2} - p_m)(l_m - l_2) \leqslant 0,$$

і нерівність справджується лише у випадку $l_{m-1} = l_1$ і $l_m = l_2$, а отже коли $l_1 = \cdots = l_m$. Аналогічно, якщо число m є непарним, і оскільки $l_1 = l_2$, отримуємо

$$c' - c \leqslant p_{m-2}(l_1 - l_m) + p_{m-3}(l_2 - l_{m-1}) + p_{m-1}(l_{m-1} - l_1) + p_m(l_m - l_2) = \\ = (p_{m-3} - p_{m-1})(l_1 - l_{m-1}) + (p_{m-2} - p_m)(l_1 - l_m) \leqslant 0,$$

Знову, нерівність справджується лише у випадку $l_1 = \cdots = l_m$. □

3.10 Вправи до розділу 3

Підрозділ 3.1

В. 3.10.1. Нехай A — скінченний алфавіт і P — префіксно замкнена підмножина в A^*. Доведіть, що множина P — нескінченна тоді і тільки тоді, коли існує нескінченна послідовність $(p_n)_{n\geqslant 1}$ елементів у P така, що

$$p_1 < p_2 < p_3 < \cdots .$$

В. 3.10.2. Нехай A — скінченний алфавіт з k літер і $X \subset A^+$ — префіксний код. Для натурального числа $n \geqslant 1$ означимо $\alpha_n = \mathrm{Card}(X \cap A^n)$. Доведіть, що

$$\mathrm{Card}(XA^* \cap A^n) = \sum_{i=1}^{n} \alpha_i k^{n-i} \qquad \text{і} \qquad \sum_{n\geqslant 1} \alpha_n k^{-n} \leqslant 1.$$

(Звідси випливає елементарне доведення наслідку 2.4.6 для префіксних кодів. Див. також твердження 3.7.1.)

Підрозділ 3.2

В. 3.10.3. Нехай A — непорожній алфавіт. $X \subset A^+$ — префіксний код, $P = XA^-$ і $\mathcal{A} = (P, 1, 1)$ — літерний автомат вільного моноїда X^*. Розглянемо автомат $\mathcal{B} = (Q, i, i)$, який є детермінованим, впорядкованим, і таким, що $X^* = \mathrm{Stab}(i)$. Доведіть, що існує сюр'єктивне відображення $\rho\colon P \to Q$ з $\rho(1) = i$ і таке, що $\rho(p \cdot a) = \rho(p) \cdot a$ для $a \in A$.

В. 3.10.4. Префіксний код X називається *ланцюгом*, якщо існують диз'юнктні непорожні множини Y, Z такі, що об'єднання $Y \cup Z$ є префіксною множиною та $X = Y^*Z$.

Нехай X — префіксний код над непорожнім алфавітом A й $\mathcal{A}(X) = (Q, i, t)$ — мінімальний автомат коду X. Доведіть, що такі умови є еквівалентними:

(*i*) $\mathrm{Stab}(i) \neq 1$;
(*ii*) X — ланцюг;
(*iii*) існує слово $u \in A^+$ таке, що $u^{-1}X = X$.

Підрозділ 3.3

В. 3.10.5. Нехай A — непорожній алфавіт і $M(A)$ — моноїд префіксних підмножин вільного моноїда A^* з індукованою з A^* напівгруповою операцією. Доведіть, що $M(A)$ – вільний моноїд і крім того множина максимальних (відп. розпізнуваних) префіксним множин є унітарним справа підмоноїдом у $M(A)$.

(Підказка: Використайте вправу 2.8.9 і множину $\lambda(X) = \min\limits_{x \in X} |x|$.)

Підрозділ 3.4

В. 3.10.6. Доведіть, що кількість префіксно-замкнених множин, які складаються з n елементів, на алфавіті з k літер дорівнює

$$\frac{1}{kn+1}\binom{kn+1}{n} = \frac{1}{(k-1)n+1}\binom{kn}{n}.$$

Для цього, нехай L — єдина множина слів над алфавітом $\{a, b\}$ така, що $L = aL^k \cup b$. Покладемо

$$\|w\| = (k-1)|w|_a - |w|_b.$$

Доведіть, що

(*i*) L є множиною слів w таких, що $\|w\| = -1$ і $\|u\| \geqslant 0$ для довільного власного префікса u слова w;
(*ii*) кожне слово w над алфавітом $\{a, b\}$ таке, що $\|w\| = -1$ має рівно одне спряжено слово в множині L;
(*iii*) існує бієктивне відображення між префіксно-замкненими множинами на k-елементному алфавіті та словами x множини L.

В. 3.10.7. Нехай $A \neq \varnothing$, X і Y — скінченні непорожні підмножини вільного моноїда A^* такі, що добуток XY є однозначним. Доведіть, якщо XY є максимальним префіксним кодом, то X і Y — максимальні префіксні коди.

(Підказка: Використайте той факт, що $\pi(X)\pi(Y) = 1$ для довільного додатнього розподілу Бернуллі на алфавіті A, а потім скористайтесь твердженням 2.5.29.)

В. 3.10.8. Нехай $A \neq \varnothing$, X і Y — два префіксні коди над алфавітом A та

$$P = A^* \setminus XA^*, \qquad Q = A^* \setminus YA^*.$$

Покладемо $R = P \cap Q$. Доведіть, що існує єдиний префіксний код Z такий, що

$$Z = RA \setminus R.$$

Доведіть, що

$$Z = (X \cap Q) \cup (X \cap Y) \cup (P \cap Y).$$

також, доведіть, якщо X і Y — максимальні префіксні множини, то Z також є максимальною префіксною множиною.

В. 3.10.9. Нехай A — скінченний алфавіт. Доведіть, що сім'я розпізнуваних максимальних префіксних кодів є найменшою сім'єю $\mathcal{F}$ множин вільного моноїда A^* такою, що

(*i*) $A \in \mathcal{F}$;

(*ii*) якщо $X, Y \in \mathcal{F}$ і якщо $X = X_1 \cup X_2$ — розбиття на розпізнувані множини X_1 і X_2, то
$$Z = X_1 \cup X_2Y \in \mathcal{F};$$

(*iii*) якщо $X, Y \in \mathcal{F}$ і якщо $X = X_1 \cup X_2$ — розбиття на розпізнувані множини X_1 і X_2, то
$$Z = X_1^*X_2 \in \mathcal{F}.$$

Підрозділ 3.5

В. 3.10.10. Нехай $A \neq \varnothing$ і X — префіксний код над алфавітом A. Доведеть, що такі умови є еквівалентними:

(*i*) $A^*X = X^+$;

(*ii*) X — семафорний код і мінімальна множина семафорів $S = X \setminus A^+X$ задовольняє умову
$$SA^* \cap A^*S = SA^*S \cup S.$$

Зауважимо, що для коду $X = A^*w \setminus A^*wA^+$, ці умови виконується у випадку, коли слово w є необлямованим.

В. 3.10.11. Нехай $A \neq \varnothing$ і $J \subseteq A^+$ — двобічний ідеал. Для кожного слова $x \in J$ через $\|x\|$ позначимо найбільше ціле число n таке, що $x \in J^n$, і покладемо $\|x\| = 0$ для $x \notin J$. Доведіть, що

$$\|x\| + \|y\| \leqslant \|xy\| \leqslant \|x\| + \|y\| + 1,$$

для всіх $x, y \in A^*$.

Підрозділ 3.6

В. 3.10.12. Нехай $X \subset A^+$ — скінченний максимальний префіксний код над непорожнім алфавітом A. Доведіть, якщо X містить літеру $a \in A$, то існує натуральне число $n \geqslant 1$ таке, що a^n є синхронізацією.

В. 3.10.13. Нехай $\mathcal{A}$ — повний детермінований автомат з n станами. Доведіть, якщо автомат $\mathcal{A}$ є синхронізованим, то існує слово-синхронізація довжини щонайбільше n^3 в $\mathcal{A}$.

В. 3.10.14. Нехай $n \geqslant 1$ — натуральне число і M — моноїд відображень з $Q = \mathbb{Z}/n\mathbb{Z}$ в себе, породжений двома відображеннями a і b, визначеними для $i \in Q$ наступним чином: $ia = i + 1$ і

$$ib = \begin{cases} j > i+1, & \text{якщо } 0 \leqslant i < n-t, \\ i+1, & \text{якщо } n-t \leqslant i < n, \end{cases}$$

для деякого цілого числа t такого, що $1 \leqslant t \leqslant n$. Метою цієї вправи є довести, що мінімальний $\operatorname{rank} d$ елементів моноїда M ділить число n, і що $ib \equiv i+1 \mod d$ для всіх $i \in Q$.

Для всіх натуральних чисел e, f таких, що $0 \leqslant e < f \leqslant n$ означимо $I_{e,f} = \{e, e+1, \ldots, f-1\}$ і

$$M_{e,f} = \{m \in M \colon Qm = I_{e,f} \quad \text{і} \quad im = i \quad \text{для всіх} \quad i \in I_{e,f}\}.$$

(a) Доведіть, що

$$I_{e,f}a^j = I_{e+j,f+j} \qquad \text{і} \qquad a^{-j}M_{e,f}a^j = M_{e+j,f+j},$$

для довільного $j \in Q$.

(b) Доведіть, що множина $M_{0,t}$ є непорожньою.
(Підказка: Доведіть, що елемент ba^{-1} має степінь у множині $M_{n-t,n}$.)

(c) Нехай d — найменше натуральне число таке, що множина $M_{0,d}$ э непорожньою. Доведіть, що множина $M_{0,d}$ утворюється з одного такого елемента m такого, що $im \equiv i \mod d$ для всіх $i \in Q$.
(Підказка: Припустимо протилежне, нехай j — найменше ціле число таке, що $jm \not\equiv j \mod d$. Використаємо $a^{j-d}m$ для доведення того, що можна звести до випадку $j = d$. Тоді доведемо, що деяка степінь елемента ma фіксує інтервал, що містить менше елементів за d.)

(d) Доведіть, що число d ділить число n.
(Підказка: Нехай $n = dq + r$ з $q \geqslant 1$ і $0 \leqslant r < d$. Доведіть, що деяка степінь елемента $a^{n-r}m$ міститься в множині M_r.)

(e) Доведіть, що $ib \equiv i+1 \mod d$ для кожного $i \in Q$.

В. 3.10.15. Нехай X — максимальний префіксний код на алфавіті $A = \{a, b\}$. Нехай $a^n \in X$ і $Y = X \cap a^*ba^*$. Покладемо $Y = \{y_0, y_1, \ldots, y_{n-1}\}$ з $y_i = a^iba^j$. Припустимо, що

(*i*) існує натуральне число $m \geqslant 1$ таке, що a^m не є множником слова в X;
(*ii*) для кожного i маємо $|y_i| \leqslant n$ з нерівністю тоді і тільки тоді, коли $n-t \leqslant i \leqslant n-1$;
(*iii*) довжини слів множини Y є взаємно первинними числами.

Доведіть, що код X є синхронізованим. (Підказка: Використайте вправу 3.10.14.)

В. 3.10.16. Нехай $X \subset A^+$ — префіксний код і $X = Y \circ Z$ його максимальний розклад. Доведіть, якщо $X = Y' \circ Z'$ з префіксним кодом Z' і змаксимальним префіксним кодом Y', то $Z'^* \subset Z^*$.

Підрозділ 3.7

В. 3.10.17. Нехай $X \subset A^+$ — тонкий максимальний код і $\pi\colon X \to]0,1]$ — функція така, що

$$\sum_{x\in X} \pi(x) = 1.$$

Означимо ентропію коду X (стосовно до π) так:

$$H(X) = -\sum_{x\in X} \pi(x) \log_k \pi(x),$$

де $k = \mathrm{Card}(A)$. Покладемо $\lambda(X) = \sum_{x\in X} |x|\pi(x)$.

Доведіть, що $H(X) \leqslant \lambda(X)$ і, що рівність виконується тоді і тільки тоді, коли $\pi(x) = k - |x|$ для $x \in X$.

Доведіть, якщо код X є скінченним і має n елементів, то $H(X) \leqslant \log_k n$.

Підрозділ 3.8

В. 3.10.18. Доведіть, що $u(z) = \sum_n u_n z^n$ є породжуючим рядом тонкого максимального префіксного коду на k літерах тоді і тільки тоді, коли справджуються наступні умови:

(*i*) $\sum_{n\geqslant 1} u_n k^{-n} = 1$;

(*ii*) існує натуральне число $p \geqslant 1$ таке, що ряд $v(z) = \sum_n v_n z^n$, який визначається за формулою $u(z) - 1 = v(z)(kz - 1)$ задовольняє умову $v_{n+p} \leqslant v_n(k^p - 1)$ для всіх $n \geqslant 1$.

(Підказка: Доведіть, якщо умова (*ii*) справджується, то ряд u є розподілом довжин максимального префіксного коду X такого, що a^{2p} не є множником жодного з слів множини X.)

В. 3.10.19. Нехай X — тонкий максимальний префіксний код такий, що найбільший спільний дільник довжини слів в X дорівнює 1. Доведіть, що існує код з таким ж розподілом довжин, який є тонким, максимальним і синхронізованим.

(Підказка: Використати вправу 3.10.15.)

Підрозділ 3.9

В. 3.10.20. Мета цієї вправи полягає в тому, щоб показати, що коди Ґоломба з прикладу 3.4.3 є оптимальними префіксними кодами для джерела цілих чисел з геометричним розподілом, який визначається

$$\pi(n) = p^n q, \tag{3.33}$$

для додатних дійсних чисел p, q, що задовольняють умову $p + q = 1$.

Доведіть, що існує єдине ціле число m таке, що

$$p^m + p^{m+1} \leqslant 1 < p^{m-1} + p^m. \tag{3.34}$$

Покажіть, що застосування алгоритму Хаффмана до геометричного розподілу, наведеного у формулі (3.33), дає код з тим же розподілом довжини, що і код Ґоломба порядку m, де число m визначається за формулою (3.34). Це доводить оптимальність коду Ґоломба.

(Підказка: Працюйте над усіченим, але зростаючим джерелом, оскільки алгоритм Гаффмана працює тільки на скінченних алфавітах.)

В. 3.10.21. Доведіть, що код, створений алгоритмом Варна, справді є оптимальним.

(Підказка: Розглянемо повний префіксний код X_1, побудований за алгоритмом, і припустимо, що він не є оптимальним, і розглянемо повний префіксний код X_2, який є оптимальним. Покажіть, що існує слово $x_1 \in X_1$, яке міститься в X_2A^-, та існує слово $x_2 \in X_2$, яке міститься в X_1A^-. Розглянемо слово $p \in X_2$, яке має слово x_1 як префікс і таке, що $pA \subset X_2$ є листками, і побудуємо

$$X_3 = X_2 \setminus (pA \cup \{x_2\}) \cup \{p\} \cup x_2A.$$

Покажіть, що X_3 має вартість меншу або рівну вартості X_2 і ближче до X_1 в тому сенсі, що

$$\mathrm{Card}\left((X_1 \cup X_1A^-) \cap (X_3 \cup X_3A^-)\right) < \mathrm{Card}\left((X_1 \cup X_1A^-) \cap (X_2 \cup X_2A^-)\right).)$$

Нотатки до розділу 3

Результати перших чотирьох розділів відносяться до фольклору, і вони відомі читачам, знайомим з теорією автоматів або з деревами. Код Еліа (приклад 3.1.1) означено в праці Еліа [64].

Деякі конкретні коди використовуються для цілей стиснення для кодування числових даних за відомим розподілом ймовірностей. Вони з'являються, зокрема, в контексті цифрового аудіо- та відеокодування. Закодовані дані є цілими числами і, таким чином, ці коди є нескінченними. У прикладі 3.4.3 представлені коди Ґоломба, які введено в праці Ґоломба [81]. Коди Ґоломба—Райса введені Райсом у препринті [168]. Експоненціальні коди Ґоломба–Райса введено в праці [200], див. також [175]. Експоненціальні коди Ґоломба використовуються на практиці в цифрових передачах. Зокрема, вони є частиною стандарту стиснення відео, технічно відомого як **H.264/MPEG-4 Advanced Video Coding** (**AVC**), див., наприклад, [169].

Гіпотеза однозначності є необхідною в твердженні 3.4.13, як показала Брюєр у праці [40].

Семафорні коди введені Шютценбергером у [183] під назвою $\mathcal{J}$-коди. Всі результати, наведені у підрозділі 3.5, можна знайти в цій праці, яка також містить теорему 3.6.12 і твердження 3.7.18.

Поняття синхронізованого префіксного коду інтенсивно вивчалося в контексті теорії автоматів. Важливість синхронізованих префіксних кодів для відновлення помилок було підкреслено в праці [46]. У статті [68] доведено, що майже всі скінченні

максимальні бінарні префіксні коди є синхронізованими. Це означає, якщо через $\sigma(n)$ позначається кількість синхронізованих максимальних бінарних префіксних кодів з n елементами, а через $\alpha(n)$ позначається загальна кількість максимальних кодів з двома елементами, то $\sigma(n)/\alpha(n)$ наближається до 1. Нагадаємо з формули (3.13), що $\alpha(n)$ є n-им числом Каталана. У праці [36] доведено, що синхронізований максимальний бінарний префіксний код з n елементами має синхронізацію довжини щонайбільше $O(hn \log n)$, де h — максимальна довжина слів коду X.

Давайте нагадаємо *проблему Черного* (*Černý's problem*): нехай дано повний детерміністичний автомат з n станами, якою є точна верхня грань довжини слова-синхронізації, як функції від n? *Гіпотеза Черного* (*Černý's conjecture*) стверджує, що кожен синхронізований сильно зв'язний детерміністичний автомат має слово-синхронізацію довжини щонайбільше $(n-1)^2$. Див. вправу 3.10.13, статті [48,153,159] та розділ відкритих проблем. Приклад 3.6.13 отриманий конструкцією Перрена [157] (див. вправу 14.8.9). Вправа 3.10.15 взята з праці [188]. Максимальні розклади префіксних кодів і твердження 3.6.14 взято з дисертації Перро [158].

Результати розділу 3.7 викладено в іншій термінології в монографії Феллера [66].

Теорема 3.8.2 є зі статті [24]. Метод розщеплення стану, використаний у доведенні леми 3.8.6, надихається символічною динамікою (див. [148] або [13]). Перетворення між різними ваговими автоматами, що розпізнають заданий ряд, що використовуються в доведенні теореми, систематично вивчалися в праці [28].

Алгоритм Ґаффмана вперше описаний в статті Ґаффмана [96], представлений у більшості підручників з теорії алгоритмів. Він має численні застосування в теорії стиску даних, і було розроблено таку варіацію, як адаптивний алгоритм Хаффмана, див [108].

Коди з обмеженням довжини запису мають застосування в практичному кодуванні, див. [128].

Випадок кодових слів з однаковими вагами і нерівними літерними вартостями був розв'язаний Варном у праці [202]. Інший алгоритм можна знайти в статті [156].

Карп у [103] дав перший алгоритм, що забезпечує розв'язок загальної задачі з цілочисельними вартостями. Його алгоритм зводиться до задачі цілочисельного програмування.

Інший підхід Голіна і Роте [79] використовує динамічне програмування. Їх алгоритм дає розв'язок за час $O(n^{k+2})$, де n — кількість кодових слів і k — найбільша з вартостей літер алфавіту A. Цей алгоритм був покращений до $O(n^k)$ у випадку бінарного алфавіта в праці [39].

Впорядковані префіксні коди зазвичай називаються *алфавітними деревами* (*alphabetic tree*). Використання методів динамічного програмування для побудов оптимальних алгебраїчних дерев повертає нас до праці Гільберта та Мура [76]. Їх алгоритм має складність $O(n^3)$ у часі та $O(n^2)$ у просторі. Кнут у праці [107] понизив час до $O(n^2)$.

Ми слідуємо монографії Кнута [109] для експозиції та доведення алгоритму Гарсія–Вахса (див. також [73] і [105]). Алгоритм Гарсія–Вахса є простішим за попередній алгоритм запропонований Гу та Такер у праці [93], який також описаний у першому виданні монографії Кнута. Для доведення та детального описання алгоритму Гу-Такера, і для доповнення див. [95] і [94].

Не існує відомого алгоритму поліноміального часу для загальної проблеми, а також не відомо, чи ця задачає **NP**-складною. Схема апроксимації за поліноміальний час, яка є алгоритмом, що обчислює розв'язок, який є оптимальним з точністю до $1+\varepsilon$ за час $O\left(n \log n \exp\left(O\left(\frac{1}{\varepsilon^2} \log \frac{1}{\varepsilon^2}\right)\right)\right)$ викладено в праці [80].

Алгоритм за кубічний час для розв'язання оптимальної алфавітної префіксної задачі з різними літерними викладено в праці [98].

Результати вправ 3.10.18 і 3.10.19 взято зі статті [188]. Існує сильна взаємозв'язок з теоремою про фарбування доріг, доведеною в розділі 10.

Моноїд префіксних підмножин, означений у вправах 3.10.5, вивчався Ласезом у праці [121]. Вправа 3.10.6 є добре відомим результатом у комбінаториці, див. [131,132]. Вправа 3.10.20 взята з праці [70]. Геометричний розподіл цієї вправи виникає з кодування довжин рядів, де послідовність 0^n1 кодується числом n. Якщо джерело продукує 0 і 1 незалежно від ймовірності p і q, то ймовірність слова 0^n1 дорівнює точно $\pi(n)$. Це представляє практичний інтерес, якщо ймовірність p є великою, оскільки очікуються довгі прогони літери 0, і кодування довжини пробігу реалізує логарифмічне стиснення.

Розділ 4

Автомати

У цьому розділі ми вивчаємо однозначні автомати. Основна ідея — замінити обчислення на слова шляхом обчислень на шляхах, помічених словами. Це техніка, яка добре відома в теорії формальних мов. Вона буде використовуватися цьому розділі в спеціальній формі, що відноситься до характеристичної властивості кодів.

У цій системі відліку головним фактом є еквівалентність кодів і однозначних автоматів. Єдиності шляхів у однозначних автоматах відповідає єдиність факторизації коду. Однозначні автомати появляються як узагальнення детермінованих автоматів аналогічно, як і поняття коду розширює поняття префіксного коду.

Представлено пристрої для кодування та декодування з використанням перетворювачів. Введено спеціальний клас перетворювачів, які називаються послідовними перетворювачами. В розділі 5 буде доведено, що це пов'язано з затримкою дешифрування.

Розділ організований наступним чином.

У першому підрозділі ми вивчаємо однозначні автомати стосовно їх зв'язку з кодами. У наступному підрозділі визначається квітковий автомат. Ми показуємо, що це універсальний автомат у тому сенсі, що будь-який однозначний автомат, пов'язаний з кодом, може бути отриманий шляхом зменшення квіткового автомата цього коду. Ми також показуємо, як розкласти квітковий автомат композиції двох кодів.

В останньому розділі ми використовуємо перетворювачі. Введено алгоритм перетворення перетворювача, що реалізує функцію, в послідовний (можливо, нескінченний) перетворювач.

4.1 Однозначні автомати

Автомат $\mathcal{A} = (Q, I, T)$ над алфавітом A називається *однозначним*, якщо для довільних станів $p, q \in Q$ і слова $w \in A^*$, існує не більше одного шляху зі стану p у стан q з міткою w в автоматі $\mathcal{A}$.

Нагадаємо, з підрозділу 1.10, що через $|\mathcal{A}|$ позначатимемо *поведінку* автомата $\mathcal{A}$. Для кожного слова u коефіцієнт $(|\mathcal{A}|, u)$ — це кількість успішних шляхів, позначених словом u в автоматі $\mathcal{A}$.

Твердження 4.1.1. *Нехай $\mathcal{A} = (Q, i, t)$ — впорядкований автомат з єдиним початковим станом i та єдиним кінцевим станом t. Тоді автомат $\mathcal{A}$ є однозначним тоді і тільки тоді, коли $|\mathcal{A}|$ є характеристичним рядом.*

Доведення. Якщо автомат $\mathcal{A}$ є однозначним, то очевидно, що $|\mathcal{A}|$ є характеристичним рядом.

Навпаки, припустимо, що існує два різні шляхи зі стану p в стан q помічений словом w для деяких станів $p, q \in Q$ і слова $w \in A^*$, то вибравши шляхи $i \xrightarrow{u} p$ і $q \xrightarrow{v} t$, отримуємо, що

$$(|\mathcal{A}|, uwv) \geqslant 2,$$

протиріччяю □

Нагадаємо з підрозділу 1.10, що автомат зірка $\mathcal{A}^*$ пов'язаний з автоматом $\mathcal{A}$ є таким, що $|\mathcal{A}^*| = |\mathcal{A}|^*$.

Твердження 4.1.2. *Нехай $X \subset A^+$ і $\mathcal{A}$ є автомат такий, що $|\mathcal{A}| = X$. Тоді множина X є кодом тоді і лише тоді, коли зірка $\mathcal{A}^*$ автомата $\mathcal{A}$ є однозначним автоматом.*

Доведення. За твердженням 1.10.5 маємо, що $|\mathcal{A}^*| = (\underline{X})^*$. Оскільки автомат $\mathcal{A}^*$ є впорядкованим, то твердження 4.1.1 показує, що автомат $\mathcal{A}^*$ є однозначним тоді і тільки тоді, коли $|\mathcal{A}^*|$ є характеристичним рядом. Позаяк $L(\mathcal{A}^*) = X^*$, це означає, що автомат $\mathcal{A}^*$ є однозначним тоді і тільки тоді, коли $\underline{X}^* = (\underline{X})^*$. Таким чином, ми отримуємо, що наше твердження випливає з твердження 2.6.1. □

Зважаючи на твердження 4.1.2, можна визначити, чи є множина X, задана однозначним автоматом $\mathcal{A}$, кодом, обчислюючи автомат $\mathcal{A}^*$ і перевіряючи, чи автомат $\mathcal{A}^*$ є однозначним. Для цього ми можемо використовувати наступний метод.

Нехай $\mathcal{A} = (Q, I, T)$ — автомат над алфавітом A. *Квадратом $\mathcal{S}$ автомата $\mathcal{A}$* називається автомат

$$\mathcal{S}(\mathcal{A}) = (Q \times Q, I \times I, T \times T),$$

побудований, визначивши, що

$$(p_1, p_2) \xrightarrow{a} (q_1, q_2)$$

є ребром автомата $\mathcal{S}(\mathcal{A})$ тоді і тільки тоді, коли

$$p_1 \xrightarrow{a} q_1 \qquad \text{і} \qquad p_2 \xrightarrow{a} q_2$$

є ребрами автомата $\mathcal{A}$.

Твердження 4.1.3. *Автомат $\mathcal{A} = (Q, I, T)$ є однозначним тоді і тільки тоді, коли не існує шляху в автоматі $\mathcal{S}(\mathcal{A})$ вигляду*

$$(p, p) \xrightarrow{u} (r, s) \xrightarrow{v} (q, q) \tag{4.1}$$

з $r \neq s$.

Доведення. Існування шляху вигляду (4.1) в автоматі $\mathcal{S}(\mathcal{A})$ еквівалентно існуванню пари шляхів

$$p \xrightarrow{u} r \xrightarrow{v} q \qquad \text{і} \qquad p \xrightarrow{u} s \xrightarrow{v} q$$

з однією міткою uv в автоматі $\mathcal{A}$. □

Щоб прийняти рішення, чи є розпізнавана множина X, визначена однозначним скінченним автоматом $\mathcal{A}$ є кодом, достатньо обчислити автомат $\mathcal{A}^*$ і перевірити, чи автомат $\mathcal{A}^*$ є однозначним, перевіряючи скінченний автомат $\mathcal{S}(\mathcal{A})$, шукаючи шляхи вигляду (4.1).

Приклад 4.1.4. Розглянемо знову автомат $\mathcal{A}^*$ з прикладу 1.10.7, повторений тут для зручності на рис. 4.1. Автомат $\mathcal{S}(\mathcal{A}^*)$ зображено на рис. 4.2, де витягується лише

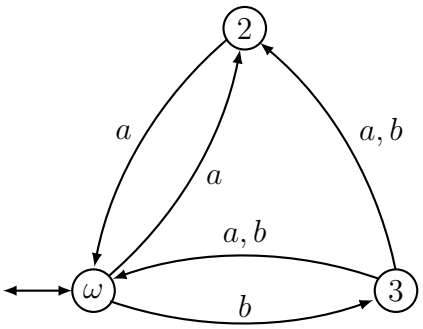


Рис. 4.1: Однозначний автомат $\mathcal{S}(\mathcal{A}^*)$

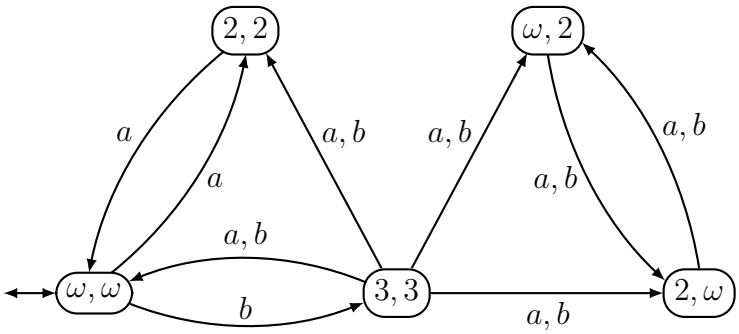


Рис. 4.2: Частина квадрата автомата $\mathcal{S}(\mathcal{A}^*)$

частина, доступна зі станів (q, q). Це доводить, що автомат $\mathcal{A}^*$ є однозначним.

Наступне твердження є доповненням до твердження 4.1.2.

Твердження 4.1.5. *Нехай $\mathcal{A} = (Q, 1, 1)$ — однозначний автомат над алфавітом A з єдиним початковим і кінцевим станом. Тоді його поведінка $|\mathcal{A}|$ є характеристичним рядом деякого вільного підмоноїда в A^*.*

Доведення. Нехай $M \subset A^*$ — така підмножина, що $|\mathcal{A}| = \underline{M}$. Очевидно, що множина M є підмоноїдом вільного моноїда A^*. Ми доведемо, що M є стійким підмоноїдом. Для цього, припустимо, що

$$u, wv, uw, v \in M.$$

Тоді в автоматі $\mathcal{A}$ існують шляхи

$$1 \xrightarrow{u} 1, \qquad 1 \xrightarrow{wv} 1, \qquad 1 \xrightarrow{uw} 1, \qquad 1 \xrightarrow{v} 1.$$

Два середні шляхи факторизуються як

$$1 \xrightarrow{w} p \xrightarrow{v} 1, \qquad 1 \xrightarrow{u} q \xrightarrow{w} 1,$$

для деяких станів $p, q \in Q$. Таким чином, існує два шляхи

$$1 \xrightarrow{u} 1 \xrightarrow{w} p \xrightarrow{v} 1,$$
$$1 \xrightarrow{u} q \xrightarrow{w} 1 \xrightarrow{v} 1.$$

Оскільки автомат $\mathcal{A}$ є однозначним, то ці шляхи збігаються, звідки випливає, що $1 = p = q$. Отже, отримуємо, що $w \in M$. Отож, моноїд є стійким, а за твердженням 2.2.6 він є вільним. □

Наступний результат стосується визначника матриці, який природним чином пов'язаний з автоматом. Він має самостійний незалежний інтерес, і буде використаний пізніше, у розділі 7. Нагадаємо, що через $\alpha(w)$ позначаємо комутативний образ слова $w \in A^*$ і $\alpha(\sigma)$ комутативний образ формального ряду σ. Формула (4.2) дає вираз полінома $1 - \alpha(\underline{X})$ для скінченного коду X.

Твердження 4.1.6. *Нехай $X \subset A^+$ — скінченний код над непорожнім алфавітом A й $\mathcal{A} = (Q, 1, 1)$ — однозначний впорядкований скінченний автомат, який розпізнає вільний моноїд X^*. Нехай M — $Q \times Q$-матриця з елементами в множині комутативних поліномів $\mathbb{Q}[A]$ з раціональними коефіцієнтами над алфавітом A така, що $M_{p,q}$ є сумою елементів множини*

$$A_{pq} = \left\{ a \in A \colon p \xrightarrow{a} q \right\}.$$

Тоді

$$1 - \alpha(\underline{X}) = \det(I - M). \tag{4.2}$$

Доведення. Кожен шлях $p \xrightarrow{w} q$ з $q \neq 1$ і $w \in A^+$ проходить через стан 1. В іншому випадку $uw^*v \in X$ для слів u та v таких, що $1 \xrightarrow{u} q \xrightarrow{v} 1$, а це суперечить скінченності коду X. Отож, ми можемо вибрати множину $Q = \{1, 2, \ldots, n\}$ таким чином, що як тільки $i \xrightarrow{a} j$ для $a \in A$, $j \neq 1$, то $i < j$. Для $i, j \in Q$ означимо елемент з множини $\mathbb{Q}[A]$ за формулою

$$r_{ij} = \delta_{ij} - \underline{A}_{ij}, \tag{4.3}$$

де δ_{ij} — символ Кронекера. Нехай

$$\Delta = \sum_{\sigma \in \mathfrak{S}_n} (-1)^{\varepsilon(\sigma)} r_{1,1\sigma} r_{2,2\sigma} \cdots r_{n,n\sigma}$$

— поліном, де через $\varepsilon(\sigma) = \pm 1$ позначається знак підстановки σ. За означенням, $\varepsilon(\sigma) = 1$, якщо σ — парна підстановка, і $\varepsilon(\sigma) = -1$ в протилежному випадку. Згідно добре відомої формули для визначників маємо

$$\det(I - M) = \alpha(\Delta).$$

Таким чином, достатньо довести, що

$$\Delta = 1 - \underline{X}. \tag{4.4}$$

Для цього, нехай

$$\Delta_\sigma = r_{1,1\sigma} r_{2,2\sigma} \cdots r_{n,n\sigma},$$

а отже отримуємо, що

$$\Delta = \sum_{\sigma \in \mathfrak{S}_n} (-1)^{\varepsilon(\sigma)} \Delta_\sigma.$$

Розглянемо підстановку $\sigma \in \mathfrak{S}_n$ таку, що $\Delta_\sigma \neq 0$. Якщо $\sigma \neq 1$, то вона має хоча б один цикл $(i_1, i_2, \ldots, i_k)$ довжини $k \geqslant 2$. Оскільки $\Delta_\sigma \neq 0$, за формулою (4.3) множини $A_{i_1 i_2}, A_{i_2 i_3}, \ldots, A_{i_k i_1}$ є непорожніми. Звідси випливає, що цикл $(i_1, i_2, \ldots, i_k)$ містить стан 1. Отже, кожна підстановка σ з $\Delta_\sigma \neq 0$ складається з фіксованих точок і одного циклу, що містить стан 1. Якщо цим циклом є $(i_1, i_2, \ldots, i_k)$ з $i_1 = 1$, то

$$1 < i_2 < \cdots < i_k$$

за вибором впорядкування станів у автоматі $\mathcal{A}$. Покладемо $X_\sigma = A_{1 i_2} A_{i_2 i_3} \cdots A_{i_k, 1}$. Тоді $\Delta_\sigma = (-1)^k X_\sigma$ і також $(-1)\varepsilon(\sigma) = (-1)^{k+1}$ оскільки цикл довжини k має ту ж парність, що і $k + 1$.

Множина X_σ складається зі слів $a_1 a_2 \cdots a_k$ з $a_i \in A$ і така, що

$$1 \xrightarrow{a_1} i_2 \xrightarrow{a_2} i_3 \xrightarrow{a_3} \cdots \xrightarrow{a_{k-1}} i_k \xrightarrow{a_k} 1.$$

Ці слова містяться в коді X. Через S позначимо множину підстановок $\sigma \in \mathfrak{S}_n \setminus \{1\}$, які мають рівно один нетривіальний цикл, а саме цикл, який містить 1. Тоді $X = \sum_{\sigma \in S} \underline{X}_\sigma$, оскільки кожне слово в коді X є міткою єдиного шляху $(1, i_2, i_3, \ldots, i_k, 1)$ з $1 < i_2 < \cdots < i_k$. Звідси випливає, що

$$\Delta = 1 + \sum_{\sigma \in S} (-1)^{\varepsilon(\sigma)} \Delta_\sigma = 1 - \sum_{\sigma \in S} \underline{X}_\sigma = 1 - \underline{X},$$

що і завершує доведення. □

Приклад 4.1.7. Нехай $X = \{aa, ba, bb, baa, bba\}$. Це є код з прикладу 2.3.7. Однозначний автомат визначений на рис. 4.1 розпізнає моноїд X^*. Тут матриця M має вигляд

$$M = \begin{bmatrix} 0 & a & b \\ a & 0 & 0 \\ a + b & a + b & 0 \end{bmatrix}$$

і легко перевіряється, що $\det(I - M) = 1 - \alpha(\underline{X})$.

Однозначними раціональними операціями на множинах слів є:

(*i*) диз'юнктне об'єднання;
(*ii*) однозначний добуток;
(*iii*) операція зірка коду.

Нагадаємо, що добуток XY називається *однозначним*, якщо з $xy = x'y'$ для $x, x' \in X$, $y, y' \in Y$ випливає, що $x = x'$ і $y = y'$. Зірка коду, звичайно, є вільним підмоноїдом.

Сім'є *однозначних раціональних підмножин* вільного моноїда A^* називається найменша сім'я підмножин моноїда A^*, що містить скінченні множини, і є замкненою стосовно однозначних раціональних операцій. Описання раціональної множини однозначними раціональними операціями називається *однозначним раціональним виразом* або *однозначним регулярним виразом*.

Твердження 4.1.8. *Кожне раціональна множина є однозначно раціональною.*

Доведення. За твердженням 1.4.1 кожна раціональна множина розпізнається скінченним детермінованим автоматом. У цьому випадку, формули (1.10)–(1.12) забезпечують однозначний раціональний вираз для цієї множини. □

Приклад 4.1.9. Нехай $A = \{a, b\}$. Однозначним раціональним виразом для множини A^*bA^* є a^*bA^* (або A^*ba^*).

4.2 Квітковий автомат

У цьому розділі ми описуємо конструкцію "універсального автомата", який розпізнає підмоноїд вільного моноїда A^*.

Нехай X — довільна непорожня підмножина вільного моноїда A^+. Ми означимо автомат

$$\mathcal{A}_D(X) = (Q, I, T)$$

наступним чином

$$Q = \{(u, v) \in A^* \times A^* \colon uv \in X\}, \qquad I = \{1\} \times X, \qquad T = X \times \{1\},$$

з ребрами $(u, v) \xrightarrow{a} (u', v')$ тоді і тільки тоді, коли $ua = u'$ і $v = av'$. Іншими слова, ребрами автомата $\mathcal{A}_D(X)$ є

$$(u, av) \xrightarrow{a} (ua, v), \qquad uav \in X.$$

Це еквівалентно тому, що множина ребер автомата $\mathcal{A}_D(X)$ є диз'юнктним об'єднанням множин ребер зображених на рис. 4.3 для кожного слова $x = a_1a_2 \cdots a_n$ з множини

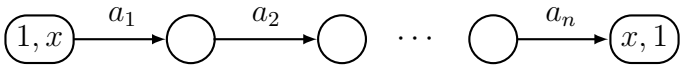


Рис. 4.3: Ребра автомата $\mathcal{A}_D(X)$ для слова $x = a_1a_2 \cdots a_n$

X. Автомат $\mathcal{A}_D(X)$ є однозначним і розпізнає множину X, тобто

$$|\mathcal{A}_D(X)| = \underline{X}.$$

Квітковим автоматом множини X є за означенням зірка автомата $\mathcal{A}_D(X)$, яка отримується конструкцією, описаною в підрозділі 1.10, і позначаються $\mathcal{A}_D^*(X)$, а не $(\mathcal{A}_D(X))^*$. Через φ_D ми позначатимемо пов'язане зображення. Таким чином, наслідуючи конструкцію підрозділу 1.10, автомат $\mathcal{A}_D^*(X)$ отримується за два кроки наступним чином. Почавши з автомата $\mathcal{A}_D(X)$, додамо новий стан ω і ребра

$$\begin{array}{rcl} \omega \xrightarrow{a} (a, v) & \text{для} & av \in X; \\ (u, a) \xrightarrow{a} \omega & \text{для} & ua \in X; \\ \omega \xrightarrow{a} \omega & \text{для} & a \in X. \end{array}$$

Цей автомат є тепер обрізаним. Стани в $1 \times X$ і $X \times 1$ більше не є доступними або кодоступними, а отже, зникають. Зазвичай стан ω позначається через $(1, 1)$. Тоді автомат $\mathcal{A}_D^*(X)$ набуває вигляду

$$\mathcal{A}_D^*(X) = (P, (1, 1), (1, 1)),$$

зі станами

$$P = \big\{(u, v) \in A^+ \times A^+ \colon uv \in X\big\} \cup \{(1, 1)\},$$

і також існує чотири типи ребер

$$\begin{array}{rcll} (u, av) \xrightarrow{a} (ua, v) & \text{для} & uav \in X, & (u, v) \neq (1, 1), \\ (1, 1) \xrightarrow{a} (a, v) & \text{для} & av \in X, & v \neq 1, \\ (u, a) \xrightarrow{a} (1, 1) & \text{для} & ua \in X, & u \neq 1, \\ (1, 1) \xrightarrow{a} (1, 1) & \text{для} & a \in X. & \end{array}$$

Термінологія натхненна графічним зображенням цього автомата. Справді, кожне слово $x \in X$ визначає простий шлях

$$(1, 1) \xrightarrow{x} (1, 1)$$

в автоматі $\mathcal{A}_D^*(X)$. Якщо $x = a \in A$, то цей шлях є ребро

$$(1, 1) \xrightarrow{a} (1, 1).$$

Якщо $x = a_1 a_2 \cdots a_n$ з $n \geqslant 2$, то цей шлях є ребро

$$(1, 1) \xrightarrow{a_1} (a_1, a_2 \cdots a_n) \xrightarrow{a_2} (a_1 a_2, a_3 \cdots a_n) \xrightarrow{a_3} \cdots \xrightarrow{a_{n-1}} (a_1 a_2 \cdots a_{n-1}, a_n) \xrightarrow{a_n} (1, 1).$$

Приклад 4.2.1. Нехай $X = \{aa, ba, bb, baa, bba\}$. Квітковий автомат множини X зображено на рис. 4.4.

Теорема 4.2.2. *Нехай X — непорожня підмножина вільної напівгрупи A^+. Наступні умови є еквівалентними:*

(*i*) *X є кодом;*

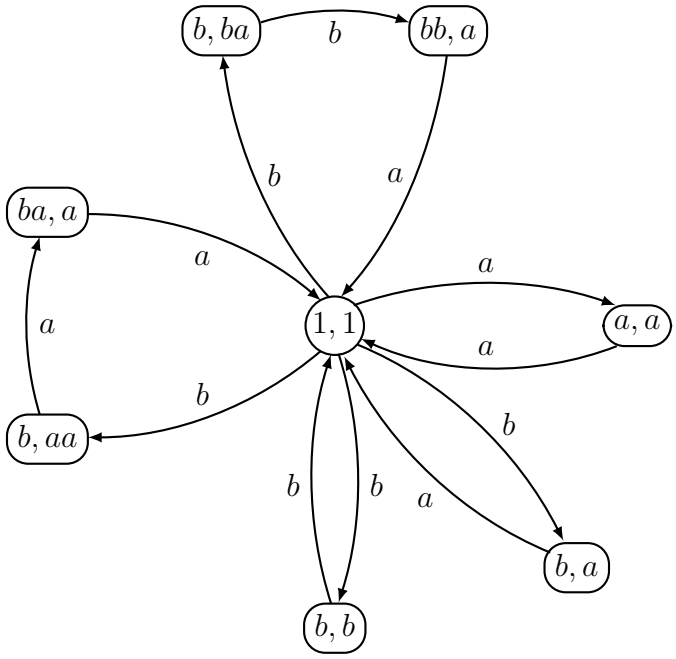


Рис. 4.4: Квітковий автомат множини $X = \{aa, ba, bb, baa, bba\}$

(*ii*) *для довільного однозначного автомата* $\mathcal{A}$*, який розпізнає множину* X*, автомат* $\mathcal{A}^*$ *є однозначним;*
(*iii*) *квітковий автомат* $\mathcal{A}_D^*(X)$ *є однозначним;*
(*iv*) *Існує однозначний автомат* $\mathcal{A} = (Q, 1, 1)$*, який розпізнає вільний моноїд* X^* *і* X *є мінімальною множиною породжуючих елементів вільного моноїда* X^**.*

Доведення. Імплікація $(i) \Longrightarrow (ii)$ — це твердження 4.1.2.

Імплікація $(ii) \Longrightarrow (iii)$ є очевидною.

Для доведення імплікації $(iii) \Longrightarrow (iv)$ достатньо показати, що X є мінімальною породжуючою множиною вільного моноїда X^*. Припустимо протилежне і нехай $x \in X$, $y, z \in X^+$ — слова такі, що $x = yz$. Тоді існує в автоматі $\mathcal{A}_D^*(X)$ простий шлях

$$(1,1) \xrightarrow{x} (1,1)$$

і шлях

$$(1,1) \xrightarrow{y} (1,1) \xrightarrow{z} (1,1),$$

який також має мітку слово x. Ці шляхи є різними, а отже автомат $\mathcal{A}_D^*(X)$ є неоднозначним.

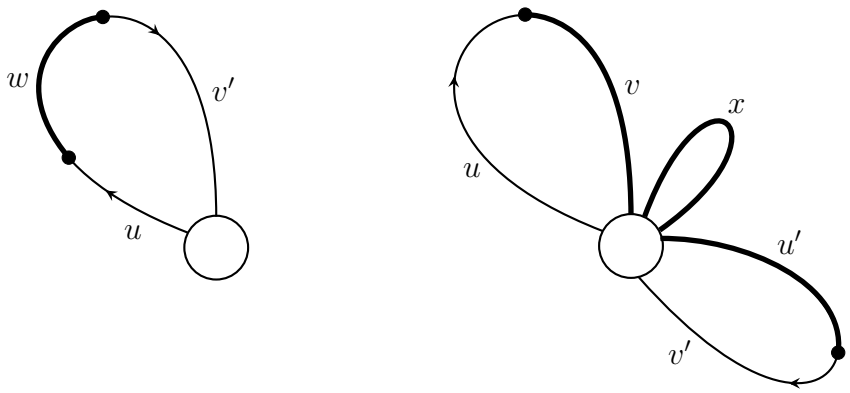
На завершенні, для доведення імплікації $(iv) \Longrightarrow (i)$, зауважимо, що за твердженням 4.1.5, моноїд X^* є вільним. Отож, множина X є кодом. □

Тепер ми чітко опишемо шляхи в квітковому автоматі коду.

Твердження 4.2.3. *Нехай* $X \subset A^+$ *— код. Наступні умови є еквівалентними для всіх слів* $w \in A^*$ *та всіх станів* (u, v)*,* (u', v') *в автоматі* $\mathcal{A}_D^*(X)$*:*

(*i*) *в автоматі* $\mathcal{A}_D^*(X)$ *існує шлях* $c\colon (u,v) \xrightarrow{w} (u',v')$;
(*ii*) $w \in vX^*u' \vee (uw = u' \wedge v = wv')$;
(*iii*) $uw \in X^*u' \wedge wv' \in vX^*$.

Доведення. (*i*) $\Longrightarrow$ (*ii*) Якщо c — простий шлях, то він є шляхом в автоматі $\mathcal{A}_D$. Отже, $uw = u'$ і $v = wv'$ (рис. 4.5(a)).



(a) (b)

Рис. 4.5: Шляхи в квітковому автоматі

В іншому випадку шлях c розкладається в

$$c\colon (u,v) \xrightarrow{v} (1,1) \xrightarrow{x} (1,1) \xrightarrow{u'} (u',v')$$

з $w = vxu'$ та $x \in X^*$ (рис. 4.5(b)).

(*ii*) $\Longrightarrow$ (*iii*) Якщо $w \in vX^*u'$, то $uw \in uvX^*u' \subset X^*u'$ і $w \in vX^*u'v' \subset vX^*$, оскільки $uv, u'v' \in X \cup \{1\}$. Якщо $uw = u'$ і $v = wv'$, то формули є очевидними.

(*iii*) $\Longrightarrow$ (*i*) За припущенням, існують слова $x, y \in X^*$ такі, що $uw = xu'$, $wv' = vy$. Нехай $z = uwv'$. Тоді

$$z = uwv' = xu'v' = uvy \in X^*.$$

Кожна з цих трьох факторизацій визначає шлях в автоматі $\mathcal{A}_D^*(X)$ (див. рис. 4.5):

$$\begin{aligned}
c\colon (1,1) &\xrightarrow{u} (\overline{u},\overline{v}) \xrightarrow{w} (\overline{u'},\overline{v'}) \xrightarrow{v'} (1,1),\\
c'\colon (1,1) &\xrightarrow{x} (1,1) \xrightarrow{u'} (u',v') \xrightarrow{v'} (1,1),\\
c''\colon (1,1) &\xrightarrow{u} (u,v) \xrightarrow{v} (1,1) \xrightarrow{y} (1,1).
\end{aligned}$$

Зауважимо, що тут шляхи $(1,1) \xrightarrow{u} (u,v) \xrightarrow{v} (1,1)$ і $(1,1) \xrightarrow{u'} (u',v') \xrightarrow{v'} (1,1)$ можуть мати довжину 0. Оскільки множина X є кодом, то автомат $\mathcal{A}_D^*(X)$ є однозначним, а отже $c = c' = c''$. Ми отримуємо, що $(u,v) = (\overline{u},\overline{v})$ і $(u',v') = (\overline{u'},\overline{v'})$. Отож, маємо

$$(u,v) \xrightarrow{w} (u',v'),$$

що завершує доведення імплікації. □

Квітковий автомат коду має "багато" станів. Зокрема, квітковий автомат нескінченного коду є нескінченним, навіть якщо існує скінченний однозначний автомат, що розпізнає вільний моноїд X^*, коли код X є розпізнуваним. Ми покажемо, що автомат $\mathcal{A}_D^*(X)$ є універсальним серед автоматів, що розпізнають вільний моноїд X^*, у наступному сенсі.

Розглянемо два однозначні автомати

$$\mathcal{A} = (P, 1, 1) \qquad \text{і} \qquad \mathcal{B} = (Q, 1, 1),$$

та їх асоційовані зображення $\varphi_\mathcal{A}$ і $\varphi_\mathcal{B}$. Відображення $\rho\colon P \to Q$ називається *редукцією* автомата $\mathcal{A}$ на автомат $\mathcal{B}$, якщо воно є сюр'єктивним, $\rho(1) = 1$ і якщо, для всіх слів $w \in A^*$ виконується умова

$$(q, \varphi_\mathcal{B}(w), q') = 1$$

тоді і тільки тоді, коли існують стани $p, p' \in P$ такі, що

$$(p, \varphi_\mathcal{A}(w), p') = 1, \qquad \rho(p) = q, \qquad \rho(p') = q'.$$

Означення стверджує, якщо $p \xrightarrow{w} p'$ є шляхом в автоматі $\mathcal{A}$, то $\rho(p) \xrightarrow{w} \rho(p')$ є шляхом в автоматі $\mathcal{B}$. Навпаки, шлях $q \xrightarrow{w} q'$ в автоматі $\mathcal{B}$ може бути "піднятий" до деякого шляху $p \xrightarrow{w} p'$ в автоматі $\mathcal{A}$ з $p \in \rho^{-1}(q), p' \in \rho^{-1}(q')$.

Іншим шляхом зображення означення є наступний. Матриця $\varphi_\mathcal{B}(w)$ можна отримана з матриці $\varphi_\mathcal{A}(w)$ шляхом розбиття останньої на блоки, індексовані парою класів еквівалентності, визначеної відображенням ρ, а потім замінити нульові блоки на 0, а нульові блоки — на 1.

Зауважимо, якщо відображення ρ є редукцією автомата $\mathcal{A}$ на автомат $\mathcal{B}$, то для всіх слів $w, w' \in A^*$, виконується така імплікація:

$$\varphi_\mathcal{A}(w) = \varphi_\mathcal{A}(w') \qquad \Longrightarrow \qquad \varphi_\mathcal{B}(w) = \varphi_\mathcal{B}(w').$$

Отже, існує єдиний сюр'єктивний морфізм

$$\widehat{\rho}\colon \varphi_\mathcal{A}(A^*) \to \varphi_\mathcal{B}(A^*)$$

такий, що $\varphi_\mathcal{B} = \widehat{\rho} \circ \varphi_\mathcal{A}$. Морфізм $\widehat{\rho}$ називається *морфізмом асоційованим* з редукцією ρ.

Твердження 4.2.4. *Нехай $\mathcal{A} = (P, 1, 1)$ і $\mathcal{B} = (Q, 1, 1)$ — два однозначні впорядковані автомати. Тоді існує хоча б одна редукція автомата $\mathcal{A}$ на автомат $\mathcal{B}$. Якщо $\rho\colon P \to Q$ — редукція, то*

(1) $|\mathcal{A}| \subseteq |\mathcal{B}|$;
(2) $|\mathcal{A}| = |\mathcal{B}|$ *тоді і тільки тоді, коли* $\rho^{-1}(1) = 1$.

Доведення. Нехай $\rho\colon P \to Q$ і $\rho'\colon P \to Q$ — дві редукції автомата $\mathcal{A}$ на автомат $\mathcal{B}$. Нехай $p \in P$ і $q = \rho(p)$, $q' = \rho'(p)$. Нехай $u, v \in A^*$ — слова такі, що $1 \xrightarrow{u} p \xrightarrow{v} 1$ в автоматі $\mathcal{A}$. Тоді ми отримуємо в автоматі $\mathcal{B}$ шляхи

$$1 \xrightarrow{u} q \xrightarrow{v} 1 \qquad \text{і} \qquad 1 \xrightarrow{u} q' \xrightarrow{v} 1.$$

Оскільки автомат $\mathcal{B}$ є однозначним, то $q = q'$. Отож, отримуємо $\rho = \rho'$.

(1). Якщо $w \in |\mathcal{A}|$, то існує шлях $1 \xrightarrow{w} 1$ в автоматі $\mathcal{A}$, а отже існує шлях $1 \xrightarrow{w} 1$ в автоматі $\mathcal{B}$. Таким чином, отримуємо, що $w \in |\mathcal{B}|$.

(2). Нехай $w \in |\mathcal{B}|$. Тоді існує шлях $p \xrightarrow{w} p'$ в автоматі $\mathcal{A}$ з $\rho(p) = \rho(p') = 1$. Якщо $1 = \rho^{-1}(1)$, то це є успішній шлях в автоматі $\mathcal{A}$ і $w \in |\mathcal{A}|$. Навпаки, нехай $p \neq 1$. Нехай $1 \xrightarrow{u} p \xrightarrow{v} 1$ — простий шлях в автоматі $\mathcal{A}$. Тоді $uv \in X$, де X — база поведінки $|\mathcal{A}|$. Тепер в автоматі $\mathcal{B}$ маємо we have $1 \xrightarrow{u} \rho(p) \xrightarrow{v} 1$. Оскільки $|\mathcal{A}| = |\mathcal{B}|$, то маємо $\rho(p) \neq 1$. Отож, отримуємо $\rho^{-1}(1) = 1$. □

Твердження 4.2.5. *Нехай $X \subset A^+$ — код і $\mathcal{A}^*_D(X)$ — його квітковий автомат. Для кожного однозначного впорядкованого автомата $\mathcal{A} = (Q, 1, 1)$, який розпізнає вільний моноїд X^*, існує редукція автомата $\mathcal{A}^*_D(X)$ на автомат $\mathcal{A}$.*

Доведення. Нехай Let $\mathcal{A}^*_D(X) = (P, (1,1), (1,1))$. Визначимо відображення $\rho\colon P \to Q$ наступним чином. Нехай $p = (u, v) \in P$. Якщо $p = (1, 1)$, то покладемо $\rho(p) = 1$. В іншому випадку $uv \in X$, та існує єдиний шлях $c\colon 1 \xrightarrow{u} q \xrightarrow{v} 1$ в автоматі $\mathcal{A}$. Тоді покладемо $\rho(p) = q$.

Відображення ρ є сюр'єктивним. Нехай справді $q \in Q$, $q \neq 1$. Нехай

$$c_1\colon 1 \xrightarrow{u} q \qquad \text{і} \qquad c_2\colon q \xrightarrow{v} 1$$

— прості шляхи в автоматі $\mathcal{A}$. Тоді $uv \in X$ і стан $p = (u, v) \in P$ задовольняє умову $\rho(p) = q$.

Тепер перевіримо, що відображення ρ є редукцією. Для цього, припустимо спочатку, що для слова $w \in A^*$, і $q, q' \in Q$, існує шлях в автоматі $\mathcal{A}$ зі стану q в стан q', який має мітку слово w. Розглянемо два простих шляхи

$$e\colon 1 \xrightarrow{u} q \qquad \text{і} \qquad e'\colon q' \xrightarrow{v} 1$$

в автоматі $\mathcal{A}$. Тоді в автоматі $\mathcal{A}$ існує шлях

$$1 \xrightarrow{u} q \xrightarrow{w} q' \xrightarrow{v} 1.$$

Отже, отримуємо, що $uwv' \in X^*$. Таким чином,

$$uwv' = x_1 x_2 \cdots x_n$$

для деяких $x_1, x_2, \ldots, x_n \in X$. Оскільки шлях e є простим, то слово u є префіксом слова x_1, і аналогічно отримуємо, що v' є суфіксом слова x_n. Поклавши $x_1 = uv$ і $x_n = u'v'$, маємо

$$uwv' = uvx_2 \cdots x_n = x_1 x_2 \cdots x_{n-1} u'v',$$

звідки випливає, що $uw \in X^*u'$ і $wv' \in uX^*$. За твердженням 4.2.3 отримуємо $((u, v), \varphi_D(w), (u', v')) = 1$.

Припустимо тепер навпаки, що

$$(p, \varphi_D(w), p') = 1 \tag{4.5}$$

для деяких $p = (u, v)$, $p' = (u', v')$ і $w \in A^*$. Нехай $q = \rho(p)$ і $q' = \rho(p')$. За конструкцією, існують в автоматі $\mathcal{A}$ шляхи

$$1 \xrightarrow{u} q \xrightarrow{v} 1 \qquad \text{і} \qquad 1 \xrightarrow{u'} q' \xrightarrow{v'} 1. \tag{4.6}$$

За твердженням 4.2.3 формула (4.5) еквівалентна умові

$$\{uw = u' \text{ і } v = wv'\} \qquad \text{або} \qquad \{w = vxu' \text{ для деякого слова } x \in X^*\}.$$

У першому випадку маємо, що $uv = uwv' = u'v'$. Отож, два шляхи (4.6) збігаються, даючи шлях в автоматі $\mathcal{A}$,

$$1 \xrightarrow{u} q \xrightarrow{w} q' \xrightarrow{v'} 1.$$

У другому випадку існує в автоматі $\mathcal{A}$ шлях

$$q \xrightarrow{v} 1 \xrightarrow{x} 1 \xrightarrow{u'} q'.$$

Таким чином, в обох випадках отримуємо, що $(p, \varphi_D(w), p') = 1$. □

Приклад 4.2.6. Для коду

$$X = \{aa, ba, bb, baa, bba\}$$

квітковий автомат зображено на рис. 4.6.

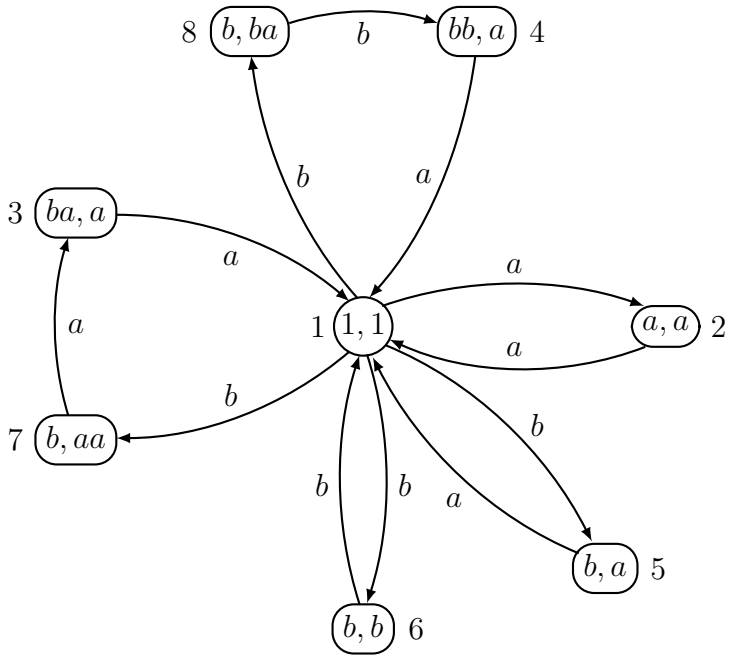


Рис. 4.6: Квітковий автомат коду $X = \{aa, ba, bb, baa, bba\}$ з його перенумерованими станами

Розглянемо автомат, зображений на рис. 4.7. Відображення $\rho\colon P \to 1, 2, 3$ визначається наступним чином:

$$\begin{aligned}
&\rho((a, a)) = \rho((ba, a)) = \rho((bb, a)) = 2,\\
&\rho((b, a)) = \rho((b, b)) = \rho((b, aa)) = \rho((b, ba)) = 3,\\
&\rho((1, 1)) = 1.
\end{aligned}$$

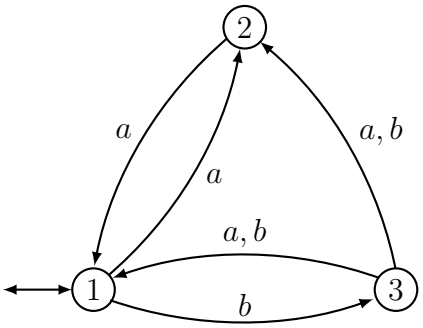


Рис. 4.7: Інший автомат, що розпізнає вільний моноїд X^*

Матрицями асоційованих зображень (зі станами занумерованими, як зазначено на рис. 4.6 і рис. 4.7) є

$$\varphi_D(a) = \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \end{matrix} \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \qquad \varphi(a) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix},$$

$$\varphi_D(b) = \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \end{matrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}, \qquad \varphi(b) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

Концепція редукції дає змогу вказати на зв'язок між квітковими автоматами складеного коду та його компонентів.

Твердження 4.2.7. *Нехай $Y \subset B^+$, $Z \subset A^+$ — два композиційовні коди та $X = Y \circ_\beta Z$. Якщо код Y є повним, то існує редукція автомата $\mathcal{A}_D^*(X)$ на автомат $\mathcal{A}_D^*(Z)$. Більше того, автомат $\mathcal{A}_D^*(Y)$ можна ідентифікувати через відображення β з обмеженням автомата $\mathcal{A}_D^*(X)$ на стани в $Z^* \times Z^*$.*

Доведення. Нехай P і S — множини станів автоматів $\mathcal{A}_D^*(X)$ і $\mathcal{A}_D^*(Z)$, відповідно, і нехай φ_X і φ_Z — зображення асоційовані до автоматів $\mathcal{A}_D^*(X)$ і $\mathcal{A}_D^*(Z)$.

Означимо відображення $\rho\colon P \to S$ наступним чином. Спочатку, нехай $\rho((1,1)) = (1,1)$. Далі розглянемо $(u,v) \in P\backslash\{(1,1)\}$. Тоді $uv \in Z^+$. Отже, існують єдині $z, \overline{z} \in Z^*$ і $(r,s) \in S$ такі, що

$$u = zr \qquad \text{і} \qquad v = s\overline{z}$$

(див. рис. 4.8). Тоді нехай $\rho(u,v) = (r,s)$. Відображення ρ є сюр'єктивним. Справді,

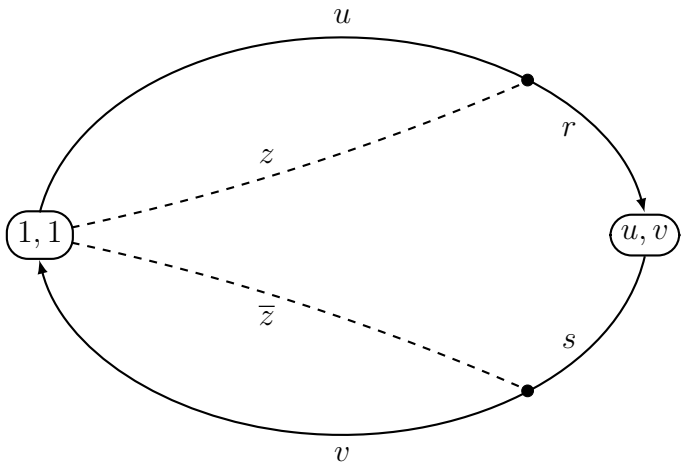


Рис. 4.8: Розклад пелюстки.

кожне слово в коді Z зустрічається в щонайменше одному слові в коді X, і таким чином, кожен стан в S досягається в уточненні стану в P.

Щоб показати, що відображення ρ є редукцією, припустимо, що

$$((u, v), \varphi_X(w), (u', v')) = 1.$$

Нехай

$$(r, s) = \rho((u, v)), \qquad (r', s') = \rho((u', v')) \qquad \text{і} \qquad z, \overline{z}, z', \overline{z}' \in Z^*$$

є такими, що

$$u = zr, \qquad v = s\overline{z}, \qquad u' = z'r', \qquad v' = s'\overline{z}'.$$

За твердженням 4.2.3 маємо, що $uw \in X^*u'$ і $wv' \in vX^*$. Таким чином, отримуємо, що $zrw \in Z^*r'$ і $ws'\overline{z}' \in sZ^*$, а це означає, що $zrws' \in Z^*$ і $rws'\overline{z} \in Z^*$. Це в свою чергу показує, з огляду на стабільність вільного моноїда Z^*, що $rws' \in Z^*$. Покладемо $zrw = \widehat{z}r'$, з $z \in Z^*$. Тоді

$$\widehat{z}(r's') = z(rws'),$$

і кожен з цих чотирьох множників у цьому рівнянні міститься у вільному моноїді Z^*. З того, що Z є кодом, отримуємо, що або $\widehat{z} = zt$ або $z = \widehat{z}t$ для деякого слова $t \in Z^*$. У першому випадку отримуємо, що $tr's' = rws'$, звідки випливає, що $rw \in Z^*r'$. З другого випадку випливає, що $r's' = trws'$. Оскільки $r's' \in \{1\} \cup Z$, то це зумовлює, що $t = 1$ або $rws' = 1$. В обидвох випадках маємо $rw \in Z^*r'$. Таким чином, $rw \in Z^*r'$, і аналогічно отримуємо $ws' \in sZ^*$. За твердженням 4.2.3 маємо, що

$$((r, s), \varphi_X(w), (r', s')) = 1.$$

Припустимо протилежне, що

$$((r, s), \varphi_X(w), (r', s')) = 1.$$

Тоді за твердженням 4.2.3 маємо, що

$$rw = zr' \qquad \text{і} \qquad ws' = sz$$

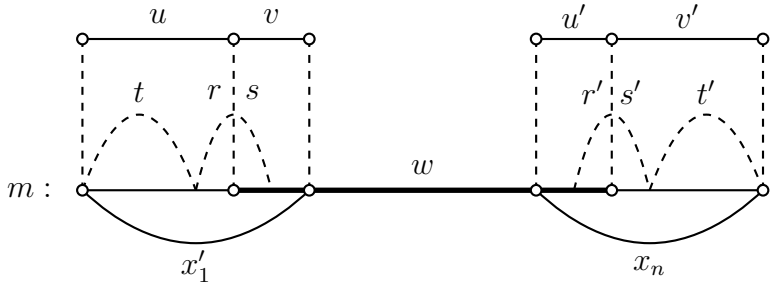
для деяких $z, z' \in Z^*$. Тоді $rws' \in Z^*$, і оскільки код Y будучи повним, отримуємо, що існують $t, t' \in Z^*$ такі, що

$$m = trws't' \in X^*.$$

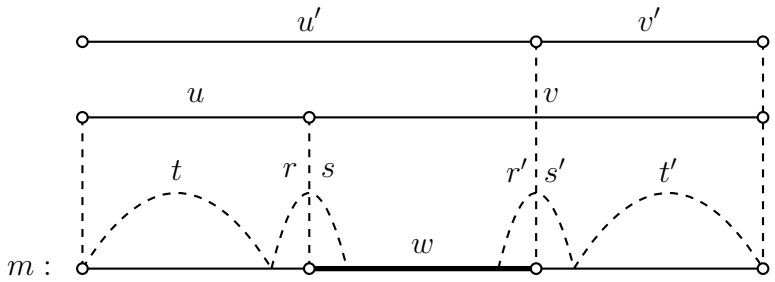
Нехай

$$m = trws't' = trsz't' = tzr's't' = x_1 \cdots x_n$$

з $n \geqslant 1$ і $x_1, \cdots, x_n \in X$. Ми можемо припускати, що t і t' можемо вибрати мінімальної множини так, що t власним префіксом слова x_1 і t' є власним суфіксом слова x_n. Але тоді, оскільки $m \in Z^*$ і також $trs \in Z^*$, то trs є префіксом слова x_1 і $r's't'$ є суфіксом слова x_n (рис. 4.9). Означимо



(a)



(b)

Рис. 4.9: У випадку **(a)** $n > 1$ і випадку **(b)** $n = 1$

$$\begin{array}{lll} x_1 = uv & \text{з} & u = tr, \quad v \in sZ^*, \\ x_n = u'v' & \text{з} & u' = t'r', \quad v' \in s'Z^*. \end{array}$$

Тоді (u, v) і (u', v') є станами автомата $\mathcal{A}_D^*(X)$, і більше того

$$\rho((u, v)) = (r, s), \qquad \rho((u', v')) = (r', s'),$$

і

$$m = uwv' = uvx_2 \cdots x_n = x_1 \cdots x_{n-1}u'v'.$$

Отож, отримуємо

$$uw \in X^* u' \qquad \text{і} \qquad wv' \in vX^*.$$

На завершенні розглянемо множину R станів автомата $\mathcal{A}_D^*(Y)$. Тоді R можна ототожнити з множиною

$$R' = \{(u, v) \in P \colon u, v \in Z^*\}.$$

Ребра автомата $\mathcal{A}_D^*(Y)$ відповідають таким шляхам

$$(u, v) \longrightarrow (u', v')$$

автомата $\mathcal{A}_D^*(X)$ з кінцевими точками в R' і з міткою в Z. □

Приклад 4.2.8. Нагадаємо з розділу 2, що код

$$X = \{aa, ba, bb, baa, bba\}$$

є композицією кодів

$$Y = \{cc, d, e, dc, ec\} \qquad \text{і} \qquad Z = \{a, ba, bb\}.$$

Квітковий автомат $\mathcal{A}_D^*(X)$ зображено на рис. 4.6. Квітковий автомат $\mathcal{A}_D^*(Z)$ зображено на рис. 4.10. Він отримується з автомата $\mathcal{A}_D^*(X)$ редукцією

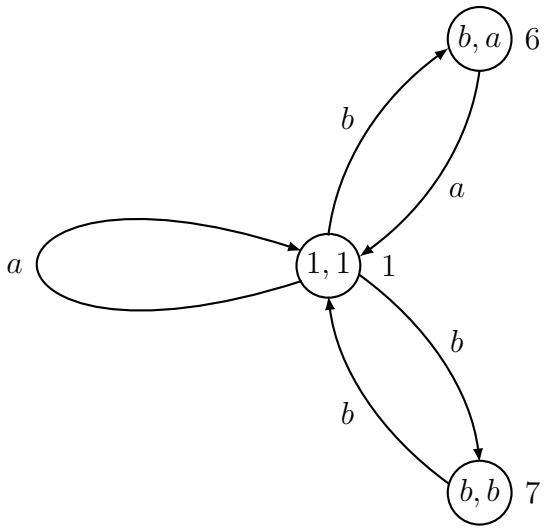


Рис. 4.10: Квітковий автомат коду Z

$$\begin{aligned}
&\rho(1) = \rho(2) = \rho(3) = \rho(4) = \overline{1},\\
&\rho(6) = \rho(8) = \overline{6},\\
&\rho(5) = \rho(7) = \overline{7}.
\end{aligned}$$

Квітковий автомат $\mathcal{A}_D^*(Y)$ зображено на рис. 4.11.

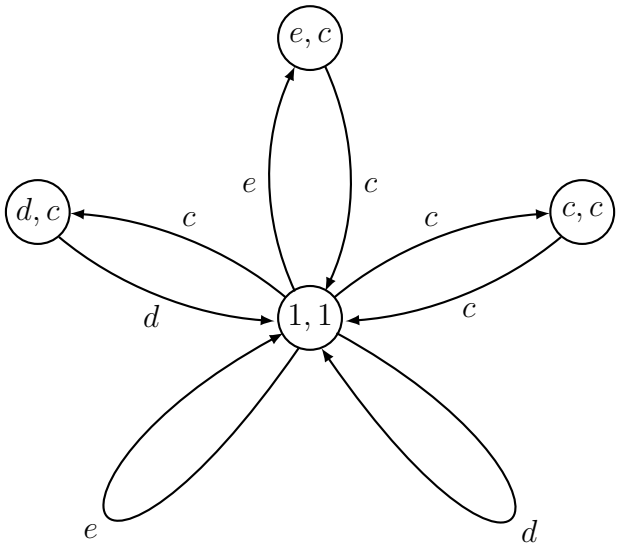


Рис. 4.11: Квітковий автомат коду Y

4.3 Декодери

Нехай $X \subset A^+$ — код і $\beta\colon B^* \to A^*$ — морфізм кодування для коду X. Позаяк відображення β є ін'єктивним, то існує часткове відображення

$$\gamma\colon A^* \to B^*$$

з областю визначення X^* і таке, що

$$\gamma(\beta(u)) = u \qquad \text{для всіх} \qquad u \in B^*.$$

Ми будемо називати часткове відображення γ *функцією декодування* для коду X.

Морфізм кодування $\beta\colon B^* \to A^*$ можна реалізувати літерним перетворювачем з одним станом, де множиною міток ребер будуть просто пари $(b, \beta(b))$ для $b \in B$.

Приклад 4.3.1. Розглянемо кодування. визначене наступним чином:

$$\gamma(a) = 00, \qquad \gamma(b) = 1 \qquad \text{і} \qquad \gamma(c) = 01.$$

Відповідний кодуючий перетворюювач зображено на рис. 4.12.

Перетворювачі для декодування більш цікаві. Для кодування та декодування ми маємо справу з перетворювачами, які визначають однозначні відображення в обох напрямках. Нам будуть потрібні два додаткові поняття.

Літерний перетворювач називається *детерміністичним* (відп. *однозначним*), якщо його асоційований вхідний автомат є детерміністичним (відп. однозначним).

Очевидно, що відношення, яке реалізується детермінованим перетворювачем, є відображенням. Кожен раз, коли існує шлях

$$p \xrightarrow{u|w} q,$$

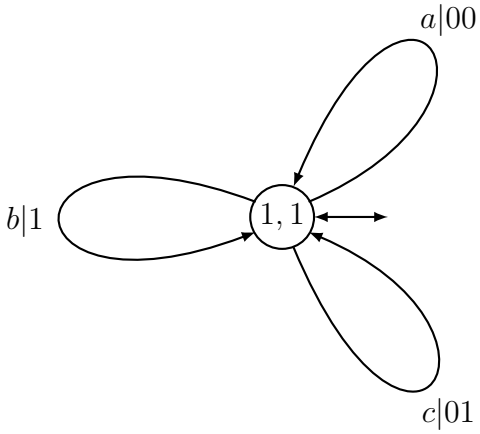


Рис. 4.12: Простий кодер

який починається в стані p з вхідною міткою u та вихідною міткою w, ми писатимемо

$$p \cdot u \quad \text{для} \quad q \qquad \text{і} \qquad p * u \quad \text{для} \quad w.$$

Зауважимо, що виконується рівність

$$p \cdot uv = p \cdot u \cdot v.$$

Це є рівність (1.7). Також виконується рівність

$$p * uv = (p * u)(p \cdot u * v). \tag{4.7}$$

Справді, якщо існує шлях, який починається в стані p з вхідною міткою uv, то він є вигляду

$$p \xrightarrow{u|w} q \xrightarrow{v|z} r$$

для станів

$$q = p \cdot u \qquad \text{та} \qquad r = q \cdot v$$

і вихідними мітками

$$w = p * u \qquad \text{та} \qquad z = q * v.$$

Звідси випливає рівність

$$wz = (p * u)(p \cdot u * v),$$

що і треба було довести.

Нехай $\beta\colon B^* \to A^*$ — морфізм кодування зі скінченними алфавітами A та B, і нехай $X = \beta(B)$. *Префіксний перетворювач* $\mathcal{T}$ над алфавітами B і A асоційований до відображення β має в якості станів множину власних префіксів слів у множині X. Стан, який відповідає порожньому слову 1 є початковим і кінцевим станом. Існує ребро $p \xrightarrow{a|-} pa$, де тире $(-)$ зображає порожнє слово, для кожного префікса p і літери a таких, що pa є префіксом, та ребро $p \xrightarrow{a|b} 1$ для кожного стану p і літери a з $pa = \beta(b) \in X$. Зауважимо, що для кожного ребра $p \xrightarrow{a|v} q$ префіксного перетворювача, виконується рівність

$$pa = \beta(v)q. \tag{4.8}$$

Зауважимо також, що префіксний перетворювач є скінченним, коли алфавіт B скінченним, а отже коли код X є скінченним.

Твердження 4.3.2. *Для довільного морфізму кодування $\beta\colon B^* \to A^*$, префіксний перетворювач $\mathcal{T}$ асоційований до морфізму β є однозначним і реалізує функцію декодування. У випадку коли код $\beta(B)$ є префіксний, то перетворювач $\mathcal{T}$ є детермінованим.*

Доведення. Нехай $\mathcal{A}$ — вхідний автомат префіксного перетворювача $\mathcal{T}$. Тоді $\mathcal{A} = \mathcal{B}^*$, де $\mathcal{B}$ — автомат, стани якого є префіксами слів у коді X. За твердженням 4.1.2 автомат $\mathcal{A}$ є однозначним. Більше того, кожен простий шлях $1 \longrightarrow 1$ є поміченим конструкцією з $(\beta(b), b)$ для деякої літери $b \in B$. Таким чином, префіксний перетворювач $\mathcal{T}$ реалізує асоційовану функцію декодування. У випадку, коли код є префіксним, то декодер є детермінованим. □

Приклад 4.3.3. Декодер, який відповідає префіксному кодові

$$X = \{1, 00, 01\}$$

зображено на рис. 4.13. На рисунку тире означає відсутність виходу. Також, на

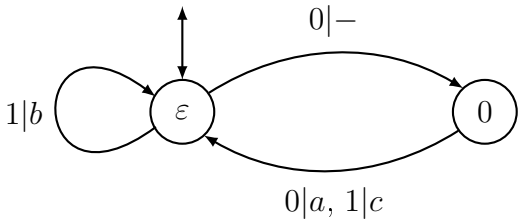


Рис. 4.13: Детермінований декодер для коду $X = \{1, 00, 01\}$

рис. 4.13 через ε позначається порожнє слово.

Приклад 4.3.4. Розглянемо код $X = \{00, 10, 100\}$. Декодер, наданий конструкцією зображено на рис. 4.14. Знову на рисунку через ε позначається порожнє слово.

Зауважимо, що перетворювач, побудований у доведенні, є скінченним (тобто має скінченну кількість станів), коли код є скінченним.

Припустимо, що код X є скінченним. Як наслідок твердження, декодування завжди може бути реалізовано в лінійному часі стосовно довжини кодованого рядки (розглядаючи число станів перетворювача як константу). Справді, для заданого слова $w = a_1 \cdots a_n$ довжини n для декодування, обчислюється послідовність множин S_i стану, доступних з початкового стану для кожного префікса $a_1 \cdots a_i$ довжини i, в припущенні, що $S_0 = \{\varepsilon\}$. Звичайно, кінцевий стан ε міститься в множині S_n. Працюючи в зворотному напрямку, ми встановлюємо $q_n = \varepsilon_i$, ідентифікуючи в кожній множині S_i єдиний стан q_i такий, що існує ребро $q_i \xrightarrow{a_i} q_{i+1}$ у вхідному автоматі. Єдиність випливає від однозначності перетворювача. Відповідна послідовність вихідних міток дає декодування.

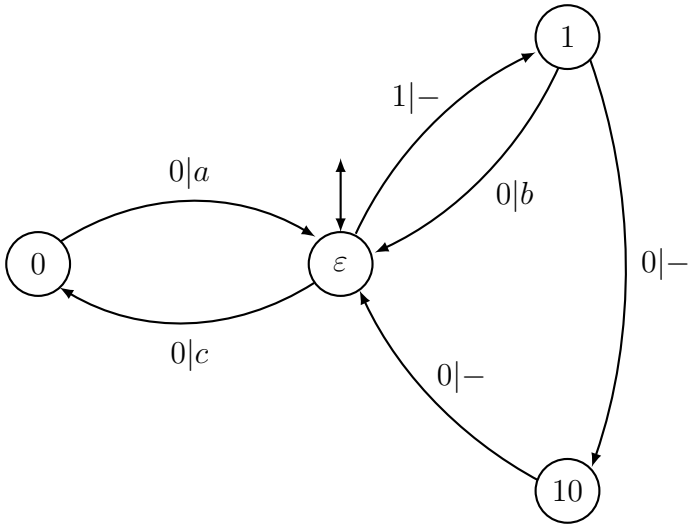


Рис. 4.14: Однозначний декодер для коду $X = \{00, 10, 100\}$, який не є префіксним

Приклад 4.3.5. Розглянемо знову код

$$C = \{00, 10, 100\}.$$

Декодування послідовності

10001010000

зображено на рис. 4.15. Тут знову на рисунку через ε позначається порожнє слово.

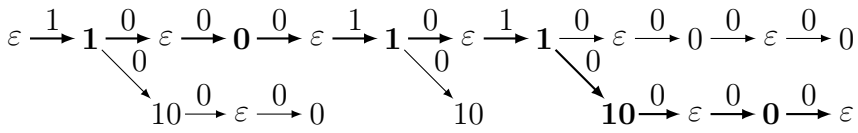


Рис. 4.15: Декодування послідовності 10001010000

Рух зліва направо виробляє дерево можливих шляхів у декодері на рис. 4.14. Рух у зворотному напрямку від стану ε в останньому стовпці виробляє успішний шлях, позначений жирним шрифтом.

Поняття детермінованого перетворювача є занадто обмеженим для кодування та декодування, оскільки не дозволяє переглядати вхід або еквівалентно затримку на виході. Поняття послідовного перетворювача, який буде впроваджено, заповнює цю прогалину.

Послідовний перетворювач над вхідним алфавітом A та вихідним алфавітом B складається з детермінованого перетворювача над A та B і вихідної функції. Ця функція відображає кінцеві стани перетворювача в слова на вихідному алфавіті B. Функція $f\colon A^* \to B^*$, реалізована послідовним перетворювачем, отримується шляхом

додавання до значення детермінованого перетворювача зображення функції виходу на вхідному стані. Формально, значення на вхідному слові $x \in A^*$ визначається так:

$$f(x) = g(x)\sigma(i \cdot x),$$

де $g(x) \in B^*$ — значення детермінованого перетворювача на вхідному слові x, $i \cdot x$ — стан, що досягається з вхідного стану i словом x, і σ — функція виходу. Це визначається, тільки якщо стан $i \cdot x$ є кінцевим станом.

Детерміновані перетворювачі є окремим випадком послідовних перетворювачів. Вони отримується тоді, коли функція виводу завжди приймає значення 1.

Приклад 4.3.6. Автомат, наведений на рис. 4.16, обчислює для кожного вхідного

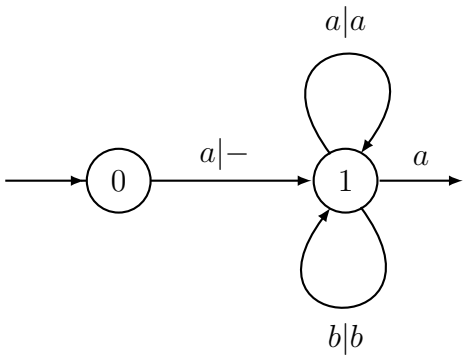


Рис. 4.16: Послідовний перетворювач, що реалізує циклічний зсув на словах, що починаються з літери a

слова вигляду aw вихідне слово wa. Він визначений на вхідних словах, які не починаються з літери a. Початковий стан дорівнює 0, а стан 1 є кінцевим. Вихідна функція σ задовольняє задовольняє умову $\sigma(1) = a$ (значення σ вказується на рисунку, як мітка вихідного ребра).

На відміну від автоматів, що не завжди вірно, скінченний перетворювач еквівалентний скінченному послідовному перетворювачу. Тим не менш, існує процедура обчислення (можливо, нескінченного) послідовного перетворювача $\mathcal{S}$, еквівалентного даному літерному перетворювачу $\mathcal{T}$, що реалізує функцію.

Нехай $\mathcal{T} = (Q, I, T)$ — літерний буквальний перетворювач, що реалізує функцію $A^* \to B^*$. Визначимо послідовний перетворювач $\mathcal{S}$ наступним чином. Станами перетворювача $\mathcal{S}$ є множини пар (u, p). Кожна пара (u, p) складається з вихідного слова $u \in B^*$ і стану $p \in Q$ перетворювача $\mathcal{T}$.

Ребрами перетворювача $\mathcal{S}$ є наступними. Для стану s перетворювача $\mathcal{S}$ і вхідної літери $a \in A$, спочатку обчислимо множину $\overline{s}$ пар (uv, q) таку, що існує пара (u, p) в стані s і ребро $p \xrightarrow{a|v} q$ в $\mathcal{T}$. На другому кроці вибираємо найдовший спільний префікс z всіх слів uv, та означимо множину t наступним чином

$$t = \{(w, q) \colon (zw, q) \in \overline{s}\}.$$

Множина t є станом перетворювача $\mathcal{S}$. Це визначає ребро зі стану s у стан t з міткою (a, z). Початковим станом є множина

$$\{(1, i) \colon i \in I\}.$$

Кінцевими станами є множини t, які містять пару (u, q) з $q \in T$, що є кінцевим станом у перетворювачі $\mathcal{T}$. Оскільки перетворювач $\mathcal{T}$ реалізує функцію, то дві пари (u, q) і (u', q') в одному і тому ж кінцевому стані t з $q, q' \in T$ задовольняють умову $u = u'$.

Функція виходу σ перетворювача $\mathcal{S}$ визначається на стані t перетворювача $\mathcal{S}$ за формулою $\sigma(t) = u$, де u — єдине слово таке, що (u, q) є в t для деякого стану $q \in T$. Станами перетворювача $\mathcal{S}$ є множинами пар, доступними з початкового стану перетворювача $\mathcal{S}$. Слова, що появляються, як перші компоненти у парах (u, p), будуть називатися *лишками*.

Процес побудови нових станів перетворювача $\mathcal{S}$ не припиниться, якщо довжини залишків не обмежені. Існують апріорні межі для максимальних довжин лишків, коли детермінізація можлива. Це робить процедуру ефективною у цьому випадку.

Приклад 4.3.7. Розглянемо перетворювач, зображений на рис. 4.17. Результатом

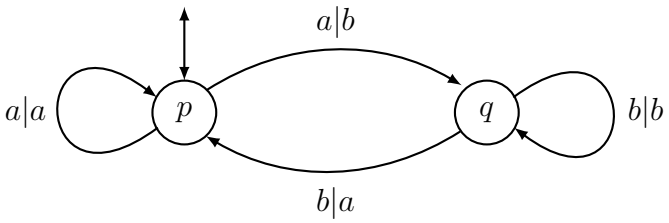


Рис. 4.17: Інший перетворювач, що реалізує циклічний зсув на словах, що починаються з літери a

алгоритму детермінації є перетворювач, зображений на рис. 4.16. Стан 0 складається з пари $(1, p)$, а стан 1 утворюється з пар (a, p) і (b, q).

Нехай $\mathcal{S} = (P, I, S)$ — літерний перетворювач над алфавітами A, B і $\mathcal{T} = (Q, J, T)$ — літерний перетворювач над алфавітами B, C. Позначимо через $\mathcal{S} \circ \mathcal{T}$ літерний перетворювач $\mathcal{U}$ над алфавітами A, C, визначений

$$\mathcal{U} = (P \times Q, I \times J, S \times T)$$

з ребрами

$$(p, q) \xrightarrow{a|w} (r, s)$$

для всіх ребер $p \xrightarrow{a|v} r$ у перетворювачі $\mathcal{S}$ і шляхи $q \xrightarrow{v|w} s$ у перетворювачі $\mathcal{T}$. Перетворювач $\mathcal{U} = \mathcal{S} \circ \mathcal{T}$ називається перетворювачем, *складеним* з перетворювачів $\mathcal{S}$ і $\mathcal{T}$.

Твердження 4.3.8. *Відношення, реалізоване складеним перетворювачем $\mathcal{S} \circ \mathcal{T}$ є композицією відношень, реалізованих перетворювачами $\mathcal{S}$ і $\mathcal{T}$.*

Доведення. Існує шлях There is a path $(p,q) \xrightarrow{u|w} (r,s)$ у перетворювачі $\mathcal{U} = \mathcal{S} \circ \mathcal{T}$ тоді і тільки тоді, коли існує шлях $p \xrightarrow{u|v} r$ у перетворювачі $\mathcal{S}$ і шлях $q \xrightarrow{v|w} s$ у перетворювачі $\mathcal{T}$. Таким чином, $(u,w) \in A^* \times C^*$ є елементом відношення, реалізованого перетворювачем $\mathcal{U}$ тоді і тільки тоді, коли існує слово $v \in B^*$ таке, що (u,v) є елемент, якщо відношення реалізоване перетворювачем $\mathcal{S}$ і (v,w) належить відношенню, реалізованим перетворювачем $\mathcal{T}$. □

Твердження 4.3.9. *Якщо $\mathcal{S}$ і $\mathcal{T}$ — однозначні перетворювачі, то перетворювач $\mathcal{S}\circ\mathcal{T}$ є однозначним.*

Доведення. Нехай $u = a_1 a_2 \cdots a_n$ — слово з $a_i \in A$ та $n \geqslant 0$. Припустимо, що існують два шляхи в $\mathcal{U} = \mathcal{S}\circ\mathcal{T}$ з тією ж міткою вводу u і тим же самим початковим і кінцевим станом. Точніше, припустимо, що в перетворювачі $\mathcal{U}$ існують шляхи

$$(p_0,q_0) \xrightarrow{a_1|w_1} (p_1,q_1) \xrightarrow{a_2|w_2} \cdots (p_{n-1},q_{n-1}) \xrightarrow{a_n|w_n} (p_n,q_n),$$
$$(p'_0,q'_0) \xrightarrow{a_1|w'_1} (p'_1,q'_1) \xrightarrow{a_2|w'_2} \cdots (p'_{n-1},q'_{n-1}) \xrightarrow{a_n|w'_n} (p'_n,q'_n)$$

з $(p_0,q_0) = (p'_0,q'_0)$ і $(p_n,q_n) = (p'_n,q'_n)$. Тоді існують у перетворювачі $\mathcal{S}$ два шляхи

$$p_0 \xrightarrow{a_1|v_1} p_1 \xrightarrow{a_2|v_2} \cdots p_{n-1} \xrightarrow{a_n|v_n} p_n$$

і

$$p'_0 \xrightarrow{a_1|v'_1} p'_1 \xrightarrow{a_2|v'_2} \cdots p'_{n-1} \xrightarrow{a_n|v'_n} p'_n$$

для відповідних слів $v_1,\cdots,v_n,v'_1,\cdots,v'_n$, і, у перетворювачі $\mathcal{T}$ два шляхи

$$q_0 \xrightarrow{v_1|w_1} q_1 \xrightarrow{v_2|w_2} \cdots q_{n-1} \xrightarrow{v_n|w_n} q_n$$

і

$$q'_0 \xrightarrow{v'_1|w'_1} q'_1 \xrightarrow{v'_2|w'_2} \cdots q'_{n-1} \xrightarrow{v'_n|w'_n} q'_n.$$

Оскільки перетворювач $\mathcal{S}$ є однозначним, то ці два шляхи збігаються, а отже $p_i = p'_i$ і $v_i = v'_i$ для всіх $i = 1,\ldots,n$. Оскільки перетворювач $\mathcal{T}$ є однозначним і два шляхи мають однакову вхідну мітку, то вони збігаються. Таким чином, $q_i = q'_i$ і $w_i = w'_i$ для всіх $i = 1,\ldots,n$. Отож, два шляхи в перетворювачі $\mathcal{U}$ збігаються. □

Наслідок 4.3.10. *Нехай $X = Y \circ Z$ — код над алфавітом A, що є композицією коду Y над алфавітом B і коду Z над алфавітом A, і нехай $\gamma\colon B^* \to C^*$ і $\delta\colon A^* \to B^*$ — відображення кодування для Y і Z. Якщо $\mathcal{S}$ і $\mathcal{T}$ є однозначними перетворювачами, які реалізують відображення γ і δ, то композиція $\mathcal{T}\circ\mathcal{S}$ реалізує функцію декодування $\gamma\circ\delta\colon A^* \to C^*$.*

Приклад 4.3.11. Нехай

$$X = \{aa, ba, baa, bb, bba\}, \qquad Y = \left\{\overline{aa}, \overline{b}, \overline{b}\overline{a}, \overline{c}, \overline{ca}\right\} \qquad \text{і} \qquad Z = \{a, ba, bb\}.$$

Тоді $X = Y \circ_\beta Z$ з $B = \left\{\overline{a},\overline{b},\overline{c}\right\}$ і $\beta(\overline{a}) = a$, $\beta(\overline{b}) = ba$ і $\beta(\overline{c}) = bb$. Префіксний перетворювач $\mathcal{S}$ коду Z, суфіксний перетворювач $\mathcal{T}$ коду Y, і їх композиція зображені на рис. 4.18, з $C = \{c,d,e,f,g\}$.

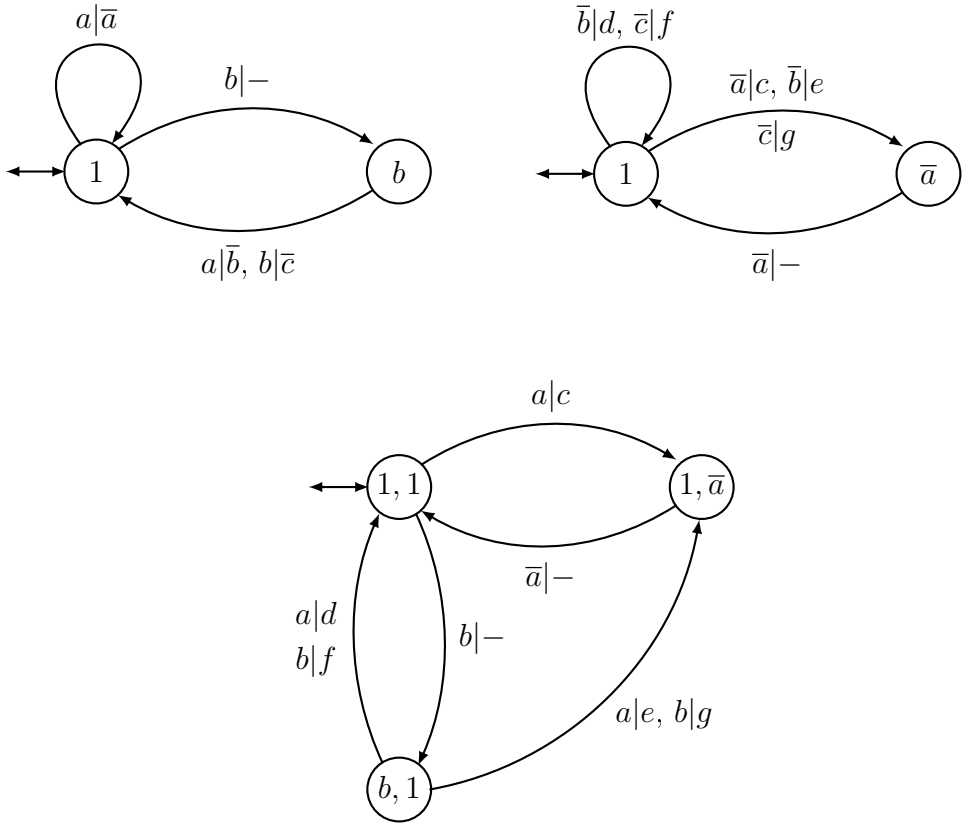


Рис. 4.18: Перетворювачі $\mathcal{T}$, $\mathcal{S}$ і $\mathcal{T} \circ \mathcal{S}$

Твердження 4.3.12. *Якщо $\mathcal{S}$ і $\mathcal{T}$ — детерміновані перетворювачі, то перетворювач $\mathcal{S} \circ \mathcal{T}$ є детермінованим.*

Доведення. Нехай

$$(p, q) \xrightarrow{a|w} (r, s) \qquad \text{і} \qquad (p, q) \xrightarrow{a|w'} (r', s')$$

— два ребра перетворювача $\mathcal{U} = \mathcal{S} \circ \mathcal{T}$. Тоді існують ребра

$$p \xrightarrow{a|v} r \qquad \text{і} \qquad p \xrightarrow{a|v'} r'$$

у перетворювачі $\mathcal{S}$ і шляхи

$$q \xrightarrow{v|w} s \qquad \text{і} \qquad q \xrightarrow{v'|w'} s'$$

у перетворювачі $\mathcal{T}$. Позаяк перетворювач $\mathcal{S}$ є детермінованим, то

$$v = v' \qquad \text{і} \qquad r = r'.$$

Оскільки перетворювач $\mathcal{T}$ є детермінованим, то звідси в свою чергу випливає, що

$$w = w' \qquad \text{і} \qquad s = s'.$$

Отож два ребра в перетворювачі $\mathcal{U} = \mathcal{S} \circ \mathcal{T}$ збігаються. □

4.4 Вправи до розділу 4

Підрозділ 4.1

В. 4.4.1. Доведіть, що підмоноїд M вільного моноїда A^* є розпізнуваним і вільним тоді і тільки тоді, коли існує однозначний впорядкований автомат $\mathcal{A} = (Q, 1, 1)$, що розпізнає моноїд M.

Підрозділ 4.2

В. 4.4.2. Нехай X — підмножина вільної множини A^+ і $\mathcal{A}^*_D(X) = (P, (1,1), (1,1))$ — квітковий автомат множини X. Нехай φ — асоційоване зображення. Доведіть, що

$$((p,q), \varphi(w), (r,s)) = (q(\underline{X})^* r, w) + (pw, r)(q, ws),$$

для всіх станів $(p,q), (r,s) \in P$ і слів $w \in A^*$.

В. 4.4.3. Нехай $\mathcal{A} = (P, i, T)$ і $\mathcal{B} = (Q, j, S)$ — два автомати і $\rho\colon P \to Q$ — редукція з $\mathcal{A}$ на $\mathcal{B}$ така, що $i = \rho^{-1}(j)$. Доведіть, якщо автомат $\mathcal{A}$ є детермінованим, то автомат $\mathcal{B}$ є також детермінованим.

Нотатки до розділу 4

Однозначні автомати та їх відношення до кодів вперше зустрічаються в працях Шюценбергера [182, 185]. Вони також зустрічаються під назвою *інформаційних машин без втрат* (*information lossless machines*) у праці Гаффмана [97], див. також монографії [110–113].

Однозначні автомати тісно пов'язані з поняттям відображень зі скінченними прообразами, що використовуються в символьній динаміці (див. [128]). Зв'язок полягає в тому, що в скінченному однозначному автоматі будь-яке слово є міткою скінченної кількості шляхів. Ця кількість обмежена квадратом кількості станів автомата. Справді, для будь-якої пари p і q станів автомата $\mathcal{A}$ та будь-якого слова w існує не більше одного шляху $p \xrightarrow{w} q$.

Твердження 4.1.6 появляється в статті Шюценбергера [185]. Формулу (4.2) можна записати в термінах некомутативних змінних, використовуючи поняття *квазідетермінанта* (*quasideterminant*) (див. [3, 74]).

Для створення всебічного знання про перетворювачі необхідно звернутися до монографій Ейленберґа [62] або Берстеля [31]. Про відносно недавні результати по цій тематиці див. монографії Сакаровіча [172, 173].

Про алгоритм детермінації перетворювачів див. монографії групи математиків Лотарі [134–136]. Декодування в лінійному часі за допомогою однозначного перетворювача базується на покритті Шюценбергера однозначним автоматом, див. [172, 173].

Розділ 5

Затримка дешифрування

Цей розділ присвячений кодам зі скінченною затримкою дешифрування. Інтуїтивно, коди зі скінченною затримкою дешифрування можна декодувати, зліва направо, зі скінченним переглядом. Існує очевидний практичний інтерес до цієї умови. Коди зі скінченною затримкою дешифрування утворюють сім'ю, яка розташована між префіксними та загальними кодами. Існує два способи визначення затримки дешифрування, підрахуванням або кодових слів, або літер. Перший спосіб називається *вербальною затримкою*, або просто коротше *затримкою*, а другий — *літерною затримкою*.

Підрозділ 5.1 присвячений кодам зі скінченною затримкою вербального дешифрування. Спочатку ми викладаємо попередній необхідний матеріал. Зокрема, ми доводимо характеризацію затримки дешифрування з точки зору спрощення слів.

У підрозділі 5.2 ми доводимо теорему Щюценбергера (терема 5.2.4), яка стверджує, що скінченний максимальний код зі скінченною затримкою дешифрування є префіксним. Ми доводимо, що кожен раціональний код зі скінченною затримкою дешифрування міститься в максимальному раціональному коді з тою самою скінченною затримкою дешифрування (терема 5.2.9).

У підрозділі 5.3 розглядається затримка літерного дешифрування, тобто затримка дешифрування, де беруться до уваги вирази літер замість слів коду. Код зі скінченною затримкою літерного дешифрування називається *слабко префіксним*. Вводиться поняття автомата зі скінченною затримкою, який називається також *слабо детермінованим*. Доведено еквівалентність між слабко префіксними кодами та слабо детермінованими автоматами (твердження 5.3.4). Ми використовуємо цю характеризацію для того, щоб дати ще одне доведення теореми Шютценбергера. Далі ми доведемо, що існує раціональне поповнення з тією ж літерною затримкою дешифрування (теорема 5.3.7).

5.1 Затримка дешифрування

Будемо говорити, що підмножина X вільної напівгрупи A^+ має *скінченну затримку вербального дешифрування*, якщо існує ціле число $d \geqslant 0$ таке, що виконується умова

$$xy \leqslant x'y' \qquad \Longrightarrow \qquad x = x', \tag{5.1}$$

для $x, x' \in X$, $y \in X^d$, $y' \in X^*$. (Нагадаємо, що ми пишемо $u \leqslant u'$ для зображення того, що слово u є префіксом слова u'.) Якщо ця умова викнується для цілого числа d, то ми кажемо, що множина X *має затримку вербального дешифрування* d. Якщо це можливо, то ми опускаємо цей термін вербальний. Заборонена конфігурація для скінченної затримки дешифрування зображена на рис. 5.1.

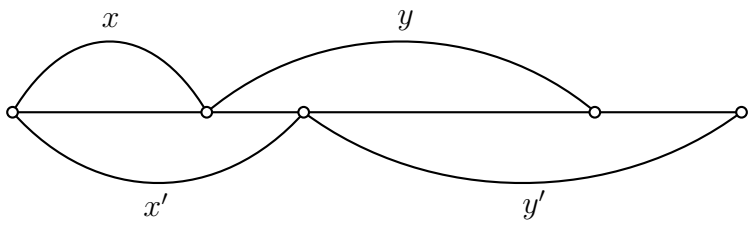


Рис. 5.1: Заборонена конфігурація для скінченної затримки дешифрування

Вище викладене означення можна переформулювати наступним чином. Нехай $w \in A^*$ — слово, яке має два префікси у вільній напівгрупі X^+ таке, що найкоротше з них міститься в X^{1+d}. Тоді два префікси починаються з одного і того ж слова в X.

Якщо множина X має затримку вербального дешифрування d, то вона також має затримку вербального дешифрування d' для кожного цілого $d' \geqslant d$. Найменше ціле число d, яке задовольняє умову (5.1) називається *мінімальною затримкою вербального дешифрування* множини X. Якщо такого цілого числа не існує, то будемо вважати, що множина X має *нескінченну затримку вербального дешифрування*.

Це поняття затримку дешифрування є, очевидно, орієнтованим зліва-направо. Дуже просто визначити дуальне поняття (працюючи справа наліво). Термінологію обґрунтовує наступне спостереження: під час здійснення граматичного аналізу вхідного слова зліва-направо затримка між моментом, коли можливий множник X-факторизації є виявленим, і моментом, коли ці множники остаточно чинні, є обмеженою затримкою дешифрування.

Якщо затримка дешифрування множини X є нескінченною, то існують слова $x, x' \in X$ з $x \neq x'$ і $y_1, y_2, \ldots, y_n, y'_1, y'_2, \ldots, y'_n \in X$ такі, що $xy_1y_2\cdots y_n$ є префіксом слова $x'y'_1y'_2\cdots y'_n$ для всіх $n \geqslant 1$, або навпаки.

З визначення випливає, що множини з затримкою $d = 0$ є префіксними кодами. Це є причиною, чому префіксні коди також називаються *миттєвими кодами*. У цьому сенсі коди зі скінченною затримкою є природним узагальненням префіксних кодів.

Твердження 5.1.1. *Підмножина X вільної напівгрупи A^+, яка має скінченну затримку дешифрування є кодом.*

Доведення. Нехай множина X має затримку дешифрування d. Ми можемо вважати, що $X \neq \varnothing$. Припустимо, що виконується рівність

$$w = x_1x_2\cdots x_n = y_1y_2\cdots y_m,$$

для деяких $n, m \geqslant 1$, $x_1, \ldots, x_n, y_1, \ldots, y_m \in X$. Нехай $z \in X$. Тоді $wz^d \in y_1X^*$. За умовою (5.1) маємо, що $x_1 = y_1$, $x_2 = y_2$ і т.д. Отож, множина X є кодом. □

Приклад 5.1.2. Суфіксний код

$$X = \{aa, ba, b\}$$

має нескінченну затримку дешифрування. Справді, для всіх цілих $d \geqslant 0$ слово $b(aa)^d \in X^{1+d}$ є префіксом слова $y(aa)^d$ такого, що $y = ba \neq b$.

Для підмножини $X \subset A^+$, означимо, як і в підрозділі 2.3, послідовність $(U_n)_{n\geqslant 0}$ підмножин вільного моноїда A^*, прийнявши

$$U_1 = X^{-1}X \setminus \{1\}, \qquad U_{n+1} = X^{-1}U_n \cup U_n^{-1}X, \qquad n \geqslant 1.$$

Твердження 5.1.3. *Множина X має скінченну затримку дешифрування тоді і тільки тоді, коли множина U_n є порожньою для деякого цілого числа n.*

Доведення. За лемою 2.3.4 для натурального числа $n \geqslant 1$ маємо, що $u \in U_n$ тоді і тільки тоді, коли існують слова $x_1, \ldots, x_i, y_1, \ldots, y_j \in X$ з $x_1 \neq y_1$, $i+j = n+1$ і слово u є суфіксом слова y_j такі, що $x_1 \cdots x_i u = y_1 y_2 \cdots y_j$. Ми спочатку перевіримо, що у випадку, коли множина X має затримку дешифрування d, то $U_{2d+1} = \varnothing$. Припустимо протилежне. Нехай слова $x_1, \ldots, x_i, y_1, \ldots, y_j \in X$ є такими, що $x_1 \cdots x_i u = y_1 y_2 \cdots y_j$ з $i + j = 2d + 2$, u є суфіксом слова y_j і $x_1 \neq y_1$. Тоді $i - 1 \leqslant d - 1$, оскільки в протилежному випадку мали б $x_1 = y_1$. Аналогічно отримуємо, що $j - 2 \leqslant d - 1$, оскільки в протилежному випадку, з $y_j = vu$, ми мали б $y_1 y_2 \cdots y_{j-1} v = x_1 \cdots x_i$, а отже знову виконується рівність $x_1 = y_1$. Отож, $i+j \leqslant 2d+1$. Отримали протиріччя.

Отже, ми доведемо, якщо $U_n = \varnothing$, то множина X має затримку дешифрування $n - 1$. Нехай справді $x, x' \in X$, $y \in X^{n-1}$, $y' \in X_j$ для $j \geqslant 0$ і $u \in A^*$ є такими, що $xyu = x'y'$. Якщо $x \neq x'$, то $u \in U_m$ для деякого натурального числа $m \geqslant n$, протиріччя. Звідси випливає рівність $x = x'$, а це доводить, що множина X має затримку дешифрування $n - 1$. □

Приклад 5.1.4. Множина

$$X = \{a, ab, bc, cd, de\}$$

має затримку дешифрування 2. Отримуємо, що

$$U_1 = \{b\}, \qquad U_2 = \{c\}, \qquad U_3 = \{d\}, \qquad U_4 = \{e\}, \qquad U_5 = \varnothing.$$

Ми переформулюємо означення затримки дешифрування наступним чином. Нехай X — код. Будемо говорити, що слово $s \in A^*$ є *спрощуваним* для коду X, якщо

$$xsv \in X^* \qquad \Longrightarrow \qquad sv \in X^*,$$

для всіх $x \in X^*$ і $v \in A^*$.

Твердження 5.1.5. *Код X має затримку дешифрування d тоді і тільки тоді, коли всі слова в X^d є спрощуваними.*

Доведення. Спочатку припустимо, що код X має затримку дешифрування d. Нехай $x \in X^d$, $x_1, \ldots, x_p \in X$ і $v \in A^*$ такі, що $x_1 \cdots x_p x v \in X^*$. Таким чином,

$$x_1, \ldots, x_p x v = y_1 \cdots y_q$$

для деяких слів $y_1, \dots, y_q \in X$. Позаяк код X має затримку дешифрування d, то звідси випливає, що $x_1 = y_1, \dots, x_p = y_p$, звідки отримуємо, що $q \geqslant p$ і $xv = y_{p+1} \cdots y_q$. Отож, $xv \in X^*$. Це доводить, що слово x є спрощуваним.

Навпаки, припустимо, що $y \in X^d$. Нехай $x, x' \in X$ і $u \in A^*$ — такі слова, що $xyu \in x'X^*$. Тоді $yu \in X^*$. Оскільки множина X є кодом, то звідси випливає, що $x = x'$. Отож, код X має затримку дешифрування d. □

Наступне твердження охарактеризовує декодери кодів зі скінченною затримкою дешифрування в термінах послідовних перетворювачів, введених в підрозділі 4.3.

Твердження 5.1.6. *Нехай $X \subset A^+$ — скінченний код і $\beta\colon B^* \to A^*$ — морфізм кодування для коду X. Відповідна функція декодування $A^* \to B^*$ є реалізовною скінченним послідовним перетворювачем тоді і тільки тоді, коли код X має скінченну вербальну затримку дешифрування.*

Доведення. Припустимо спочатку, що X має скінченну вербальну затримку дешифрування d. За твердженням 4.3.2 префіксний перетворювач $\mathcal{T}$ асоційований з відображенням β реалізує відповідну функцію декодування γ з A^* в B^*. Нехай $\mathcal{S}$ — послідовний перетворювач, отриманий з $\mathcal{T} = (Q, 1, 1)$ процедурою детермінізації, описаної в підрозділі 4.3. Нехай U — множина лишок, що є словами $u \in B^*$ таким, що (u, p) належить до стану перетворювача $\mathcal{S}$ для деякого стану p перетворювача $\mathcal{T}$. Ми доведемо, що кожне слово $u \in U$ має довжину, яка не перевищує d. Це доведе, що перетворювач $\mathcal{S}$ є скінченним, а отже функція декодування є реалізовною скінченним послідовним перетворювачем.

Для цього зауважимо, якщо дві пари $(w, q), (w', q') \in B^* \times Q$ належать до одного стану перетворювача $\mathcal{S}$, то $\beta(w)q = \beta(w')q'$. Це виконується для початкового стану $(1, 1) \in B^* \times Q$, де черзе другу одиницю 1 ми позначаємо початковий стан перетворювача $\mathcal{T}$. Далі, якщо $(w, q), (w', q') \in t$ є двома парами, які належать до деякого стану $t \neq (1, 1)$ перетворювача $\mathcal{S}$, то за означенням перетворювача $\mathcal{S}$ існує ребро $s \xrightarrow{a,z} t$ в $\mathcal{S}$ для деяких $a \in A$ і $z \in B^*$. Таким чином, існують дві пари $(u, p), (u', p')$ в стані s і два ребра

$$p \xrightarrow{a|v} q \qquad \text{і} \qquad p' \xrightarrow{a|v'} q'$$

в перетворювачі $\mathcal{T}$ такі, що $uv = zw$ і $u'v' = zw'$. Ми доводимо індукцією по довжині шляху від початкового стану до стану t в перетворювачі $\mathcal{S}$. Таким чином, ми можемо припускати, що $\beta(u)p = \beta(u')p'$. Оскільки

$$p \xrightarrow{a|v} q \qquad \text{і} \qquad p' \xrightarrow{a|v'} q'$$

є ребрами в перетворювачі $\mathcal{T}$, то за рівністю (4.8) маємо, що $pa = \beta(v)q$ і $p'a = \beta(v')q'$. Це має на увазі в свою чергу, що $\beta(uv)q = \beta(u'v)q'$.Спрощення обох сторін значенням $\beta(z)$ дає рівність $\beta(w)q = \beta(w')q'$.

Розглянемо тепер пару $(u, p) \in B^+ \times Q$, яка належить стану перетворювача $\mathcal{S}$. Оскільки слово u є непорожнім, то за означенням перетворювача $\mathcal{S}$ існує інша пара (u', p') у тому ж самому стані перетворювача $\mathcal{S}$ така, що слова u й u' не мають непорожнього спільного префікса. За нашим попереднім зауваженням маємо, що $\beta(u)p = \beta(u')p'$. Оскільки слово p' є префіксом деяких кодових слів, то слово $\beta(u)$ є префіксом слова $\beta(u'b)$ для деякої літери $b \in B$. Тепер покладемо

$$\beta(u) = xy \qquad \text{і} \qquad \beta(u'b) = x'y',$$

для деяких $x, x' \in X$, $y, y' \in X^*$. Оскільки слова u й u' починаються різними літерами, то маємо, що $x \neq x'$. За означенням затримки дешифрування, звідси випливає, що $|u| \leqslant d$, що завершує доведення першої імплікації.

Навпаки, припустимо, що $\mathcal{S} = (Q, i, \sigma)$ — послідовний перетворювач з вихідною функцією σ, яка реалізує відповідну функцію декодування γ з A^* в B^*. Нехай d — максимальна довжина слів $\sigma(p)$ для $p \in Q$. З урахуванням застосування знову умови (5.1), нехай $x, x' \in X$ і $y, y' \in X^*$ – слова такі, що $xy \leqslant x'y'$ і $x \neq x'$. Ми доведемо, що $y \in X^{d'}$ для деякого цілого числа $d' < d$. Нехай p — стан, досягнутмй з початкового стану i, читаючи слово x. У цьому читанні немає виводу, оскільки слово xy є префіксом слова $x'y'$, і, оскільки $x \neq x'$, то не можна вирішити, чи виводити $\gamma(x)$ або $\gamma(x')$. Таким чином, ми маємо ребро $i \xrightarrow{xy|1} p$. Більше того, якщо слово u визначене так $\beta(u) = xy$, то $\sigma(p) = u$. Оскільки $|u| \leqslant d$ і $\beta(u) \in X^{1+d'}$, то маємо $1 + d' \leqslant d$, а отже $d' < d$. Таким чином, код X має вербальну затримку дешифрування d. □

Приклад 5.1.7. Розглянемо код

$$X = \{a, b, abc\}$$

над алфавітом $A = \{a, b, c\}$, з $B = \{\overline{a}, \overline{b}, \overline{c}\}$ і морфізм кодування визначений так:

$$\overline{a} \mapsto a, \qquad \overline{b} \mapsto b, \qquad \overline{c} \mapsto abc.$$

Код X має вербальну затримку дешифрування 2. Префіксний перетворювач $\mathcal{T}$ і послідовний перетворювач $\mathcal{S}$ отримуються детермінізацією, як це зображено на рис. 5.2. Стани перетворювача $\mathcal{S}$ перенумеровані $1, 2, 3$, а відповідність з станами, отриманими

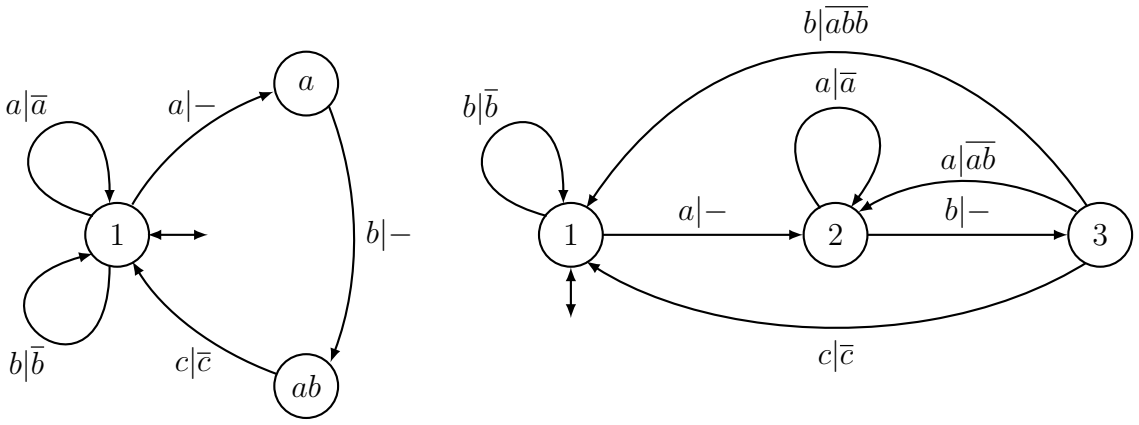


Рис. 5.2: Перетворювачі $\mathcal{T}$ і $\mathcal{S}$

за допомогою процедури детермінування, і функцією виходу σ наведені в табл. 5.1.

стан	1	2	3
пари	$(1,1)$	$(\overline{a},1)$ $(1,a)$	$(\overline{ab},1)$ $(1,ab)$
вихід	1	$\overline{a}$	$\overline{ab}$

Табл. 5.1: Стани та функція виходу для послідовного перетворювача $\mathcal{S}$

5.2 Максимальні коди

Тепер ми вивчаємо максимальні коди зі скінченною затримкою дешифрування. Наступний результат є подібний до твердження 2.5.6.

Твердження 5.2.1. *Нехай X — підмножина вільної напівгрупи A^+, яка має скінченну затримку дешифрування. Якщо $y \in A^+$ — необлямоване слово таке, що*

$$X^*yA^* \cap X^* = \varnothing,$$

то множина $Y = X \cup \{y\}$ має скінченну затримку дешифрування.

Доведення. Розглянемо множину $V = X^*y$. Вона є префіксним кодом. Справді, припустимо, що $v = xy$ і $v' = x'y$ є такими, що $x, x' \in X^*$ і $v < v'$. Тоді неодмінно $v \leqslant x'$, оскільки слово y є необлямованим. Але тоді $x' \in X^*yA^*$, протиріччя. Зауважимо також, що

$$V^+A^* \cap X^* = \varnothing,$$

оскільки $V^+A^* \cap VA^*$.

Нехай множина X має затримку дешифрування d і $e = d + |y|$. Ми доведемо, що множина Y має затримку дешифрування e. Для цього розглянемо відношення

$$w = y_1y_2 \cdots y_{e+1}u = y'_1y'_2 \cdots y'_n$$

з $y_1, y_2, \ldots, y_{e+1}, y'_1, y'_2, \ldots . y'_n \in Y$ і $u \in A^*$, та припустивши протилежне, припустимо, що $y_1 \neq y'_1$.

Спочатку перевіримо, що одне зі слів $y_1, y_2, \ldots, y_{e+1}$ дорівнює слову y. Припустимо протилежне. Тоді $y_1 \cdots y_{d+1} \in X^{d+1}$. Нехай q — найменше натуральне число таке, що

$$y_1 \cdots y_{d+1} \leqslant y'_1 \cdots y'_q$$

(див. рис. рис. 5.3). Затримка множини дорівнює d і $y_1 \neq y'_1$, а отже одне серед слів $y'_1, \ldots, y'_q$ має дорівнювати y. Ми не можемо мати $y_i = y$ для індексу $i < q$, оскільки в іншому випадку маємо, що $y_1 \cdots y_{d+1} \in V^+A^* \cap X^*$. Таким чином, $y'_q = y$ і $y'_1 \cdots y'_q \in V$. Зауважимо, що $y'_1 \cdots y'_{q-1} \leqslant y_1 \cdots y_{d+1}$. Далі, $|y_{d+2} \cdots y_{e+1}| \geqslant e - d = |y|$. Звідси випливає, що

$$y'_1 \cdots y'_q \leqslant y_1 \cdots y_{e+1}.$$

Але тоді $y_1 \cdots y_{e+1} \in X^* \cap X^*yA^*$, що є неможливим. Це показує, що твердження, а саме, що одне зі слів $y_1, y_2, \ldots, y_{e+1}$ дорівнює слову y.

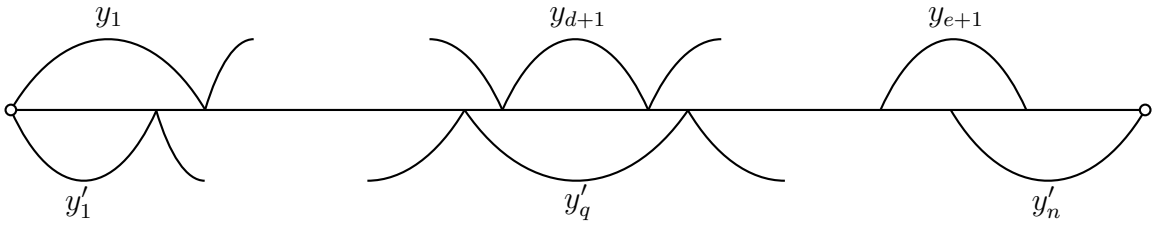


Рис. 5.3: Дві факторизації слова w

Звідси випливає, що слово w має префікс $y_1y_2\cdots y_p$ у множині V такий, що $y_1,\dots,y_{p-1}\in X$ і $y_p=y$. За припущенням одне зі слів $y'_1,\dots,y'_n$ має дорівнювати слову y. Таким чином, слово w має префікс $y'_1y'_2\cdots y'_q$ у множині V такий, що $y'_1,\dots,y'_{q-1}\in X$ і $y'_q=y$. З того, що код V є префіксним, маємо

$$y_1y_2\cdots y_{p-1}=y'_1y'_2\cdots y'_{q-1}.$$

Оскільки множина X є кодом, то звідси та з припущення $y_1\neq y'_1$ випливає, що $p=q=1$. Але тоді $y_p=y=y'_q$. З останнього випливає фінальне протиріччя. □

Твердження 5.2.1 має наступний цікавий наслідок.

Теорема 5.2.2. *Нехай X — тонка підмножина вільної напівгрупи A^+. Якщо множина X має скінченну затримку дешифрування, то наступі умови є еквівалентними:*

(i) X є максимальним кодом;
(ii) X є максимальним у сім'ї кодів зі скінченною затримкою дешифрування.

Доведення. Випадок, коли алфавіт A має рівно одну літеру є очевидним. Таким чином, ми припускаємо, що $\mathrm{Card}(A)\geqslant 2$.

Достатньо довести імплікацію $(ii)\Longrightarrow(i)$. Для цього достатньо показати, що код X є повним. Припустимо протилежне та розглянемо слово u,яке не э множником слова у вільному моноїді X^*. Враховуючи твердження 1.3.6 маємо, що існує слово $v\in A^*$ таке, що слово $y=uv$ є необлямованим. Але тоді $A^*yA^*\cap X^*=\varnothing$ і за твердженням 5.2.1 множина $X\cup\{y\}$ має скінченну затримку дешифрування. Отримали протиріччя. □

Нехай X — підмножина вільної напівгрупи A^+ над алфавітом A. Будемо говорити, що слово p є *сильно поповнювальним справа* для множини X, якщо для всіх слів $u\in A^*$ існує слово $v\in A^*$ таке, що $puv\in X^*$. Очевидно, що сильно поповнювальне справа слово є поповнювальним справа. Множина сильно поповнювальних справа слів для множини X позначається через $E(X)$.

Наступне твердження є аналогом теореми 2.5.5 для кодів зі скінченною затримкою дешифрування, оскільки воно стверджує, що максимальні коди зі скінченною затримкою дешифрування задовольняють умову, яка є сильнішою за умову бути повним кодом.

Твердження 5.2.3. *Нехай $X\subset A^+$ — максимальний код із затримкою дешифрування d. Тоді для довільних $x\in X^d$ і $u\in A^*$ існує слово $v\in A^*$ таке, що $xuv\in X^*$. Іншими словами $X^d\subseteq E(X)$.*

Доведення. Випадок, коли алфавіт A має рівно одну літеру є очевидним. Таким чином, ми припускаємо, що $\mathrm{Card}(A) \geqslant 2$.

Нехай $x \in X^d$ і $u \in A^*$. За твердження 1.3.6 існує слово $v \in A^*$ таке, що слово $y = xuv$ є необлямованим. Звідси випливає, що

$$X^* y A^* \cap X^* \neq \varnothing.$$

Справді, множина $X \cup \{y\}$ мала б бути кодом за твердженнями 5.2.1 і 5.1.1, а це суперечить максимальності коду X.

Отже, існують $z \in X^*$ і $w \in A^*$ такі, що $zyw \in X^*$. За твердженням 5.1.5 слово x є спрощуваним. Отож, з $zyw = zxuvw \in X^*$ випливає, що $xuvw \in X^*$. Це доводить, що слово x є сильно поповнювальним справа. □

Тепер ми формулюємо та доводимо важливий результат.

Теорема 5.2.4 (Шюценбергер). *Кожен скінченний максимальний код зі скінченною затримкою дешифрування є префіксним.*

Доведення. Припустимо протилежне, що існує скінченний максимальний код X зі скінченною затримкою дешифрування, який не є префіксним. Через P позначимо множину префіксів слів у вільному моноїді X^*. Означимо (див. рис. 5.4).

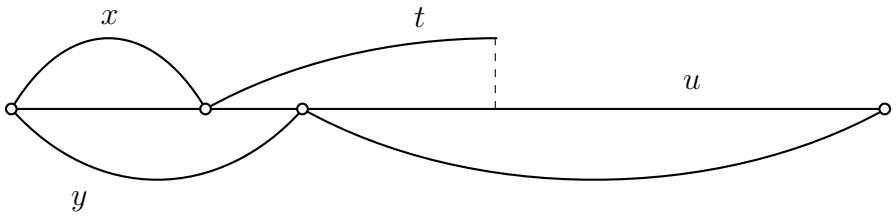


Рис. 5.4: Елемент t множини T

$$T = \{t \in P\colon \text{ існують } x, y \in X \text{ такі, що } x \neq y \text{ і } xtA^* \cap yX^* \neq \varnothing\}.$$

Спочатку зауважимо, що множина T містить порожнє слово. Справді, оскільки код X не є префіксним, то існують слова $x, y \in X$ такі, що $y = xu$ для деякого слова $u \in A^+$. Таким чином, отримуємо, що множина $xA^* \cap \{y\}$ є непорожньою. Звідси випливає, що $1 \in T$. Отож, множина T не є порожньою.

Далі покажемо, що множина T є скінченною. Нехай L — максимальна довжина слів у коді X. Прупустимо, що існує слово $t \in T$ довжини $|t| \geqslant dL$, де X має затримку дешифрування d. Оскільки $t \in T$, то $t = x_1 \cdots x_d t'$ для деяких кодових слів $x_1, \ldots, x_d \in X$ і деякого слова $t' \in P$.

Нехай $x, y \in X$ — різні слова такі, що множина $xtA^* \cap yX^*$ є непорожньою. Маємо $xtu = yw$ для деякого слова $w \in X^*$. Отже, $xx_1 \cdots x_d t'u = yw$, і оскільки код X має затримку дешифрування d, то отримуємо, що $x = y$, протиріччя. Таким чином, слово t не може бути елементом множини T. Звідси випливає, що всі слова множини T мають довжини менші за dL, а отже множина T є скінченною.

Розглянемо тепер деяке слово t множини T максимальної довжини. Маємо, що множина $xtA^* \cap yX^*$ є непорожньою для деяких різних слів $x, y \in X$. Таким чином, $xtu \in yX^*$ для деякого слово u, і ми можемо припускати, що $u \in A^+$. Справді, якщо $u = 1$, ми замінимо слово u іншим словом коду X. Покладемо $u = au'$, де a є першою літерою слова u. Ми збираємося довести, що $ta \in P$, звідки випливає, що $ta \in T$, протиріччя.

Приймемо $w = zta$, де z — слово максимальної довжини в скінченому коді X. За твердженням 2.5.6 множина $X^*wA^* \cap X^*$ є непорожньою. Таким чином існують слова $x_1, \ldots, x_n, y_1, \ldots, y_m \in X$ і $v \in A^*$ такі, що

$$x_1 \cdots x_n ztav = y_1 \cdots y_m$$

(див. рис. 5.5).

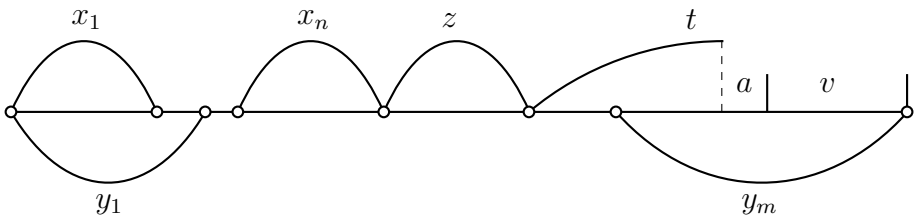


Рис. 5.5: Поповнення слова $w = zta$

Візьмемо мінімальне натуральне число n. Якщо $n \geqslant 1$, то маємо

$$x_1(x_2 \cdots x_n zt)av = y_1 \cdots y_m \qquad \text{і} \qquad t' = x_2 \cdots x_n zt \in P,$$

оскільки $t \in P$. Таким чином, множина $x_1 t' A^*$ перетинає множину $y_1 X^*$, і оскільки $t' \notin T$, то маємо $x_1 = y_1$. Отож,

$$x_2 \cdots x_n ztav = y_2 \cdots y_m,$$

а це суперечить мінімальності натурального числа n. Таким чином,

$$n = 0 \qquad \text{і} \qquad ztav = y_1 \cdots y_m$$

(див. рис. 5.6).

Зауважимо, що оскільки z є словом максимальної довжини, то слово y_1 є префіксом слова z. Припустимо протилежне, що $y_1 \neq z$. Тоді для деякого префікса t_1 слова $y_2 \cdots y_m$ маємо, що $y_1 t_1 = zt$. Оскільки $t \in P$, то множина $y_1 t_1 A^*$ перетинає множину zX^* і ми отримуємо, що $t_1 \in T$, протиріччя, оскільки

$$|y_1| < |z| \qquad \Longrightarrow \qquad |t_1| > |t|.$$

Отож,

$$y_1 = z \qquad \text{і} \qquad tav = y_2 \cdots y_m.$$

Таким чином, $ta \in P$, що і вимагалось довести. Це і завершує доведення теореми. □

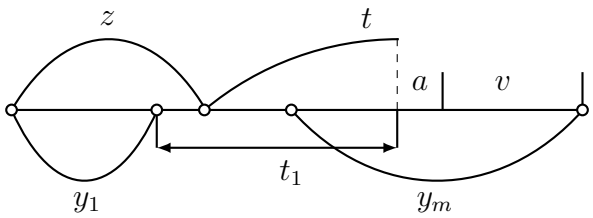


Рис. 5.6: Наслідком $y_1 \neq z$ є, що $zt = y_1 t_1$

Теорему 5.2.4 можна переформулювати еквівалентним чином так:

Теорема 5.2.4. *Кожен максимальний скінченний код є або префіксним, або має нескінченну затримкою дешифрування.*

Наступні приклади показують, що теорема 5.2.4 є оптимальною в багатьох напрямках.

Приклад 5.2.5. Суфіксний код

$$X = \{aa, ba, b\}$$

є скінченним максимальним кодом і має нескінченну затримку дешифрування.

Приклад 5.2.6. Код

$$X = \{ab, abb, baab\}$$

має скінченну затримку дешифрування 1. Він не є ні префіксним, ні максимальним: справді, слово $bbab$, для прикладу, можна додати до нього.

Приклад 5.2.7. Код

$$X = ba^*$$

є максимальним і суфіксним. Він має мінімальну затримку дешифрування 1. Цей код є префіксним, але не є нескінченним.

Решта цього розділу присвячена доведенню аналога теореми 2.5.24 для кодів зі скінченною затримкою дешифрування. Наступний приклад показує, що конструкція, використана в доведенні теореми 2.5.24, не застосовується в цьому контексті.

Приклад 5.2.8. Нехай

$$X = \{a, ab\}, \qquad A = \{a, b\} \qquad \text{і} \qquad y = bba,$$

як в прикладі 2.5.26. Множина $Y = X \cup y(Uy)^*$ з $U = A^* \setminus (X^* \cup A^* y A^*)$, побудована в доведенні теореми 2.5.24 є максимальним кодом, але вона має нескінченну затримку дешифрування. Справді, слово $y' = ya^d bby$ є в множині Y для кожного натурального числа d, і має власний префікс ya^d в Y^{d+1}.

Теорема 5.2.9. *Кожен раціональний код зі скінченною затримкою дешифрування d міститься в максимальному раціональному коді з тою самою скінченною затримкою дешифрування d.*

Нехай X — непорожній код із затримкою дешифрування d. Якщо $d = 0$, то код X є префіксним і наступний результат є очевидний: нехай L — множина власних префіксів слів множини X і $\overline{L} = A^* \setminus L$ — його доповнення. Нехай $X' = \overline{L} \setminus \overline{L}A^+$. Тоді $Y = X \cup X'$ є, легко бачити, максимальним префіксним кодом, який містить код X. Якщо код X є раціональним, то Y є також раціональним кодом.

Далі будемо вважати, що $d \geqslant 1$. Нехай Q — множина слів, які не мають префіксів у X, і які не є множником у жодному слові коду X. Тепер, нехай P — множина слів в множині Q, які є мінімальними для префіксного порядку: $P = Q \setminus QA^+$. Зауважимо, що множина P є префіксним кодом. Більше того, слова в множинах P та X є непорівняльними стосовно префіксного порядку.

Будемо говорити, що пара $(w, p) \in X^* \times P$ є *доброю*, якщо w є найдовшим префіксом в X^* слова wp. Зауважимо, якщо пара (w, p) э доброю, то ця пара повністю визначається словом wp. Зауважимо, що кожна пара $(1, p)$ для слова $p \in P$ є доброю.

Будемо говорити, що пара $(w, p) \in X^* \times P$ є *дуже доброю*, якщо пара (uw, p) є доброю для довільного слова $u \in X^*$. Зауважимо, якщо пара (w, p) є дуже доброю, то пара (uw, p) є також дуже доброю для довільного слова $u \in X^*$.

Нехай S' — множина слів v вигляду $v = wp$ таких, що пара (w, p) є доброю, але не є дуже доброю. Тоді означимо $S = P \cup S'$. Зауважимо, що множина $P \cap S'$ може бути непорожньою, і що довільний елемент множини $S' \setminus P$ є вигляду wp, де пара (w, p) є доброю, але не є дуже доброю і $w \in X^+$. Більше того, нехай R — множина слів v вигляду $v = xwp$ таких, що $x \in X$ і $w \in X^*$, пара (xw, p) є дуже доброю, і $wp \in S$ з доброю парою (w, p). Тоді ми означимо

$$Y = X \cup RS^*. \tag{5.2}$$

Твердження 5.2.10. *Множина Y є кодом із затримкою дешифрування d.*

Доведення твердження 5.2.10 спирається на декілька наступних лем.

Лема 5.2.11. *Якщо пара (m, p) є доброю, але не є дуже доброю, то існують різні слова x' і x'' в X, факторизація $p = p_1p_2$ з $p_1 \neq \varepsilon$, і $w, v \in X^*$ такі, що $x'wmp = x''vp_2$.*

Доведення. Оскільки пара (m, p) не є дуже доброю, то можемо знайти слова $w', v' \in X^*$ і факторизація $p = p_1p_2$ з $p_1 \neq \varepsilon$ такі, що $w'mp = v'p_2$. Виберемо таке відношення найкоротшої довжини. Тоді слово w' є непорожнім, оскільки пара (m, p) є доброю, і слово v' є непорожнім, оскільки $|p| > |p_2|$. Таким чином (див. рис. 5.7) $w' = x'w$,

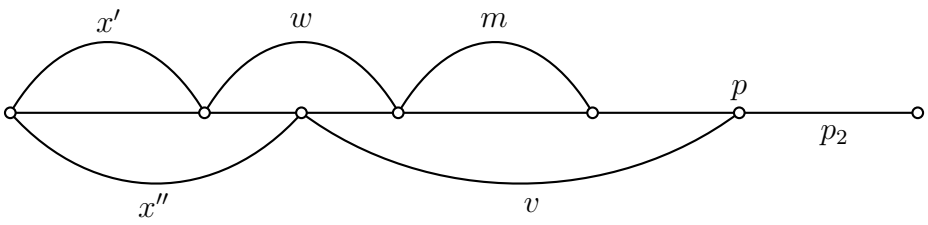


Рис. 5.7: Добра пара, яка не є дуже доброю парою

$v' = x''v$ з $w, v \in X^*$, $x', x'' \in X$. З мінімальності отримуємо, що $x' \neq x''$. □

Лема 5.2.12. *Множина $S \cap X^d A^*$ є порожньою.*

Доведення. Припустимо, що $s = ut$ з $s \in S$, $u \in X^d$ і $t \in A^*$. Зауважимо, що слово s не міститься в P, оскільки воно має префікс у коді X. Таким чином, $s = mp$, з парою (m, p), яка є доброю, але не є дуже доброю. Маємо $mp = ut$ і слово u не може бути довшим за m, оскільки пара (m, p) є доброю. Отож, $m = um'$ з $m' \in A^*$. Далі за лемою 5.2.11 можна знайти два різні слова $x', x'' \in X$, факторизацію $p = p_1 p_2$ з $p_1 \neq \varepsilon$, s $w, v \in X^*$ такі, що $x'wmp = x''vp_2$.

Отож,

$$x''vp_2 = x'wum'p_1p_2$$

і звідси випливає, що

$$x''v = x'wum'p_1,$$

а це суперечить тому факту, що код X має затримку дешифрування d, оскільки $v \in X^*$ і $u \in X^d$. □

Лема 5.2.13. *Нехай $u, v \in X^*$, $r = mp \in R$ де пара (m, p) дуже доброю. Тоді:*

(*i*) *слово ur не може бути префіксом слова v, тобто множина $X^*RA^* \cap X^*$ є порожньою;*
(*ii*) *якщо слово v є префіксом слова ur, який не є коротшим за слово um, то $v = um$;*
(*iii*) *якщо слово um є префіксом слова v та слова ur і v є сумісними стосовно префіксного порядку, то $um = v$.*

Доведення. (*i*) Припустимо, що $urt = v$ для деякого слова $t \in A^*$. Тоді $umpt = v$. Оскільки слово p не є множником жодного слова в X, то декодуючи слово $v \in X^*$, знайдемо таке слово $p = p_1p_2$, що $p_1, p_2 \neq \varepsilon$ і $ump_1 \in X^*$, а це суперечить тому факту, що пара (m, p) є дуже доброю.

(*ii*) Маємо, що $ump = ur = vt$ для деякого слова $t \in A^*$. Оскільки $|um| \leqslant |v|$, то слово v має непорожній суфікс у слові p: існує факторизація $p = p_1p_2$ така, що $ump_1 = v$. Також, позаяк пара (m, p) є дуже доброю, то маємо $p_1 = \varepsilon$ і $v = um$.

(*iii*) Оскільки слова ur і v є сумісними стосовно префіксного порядку, то одне з них є префіксом іншого. За твердженням (*i*) слово v є префіксом слова ur. Оскільки слово um є префіксом слова v, то застосувавши твердження (*ii*), отримуємо, що $v = um$. □

Лема 5.2.14. *Нехай $v \in X^*$, $s = mp \in S$, де пара (m, p) доброю. Тоді:*

(*i*) *слово s не може бути префіксом слова v, тобто множина $SA^* \cap X^*$ є порожньою;*
(*ii*) *якщо слово v є префіксом слова s, який не є коротшим за слово m, то $v = m$;*
(*iii*) *якщо слово m є префіксом слова v та слова s і v є сумісними стосовно префіксного порядку, то $m = v$.*

Доведення. (*i*) Припустимо, що $v = st$ для деякого слова $t \in A^*$. Тоді $v = mpt$. Оскільки слово p не є множником жодного слова з коду X, то маємо, що $p = p_1p_2$ для деяких $p_1, p_2 \neq \varepsilon$ і $v = mp_1$, а суперечить тому, що пара (m, p) доброю.

(*ii*) Припустимо, що $mp = s = vt$ для деякого слова $t \in A^*$. Оскільки $|m| \leqslant |v|$, то $p = p_1p_2$ для $v = mp_1$. Також, оскільки пара (m,p) є доброю, то $p_1 = \varepsilon$ і $v = m$.

(*iii*) Оскільки слова s і v є сумісними стосовно префіксного порядку, то одне з них э префіксом іншого. За твердженням (*i*) слово v є префіксом слова s. Оскільки слово m є префіксом слова v, то використавши твердження (*ii*) отримуємо, що $m = v$. □

Лема 5.2.15. *Множини X^*R і S є префіксними кодами.*

Доведення. Спочатку розглянемо множину X^*R. Припустимо, що $u, u' \in X^*$, $r, r' \in R$ і слово ur є префіксом слова $u'r'$. Вважатимемо, що We $r = mp$, $r' = m'p'$, де пари (m, p) і (m', p') є дуже добрими. Тоді слово ump є префіксом слова $u'm'p'$. Таким чином, слова um і $u'm'$ є порівняльними стосовно префіксного порядку. Більше того, слова ur і $u'm'$ є порівняльними стосовно префіксного порядку, і оскільки всі ці чотири слова є префіксами слова $u'r'$, то слова $u'r'$ і um є також порівняльними стосовно префіксного порядку. За лемою 5.2.13(*iii*) маємо, що $um = u'm'$. Отож, слово p є префіксом слова p'. Таким чином, $p = p'$, оскільки P є префіксним кодом. Звідси випливає, що $ur = u'r'$, а отже X^*R є префіксним кодом.

Маємо $S = S' \cup P$. Оскільки слова в кодах P і X є непорівняльними стосовно префіксного порядку, множина $S' \setminus P$ міститься в X^+P, множина P э префіксною, то зводиться до того, щоб показати, що множина S' є префіксною. Нехай u і u' — слова з S' і приймемо $u = wp$ і $u' = w'p'$, де (w, p) і (w', p') є добрими парами. Припустимо, що $wp \leqslant w'p'$. Якщо $w = w'$, то $p = p'$ та пари (w, p) і (w', p') збігаються. Ми вважатимемо, що $w \neq w'$.

Маємо $w < w'$, оскільки, якщо виконується умова $w' < w$ і позаяк слово w є префіксом слова $w'p'$, то пара слів (w', p') не буде доброю. Насправді, $wp \leqslant w'$, оскільки в іншому випадку $w < w' \leqslant wp$ і пара (w, p) не буде доброю.

Отож, слово wp є префіксом слова w'. Позаяк слово p не є множником слова з коду X, то існує факторизація $p = p_1p_2$ з $p_1, p_2 \neq= \varepsilon$ такі, що wp_1 міститься в X^*, а це суперечить тому, що пара слів (w, p) є доброю. □

Лема 5.2.16. *Виконуєтьсяа такі умови:*

(*i*) $SA^* \cap X^*RA^* = \varnothing$;
(*ii*) $SA^* \cap Y^* = \varnothing$.

Доведення. (*i*) Нехай $s \in S$, $r \in R$ і $v \in X^*$ — такі слова, що s і vr є порівняльними стосовно префіксного порядку. Ми не можемо мати, що $s \in P$, оскільки $vr \in X^+A^*$. Покладемо $s = mp$ і $r = m'p'$, де пара (m, p) є доброю, але не дуже доброю, а пара $(m', p")$ є дуже доброю. Тоді слова m і vm' є порівняльними стосовно префіксного порядку.

Якщо слово vm' є префіксом слова m, оскільки слова vr і m є порівняльними стосовно префіксного порядку, а з леми 5.2.13(*iii*) випливає, що $vm' = m$. Якщо припустимо протилежне, тобто слово m є префіксом слова vm', то оскільки слова s і vm' є порівняльними стосовно префіксного порядку, з леми 5.2.14(*iii*) випливає, що $m = vm'$. Таким чином, отримуємо, що $m = vm'$ в обох випадках. Позаяк $s = mp$ і $vr = vm'p'$, то отримуємо, що слова p і p' є порівняльними стосовно префіксного порядку. Отож, $p = p'$, оскільки множина P є префіксним кодом. Ми робимо висновок, що $s = vr$.

Позаяк пара $(vm', p) = (m, p)$ не є дуже доброю, то ми досягаємо протиріччя з фактом, що пара $(m', p') = (m', p)$ є дуже доброю.

(ii) За лемою 5.2.14(i) маємо, що $SA^* \cap X^* = \varnothing$. Оскільки $Y = X \cup RS^*$, то бачимо, що $Y^* \subseteq X^* \cup X^*RA^*$, а отже з твердження (i) випливає, що $SA^* \cap Y^* = \varnothing$. □

Доведення твердження 5.2.10. Достатньо довести лише, що множина Y має затримку дешифрування d, оскільки вона обов'язково є кодом за твердженням 5.1.1. Припустимо протилежене, нехай множина Y не має затримки дешифрування d. Ми можемо знайти слова $y_1, \ldots, y_{d+1}, z_1, \ldots, z_n \in Y$, $w \in A^*$ такі, що

$$y_1 y_2 \cdots y_{d+1} w = z_1 \cdots z_n, \tag{5.3}$$

де $y_1 \neq z_1$. Не зменшуючи загальності, ми можемо вважати, що $|w| < |z_n|$, бо в іншому випадку слово z_n є суфіксом слова w and ми можемо скоротити співвідношення шляхом спрощення слова z_n.

Оскільки код X має затримку дешифрування d, то не всі слова $y_1, \ldots, y_{d+1}, z_1, \ldots, z_n$ є елементами коду X. Таким чином, якщо всі слова z_j є в X, то деяке слово y_i є елементом множини $Y \setminus X$, а отже є в RA^*. Тоді $y_1 \cdots y_{d+1} w \in X^*RA^*$ і $z_1 \cdots z_n \in X^*$. Це суперечить лемі 5.2.13(i). Ми робимо висновок, що деяке слово z_j є елементом множини $Y \setminus X$.

Припустимо, що всі слова y_i є елементами коду X. За припущенням довжини на слово w маємо, що слово $y_1 \cdots y_{d+1}$ міститься в $z_1 \cdots z_{n-1}A^*$. Якщо одне зі слів $z_1, \ldots, z_{n-1}$ міститься в $Y \setminus X$, то $y_1 \cdots y_{d+1} \in X^* \cap X^*RA^*$, а це суперечить лемі 5.2.13(i). Таким чином, отримуємо $z_1, \ldots, z_{n-1} \in X$ і $z_n \in Y \setminus X$. Оскільки $z_n \in RS^*$, то можемо записати $z_n = xurpm$, з $x \in X$, $u \in X^*$, $m \in S^*$, пара (xu, p) є дуже доброю, і $up \in S$, пара (u, p) є доброю.

Маємо

$$y_1 \cdots y_{d+1} w = z_1 \cdots z_{n-1} xurpm.$$

Таким чином, слова $z_1 \cdots z_{n-1} xup$ і $y_1 \cdots y_{d+1}$ є порівняльними стосовно префіксного порядку. Якщо слово $z_1 \cdots z_{n-1} xu$ є префіксом слова $y_1 \cdots y_{d+1}$, то за лемою 5.2.13(iii) вони збігаються. Але з рівності $y_1 \cdots y_{d+1} = z_1 \cdots z_{n-1} xu$ випливає, що $y_1 = z_1$, оскільки множина X є кодом, протиріччя.

Таким чином, слово $y_1 \cdots y_{d+1}$ є префіксом слова $z_1 \cdots z_{n-1} xu$. Позаяк $y_1 \neq z_1$, і оскільки код X має затримку дешифрування d, то $n = 1$ і $y_1 = x$. Отож, слово $y_1 \cdots y_{d+1}$ є префіксом слова xu, а отже слово $y_1 \cdots y_{d+1}$ є префіксом слова u. Звідси випливає, що отже слово $y_1 \cdots y_{d+1}$ є префіксом слова $up \in S$, що суперечить лемі 5.2.12.

Зі всього цього випливає, що деякі слова y_i і z_j не є елементами коду X, а отже вони містяться в множині RS^*. Візьмемо такі мінімальні i та j. Тоді $y_i = ru$ і $z_j = r'u'$ для деяких $r, r' \in R$. Більше того, слова $y_1 \cdots y_{i-1} r$ і $z_1 \cdots z_{j-1} r'$ є порівняльними стосовно префіксного порядку за рівністю (5.3). Тоді з леми 5.2.15 отримуємо, що

$$y_1 \cdots y_{i-1} r = z_1 \cdots z_{j-1} r'.$$

Ми можемо записати $r = xmp$, $r' = x'm'p'$, де (xm, p) і $(x'm', p')$ є дуже добрі пари та (m, p) і (m', p') є добрими парами, а також $mp, m'p' \in S$. Тоді з рівності

$$y_1 \cdots y_{i-1} xmp = z_1 \cdots z_{j-1} x'm'p'$$

за означенням дуже доброї пари випливає, що $p = p'$, оскільки всі слова

$$y_1, \dots, y_{i-1}, z_1, \dots, z_{j-1}, x, x', m, m'$$

є елементами вільного моноїда X^*. Отож, отримуємо

$$y_1, \dots, y_{i-1}xm = z_1, \dots, z_{j-1}x'm'.$$

Якщо $i, j \geqslant 2$, то $y_1 = z_1$, оскільки множина X є кодом, отримали протиріччя.

Звідси випливає, що маємо мати, що $i = 1$ або $j = 1$, тобто одне зі слів y_1 або z_1 міститься в множині RS^*. Припустимо, що $i = 1$ і $j > 1$. Тоді отримуємо

$$xm = z_1 \cdots z_{j-1}x'm',$$

звідки випливає, що $x = z_1$ і

$$m = z_2 \cdots z_{j-1}x'm'.$$

Зауважимо, що $m \neq 1$. Оскільки пара $(x'm', p)$ є дуже доброю, то пара

$$(z_2 \cdots z_{j-1}x'm', p)$$

є також дуже доброю. Тепер ця пара збігається з парою (m, p), яка не є дуже доброю, протиріччя.

Таким чином, отримуємо, що одночасно не виконуються умови $i = 1$ та $j > 1$. Аналогічно доводиться, що що одночасно не виконуються умова $i > 1$, чи умова $j = 1$. Таким чином, маємо, що $i = j = 1$, тобто $y_1, z_1 \in RS^*$. Оскільки множини R і S є префіксними кодами, то за лемою 5.2.15 виконується одна з умов

$$y_1 = rs_1s_2, \quad z_1 = rs_1 \qquad \text{або} \qquad y_1 = rs_1, \quad z_1 = rs_1s_2,$$

де $r \in R$, $s_1, s_2 \in S^*$, $s_2 \neq \varepsilon$. У першому випадку, за рівністю (5.3) і після спрощення на z_1 отримуємо, що

$$z_2 \cdots z_n = s_2y_2 \cdots y_{d+1}w,$$

що суперечить лемі 5.2.16(ii). Таким чином, виконується другий випадок. Знову за рівністю (5.3) маємо, що

$$y_2 \cdots y_{d+1}w = s_2z_1 \cdots z_n.$$

Щоб уникнути такого ж протиріччя, ми повинні мати, що слово $y_2 \cdots y_{d+1}$ є власним префіксом слова s_2. З леми 5.2.16(i) виводимо, що слова $y_2, \dots, y_{d+1}$ містяться в коді X.

Ми можемо записати $s_2 = ss_3$, де $s \in S$, $s_3 \in S^*$. Оскільки $d \geqslant 1$, то слово y_2 є префіксом слова s_2, звідки випливає, що слово y_2 є префіксом слова s, або навпаки. Таким чином, $s \notin P$, а отже $s \in S'$. Ми виводимо, що можемо писати $s = mp$ для деякої доброї, але не дуже доброї пари (m, p), і за лемою 5.2.11 існують слова $f, n \in X^*$, $x, x' \in X$ з $x \neq x'$ такі, що $xnmp = x'fq$ з $|q| < |p|$.

Ми знаємо, що слово $y_2 \cdots y_{d+1}$ є власним префіксом слова $s_2 = mps_3$. Тепер, слово m не є префіксом слова $y_2 \cdots y_{d+1}$, оскільки в протилежному випадку за лемою 5.2.14(iii) ми отримуємо, що $m = y_2 \cdots y_{d+1}$ і слово $mp \in S$ має префікс в X^d, а це суперечить лемі 5.2.12. Отож, слово $y_2 \cdots y_{d+1}$ є префіксом слова m. Нехай $m = y_2 \cdots y_{d+1}g$. Тоді $xny_2 \cdots y_{d+1}gp = x'fq$, і оскільки $|q| < |p|$ і $n, f \in X^*$, а це суперечить тому факту, що код X має затримку дешифрування d. □

Твердження 5.2.17. *Множина Y є повним кодом.*

Якщо код X є щільною множиною, то множина Y щільна і тому є повною. Отже, можемо вважати, що X — тонкий код. Доведення твердження 5.2.17 спирається на наступну лему.

Лема 5.2.18. *Якщо X є тонким кодом, то множина $P \cup (X \setminus XA^+)$ є максимальним префіксним кодом.*

Доведення. Нехай $Z = P \cup (X \setminus XA^+)$. Тоді два елементи цього об'єднання є префіксними кодами. Більше того, кожне слово в множині P є непорівняльним стосовно префіксного порядку з довільним словом з коду X. Таким чином, множина Z є префіксним кодом, бо за припущенням маємо, що $X \neq \varnothing$, звідки випливає, що $1 \notin Z$.

Доведемо, що множина Z є повною справа. Нехай $w \in A^*$. Припустимо, що слово w не є порівняльним з X. Виберемо деяке слово u, яке не є множником жодного слова з коду X. Зауважимо, що таке слово існує, оскільки код X є тонким. Тоді слово wu не є множником довільного слова з коду X, а отже слово wu не має префіксів у X. Таким чином, слово wu має префікс з множини P, звідки випливає, що множина $wA^* \cap ZA^*$ є непорожньою. □

Доведення твердження 5.2.17. Виберемо деяке слово $v \in X^d$. Ми доведемо, що для довільного слова w множина $vwA^* \cap Y^*$ є непорожньою, а звідси випливатиме, що множина Y є повною. Припустимо протилежне, що

$$vwA^* \cap Y^* = \varnothing. \tag{5.4}$$

Ми можемо записати, що $vw = y_1 \cdots y_n u$ з $y_1, \ldots, y_n \in Y$ і зі словом u мінімальної довжини серед усіх таких факторизацій. Зауважимо, оскільки слово v міститься в $X^d \subseteq Y^*$, то слово v є обов'язково префіксом слова $y_1 \cdots y_n$. За лемою 5.2.18 знайдемо слово $p \in P \cup (X \setminus XA^+)$ таке, що p й u є порівняльними.

Ми стверджуємо, якщо слово p_1 є непорожнім префіксом слова p, то $y_1 \cdots y_n p_1 \notin Y^*$. Справді, якщо $y_1 \cdots y_n p_1 \in Y^*$, то оскільки слова p й u є порівняльними, то або слово p_1 є префіксом слова u, що суперечить мінімальності слова u, або u є префіксом слова p_1, а це суперечить умові (5.4).

За припущенням, слово p не міститься в коді X, а отже p є в P. Виберемо тепер мінімальне ціле число $i \in \{1, \ldots, n+1\}$ таке, що $y_i, y_{i+1}, \ldots, y_n$ є в X, а $i = n+1$ означає, що $y_n \notin X$. Тоді для кожного цілого числа j з $i \leqslant j \leqslant n$, пара $(y_j y_{j+1} \cdots y_n, p)$ є доброю: справді, якщо це не так, то $p = p_1 p_2$ з $p_1 \neq \varepsilon$ і $y_j \cdots y_n p_1 \in X^*$, що суперечить припущенню (див. рис. 5.8)

Візьмемо найменше таке ціле число $n+1 \geqslant j \geqslant i$, що $y_j y_{j+1} \cdots y_n p \in S$. Зауважимо, що таке ціле j існує оскільки $p \in S$. Якщо $j > i$, то $y_{j-1} y_j \cdots y_n p \in R$, бо справді пара $(y_{j-1} y_j \cdots y_n, p)$ є дуже доброю. Оскільки $R \subset Y$, то це суперечить нашому припущенню.

Таким чином, $j = i$. Якщо $i > 1$, то слово y_{i-1} не належить коду X, а отже воно міститься в RS^*. Тоді $y_{i-1} y_i \cdots y_n p \in RS^*$, оскільки $y_i \cdots y_n p \in S$, і ми знаходимо протиріччя з нашим припущенням.

Таким чином, ми звели до $i = 1$ і $y_1 \cdots y_n p \in S$. Звідси випливає, що пара $(y_1 \cdots y_n, p)$ є доброю, але не є дуже доброю, оскільки $y_1 \cdots y_n \neq \varepsilon$. Таким чином, за

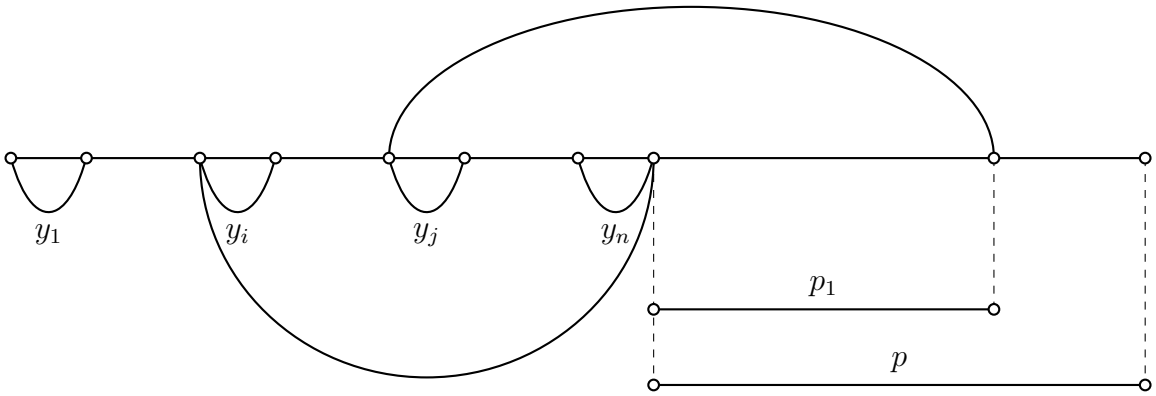


Рис. 5.8: Факторизація слова $y_1 \cdots y_n p$ з $y_i, \ldots, y_n \in X$ і $y_j \cdots y_n p_1 \in X^*$

лемою 5.2.11 знайдемо різні слова $x, x' \in X$ такі, що множина $xX^*y_1 \cdots y_n p \cap x'X^*p_2$ є непорожньою для деякої факторизації $p = p_1p_2$, $p_1 \neq \varepsilon$. Оскільки слово v є префіксом слова $y_1 \cdots y_n$, то останнє суперечить тому факту, що код X має затримку d. □

З вище викладеного доведення випливає така властивість: якщо тонкий код X^*A^+ зі затримкою дешифрування d є повним, то для довільного слова $x \in X^d$ й $u \in A^*$ існує слово $v \in A^*$ таке, що $xuv \in X^*$. Справді, тонкий повний код є максимальним за теоремою 2.5.13, а отже $X = Y$. Зауважимо, що ця властивість є також наслідком твердженням 5.2.3.

Твердження 5.2.19. *Якщо код X є раціональним, то множина Y є раціональним кодом.*

Доведення. Оскільки код X є раціональним, то множина $F(X)$ всіх його множників є раціональною. Звідси випливає, що множина $Q = A^* \setminus (F(X) \cup XA^*)$ є раціональною. Оскільки, $P = Q \setminus QA^+$, то множина P є також раціональною.

Нехай c — літера, що не належить алфавіту A і $\pi\colon (A \cup c)^* \to A^*$ — проекція така, що стирає (викреслює) літеру c. Для $u, p \in A^*$, ми будемо говорити, що слово ucp є *добрим* (відп. *дуже добрим*), якщо такою є пара (u, p). Через S_0 (відпо S_1) будемо позначати множину добрих (відп. дуже добрих) слів.

Нехай

$$L = (\pi^{-1}(X^*) \cap A^*cA^+)A^*.$$

Таким чином, L є множиною слів, які починаються із слова $z = ucw$ з $w \neq \varepsilon$ і $uw \in X^*$. Множина L є раціональною. Ми стверджуємо, що $S_0 = X^*cP \setminus L$, звідки випливає, що множина S_0 є раціональною.

У порядку доведення нехай $ucp \in S_0$. Тоді очевидно, що $u \in X^*$ і $p \in P$. Більше того, з припущення $ucp \in L$ випливає існування факторизації $p = ww'$ такої, що $w \neq \varepsilon$ і $uw \in X^*$, а це суперечить тому, що пара (u, p) є доброю. Навпаки, якщо $u \in X^*$, $p \in P$ і $ucp \notin L$, то не існує префікса слова up у вільному моноїді X^* строго довшого за слово u. Отож пара (u, p) є доброю і $ucp \in S_0$.

Аналогічно, $ucp \in S_1$ тоді і тільки тоді, коли $u \in X^*$, $p \in P$ і $X^*ucp \cap L = \varnothing$. Звідси випливає, що множина $S_1 = X^*cP \setminus (X^*)^{-1}L$ є раціональною.

Нехай R_0 — множина слів вигляду $xucp$, з $x \in X$ і $u \in X^*$, які є дуже добрими та такими, що $u = \varepsilon$ або слово ucp є добрим, але не є дуже добрим. Іншими словами,

$$R_0 = S_1 \cap X\left(P \cup (S_0 \setminus S_1)\right).$$

Звідси випливає, що множина R_0 є раціональною. Очевидно, що $R = \pi(R_0)$. Нагадаємо, що S' — множина слів вигляду up, де пара (u, p) є доброю, але не є дуже доброю. Отже, отримуємо, що $S' = \pi(S_0 \setminus S_1)$.

Це доводить, що множини S' і R є раціональними. Таким чином, множини $S = P \cup S'$ і $Y = X \cup RS^*$ також є раціональними. □

Доведення теореми 5.2.9. Нехай X — раціональний код із затримкою дешифрування d. Тоді код Y, визначений за рівнянням (5.2) має затримку d за твердженням 5.2.10. За твердженнями 5.2.17 і 5.2.19 код Y є раціональним і повним. Позаяк за твердженням 2.5.20 раціональний код є тонким, і за теоремою 2.5.13 тонкий і повний код є максимальним, то звідси випливає твердження теореми. □

Зауважимо, якщо код X є тонким, то Y також є тонким (вправа 5.4.10). Таким чином, довільний тонкий код із затримкою дешифрування d міститься в максимальному коді з тією ж затримкою дешифрування.

Приклад 5.2.20. Скінченний код $X = \{a, ab\}$ має затримку дешифрування 1. Маємо, що $P = \{ba, bb\}$. Добрими парами є такі, що мають вигляд (x, bb) і (x, ba) з $x \in X^*ab \cup \{\varepsilon\}$. Вони також є дуже добрими, виключаючи випадок, коли $x = \varepsilon$. Таким чином, маємо, що $S = P$ і $R = \{ab^3, ab^2a\}$. На завершенні отримуємо, що

$$Y = \{a, ab\} \cup \left\{ab^3, ab^2a\right\}\{bb, ba\}^*$$

є повним кодом із затримкою дешифрування 1, який містить код X. Автомат, який розпізнає вільний моноїд Y^* зображено на рис. 5.9.

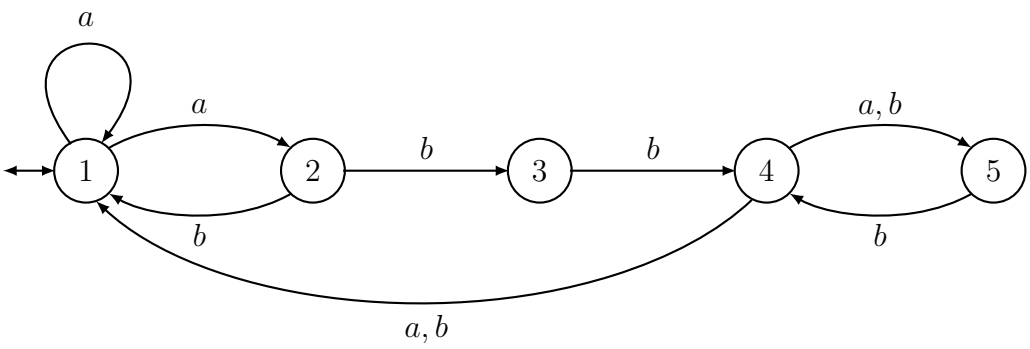


Рис. 5.9: Автомат, який розпізнає вільний моноїд Y^*

Зауважимо, що існує більш простіший повний код із затримкою дешифрування 1, який містить код X, а саме код ab^*. Було б цікаво мати повну процедуру, яка дає цей код безпосередньо. У наступному підрозділі ми побачимо процедуру, яка дає цей код, але для іншого означення затримки дешифрування (див. приклад 5.3.9).

5.3 Слабко префіксні коди

Існує ще одне означення, близьке до попереднього, де підраховується затримка літер алфавіта замість слів коду. Множина $X \subset A^+$ називається *слабко префіксною*, якщо існує натуральне число d таке, що виконується умова:

> якщо слово xu є префіксом слова $x'y'$ з $x, x' \in X$, слово u є префіксом слова з множини X^*, і $y' \in X^*$, то з $|u| \geqslant d$ випливає рівність $x = x'$.

Якщо ця умова виконується, то ми також будемо говорити, що множина X має *літерну затримку дешифрування* d.

Найменше ціле число d таке, що виконується вище зазначена імплікація називається *мінімальною літерною затримкою дешифрування*. Якщо такого цілого числа не існує, то будемо говорити, що множина має *нескінченну літерну затримку дешифрування*.

Твердження 5.3.1. *Нехай X — множина з мінімальною словесною затримкою дешифрування d і мінімальною літерною затримкою дешифрування e. Тоді*

$$d \leqslant e \leqslant d \max\{|x| \colon x \in X\}.$$

Доведення. Справді, припустимо, що множина X має літерну затримку дешифрування e, і розглянемо слова $x, x' \in X$, $y \in X^e$ та $y' \in X^*$ такі, що $xy \leqslant x'y'$. Оскільки $|y| \geqslant e$, то маємо, що $x = x'$, звідки випливає, що множина X має словесну затримку дешифрування e.

Навпаки, припустимо, що множина X має словесну затримку дешифрування d. Нехай $x, x' \in X$ і u є префіксом слова в X^* і $y \in X^*$ такі, що $xu \leqslant x'y'$ стосовно префіксного порядку з $|u| \leqslant d \max\{|x| \colon x \in X\}$ (див. рис. 5.10). За умовою на довжину

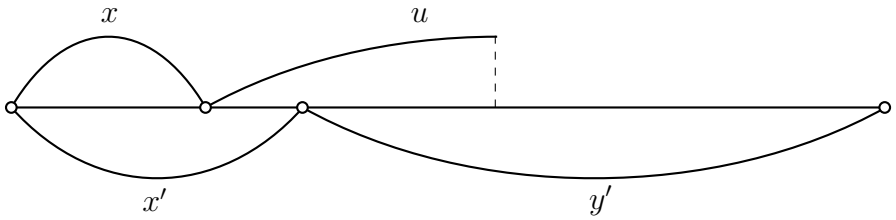


Рис. 5.10: Заборонена конфігурація для слабко префіксних кодів

маємо, що існує слово $y \in X^d$, яке є префіксом слова u. Таким чином, отримуємо $xy \leqslant xu \leqslant x'y'$. Оскільки множина X має словесну затримку дешифрування d, то $x = x'$. □

Таким чином, скінченна множина має одночасно скінченну затримку дешифрування для обох понять, але приклад $X = \{b\} \cup ba^*c \cup a^*d$ показує, що означення розрізняються, коли множина X є нескінченною. Справді, ця множина X має словесну затримку дешифрування 1, але вона має нескінчену літерну затримку дешифрування, оскільки для всіх натуральних значень n умова означення не виконується для $x = b$, $u = a^n$, $x' = ba^nc$ і $y' = \varepsilon$.

Твердження 5.3.2. *Слабко префіксна множина є кодом.*

Доведення. Нехай множина X має літерну затримку дешифрування d. За твердженням 5.3.1 множина X має словесну затримку дешифрування d, і за твердженням 5.1.1 множина X є кодом. □

Будемо говорити, що автомат $\mathcal{A}$ *має затримку* d, якщо для довільної пари шляхів

$$p \xrightarrow{a} q \xrightarrow{z} r, \qquad p \xrightarrow{a} q' \xrightarrow{z} r',$$

з $|z| = d$ випливає рівність $q = q'$. Таким чином, кожен детермінований автомат має затримку 0. Автомат зі скінченною затримкою також називається *слабко детермінованим*. Зауважимо, якщо автомат $\mathcal{A}$ має затримку d, то для довільного слова w і для довільної пари шляхів

$$p \xrightarrow{w} q \xrightarrow{z} r, \qquad p \xrightarrow{w} q' \xrightarrow{z} r',$$

з $|z| = d$, шляхи $p \xrightarrow{w} q$ і $p \xrightarrow{w} q'$ збігаються.

Твердження 5.3.3. *Сильно зв'язний слабко детермінований автомат є однозначним.*

Доведення. Справді, нехай $c\colon p \xrightarrow{w} q$ і $c'\colon p \xrightarrow{w} q$ — два шляхи в автоматі $\mathcal{A}$ зі стану p в стан q з однаковою міткою w. Оскільки автомат $\mathcal{A}$ сильно зв'язним, то для довільного $d \geqslant 0$ існує шлях $q \xrightarrow{z} r$ з $|z| = d$. Звідси випливає, що $c = c'$. □

Наступне твердження доводить, що код X є слабко префіксним тоді і тільки тоді, коли вільний моноїд X^* розпізнається деяким слабко детермінованим автоматом $\mathcal{A} = (Q, 1, 1)$.

Твердження 5.3.4. *Нехай X — код і $\mathcal{A} = (Q, 1, 1)$ — автомат із затримкою d, що розпізнає вільний моноїд X^*. Тоді код X має літерну затримку дешифрування d. Навпаки, якщо код X має скінченну літерну затримку дешифрування, то автомат можна вибрати так, що він буде мати туж саму затримку, що і код X.*

Доведення. Спочатку припустимо, що вільний моноїд X^* розпізнається автоматом $\mathcal{A} = (Q, 1, 1)$ із затримкою d. Ми покажемо, що код X має словесну затримку дешифрування d. Нехай $x, x' \in X$, $u \in A^*$ — префікс слова в X^* з $|u| = d$ і $y' \in X^*$ такі, що $xu \leqslant x'y'$. Оскільки автомат $\mathcal{A}$ розпізнає вільний моноїд X^*, то існують шляхи

$$c\colon 1 \xrightarrow{x} 1 \xrightarrow{u} p \qquad \text{і} \qquad c'\colon 1 \xrightarrow{x'} 1 \xrightarrow{y'} 1.$$

Позаяк слово xu є префіксом слова $x'y'$, то шлях c' має розклад

$$c'\colon 1 \xrightarrow{x} q \xrightarrow{u} p' \xrightarrow{w} 1,$$

для деяких станів q, p' і деякого слова w. Оскільки $|u| = d$, то два шляхи c і c' мають однаковий префікс довжини $|x|$, а отже $q = 1$. Припустимо, що слово x є префіксом слова x'. Тоді $x' = xz$ для деякого слова $z \in A^*$, і шлях $1 \xrightarrow{x'} 1$ розкладається в $1 \xrightarrow{x} 1 \xrightarrow{z} 1$. Це доводить, що $z \in X^*$, а отже $z = \varepsilon$. Таким чином, отримуємо $x = x'$. В іншому випадку міркування є аналогічними з точністю до симетрії.

Навпаки, нехай код X має літерну затримку дешифрування d, $\mathcal{A} = (Q, i, T)$ — обрізаний детермінований автомат, що розпізнає множину X і $\mathcal{A}^* = (Q \cup \omega, \omega, \omega)$ — зірка автомата $\mathcal{A}$. Ми покажемо, що автомат $\mathcal{A}^*$ має затримку d. Припустимо, що

$$p \xrightarrow{a} q \xrightarrow{z} r \qquad \text{і} \qquad p \xrightarrow{a} q' \xrightarrow{z} r'$$

з $|z| = d$. Тоді за побудовою автомата $\mathcal{A}^*$ один із станів q, q' збігається зі станом ω. Нехай для прикладу $q = \omega$. Оскільки автомат $\mathcal{A}^*$ є обрізаним, то існує шлях $\omega \xrightarrow{w} p$ і ми можемо припускати, що цей шлях не проходить через стан ω наскрізь. Ми також маємо шлях $r' \xrightarrow{v} \omega$ (див. рис. 5.11). Тоді $wa \in X$ і $wazv \in X^*$. Нехай

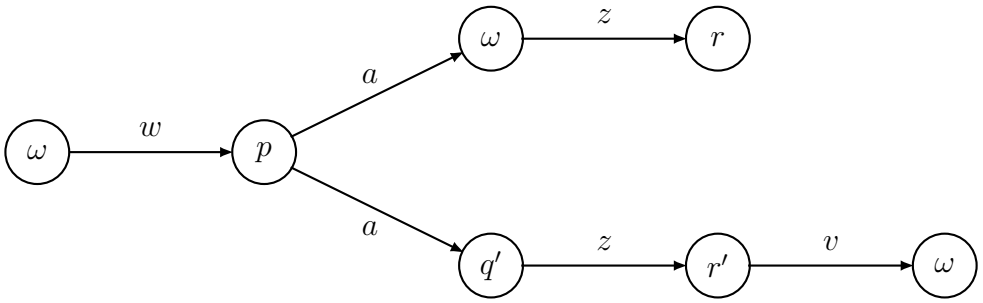


Рис. 5.11: Два шляхи в автоматі $\mathcal{A}^*$

$x = wa$ і $wazv = x'y'$ з $x' \in X$ і $y' \in X^*$. Оскільки множина X має літерну затримку дешифрування d, то $x = x'$. Звідси випливає, що $y = zv$. Отже в автоматі $\mathcal{A}^*$ існують шляхи

$$\omega \xrightarrow{x'} q' \xrightarrow{y'} \omega \qquad \text{і} \qquad \omega \xrightarrow{x'} \omega \xrightarrow{y'} \omega.$$

Позаяк автомат $\mathcal{A}^*$ є однозначним, то звідси випливає, що $q' = \omega$. Таким чином, автомат $\mathcal{A}^*$ має затримку d. □

Ми можемо зауважити, шо описаний вище автомат $\mathcal{A}^*$ може бути використаним для перевірки того, чи код є слабко префіксним, а також для обчислення мінімальної літерної затримки дешифрування.

Ми тепер повернемося до максимальних слабко префіксних кодів. Наступний результат є аналогом твердження 5.2.3.

Твердження 5.3.5. *Нехай X — максимальний код з літерною затримкою дешифрування d. Тоді кожне поповнювальне справа слово $u \in A^*$ довжини d є сильно поповнювальним справа.*

Доведення. Нехай $v \in A^*$. За твердженням 1.3.6 існує слово $w \in A^*$ таке, що слово uvw є необлямованим. За твердженням 5.2.1 існують слова $x \in X^*$ і $t \in A^*$ такі, що $xuvwt \in X^*$. Позаяк код X має літерну затримку дешифрування d і слово u є поповнювальним справа, то це слово є спрощуваним. Таким чином $uvwt \in X^*$, звідки випливає, що слово uv є поповнювальним справа. □

Будемо говорити, що автомат $\mathcal{A}$ є *слабко повним* або *d-повним*, якщо для довільного шляху $p \xrightarrow{w} q$ з $|w| = d$, існує шлях $p \xrightarrow{wa} q'$ для кожної літери $a \in A$. Зауважимо, що цей шлях не обов'язково починається із шляху $p \xrightarrow{w} q$.

Якщо автомат $\mathcal{A}$ є d-повним, то за індукцією для кожного шляху $p \xrightarrow{w} q$ з $|w| = d$ і для кожного слова x існує шлях $p \xrightarrow{wx} q'$.

Твердження 5.3.6. *Нехай X — тонкий код з літерною затримкою дешифрування d і $\mathcal{A} = (Q, 1, 1)$ — обрізаний автомат із затримкою d і розпізнає вільний моноїд X^*. Код X є повним тоді і тільки тоді, коли автомат $\mathcal{A}$ є d-повним.*

Доведення. Спочатку припустимо, що код X є повним. Нехай $p \xrightarrow{w} q$ — шлях в автоматі $\mathcal{A}$ з $|w| = d$ і $a \in A$ — довільна літера. Позаяк автомат $\mathcal{A}$ є обрізаним то існує шлях $1 \xrightarrow{u} p$. Оскільки код X є тонким і повним, то він є максимальним кодом за теоремою 2.5.13. За твердженням 5.3.5 слово uwa є поповнювальним справа. Отож, існує шлях $1 \xrightarrow{u} p' \xrightarrow{wa} q'$. Оскільки автомат $\mathcal{A}$ має затримку d і $|w| = d$, то $p = p'$ (див. рис. 5.12). Звідси випливає, що автомат $\mathcal{A}$ є d-повним.

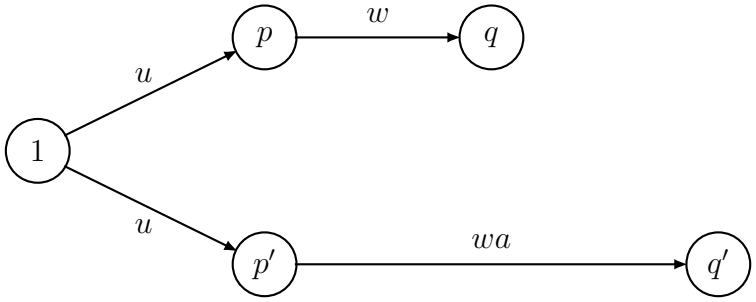


Рис. 5.12: Доведення d-повноти автомата $\mathcal{A}$

Навпаки, нехай $x \in X^+$ — слово довжини не менше d. Позаяк автомат $\mathcal{A}$ є d-повним, то для кожного слова $w \in A^*$ існує шлях $1 \xrightarrow{xw} p$. Звідси випливає, що код X є повним, оскільки автомат $\mathcal{A}$ є обрізаним. □

Ми можемо використати попередні результати для іншого доведення теореми 5.2.4. Нехай X — скінченний максимальний код. Припустимо протилежне: нехай словесна затримка дешифрування коду X є строго додатною. Оскільки код X є скінченним, то його його літерна затримка дешифрування d є також скінченною та строго додатною. За твердженням 5.3.4 існує скінченний d-повний автомат $\mathcal{A} = (Q, 1, 1)$ з мінімальною затримкою d який розпізнає вільний моноїд X^*.

Спочатку ми покажемо, що можна припустити, що автомат $\mathcal{A}$ є *розгорнутим* в тому сенсі, що всі стани в $\mathcal{A}$, крім початкового стану 1, мають напівстепінь входу 1. Цю властивість можна отримати, застосувавши наступний метод розщеплення стану:

> Нехай $q \neq 1$ — стан з напівстепінню входу $r > 1$. Цей стан розбивається на r копії, кожна з яких має напівстепінь входу 1 і з однаковими вихідними ребрами. Оскільки код X є скінченним, то всі цикли в автоматі $\mathcal{A}$ містять стан 1. Отже, поділ станів може бути повторений лише скіченною кількістю разів. Зрозуміло, що розщеплення станів зберігає затримку і d-повноту.

Припустимо тепер, що автомат $\mathcal{A}$ є розгорнутим і має мінімально можливу кількість станів. Оскільки автомат $\mathcal{A}$ має мінімвльну затримку дешифрування d, то існує

стан q такий, що існують ребра (q, a, r) і (q, a, r') з $r \neq r'$ і шляхи помічені $v \in A^{d-1}$, що виходять із r і r'. Доведемо, що $r, r' \neq 1$. Припустимо протилежне, що $r' = 1$. Нехай u — слово максимальної довжини таке, що існує шлях $r \xrightarrow{vu} 1$, що розкладається як $r \xrightarrow{v} s \xrightarrow{u} 1$ з простим шляхом $s \xrightarrow{u} 1$. Зауважимо, що слово vu є непорожнім, оскільки в протилежному випадку $r = 1 = r'$. Нехай b — перша літера слова uv. Зауважимо, що не існує шляху поміченого словом vb, який виходить зі стану 1, оскільки автомат $\mathcal{A}$ має мінімальну затримку дешифрування d (в протилежному випадку ми матимемо два шляхи $q \xrightarrow{a} 1 \xrightarrow{vb}$ і $q \xrightarrow{a} r \xrightarrow{vb}$ помічені словом avb, який починається зі стану q з різними початковими ребрами). Розглянемо тепер останню літеру c слова vu ш стан t такі, що $(t, c, 1)$ є останнім ребром шляху $r \xrightarrow{vu} 1$. Оскільки автомат $\mathcal{A}$ є d-повним, то існує шлях помічений словом cvb, який виходить зі стану t. Нехай (t, c, t') — перше ребро шляху (див. рис. 5.13, який відповідає випадку $u \neq \varepsilon$

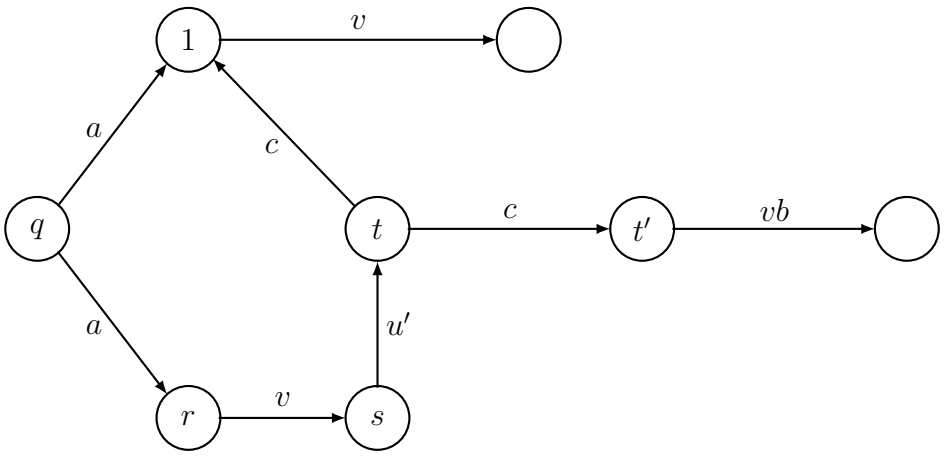


Рис. 5.13: Доведення, що $r' \neq \varepsilon$

і де $u = u'c$). Маємо $t' \neq 1$, оскільки не існує шляху поміченого словом vb і виходить з порожнього слова ε. Нехай $w \neq \varepsilon$ — слово таке, що існує простий шлях $t' \xrightarrow{w} 1$. Тоді існує простий шлях $s \xrightarrow{vu} 1$. Отримуємо протиріччя, оскільки слово uw є строго довшим, ніж u.

Нехай $\mathcal{A}' = (Q', 1, 1)$ — автомат утворений ототожненням станів r і r'. Оскільки $r, r' \neq 1$ і порядки входу обидвох цих станів дорівнюють 1 і туж ааму мітку на вхідному ребрі, то автомат $\mathcal{A}'$ також розпізнає вільний моноїд X^* і є розгорнутим. Оскільки в автоматі $\mathcal{A}'$ є строго менше станів, ніж у автоматі $\mathcal{A}$, ми отримуємо остаточне протиріччя.

Тепер доведемо такий результат, який є варіацією теореми 5.2.9. Доведення використовує автомати, і це проілюстровано в прикладі 5.3.10.

Теорема 5.3.7. *Кожен слабко префіксний раціональний код можна вкласти в максимальний слабко префіксний раціональний код з тією самою затримкою.*

Ми скористаємося наступною лемою. В доведенні ми використовуємо $q \xrightarrow{u}$ для позначення деякого шляху, який починається зі стану q і слово u є його міткою.

Лема 5.3.8. *Нехай $\mathcal{A} = (Q, 1, 1)$ — обрізаний автомат із затримкою дешифрування d. Можна отримати, додавши до автомата $\mathcal{A}$ скінченну кількість станів і ребер, обрізнай автомат $\mathcal{B} = (Q', 1, 1)$, який має затримку дешифрування d є d-повним.*

Доведення. У випадку $d = 0$ ми просто додамо в автомат $\mathcal{B}$ ребро $(q, a, 1)$ для всіх станів q і літер $a \in A$, для яких не існує ребра, що виходить з q і позначається літерою a в автоматі $\mathcal{A}$. Доведення для $d \geqslant 1$ складається з декількох етапів.

1. Ми почнемо з означення нового автомата $\mathcal{B}_0$. Додамо множину Q' станів, які позначаються $q(w)$, для $w \in A^*$, з $1 \leqslant |w| \leqslant d$, і покладемо $q(1) = 1$. Додамо ребра:

$$q(w) \xrightarrow{a} q(w'), \qquad \text{для} \quad w = aw',\ a \in A.$$

Позначимо через $\mathcal{B}_0 = (Q \cup Q', 1, 1)$ такий новий автомат. Очевидно, що автомат $\mathcal{B}_0$ також має затримку дешифрування d. Зауважимо, для подальшого використання на останньому етапі далі, що кожен стан з Q' є кодоступним, оскільки для кожного стану $q(w)$ маємо шлях $q(w) \xrightarrow{w} 1$.

Буде зручно називати *майбутнім* стану q множину слів w довжини $\leqslant d$ таких, що існує деякий шлях $q \xrightarrow{w}$. Зауважимо, що в автоматі $\mathcal{B}_0$ майбутнє стану $q(w)$ з $|w| = d$ — це множина префіксів слова w.

2. Тепер побудуємо послідовність автоматів $\mathcal{B}_1, \mathcal{B}_2, \ldots$ таку, що кожен з цих автоматів має ті ж самі стани, що і автомат $\mathcal{B}_0$. Очевидно, що така послідовність є скінченною. Ми покажемо, що всі автомати $\mathcal{B}_i$ цієї послідовності мають затримку дешифрування d. Нехай $\mathcal{B}_n$ — останній елемент цієї послідовності. Ми доведемо, що автомат $\mathcal{B}_n$ є d-повним. Якщо автомат $\mathcal{B}_i$ побудовано і він не є d-повним, то для деякого слова $u \in A^d$, деякої літери b і деякого стану q автомата $\mathcal{B}_i$, існує шлях $q \xrightarrow{u}$, але не існує шляху $q \xrightarrow{ub}$. Тоді, записавши $ub = aw$, з $a \in A$, ми додаємо до автомата $\mathcal{B}_i$ ребро $q \xrightarrow{a} q(w)$, і це буде новим автоматом $\mathcal{B}_{i+1}$ (див. рис. 5.14).

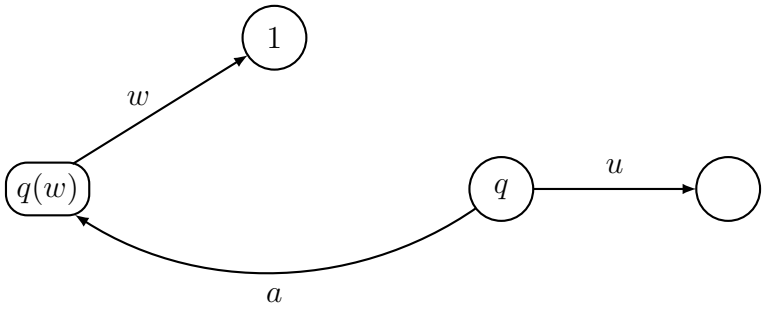


Рис. 5.14: Нове ребро $(q, a, q(w))$ додано в автоматі $\mathcal{B}_{i+1}$ (з $ub = aw$, оскільки не існує ребра $q \xrightarrow{ub}$)

3. Ми тепер доведемо технічну властивість: для кожного невід'ємного цілого числа i та для кожного стану p майбутнє стану p в автоматі $\mathcal{B}_i$ збігається з майбутнім стану p в автоматі $\mathcal{B}_0$. Звідси випливає, що для кожного слова $m \in A^d$ майбутнє стану $q(m)$ в кожному автоматі $\mathcal{B}_i$ збігається з множиною префіксів слова m.

Достатньо довести, якщо існує шлях $p \xrightarrow{v}$ в автоматі $\mathcal{B}_{i+1}$ з $|v| \leqslant d$, то існує завжди шлях $p \xrightarrow{v}$ в автоматі $\mathcal{B}_i$.

Для цього можемо припустити, що шлях $p \xrightarrow{v}$ в автоматі $\mathcal{B}_{i+1}$ передбачає нове ребро $q \xrightarrow{a} q(w)$, створене на етапі 2, де слово u є таким, що $ub = aw$, і шлях $q \xrightarrow{u}$ належить автоматові $\mathcal{B}_i$. Отож, ми можемо припускати, що цей шлях має вигляд

$$p \xrightarrow{v_1} q \xrightarrow{a} q(w) \xrightarrow{v_2} p'$$

з $v = v_1 a v_2$, причому останній відрізок шляху $q(w) \xrightarrow{v_2} p'$ міститься в автоматі $\mathcal{B}_i$. Тепер $|v_2| < d$, отож з припущення індукції про майбутнє стану $q(w)$ випливає, що слово v_2 є власним префіксом слова w. Таким чином, за побудовою нового ребра, існує в автоматі $\mathcal{B}_i$ шлях $q \xrightarrow{av_2}$, оскільки слово av_2 є префіксом слова u. Отже, ми отримуємо в автоматі $\mathcal{B}_{i+1}$ шлях $p \xrightarrow{v}$ з меншою кількістю появ нового ребра. Отже, шлях $p \xrightarrow{v}$ існує в автоматі $\mathcal{B}_{i+1}$, без появи нового ребра, і таким чином, цей шлях також міститься в автоматі $\mathcal{B}_i$, що доводить крок індукції.

4. Припустимо, що автомат $\mathcal{B}_i$ має затримку дешифрування d. Ми доведемо, що автомат $\mathcal{B}_{i+1}$ має ту ж саму затримку дешифрування. Припустимо, що для деяких станів p, p_1, p_2, деякої літери c і деякого слова $v \in A^d$, в автоматі $\mathcal{B}_{i+1}$ існує два шляхи $p \xrightarrow{c} p_1 \xrightarrow{v}$ і $p \xrightarrow{c} p_2 \xrightarrow{v}$. За пунктом 3 деякі шляхи $p_1 \xrightarrow{v}$ і $p_2 \xrightarrow{v}$ існують в автоматі $\mathcal{B}_i$. Якщо ребра $p \xrightarrow{c} p_1$ і $p \xrightarrow{c} p_2$ існують в автоматі $\mathcal{B}_i$, то $p_1 = p_2$, оскільки автомат $\mathcal{B}_i$ має затримку дешифрування d. В іншому випадку, $p_1 \neq p_2$, і рівно одно з двох ребер $p \xrightarrow{c} p_1$ або $p \xrightarrow{c} p_2$, нехай це буде скажемо $p \xrightarrow{c} p_1$, є новим ребром $q \xrightarrow{a} q(w)$, а інше ребро міститься в автоматі $\mathcal{B}_i$. Тоді $p = q$, $c = a$, $p_1 = q(w)$, а отже отримуємо $v = w$ за пунктом 2, оскільки довжина слова v дорівнює d. Отож, розглядаючи інше ребро (яке є в автоматі $\mathcal{B}_i$), ми бачимо, що існує шлях $q \xrightarrow{aw}$ в автоматі $\mathcal{B}_i$. Це суперечить припущенню, яке призвело до побудови на етапі 2.

5. Нехай $\mathcal{B}' = (Q \cup Q'', 1, 1)$ — обрізана частина автомата $\mathcal{B} = (Q \cup Q', 1, 1)$. Він все ще має затримку дешифрування d, і ми покажемо, що він все ще є d-повним. Припустимо, що існує шлях $p \xrightarrow{u}$ в автоматі $\mathcal{B}'$, і нехай a – літера. Оскільки автомат $\mathcal{B}$ є d-повним, то існує шлях $p \xrightarrow{ua}$ в автоматі $\mathcal{B}$. Оскільки стан p є доступним, то кожен стан в цьому шляху є доступним. Оскільки всі стани в Q' є кодоступними, то всі стани на шляху є одночасно доступними та кодоступними. Таким чином, цей шлях міститься в автоматі $\mathcal{B}'$. Це завершує доведення леми. □

Доведення теореми 5.3.7. Нехай X — непорожній раціональний код з літерною затримкою дешифрування d. За твердженням 5.3.4 існує однозначний автомат $\mathcal{A} = (Q, 1, 1)$ із затримкою дешифрування d, що розпізнає вільний моноїд X^*. Ми можемо припускати, що автомат $\mathcal{A}$ є обрізаним. За лемою 5.3.8 ми можемо вкласти автомат $\mathcal{A}$ в обрізаний автомат $\mathcal{B} = (Q', 1, 1)$, який має затримку дешифрування d і є d-повним.

Позаяк $\mathcal{B}$ є сильно зв'язним автоматом зі скінченною затримкою дешифрування, то за твердженням 5.3.3 він є однозначним. Таким чином, множина, яка розпізнається автоматом $\mathcal{B}'$ має вигляд Y^*, для деякого раціонального коду Y, що містить код X. Більше того, код Y має затримку дешифрування d, за твердженням 5.3.4, і він є повним за твердженням 5.3.6. Отож, Y є максимальним раціональним кодом із затримкою дешифрування d, який містить код X. □

Приклад 5.3.9. Нехай $X = \{a, ab\}$, визначений у прикладі 5.2.20. Використавши твердження 5.3.4, ми отримуємо автомат, зображений ліворуч на рис. 5.15. Застосувавши метод теореми 5.3.7 до цього автомата, ми отримуємо автомат, зображений праворуч на рис. 5.15. Це дає повний код $Y = ab^*$, який містить код X.

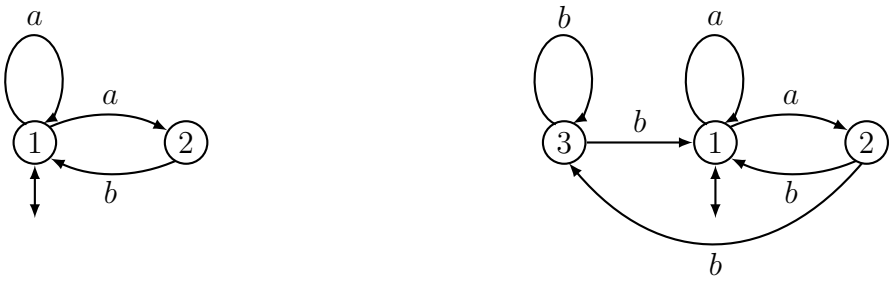


Рис. 5.15: Поповнення коду $X = \{a, ab\}$

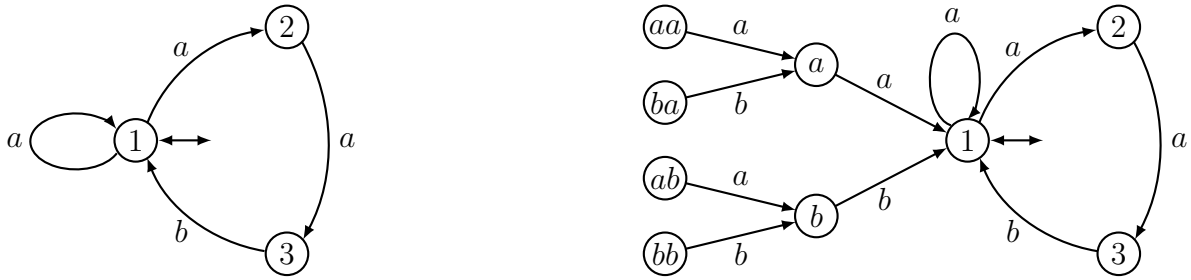


Рис. 5.16: Автомати $\mathcal{A}$ та $\mathcal{B}_0$

Приклад 5.3.10. Нехай $\mathcal{A}$ — автомат, зображений ліворуч на рис. 5.16. Він має затримку дешифрування 2 і розпізнає вільний моноїд $\{a, aab\}^*$, який є кодом з літерною затримкою дешифрування 2.

Автомат $\mathcal{B}_0$ зображений праворуч на рис. 5.16 (ми позначаємо нові стани через w замість $q(w)$ для спрощення зображення). Остаточний автомат $\mathcal{B}$ зображений на рис. 5.17 після видалення недоступних станів.

5.4 Вправи до розділу 5

Підрозділ 5.1

В. 5.4.1. Доведіть, що затримка дешифрування коду X є нескінченною тоді і тільки тоді, коли існує нескінченний шлях в графі G_X, який визначений в підрозділі 2.7, що починається у вершині в коді X. Якщо код X є скінченним, то це відбувається тоді і тільки тоді, коли існує цикл в графі G_X, який доступний з деякої вершини в коді X.

В. 5.4.2. (a) Доведіть, що код X має затримку дешифрування d, якщо довільні диз'юнктні факторизації $x_1 \cdots x_n p = y_1 \cdots y_m$, де $x_1, \ldots, x_n, y_1, \ldots, y_m$ є словами над X і p є префіксом слова в алфавіті X, що задовольняє нерівність $n \leqslant d$.

(b) Нехай $e_1 \cdots e_n$ — послідовність ребер шляху e з вершини s до вершини t в префіксному графі коду X. Поява e_i називається *парною* (*непарною*), якщо кількість перетинних ребер серед $e_1, \ldots, e_i$ є парним (непарним) числом. Доведіть це у двох

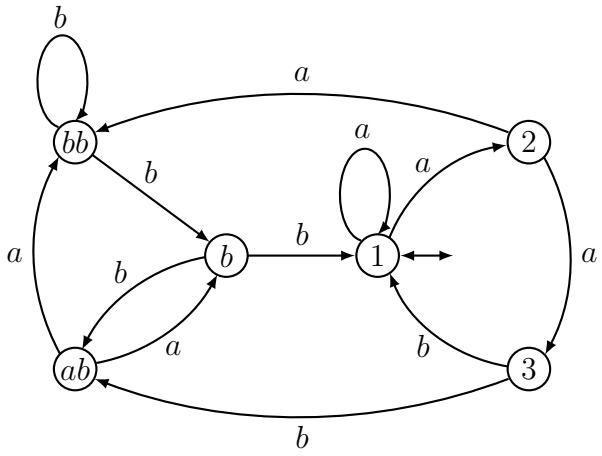


Рис. 5.17: Автомат $\mathcal{B}$

факторизаціях

$$(i)\ sy_1 \cdots y_l t = x_1 \cdots x_k \qquad \text{або} \qquad (ii)\ sy_1 \cdots y_l = x_1 \cdots x_k t,$$

кількість c перетинних ребер є непарним або парним, відповідно до (i) або (ii). Доведіть далі, що l — кількість парних ребер і k — кількість непарних ребер.

(c) Опишіть алгоритм за лінійний час для обчислення затримки дешифрування, припустивши, що не існує циклу в префіксному графі.

В. 5.4.3. Нехай Y і Z — композиційовні коди з зі скінченними затримками дешифрування $d(Y)$ і $d(Z)$. Доведіть, що код $X = Y \circ Z$ має скінченну затримку дешифрування $d(X) \leqslant d(Y) + d(Z)$.

(Підказка: Доведіть, що для $y \in X^{d(Y)}$, $z \in X^{d(Z)}$, слово yz є спрощенням для коду X.)

В. 5.4.4. Нехай $X = \{x, y\}$ — двоелементний код. Доведіть, що X має скінченну затримку дешифрування.

(Підказка: Використайте індукцію по $|x|+|y|$, і застосуйте результати вправи 5.4.3.)

В. 5.4.5. Нехай $X \subset A^*$ — скінченний код.

(a) Доведіть, що існує найменший підмоноїд M, який містить вільний моноїд X^* такий, що M є породженим кодом зі скінченною затримкою дешифрування.

(b) Нехай $Y \subset A^*$ — база підмоноїда, доведення якої сформульовано в (a). Доведіть по аналогії, як в твердженні 2.2.18, що

$$Y \subset X(Y^*)^{-1} \cap (Y^*)^{-1}X.$$

З цього виведіть, якщо код X не має скінченної затримки дешифрування, то

$$\mathrm{Card}(Y) \leqslant \mathrm{Card}(X) - 1.$$

В. 5.4.6. Доведіть, що код X має вербальну затримку дешифрування d тоді і лише тоді, коли код X^d має вербальну затримку дешифрування 1.

В. 5.4.7. Нехай $X \subset A^+$ — код. Доведіть, якщо обидві множини $E(X)$ сильно поповнювальних справа слів і $S(X)$ спрощувань (слів) є непорожніми, то вони збігаються.

В. 5.4.8. Нехай $X \subset A^+$ — код. Нехай $S(X)$ — множина спрощувань (слів) і $E(X)$ — множина сильно поповнювальних справа слів. Нехай $U = S(X) \setminus S(X)A^+$. *Строгим правим контекстом* слова $w \in A^*$ називається слово $v \in A^*$ таке, що існують $x_1, \dots, x_n \in X$ з $wv = x_1 x_2 \cdots x_n$ і v є власним суфіксом слова x_n. Множину строгих правих контекстів слова w позначатимемо через $C_r(w)$.

Доведіть, якщо $S(X) = E(X) \neq \varnothing$, то для всіх слів $w \in A^*$ виконуються такі твердження:

(1) множина $C_r(w)$ є префіксною;
(2) добуток $C_r(w)U$ є однозначним;
(3) якщо $w \in S(X)$, то добуток $C_r(w)U$ є максимальною префіксною множиною.

В. 5.4.9. Використайте вправи 5.4.7, 5.4.8 і 3.10.7 для доведення теореми 5.2.4.

В. 5.4.10. Доведіть, якщо X є тонким кодом із затримкою дешифрування d, то код Y, означений рівністю (5.2) є тонким.

(Підказка: Доведіть, якщо $p \in P$, $a \in A$, то $pa \notin P$. Потім послідовно доведіть, що множини S, R і S^* є тонкими.)

Підрозділ 5.3

В. 5.4.11. У цій вправі ми називаємо *правою затримкою* автомата, що називається просто затримкою в нашому тексті, і ми будемо називати *лівою затримкою* затримку оберненого автомата, тобто автомата, отриманого обертанням ребер даного автомата. Подібно, будемо говорити, що автомат є є *d-повним справа*, якщо він є d-повним, і *d-повним зліва*, якщо його обернений автомат є d-повним.

Будемо говорити, що автомат має *бізатримку* (d, d'), якщо він має ліву затримку d і праву затримку d'. Аналогічно казатимемо, що автомат є (d, d')-*повним*, якщо він є d-повним зліва та d'-повним справа. Ми вводимо нове поняття для роботи за автоматами зі скінченною бізатримкою.

Розширений автомат з бізатримкою (d, d') — це автомат на множині станів Q, де множина E ребер, крім звичайних ребер, включає *граничні ребра*. *Пряме* граничне ребро має початок $q \in Q$ та мітку $a \in A$, але не має кінця. *Обернене* граничне ребро має мітку $a \in A$ та кінець $q \in Q$, але не має початку. Ми розширюємо поняття шляху, допускаючи, що шлях, можливо, може починатися із оберненого граничного ребра та закінчуватися прямим граничним ребром. Позначатимемо через $F(p)$ множину ребер, які починаються в стані p і через $P(p)$ множину ребер, які закінчуються в стані p. Також, через $\lambda(e)$ позначатимемо мітку ребра e.

Кожен стан q розширеного автомата приєднав до нього пару (U_q, V_q), де U_q — множина слів довжини d і V_q — множина слів довжини d'. Подібно, кожне ребро e має таку пару $(U_e, V_e) \in A^d \times A^{d'}$. Для них виконуються такі *умови сумісності*:

(1) для кожного стану p сім'я множин $\lambda(e)V_e$ для $e \in F(p)$ утворює розбиття множини $V_p A$;
(2) для кожного стану p і кожного ребра $e \in F(p)$ виконується рівність $U_p = U_e$;

(3) для кожного стану q сім'я множин $U_e\lambda(e)$ для $e \in P(q)$ утворює розбиття множини AU_q;
(4) для кожного стану q і кожного ребра $e \in P(q)$ виконується рівність $V_q = V_e$.

Доведіть, що два наступні об'єкти збігаються:

(i) розширений автомат з бізатримкою (d, d') без граничних ребер;
(ii) (d, d')-повний автомат з бізатримкою (d, d') з множиною U_p (відп., V_p) рівній для кожного стану p множині всіх міток шляхів довжини d (відп., d'), які закінчуються в стані p (відп., починаються в стані p).

(Підказка: Доведіть індукцією по $k \geqslant 0$, що в розширеному автоматі з бізатримкою (d, d') без граничних ребер, для $0 \leqslant k \leqslant d' + 1$, множина міток шляхів довжини $\leqslant k$, які починаються в стані p є множиною префіксів множини V_pA довжини $\leqslant k$.)

В. 5.4.12. Означимо для стану p розширеного автомата некомутативний многочлен

$$\partial(p) = \underline{U_p}\,\underline{V_p}\,\underline{A} - \underline{A}\,\underline{U_p}\,\underline{V_p},$$

і для його ребра e многочлен

$$\partial(e) = \zeta U_e\lambda(e)V_e,$$

з

$$\zeta = \begin{cases} 1, & \text{якщо } e \text{ — пряме граничне ребро;} \\ -1, & \text{якщо } e \text{ — обернене граничне ребро;} \\ 0, & \text{в інших випадках.} \end{cases}$$

Доведіть, що

$$\sum_{p\in Q} \partial(p) = \sum_{e\in E} \partial(e).$$

Отримайте з цього, що сума $\partial(e)$ для всіх граничних ребер, що називається *балансом* автомата, належить до ґратки L, породженої многочленами $f_w = w\underline{A} - \underline{A}w$ для слова $w \in A^{d+d'}$.

В. 5.4.13. Доведіть, що нижче перелічені помічені графи задовольняють означення розширеного автомата.

1. Автомат $\mathcal{A}_0$ з множиною станів $Q = A^{d+d'}$, з $U_{uv} = u$ і $V_{uv} = v$ для $u \in A^d$, $v \in A^{d'}$. Множина ребер цього автомата є $A^{d+d'+1}$ з $U_{uav} = u$, $\lambda(uav) = a$ та $V_{uav} = v$. Більше того, $F(uv) = uvA$ і $P(uv) = Auv$.

2. Автомат $\mathcal{A}_{-x}$ утворюється з автомата $\mathcal{A}_0$ шляхом видалення єдиного стану x. Доведіть, що в автоматі $\mathcal{A}_{-x}$ виконується рівність

$$\sum_{e\in E} \partial(e) = -f_x.$$

3. Автомат $\mathcal{A}_x$ утворюється з автомата $\mathcal{A}_0$ шляхом видалення усіх ребер, крім інцидентних стану x[1]. Доведіть, що в автоматі $\mathcal{A}_x$ виконується рівність

$$\sum_{e\in E} \partial(e) = f_x.$$

[1]Інцидентність — поняття, що використовується тільки для ребра і вершини: якщо v_1, v_2 — вершини, а $e = (v_1, v_2)$ — ребро, що їх з'єднує, тоді вершина v_1 і ребро e *інцидентні*, вершина v_2 і ребро e також інцидентні. Дві вершини (або два ребра) інцидентними бути не можуть. Для позначення найближчих вершин (ребер) використовується поняття *суміжності*.

В. 5.4.14. Будемо говорити, що ребро e розширеного автомата є *простим*, якщо множини U_e та V_e мають лише один елемент. Доведіть, що додаванням скінченної кількості станів і ребер, кожен розширений автомат можна перетворити в такий, що всі граничні ребра нового автомата будуть простими.

В. 5.4.15. Доведіть, що кожен розширений автомат $\mathcal{A}$ можна вкласти в розширений автомат $\mathcal{B}$, який не має граничного ребра в розумінні, що кожне звичайне ребро автомата $\mathcal{A}$ є ребром автомата $\mathcal{B}$.

(Підказка: Спочатку припустіть, що всі граничні ребра є простими. Запишіть

$$\sum_{e\in E} \partial(e) = \sum b_x f_x,$$

де коефіцієнити b_x є цілими числами. Якщо $b_x > 0$, то додайте b_x копій автомата $\mathcal{A}_{-x}$, і якщо $b_x < 0$, то додайте $-b_x$ копій автомата $\mathcal{A}_x$. Отриманий розширений автомат є таким, що $\sum_{e\in E} \partial(e) = 0$. Нарешті з'єднайте кожне пряме граничне ребро e з оберненим граничним ребром e' так, щоб виконувалася рівність $\partial(e) + \partial(e') = 0$.)

В. 5.4.16. Метою цієї вправи є доведення того факту, що будь-який раціональний код із скінченною літерною затримкою в обох напрямках міститься в максимальному раціональному коді зі скінченною літерною затримкою.

Нехай $\mathcal{A} = (Q, 1, 1)$ — автомат з бізатримкою (d, d'). Ми використаємо ряд кроків щоб перетворити автомат $\mathcal{A}$ в автомат з тією ж самою бізатримкою і який був би (d, d')-повним. Доведіть, якщо $\mathcal{A}$ є автоматом з бізатримкою (d, d'), то спочатку можна визначити пари (U_q, V_q), а тоді додати граничні ребра для того, щоб отримати розширений автомат.

Зробіть з цього висновок, використавши вправу 5.4.15, що кожен код з літерною бізатримкою (d, d') можна вкласти в максимальний код з літерною бізатримкою (d, d').

В. 5.4.17. Розглянемо автомат з бізатримкою $(1, 1)$, зображений на рис. 5.18 ліворуч. Доведіть, що $(1, 1)$-повний автомат, побудований методом, викладеним у вправі 5.4.16, є саме таким, як автомат зображений на рис. 5.18 праворуч.

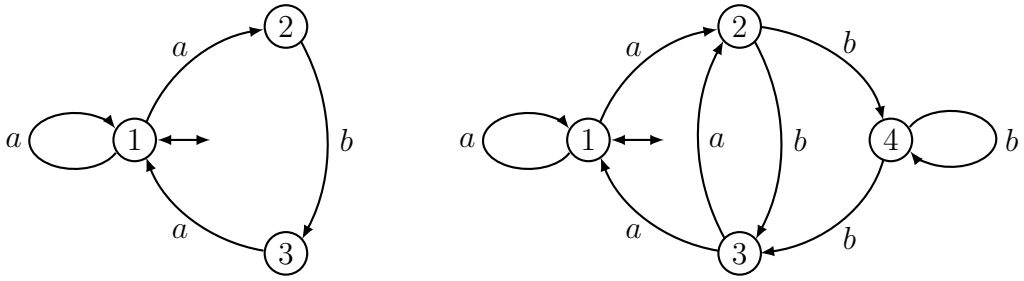


Рис. 5.18: Автомати з бізатримкою $(1, 1)$

Нотатки до розділу 5

Поняття затримки дешифрування появляється ще на самому початку розвитку теорії кодів в працях [76] і [6]. Теорема 5.2.4 пов'язана з працею Шютценбергера [187] і як гіпотеза вона була висловлена в [76]. Неповне доведення теореми 5.2.4 зустрічається в працях А. А. Маркова [9, 10, 149]. Доведення результату, більш загального за теорему 5.2.4, було опубліковано в праці Шютценбергера [187]. Викладене нами доведення теореми 5.2.4 належить Веронік Брюер (Véronique Bruyère) (див. [41] або частину 6 монографії [134]). Оригінальне доведення Шютценбергера теореми 5.2.4 викладено у вправі 5.4.9. Твердження 5.1.6 взято з праці [51].

Теорема 5.2.9 належить праці citeBruyere-Wang-Zhang-1990. Ми дотримувались доведень, викладених у цій праці, за винятком твердження 5.2.19.

Поняття автомата зі скінченною затримкою відоме в ранній теорії автоматів як *інформаційні машини без втрат скінченного порядку* (*information lossless machines of finite order*) (див. монографію Когаві [110–112]). Це поняття пов'язане з поняттям *відображення близкості справа* (*right closing map*) в символічній динаміці (див. [128]). Цей термін вперше був введений Кітченсом у його дисертації [106]. Теорема 5.3.7 належить праці [41].

Конструкція леми 5.3.8 взята зі статті [21]. Ми наслідували представлення конструкції леми 5.3.8 запропоноване Брюер та Летте в праці [42], і приклад 5.3.10 також взято з цієї статті.

Вправа 5.4.5 взята з праці [33]. Аналогічний результат доведено в монографії Саломаа [11, 174]. Вправа 5.4.6 взята з праці Ніва [154]. Вправа 5.4.7 взята з праці Шютценбергера [187]. Вправи 5.4.11–5.4.17 взяті зі статті [21], у якій вводиться поняття розширеного автомата і він називається *молекулою* (*molecule*). Ця назва "молекула" використовується метафорично та відноситься до можливості використовувати граничні ребра як обшивання.

Зазначимо наступний результат, про який тут не було повідомлено: *для трielементного коду* $X = \{x, y, z\}$ *існує щонайбільше одне нескінченне справа слово з двома різними* X*-факторизаціями* [102].

Розділ 6

Біфіксні коди

Завданням цього розділу є описання структури максимальних біфіксних кодів. Ця сім'я кодів має досить чудові властивості та їх можна описати досить задовільно та повно.

Як і в решті цієї книги, ми будемо працювати в межах сім'ї тонких кодів. Як ми побачимо, ця сім'я містить усі звичні приклади, і більшість основних властивостей поширюються на цю сім'ю, коли вони дотримуються у простому (тобто скінченому чи розпізнаваному) випадку.

Кожному тонкому максимальному біфікс-коду будуть прив'язані два основних параметри: його *степінь* та його *ядро*. Степінь — це натуральне число, яке є, як ми побачимо в розділі 9, степеню групи підстановки, пов'язаної з кодом. Ядро — це множинна кодових слів, які є власними множниками деяких кодових слів. Ми доведемо, що ці два параметри характеризують тонкий максимальний біфіксний код.

У першому підрозділі ми вводимо поняття *синтаксичного аналізу* чи *розкладу* (*parse*) слова щодо біфіксного коду. Це дозволяє нам визначити цілочисельну функцію, яку називають *індикатором* біфіксного коду. Ця функція буде досить корисною у цьому та наступних розділах.

У другому підрозділі ми даємо ряд еквівалентних умов того, щоб тонкий код був максимальним біфіксним. Те, що тонкі максимальні біфіксні коди є крайніми об'єктами, відображається в спостереженні, що підмножина їх властивостей є достатньою для їх повної характеризації. Ми також даємо перетворення (яке називається *внутрішнім перетворенням*), яке зберігає сім'ю максимальних біфіксних кодів.

Підрозділ 6.3 містить означення степеня тонкого максимального біфіксного коду. Він визначається як кількість *інтерпретацій* слова, яка не є множником кодового слова. Це число не залежить від обраного слова. Цей факт буде використаний для доведення більшості основних властивостей біфіксних кодів. Доведемо, що степінь є інваріантною при внутрішньому перетворенні.

У четвертому підрозділі буде описана побудова тонкого максимального біфіксного коду, що має задані степінь і ядро. Ми також описуємо похідний код тонкого максимального біфіксного коду. Це код, степінь якого на одиницю менша за ступінь вихідного коду. Обидві конструкції є наслідком фундаментального результату (теорема 6.4.3), який характеризує такі множини слів, які можна поповнити в скінченному максимальному біфіксному коді без зміни ядра.

Підрозділ 6.5 присвячений вивченню скінченних максимальних біфіксних кодів.

Доведено, що для фіксованого степеня та фіксованого розміру алфавіту існує лише обмежена кількість таких кодів. Далі доведено, що на цій скінченній множині внутрішнє перетворення діє транзитивно.

В останньому підрозділі ми доведемо, що будь-який раціональний біфіксний код міститься в максимальному раціональному біфіксному коді (теорема 6.6.1).

6.1 Основні властивості

Біфіксним кодом називається підмножина X вільної напівгрупа A^+, яка є одночасно префіксною та суфіксною. Іншими словами, виконуються умови

$$XA^+ \cap X = \varnothing \qquad \text{і} \qquad A^+X \cap X = \varnothing. \tag{6.1}$$

Приклад 6.1.1. Кожен код X утворений зі слів одинакової довжини є біфіксним.

Приклад 6.1.2. Нехай A — алфавіт, що містить дві різні літери a, b. Довільна множина $X = \{a\} \cup bYb$ з $Y \subseteq (A \setminus \{b\})^*$ є біфіксним кодом.

Приклад 6.1.3. Якщо X та Y — біфіксні коди, то їх добуток XY є біфіксним кодом.

Приклад 6.1.4. Нехай $A = \{a, b\}$. При огляді множина

$$X = \left\{a^3, a^2ba, a^2b^2, ab, ba^2, baba, bab^2, b^2a, b^3\right\}$$

видається біфіксним кодом. Він появиться в декількох місцях пізніше.

Використання біфіксних кодів для передачі інформації пов'язане з можливістю обмеження наслідків помилок, що виникають при передачі, за допомогою схеми двобічного декодування. Припустимо, що ми використовуємо бінарний біфіксний код для передачі даних. Припустимо також, що для передачі повідомлення групуються у блоки з N символів джерела, кодованих як N кодових слів.

Припустимо також, що в блоці $x_1 \cdots x_N$ з N кодових слів сталася помилка під час передачі, що унеможливлює розшифрування слова x_i (див. рис. 6.1). Блок $x_1 \cdots x_N$

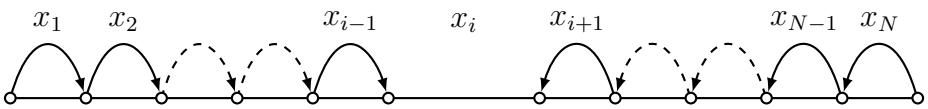


Рис. 6.1: Декодування блоку N кодових слів: слово $x_1 \cdots x_{i-1}$ правильно розшифровується зліва направо, слово $x_{i+1} \cdots x_N$ правильно розшифровується справа наліво. Помилка розташована в слові x_i.

спочатку розкодовується з використанням звичайної зліва направо послідовності розшифрувань і кодових слів з x_1 до x_{i-1} і він є правильно розшифрованим. Однак, декодувати слово x_i неможливо. Потім запускається новий процес декодування, цього разу справа наліво. Якщо відбулася максимум одна помилка, то знову кодові слова від x_N до x_{i+1} дешифруються правильно. Таким чином, у блоці з N закодованих

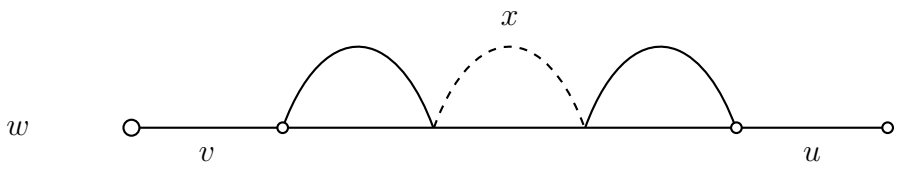


Рис. 6.2: X-розклад (v, x, u) слова w

вихідних символів буде ідентифіковано неправильне кодове слово. Ці коди використовуються для передачі зображень, див. приклади 6.2.5 та 6.2.6.

Нехай X — підмножина вільної напівгрупи A^+. *X-розкладом* (або просто *розкладом*) слова $w \in A^*$ називається трійка (v, x, u) (див. рис. 6.2). така, що $w = vxu$ і

$$v \in A^* \setminus A^*X, \qquad x \in X^* \qquad \text{і} \qquad u \in A^* \setminus XA^*.$$

Інтепретацією слова $w \in A^*$ називається трійка (v, x, u) така, що $w = vxu$ і

$$v \in A^{-}X, \qquad x \in X^* \qquad \text{і} \qquad u \in XA^{-}.$$

Якщо X — біфіксний код, то

$$A^{-}X \subseteq A^* \setminus A^*X \qquad \text{і} \qquad XA^{-} \subseteq A^* \setminus XA^*,$$

а отже кожна інтерпретація слова w є також розкладом слова w.

Точкою в слові $w \in A^*$ називається пара $(r, s) \in A^* \times A^*$ така, що $w = rs$. Слово w таким чином, має $|w| + 1$ точок. Будемо говорити, що розбір (v, x, u) слова w проходить через точку (r, s), якщо $x = yz$ для деяких слів $y, z \in X^*$ таких, що

$$r = vy \qquad \text{і} s = zu$$

(див. рис. 6.3).

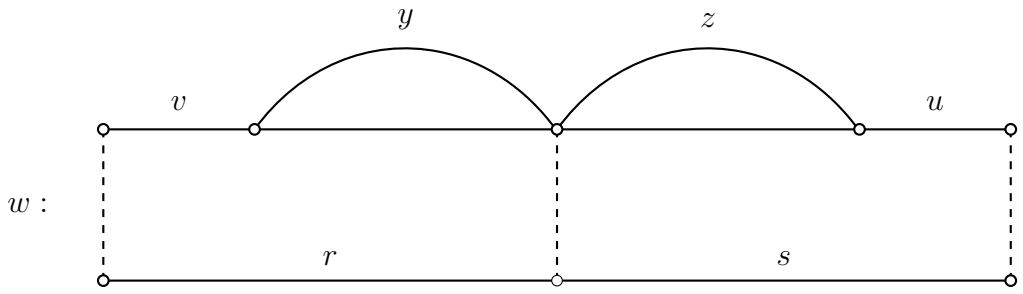


Рис. 6.3: Розклад слова w, яке проходить через точку (r, s)

Твердження 6.1.5. *Нехай $X \subset A^+$ — біфіксний код. Для кожної точки слова $w \in A^*$ існує один і лише один розклад, що проходить через цю точку.*

Доведення. Нехай (r, s) — точка слова $w \in A^*$. Позаяк код X є префіксним, то за твердженням 3.1.6 існує єдине слово $z \in X^*$ і єдине слово $u \in A^* \setminus XA^*$ такі, що $s = zu$. Аналогічно, оскільки код X є суфіксним, то $r = vy$ для єдиного слова $v \in A^* \subseteq A^*X$ і єдиного слова $y \in X^*$. Очевидно, що (v, yz, u) є розкладом слова w, який проходить через точку (r, s). Єдиність цього розкладу випливає з єдиності факторизації слів s і r. □

Твердження 6.1.6. *Нехай $X \subset A^+$ — біфіксний код. Тоді для кожного слова $w \in A^*$, існують бієкції між такими множинами:*

(*i*) *множина розкладів слова w;*
(*ii*) *множина префіксів слова w, які не мають суфіксів у коді X;*
(*iii*) *множина суфіксів слова w, які не мають префіксів у коді X.*

Доведення. Покладемо $V = A^* \setminus A^*X$ і $U = A^* \setminus XA^*$. Для кожного розкладу (v, x, u) слова w слово v міститься в множині V і воно є префіксом слова w. Таким чином слово v є елементом множини префіксів слова w, які не мають суфіксів у коді X. Навпаки, якщо $w = vw'$ і $v \in V$, покладемо $w' = xu$ з $x \in X^*$ і $u \in U$, а це є можливим, оскільки код X є префіксним. Тоді трійка (v, x, u) є розкладом. З единосты факторизації $w' = xu$ випливає, що відображення $(v, x, u) \mapsto v$ є бієктивним з множини розкладів слова w на множину префіксів слова w, які не мають суфіксів у коді X.

Побудова бієкції між множинами (*i*) та (*iii*) є аналогічною. □

Нехай X — підмножина вільної напівгрупи A^+. *Індикатором* або *характеристичною функцією* множини X називається формальний ряд L_X (або просто L), який ставить кожному слову w кількість (L, w) X-розкладів слова w. Поклавши

$$U = A^* \setminus XA^* \qquad \text{і} \qquad V = A^* \setminus A^*X,$$

отримуємо

$$L = \underline{V}\ \underline{X}^*\underline{U}. \tag{6.2}$$

Нехай X — біфіксний код. Тоді маємо $\underline{X}\ \underline{A}^* = \underline{XA}^*$, оскільки множина X є префіксною, і $\underline{A}^*\underline{X} = \underline{A^*X}$ оскільки множина X є суфіксною. Отож, маємо, що

$$\underline{U} = \underline{A}^* - \underline{X}\ \underline{A}^* = (1 - \underline{X})\underline{A}^* \qquad \text{і} \qquad \underline{V} = \underline{A}^*(1 - \underline{X}).$$

Підставивши останні дві рівності у (6.2), отримуємо

$$L = \underline{A}^*(1 - \underline{X})\underline{A}^*. \tag{6.3}$$

Цю рівність також можна записати так

$$L = \underline{V}\ \underline{A}^* = \underline{A}^*\underline{U}. \tag{6.4}$$

Зауважимо, що остання рівність є алгебраїчним формулюванням твердження 6.1.6.

З формули (6.3) отримуємо зручний вираз для кількості розкладів слова $w \in A^*$:

$$(L, w) = |w| + 1 - (\underline{A}^*\underline{X}\ \underline{A}^*, w). \tag{6.5}$$

Член $(\underline{A^*}\,\underline{X}\,\underline{A^*}, w)$ дорівнює кількості входжень слів з множини X, як множників слова w. Таким чином, з формули (6.5) ми бачимо, що для будь-яких біфіксних кодів X і Y виконується така імплікація:

$$Y \subseteq X \qquad \Longrightarrow \qquad L_X \leqslant L_Y. \tag{6.6}$$

Нагадаємо, що позначення $L_X \leqslant L_Y$ означає, що $(L_X, w) \leqslant (L_Y, w)$ для всіх слів w вільного моноїда A^*.

Твердження 6.1.7. *Нехай $X \subset A^+$ — біфіксний код, $U = A^* \setminus XA^*$, $V = A^* \setminus A^*X$ і L — індикатор коду X. Тоді*

$$\underline{V} = \underline{L}(1 - \underline{A}), \qquad \underline{U} = (1 - \underline{A})\underline{L}, \tag{6.7}$$

$$1 - \underline{X} = (1 - \underline{A})\underline{L}(1 - \underline{A}). \tag{6.8}$$

Доведення. Формула (6.7) випливає з формули (6.4), а (6.8) є безпосереднім наслідком формули (6.3). □

Твердження 6.1.8. *Нехай $X \subset A^+$ — біфіксний код і L — індикатор коду X. Тоді*

$$1 \leqslant (L, w) \leqslant |w| + 1, \tag{6.9}$$

для всіх слів $w \in A^*$. Зокрема, $(L, \varepsilon) = 1$. Далі, для всіх слів $u, v, w \in A^*$ виконується нерівність

$$(L, v) \leqslant (L, uvw). \tag{6.10}$$

Доведення. Для даного слова w існує не більше ніж $|w| + 1$ і щонайменше один (а саме порожнє слово) префікс слова w, що не має суфікса в коді X. Таким чином, формула (6.9) є наслідком твердження 6.1.6.

Далі, кожен розклад слова u можна продовжити до розкладу слова uvw. Цей розклад слова uvw однозначно визначається розкладом слова v (твердження 6.1.5). Звідси випливає формула (6.10). □

Приклад 6.1.9. Індикатор L біфіксного коду $X = \varnothing$ задовольняє умову

$$(L, w) = |w| + 1,$$

для всіх слів $w \in A^*$.

Приклад 6.1.10. Для біфіксного коду $X = A$, індикатор набуває значення

$$(L, w) = 1,$$

для всіх слів $w \in A^*$.

Наступне твердження дає описання формальних степеневих рядів, які є індикаторами.

Твердження 6.1.11. *Формальний степеневий ряд $L \in \mathbb{Z}\langle\langle A\rangle\rangle$ є індикатором біфіксного коду тоді і тільки тоді, коли він задовольняє такі умови:*

(*i*) *для довільних літери* $a \in A$ *та слова* $w \in A^*$ *виконуються нерівності*

$$0 \leqslant (L, aw) - (L, w) \leqslant 1, \tag{6.11}$$

$$0 \leqslant (L, wa) - (L, w) \leqslant 1; \tag{6.12}$$

(*ii*) *для довільних літер* $a, b \in A$ *та слова* $w \in A^*$ *виконуються нерівності*

$$(L, aw) + (L, wb) \geqslant (L, w) + (L, awb); \tag{6.13}$$

(*iii*) $(L, \varepsilon) = 1$.

Доведення. Припустимо, що L — індикатор деякого біфіксного коду X. З формули (6.7) випливає, що коефіцієнти рядів $L(1 - \underline{A})$ і $(1 - \underline{A})L$ дорівнюють 0 або 1. Для слова $w \in A^*$ та літери $a \in A$ маємо, що

$$(L(1 - \underline{A}), aw) = (L, aw) - (L, w) \quad \text{і} \quad (L(1 - \underline{A}), wa) = (L, wa) - (L, w).$$

Таким чином, виконується нерівності (6.11) і (6.12). Нарешті, з формули (6.8) випливає, що $(L, \varepsilon) = 1$ для порожнього слова ε, а також для довільних літер $a, b \in A$ та слова $w \in A^*$ з рівності

$$-(X, awb) = (L, awb) - (L, aw) - (L, wb) + (L, w)$$

випливає нерівність (6.13).

Навпаки, припустимо, що формальний степеневий ряд L задовольняє умови (*i*), (*ii*) та (*iii*). Покладемо $S = (1 - \underline{A})L$. Тоді

$$(S, 1) = (L, 1) = 1.$$

Далі, для довільних літери $a \in A$ та слова $w \in A^*$ маємо, що

$$(S, aw) = (L, aw) - (L, w).$$

З нерівності (6.11) випливає, що

$$0 \leqslant (S, aw) \leqslant 1,$$

а це доводить, що S є характеристичним рядом деякої множини U, яка містить порожнє слово ε. Далі, якщо $a, b \in A$ та $w \in A^*$, то за нерівністю (6.13) отримуємо, що

$$(S, aw) = (L, aw) - (L, w) \geqslant (L, awb) - (L, wb) = (S, awb).$$

Таким чином, з умови $awb \in U$ випливає, що $aw \in U$, а це показує, що множина U префіксно замкненою.

За твердженням 3.1.6 множина $X = UA \setminus U$ є префіксним кодом і

$$1 - \underline{X} = \underline{U}(1 - \underline{A}).$$

Симетрично отримуємо, що формальний ряд $T = L(1 - \underline{A})$ є характеристичним рядом деякої непорожньої суфіксно замкненої множини V, множина $Y = AV - V$ є суфіксним кодом і

$$1 - \underline{Y} = (1 - \underline{A})\underline{V}.$$

На завершенні отримуємо, що

$$1 - \underline{X} = \underline{U}(1 - \underline{A}) = (1 - \underline{A})L(1 - \underline{A}) = (1 - \underline{A})\underline{V} = 1 - \underline{Y}.$$

Отож, $X = Y$ і X є біфіксним кодом з індикатором L. □

Формулювання наступного твердження використовується для обчислення індикатора біфіксного коду.

Твердження 6.1.12. *Нехай $X \subset A^+$ — біфіксний код і L — індикатор коду X. Тоді*

$$(L, ua) = \begin{cases} (L, u), & \text{якщо } ua \in A^*X; \\ (L, u) + 1, & \text{в іншому випадку,} \end{cases} \tag{6.14}$$

для довільних літери $a \in A$ та слова $w \in A^*$.

Доведення. Формула (6.14) випливає з рівності (6.7). □

Приклад 6.1.13. Нехай $A = \{a, b\}$ та $X = \{a\}$. Тоді $L_X(w) = |w|_b + 1$. Справді, цей результат безпосередньо випливає з рівності (6.5). Також, цю рівність можна отримати з рівності (6.14): скануючи префікси в слові w зліва направо, індикатор залишається постійним кожного разу, коли зустрічається літера a.

Наступне твердження показує, як умову бути біфіксним кодом можна виразити на мові детермінованого автомата, що розпізнає вільний моноїд X^*.

Твердження 6.1.14. *Нехай X — префіксний код над алфавітом A й $\mathcal{A} = (Q, 1, 1)$ — обрізаний детермінований автомат, що розпізнає вільний моноїд X^*. Тоді код X є біфіксним тоді і лише тоді, коли для кожного стану $q \in Q$ і слова $w \in A^*$, з умови $q \cdot w = 1 \cdot w$ випливає рівність $q = 1$.*

Доведення. Припустимо спочатку, що припущення твердження виконуються. Ми доведемо, що моноїд X^* є унітарним зліва. Нехай u і v — слова такі, що $u, vu \in X^*$. Приймемо $q = 1 \cdot v$. Тоді

$$1 \cdot u = 1 \qquad \text{і} \qquad 1 \cdot vu = (1 \cdot v) \cdot u = 1.$$

Приймемо $q = 1 \cdot v$. Тоді $q \cdot u = 1$, і з припущення випливає рівність $q = 1$. Це доводить, що $1 \cdot v = 1$, а отже $v \in X^*$.

Припустимо навпаки, що моноїд X^* є унітарним зліва та нехай w — таке слово, що $1 \cdot w = q \cdot w$ для деякого стану $q \in Q$. Приймемо $p = q \cdot w$ і нехай u та v — такі слова, що $1 \cdot u = q$ і $p \cdot v = 1$. Тоді

$$1 \cdot uwv = 1 \cdot wv = 1,$$

а це доводить, що $uwv, wv \in X^*$. Оскільки моноїд X^* є унітарним зліва, то $u \in X^*$. Звідси в свою чергу випливає, що $q = 1$. □

Умови твердження 6.1.14 справджуються для автомата, який називається *біде-терміно́ваним* у тому сенсі, що для довільних ребер (p, a, q) і (r, a, s) з $p, q, r, s \in Q$ і $a \in A$ виконується властивість:

$$p = r \quad \text{тоді і тільки тоді, коли} \quad q = s.$$

6.2 Максимальні біфіксні коди

Біфіксний код $X \subset A^+$ називається *максимальним*, якщо для довільного біфіксного коду $Y \subset A^+$ з включення $X \subseteq Y$ випливає рівність $X = Y$. Як і в розділі 3 зручно зауважити, що множина $\{\varepsilon\}$ є максимально біфіксною, але не є кодом. Ми почнемо з того, що дамо ряд еквівалентних умов для того, щоб тонкий код був максимальним біфіксним.

Твердження 6.2.1. *Нехай X — тонка підмножина вільної напівгрупи A^+. Тоді такі умови є еквівалентними:*

(i) *X є максимальним кодом і є біфіксним;*
(ii) *X є максимальним біфіксним кодом;*
(iii) *X є максимальним префіксним кодом і є максимальним суфіксним кодом;*
(iv) *X є повним зліва префіксним кодом;*
(iv') *X є повним справа суфіксним кодом;*
(v) *X є повним зліва і повним справа кодом.*

Доведення. Імплікація $(i) \Rightarrow (ii)$ є очевидною.

$(ii) \Rightarrow (iii)$ Якщо X є максимальним префіксним кодом, то за теоремою 3.3.8 множина X є максимальним кодом, а отже X є максимальним суфіксним кодом. Аналогічно, якщо X є максимальним суфіксним кодом, то X є максимальним префіксним кодом. Отож, припустимо, що X не є ні максимальним ні максимальним суфіксним кодом. Нехай слова $y, z \notin X$ є такими, що множина $X \cup \{y\}$ є префіксною, а множина $X \cup \{z\}$ є суфіксною. Оскільки множина $X \cup \{yt\}$ є префіксною для довільного слова t, звідси випливає, що множина $X \cup \{yz\}$ є префіксною, а отже також є біфіксною. Більше того, $yz \notin X$, оскільки в протилежному випадку множина $X \cup \{y\}$ не буде префіксною. Це суперечить твердженню (ii).

Імплікації $(iii) \Rightarrow (iv)$ і $(iii) \Rightarrow (iv')$ є безпосередньо випливають з наслідку 3.3.4, який стверджує, що максимальний префіксний код є повним справа, та до нього дуального.

$(iv) \Rightarrow (v)$ Код X є повним і тонким. Таким чином, він є максимальним. Це доводить, що код X максимальним префіксним, а це, в свою чергу, означає, що він є повним. Доведення імплікації $(iv') \Rightarrow (v)$ є аналогічним.

$(v) \Rightarrow (i)$ Повний тонкий код є максимальним. За теоремою 3.3.8 повний справа тонкий код є префіксним. Аналогічно доводиться, що код X є суфіксним. □

Код, який є одночасно максимальним префіксним і максимальним суфіксним є завжди максимальним біфіксним кодом, і обернене твердження виконується, як ми побачимо далі, для тонких кодів. Однак для кодів, які не є тонкими, це твердження не виконується (див. приклад 6.2.4).

Приклад 6.2.2. Груповий код, який визначений у підрозділі 2.2, є біфіксним і є максимальним кодом.

Приклад 6.2.3. Нехай $A = \{a, b\}$ і

$$X = \left\{a^3, a^2ba, a^2b^2, ab, ba^2, baba, bab^2, b^2a, b^3\right\}.$$

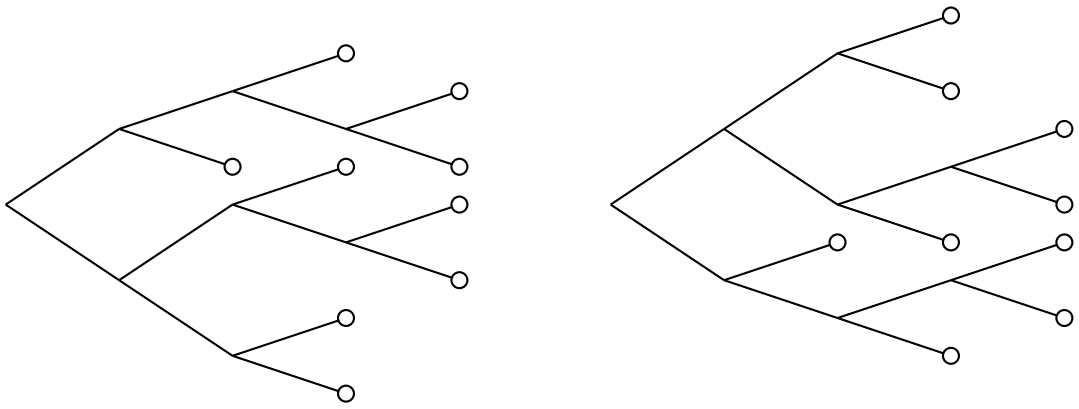


Рис. 6.4: Літерні зображення коду X (ліворуч) і його оберненого коду $\widetilde{X}$ (праворуч)

За перевіркою літерного зображення (див. рис. 6.4), X є, легко бачити, максимальним префіксним кодом.

Обернений код $\widetilde{X}$, зображений праворуч на рис. 6.4, також є максимальним префіксним. Отож, X є максимальним біфіксним кодом. Зауважимо, що код $\widetilde{X}$ збігається з множиною отриманою з коду X заміною літер a та b (відображення відносно горизонтальної осі). Це винятковий факт, який буде пояснено пізніше (див. приклад 6.5.3).

Приклад 6.2.4. Нехай $A = \{a, b\}$ і $X = \{wab^{|w|} : w \in A^*\}$ (див. приклади 2.4.12 і 3.3.9). Множина X є максимальним, щільним справа кодом, який є суфіксним, але не є префіксним. Множина $Y = X \setminus XA^+$ є максимальною префіксною і є суфіксною, але не є максимальною суфіксною, оскільки $Y \neq X$. Таким чином, код Y є також максимальним біфіксним, бо задовольняє умову (ii) твердження 6.2.1, але не задовольняє умову (iii).

Приклад 6.2.5. Існує оборотна версія кодів Ґоломба-Райса, описаних в прикладі 3.4.4. Ці коди є біфіксними, які мають однаковий розподіл довжин. Відмінність від кодів Ґоломба-Райса полягає в тому, що базове слово 1^i0 замінено на слово $10^{i-1}1$ для $i \geqslant 1$. Оскільки множина базових слів утворює код біфіксний код, то множина всіх кодових слів є також біфіксним кодом. *Оборотний код Ґоломба-Райса* порядку k, яких позначається RG_k, і визначається регулярним виразом

$$RG_k = (0 + 10^*1)(0 + 1)^k.$$

На рис. 6.5 зображено коди RG_k для $k = 0, 1, 2$.

Приклад 6.2.6. Існує також оборотна версія експоненціальних кодів Ґоломба (приклад 3.4.5), які є біфіксними кодами з однаковим розподілом довжин. Код REG_0 є біфіксним кодом

$$REG_0 = 0 + 1(00 + 10)^*(0 + 1)1,$$

і код порядку k є

$$REG_k = REG_0(0 + 1)^k.$$

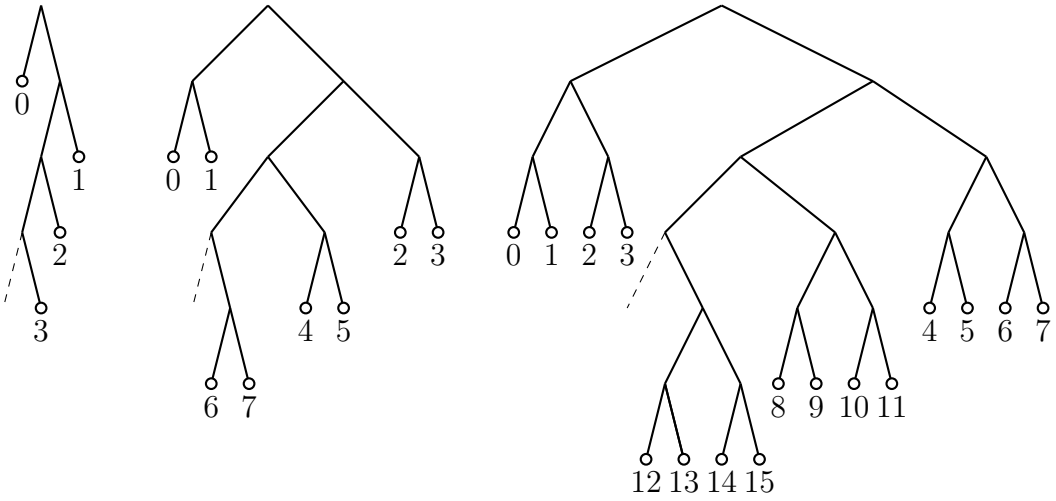


Рис. 6.5: Оборотні коди Ґоломба-Райса порядків $0, 1, 2$

Зауважимо, що код REG_0 дорівнює його оборотному, тобто $\widetilde{REG_0} = REG_0$. Це доводить, що код REG_0 є біфіксним. Інші коди є також біфіксними, оскільки вони є добутками двох біфіксних кодів. Коди REG_k зображено для $k = 0$ на рис. 6.6 і для

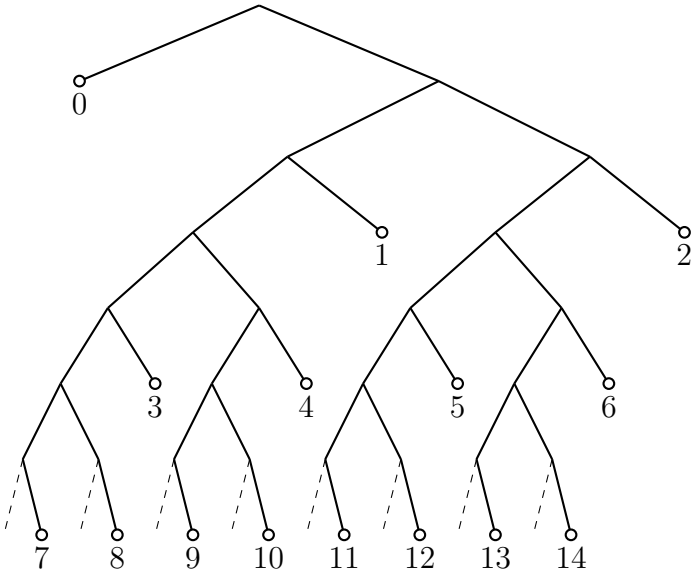


Рис. 6.6: Оборотний екпоненціальний код Ґоломба порядку 0

$k = 1$ на рис. 6.7, відповідно.

Наступне твердження дає різну характеристику максимальних біфіксних кодів всередині сім'ї тонких кодів.

Твердження 6.2.7. *Тонкий код X є максимальним біфіксним тоді і тільки тоді, коли для всіх слів $w \in A^*$ існує натуральне число n таке, що $w^n \in X^*$.*

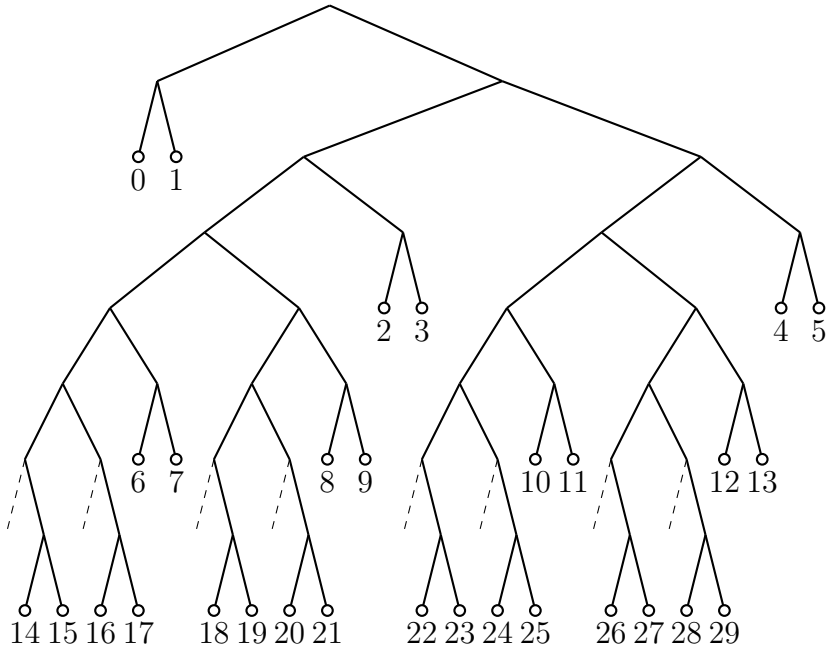


Рис. 6.7: Оборотний екпоненціальний код Ґоломба порядку 1

Доведення. Припустимо, що для всіх слів $w \in A^*$ існує натуральне число $n \geqslant 1$ таке, що $w^n \in X^*$. Тоді код X, очевидно, є повним справа та повним зліва. Отож, X є максимальним біфіксним кодом за твердженням 6.2.1.

Навпаки, нехай X — максимальний біфіксний код і $w \in A^*$. Розглянемо слово $u \in \overline{F}(X)$, що не є множником слова з коду X. Оскільки код X є повним справа, то для всіх натуральних $i \geqslant 1$ існує слово v_i таке, що

$$w^i u v_i \in X^*.$$

Позаяк $u \in \overline{F}(X)$, то існує префікс s_i слова u такий, що $w^i s_i \in X^*$.

Нехай k, m з $k < m$ — натуральні числа такі, що $s_k = s_m$. Прийнявши $n = m - k$, маємо, що

$$w^k s_k \in X^* \qquad \text{і} \qquad w^m s_m = w^n w^k s_k \in X^*.$$

Оскільки моноїд X^* є унітарним зліва, то звідси випливає, що $w^n \in X^*$. □

Тепер ми опишемо операцію, яка дає можливість побудувати максимальні біфіксні коди шляхом послідовних перетворень.

Твердження 6.2.8. *Нехай X — код, який є максимальним префіксним і максимальним суфіксним, і нехай $w \in A^*$. Позначимо*

$$\begin{aligned} G &= Xw^{-1}, & D &= w^{-1}X, \\ G_0 &= (wD)w^{-1}, & D_0 &= w^{-1}(Gw), \\ G_1 &= G \setminus G_0, & D_1 &= D \setminus D_0. \end{aligned} \tag{6.15}$$

Якщо $G_1 \neq \varnothing$ *і* $D_1 \neq \varnothing$, *то множина*

$$Y = (X \cup w \cup G_1(wD_0^*)D_1) \setminus (Gw \cup wD) \tag{6.16}$$

є максимальним префіксним і максимальним суфіксним кодом. Більше того,

$$\underline{Y} = \underline{X} + (1 - \underline{G})\, w \left(1 - \underline{D_0}^* \underline{D_1}\right). \tag{6.17}$$

Доведення. За означенням, Gw є множиною слів у коді X, які закінчуються словом w. Аналогічно, wD є множиною слів у коді X, які починаються словом w. Далі, G_0w є множиною слів в коді X, які починаються та закінчуються словом w. Отож, G_1w є множиною слів у коді X, які закінчуються словом w і не починаються зі слова w.

Позаяк $D_1 \neq \varnothing$, то множина D є непорожньою. Далі $\varepsilon \notin D$, оскільки в протилежному випадку маємо $w \in X$, і врахувавши, що код X є біфіксним, то отримуємо, що $G = D = \{\varnothing\}$, а отже $D_0 = \{\varnothing\}$ і на завершенні маємо $D_1 = \varnothing$, протиріччя. Таким чином, слово w є власним префіксом слова з коду X, і за твердженням 3.4.9, множини D і

$$Y_1 = (X \cup w) \setminus wD$$

є максимальними префіксними кодами.

Далі,

$$Gw = X \cap A^*w \qquad \text{і} \qquad wD = X \cap wA^*.$$

Також,

$$G_0w = wD \cap A^*w = X \cap wA^* \cap A^*w.$$

Аналогічно отримуємо, що

$$wD_0 = Gw \cap wA^* = X \cap wA^* \cap A^*w.$$

Таким чином,

$$wA^* \cap A^*w \cap X = Gw \cap wD = wD_0 = G_0w. \tag{6.18}$$

Тепер зауважимо, що $G = G_0 \cup G_1$. Звідси та з (6.18) отримуємо, що

$$Gw \cup wD = G_0w \cup G_1w \cup wD = wD_0 \cup G_1w \cup wD = G_1w \cup wD,$$

оскільки $D_0 \subseteq D$. Аналогічно доводиться рівність

$$Gw \cup wD = Gw \cup wD_1.$$

Таким чином, отримуємо, що

$$Y = (Y_1 \cup G_1wD_0^*D_1) \setminus G_1w.$$

Зауважимо, що $G_1w \subset Y_1$, оскільки G_1w є множиною слів в коді X, які закінчуються словом w і не починаються словом w, а отже $G_1w \subset X \setminus wD$. Оскільки множина $D = D_1 \cup D_0$ є максимальним префіксним кодом і $D_1 \neq \varnothing$, то за твердженням 3.4.12 множина $D_0^*D_1$ є максимальним префіксним кодом. Звідси та з того факту, що Y_1 є максимальним префіксним кодом з наслідку 3.4.7 випливає, що множина Y є максимальним префіксним кодом.

Симетрично можна послідовно довести, що

$$Y_2 = (X \cup w) \setminus wG \qquad \text{і} \qquad Y' = (Y_2 \setminus wD_1) \cup G_1 G_0^* w D_1$$

є максимальними суфіксними кодами. З рівностей (6.18) отримуємо за індукцією, що

$$G_0^* w = w D_0^*.$$

Таким чином, $Y' = Y$, а отже множина Y також є максимальним суфіксним кодом.

Для доведення рівності (6.17) покладемо

$$\sigma = \underline{X} + (1 - \underline{G})\, w \left(1 - \underline{D_0}^* \underline{D_1}\right).$$

Тоді

$$\begin{aligned} \sigma &= \underline{X} + w - \underline{G}w - w\underline{D_0}^* D_1 + \underline{G}w\underline{D_0}^* \underline{D_1} = \\ &= \underline{X} + w - \underline{G}w - w\underline{D_0}^* \underline{D_1} + \underline{G_0}w\underline{D_0}^* \underline{D_1} + \underline{G_1}w\underline{D_0}^* \underline{D_1}. \end{aligned}$$

Оскільки $\underline{G_0}w = w\underline{D_0}$, то отримуємо

$$\begin{aligned} \sigma &= \underline{X} + w - \underline{G}w - w\underline{D_0}^* \underline{D_1} + w\underline{D_0 D_0}^* \underline{D_1} + \underline{G_1}w\underline{D_0}^* \underline{D_1} = \\ &= \underline{X} + w - \underline{G}w - w\underline{D_1} + \underline{G_1}w\underline{D_0}^* \underline{D_1}. \end{aligned}$$

Множини $G_1 w$, D_0 і D_1 є префіксними, а також $D_0 \neq \varnothing$, оскільки в протилежному випадку $w \in X$. Отож, добутки у вище викладених виразах є однозначними. Далі з рівностей (6.18) випливає, що $G_1 w \cap wD = \varnothing$. Звідси випливає рівність

$$\underline{Gw \cup wD} = \underline{G_1}w + w\underline{D}.$$

Таким чином, отримуємо, що

$$\sigma = \underline{X} + w + \underline{G_1 w D_0^* D_1} - \underline{Gw \cup wD} = Y,$$

оскільки $Gw \cup wD \subset X$. □

У цьому випадку кажуть, що код Y отримується з коду X *внутрішніми перетвореннями* (стосовно слова w).

Приклад 6.2.9. Нехай $A = \{a, b\}$ і розглянемо однорідний код $X = A^2$. Нехай $w = a$. Тоді $G = D = A$ і $G_0 = D_0 = \{a\}$. Отже, код Y, визначений Формулою (6.16), є

$$Y = \{a\} \cup ba^*b.$$

Зауважимо, що Y є груповим кодом, як і код X.

Легко бачити, що з формули (6.16) випливає, що для скінченного коду X код Y є скінченним тоді і тільки тоді, коли $D_0 = \varnothing$. Цей випадок заслуговує на особливу увагу.

Твердження 6.2.10. *Нехай X — скінченний максимальний біфіксний код і $w \in A^*$. Покладемо*

$$G = Xw^{-1}, \qquad D = w^{-1}X. \tag{6.19}$$

Якщо $G \neq \varnothing$, $D \neq \varnothing$ і $Gw \cap wD = \varnothing$, то множина

$$Y = (X \cup w \cup GwD) \setminus (Gw \cup wD) \tag{6.20}$$

є скінченним максимальним біфіксним кодом, і

$$\underline{Y} = \underline{X} + (\underline{G} - 1)\, w\, (\underline{D} - 1)\,. \tag{6.21}$$

Навпаки, нехай Y — скінченний максимальний біфіксний код. Нехай $w \in Y$ — слово таке, що існує максимальний префіксний код D і максимальний суфіксний код G такі, що $GwD \subseteq Y$. Тоді

$$X = (Y \setminus (w \cup GwD)) \cup (Gw \cup wD) \tag{6.22}$$

є скінченним максимальним біфіксним кодом, а також крім того виконуються рівності (6.19), (6.20) *і* (6.21).

Доведення. Якщо $Gw \cap wD = \varnothing$, то з формули (6.18) випливає, що в термінах твердження 6.2.8 виконується умова $G_0 = D_0 = \varnothing$. Тоді рівність (6.16) спрощується до рівності (6.20). Формула (6.21) безпосередньо випливає з формули (6.17).

Навпаки, спочатку доведемо, що множина X є максимальним префіксним кодом. Покладемо

$$Z = (Y \setminus w) \cup wD.$$

Оскільки Y є максимальним префіксним кодом за твердженням 6.2.1 та оскільки код D є максимальним префіксним і $w \in Y$, то з наслідку 3.4.8 випливає, що множина Z є максимальним префіксним кодом. Далі зауважимо, що

$$X = (Z \setminus GwD) \cup Gw.$$

Множина Gw міститься в ZA^-, оскільки $Gw \subset (Y \setminus w)A^-$. Далі ми доведемо, що множина Gw є префіксною. Справді припустимо, що $gw = g'wt$ для деяких $g, g' \in G$, $t \in A^*$. Нехай d — слово в множині D максимальної довжини. Оскільки множина D є максимальною префіксною, то або слово td є власним префіксом слова в D, або слово td має префікс у множині D. Перший випадок виключається тим, що слово d має максимальну довжину. Таким чином, слово td має префікс, скажемо d' в множині D. Слово $g'wd'$ є префіксом слова $g'wtd = gwd$. Оскільки обидва є в префіксній множині Y, то вони збігаються. Отож, $d' = td$ і оскільки слово d має максимальну довжину, то отримуємо $t = \varepsilon$. Це завершує доведення нашого випадку.

Далі, для всіх $g \in G$, маємо $D = (gw)^{-1}Z$. Справді, з включення $gwD \subset Z$ випливає, що $D \subset (gw)^{-1}Z$, і позаяк D є максимальним префіксним кодом, то виконується рівність $D = (gw)^{-1}Z$.

З огляду на твердження 3.4.10 множина X є максимальним префіксним кодом. Симетрично доводиться, що X максимальним суфіксним кодом. Оскільки код X є скінченним, то він є максимальним біфіксним кодом.

Залишилося довести, що код Y отримується з коду X внутрішнім перетворенням. По-перше, включення $Gw \subset X$ випливає з рівності (6.22), маючи на увазі, що $G \subset Xw^{-1}$, а оскільки G є максимальним суфіксним кодом, то виконується рівність

$$G = Xw^{-1}.$$

Симетрично $D = w^{-1}X$. Більше того, $G \neq \varnothing$ і $D \neq \varnothing$, оскільки вони є максимальними кодами. Ми доведемо, шо

$$Gw \cap wD = \varnothing.$$

Якщо $gw = wd$ для деяких $g \in G$, $d \in D$, то $ggw = gwd \in GwD \subset Y$. Отож, отримуємо, що $w, ggw \in Y$, що є неможливим, оскільки код Y є суфіксним.

З $w \in Y$ отримуємо, що $Gw \cap Y = \varnothing$, бо в протилежному випадку код Y не був би суфіксним. Подібно отримуємо, що $wD \cap Y = \varnothing$, оскільки код Y є префіксним. Тоді, як результат формули (6.22) рівність

$$X \setminus (Gw \cup wD) = Y \setminus (w \cup GwD)$$

випливає з (6.20). □

Приклад 6.2.11. Нехай $A = \{a, b\}$ і $X = A^3$. Розглянемо слово $w = ab$. Тоді $G = D = A$ і $Gw \cap wD = \varnothing$. Отже твердження 6.2.10 дає скінченний код Y. Цей код отримується шляхом опускання на рис. 6.8 пунктирних ліній та приєднанням до

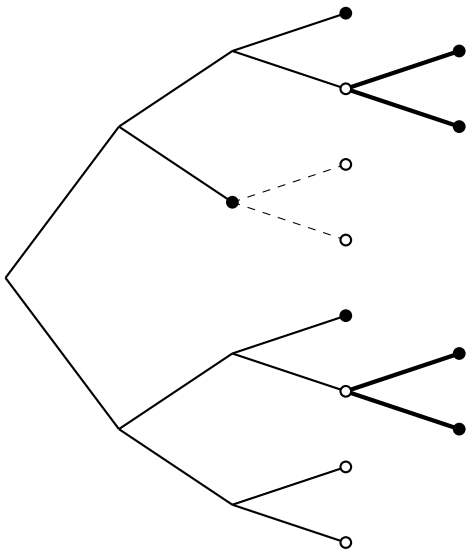


Рис. 6.8: Внутрішнє перетворення

жирних ліній.

6.3 Степінь

В цьому підрозділі, ми вивчаємо індикатор тонкого максимального біфіксного коду. Для таких біфіксних кодів відбуваються деякі спрощення.

Нехай $X \subset A^+$ — біфіксний код,

$$U = A^* \setminus XA^* \qquad \text{і} \qquad V = A^* \setminus A^*X,$$

і нехай $L = \underline{V}\ \underline{X}^*\underline{U}$ — індикатор коду X. Якщо X — максимальний префіксний код, то $U = P$, де $P = XA^-$ — множина власних префіксів слів у коді X. Подібним чином, для максимального суфіксного коду, ми маємо $V = S$, де $S = A^-X$ — множина власних суфіксів слів у коді X. Звідси випливає, якщо код X є максимальним префіксним і максимальним суфіксним, то кожен розклад слова є інтерпретацією. Тоді маємо, що

$$L = \underline{S}\ \underline{X}^*\underline{P} = \underline{S}\ \underline{A}^* = \underline{A}^*\underline{P}. \tag{6.23}$$

Ця основна формула використовується часто. Це означає, що кількість розкладів слова дорівнює кількості його суфіксів, які містяться в множині P, або еквівалентно, кількості його префіксів, які містяться в множині S. Нехай X є підмножиною відьної напівгрупи A^+. Позначимо через

$$H(X) = A^-XA^- = \left\{w \in A^* \colon A^+wA^+ \cap X \neq \varnothing\right\}$$

множину *внутрішніх множників слів* у коді X. Нехай

$$\overline{H}(X) = A^* \setminus H(X).$$

Очевидно, що кожен внутрішній множник є множником слова в коді X. Обернене твердження може бути хибним. Множина $H(X)$ і множина

$$F(X) = \{w \in A^* \colon A^*wA^* \cap X \neq \varnothing\}$$

множників слів в коді X співвідносяться так:

$$F(X) = H(X) \cup XA^- \cup A^-X \cup X,$$

і для $\overline{F}(X) = A^* \setminus F(X)$ маємо, що

$$A^+\overline{H}(X)A^+ \subset \overline{F}(X) \subset \overline{H}(X).$$

Вище викладені співвідношення доводять, що множина $\overline{H}(X)$ є непорожньою тодіі тільки тоді, коли множина $\overline{F}(X)$ є непорожньою, а отже код X є тонким тоді і лише тоді, коли $\overline{H}(X) \neq \varnothing$.

Теорема 6.3.1. *Нехай $X \subset A^+$ — біфіксний код. Тоді X є тонким максимальним кодом тоді і тільки тоді, коли його індикатор L є обмеженим. У цьому випадку*

$$\overline{H}(X) = \{w \in A^* \colon (L, w) = d\}, \tag{6.24}$$

де $d = \max\{(L, w) \colon w \in A^*\}$.

Доведення. Нехай X — тонкий максимальний біфіксний код. Нехай $w \in \overline{H}(X)$ і $w' \in A^*$. За формулою (6.23) маємо $(L, ww') = (\underline{S}\ \underline{A}^*, ww')$. Таким чином, кількість розкладів слова ww' дорівнює кількості префіксів слова ww', яке є елементом множини $S = A^-X$. Оскільки $w \in \overline{H}(X)$, то не існує префіксів у множині S, що є строго довшими за слово w. Таким чином, усі ці префікси є префіксами слова w. Знову, використавши формулу (6.23), це доводить, що $(L, ww') = (L, w)$. Тепер за твердженням 6.1.8 маємо, що $(L, ww') \geqslant (L, w')$. Таким чином, отримуємо

$$(L, w') \leqslant (L, w),$$

Звідки випливає, що індикатор L є обмеженим на A^* його значенням для слова в множині $\overline{H}(X)$. Це доводить також, що L сталою на множині $\overline{H}(X)$. Отож,

$$\overline{H}(X) = \{w \in A^* \colon (L, w) = d\}.$$

Для доведення оберненого включення, розглянемо внутрішній множник $w \in H(X)$. Тоді існують слова $p, s \in A^+$ такі, що $w' = pws \in X$. Звідси випливає, що

$$(L, w') \geqslant (L, w) + 1.$$

Справді, кожен розклад слова w можна продовжити в розклад слова w', і слово w' має додатковий розклад, а саме $(1, w', 1)$. Це доводить, що для внутрішнього множника w, число (L, w) є строго меншим за максимальне значення d. Таким чином, формула (6.24) доведена.

Навпаки, припустимо, що X є біфіксний код з обмеженим індикатором L, нехай

$$d = \max\{(L, w) \colon w \in A^*\}$$

і $v \in A^*$ — слово таке, що $(L, v) = d$. Ми використаємо формулу (6.3), яку перепишемо так

$$\underline{X}\ \underline{A}^* = \underline{A}^* + (\underline{A} - 1)L.$$

Нехай $w \in A^+$ — довільне непорожнє слово та покладемо $w = au$, з $a \in A$ й $u \in A^*$. Тоді

$$(\underline{X}\ \underline{A}^*, wv) = (\underline{A}^* + (\underline{A} - 1)L, auv) = 1 + (L, uv) - (L, auv).$$

За твердженням 6.1.8 обидва значення (L, uv) і (L, auv) є більші, або рівні значенню (L, v). За вибором слова v маємо, що $(L, uv) = (L, auv) = d$.

Таким чином, $(\underline{X}\ \underline{A}^*, wv) = 1$. Таким чином ми довели, що $wv \in XA^*$ для всіх слів $w \in A^+$. З цього випливає, що множина XA^* є щільною справа та код X є тонким. Справді, ми маємо $v \in \overline{H}(X)$, скільки для всіх $g, d \in A^+$ маємо $gv \in XA^*$, а отже $gvd \notin X$. Таким чином, X є тонким максимальним префіксним кодом. Симетрично доводиться, що код X максимальним суфіксним. Звідси та твердження 6.2.1 випливає обернена імплікація. □

Нехай X — тонкий максимальний біфіксний код і L — його індикатор. *Степеню* кода X, яку будемо позначати через $d(X)$ або просто d, називається число

$$d(X) = \max\{(L, w) \colon w \in A^*\}.$$

Згідно теореми 6.3.1 степінь d — це кількість розкладів будь-якого слова, яке не є внутрішнім множником кода X. Перш ніж продовжити, давайте проілюструємо поняття степеня декількома прикладами.

Приклад 6.3.2. Нехай φ — морфізм з вільного моноїда A^* на групу G, і нехай G' — підгрупа в G. Нехай X — груповий код, для якого $X^* = \varphi^{-1}(G')$. Ми бачимо, що X є максимальним біфіксним кодом, і, що код X є тонким тоді і тільки тоді, коли група G' має скінченний індекс в групі G (приклад 2.5.22).

Степінь коду X дорівнює індексу підгрупи G' в групі G. Справді, нехай $w \in \overline{H}(X)$ — слово, яке не є внутрішнім множником слова з коду X, і розглянемо відображення ψ, що ставить у відповідність кожному слову $u \in A^*$ єдине слово $p \in P = XA^-$ таке, що $uw \in X^*p$. Кожне слово p, яке отримується так, є суфіксом слова w. Множина $\psi(A^*)$ є множиною суфіксів слова w, які містяться в множині P. Оскільки $w \in \overline{H}(X)$, то маємо, що $\operatorname{Card}\psi(A^*) = d(X)$. Далі, маємо

$$\psi(u) = \psi(v) \qquad \Longleftrightarrow \qquad G'\varphi(u) = G'\varphi(v),$$

для $u, v \in A^*$. Справді, якщо $\psi(u) = \psi(v) = p$ то $uw, vw \in X^*p$, а отже отримуємо, що $\varphi(u), \varphi(v) \in G'\varphi(p)\varphi(w)^{-1}$. Навпаки, нехай $G'\varphi(u) = G'\varphi(v)$ і $r \in A^*$ — слово таке, що $uwr \in X^*$. Тоді $\varphi(vwr) \in G'\varphi(u)\varphi(wr) \subseteq G'$, звідки випливає, що $vwr \in X^*$. Оскільки $\psi(u)$ і $\psi(v)$ є суфіксами слова w, то одне зі слів $\psi(u)r$ і $\psi(v)r$ є суфіксом іншого. Позаяк X є суфіксним кодом, то звідси випливає, що $\psi(u) = \psi(v)$.

Це доводить, що індекс підгрупи G' у групі G дорівнює $d(X)$. За твердженням 1.13.1, $d(X)$ також дорівнює степені групи підстановок , яка відповідає дії групи G на суміжних класах підгрупи G', як це було визначено в підрозділі 1.13.

Приклад 6.3.3. Лише максимальний біфіксний код степені 1 над алфавітом A є $X = A$.

Приклад 6.3.4. Кожен максимальний біфіксний код степеня 2 над алфавітом A має вигляд

$$X = C \cup BC^*B, \tag{6.25}$$

де A є диз'юнктним об'єднанням множин B і C з $B \neq \varnothing$.

Справді, нехай $C = A \cap X$ і $B = A \setminus C$. Кожна літера $b \in B$ має два розклади, а саме $(\varepsilon, \varepsilon, b)$ і $(b, \varepsilon, \varepsilon)$. Таким чином, слово, яке є внутрішнім множником слова $x \in X$ не може містити літери з множини B, оскільки в протилежному випадку x мало б мати щонайменше три розклади. Отож, множина H внутрішніх множників коду X задовольняє включення $H \subseteq C^*$. Далі розглянемо слово $x \in X$. Тоді, або слово x є літерою, і тоді воно міститься в множині C, або в іншому випадку слово x має вигляд $x = aub$ для деяких літер $a, b \in A$ та слова $u \in H \subseteq C^*$. Позаяк код X є біфіксним, то жодна з літер a та b не є елементом множини C. Таким чином, отримуємо, що $X \subseteq C \cup BC^*B$. З максимальності коду X випливає рівність (6.25).

Це доводить, що кожен максимальний біфіксний код степеня 2 є груповим кодом. Справді, код визначений рівністю (6.25), отриманий розгляненим морфізмом з вільного моноїда A^* фактор-групу $\mathbb{Z}/2\mathbb{Z}$, означений за формулами $\varphi(B) = \{\overline{1}\}$ і $\varphi(C) = \{\overline{0}\}$. Це доводить також, що кожен максимальний біфіксний код степеня 2 є раціональним. Але це є хибним для максимального біфіксного коду степеня 3 (див. приклад 6.4.8).

Приклад 6.3.5. Розглянемо множину

$$Y = \{a^n b^n : n \in \mathbb{N}\}.$$

Вона є біфіксним кодом, який не є максимальним біфіксним, оскільки множна $Y \cup ba$ є біфіксним кодом. Також множина Y є тонкою, оскільки $ba \in \overline{F}(Y)$. Код Y не міститься в тонкому максимальному біфіксному коді. Справді, припустимо, що X є тонким максимальним біфіксним кодом степеня d, який містить код Y. Тоді для довільного цілого числа $n \geqslant 0$ слово a^n має $n+1$ розкладів, оскільки воно має $n+1$ суфіксів, які всі є власними префіксами слова в множині Y, а отже в коді X. Оскільки $d \leqslant n$, то це є неможливим. Насправді, код Y міститься в коді Дика над алфавітом $\{a, b\}$ (див. приклад 2.2.13).

Приклад 6.3.6. Нехай $X, Y \subset A^+$ — два максимальні біфіксні коди. Тоді їх добуток XY є максимальним біфіксним тонким кодом і

$$d(XY) = d(X) + d(Y).$$

Перша частина насправді випливає з наслідку 3.4.2. Далі, нехай $w \in \overline{H}(XY)$ — слово, яке не є внутрішнім множником добутку XY. Тоді $w \in \overline{H}(X)$ і $w \in \overline{H}(Y)$. Префікси слова w, які є також власними суфіксами добутку XY, є двох видів. По-перше, існують $d(Y)$ префіксів слова w, які є власними суфіксами слів у коді Y. По-друге, існують $d(X)$ префіксів слова w, які є власними суфіксами слів у коді X. Для кожного такого префікса покладемо $w = uv$. Слово v не є власним префіксом слова в коді Y, оскільки в протилежному випадку слово w було б внутрішнім множником коду XY. Таким чином, слово v має префікс y в коді Y і слово uy є префіксом слова w, яке є власним суфіксом слова в добутку XY. Вони є лише префіксами слова w, які містяться в множині $A^-(XY)$. Оскільки слово w має $d(XY)$ розкладів по відношенню до добутку XY, то звідси випливає формула

$$d(XY) = d(X) + d(Y).$$

Тепер означимо формальний степеневий ряд, який відповідає коду X і відіграє фундаментальну роль наступним чином. Нехай X — тонкий максимальний біфіксний код над алфавітом A. *Баштою* над кодом X називається формальний степеневий ряд T_X (також будемо писати T, коли відомо над яким кодом це визначено та не створює протирічь), визначений за формулою

$$(T_X, w) = d - (L_X, w). \tag{6.26}$$

Наступне твердження дає простий шлях для обчислення значення башти та безпосередньо виливає з твердження 6.1.12.

Твердження 6.3.7. *Нехай $X \subset A^+$ — тонкий максимальний біфіксний код. Тоді*

$$(T_X, ua) = \begin{cases} (T_X, u), & \text{якщо } ua \in A^*X; \\ (T_X, u) - 1, & \text{в іншому випадку.} \end{cases} \tag{6.27}$$

для довільного слова $u \in A^*$ та літери $a \in A$.

Наступне твердження констатує деякі корисні елементарні факти про формальний степеневий ряд T.

Твердження 6.3.8. *Нехай X — тонкий максимальний біфіксний код степеня d над алфавітом A. Позначимо*

$$P = XA^- \qquad і \qquad S = A^-X,$$

і нехай T_X — башта над кодом X. Тоді

$$(T_X, w) = 0 \qquad \text{тоді і лише тільки тоді, коли} \qquad w \in \overline{H}(X),$$

і

$$1 \leqslant (T_X, w) \leqslant d - 1, \tag{6.28}$$

для $w \in H(X)$. Далі $(T_X, \varepsilon) = d - 1$ і

$$\underline{X} - 1 = (\underline{A} - 1)T_X(\underline{A} - 1) + d(\underline{A} - 1), \tag{6.29}$$

$$\underline{P} = (\underline{A} - 1)T_X + d, \tag{6.30}$$

$$\underline{S} = T_X(\underline{A} - 1) + d. \tag{6.31}$$

Доведення. З теореми 6.3.1 випливає, що $(T_X, w) = 0$ тоді і тільки тоді, коли $w \in \overline{H}(X)$. Для всіх інших слів виконується нерівність

$$1 \leqslant (T_X, w).$$

Також

$$(T_X, w) \leqslant d - 1,$$

оскільки всі слова мають щонайменше один розклад, і

$$(T_X, \varepsilon) = d - 1,$$

оскільки порожнє слово ε має рівно один розклад.

Далі, за означенням башти T_X маємо, що

$$T_X + L_X = dA^*,$$

звідки отримуємо

$$T_X(1 - \underline{A}) + L_X(1 - \underline{A}) = (1 - \underline{A})T_X + (1 - \underline{A})L_X = d.$$

Код X є максимальним, отже

$$P = A^* \setminus XA^* \qquad \text{і} \qquad S = A^* \setminus A^*X.$$

Отож, можемо застосувати твердження 6.1.7 з $P = U$ і $S = V$. Тоді з рівностей (6.7) і означення башти T_X отримуємо рівності

$$\underline{P} = (\underline{A} - 1)T_X + d \qquad \text{і} \qquad \underline{S} = T_X(\underline{A} - 1) + d.$$

Також, оскільки

$$\underline{X} - 1 = \underline{P}(\underline{A} - 1) = ((\underline{A} - 1)\underline{T_X} + d)(\underline{A} - 1),$$

то отримуємо рівність

$$\underline{X} - 1 = (\underline{A} - 1)T_X(\underline{A} - 1) + d(\underline{A} - 1).$$

□

Твердження 6.3.8 показує, що носій формального степеневого ряду T_X міститься в множині $H(X)$. Зауважимо, якщо два тонких максимальних біфіксних коди X і X' мають одну башту, то вони збігаються. Справді, за твердженням 6.3.8 коди X і X' мають рівні степені, оскільки

$$d(X) - 1 = (T_X, 1) = (T'_X, 1) = d(X') - 1.$$

Але тоді з рівності (6.29) випливає, що $X = X'$.

Кожен раз, коли тонкий максимальний біфіксний код степені $d = d(X)$ задовольняє рівність

$$\underline{X} - 1 = (\underline{A} - 1)\underline{T}(\underline{A} - 1) + d(\underline{A} - 1),$$

для деякого формального степеневого ряду T, то T має бути баштою на X. Наступне твердження дає достатню умову для отримання того ж висновку, без припущення, що ціле число d дорівнює $d(X)$.

Твердження 6.3.9. *Нехай $T, T' \in \mathbb{Z}\langle\langle A\rangle\rangle$ $d, d' \geqslant 1$ — цілі числа такі, що*

$$(\underline{A} - 1)T(\underline{A} - 1) + d(\underline{A} - 1) = (\underline{A} - 1)T'(\underline{A} - 1) + d'(\underline{A} - 1). \tag{6.32}$$

Якщо існує слово $w \in A^*$ таке, що $(T, w) = (T', w)$, то

$$T = T' \qquad і \qquad d = d'.$$

Доведення. Після домноження з обох боків на $A^* = (1 - \underline{A})^{-1}$ рівність (6.32) перетвориться в таку

$$T - dA^* = T' - d'A^*.$$

Якщо $(T, w) = (T', w)$, то $(dA^*, w) = (d'A^*, w)$. Таким чином, $d = d'$, звідки випливає, що $T = T'$. □

Тепер ми звернемо увагу на вплив внутрішнього перетворення (твердження 6.2.8) на башту над тонким максимальним біфіксним кодом X. Нагадаємо, за умови, що w таке слово, що множини G_1 і D_1 обидві є непорожніми, де

$$G = Xw^{-1}, \qquad D = w^{-1}X, \qquad G_0 = (wD)w^{-1}, \qquad D_0 = w^{-1}(Gw),$$

$$G_1 = G \setminus G_0, \qquad D_1 = D \setminus D_0,$$

код Y, який визначається

$$\underline{Y} = \underline{X} + (1 - \underline{G})\, w \left(1 - \underline{D_0}^* \underline{D_1}\right)$$

є максимальним біфіксним. За твердженням 3.4.9 множини $G = Xw^{-1}$ і $D = w^{-1}X$ є максимальною суфіксними та максимальною префіксною, відповідно. Нехай U — множина власних правих множників множини G, і V — множина власних префіксів множини D. Тоді D_0^*V є множиною власних префіксів слів у множині $D_0^*D_1$, оскільки $D = D_0 \cup D_1$. Отже, отримуємо, що

$$\underline{G} - 1 = (\underline{A} - 1)\underline{U}, \qquad і \qquad \underline{D_0}^* \underline{D_1} - 1 = \underline{D_0}^* \underline{V}(\underline{A} - 1).$$

Повернувшись до коду Y, отримуємо

$$\underline{Y} - 1 = \underline{X} - 1 + (\underline{A} - 1)\underline{U}w\underline{D_0}^*\underline{V}(\underline{A} - 1).$$

Нехай T — башта над кодом X. Тоді використавши формулу (6.29), отримуємо

$$\underline{Y} - 1 = (\underline{A} - 1)\left(T + \underline{U}w\underline{D_0}^*\underline{V}\right)(\underline{A} - 1) + d\,(\underline{A} - 1)\,.$$

Зауважимо, оскільки код X є тонким, то обидві множини G і D є тонкими. Звідси отримуємо, що множини U та V є також тонкими. Оскільки $D_1 = D \setminus D_0 \neq \varnothing$, то множина D_0 не є максимальним кодом. Як підмножина множини D множина D_0 є тонкою, і за теоремою 2.5.13 множина D_0 не є повною. Отож, множина D_0^* є тонкою. Таким чином, множина UwD_0^*V, як добуток тонких множин, є тонкою. Далі, множина $\mathrm{supp}(T) \subset H(X)$ є тонкою. Таким чином, множина

$$\mathrm{supp}(T) \cup UwD_0^*V$$

є тонкою.

Нехай u — слово, яке не є множником слова в множині $\mathrm{supp}(T) \cup UwD_0^*V$. Тоді

$$\left(T + \underline{U}w\underline{D_0}^*\underline{V}, u\right) = 0.$$

З іншого боку, оскільки $G_1(wD_0^*)D_1$ є тонкою, то з формули (6.16) випливає, що множина Y є тонкою. Таким чином, носій башти T_Y над кодом Y є тонким. Якщо v — слово таке, що $(T_Y, v) = 0$, то

$$\left(T + \underline{U}w\underline{D_0}^*\underline{V}, uv\right) = T_Y, uv) = 0,$$

показуючи, що можна використати твердження 6.3.9. Таким чином, отримуємо

$$d(X) = d(Y) \qquad \text{і} \qquad T_Y = T + \underline{U}w\underline{D_0}^*\underline{V}.$$

Таким чином, степінь тонкого максимального біфіксного коду залишається інваріантною при внутрішніх перетвореннях.

Приклад 6.3.10. Скінченний максимальний біфіксний код

$$X = \left\{a^3, a^2ba, a^2b^2, ab, ba^2, baba, bab^2, b^2a, b^3\right\}.$$

над алфавітом $A = \{a, b\}$ з прикладу 6.2.3 має степінь 3. Це можна побачити, спостерігаючи, що жодне слово не має більше ніж 3 розклади, а слово a^3 має 3 розклади, або також факт (див. приклад 6.2.11), що код X отримується з єдиного коду A^3 шляхом внутрішнього перетворення стосовно до слова $w = ab$. Таким чином, отримуємо, що

$$d(X) = d(A^3) = 3.$$

У прикладі 6.3.10 маємо, що

$$D(= w^{-1}A^3) = G(= A^3w^{-1}) = A.$$

Отож, отримуємо, що

$$T_X = T_{A^3} + w.$$

Очевидно, що

$$T_{A^3} = 2 + a + b.$$

Отже,

$$T_X = 2 + a + b + ab.$$

Далі ми даємо характеристику формального степеневого ряду, що є вежею над деяким тонким максимальним біфіксним кодом.

Твердження 6.3.11. *Формальний степеневий ряд $T \in \mathbb{N}\langle\langle A\rangle\rangle$ є баштою над деяким тонким максимальним біфіксвим кодом тоді і лише тоді, коли він задовольняє нижче перелічені умови.*

(*i*) *Для довільних літери $a \in A$ та слова $v \in A^*$ виконуються нерівності:*

$$0 \leqslant (T, v) - (T, av) \leqslant 1, \tag{6.33}$$

$$0 \leqslant (T, v) - (T, va) \leqslant 1. \tag{6.34}$$

(*ii*) *Для довільних літер $a, b \in A$ та слова $v \in A^*$ виконуються нерівності*

$$(T, av) + (T, vb) \leqslant (T, v) + (T, avb). \tag{6.35}$$

(*iii*) *Існує слово $v \in A^*$ таке, що*

$$(T, v) = 0.$$

Доведення. Нехай X — тонкий максимальний біфіксний код степеня d, L — його індикатор і $T = dA^* - L$. Тоді рівності (6.33), (6.34) і (6.35) безпосередньо випливають з рівностей (6.11), (6.12) і (6.13), відповідно. Далі умова (*iii*) виконується для всіх слів $v \in \overline{H}(X)$, і множина $\overline{H}(X)$ э непорожньою.

Навпаки, припустимо, що формальний степеневий ряд $T \in \mathbb{N}\langle\langle A\rangle\rangle$ задовольняє умови твердження. Означимо

$$d = (T, \varepsilon) + 1 \qquad \text{і} \qquad L = d\underline{A}^* - T.$$

Тоді за побудовою, величина L задовольняє умови твердження 6.1.11, а отже L є індикатором деякого біфіксного коду X. Далі за припущенням формальний степеневий ряд T має невід'ємні коефіцієнти. Таким чином, для всіх слів $w \in A^*$ маємо, що

$$(T, w) = d - (L, w) \geqslant 0.$$

Отож, індикатор L є обмеженим. За теоремою 6.3.1 код X є максимальним і тонким. Оскільки $(T, v) = 0$ хоча б для одного слова v, то маємо $(L, v) = d$ і

$$d = \max\{(L, w) \colon w \in A^*\}.$$

Таким чином, d — степінь коду X і $T = d\underline{A}^* - L$ є баштою над X. □

Попередній результат дозволяє розбирати вежу над біфіксним кодом.

Твердження 6.3.12. *Нехай T — башта над тонким максимальним біфіксним кодом X степені $d \geqslant 2$. Тоді формальний степеневий ряд*

$$T' = T - \underline{H(X)}$$

є баштою над деяким тонким максимальним біфіксним кодом степеня $d - 1$.

Доведення. Спочатку зауважимо, що формальний степеневий ряд T' має невід'ємні коефіцієнти. Справді, за твердженням 6.3.8 маємо, що $(T, w) \geqslant 1$ тоді і тільки тоді, коли $w \in H(X)$. Отже $(T', w) \geqslant 0$ для слова $w \in H(X)$ і $(T', w) = (T, w) = 0$ в іншому випадку.

Далі, ми перевіримо три умови твердження 6.3.11.

(i) Нехай $a \in A$ та $v \in A^*$. Якщо $av \in H(X)$, то $v \in H(X)$. Звідси отримуємо, що

$$(T', av) = (T, av) - 1 \qquad \text{і} \qquad (T', v) = (T', av) - 1.$$

Таким чином, нерівність (6.33) є наслідком з відповідної нерівності для башти T. Далі, якщо $av \notin H(X)$, то $(T, av) = (T', av) = 0$. Звідси отримуємо нерівність $(T, v) \leqslant 1$. Якщо $(T, v) = 1$, то $v \in H(X)$, а отже $(T', v) = 0$. В іншому випадку, $v \in \overline{H}(X)$ і $(T', v) = 0$, як це вже зазначалося вище. В обидвох випадках, $(T', v) = 0$, а отже нерівність (6.33) виконується для формального степеневого ряду T'.

(ii) Нехай $a, b \in A$ та $v \in A^*$. Якщо $avb \in H(X)$, то $(T', w) = (T, w) - 1$ для кожного з чотирьох слів $w = avb,\ av,\ vb,\ av$. Отож, нерівність

$$(T', av) + (T', vb) \leqslant (T', v) + (T', avb)$$

у цьому випадку є наслідком відповідної нерівності для башти T. З іншого боку, якщо $avb \notin H(X)$, то як і раніше доводиться, що

$$(T, av) \leqslant 1, \qquad (T, vb) \leqslant 1 \qquad \text{і} \qquad (T', av) = (T', vb) = 0.$$

Таким чином, нерівність (6.35) виконується для формального степеневого ряду T'.

Умова (iii) твердження 6.3.11, очевидно, виконується для формального степеневого ряду T', оскільки $(T', w) = 0$ для $w \in \overline{H}(X)$. Таким чином, T' є баштою над деяким тонким максимальним біфіксним кодом. Її степінь дорівнює $1 + (T', 1)$. Оскільки $1 \in H(X)$, то $(T', 1) = d - 2$. Це завершує доведення твердження. □

Нехай X — тонкий максимальний біфіксний код степені $d \geqslant 2$, і T — башта над кодом X. Нехай X' — тонкий максимальний біфіксний код з баштою $T' = T - \underline{H(X)}$. Тоді код X' має степінь $d-1$. Код X' називається *кодом похідним* з коду X. Оскільки для індикаторів L і L' кодів X і X', маємо

$$L = d\underline{A^*} - T \qquad \text{і} \qquad L' = (d-1)\underline{A^*} - T',$$

то звідси випливає, що

$$L - L' = \underline{A^*} - T + T' = \underline{A^*} - \underline{H(X)} = \underline{\overline{H}(X)},$$

а отже

$$L = L' + \underline{\overline{H}(X)}. \tag{6.36}$$

Ми позначатимемо через $X^{(n)}$ код похідний з коду $X^{(n-1)}$ для $d(X) \geqslant n+1$, з $X^{(0)} = X$.

Твердження 6.3.13. *Для башти T над тонким максимальним біфіксним кодом X степені $d \geqslant 2$ виконується рівність*

$$T = \underline{H(X)} + \underline{H(X')} + \cdots + \underline{H(X^{(d-2)})}.$$

Доведення. За індукцією з твердження 6.3.12 випливає, що

$$T = \underline{H(X)} + \underline{H(X')} + \cdots + \underline{H(X^{(d-2)})} + \widehat{T},$$

де $\widehat{T}$ — башта над кодом степені 1. Цей код є алфавітом, а отже $\widehat{T} = 0$, що доводить твердження. □

Ми тепер опишемо множину власних префіксів і множину власних суфіксів слів похідного коду тонкого максимального біфіксного коду.

Твердження 6.3.14. *Нехай $X \subset A^+$ — тонкий максимальний біфіксний код степені $d \geqslant 2$. Нехай $S = A^-X$, $P = XA^-$, $H = A^* \setminus XA^-$ і $\overline{H} = A^* \setminus H$. Тоді виконуються такі висловлення.*

1. *Множина $S \cap \overline{H}$ є тонким максимальним префіксним кодом. Множина H є множиною її власних префіксів, тобто $S \cap \overline{H} = HA \setminus H$.*
2. *Множина $P \cap \overline{H}$ є тонким максимальним суфіксним кодом. Множина H є множиною її власних суфіксів, тобто $P \cap \overline{H} = AH \setminus H$.*
3. *Множина $S \cap H$ є множиною власних суфіксів похідного коду X'.*
4. *Множина $P \cap H$ є множиною власних префіксів похідного коду X'.*

Доведення. **1.** Нехай T — башта над кодом X і T' — башта над похідним кодом X'. За твердження 6.3.12 маємо, що $T = T' + \underline{H}$, а з твердження 6.3.8 випливає рівність

$$\underline{S} = T\,(\underline{A} - 1) + d.$$

Таким чином,

$$\underline{S} = T'(\underline{A} - 1) + d - 1 + \underline{H}(\underline{A} - 1) + 1.$$

Код X' має степінь $d - 1$. Отож, за формулою (6.31) ряд $T'(\underline{A} - 1) + d - 1$ є характеристичним рядом множини $S' = A^* \setminus X'$ власних суфіксів слів коду X'. Отож,

$$\underline{S} = \underline{H}(\underline{A} - 1) + 1 + \underline{S'} \qquad \text{і} \qquad \underline{S'} = T'(\underline{A} - 1) + d - 1.$$

Множина H є префіксно замкненою та непорожньою. Ми доведемо, що H не містить правого ідеалу. Справді, множина $\overline{H}$ є непорожньою, оскільки код X є тонким, а отже він є ідеалом. Таким чином, для кожного слова $h \in H$ і $k \in \overline{H}$, слово hk не міститься в множині H. За твердженням 3.3.3 множина $Y = HA \setminus H$ є максимальним префіксним кодом, і $H = YA^-$. Отож,

$$\underline{Y} = \underline{H}(\underline{A} - 1) + 1.$$

Крім того, множина H будучи також суфіксно замкненою, то множина Y є насправді семаформним кодом за твердженням 3.5.8. Тепер перевіримо, що $Y = S \cap \overline{H}$.

Припустимо, що $y \in Y$. Тоді з рівності $\underline{S} = \underline{Y} + \underline{S'}$ випливає, що $y \in S$. Оскільки $H = YA^-$, то маємо $y \notin H$. Таким чином, $y \in S \cap \overline{H}$. Навпаки, припустимо, що $y \in S \cap \overline{H}$. Тоді $y \neq \varepsilon$, оскільки з $d \geqslant 2$ випливає, що $H \neq \varnothing$, а отже $\varepsilon \in H$. Крім того, кожен власний префікс слова y міститься в множині $SA^- = A^* \setminus XA^- = H$, а отже є внутрішнім множником коду X. Зокрема, розглядаючи лише найдовший власний префікс, маємо $y \in HA$. Отже, $y \in HA \setminus H = Y$.

Твердження **2** доводиться аналогічно.

Щоб довести твердження **3**, зауважимо, що з того, що ми довели раніше, маємо

$$\underline{S} = \underline{Y} + \underline{S'}. \tag{6.37}$$

Далі

$$S = (S \cap H) \cup \left(S \cap \overline{H}\right) = Y \cup (S \cap H),$$

оскільки $Y = S \cap \overline{H}$. Більше того, оскільки об'єднання є диз'юнктним, то отримуємо, що $\underline{S} = \underline{Y} + \underline{S \cap H}$. Отже, $S' = S \cap H$.

Твердження **4** доводиться аналогічно. □

Теорема 6.3.15. *Нехай X — тонкий максимальний біфіксний код степені d. Тоді множина S його власних суфіксів є диз'юнктним об'єднанням d максимальних префіксних множин.*

Доведення. Якщо $d = 1$, то $X = A$ і множина $S = \{\varepsilon\}$ є максимальною префіксною. Якщо $d \geqslant 2$, то множина $Y = S \cap \overline{H}$, де $H = A^- X A^-$ і $\overline{H} = A^* \setminus H$, є максимальною префіксною за твердженням 6.3.14. Далі множина $S' = S \cap H$ є множиною власних суфіксів коду похідного від коду X. Індукцією доводимо, що множина S' є диз'юнктним об'єднанням $d - 1$ максимальних префіксних множин. Таким чином, множина $S = Y \cup S'$ є диз'юнктним об'єднанням d максимальних префіксних множин. □

Маємо зауважити, що перетворення в теоремі 6.3.15 множини S в диз'юнктні максимальні префіксні множини не є єдиною (див. вправа 6.7.8). Наступний наслідок з теореми 6.3.15 виражає чудову властивість, що середня довжина тонкого максимального біфіксного коду стосовно розподілу Бернуллі є цілим числом.

Наслідок 6.3.16. *Нехай $X \subset A^+$ — тонкий максимальний біфіксний код. Тоді для довільного додатнього розподілу Бернуллі π на вільному моноїді A^*, середня довжина коду X дорівнює його степеню.*

Доведення. Покладемо $d = d(X)$. Нехай π — додатній розподіл Бернуллі на вільному моноїді A^* і $\lambda(X)$ — середня довжина коду X. За наслідком 3.7.14 середня довжина $\lambda(X)$ коду X є скінченною і $\lambda(X) = \pi(S)$, де $S = A^- X$ — множина власних суфіксів коду X. Врахувавши теорему 6.3.15, маємо

$$\underline{S} = \underline{Y_1} + \underline{Y_2} + \cdots + \underline{Y_d},$$

де кожна множина Y_i є максимальним префіксним кодом. Як множина множників коду X, кожна множина Y_i також є тонкою. Отож $\pi(Y_i) = 1$ для $i = 1, \ldots, d$ за теоремою 2.5.16. Отже, отримуємо

$$\lambda(X) = \sum_{i=1}^{d} \pi(Y_i) = d,$$

що і треба було довести. □

Зауважимо, що наслідок 6.3.16 можна довести безпосердньо починаючи з формули (6.30). Однак, наведені нами доведення є найбільш природними.

Тепер доведемо обернене твердження до теореми 6.3.15.

Твердження 6.3.17. *Нехай X — тонкий максимальний біфіксний код. Якщо множина його власних суфіксів є диз'юнктним об'єднанням префіксних множин, то код X є біфіксним, і має степінь d.*

Доведення. Нехай $S = A^- X$. За припущенням маємо

$$\underline{S} = \underline{Y_1} + \underline{Y_2} + \cdots + \underline{Y_d},$$

де $Y_1, Y_2, \ldots, Y_d$ — максимальні префіксні множини. Нехай U_i — множина власних префіксів множини Y_i. Тоді $\underline{A}^* = \underline{Y_i}^* \underline{U_i}$, а отже $\left(1 - \underline{Y_i}\right) A^* = \underline{U_i}$, звідки отримуємо

$$\underline{A}^* = \underline{U_i} + \underline{Y_i}\ \underline{A}^*.$$

Сумуючи ці рівності отримуємо

$$d\underline{A}^* = \sum_{i=1}^{d} \underline{U_i} + \underline{S}\ \underline{A}^*.$$

Домножимо зліва на $\underline{A} - 1$. Оскільки $(\underline{A} - 1)\underline{S} = \underline{X} - 1$, то

$$-d = \sum_{i=1}^{d} (\underline{A} - 1)\, \underline{U_i} + (\underline{X} - 1)\, \underline{A}^*,$$

звідки отримуємо

$$\underline{X}\ \underline{A}^* = \underline{A}^* - \sum_{i=1}^{d} (\underline{A} - 1)\, \underline{U_i} - d.$$

З цієї формули ми отримуємо факт, що множина XA^* є щільною справа. Справді, нехай $w \in A^+$ і поклдадемо $w = au$, з $a \in A$. Кожна з таких множин Y_i є максимальною префіксною. Таким чином, кожна множина $Y_i A^*$ є щільною справа. Ми покажемо, що існує слово v таке, що одночасно $auv \in Y_i A^*$ для всіх $i \in \{1, \ldots, d\}$ і також $uv \in Y_i A^*$ для всіх $i \in \{1, \ldots, d\}$. Справді, існує слово v_1' таке, що $auv_1' \in Y_1 A^*$. Існує слово v_1'' таке, що $uv_1'v_1'' \in Y_1 A^*$. Покладемо $v_1 = v_1'v_1''$. Тоді $uv_1, auv_1 \in Y_1 A^*$. Аналогічно, існує слово v_2 таке, що обидва слова uv_1v_2 і auv_1v_2 містяться в $Y_1 A^*$ і в $Y_2 A^*$. Продовживши таким чином, отримуємо, що існує слово v таке, що $uv, auv \in Y_i A^*$ для $i = 1, \ldots, d$. Отже, для кожного $i \in \{1, \ldots, d\}$ маємо

$$\begin{aligned}\left((\underline{A} - 1)\underline{U_i}, wv\right) &= \left(\underline{A}\ \underline{U_i}, wv\right) - \left(\underline{U_i}, wv\right) = \\ &= \left(\underline{U_i}, uv\right) - \left(\underline{U_i}, wv\right) = \\ &= 0 - 0 = \\ &= 0.\end{aligned}$$

Тому,

$$(\underline{X}\ \underline{A}^*, wv) = (\underline{A}^*, wv) = 1.$$

Отож, отримуємо $wv \in XA^*$. Звідси випливає, що множина XA^* є щільним справа, або еквівалентно код X є повним справа. З огляду на твердження 6.2.1, це означає, що код X максимальним біфіксним.

Нехай $w \in \overline{H}(X)$ — слово, яке не є внутрішнім множником коду X. Тоді $w \neq U_i$ для $i \in \{1, \ldots, d\}$. Оскільки множина Y_i є максимальною префіксною, то маємо, що $w \in Y_i A^*$ для $i \in \{1, \ldots, d\}$. Звідки випливає, що слово w має рівно d префіксів, які є суфіксами слів у коді X, по одному з кожного Y_i. Таким чином, код X має степінь d. □

Приклад 6.3.18. Нехай X — скінченний максимальний біфіксний код, зображений на рис. 6.9. Башта T над кодом X зображена на рис. 6.10. (за її значеннями на мно-

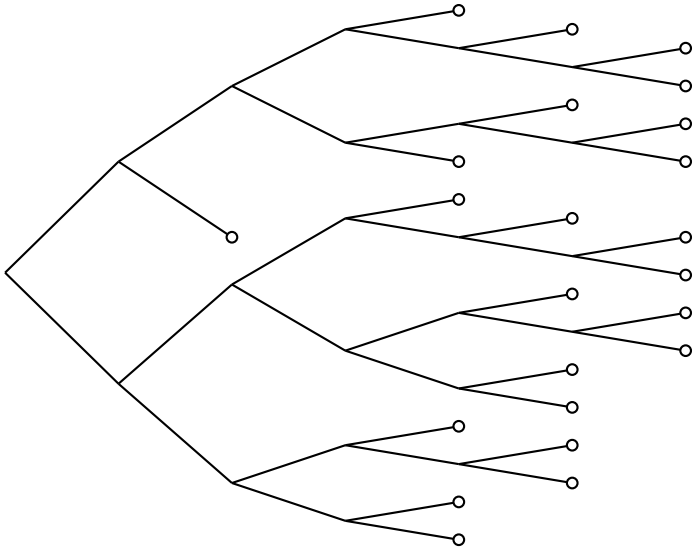


Рис. 6.9: Максимальний біфіксний код степеня 4

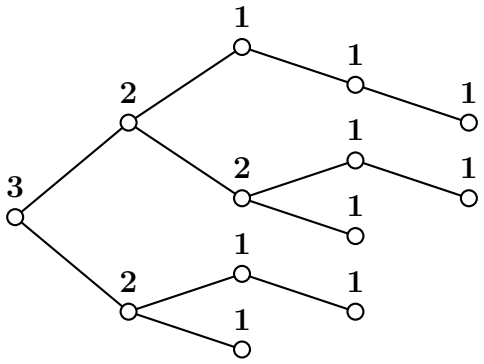


Рис. 6.10: Башта T над кодом X

жині $H(X)$). Обчислення можна зробити використавши рівність (6.27). Похідний код X' є максимальним біфіксним кодом степеня 3, і він викладений в прикладах 6.2.3

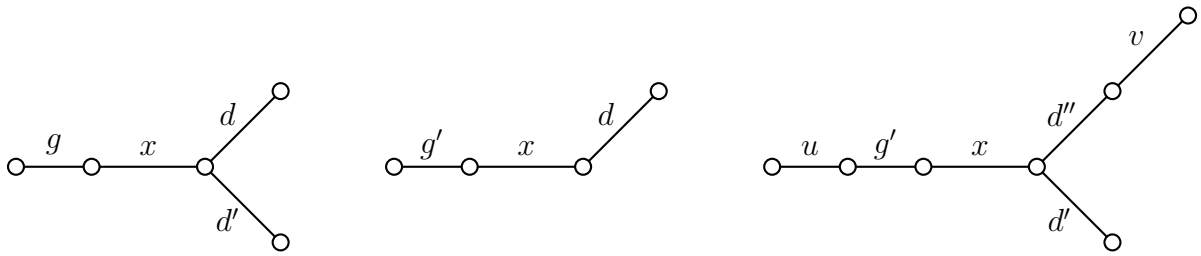


Рис. 6.11: Множина S' всіх власних суфіксів коду X'

і 6.3.10. Множина S' всіх власних суфіксів коду X', зображена на рис. 6.11. Множина S всіх власних суфіксів коду X, зображена на рис. 6.12. Максимальний префіксний

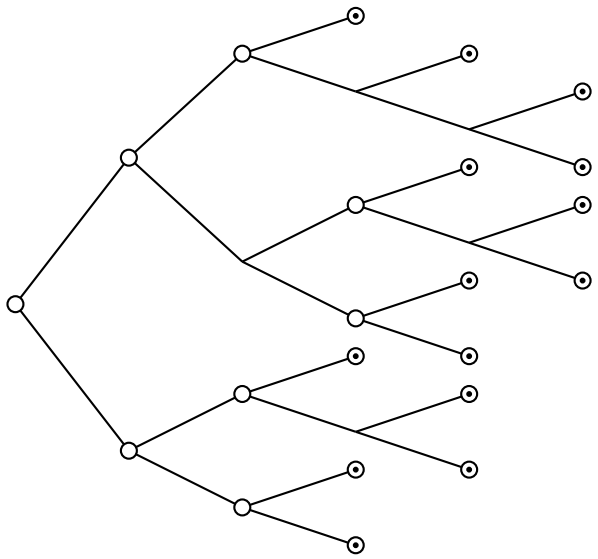


Рис. 6.12: Множина S всіх власних суфіксів коду X

код $Y = S \cap \overline{H}$ є множиною слів позначених на рис. 6.12 символом "$\odot$". Це може бути перевірено оглядом рис. 6.10, 6.11 і 6.12, що $S' = S \cap H$.

6.4 Ядро

Нехай $A \neq \varnothing$, $X \subset A^+$ і $H = A^- X A^-$ — множина внутрішніх множників множини X. *Ядром* множини X, позначатимемо через $K(X)$, або через K, якщо це не викликає плутанини, називається множина

$$K = X \cap H.$$

Таким чином, слово міститься в ядрі множини X, якщо воно міститься в X і є внутрішнім множником множини X. Як ми побачимо в цьому підрозділі, ядро є однією з головних характеристик максимального біфіксного коду.

Почнемо з розгляду того, як ядро пов'язане з обчисленням індикатора.

Твердження 6.4.1. *Нехай $X \subset A^+$ — тонкий максимальний біфіксний код степеня d і K — ядро коду X. Нехай Y — множина така, що $K \subseteq Y \subseteq X$. Тоді*

$$(L_Y, w) = (L_X, w)\,, \tag{6.38}$$

для всіх слів $w \in H(X) \cup Y$. Для всіх слів $w \in A^*$ виконується рівність

$$(L_X, w) = \min\{d, (L_Y, w)\}\,. \tag{6.39}$$

Доведення. За формулою (6.3) маємо, що

$$L_X = \underline{A}^*\,(1 - \underline{X})\,\underline{A}^* \qquad \text{і} \qquad L_Y = \underline{A}^*\,(1 - \underline{Y})\,\underline{A}^*.$$

Нехай $w \in A^*$ і $F(w)$ — множина множників цього слова. Для довільного слова $x \in A^*$, значення $(\underline{A}^* x \underline{A}^*, w)$ дорівнює кількості входжень слова x як множник в слово w. Це значення є ненульовим лише тоді, коди $x \in F(w)$. Отож з рівності

$$(\underline{A}^* \underline{X}\, \underline{A}^*, w) = \sum_{x \in F(w) \cap X} (\underline{A}^* x \underline{A}^*, w)$$

випливає, якщо $F(w) \cap X = F(w) \cap Y$, то $(L_X, w) = (L_Y, w)$. Таким чином, достатньо довести, що $F(w) \cap X = F(w) \cap Y$ для всіх слів $w \in H(X) \cup Y$. З включення $Y \subset X$ отримуємо, що $F(w) \cap Y \subset F(w) \cap X$ для всіх слів $w \in A^*$. Якщо $w \in H(X)$, то $F(w) \subset H(X)$ і $F(w) \cap X \subset K(X)$. Отож, у цьому випадку отримуємо включення $F(w) \cap X \subset F(w) \cap Y$.

Якщо $w \in Y$, то жодних власних префіксів або власних суфіксів слова w не містяться в X, оскільки код X є біфіксним. Отож, отримуємо, що

$$F(w) \cap X = \{w\} \cup \left\{A^- w A^- \cap X\right\} \subset \{w\} \cup K(X) \subset Y.$$

Більше того, у цьому випадку маємо, що $F(w) \cap X \subset F(w) \cap Y$, звідки випливає рівність (6.38).

Тепер, нехай $w \in H(X)$ — внутрішній множник коду X. Тоді $(L_X, w) < d$ за теоремою 6.3.1. З рівності (6.38) випливає, що $(L_X, w) = (L_Y, w)$. Далі, нехай $w \in \overline{H}(X)$. Тоді $(L_X, w) = d$. Використавши формулу (6.6), отримуємо нерівність $(L_X, w) \leqslant (L_Y, w)$. Звідси випливає рівність (6.39). □

Для двох формальних степеневих рядів σ і τ через $\min\{\sigma,\tau\}$ позначимо формальний степеневий ряд, який визначається так:

$$(\min\{\sigma,\tau\},w)=\min\{(\sigma,w),(\tau,w)\}.$$

Теорема 6.4.2. *Нехай X — тонкий максимальний біфіксний код степеня d і K — його ядро. Тоді*

$$L_X=\min\left\{d\underline{A}^*,L_K\right\}.$$

Зокрема, тонкий максимальний біфіксний код визначається його степенем і його ядром.

Доведення. Візьмемо $Y=K(X)$ у попередньому твердженні. Тоді формула

$$L_X=\min\left\{d\underline{A}^*,L_K\right\}.$$

випливає з рівності (6.39). Припустимо, що існує два коди X і X' з однаковими степенем d та однаковими ядрами. Оскільки $K(X)=K(X')$, то маємо $L_K(X)=L_K(X')$, звідки $L_X=L_{X'}$, що в свою чергу означає $X=X'$ за рівністю (6.8). Це завершує доведення теореми. □

Очевидно, що ядро біфіксного коду є самим біфіксним кодом. Тепер ми дамо описання тих біфіксних кодів, які навпаки є ядром якогось тонкого максимального біфіксного коду. Для цього зручно ввести позначення: для біфіксного коду $Y\in A^+$ покладемо

$$\mu(Y)=\max\left\{(L_Y,y)\colon y\in Y\right\}. \tag{6.40}$$

Величина $\mu(Y)$ набуває значення цілого невід'ємного числа або нескінченності. Для зручності вважатимемо, що $\mu(\varnothing)=0$.

Теорема 6.4.3. *Біфіксний код Y є ядром деякого тонкого максимального біфіксного коду степеня d тоді і тільки тоді, коли*

(*i*) *Y не є максимальним біфіксним кодом;*
(*ii*) $\mu(Y)\leqslant d-1$.

Доведення. Нехай X — тонкий максимальний біфіксний код степеня d і $Y=K(X)$ — його ядро. Перевіримо виконання умов (*i*) та (*ii*). Для перевірки умови (*i*) розглянемо слово $x\in X$ таке, що $(L_X,x)=\mu(X)$. Ми стверджуємо, що $x\notin H(X)$. Таким чином, $x\notin K(X)$, а це доводить, що $Y\subsetneq X$. Припустимо, що наше припущення неправильне. Тоді $uxv\in X$ для деяких слів $u,v\in A^+$. Звідси випливає, що $(L_X,uxv)\geqslant 1+(L_X,x)$ оскільки слово uxv має інтерпретацію $(1,uxv,1)$, яка не проходить через слово . Це суперечить вибору слова x, і доводить стверджуване. Далі, для всіх слів $y\in Y$ за формулою (6.38) маємо $(L_X,y)=(L_Y,y)$. Оскільки $y\in H(X)$, то $(L_X,y)\leqslant d-1$, а отже виконується умова (*ii*).

Навпаки, нехай Y — біфіксний код, що задовольняє умови (*i*) та (*ii*). Нехай $L\in\mathbb{N}\langle\langle A\rangle\rangle$ — формальний степеневий ряд, визначений для слова $w\in A^*$ наступним чином

$$(L,w)=\min\left\{d,(L_Y,w)\right\}.$$

Ми перевіримо, що формальний степеневий ряд L задовольняє три умови твердження 6.1.11. Спочатку, нехай $a \in A$ і $w \in A^*$. За нерівностями (6.11), маємо

$$0 \leqslant (L_Y, aw) - (L_Y, w) \leqslant 1.$$

Звідси випливає, якщо $(L_Y, w) < d$, то $(L, w) = (L_Y, w)$. Оскільки

$$(L_Y, aw) \leqslant (L_Y, w) + 1 \leqslant d,$$

то виконується рівність $(L_Y, aw) = (L, aw)$. З іншого боку, якщо $(L_Y, w) \geqslant d$, то

$$(L, aw) = (L, w) = d.$$

Таким чином, в обох випадках маємо

$$0 \leqslant (L, aw) - (L, w) \leqslant 1.$$

Симетрична нерівність

$$0 \leqslant (L, wa) - (L, w) \leqslant 1.$$

доводиться аналогічно. Отже виконується умова (i) твердження 6.1.11.

Нехай, для літер $a, b \in A$ і слова $w \in A^*$ виконується нерівність

$$(L_Y, aw) + (L_Y, wb) \geqslant (L_Y, w) + (L_Y, awb).$$

Розглянемо спочатку випадок, де $(L_Y, w) \geqslant d$. Тоді

$$(L, aw) = (L, wb) = (L, w) = (L, awb) = d,$$

і нерівність

$$(L, aw) + (L, wb) \geqslant (L, w) + (L, awb)$$

є очевидною. Припустимо, що $(L_Y, w) < d$. Тоді $(L_Y, aw) \leqslant d$ і $(L_Y, wb) \leqslant d$. Отже отримуємо

$$\begin{aligned}(L, aw) + (L, wb) &= (L_Y, aw) + (L_Y, wb) \geqslant \\ &\geqslant (L_Y, w) + (L_Y, awb) \geqslant \\ &\geqslant (L, w) + (L, awb),\end{aligned}$$

оскільки $L \leqslant L_Y$. Отже виконується умова (ii) твердження 6.1.11. Нарешті, ми маємо, що $(L_Y, \varepsilon) = 1$, звідки випливає рівність $(L, \varepsilon 1) = 1$.

Таким чином, за твердженням 6.1.11 формальний степеневий ряд L є індикатором для деякого біфіксного коду X. Далі, оскільки ряд L є обмеженим, то код X є тонким і максимальним біфіксним за теоремою 6.3.1. Подібними міркуваннями, оскільки код Y не є максимальним, то формальний степеневий ряд L_Y є необмеженим. Отже, $\max\{L, w) \colon w \in A^*\} = d$, а це доводить, що код X має степінь d.

Ми тепер доведемо, що $Y = X \cap H(X)$, тобто Y є ядром коду X. Спочатку доведемо включення $Y \subset H(X)$. Справді, якщо $y \in Y$, то

$$(L, y) \leqslant (L_Y, y) \leqslant \mu(Y) \leqslant d - 1.$$

Отож, за теоремою 6.3.1 маємо $y \in H(X)$. Далі, зауважимо, що достатньо довести рівність

$$X \cap H(X) = Y \cap H(X),$$

а це еквівалентне доведенню того, що виконується твердження

$$(X, w) = (Y, w) \qquad \text{для всіх слів } \ w \in H(X).$$

Ми доведемо це за індукцією за довжиною слова w. Очевидно, нерівність виконується для $|w| = 0$. Далі, нехай $w \in H(X) \setminus \{\varepsilon\}$. Тоді $(L, w) \leqslant d - 1$. Таким чином, $(L, w) = (L_Y, w)$. Це в свою чергу означає

$$(\underline{A}^* \underline{X}\, \underline{A}^*, w) = (\underline{A}^* \underline{Y}\, \underline{A}^*, w)\,.$$

Але $F(w) \subset H(X)$. Таким чином, за припущенням індукції маємо, що $(X, s) = (Y, s)$ для всіх власних множників слова w. Таким чином ця рівність зводиться до такої $(\underline{X}, w) = (\underline{Y}, w)$. □

Опишемо тепер зв'язок між ядром та операцією взяття похідного коду.

Твердження 6.4.4. *Нехай X — тонкий максимальний біфіксний код степеня $d \geqslant 2$ і $H = A^- X A^-$. Покладемо*

$$K = X \cap H, \qquad Y = HA \setminus H \qquad і \qquad Z = AH \setminus H.$$

Тоді код X' похідний від коду X дорівнює

$$X' = K \cap (Y \cap Z). \tag{6.41}$$

Крім того, маємо

$$K = X \cap X'. \tag{6.42}$$

Доведення. Нехай $S = A^- X$ і $P = X A^-$ — множини власних правих множників і власних префіксів слів в коді X. Нехай $S' = S \cap H$ і $P' = P \cap H$. За твердженням 6.3.14, S' є множиною власних суфіксів слів в X' і, аналогічно, P' є множиною власних префіксів слів в X'. Таким чином, отримуємо

$$\underline{X'} - 1 = (\underline{A} - 1)\underline{S'} = \underline{A}\ \underline{S'} - \underline{S'}.$$

З рівності маємо $S' = S \cap H$, маємо $AS' = AS \cap AH$ і $\underline{A}\ \underline{S'} = \underline{A}\ \underline{S} \odot \underline{A}\ \underline{H}$, де через $\odot$ ми позначаємо добуток Адамара (див. підрозділ 1.7). Отож, отримуємо, що

$$\underline{X'} - 1 = (\underline{A}\ \underline{S} \odot \underline{A}\ \underline{H}) - \underline{S'}.$$

Тепер зауважимо, що за твердженням 6.3.14 множина Z є максимальним суфіксним кодом з власними суфіксами H. Таким чином, отримуємо, що $\underline{Z} - 1 = (\underline{A} - 1)\underline{H}$, звідки випливає, що $\underline{A}\ \underline{H} = \underline{Z} - 1 + \underline{H}$. Аналогічно, з рівності $\underline{X} - 1 = (\underline{A} - 1)\underline{S}$ отримуємо $\underline{A}\ \underline{S} = \underline{X} - 1 + \underline{S}$. Зробивши підстановку, отримуємо

$$\begin{aligned}
\underline{X'} - 1 &= (\underline{A}\ \underline{S} \odot \underline{A}\ \underline{H}) - \underline{S'} = \\
&= (\underline{X} - 1 + \underline{S}) \odot (\underline{Z} - 1 + \underline{H}) = \\
&= \underline{X \cap Z} + \underline{S \cap Z} + \underline{X \cap H} + \underline{S \cap H} + 1 - (1 \odot \underline{H}) - (\underline{S} \odot 1) - \underline{S'}.
\end{aligned}$$

Справді, інші члени набувають значення 0, оскільки ні код X, ні множина Z не містять порожнього слова. Далі, за твердженням 6.3.14 отримуємо $Z = P \cap \overline{H}$, звідки випливає, що

$$X \cap Z = X \cap P \cap \overline{H} = \varnothing.$$

Також за означенням маємо, що $S' = S \cap H$ і $K = X \cap H$. Більше того, $1 \odot \underline{H} = \underline{S} \odot 1 = 1$. Таким чином, наша рівність набуває вигляду

$$\underline{X'} - 1 = \underline{S \cap Z} + \underline{K} - 1.$$

На завершенні, зауважимо, що за твердженням 6.3.14 отримуємо $Y = S \cap \overline{H}$. Отож, маємо, що

$$S \cap Z = S \cap P \cap \overline{H} = Y \cap Z$$

і остаточно

$$X' = K \cup (Y \cap Z),$$

а це доводить рівність (6.41). Далі

$$X \cap X' = (K \cap X) \cup (X \cap Y \cap Z).$$

Тепер, отримуємо

$$X \cap Y \cap Z = X \cap P \cap S \cap \overline{H} = \varnothing$$

і $K \cap X = K$. А отже виконується рівність $X \cap X' = K$. □

Твердження 6.4.5. *Нехай X — тонкий максимальний біфіксний код степеня $d \geqslant 2$ і X' — похідний код від коду X. Тоді*

$$K(X') \subset K(X) \subsetneq X'. \tag{6.43}$$

Доведення. Спочатку доведемо, що $H(X') \subset H(X)$. Справді, нехай $w \in H(X')$. Тоді $(T_{X'}, w) \geqslant 1$, де $T_{X'}$ — башта над кодом X'. За твердження 6.3.12 маємо, що

$$(T_{X'}, w) = (T_X, w) - (H(X), w).$$

Отож, $(T_X, w) \geqslant 1$. Це в свою чергу за твердженням 6.3.8 означає, що $w \in H(X)$. За означенням маємо $K(X') = X' \cap H(X')$. Отож, $K(X') \subset X' \cap H(X)$. З твердження 6.4.4 випливає $X' = K(X) \cup (Y \cap Z)$, де Y і Z — диз'юнктні підмножини з $H(X)$. Отож, $X' \cap H(X) = K(X)$. Звідси випливає, що $K(X') \subset K(X)$. Далі з формули (6.42) також випливає, що $K(X) \subset X'$. Нарешті, ми не можемо мати рівності $K(X) = X'$, оскільки за теоремою 6.4.3 множина $K(X)$ не є максимальним біфіксним кодом. □

Оберненим до твердження 6.4.5 є наступна теорема.

Теорема 6.4.6. *Нехай X' — тонкий максимальний біфіксний код. Для кожної множини Y такої, що*

$$K(X') \subset Y \subsetneq X', \tag{6.44}$$

існує єдиний тонкий максимальний біфіксний код X такий, що

$$K(X) = Y \qquad і \qquad d(X) = 1 + d(X').$$

Більше того, код X' є похідним коду X.

Доведення. Спочатку покажемо, що множина Y є ядром деякого біфіксного коду. Для цього, перевіримо умови теореми 6.4.3. Зі строгого включення $Y \subsetneq X'$ випливає, що множина Y не є максимальним кодом. Далі, за твердженням 6.4.1 маємо, що $(L_Y, y) = (L_{X'}, y)$ для $y \in Y$. Отож, прийнявши $d = d(X') + 1$, ми маємо

$$\mu(Y) \leqslant d(X') = d - 1.$$

За теоремою 6.4.3 існує тонкий максимальний біфіксний код X, який має степінь d такий, що $K(X) = Y$. За теоремою 6.4.2 цей код єдиний. Залишилось довести, що X' є похідним кодом коду X. Нехай Z — похідний код коду X. За твердженням 6.4.5 маємо, що

$$K(Z) \subset K(X) = Y \subsetneq Z.$$

Отож, ми можемо застосувати твердження 6.4.1 для доведення того, що

$$(L_Z, w) = \min\{d - 1, (L_Y, w)\},$$

для всіх слів $w \in A^*$. З включень формули (6.44) отримуємо за твердженням 6.4.1, що

$$(L_{X'}, w) = \min\{d - 1, (L_Y, w)\},$$

для всіх слів $w \in A^*$. Таким чином, $L_{X'} = L_Z$, звідки випливає, що $Z = X'$. □

Твердження 6.4.5 показує, що ядро коду розташоване в деякому "інтервалі", що визначається похідним цього коду. Теорема 6.4.6 стверджує, що всі "точки" цього інтервалу можна ефективно використовувати.

Точніше, твердження 6.4.5 і теорема 6.4.6 показують, що існує бієктивне відображення між множиною тонких максимальних біфіксних кодів степеня $d \geqslant 2$ і парами (X', Y) утвореними тонким максимальним біфіксним кодом X' степеня $d - 1$ і множиною Y, яка задовольняє умову (6.44). Ця бієкція ставить у відповідність коду X пару $(X', K(X))$, де X' — похідний код коду X.

Приклад 6.4.7. Як видно з прикладу 6.3.4 кожен максимальний біфіксний код степеня 2 має вигляд

$$X = C \cup BC^*B,$$

де алфавіт A є диз'юнктним об'єднанням множин B і C, і крім того $B \neq \varnothing$. Це спостереження можна встановити також за допомогою теореми 6.4.6. Справді, похідний код максимального біфіксного коду степеня 2 має степінь 1, а отже збігається з алфавітом A. Тоді для кожної власної підмножини C множини A існує єдиний максимальний біфіксний код степеня 2, ядро якого збігається з множиною C. Цей код, очевидно, є кодом, наведеним вищевказаною формулою.

Приклад 6.4.8. Кількість максимальних біфіксних кодів степеня 3 над скінченним алфавітом , що має принаймні дві літери, є нескінченною. Справді, розглянемо нескінченний тонкий максимальний біфіксний код X' степеня 2. Його ядро $K(X')$ є підмножиною алфавіта A, а отже є скінченним. З огляду на теорему 6.4.6 кожна множина K, яка містить ядро $K(X')$ і строго міститься в коді X' є ядром деякого максимального біфіксного коду степеня 3. Таким чином, їх існує нескінченно багато максимальних біфіксних кодів степеня 3 над скінченним алфавітом . Також, вибір множини $K(X)$, яка не є раціональною, дає біфіксний код X степеня 3, який не є раціональним (вправа 6.7.14).

6.5 Скінченні максимальні біфіксні коди

Скінченні максимальні біфіксні коди мають досить дивовижні властивості, які роблять їх захоплюючими об'єктами.

Твердження 6.5.1. *Нехай $X \subset A^+$ — скінченний максимальний біфіксний код степеня d. Тоді $a^d \in X$ для кожної літери $a \in A$,.*

Доведення. Нехай $a \in A$. За твердження 6.2.7 існує ціле додатне число n таке, що $a^n \in X$. Оскільки код X є скінченним, то існує ціле число k таке, що слово a^k не є внутрішнім множником коду X. Кількість розкладів слова a^k дорівнює d. Також кількість суфіксів слова a^k, які є власними префіксами слів у коді X, дорівнює n. Отож, отримуємо, що $n = d$. □

Зауважимо, що в термінології, введеній у розділі 2, твердження 6.5.1 еквівалентно тому, що порядок кожної літери дорівнює порядку коду.

Зауважимо, що як наслідок цього результату те, що, в загальному випадку, важливо поповнити скінченний біфіксний код до максимального біфіксного коду, який є скінченним. Розглянемо, для прикладу, алфавіт $A = \{a, b\}$ і код $X = \{a^2, b^3\}$ над ним. Скінченний максимальний біфіксний код, що містить код X, матиме одночасно степінь 2 та степінь 3.

Ми тепер доведемо такий результат:

Теорема 6.5.2. *Нехай A — скінченна множина і d — додатне ціле число. Тоді існує лише скінченна кількість скінченних максимальних біфіксних кодів над алфавітом A зі степенем d.*

Доведення. Алфавіт A є єдиним максимальним біфіксним кодом над A, який має степінь 1. Аргументуючи індукцією по степеню d, припустимо, що існує лише скінченна кількість скінченних максимальних біфіксних кодів степеня d. Кожен скінченний максимальний біфіксний код степеня $d+1$ визначається його ядром, яке є підмножиною похідного коду X'. Оскільки X' є скінченним максимальним біфіксним кодом степеня d існує лише скінченна кількість ядер, що і завершує доведення теореми. □

Через $\beta_k(d)$ позначимо кількість скінченних максимальних біфіксних кодів степеня d над k-літерним алфавітом A.

Очевидно, що $\beta_k(1) = 1$. Також маємо $\beta_k(2) = 1$. Справді, $X = A^2$ є, з огляду на приклад 6.2.4, лише скінченним максимальним біфіксним кодом степеня 2. Легко бачити також, що $\beta_1(d) = 1$ для всіх додатних цілих чисел d.

Приклад 6.5.3. Ми перевіримо, що

$$\beta_2(3) = 3. \tag{6.45}$$

Нехай справді $A = \{a, b\}$ і $X \subset A^+$ — скінченний максимальний біфіксний код степеня 3. Похідний код X' є обов'язково $X' = A^2$, оскільки він є лише скінченним максимальним біфіксним кодом степеня 2. Нехай $K = X \cap X'$ — ядро коду X. Отож, отримуємо, що $K \subset A^2$.

За твердженням 6.5.1 маємо, що $a^3, b^3 \in X$. Отож, ядро K не може містити a^2 або b^2. Звідси випливає, що $K \subset \{ab, ba\}$. Далі ми виключаємо випадок $K = \{ab, ba\}$.

Припустимо насправді, що виконується рівність $K = \{ab, ba\}$. Для кожного додатнього цілого числа k слово $(ab)^k$ має рівно два X-розклади. Але оскільки код X є скінченним, то існує ціле число k таке, що $(ab)^k \in \overline{H}(X)$ і слово $(ab)^k$ змушене мати три X-розклади. Отримали протиріччя.

Таким чином, залишилось три кандидати для ядра K: $K = \varnothing$, що відповідає випадку $X = A^3$, тоді $K = \{ab\}$, що дає код X з прикладу 6.2.3, і $K = \{ba\}$, що дає обернений код $\widetilde{X}$ до коду X з прикладу 6.2.3. Це доводить рівність (6.45). Зауважимо також, що це пояснює, чому код $\widetilde{X}$ отримується з коду X шляхом заміни літер a і b: ця властивість виконується, коли вона виконується для ядра коду.

Тепер ми покажемо, як побудувати всі скінченні максимальні біфіксні коди послідовністю внутрішніх перетворень, починаючи з однорідного коду.

Теорема 6.5.4 (Сезарі). *Нехай A — скінченний алфавіт і d — додатне ціле число. Для кожного скінченного максимального біфіксного коду $X \subset A^+$ степеня d існує скінченна послідовність внутрішніх перетворень, які, починаючи з однорідного коду A^d, дає код X.*

Доведення. Нехай K — ядро коду X. Якщо $K = \varnothing$, то $X = A^d$ і немає, що доводити. Це виконується також, якщо $\mathrm{Card}(A) = 1$. Таким чином, ми припускатимемо, що $K \neq \varnothing$ і $\mathrm{Card}(A) \geqslant 2$. Нехай $x \in K$ — слово, яке не є множником іншого слова з ядра K. Ми покажемо, що існують максимальний суфіксний код G і максимальний префіксний код D такий, що

$$GxD \subset X. \tag{6.46}$$

Припустимо протилежне. Нехай $P = XA^-$. Оскільки $x \in K$, то слово x є внутрішнім множником. Таким чином, множина Px^{-1} є непорожньою. Тоді для всіх слів $g \in Px^{-1}$ існує два слова d і d' такі, що

$$gxd, gxd' \in X \qquad \text{і} \qquad X(xd)^{-1} \neq X(xd')^{-1}.$$

Припустимо протилежне. Тоді для деякого слова $g \in Px^{-1}$ усі множини $X(xd)^{-1}$ з словом d, яке пробігає слова, такі, що $gxd \in X$, є рівними. Нехай

$$D = \{d\colon gxd \in X\}$$

і $G = X(xd)^{-1}$, де d — довільний елемент множини D. Тоді $GxD \subset X$, а це суперечить нашому припущенню. Отримане припущення доводить існування слів d і d'.

Серед усіх трійок (g, d, d') таких, що

$$gxd, gxd' \in X \qquad \text{і} \qquad X(xd)^{-1} \neq X(xd')^{-1},$$

виберемо одну з мінімальним значенням $|d| + |d'|$. Для цієї фіксованої трійки (g, d, d') покладемо

$$G = X(xd)^{-1} \qquad \text{і} \qquad G' = X(xd')^{-1}.$$

Тоді G і G' є різними максимальними суфіксними кодами. Розглянемо довільне слово $h \in G \setminus G'$. Тоді, або слово h є власним правим множником деякого слова в коді G', або слово h має слово в коді G' як власний суфікс. Таким чином, помінявши при необхідності коди G і G', існують слова $u, g' \in A^+$ такі, що

$$g' \in G \qquad \text{і} \qquad ug' \in G'.$$

Зауважимо, що звідси випливає, що

$$g'xd \in X \qquad \text{і} \qquad ug'xd' \in X.$$

Тепер розглянемо слово $ug'xd$. Звичайно, що $ug'xd \notin X$. Далі $ug'xd \notin P$, оскільки в протилежному випадку $g'xd \in K$, і слово x буде множника іншого слова в ядрі K, що суперечить припущенню. Оскільки $ug'xd \notin P \cup X$, то слово $ug'xd$ має власний префікс у коді X. Цей префікс не може бути префіксом слова $ug'x$, оскільки $ug'xd' \in X$. Отже, слово $ug'xd$ має $ug'x$ як власний префікс. Таким чином, існує факторизація $d = d''v$ з $d'', v \in A^+$ і $ug'xd'' \in X$.

Тепер зауважимо, що трійка (ug', d', d'') має ті ж властивості, що і трійка (g, d, d'). Справді, обидва слова $ug'xd'$ і $ug'xd'$ містяться в коді X. Також маємо, що

$$X(xd')^{-1} \neq X(xd'')^{-1},$$

оскільки $gxd' \in X$, але $gxd'' \notin X$: це випливає з того факту, що слово gxd'' є власним префіксом слова $gxd \in X$ (рис. 6.13). Таким чином, трійка (ug', d', d'') задовольняє

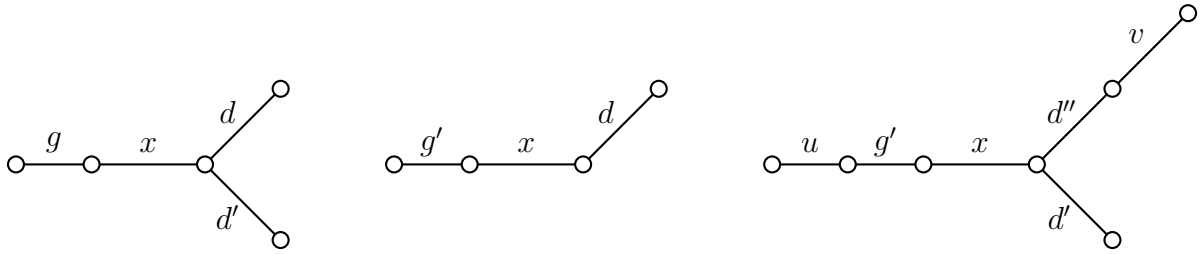


Рис. 6.13: З трійки трійка (g, d, d') до трійки (ug', d', d'')

тим же обмеженням, що і трійка (g, d, d'): проте, $|d'|+|d''| < |d'|+|d|$. Звідси отримуємо протиріччя, що і доводить включення (6.46). Нехай

$$Y = (X \cup Gx \cup xD) \setminus (\{x\} \cup GxD). \tag{6.47}$$

Зважаючи на твердження 6.2.10 множина Y є скінченним максимальним біфіксним кодом і, крім того, внутрішнє перетворення відносно x відображає множину Y в X. Нарешті з (6.47) отримуємо, що

$$\begin{aligned}\operatorname{Card}(Y) &= \operatorname{Card}(X) + \operatorname{Card}(G) + \operatorname{Card}(D) - 1 - \operatorname{Card}(G)\operatorname{Card}(D) = \\ &= \operatorname{Card}(X) - (\operatorname{Card}(G) - 1)(\operatorname{Card}(D) - 1).\end{aligned}$$

Оскільки код G є максимальним суфіксним і $\operatorname{Card}(A) \geqslant 2$, то маємо $\operatorname{Card}(G) \geqslant 2$. З тієї ж причини, отримуємо $\operatorname{Card}(D) \geqslant 2$. Отож,

$$\operatorname{Card}(Y) \leqslant \operatorname{Card}(X) - 1. \tag{6.48}$$

Аргументуючи індукцією про кількість елементів, можна припустити, що код Y отримується з A^d скінченною кількістю внутрішніх перетворень. Це завершує доведення теореми. □

Зауважимо, що за теоремою 6.5.4 (та формулою (6.48)) кожен скінченний максимальний біфіксний код $X \subset A^+$ степеня d задовольняє умову

$$\mathrm{Card}(X) \geqslant \mathrm{Card}(A^d), \tag{6.49}$$

причому маємо рівність тоді і лише тоді, коли $X = A^d$. Цей результат можна довести безпосередньо наступним чином (див. також вправу 3.10.17).

Нехай X — скінченний максимальний префіксний код і

$$\lambda = \sum_{x \in X} |x| k^{-|x|}$$

з $k = \mathrm{Card}(A)$. Число λ — це середня довжина коду X по відношенню до рівномірного розподілу Бернуллі на вільному моноїді A^*. Доведемо нерівність

$$\mathrm{Card}(X) \geqslant k^{\lambda}. \tag{6.50}$$

Для максимального біфіксного коду X степеня d за наслідком 6.3.16 маємо $\lambda = d$, а отже нерівність (6.49) випливає з нерівності (6.50). Для доведення нерівності (6.50), нехай $n = \mathrm{Card}(X)$. Тоді

$$\lambda = \sum_{x \in X} k^{-|x|} \log_k k^{|x|},$$

$$\log_k n = \sum_{x \in X} k^{-|x|} \log_k n.$$

Остання рівність випливає з рівності $1 = \sum_{x \in X} k^{-|x|}$, яка випливає з того факту, що X є скінченним максимальним префіксним кодом. Таким чином, отримуємо

$$\lambda - \log_k n = \sum_{x \in X} k^{-|x|} \log_k (k^{|x|}/n).$$

Оскільки $\sum_{x \in X} k^{-|x|} = 1$ і оскільки функція log є увігнутою, то маємо

$$\sum_{x \in X} k^{-|x|} \log_k (k^{|x|}/n) \leqslant \log_k \left(\sum_{x \in X} k^{-|x|} \, \frac{k^{|x|}}{n} \right),$$

а отже отримуємо, що

$$\lambda - \log_k n \leqslant \log_k \left(\sum_{x \in X} \frac{1}{n} \right) = 0.$$

Звідси випливає нерівність (6.50).

Приклад 6.5.5. Нехай $A = \{a, b\}$ і X — скінченний максимальний біфіксний код степеня 4 з літерним зображенням, яке представлено на рис. 6.14. Ядром коду X є множина

$$K = \left\{ ab, a^2b^2 \right\}.$$

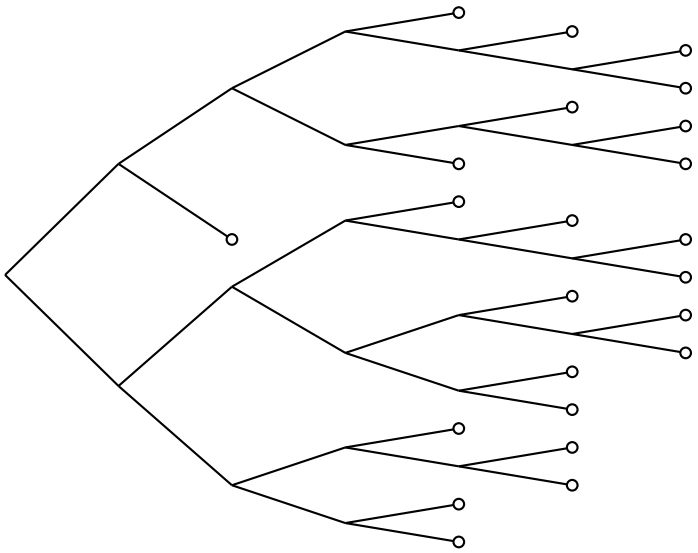


Рис. 6.14: Код X

Немає пари (G, D), яка складається з максимального суфіксного коду G та максимального префіксного коду D таких, що

$$GabD \subset X.$$

З іншого боку маємо, що виконується включення

$$Aa^2b^2A \subset X.$$

Код X отримується з коду Y, зображеного на рис. 6.15. внутрішнім перетворення

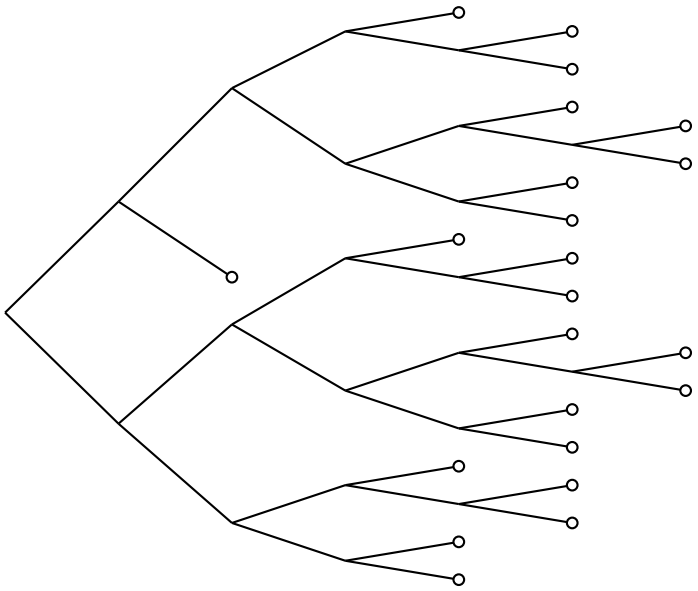


Рис. 6.15: Код Y

відносно слова a^2b^2. Код Y отримується з коду A^4 послідовністю внутрішніх перетворень відносно слів aba, ab^2 і ab.

Ми тепер опишемо конструкцію скінченного максимального біфіксного коду, утвореного з його похідного коду.

Нехай $Y \subset A^+$ — біфіксний код. Слово $w \in A^*$ називається *повним* (стосовно коду Y), якщо існує інтерпретація, що проходить через будь-яку точку слова w. Еквівалентно сказати тому, що слово w э повним, якщо розклад слова w є інтерпретацією.

Біфіксний код Y називається *недостатнім*, якщо множина повних слів стосовно коду Y є скінченною.

Твердження 6.5.6. *Тонкий максимальний біфіксний код X над скінченним алфавітом A є скінченним тоді і тільки тоді, коли його ядро K є недостатнім кодом.*

Доведення. Припустимо спочатку, що код X є скінченним і d — його степінь. Розглянемо слово $w \in \overline{H}(X)$. Тоді слово w має рівно d X-інтерпретацій. Це не всі K-інтерпретації, оскільки K — це підмножина похідного коду X, що має степінь $d-1$. Таким чином, існує точка слова w, через яку не проходить K-інтерпретація. Отже, слово w не є повним для ядра K. Це доводить, що множина повних слів відносно множини K, містить в $H(X)$. Оскільки множина $H(X)$ є скінченною, то ядро K є недостатнім.

Навпаки, припустимо, що код X є нескінченним. Оскільки алфавіт A є скінченним, то існує нескінченна послідовність $(a_n)_{n\geqslant 0}$ літер така, що поклавши $P = XA^-$,

$$p_n = a_0a_1\cdots a_n \in P,$$

для всіх цілих $n \geqslant 0$. Ми покажемо, що існує ціле число k таке, що всі слова $a_ka_{k+1}\cdots a_{k+l}$ для $l \geqslant 1$ є повними відносно ядра K. Зауважимо, що існує щонабільше $d(X)$ цілих чисел n для яких слово p_n є власним суфіксом слова в коді X. Аналогічно, існує щонабільше $d(X)$ цілих чисел n таких, що

$$a_{n+1}a_{n+2}\cdots a_{n+m} \in P,$$

для всіх цілих $m \geqslant 1$. Справді, кожне таке ціле число n визначає інтерпретацію кожного слова $a_0a_1\cdots a_r$, $(r > n)$, яка відмінна від інтерпретацій, що ставляться у відповідність іншим цілим числам.

Ці спостереження показують, що існує ціле число k таке, що для всіх $n \geqslant k$ виконується така умова: слово p_n має суфікс у коді X і слово $a_{n+1}a_{n+2}\cdots a_{n+m}$ є в коді X для деякого цілого числа $m \geqslant 1$. З цієї властивості випливає за індукцією, що для всіх $n \geqslant k$, існує ціле число $i \leqslant k$ таке, що $a_i\cdots a_n \in X^*$.

Нехай $w_l = a_ka_{k+1}\cdots a_{k+l}$ для $l \geqslant 1$. Покажемо, що через кожну точку слова w_l проходить K-інтерпретація. Справді, нехай

$$u = a_ka_{k+1}\cdots a_n, \qquad v = a_{n+1}a_{n+2}\cdots a_{k+l},$$

для деякого $k \leqslant n \leqslant k+1$. Існує ціле число $i \leqslant k$ таке, що $a_i\cdots a_{k-1}u \in X^*$, та існує ціле число $m \geqslant k+1$ таке, що $va_{k+1}\cdots a_m \in X^*$. Насправді, ці два слова містяться в $H(X)\cap X^*$, а отже вони містяться в моноїді K^*. Це показує, що ядро K є достатньою множиною, що і завершує доведення. □

З попереднього твердження випливає такий результат.

Теорема 6.5.7. *Нехай X' — скінченний максимальний біфіксний код степеня $d-1$ з ядром K'. Для кожної недостатньої підмножини K коду X', яка містить ядро K', існує скінченний максимальний біфіксний код X степеня d, що мають ядро K. Тоді похідним коду X є код X'.*

Доведення. Оскільки K — недостатня підмножина, то K не є максимальним біфіксним кодом. Таким чином, $K' \subset K \subsetneq X'$. З огляду на теорему 6.4.6, існує єдиний тонкий максимальний біфіксний код X степеня d і з ядром K. Тоді похідний код коду X збігається з кодом X'. За твердженням 6.5.6 код X є скінченним. □

Наступний наслідок пропонує метод для побудови всіх скінченних максимальних біфіксних кодів шляхом зростання степенів.

Наслідок 6.5.8. *Для довільного цілого числа $d \geqslant 2$ відображення*

$$X \mapsto K(X)$$

є бієкцією множини скінченних максимальних біфіксних кодів степеня d на множину всіх недостатніх підмножин K скінченних максимальних біфіксних кодів X' степеня $d-1$ таких, що

$$K(X') \subset K \subsetneq X'.$$

Приклад 6.5.9. Нехай $A = \{a, b\}$. Для кожного цілого числа $n \geqslant 0$ існує єдиний скінченний максимальний біфіксний код $X_n \subset A^+$ степеня $n+2$ з ядром

$$K_n = \left\{a^i b^i : 1 \leqslant i \leqslant n\right\}.$$

Для $n = 0$ ми маємо $K_0 = \varnothing$ і $X_0 = A^2$. Припустимо, що за індукцією ми побудували код X_n. Тоді $K_n \subset X_n$ і також $a^{n+2}, b^{n+2} \in X_n$, оскільки $d(X_n) = n+2$. Ми покажемо, що $a^{n+1}b^{n+1} \in X_n$. Справді, жоден власний префікс слова $a^{n+1}b^{n+1}$ не міститься в коді X_n, оскільки кожен має суфікс в коді X_n або є власним суфіксом слова a^{n+2}. Розглянемо тепер слово $a^{n+1}b^{n+k}$ для достатньо великого цілого числа k. Оскільки код X_n є скінченним, то існує деякий префікс $a^{n+1}b^{n+r} \in X_n$ для деякого цілого числа $r \geqslant 1$. Якщо $r \geqslant 2$, то b^{n+2} є суфіксом цього слова. Таким чином, отримуємо, що $r = 1$ і $a^{n+1}b^{n+1} \in X_n$.

Очевидно, що $K_n \subset K_{n+1}$. Множина K_{n+1} є недостатньою. Насправді, слово a не має K_{n+1} інтерпретації,яка проходить через точку $(a, 1)$ і слово b немає інтерпретації, яка проходить через точку $(1, b)$. Таким чином, множина повних слув збігається з $\{\varepsilon\}$. На завершенні маємо, що

$$K_n \subset K_{n+1} \subsetneq X_n.$$

Це доводить існування та єдиність коду X_{n+1}, використавши теорему 6.5.7.

Код X_1 є кодом степеня 3 і його описано в прикладі 6.2.3. Код X_2 є кодом степеня 4 з прикладу 6.5.5.

Ми завершуємо цей підрозділ з деякими зауваженнями про розподіл довжин біфіксних кодів. На противагу до випадку префіксних кодів, є хибним твердження, що довільна послідовність $(u_n)_{n\geqslant 1}$ цілих чисел така, що $\sum_{n\geqslant 1} u_n k^{-n} \leqslant 1$ є розподілом довжин біфіксного коду на k літерах. Для прикладу, не існує біфіксного коду над алфавітом $\{a,b\}$, який має той ж самий розподіл, що і префіксний код $\{a, ba, bb\}$. Справді, такий код має містити літеру, скажемо a, і тоді можливим словом довжини 2 є лише bb. Ми доведемо, що виконується таке твердження.

Твердження 6.5.10. *Для кожної послідовності $(u_n)_{n\geqslant 1}$ цілих чисел такої, що*

$$\sum_{n\geqslant 1} u_n k^{-n} \leqslant \frac{1}{2} \tag{6.51}$$

існує біфіксний код над алфавітом з k літер з розподілом довжин $(u_n)_{n\geqslant 1}$.

Доведення. Ми доведемо за індукцією по $n \geqslant 1$, що існує біфіксний код X_n з розподілом довжин $(u_n)_{1\leqslant i\leqslant n}$ на алфавіті A, який складається з k символів. Це твердження є істинним для $n = 1$, оскільки $u_1 k^{-1} \leqslant 1/2$, а отже $u_1 < k$. Припустимо, що твердження індукції істинне для натурального числа n. Тоді за (6.51) маємо

$$\sum_{i=1}^{n+1} u_i k^{-i} \leqslant \frac{1}{2}$$

або еквівалентно, домноживши обидва боки нерівності на $2k^{n+1}$, отримуємо

$$2\left(u_1 k^n + \cdots + u_n k + u_{n+1}\right) \leqslant k^{n+1},$$

звідки випливає, що

$$u_{n+1} \leqslant 2u_{n+1} \leqslant k^{n+1} - 2\left(u_1 k^n + \cdots + u_n k\right). \tag{6.52}$$

Оскільки код X_n є біфіксним за припущенням індукції, то маємо

$$\operatorname{Card}\left(X_n A^* \cap A^{n+1}\right) = \operatorname{Card}\left(A^* X_n \cap A^{n+1}\right) = u_1 k^n + \cdots + u_n k.$$

Отож, отримуємо

$$\begin{aligned}\operatorname{Card}\left((X_n A^* \cup A^* X_n) \cap A^{n+1}\right) &\leqslant \operatorname{Card}\left(X_n A^* \cap A^{n+1}\right) + \operatorname{Card}\left(A^* X_n \cap A^{n+1}\right) \leqslant \\ &\leqslant 2\left(u_1 k^n + \cdots + u_n k\right).\end{aligned}$$

З нерівності (6.52) випливає, що

$$\begin{aligned}u_{n+1} &\leqslant k^{n+1} - 2\left(u_1 k^n + \cdots + u_n k\right) \leqslant \\ &\leqslant \operatorname{Card}\left(A^{n+1}\right) - \operatorname{Card}\left((X_n A^* \cup A^* X_n) \cap A^{n+1}\right) = \\ &= \operatorname{Card}\left(A^{n+1} \setminus (X_n A^* \cup A^* X_n)\right).\end{aligned}$$

Це доводить, що можна вибрати множину Y слів u_{n+1} довжини $n+1$ на алфавіті A, яка не має префіксів або суфіксів в коді X_n. Тоді множина $X_{n+1} = Y \cap X_n$ є біфіксною, що завершує доведення. □

Обмеження $1/2$ у формулюванні твердження 6.5.10 не найкраще із можливих. Можна припустити, що висловлення має $3/4$ замість $1/2$. Для зручності ми називаємо послідовність (u_n) цілих чисел є *k-реалізовною*, якщо існує біфіксний код на k символах з таким розподілом довжини.

Зафіксуємо натуральне число $N \geqslant 1$ та впорядкуємо послідовності $(u_n)_{1\leqslant n\leqslant N}$ цілих чисел, поклавши $(u_n) \leqslant (v_n)$ тоді і тільки тоді, коли $u_n \leqslant v_n$ для $1 \leqslant n \leqslant N$. Якщо $(u_n) \leqslant (v_n)$ і послідовність (v_n) є k-реалізовною, то послідовність (u_n) є k-реалізовною також. В таблиці 6.1 викладено значення максимальних 2-реалізовних послідовностей для $N \leqslant 4$. Покладемо $u(z) = \sum u_n z^n$. Для кожного значення змінної N ми перераховуємо у спадному лексикографічному порядку максимальну реалізовну послідовність із відповідним значенням суми $u(1/2) = \sum u_n 2^{-n}$. Розподілу із значенням 1 відповідають максимальні біфіксні коди. Наприклад, розподіл $(0, 1, 4, 4)$ відповідає максимальному біфіксному коду з прикладу 6.2.3.

	2			3				4				
N	u_1	u_2	$u(1/2)$	u_1	u_2	u_3	$u(1/2)$	u_1	u_2	u_3	u_4	$u(1/2)$
	2	0	1.0000	2	0	0	1.0000	2	0	0	0	1.0000
	1	1	0.7500	1	1	1	0.8750	1	1	1	1	0.9375
				1	0	2	0.7500	1	0	2	1	0.8125
								1	0	1	3	0.8125
								1	0	0	4	0.7500
	0	4	1.0000	0	4	0	1.0000	0	4	0	0	1.0000
				0	3	1	0.8750	0	3	1	0	0.8750
								0	3	0	1	0.8125
				0	2	2	0.7500	0	2	2	2	0.8750
								0	2	1	3	0.8125
								0	2	0	4	0.7500
				0	1	5	0.8750	0	1	5	1	0.9375
								0	1	4	4	1.0000
								0	1	3	5	0.9375
								0	1	2	6	0.8750
								0	1	1	7	0.8125
								0	1	0	9	0.8125
				0	0	8	1.0000	0	0	8	0	1.0000
								0	0	7	1	0.9375
								0	0	6	2	0.8750
								0	0	5	4	0.8750
								0	0	4	6	0.8750
								0	0	3	8	0.8750
								0	0	2	10	0.8750
								0	0	1	13	0.9375
								0	0	0	16	1.0000

Табл. 6.1: Список максимальних 2-реалізовних розподілів довжин довжини щонайбільше $N \leqslant 4$

По таблиці 6.1 можна перевірити, що мінімальне значення сум $u(1/2)$ дорівнює

3/4. Оскільки перелічені розподіли є максимальними для компонентного порядку, це показує, що для кожної послідовності $(u_n)_{1\leqslant n\leqslant N}$ з $N \leqslant 4$ такої, що $u(1/2) \leqslant 3/4$, існує бінарний біфіксний код X такий, що $u_X = u$.

Оскільки тонкий максимальний біфіксний код X за твердженням 6.2.1 є також максимальним, як код, його породжуючий ряд задовольняє умову $f_X(1/k) = 1$, де k — кількість літер в алфавіті. У таблиця 6.2 перераховані розподіли довжин скінченних максимальних біфіксних кодів степеня $d \leqslant 4$ над алфавітом $\{a, b\}$. Для кожного степеня, останній стовпчик містить кількість біфіксних кодів з цим розподілом, із загальною кількістю 73 степеня 4. Існує 39 з них з $\{a, b\}^3$ як похідні, та 34 з одним із двох інших біфіксних кодів 3-uo степеня (див. вправи).

d	1		2		3				4							
	2	1	0	4	1	0	0	8	1	0	0	0	16			1
										0	0	1	12	4		6
										0	0	2	8	8		6
										0	0	2	9	4	4	8
										0	0	3	5	8	4	6
										0	0	3	6	4	8	4
										0	0	3	6	5	4	4	4
										0	0	4	3	5	8	4	4
						0	1	4	4	2	0	1	0	5	12	4	2
											0	1	0	6	8	8	2
											0	1	0	6	9	4	4	4
											0	1	0	7	5	8	4	4
											0	1	0	7	6	5	4	4	2
											0	1	0	8	2	9	4	4	2
											0	1	1	3	9	8	4		4
											0	1	1	4	6	8	8		4
											0	1	1	4	6	9	4	4	4
											0	1	1	5	3	9	8	4	4
											0	1	2	2	4	9	12	4	2
		1			1				3										73

Табл. 6.2: Розподіл по довжині бінарних скінченних максимальних біфіксних кодів степеня, шо не перевищує 4

6.6 Поповнення

Для скінченного біфіксного коду X проста конструкція показує, що він міститься в максимальному раціональному біфіксному коді. Справді, або код X вже є максимальним, або він є для кожного достатньо великого цілого числа d ядром максимального раціонального біфіксного коду степеня d (теорема 6.4.3 і та вправа 6.7.10).

Для раціонального біфіксного коду X, який не є максимальним, взагалі не вірно, що він є ядром деякого максимального раціонального біфіксного коду. Замість того, щоб діяти ззовні, додаючи слова, що мають слова коду X як множники, треба працювати зсередини, додаючи перші слова, які є множниками слів коду X (і тому містяться в ядрі результату).

Теорема 6.6.1. *Кожен раціональний біфіксний код міститься в максимальному раціональному біфіксному коді.*

Нехай $Y \subset A^*$ — біфіксний код. Нагадаємо, що *індикатором* коду Y називається формальний ряд, означений так:

$$L_Y = \underline{A}^*(1 - \underline{Y})\underline{A}^*.$$

Нам знадобиться декілька властивостей індикатора, згрупованих у наступній лемі для зручності.

Лема 6.6.2. *Нехай $Y \subset A^*$ — біфіксний код і L — його індикатор. Тоді для довільних слів $u, v, w \in A^*$ і довільної літери $a \in A$ виконуються такі умови:*

(1) *для кожного натурального числа i з $1 \leqslant i \leqslant (L, w)$, існує префікс p слова w такий, що $(L, p) = i$;*
(2) *якщо Y — раціональна множина і не є максимальним кодом, то для кожного слова u множина значень $\{(L, uv) \colon v \in A^*\}$ є необмеженою;*
(3) *$(L, w) = (L, wa)$ тоді і тільки тоді, коли слово wa має суфікс в коді Y;*
(4) *якщо $(L, v) = (L, uv)$, то слово uv має префікс в коді Y;*
(5) *якщо $Y \subset Z$, то $L_Y \geqslant L_Z$.*

Доведення. Властивість (1) є безпосередньо очевидним наслідком формули (6.12) з твердження 6.1.11.

Для доведення властивості (2) зауважимо, що за твердженням 2.5.20 раціональний код є тонким. Якщо множина Y є раціональною і не є максимальною, то індикатор L є необмеженим за теоремою 6.3.1. Звідси випливає, що величина (L, v) є достатньо великою, і аналогічно за твердженням 6.1.8 отримуємо, що $(L, uv) \geqslant (L, v)$.

(3) За формулою 6.5 маємо, що величина (L, w) дорівнює $|w| + 1$ — кількості множників слова w, які містяться в множині Y. Ця кількість множників є тою ж самою і для слова wa, за винятком випадків, коли слово wa має суфікси в множині Y, і в цьому випадку слово wa має рівно на один множник більше, оскільки Y є суфіксним кодом. Звідси випливає властивість (3).

(4) Припустимо, що $(L, v) = (L, uv)$. За твердженням 6.1.8 маємо, що $(L, v) = (L, u'v)$ для кожного суфікса u' слова u. Отже за симетричним твердженням до (3),

простою математичною індукцією по довжині суфікса u', починаючи з $|u'| = 1$, доводиться, що слово $u'v$ має префікс у множині Y. Таким чином слово uv має префікс у множині Y.

Властивість (5) випливає з імплікації (6.6). □

Ідея конструкції для доведення теореми 6.6.1 полягає в наступному. Почавши з раціонального біфіксного коду $X = X_0 \subset A^+$, ми будуємо спадну послідовність множин $(X_n)_{n\geqslant 1}$, які всі представлені як раціональні біфіксні коди. Далі доведемо, що для деякого натурального числа n множина X_n є максимальним раціональним біфіксним кодом, що містить код X, тим самим доводячи теорему.

Для довільної множини Y покладемо $P(Y) = Y \setminus YA^+$. $P(Y)$ є множиною слів множини Y, які є мінімальними для префіксного порядку. Таким чином, $w \in P(Y)$ тоді і тільки тоді, коли слово міститься в Y і воно не має власних префіксів у множині Y. Множина $P(Y)$ є префіксною. Далі, через $I(Y)$ позначимо множину слів вільного моноїда A^*, які є непорівняльними зі словами з множини Y стосовно префіксного порядку. Іншими словами, $w \in I(Y)$ тоді і тільки тоді, коли слово w не є префіксом слова в Y і немає префікса в Y. Деякий час ми будемо використовувати алгебраїчне формулювання $I(Y) = A^* \setminus (YA^- \cup YA^*)$. На завершенні, ми позначимо через $\overline{Y}$ множину $P(I(Y))$. Множина $\overline{Y}$ називається *супутником* множини Y. Таким чином, $w \in \overline{Y}$ тоді і тільки тоді, коли слово w є непорівняльним зі словами множини Y і коже власний префікс слова w є префіксом слова в Y. Справді, власний префікс слова w є префіксом слова множини Y або має префікс в Y, але другий випадок виключається, оскільки це означатиме, що слово w має префікс у множині Y, а отже це слово можна порівняти з елементами множини Y.

Супутника множини не слід плутати з його доповненням. Нагадаємо також, що через A^-Y (відповідно, YA^-) позначається множина власних суфіксів (відповідно, префіксів) слів у множині Y.

Твердження 6.6.3. *Нехай $X = X_0$ — біфіксний код. Означимо рекурентно для цілих чисел $n \geqslant 0$:*

$$L_n = L_{X_n}, \tag{6.53}$$
$$V_n = \{w \in A^* \colon (L_n, w) = n+1\}, \tag{6.54}$$
$$Z_n = I(X_n) \cap P(V_n), \tag{6.55}$$
$$X_{n+1} = X_n \cup (Z_n \setminus A^-X). \tag{6.56}$$

Для кожного натурального числа $n \geqslant 1$ множина X_n є біфіксним кодом і $(L_n, w) \leqslant n$ для всіх слів $w \in X_n \setminus X$.

Доведення. Припустимо, що X_n є біфіксним кодом і задовольняє нерівність у твердженні. Ми доведемо, що аналогічне виконується для X_{n+1}. За рівність (6.55) множина Z_n є префіксним кодом, який є непорівняльним з X_n стосовно префіксного порядку. З огляду на рівність (6.56) множина X_{n+1} є об'єднанням двох префіксних кодів, які є непорівняльними стосовно префіксного порядку, оскільки множина $(Z_n \setminus A^-X)$ міститься в $I(X_n)$. Таким чином, сама множина X_{n+1} є префіксним кодом.

Ми доведемо, що X_{n+1} є суфіксним кодом. Припустимо протилежне: для деяких слів $x, x' \in X_{n+1}$, слово x є власним суфіксом слова x'. За побудовою маємо два випадки: або $x \in X_n$, або $x \in Z_n \setminus A^-X$.

У першому випадку, маємо, що $x' \notin X_n$, оскільки множина X_n є суфіксним кодом за індукцією. Таким чином, $x' \in Z_n \setminus A^-X$ та $x' \in P(V_n)$, а отже x' міститься в V_n, і за означенням останнього отримуємо, що $(L_n, x') = n+1$. Запишемо $x' = wa$, де $a \in A$. Оскільки слово x' має суфікс у коді X_n (назвемо його x), то за лемою 6.6.2(3) маємо $(L_n, w) = (L_n, wa)$. Отож $(L_n, w) = n+1$, звідки випливає, що $w \in V_n$. Це суперечить тому, що $x' \in P(V_n)$.

У другому випадку маємо, що $x \in Z_n$, а отже $x \in V_n$ і $(L_n, x) = n+1$. Більше того, $x' \notin X$, бо в протилежному випадку мали б, що $x \in A^-X$. Припустимо, що $x' \in X_n$. Тоді $x' \in X_n \setminus X$ і за припущення індукції отримуємо, що $(L_n, x') \leqslant n$. За твердженням 6.1.8 отримуємо протиріччя, оскільки слово x є множником слова x'. Таким чином, маємо, що $x' \in Z_n \setminus A^-X$. Звідси випливає, що $x' \in V_n$, а отже $(L_n, x') = n+1 = (L_n, x)$. З леми 6.6.2(4) ми отримуємо, що слово x' має префікс в коді X_n. Отримали протиріччя, оскільки $x' \in Z_n \subset I(X_n)$.

Залишилося довести, що $(L_{n+1}, x) \leqslant n+1$ для $x \in X_{n+1} \setminus X$. Справді, нехай $x \in X_{n+1} \setminus X$. Оскільки $X_n \subset X_{n+1}$, то за лемою 6.6.2(5) маємо, що $(L_{n+1}, x) \leqslant (L_n, x)$. Ми робимо висновок, що X_{n+1} — це біфіксний код. Зауважимо, що $L_{n+1} \geqslant L_n$ за лемою 6.6.2(5) оскільки X_n є підмножиною в X_{n+1}. Якщо $x \in X_n$, то за припущенням індукції маємо $(L_n, x) \leqslant n$, а якщо $x \notin X_n$, то $x \in Z_n \subset V_n$, а отже $(L_n, x) = n+1$. В обидвох випадках ми отримуємо, що $(L_{n+1}, x) \leqslant n+1$. □

Зауважимо, що у формулюванні твердження 6.6.3 об'єднання, яке визначає коди X_{n+1} є диз'юнктним, оскільки $Z_n \subset I(X_n)$ і множина $I(X_n)$ не може перетинати код X_n.

Лема 6.6.4. *Нехай $X = X_0$ — раціональний біфіксний код. Тоді X_n є раціональною множиною для довільного натурального числа $n \geqslant 1$.*

Доведення. Ми доведемо твердження індукцією по n. Для $n = 0$ за припущенням. Припустимо далі, що множина X_n є раціональною. Нехай $U_n = A^* \setminus X_nA^*$. Множина U_n є раціональною. За формулою (6.4) для кожного слова z значення дорівнює (L_n, z) кількості суфіксів слова z, які містяться в U_n.

Нехай $\mathcal{A} = (Q, i, T)$ — детермінований автомат, що розпізнає множину U_n. Нехай $\mathcal{B} = (Q \cup \omega, \omega, T \cup \omega)$ з $\omega \notin Q$ — автомат побудований наступним чином. Переходами є такі переходи автомата $\mathcal{A}$ плюс петлі (ω, a, ω) для кожної літери a в алфавіті A ьа перехід (ω, a, q) для кожного переходу (i, a, q) автомата $\mathcal{A}$.

Тоді для кожного слова z кількість успішних шляхів помічених словом z, які починаються в ω дорівнює кількості суфіксів слова z, що містяться в множині U_n. Іншими словами, $(L_n, z) = (|B|, z)$. отже, за твердженням 1.10.4 множина V_n є раціональною. Оскільки

$$I(X_n) = A^* \setminus \left(X_nA^- \cup X_nA^*\right),$$

то множина $I(X_n)$ є раціональною. Позаяк $P(V_n) = V_n \setminus V_nA^+$, то множина $P(V_n)$ є також раціональною. Отже, множина Z_n є раціональною, а звідси випливає, що раціональною є множина X_{n+1}. □

Відтепер ми вважаємо, що $X = X_0$ — це раціональний біфіксний код. Для доведення теореми досить, з огляду на твердження 6.6.3, показати, що X_n — максимальний

біфіксний код для деякого натурального числа n. За теоремою 2.5.13 та твердженням 2.5.20 достатньо показати, що X_n є повним справа префіксним кодом. Це мета наступних лем.

Для частково впорядкованої множини S *висотою елемента* $s \in S$ називається максимальна довжина ланцюгів, які строго зростають, що закінчуються на s. Висота елемента s частково впорядкованої множини S позначається через $h(s)$. *Висотою частково впорядкованої множини* S називається максимальна висота його елементів, тому це просто максимальна довжина строго зростаючого ланцюга елементів у S. Висота є скінченною або нескінченною. Позначимо через $S^{(i)}$ множину елементів висоти i частково впорядкованої множини S.

З твердження 3.2.12 випливає, що для раціонального коду Y висота множини суфіксів коду Y, впорядкованих префіксним порядком є скінченною. Симетрична властивість виконується для суфіксних кодів. Позначимо через π висоту множини префіксів коду X для суфіксного порядку.

Нагадаємо, що через $\overline{X} = P(I(X))$ позначається супутник множини X. Таким чином, слово міститься в $\overline{X}$, якщо воно э непорівняльним зі словами множини X стосовно префіксного порядку та немає власних префіксів з цією властивістю.

Лема 6.6.5. *Висота супутника $\overline{X}$ стосовного множникового порядку не перевищує величини π.*

Доведення. Припустимо протилежне, що існує строго зростаючий ланцюг стосовно множникового порядку $x_0, x_1, x_2, \ldots, x_\pi$ довжини $\pi + 1$ з $x_i \in \overline{X}$. Позаяк супутник $\overline{X}$ є префіксним кодом, то слово x_i не є префіксом слова x_{i+1}. Ми можемо записати $x_i = p_i s_i$ так, що кожне слово p_i є власним суфіксом слова p_{i+1}, кожне слово s_i є непорожнім власним префіксом слова s_{i+1} (див. рис. 6.16).

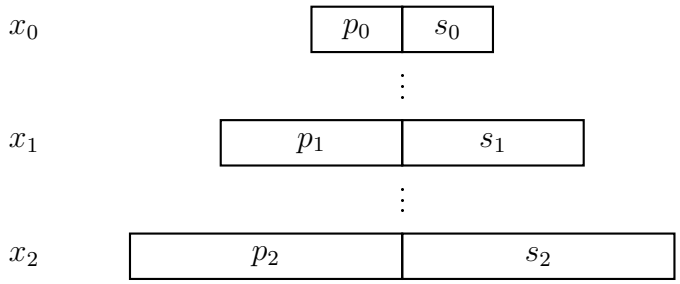


Рис. 6.16: Ланцюг для множникового порядку

Зауважимо, що $p_i \neq p_{i+1}$, оскільки слово x_i не є префіксом слова x_{i+1}. Таким чином, $p_0, \ldots, p_\pi$ є строго зростаючим ланцюгом стосовно суфіксного порядку.

Ми доведемо, що кожне слово p_i є префіксом деякого слова в множині X, звідки отримуємо протиріччя з огляду на означення величини π. Справді, кожне слово p_i є власним префіксом слова x_i. Оскільки $x_i \in P(I(X))$, то кожен власний префікс слова x_i є префіксом слова в множині X. Отож, слово p_i є префіксом слова в X. □

Розглянемо множину $\overline{X}$, супутник множини X, впорядковану множниковим порядком. Для цілого числа $i \geqslant 1$ покладемо

$$\overline{X}^{(i)} = \left\{ w \in \overline{X} \colon h(w) \leqslant i \right\},$$

де через $h(w)$ позначається довжина слова w в множині $\overline{X}$ стосовно множникового порядку. Зокрема, $\overline{X}^{(1)}$ — це множина слів у супутнику $\overline{X}$, які є мінімальними стосовно множникового порядку. З попередньої леми випливає, що $\overline{X}^{(\pi)} = \overline{X}$.

Нехай σ дорівнює 1+"висота множини суфіксів множини X стосовно префіксного порядку".

Лема 6.6.6. *Нехай T — множина слів така, що кожен власний суфікс слова з T є порівняльними стосовно префіксного порядку з деяким словом у X_n. Тоді ряд L_n є обмеженим на T.*

Доведення. Нехай $w \in T$. За твердженням 6.1.6 маємо, що $(L_n, w) = 1 + l$, де l — кількість власних суфіксів слова w, що містяться в $A^* \setminus X_n A^*$. Тепер, оскільки жоден з цих суфіксів не міститься в $I(X_n)$, то вони всі належать множині $X_n A^-$.

Таким чином, число l є обмеженим максимальною довжиною зростаючих ланцюгів префіксів множини X_n стосовно суфіксного порядку. Ця величина є обмеженою за симетричним висловлення до твердження 3.2.12, оскільки множина X_n є раціональною. □

Лема 6.6.7. *Існує натуральне число m таке, що ряд L_m є обмеженим на супутнику $\overline{X}$ множини X.*

Доведення. Ми доведемо індукцією по $i \geqslant 1$ існування натурального числа k такого, що ряд L_k є обмеженим на множині $\overline{X}^{(i)}$.

Для $i = 1$ ми доведемо, що ряд L_0 є обмеженим на множині $\overline{X}^{(1)}$. Для цього покажемо, що можна застосувати лему 6.6.6 з $n = 0$ і $T = \overline{X}^{(1)}$. Справді, припустимо протилежне, що деяке слово $v \in \overline{X}^{(1)}$ має власний суфікс s, який міститься в $I(X)$. Тоді деякий префікс слова s міститься в множині $P(I(X)) = \overline{X}$, і слово v має власний множник в множині $\overline{X}$, що суперечить означенню множини $\overline{X}^{(1)}$.

Припустимо, що $i > 1$. За припущенням індукції існують цілі числа m і l такі, що $L_m(w) \leqslant l$ для всіх слів $w \in \overline{X}^{(i-1)}$. Ми можемо припускати, що $m \leqslant l$. Нехай $k = l+\sigma$, де величина σ була визначена раніше. Позаяк $m \leqslant l+\sigma$, то маємо $X_m \subset X_{l+\sigma}$ і $L_m \geqslant L_{l+\sigma}$ за лемою 6.6.2(5). Таким чином, ряд L_k є обмеженим на множині $\overline{X}^{(i-1)}$. Залишилося довести, що ряд L_k є обмеженим на множині $\overline{X}^{(i)}$.

Нехай $w \in \overline{X}^{(i)} \setminus \overline{X}^{(i-1)}$. Ми доведемо, що кожен власний префікс u слова w є порівняльним з X_k стосовно префіксного порядку.

Справді, якщо слово u є порівняльним з X стосовно префіксного порядку, то воно є порівняльним з X_k, оскільки $X \subset X_k$. Якщо іншими словами $u \in I(X)$, то слово u має префікс v в множині X. Тоді слово v є власним множником слова w, а отже слова $v \in \overline{X}^{(i-1)}$ і $u \in \overline{X}^{(i-1)} A^*$ є порівняльними з X_k стосовно префіксного порядку за лемою 6.6.8 нижче з $T = \overline{X}^{(i-1)}$. Таким чином, застосувавши лему 6.6.6 з $T = \overline{X}^{(i)} \setminus \overline{X}^{(i-1)}$ і $n = k$, і ми виводимо, що ряд L_k є обмеженим на множині $\overline{X}^{(i)}$. □

Лема 6.6.8. *Нехай $T \subset \overline{X}$ і m, l — два цілих числа таких, що $0 \leqslant m \leqslant l$. Якщо код $X_{l+\sigma}$ не є максимальним і $(L_m, w) \leqslant l$ для довільного слова $w \in T$, то кожне слово в множині TA^* є порівняльним стосовно префіксного порядку із словом у множині $X_{l+\sigma}$.*

Доведення. Визначимо $W_i = P(V_{l+i}) \cap TA^*$ для $i \geqslant 0$. Головний крок полягає в доведенні того, що кожне слово в множині W_σ має деякий префікс у множині $X_{l+\sigma}$.

Для цього, візьмемо слово $v \in W_\sigma$. Позаяк $v \in V_{l+\sigma}$, то маємо $(L_{l+\sigma}, v) = l+\sigma+1$. Нехай $i \in \{0, \cdots, \sigma\}$. Тоді $X_{l+i} \subset X_{l+\sigma}$ і таким чином за лемою 6.6.2(5) маємо, що

$$(L_{l+i}, v) \geqslant (L_{l+\sigma}, v) = l+\sigma+1 \geqslant l+i+1.$$

Таким чином, за лемою 6.6.2(1) існує префікс p_i слова v такий, що $(L_{l+i}, p_i) = l+i+1$, а отже $p_i \in V_{l+i}$. Ми можемо навіть припустити, вибравши найкоротший префікс, що $p_i \in P(V_{l+i})$. Для $i < \sigma$ слово p_i є власним префіксом слова p_{i+1}. Справді, припустивши протилежне, що слово p_{i+1} є префіксом слова p_i, то за твердженням 6.1.8 і лемою 6.6.2(5) отримуємо, що

$$l+i+1 = (L_{l+i}, p_i) \geqslant (L_{l+i}, p_{i+1}) \geqslant (L_{l+i+1}, p_{i+1}) = l+i+2,$$

протиріччя.

Тепер, $v = tu$ для деяких слів $t \in T$ і $u \in A^*$. Ми маємо $l+i+1 > l \geqslant (L_m, t)$ за припущенням в лемі та $(L_m, t) \geqslant (L_{l+i}, t)$ за лемою 6.6.2(5), оскільки $X_m \subset X_{l+i}$. Оскільки $(L_{l+i}, p_i) = l+i+1$, то слово t має бути префіксом слова p_i за твердженням 6.1.8. Отож $p_i \in TA^*$, а отже $p_i \in W_i$.

При пустимо протилежне, що $v \in I(X_{l+\sigma})$. Ми спочатку покажемо, що звідси випливає, що $p_i \in I(X_{l+i})$.

Справді, слово p_i не може мати префікса в множині X_{l+i}, оскільки це слово мало б бути префіксом слова v, а це суперечить припущенню, що слово v не є порівняльним з множиною $X_{l+\sigma}$, яка містить множину X_{l+i}. Далі, припустимо, що слово p_i є префіксом деякого слова $x \in X_{l+i}$. Тоді слово t,яке є префіксом слова p_i є також префіксом слова x. Позаяк слово t є непорівняльним з X, то слово x не міститься в X. Таким чином, за твердженням 6.6.3 маємо, що $(L_{l+i}, x) \leqslant l+i$, звідки випливає за твердженням 6.1.8, що $(L_{l+i}, p_i) \leqslant (L_{l+i}, x) \leqslant l+i$. Але $p_i \in W_i \subset V_{l+i}$, і звідси випливає, що $(L_{l+i}, p_i) = l+i+1$, протиріччя.

Припустимо, що $i < \sigma$. Позаяк слово p_i міститься в $I(X_{l+i})$, то воно міститься в Z_{l+i}. Тепер, $p_i \notin X_{l+i+1}$, оскільки в протилежному випадку слово v має префікс у множині $X_{l+i+1} \subset X_{l+\sigma}$, що суперечить припущенню, що $v \in I(X_{l+\sigma})$. Таким чином, маємо $p_i \in A^-X$, оскільки $Z_{l+i} \setminus A^-X \subset X_{l+i+1}$.

Позаяк слово p_i є власним префіксом слова p_{i+1}, то отримуємо ланцюг σ суфіксів множини X, що суперечить означенню ланцюга σ.

Ми стверджуємо, що $v \notin I(X_{l+\sigma})$, а отже існує деяке слово $x \in X_{l+\sigma}$, яке є порівняльним із словом v. Якщо слово v є префіксом слова x, то $x \notin X$, бо в протилежному випадку слово t є порівняльним з X, суперечачи тому факту, що $t \in T \subset \overline{X}$. З твердження 6.6.3 випливає, що $(L_{l+\sigma}, x) \leqslant l+\sigma$. Тепер отримуємо $(L_{l+\sigma}, v) = l+\sigma+1$, але це суперечить твердженню 6.1.8. Отож, слово x є префіксом слова v. Таким чином, ми довели, що кожне слово в множині W_σ має префікс у множині $X_{l+\sigma}$.

Нехай тепер $w = tu$ — слово з множини TA^* з $t \in T$. За лемою 6.6.2(5) маємо

$$(L_{l+\sigma}, t) \leqslant (L_m, t) \leqslant l < l+\sigma+1.$$

Таким чином, за твердженням 6.1.8 і лемою 6.6.2(2) оскільки код $X_{l+\sigma}$ не є максимальним, то існує деяке слово u', яке є порівняльним зі словом u стосовно префіксного порядку таке, що

$$L_{l+\sigma}(tu') = l + \sigma + 1.$$

Таким чином, $v = tu' \in V_{l+\sigma}$, а отже можна навіть припускати, що $v \in P(V_{l+\sigma})$, і звідси отримуємо, що $v \in W_\sigma$. Як було вже нами доведено, слово v має префікс в множині $X_{l+\sigma}$, а з цього робимо висновок, що слово w є порівняльним зі словом у множині $X_{l+\sigma}$. □

Доведення теореми 6.6.1. За лемою 6.6.7 формальний ряд L_k є обмеженим на множині X для деякого натурального числа k. Таким чином, ми можемо знайти натуральне число l таке, що $k \leqslant l$ і $(L_k, w) \leqslant l$ для довільного слова $w \in \overline{X}$. З леми 6.6.8 та рівності $T = \overline{X}$ випливає, що кожне слово в множині XA^* є порівняльним стосовно префіксного порядку з деяким словом у множині $X_{l+\sigma}$. Нехай $w \in A^*$. Якщо слово w не є порівняльним зі словом у множині X, то воно міститься в множині XA^*, а отже є порівняльним зі словом у множині $X_{l+\sigma}$. Це доводить, що множина $X_{l+\sigma}$ є максимальним біфіксним кодом, який містить код X. Вона є раціональною за лемою 6.6.4, що завершує доведення теореми. □

Наведемо тепер приклад, який може висвітлити попереднє викладено. Нехай $X = X_0 = ba^*bb$. Дерево, яке зображає код X, розглянутий як префіксний код, представлено на рис. 6.17 ліворуч, де значення індикатора на префіксах зображено. Звідси

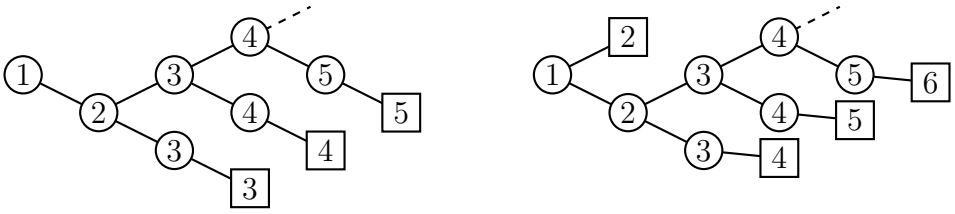


Рис. 6.17: Префіксні коди $X = ba^*bb$ й $\overline{X} = a \cup ba^*ba$.

випливає, що

$$I(X) = aA^* \cup b^2aA^* \cup babaA^* \cup ba^2baA^* \cup \cdots = aA^* \cup ba^*baA^*.$$

Таким чином, отримуємо, що $\overline{X} = a \cup ba^*ba$. Префіксний код $\overline{X}$ зображено на рис. 6.17 праворуч зі значеннями індикатора L_0 на його префіксах. Легко бачити, що за означенням індикатора L_0 маємо

$$(L_0, a) = 2 \qquad \text{і} \qquad (L_0, ba^nba) = n + 4,$$

оскільки слова a і ba^nba не мають множників у коді X. Отже, за твердженням 6.1.8 маємо, що $(L_0, w) \geqslant 2$ для довільного слова w з множини $I(X) = (a \cup ba^*ba)A^*$, і ми з цього виводимо, що $Z_0 = \varnothing$. Таким чином, отримуємо

$$X = X_1 \qquad \text{і} \qquad I(X) = I(X_1).$$

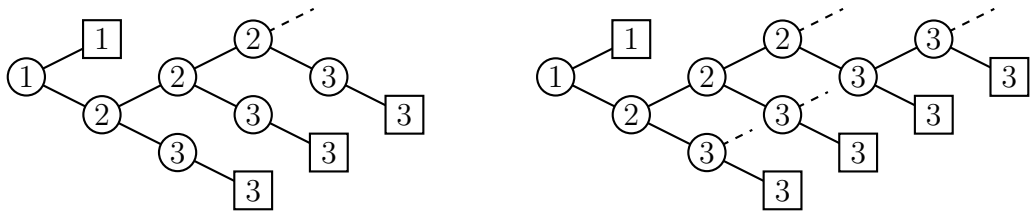


Рис. 6.18: Біфіксні коди $X_2 = a \cup ba^*bb$ і $X_4 = a \cup ba^*ba^*b$.

Тепер єдиним можливим словом у множині $Z_1 = I(X_1) \cap P(V_1)$ є літера a. Отож, маємо $Z_1 = \{a\}$ й $X_2 = X_1 \cup \{a\} = a \cup ba^*bb$, оскільки $a \notin A^-X$ (див. рис. 6.18).

Далі, $I(X_2) = ba^*baA^*$. Маємо

$$(L_2, ba^nba) = n + 4 - (n + 1) = 3,$$

оскільки лише множником слова ba^nba у множині $X2$ є літера a, яка входить $n + 1$ раз. Більше того, $(L_2, ba^nb) = 3$, а отже $ba^nba \notin P(V_2)$, і аналогічно отримуємо, що жодного слова w не міститься в множині $I(X_2)$, що міститься в $P(V_2)$. Звідси випливає, що $Z_2 = \varnothing$ і $X_3 = X_2$.

Тепер маємо

$$Z_3 = P(V_3) \cap I(X_3) = ba^*ba + b.$$

Справді,

$$(L_3, ba^nba^m) = 3 \qquad \text{і} \qquad (L_3, ba^nba^mb) = 4.$$

Таким чином, отримуємо, що

$$X_4 = a \cup ba^*bb \cup ba^*ba^+b = a \cup ba^*ba^*b.$$

Легко перевіряється, що $I(X_4) = \varnothing$, і тому код X_4 є повним справа, а отже є максимальним.

6.7 Вправи до розділу 6

Підрозділ 6.1

В. 6.7.1. Нехай $X \subset A^+$ — біфіксний код і $L = L_X$ — його індикатор. Доведіть, якщо для $u, v \in A^*$ виконується рівність $(L, uvu) = (L, u)$, то $(L, (uv)^m u) = (L, u)$ для всіх невід'ємних цілих m.

В. 6.7.2. Нехай $X \subset A^+$ — біфіксний код і H — підгрупа вільної групи над множиною A, яка породжена кодом X. Доведіть, що такі умови є еквівалентними:

(*i*) мінімальний детермінований автомат вільного моноїда X^* є бідетермінованим;
(*ii*) для довільних слів $t, u, v, w \in A^*$, з умови $tu, vu, vw \in X$ випливає, що $tw \in X$;
(*iii*) $H \cap A^* = X^*$.

В. 6.7.3. Мета цієї вправи — описати метод, який дозволяє декодувати в обох напрямках будь-який скінченний бінарний префіксний код. Нехай X — скінченний префіксний код над алфавітом $\{0, 1\}$, і нехай l — максимальна довжина слів коду X. Розглянемо послідовність $x_1, x_2, \ldots, x_n$ кодових слів. Нехай

$$w = x_1 x_2 \cdots x_n 0^l \oplus 0^l \widetilde{x}_1 \widetilde{x}_2 \cdots \widetilde{x}_n, \tag{6.57}$$

де через $\widetilde{x}$ позначаємо обернене слово до слова x, а через $\oplus$ позначається додавання за $\mod 2$. Доведіть, що слово w можна декодувати в обох напрямках зі скінченною затримкою.

Підрозділ 6.2

В. 6.7.4. Нехай $X \subset A^+$ — тонкий максимальний префіксний код. Для кожного слова $w = a_1 a_2 \cdots a_n \in \overline{F}(X)$ з $a_i \in A$, поставимо у відповідність перетворення ρ_w множини $\{1, 2, \ldots, n\}$.

(1) Доведіть, що для кожного цілого числа $i \in \{1, 2, \ldots, n\}$ існує єдине ціле число $k \in \{1, 2, \ldots, n\}$ таке, що або $a_i a_{i+1} \cdots a_k \in X$ або $a_i a_{i+1} \cdots a_n a_1 \cdots a_k \in X$. Покладемо $\rho_w(i) = k$. Це визначає для кожного слова $w \in \overline{F}(X)$ перетворення ρ_w множини $\{1, 2, \ldots, |w|\}$.
(2) Доведіть, що код X є суфіксним тоді і тільки тоді, коли перетворення ρ_w є ін'єктивним для всіх слів $w \in \overline{F}(X)$.
(3) Доведіть, що код X є повним справа тоді і тільки тоді, коли перетворення ρ_w є сур'єктивним для всіх слів $w \in \overline{F}(X)$.
(4) Виведіть з цього, що тонкий максимальний префіксний код є суфіксним тоді і тільки тоді, коли він є повним зліва (див. доведення твердження 6.2.1.

В. 6.7.5. Нехай $P = \{w\widetilde{w} \colon w \in A^*\}$ — множина *паліндромних* слів парної довжини.

(1) Доведіть, що моноїд P^* є біунітарним. Нехай X — біфіксний код такий, що $X^* = P^*$. Тоді X називається множиною *паліндромних первинних елементів*.
(2) Доведіть, що код X є повним зліва та повним справа.

В. 6.7.6. Доведіть, що два максимальні біфіксні коди, які отримані один від іншого внутрішнім перетворенням, є або обидва розпізнаваними, або обидва не є розпізнаваними.

В. 6.7.7. Доведіть, що максимальний біфіксний код $X \subset A^+$ є груповим тоді і тільки тоді, коли виконується імплікація

$$uv, uw, rv \in X^* \qquad \Longrightarrow \qquad rw \in X^* \tag{6.58}$$

для довільних слів $u, v, w, r \in A^*$.

(Підказка: використайте вправу 6.7.2.)

Підрозділ 6.3

В. 6.7.8. Нехай X — тонкий максимальний код біфіксний код степеня d. Нехай $w \in \overline{H}(X)$ і

$$1 = p_1, p_2, \ldots, p_d$$

– послідовність суфіксів слова w, які є власними префіксами коду X. Покладемо $Y_1 = 1$ і $Y_i = p_i^{-1}X$ для $2 \leqslant i \leqslant d$. Доведіть, що кожна множина Y_i є максимальною префіксною множиною, і тоді множина S власних суфіксів коду X є диз'юнктним об'єднанням множин Y_i (див. теорему 6.3.15).

В. 6.7.9. Нехай X — тонкий максимальний код біфіксний код степеня d і S — множина його власних суфіксів. Доведіть, що існує єдине розбиття множини S на два диз'юнктні об'єднання d префіксних множин Y_i, що задовольняють умови $Y_{i-1} \subset Y_i A^-$ для $2 \leqslant i \leqslant d$.

(Підказка: приймемо $Y_d = S \cap \overline{H}(X)$.)

Підрозділ 6.4

В. 6.7.10. Нехай X — скінченний біфіксний код. Доведіть, використовуючи теорему 6.4.3, що існує розпізнуваний максимальний біфіксний код, який містить код X.

В. 6.7.11. Доведіть, якщо X — розпізнуваний максимальний біфіксний код степеня $d \geqslant 2$, то похідний код є розпізнуваним.

(Підказка: використайте твердження 6.3.14.)

В. 6.7.12. Нехай X — тонкий максимальний біфіксний код степеня $d \geqslant 2$. Нехай $w \in \overline{H}(X)$ і s — найдовший префікс слова w, який є власним суфіксом коду X. Далі, нехай слово x — префікс слова w, який міститься в X. Доведіть, що найкоротше слово з s і x міститься в похідному коді X'.

(Підказка: доведіть, якщо $|x| \geqslant |s|$, то $s \in (HA \setminus H) \cap (AH \setminus H)$, з $H = A^-XA^-$.)

В. 6.7.13. Нехай X_1 і X_2 — два тонких максимальних біфіксних коди, які мають однакові ядра: $K(X_1) = K(X_2)$. Покладемо

$$\begin{aligned} P_1 &= A^* \setminus X_1A^*, \\ P_2 &= A^* \setminus X_2A^*, \\ Z &= (X_1 \cap P_2) \cup (X_1 \cap X_2) \cup (P_1 \cap X_2) \end{aligned}$$

(див. вправу 3.10.8). Доведіть, що множина Z є тонкою, максимальною та біфіксною. Використайте це для для безпосереднього доведення того, що два тонких максимальних біфіксних коди з однаковим ядром і однаковим степенем збігаються. Ця вправа є частковим випадком теореми 6.4.2 у випадку скінченних кодів.

В. 6.7.14. Доведіть, що існує максимальний біфіксний код степеня 3 на алфавіті $\{a, b\}$, який не є раціональним.

(Підказка: виберіть код з нераціональним ядром.)

Підрозділ 6.5

В. 6.7.15. Нехай X — скінченний максимальний біфіксний код. Доведіть, якщо слово $w \in A^+$ задовольняє умову

$$pwq = rws \in X \tag{6.59}$$

для деяких слів $p, q, r, s \in A^+$ і $p \neq r$, то $w \in H(X')$, де X' — похідний код коду X.

(Підказка: почніть зі слова максимальної довжини, що задовольняє умову (6.59), розгляньте слово rwq і використайте твердження 6.3.14.)

В. 6.7.16. Для скінченного коду X покладемо $l(X) = \max\{|x| \colon x \in X\}$. Доведіть, використовуючи вправу 6.7.15, якщо X є скінченним максимальним біфіксним кодом над k-літерним алфавітом, то

$$l(X) \leqslant l(X') + k^{l(X')-1},$$

де через X' позначається похідний код коду X. Позначимо через $\lambda(k, d)$ максимум довжин слів скінченного максимального біфіксного коду степеня d над k-літерним алфавітом. Доведіть, що для для довільного натурального числа $d \geqslant 2$ виконується нерівність

$$\lambda(k, d) \leqslant \lambda(k, d-1) + k^{\lambda(k,d-1)-1}.$$

Порівняйте з обмеженням, заданим теоремою 6.5.2.

В. 6.7.17. Нехай $X \subset A^+$ — скінченний максимальний біфіксний код степеня d. Нехай $a, b \in A$ і визначимо перетворення φ множини $\{0, 1, \ldots, d-1\}$ за формулою

$$a^i b^{d-\varphi(i)} \in X.$$

Доведіть, що відображення φ є бієктивним.

В. 6.7.18. Доведіть, що для кожного натурального числа $k \geqslant 2$ кількість $\beta_k(d)$ скінченних максимальних біфіксних кодів степеня d над k-літерним алфавітом є необмеженою, як функція від змінної d.

В. 6.7.19. Квізістепінь порядку n визначається індукцією наступним чином: квазістепеню порядку 0 є необлямоване слово. Квізістепеню порядку $n+1$ є слово вигляду uvu, де слово u є квізістепеню порядку n. Нехай k — ціле число і α_n — послідовність індуктивно визначена так:

$$\alpha_1 = k + 1, \qquad \alpha_{n+1} = \alpha_n(k^{\alpha_n} + 1) \qquad (n \geqslant 1).$$

Доведіть, що кожне слово над k-літерним алфавітом з довжиною щонайменше α_n має множник, який є квазістепеню порядку n.

В. 6.7.20. Нехай X — скінченний максимальний біфіксний код степеня $d \geqslant 2$ над k-літерним алфавітом. Доведіть, що

$$\max_{x\in X} |x| \leqslant \alpha_{d-1} + 2,$$

де (α_n) — послідовність, визначена у вправі 6.7.19.
(Підказка: використайте вправу 6.7.1.)
Порівняйте з обмеженням, заданим вправою 6.7.16.

В. 6.7.21. Доведіть, що кількість скінченних максимальних біфіксних кодів степеня 4 над дво-літерним алфавітом дорівнює $\beta_2(4) = 73$.

В. 6.7.22. Нехай X — тонкий максимальний біфіксний код степеня d, визначений на k-літерному алфавіті. Нехай S — множина суфіксів коду X і $(U_i)_{1\leqslant i\leqslant d}$ — диз'юнктні максимальні префіксні коди такі, що множина S є їх об'єднанням. Нехай R_i — множина префіксів коду U_i. Означимо $t(z) = \sum_{i=1}^{d} f_{R_i}(z)$. Доведіть, що породжуючий ряд коду X задовольняє умову:

$$f_X(z) - 1 = (kz-1)d + (kz-1)^2 t(z).$$

В. 6.7.23. Нехай X — тонкий максимальний біфіксний код степеня d, визначений на k-літерному алфавіті. Маємо $\frac{1}{k} f'_X(1/k) = d$, де останній вираз можна розглядати як середню довжину слів коду X стосовно рівномірного розподілу Бернуллі. Нагадаємо, що *дисперсія* довжин слів коду X дорівнює середньому квадратичному довжин мінус квадрат середнього значення довжин. Доведіть, що дисперсія визначається за формулою

$$\upsilon_X = 2t(1/k) + d - d^2,$$

де величина $t(z)$ визначена у вправі 6.7.22.

Підрозділ 6.6

В. 6.7.24. Доведіть, якщо X — префіксний код, то $Y = X \cup \overline{X}$ є максимальним префіксним кодом, де через $\overline{X}$ позначається супутник коду X. Доведіть, якщо код X є раціональним, то код Y є також раціональним.

Нотатки до розділу 6

Ідея вивчити біфіксні коди повертає нашу увагу до праць Шютценбергера [179] і Ґілберта та Мура [76]. Ці статті вже містять вагомі результати. Перше систематичне дослідження проводиться в працях Шютценбергера [180] і [181].

Твердження 6.2.1 і 6.2.7 доведено в праці [181]. Внутрішні перетворення вперше зустрічаються в статті Шютценбергера [180]. Той факт, що всі скінченні максимальні біфіксні коди можна отримати з однорідних кодів внутрішніми перетвореннями (теорема 6.5.4), доведено Івом Сезарі в статті [49]. Той факт, що середня довжина тонкого максимального біфіксного коду є цілим числом (наслідок 6.3.16), вже є у Ґілберта та Мура [76]. Це доведено в статті Шютценбергера [180] методами, розробленими в розділі 13. Теорема 6.3.15 й обернене до неї твердження (твердження 6.3.17) з'являються в праці Перрін [157]. Поняття похідного коду належить Сезарі [50].

Результати підрозділу 6.4 є узагальненням результатів стосовно тонких кодів, отриманих Сезарі в праці [50].

Теорема 6.5.2 появляється вже у праці Шютценбергера [180] з іншим доведенням (див. вправу 6.7.20). Інша частина цього розділу належить Сезарі [50]. Перерахування скінченних максимальних біфіксних кодів над дво-літерними алфавітами, було зроблено за допомогою комп'ютера. Перша програма була написана в 1975 році К. Прецетті, з використанням внутрішніх перетворень. Було згенеровано декілька тисяч кодів для $d = 5$. У 1984 році програма, написана М. Леонардом, використовуючи методи наслідку 6.5.8, дала точну кількість скінченних максимальних біфіксних кодів степеня 5 над дво-літерним алфавітом. Це число дорівнює 5 056 783 (див. [125]).

Біфіксні коди та їх розподіл довжин вивчалися з практичною мотивацією під назвою *оборотні коди змінної довжини* (див. [199], [77] і [205]). Твердження 6.5.10 взято з праці [16].

Є гіпотезою, яка називається 3/4-*гіпотезою*, те, що для довільного ряду $f(t) = \sum u_n t^n$ з цілими невід'ємними коефіцієнтами, який задовольняє умову $f(1/k) \leqslant 3/4$, існує біфіксний код X над k-літерним алфавітом такий, що $f_X = f$. Часткові результати розв'язання 3/4-гіпотези викладено в працях [206] і [56].

Теорема 6.6.1 належить Жангу та Шену [207]. Доведення теореми 6.6.1 взято з праці [43].

Код X називається *інфіксним*, якщо жодне слово з X не є власним множником іншого слова в X. Таким чином, інфіксні коди є біфіксними. Інфіксні коди вперше вивчалися в праці [99]. Задача поповнення інфіксного коду була розв'язана Іто та Т'єрреном у праці [100] для скінченних кодів і Ламом у [117] для раціональних кодів.

Вправа 6.7.3 належить [78], див. також монографію [175]. Вправа 6.7.7 зустрічається в статті [130]. Вправи 6.7.9, 6.7.13, 6.7.15 і 6.7.16 взяті з [50], а вправа 6.7.14 зі статті [181].

Розділ 7

Кругові коди

У цьому розділі ми вивчаємо певну сім'ю кодів, які називаються круговими кодами. Основна особливість цих кодів полягає в тому, що вони визначають унікальну факторизацію слів, написаних по колу. Сім'я кругових кодів має численні цікаві властивості. Вони появляються у багатьох проблемах комбінаторики на словах, про декілька з яких ми згадаємо тут.

У підрозділі 7.1 ми даємо означення кругових кодів і описуємо підмоноїд, породжений круговим кодом. Ми також описуємо деякі елементарні властивості кругових кодів. Зокрема, ми охарактеризовуємо максимальні кругові коди (теорема 7.1.10).

У підрозділі 7.2 ми вводимо послідовні уточнення поняття кругового коду. Для цього ми визначаємо поняття (p, q)-граничності. Потім ми переходимо до більш детального вивчення $(1, 0)$-граничних кодів. Зокрема, ми покажемо (твердження 7.2.10), що $(1, 0)$-граничні коди відповідають упорядкованим автоматам. Коди без ком визначаються як кругові коди, що задовольняють найсильнішу можливу умову.

Підрозділ 7.3 стосується розподілу довжин кругових кодів. Доведено дві важливі теореми. Перша дає характеристику послідовностей цілих чисел, які є розподілом довжин кругового коду (теорема 7.3.7). Друга показує, що для кожного непарного цілого числа n існує система представників класів суміжності примітивних слів довжини n, яка є не лише круговою, але навіть кома-вільною (теорема 7.3.11). Доведення цих результатів використовують подібні комбінаторні конструкції. По суті, вони засновані на понятті факторизації вільних моноїдів, яка вивчається в розділі 8.

7.1 Кругові коди

У цьому розділі ми визначаємо нову сім'ю кодів, яка природним чином враховує операцію спряження.

За означенням, підмножина X вільного моноїда A^+ називається *круговим кодом*, якщо для всіх натуральних чисел $n, m \geqslant 1$ та $x_1, x_2, \ldots, x_n \in X$, $y_1, y_2, \ldots, y_m \in X$ і $p \in A^*$, $s \in A^+$, з рівностей

$$sx_2x_3 \cdots x_np = y_1y_2 \cdots y_m, \tag{7.1}$$

$$x_1 = ps \tag{7.2}$$

випливає, що $n = m$, $p = 1$, і $x_i = y_i$ для $1 \leqslant i \leqslant n$ (див. рис. 7.1).

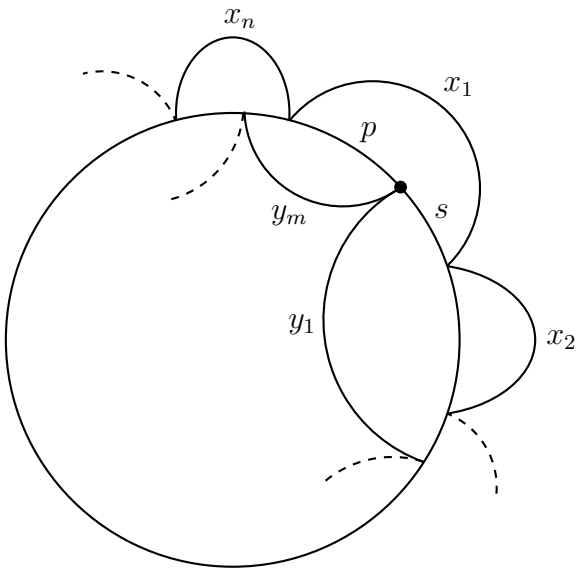


Рис. 7.1: Дві кругові факторизації

Круговий код є очевидно кодом, але як видно з прикладу 7.1.4 обернене твердження є хибним. Асиметрія у означенні лише очевидна і виходить із вибору точки розрізання на колі на рис. 7.1. Очевидно, що будь-яка підмножина кругового коду також є круговим кодом.

Зауважимо, що круговий код X не може містити два різні спряжені слова. Справді, якщо $ps, sp \in X$ з $s, p \in A^+$, то

$$s(ps)p = (sp)(sp).$$

Оскільки X є круговим, то звідси випливає, що $p = 1$, протиріччя. Більше того, всі слова в коді X є примітивними, оскільки припустивши $u^n \in X$ з $n \geqslant 2$, отримуємо

$$u(u^n)u^{n-1} = u^n u^n.$$

Звідси випливає, що $u = 1$ і знову отримуємо протиріччя.

Тепер ми різними способами охарактеризуємо підмоноїди, породжені круговими кодами. Перша характеристика полегшує маніпулювання круговими кодами. Підмоноїд M вільного моноїда A^* називається *чистим*, якщо для всіх слів $x \in A^*$ і довільного натурально числа $n \geqslant 1$ виконується імплікація

$$x^n \in M \qquad \Longrightarrow \qquad x \in M. \tag{7.3}$$

Підмоноїд M вільного моноїда A^* називається *дуже чистим*, якщо для всіх слів $u, v \in A^*$ виконується імплікація

$$uv, vu \in M \qquad \Longrightarrow \qquad u, v \in M. \tag{7.4}$$

Дуже чистий підмоноїд вільного моноїда є чистим. Обернене твердження не виконується (див. приклад 7.1.4).

Твердження 7.1.1. *Підмоноїд вільного моноїда A^* є дуже чистим тоді і лише тоді, коли його мінімальна множина породжуючих елементів є круговим кодом.*

Доведення. Нехай M — дуже чистий підмоноїд вільного моноїда A^*. Ми доведемо, що моноїд M є стійким. Нехай $m, m', xm, m'x \in M$. Тоді поклавши $u = x$, $v = mm'$, маємо $uv, vu \in M$. Звідси випливає, що $x \in M$.

Таким чином, моноїд є M стійким, а отже M є вільним моноїдом. Нехай множина X є його базисом. Припустимо, що виконуються умови (7.1) і (7.1). Покладемо $u = s$ і $v = x_2x_3 \cdots x_np$. Тоді $uv, vu \in M$. Звідси випливає, що $s \in M$. Позаяк $ps, x_2x_3 \cdots x_np \in M$, то зі стійкості моноїда M випливає, що $p \in M$. З $ps \in X$ отримуємо, що $p = 1$. Оскільки множина X є кодом, то звідси випливає, що $n = m$ і $x_i = y_i$ для $i = 1, \ldots, n$.

Навпаки, нехай X — круговий код і покладемо $M = X^*$. Для того, щоб довести, що моноїд M є дуже чистим, розглянемо два непорожніх слова $u, v \in A^+$ такі, що $uv, vu \in M$. Покладемо

$$uv = x_1x_2 \cdots x_n \qquad \text{і} \qquad vu = y_1y_2 \cdots y_m,$$

з $x_i, y_j \in X$. Існує ціле число i з $1 \leqslant i \leqslant n$ таке, що

$$u = x_1x_2 \cdots x_{i-1}p \qquad \text{і} \qquad v = sx_{i+1} \cdots x_n,$$

з $x_i = ps$, $p \in A^*$, $s \in A^+$. Тоді слово vu можна записати двома методами:

$$sx_{i+1} \cdots x_nx_1x_2 \cdots x_{i-1}p = y_1y2 \cdots y_m.$$

Оскільки X круговим кодом, звідси випливає, що $p = 1$ і $s = y_1$. Таким чином, $u, v \in M$, а це доводить, що моноїд M є дуже чистим. □

Приклад 7.1.2. Нехай $A = \{a, b\}$ і $X = a^*b$. Тоді $X^* = A^*b \cup \{1\}$. Отже, якщо $uv, vu \in X^*$, тоді слова su, v є або порожніми або закінчуються літерою b, а отже $u, v \in X^*$. Звідси випливає, що моноїд X^* є дуже чистим і код X є круговим.

Приклад 7.1.3. Нехай $A = \{a\}$ й $X = \{a^2\}$. Підмоноїд X^* вільного моноїда A^* не є, очевидно, чистим. Таким чином, X не є круговим кодом.

Приклад 7.1.4. Нехай $A = \{a, b\}$ і $X = \{ab, ba\}$. Код X не є круговим. Однак, моноїд X^* є чистим (вправа 7.4.1).

Наступне твердження описує квітковий автомат кругового коду.

Твердження 7.1.5. *Нехай $X \subset A^+$ — код і φ — зображення асоційоване з квітковим автоматом коду X. Тоді наступні умови є еквівалентними:*

(i) X є круговим кодом;
(ii) для всіх слів $w \in A^+$, відношення $\varphi(w)$ має щонайбільше одну нерухому точку.

Доведення. Для зручності через 1 ми позначатимемо стан $(1, 1)$ квіткового автомата $\mathcal{A}_D^*(X)$.

$(i) \Rightarrow (ii)$ Нехай $w \in A^+$, і $p = (u, v)$, $p' = (u', v')$ — два стани квіткового автомата $\mathcal{A}_D^*(X)$, які є нерухомими відношення $\varphi(w)$, тобто є такими, що

$$(p, \varphi(w), p) = (p', \varphi(w), p') = 1.$$

Позаяк $w \neq 1$, то з твердження 4.2.3 випливає, що $w \in vX^*u$ і $w \in v'X^*u'$. Таким чином, обидва шляхи $c\colon p \xrightarrow{w} p$ і $c'\colon p' \xrightarrow{w} p'$ проходять через стан 1.

Ми можемо припускати, що $v \leqslant v'$. Нехай $z, t \in A^*$ — слова такі, що $v' = vz$ і $w = vzt$. Тоді шляхи c, c' факторизуються наступним чином

$$c\colon p \xrightarrow{v} 1 \xrightarrow{z} r \xrightarrow{t} p \qquad \text{і} \qquad c'\colon p' \xrightarrow{v} s \xrightarrow{z} 1 \xrightarrow{t} p'.$$

Таким чином, існує два шляхи

$$d\colon 1 \xrightarrow{z} r \xrightarrow{t} p \xrightarrow{v} 1 \qquad \text{і} \qquad d'\colon 1 \xrightarrow{t} p' \xrightarrow{v} s \xrightarrow{z} 1,$$

звідки випливає, що $ztv, tvz \in X^*$. Оскільки моноїд X^* є дуже чисти, то звідси випливає, що $z, tv \in X^*$. Отже, існує шлях

$$e\colon 1 \xrightarrow{z} 1 \xrightarrow{tv} 1.$$

За однозначністю отримуємо, що $d = e$, звідки випливає, що $r = 1$. Таким чином, отримуємо що $1 \xrightarrow{t} p \xrightarrow{vz} 1$, що в порівнянні з d' дає $p = p'$. Це доводить, що відношення $\varphi(w)$ має щонайбільше одну нерухому точку.

$(ii) \Rightarrow (i)$ Нехай $u, v \in A^*$ — слова такі, що $uv, vu \in X^*$. Тоді існують два шляхи

$$1 \xrightarrow{u} p \xrightarrow{v} 1 \qquad \text{і} \qquad 1 \xrightarrow{v} q \xrightarrow{u} 1.$$

Таким чином, відношення $\varphi(uv)$ має дві нерухомі точки, а саме 1 і q. Звідси випливає, що $q = 1$, а, отже, $u, v \in X^*$. □

Тепер ми даємо описання кругових кодів у термінах суміжності. Для цього використовується наступна термінологія.

Нехай $X \subset A^+$ — код. Два слова $w, w' \in X^*$ називаються X-*спряженими*, якщо існують слова $x, y \in X^*$ такі, що

$$w = xy \qquad \text{і} \qquad w' = yx.$$

Слово $x \in X^*$ називається X-*примітивним*, якщо $x = y^n$ з $y \in X^*$ випливає рівність $n = 1$. X-*порядком* слова $x \in X^+$ називається єдине натуральне число $p \geqslant 1$ таке, що $x = y^p$ й y є X-примітивним словом. Нехай $\alpha\colon B \to A^*$ — морфізм кодування для коду X. Легко бачити, що слова $w, w' \in X^*$ є X-спряженими тоді і лише тоді, коли слова $\alpha^{-1}(w)$ і $\alpha^{-1}(w')$ є спряженими словами у вільному моноїді B^*. Так само, слово $x \in X^*$ є X-примітивним тоді і тільки тоді, коли $\alpha^{-1}(x)$ — примітивне слово в B^*.

Таким чином, X-спряження є відношенням еквівалентності на моноїді X^*. Звичайно, два слова в моноїді X^*, які є X-спряженими, є спряженими. Аналогічно, слово в коді X, яке є примітивним, також є X-примітивним. У випадку $X = A$, ми отримуємо звичні поняття спряження та примітивності.

Твердження 7.1.6. *Нехай $X \subset A^+$ — код. Тоді наступні умови є еквівалентними:*

(*i*) *X є круговим кодом;*
(*ii*) *моноїд X^* є чистим і довільні два слова в X^*, які є спряженими, є також X^*-спряженими.*

Доведення. $(i) \Rightarrow (ii)$ Позаяк моноїд X^* є дуже чистим, то він є чистим. Далі, нехай $w, w' \in X^*$ — спряжені слова. Тоді $w = uv$ і $w' = vu$ для деяких літер $u, v \in A^*$. За умовою (7.4) маємо, що $u, v \in X^*$, а це доводить, що слова w і w' є X-спряженими.

$(ii) \Rightarrow (i)$ Нехай $u, v \in A^*$ — слова такі, що $uv, vu \in X^*$. Якщо $u = 1$ або $v = 1$, то $u, v \in X^*$. В іншому випадку, нехай x і y — примітивні слова, які є коренями слова uv і vu: тоді $uv = x^n$ і $vu = y^n$ для деякого натурального числа $n \geqslant 1$. Оскільки моноїд X^* є чистим, то маємо, що $x, y \in X^*$. Далі з рівності $uv = x^n$ отримуємо розклад $x = rs$, $u = x^p r$, $v = sx^q$ для деяких слів $r \in A^*$, $s \in A^+$ і $p+q+1 = n$. Підставивши це в рівність $vu = y^n$ отримуємо, що $y = sr$. Оскільки слова x і y є спряженими, то вони є X-спряженими. Але для примітивних слів x і y існує єдина пара $(r, s') \in A^* \times A^+$ така, що $x = r's'$ і $y = s'r'$. Звідси випливає, що $r, s \in X^*$. Таким чином, $u, v \in X^*$, а це доводить, що моноїд X^* є дуже чистим. □

Твердження 7.1.7. *Нехай $X \subset A^+$ — код і $C \subset A^n$ — клас суміжності, що перетинає вільний моноїд X^* . Тоді*

$$\sum_{m \geqslant 1} \frac{1}{m} \operatorname{Card}(X^m \cap C) \geqslant \frac{1}{n} \operatorname{Card}(C). \tag{7.5}$$

Більше того, нерівність (7.5) справджується тоді і тільки тоді, коли виконуються такі умови:

(i) порядок слів у множині $C \cap X^*$ дорівнює їх X-порядку;
(ii) $C \cap X^*$ є класом X-спряженості.

Доведення. Нехай p — порядок слів у класі суміжності C. Тоді $\operatorname{Card}(C) = n/p$. Множина $C \cap X^*$ є об'єднанням класів X-суміжності. Нехай D — такий клас і покладемо $C' = C \setminus D$. Слова в множини D усі належать до X^k для однакового k, і всі вони мають однаковий X-порядок, скажемо q. Тоді $\operatorname{Card}(D) = k/q$. Позаяк $C = C' \cup D$, то

$$\sum_{m \geqslant 1} \frac{1}{m} \operatorname{Card}(X^m \cap C) = \sum_{m=1}^{n} \frac{1}{m} \operatorname{Card}(X^m \cap C') + \sum_{m=1}^{n} \frac{1}{m} \operatorname{Card}(X^m \cap D).$$

У другій сумі всі доданки зникають, крім $m = k$. Таким чином, маємо, що

$$\sum_{m=1}^{n} \frac{1}{m} \operatorname{Card}(X^m \cap D) = \frac{1}{k} \operatorname{Card}(X^k \cap D).$$

Отож, отримуємо

$$\sum_{m=1}^{n} \frac{1}{m} \operatorname{Card}(X^m \cap C) = \frac{1}{q} + \sum_{m=1}^{n} \frac{1}{m} \operatorname{Card}(X^m \cap C'). \tag{7.6}$$

Позаяк $q \leqslant p$, то маємо $\frac{1}{q} \geqslant \frac{1}{p} = \frac{1}{n} \operatorname{Card}(C)$. Це завершує доведення нерівності (7.5).

Припустимо, що виконуються умови (i) та (ii). Тоді $p = q$ і $D = C \cap X^*$. Таким чином, $C' \cap X^* = \varnothing$. Звідси випливає, що

$$\frac{1}{q} + \sum_{m=1}^{n} \frac{1}{m} \operatorname{Card}(X^m \cap C') = \frac{1}{p},$$

а це доводить, що виконується нерівність (7.5). І навпаки, припускаючи, що виконується нерівність (7.5), з нерівності (7.6) випливає, що

$$\frac{1}{p} = \frac{1}{q} + \sum_{m=1}^{n} \frac{1}{m} \operatorname{Card}(X^m \cap C') \geqslant \frac{1}{q} \geqslant \frac{1}{p},$$

звідки отримуємо, що $p = q$ і $C' \cap X^* = \varnothing$. □

Твердження 7.1.7 має такий наслідок:

Твердження 7.1.8. *Нехай $X \subset A^+$ — код. Тоді наступні умови є еквівалентними:*

(*i*) *X є круговим кодом;*
(*ii*) *для довільного натурального числа $n \geqslant 1$ і для кожного класу суміжності $C \subset A^n$, який перетинає моноїд X^*, виконується рівність*

$$\sum_{m \geqslant 1} \frac{1}{m} \operatorname{Card}(X^m \cap C) = \frac{1}{n} \operatorname{Card}(C). \tag{7.7}$$

Доведення. За твердженням 7.1.6 код X є круговим тоді і тільки тоді, коли виконуються умови:

(*iii*) X є круговим кодом;
(*iv*) два спряжені слова в X^* є X^*-спряженими.

Умова (*iii*) еквівалентна такій: X-порядок довільного слова в моноїд X^* дорівнює його порядку. Отож, код X є круговим тоді і лише тоді, коли для кожен клас суміжності C перетинає моноїд X^*, то маємо

(*v*) порядок слів в $C \cap X^*$ дорівнює їх X-порядку;
(*vi*) $C \cap X^*$ є класом X-суміжності.

З огляду на твердження 7.1.7 умови (*v*) і (*vi*) виконуються тоді і тільки тоді, коли клас суміжності $C \cap A^n$ задовольняє рівність (7.7). Це доводить твердження. □

Ми тепер доведемо результат, який є аналогічний теоремі 2.5.5.

Твердження 7.1.9. *Нехай $X \subset A^+$ — круговий код. Якщо X є максимальним, як круговий код, то X є повним.*

Доведення. Якщо $A = \{a\}$, то $X = \{a\}$. Тому ми припустимо, що $\operatorname{Card}(A) \geqslant 2$. Припустимо, що код X не є повним. Тоді існує слово, нехай це буду w, яке не є множником у моноїді X^*. За твердженням 1.3.6 існує слово $v \in A^*$ таке, що слово $y = wv$ є необлямованим.

Покладемо $Y = X \cup \{y\}$. Ми доведемо, що Y є круговим колом. Для цього, нехай x_i $(1 \leqslant i \leqslant n)$ і y_i $(1 \leqslant i \leqslant m)$ — слова в множині Y, нехай слова $p \in A^*$ і $s \in A^+$ такі, що

$$sx_2x_3 \cdots x_n p = y_1y_2 \cdots y_m \qquad \text{і} \qquad x_1 = ps.$$

Якщо всі слова x_i $(1 \leqslant i \leqslant n)$ містяться в коді X, то також всі слова y_j також містяться в X, оскільки слово y не є множником слова в моноїді X^*. Оскільки код X є круговим, то звідси випливає, що

$$n = m, \qquad p = \varepsilon \qquad \text{і} \qquad x_i = y_i \quad (1 \leqslant i \leqslant n). \tag{7.8}$$

Припустимо, що $x_i = y$ для деякого $i \in \{1, \ldots, n\}$ і припустимо спочатку, що $i \neq 1$. Тоді слово x_i є множником слова $y_1 y_2 \cdots y_m$. Позаяк $y \notin F(X^*)$ і слово y є необлямованим, то звідси випливає, що існує натуральне число $j \in \{1, 2, \ldots, m\}$ таке, що $y_j = y$ та

$$sx_2 \cdots x_{i-1} = y_1 y_2 \cdots y_{j-1} \qquad \text{і} \qquad y_{i+1} \cdots x_n p = y_{j+1} \cdots y_m.$$

Це в свою чергу означає, що

$$sx_2 \cdots x_{i-1} x_{i+1} \cdots x_n p = y_1 y_2 \cdots y_{j-1} y_{j+1} \cdots y_m,$$

і умова (7.8) отримується індукцією по довжині слів.

Розглянемо на завершенні випадок, де $i = 1$, тобто маємо, що $x_1 = y$. Позаяк

$$x_1 x_2 \cdots x_n p = p y_1 y_2 \cdots y_m,$$

то маємо, що

$$y x_2 \cdots x_n p = p y_1 y_2 \cdots y_m.$$

Тепер слово p є суфіксом слова в моноїді Y^*; далі $y \notin F(X^*)$ і слово y є необлямованим. Таким чином, $p = 1$ і $y_1 = y$. Це дає знову умову (7.8) індукцією по довжині слів. Отже, якщо код X не повним, то $Y = X \cup \{y\}$ є круговим кодом. Позаяк $y \notin X$, то X не є максимальним, як круговий код. □

З твердження 7.1.9 і теореми 2.5.13 випливає

Теорема 7.1.10. *Нехай $X \subset A^+$ — тонкий круговий код. Тоді наступні три умови є еквівалентними:*

(*i*) *X є повним;*
(*ii*) *X є максимальним кодом;*
(*iii*) *X є максимальним, як круговий код.*

Зауважимо, що максимальний круговий код $X \subset A^+$ є обов'язково нескінченна, за винятком випадків, коли $X =$. Справді, припустимо, що X є скінченним максимальним круговим кодом. Тоді за теоремою 7.1.10 він є максимальним кодом. За твердженням 2.5.15 існує для кожної літери $a \in A$ натуральне число $n \geqslant 1$ такі, що $a^n \in X$. Оскільки код X є круговим, то ми маємо мати, що $n = 1$, а отже $a \in X$ для всіх $a \in A$. Таким чином, $X = A$.

Нам буде потрібна наступна властивість, яка дозволяє нам будувати кругові коди.

Твердження 7.1.11. *Нехай Y, Z — два композиційовні коди й $X = Y \circ Z$. Якщо Y і Z є круговими, то код X є круговим.*

Доведення. Нехай $\alpha\colon B^* \to A^*$ — морфізм такий, що $X = Y \circ_\alpha Z$. Нехай $u, v \in A^*$ — такі слова, що $uv, vu \in X^*$. Тоді $uv, vu \in Z^*$, звідки випливає, що $u, v \in Z^*$, оскільки моноїд Z^* є дуже чистим. Нехай $s = \alpha^{-1}(u)$, $t = \alpha^{-1}(v)$. Тоді $st, ts \in Y^*$. Оскільки моноїд Y^* є дуже чистим, то $s, t \in Y^*$, доводячи, що $u, v \in X^*$. Таким чином, моноїд X^* є дуже чистим. □

7.2 Граничні коди

Ми вводимо спеціальні сім'ї кругових кодів, які визначаються все більш обмежуваними умовами щодо перекриття між словами. Найбільш особливим сім'єю є коди без ком, що є об'єктом важливої теореми, доведеної в наступному підрозділі.

Let $p, q \geqslant 0$ — два цілі числа. Будемо говорити, що підмоноїд M вільного моноїда A^* задовольняє умову $C(p, q)$, якщо для довільної послідовності $u_0, u_1, \cdots, u_{p+q}$ слів в моноїді A^* з припущень

$$u_{i-1}u_i \in M \qquad (1 \leqslant i \leqslant p+q) \tag{7.9}$$

випливає, що

$$u_p \in M.$$

(див. рис. 7.2). Для прикладу, умова $C(1, 0)$ просто дає імплікацію

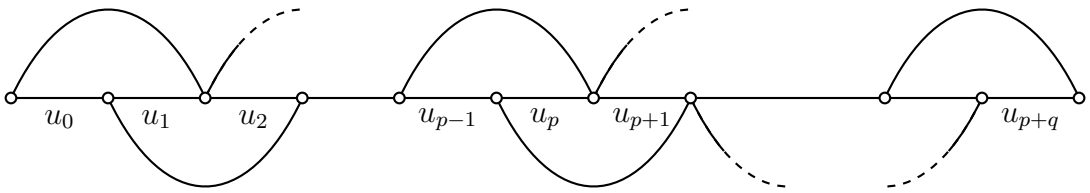


Рис. 7.2: Умова $C(p, q)$ (для p непарних і q парних).

$$uv \in M \qquad \Longrightarrow \qquad v \in M,$$

тобто моноїд M є суфіксно замкненим, а умова $C(1, 1)$ є

$$uv, vw \in M \qquad \Longrightarrow \qquad v \in M.$$

Легко перевірити, що підмоноїд M, який задовольняє умову $C(p, q)$, також задовольняє умови $C(p', q')$ для $p' \geqslant p$ і $q' \geqslant q$.

Твердження 7.2.1. *Нехай $p, q \geqslant 0$ і M — підмоноїд вільного моноїда A^*. Якщо M задовольняє умову $C(p, q)$, то моноїд M є дуже чистим.*

Доведення. Нехай $u, v \in A^*$ — такі слова, що $uv, vu \in M$. Означимо слово u_i $(0 \leqslant i \leqslant p+q)$ дорівнює u, якщо число i є парним, і дорівнює v, якщо число i є непарним. Тоді припущення (7.9) виконується, а отже або слово u, або слово v міститься в моноїді M. Помінявши місцями слова u та v, ми отримуємо обидва слова u та v є елементами моноїда M. □

Нехай M — підмоноїд вільного моноїда A^*, який задовольняє умову $C(p, q)$. За твердженням 7.2.1 моноїд M є дуже чистим. Таким чином, моноїд M є вільним. Нехай X є його базис, тобто є його мінімальною породжуючою множиною. За означенням, будемо називати множину X будемо називати (p, q)-*граничним кодом*. Код X називається *граничним*, якщо існують цілі числа $p, q \geqslant 0$ такі, що код X є (p, q)-граничним.

Твердження 7.2.2. *Кожен граничний код є круговим.*

Приклад 7.2.3. Лише $(0,0)$-граничним кодом над алфавітом A є $X = A$.

Приклад 7.2.4. $(p,0)$-граничний код X є префіксним. Припустимо справді, що код X є $(p,0)$-граничним. Якщо $p = 0$, то $X = A$. В іншому випадку візьмемо $u_0 = \cdots = u_{p-2} = \varepsilon$. Тоді для довільних u_{p-1} та u_p маємо, що

$$u_{p-1}, u_{p-1}u_p \in X^* \qquad \Longrightarrow \qquad u_p \in X^*,$$

що доводить, що моноїд X^* є право унітарним. Аналогічно, $(0,q)$-граничний код є суфіксним. Однак, префіксний код не є завжди граничним, оскільки він навіть не є обов'язково круговим.

Приклад 7.2.5. Код $X = a^*b$ є $(1,0)$-граничним. Він задовольняє навіть сильнішу умову

$$uv \in X \qquad \Longrightarrow \qquad v \in X \cup \{\varepsilon\}.$$

Приклад 7.2.6. Нехай $A = \{a,b,c\}$ й $X = ab^*c \cup \{b\}$. Множина X є біфіксним кодом. Код X не є ні $(1,0)$-граничним, ні $(0,1)$-граничним. Однак код Код X є $(2,0)$-граничним і $(0,2)$-граничним.

Приклад 7.2.7. Нехай $A = \{a_i \colon i \geqslant 0\}$ й $X = \{a_i a_{i+1} \colon i \geqslant 0\}$. Код X є круговим, що легко перевіряється. Однак, код X не є граничним. Справді, покладемо $u_i = a_i$ для $0 \leqslant i \leqslant n$. Тоді $u_{i-1}u_i \in X$ для $i \in \{1,2,\ldots,n\}$, але жодне слово u_i не міститься в моноїді X^*.

Приклад 7.2.7 показує, що обернене до твердження 7.2.2 не виконується в загальному випадку. Однак, таке твердження виконується для скінченних кодів, як це ми побачимо пізніше (теорема 10.2.7). Воно також виконується для розпізнаваних кодів (вправа 7.4.5).

Однією з причин, що робить зручним використання (p,q)-граничних кодів, є те, що вони добре поводяться щодо операції композиція кодів. У наступному твердженні ми не використовуємо позначення $X = Y \circ Z$, оскільки ми не припускаємо, що кожне слово коду Z появляється в слові коду X.

Твердження 7.2.8. *Нехай Z — код над алфавітом A, $\beta \colon B^* \to A^*$ — морфізм кодування для коду Z, і нехай Y — код над алфавітом B. Якщо код Y є (p,q)-граничним і код Z є (r,t)-граничним, то $X = \beta(Y)$ є $(p+r, q+t)$-граничним кодом.*

Доведення. Нехай слова $u_0, u_1, \ldots, u_{p+r+q+t} \in A^*$ є такими, що

$$u_{i-1}u_i \in X^* \qquad (1 \leqslant i \leqslant p+r+q+t). \tag{7.10}$$

Оскільки $X \subset Z^*$ і код Z є (r,t)-граничним, то з властивості (7.10) випливає, що

$$u_r, u_{r+1}, \ldots, u_{r+p+q} \in Z^*. \tag{7.11}$$

Позаяк код Y є (p,q)-граничним, то з (7.11) і (7.10) для $r+1 \leqslant i \leqslant p+q+r$ випливає, що $u_{r+p} \in X^*$. Таким чином, код X є $(p+r, q+t)$-граничним. □

Приклад 7.2.9. Нехай $A = \{a, b, c, d\}$ й $X = \{ba, cd, db, cdb, dba\}$. Тоді

$$X = Z_1 \circ Z_2 \circ Z_3 \circ Z_4,$$

з

$$\begin{aligned} Z_4 &= \{b, c, d, ba\}, \\ Z_3 \circ Z_4 &= \{c, d, ba, db\}, \\ Z_2 \circ Z_3 \circ Z_4 &= \{d, ba, db, cd, cdb\}. \end{aligned}$$

Коди Z_3 і Z_4 є $(0,1)$-граничними. Код $Z_3 \circ Z_4$ не є $(0,1)$-граничним, але він є $(0,2)$-граничним, за погодженням із твердженням 7.2.8. Коди Z_1 і Z_2 є $(1,0)$-граничними. Таким чином, код X є $(2,2)$-граничним. Він не є (p,q)-граничним для довільних (p,q) таких, що $p+q \leqslant 3$, як це показано на рис. 7.3.

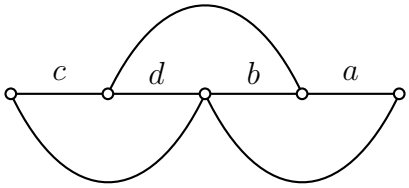


Рис. 7.3: Код X не є (p,q)-граничним для $p+q \leqslant 3$

Тепер ми дамо описання $(1,0)$-граничних кодів за допомогою автоматів. Такі коди зустрічаються в підрозділі 8.2. Для цього будемо говорити, що автомат $\mathcal{A} = (Q, 1, 1)$ є *впорядкованим*, якщо він є детермінованим і якщо виконуються такі умови: Q — частково впорядкована множина, $q \leqslant 1$ для всіх $q \in Q$ і для всіх $p, q \in Q$, і з $a \in A$ та $p \leqslant q$ випливає, що $p \cdot a \leqslant q \cdot a$.

Твердження 7.2.10. *Нехай $X \subset A^+$ — префіксний код. Множина X^* є суфіксно замкненою тоді і тільки тоді, коли моноїд X^* розпізнається деяким впорядкованим автоматом.*

Доведення. Припустимо спочатку, що множина X^* є суфіксно замкненою. Нехай $\mathcal{A}(X^*) = (Q, 1, 1)$ — мінімальний автомат моноїда X^*. Означимо частковий порядок на Q наступним чином:

$$p \leqslant q \qquad \text{тоді і тільки тоді, коли} \qquad L_p \subseteq L_q,$$

де $L_p = \{u \in A^* \colon p \cdot u = 1\}$ для кожного стану p. Це визначає частковий порядок на множині станів Q, оскільки з означення мінімального автомата випливає, що: $L_p = L_q$ тоді і тільки тоді, коли $p = q$. Далі, нехай стан $q \in Q$ і слово $u \in A^*$ є такими, що $1 \cdot u = q$. Тоді $v \in L_q$ тоді і тільки тоді, коли $uv \in X^*$. Позаяк код X є $(1,0)$-граничним, то з $uv \in X^*$ випливає, що $v \in X^*$, або також $v \in L_1$. Таким чином, $L_q \subseteq L_1$, а отже $q \leqslant 1$. Далі, якщо $p, q \in Q$ з $p \leqslant q$, та $a \in A$, нехай $v \in L_{p \cdot a}$. Тоді

$av \in L_p$, таким чином $av \in L_q$, а отже $v \in L_{q\cdot a}$. Це доводить, що $\mathcal{A}(X^*)$ є насправді впорядкованим автоматом для цього часткового порядку.

Навпаки, нехай $\mathcal{A} = (Q, 1, 1)$ — впорядкований автомат, який розпізнає моноїд X^*. Припустимо, що $uv \in X^*$ для деяких слів $u, v \in A^*$. Тоді $1 \cdot uv = 1$. Позаяк $1 \cdot u \leqslant 1$, то маємо $1 \cdot uv \leqslant 1 \cdot v$. Таким чином, отримуємо, що $1 \leqslant 1 \cdot v \leqslant 1$, а отже $1 \cdot v = 1$. Звідки випливає, що $v \in X^*$. □

Приклад 7.2.11. Розглянемо автомат $(Q, 1, 1)$, зображений на рис. 7.4. На множині

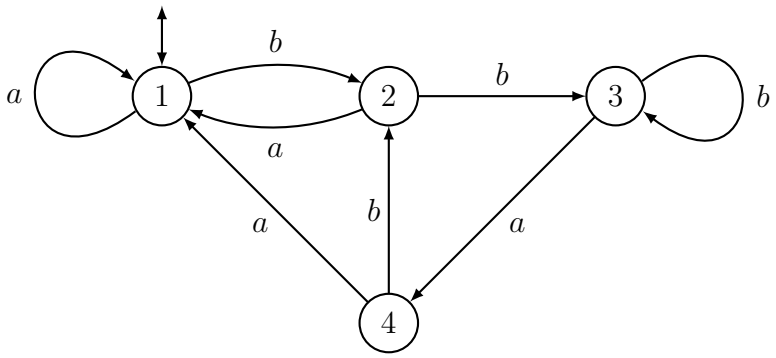


Рис. 7.4: Впорядкований автомат

станів $Q = \{1, 2, 3, 4\}$ означимо частковий порядок так: $3 \leqslant 2 \leqslant 1$ і $4 \leqslant 1$. Для цього часткового порядку, автомат $(Q, 1, 1)$ є впорядкованим. Цей автомат розпізнає підмоноїд X^*, породжений множиною

$$X = (b^2b^*a)^*\{a, ba\}.$$

Звідси випливає, що X є $(1, 0)$-граничним кодом.

Наступне твердження дає інше описання $(1, 0)$-граничних кодів.

Твердження 7.2.12. *Префіксний код $X \subset A^+$ є $(1, 0)$-граничним тоді і лише тоді, коли множина $R = A^* \setminus XA^*$ слів, які не мають префіксів у коді X, є підмоноїдом в A^*.*

Доведення. За твердженням 3.1.6 маємо, що $\underline{A}^* = \underline{X}^*\underline{R}$. Припустимо спочатку, що код X є $(1, 0)$-граничним. Нехай $u, u' \in R$ і покладемо $uu' = xr$ з $x \in X^*$ і $r \in R$. Припустимо протилежне, що $x \neq \varepsilon$. Тоді слово x не є префіксом слова u. Звідси випливає, що $x = uv$ і $vr = u'$ для деякого слова $v \in A^*$. Позаяк код X є $(1, 0)$-граничним, то маємо, що $v \in X^*$, і звідки випливає, що $v = 1$, оскільки слово v є префіксом слова u'. Таким чином $x = u$, отримали протиріччя. Отже, $x = \varepsilon$ та $uu' \in R$.

Навпаки, припустимо, що R є підмоноїдом в A^*. Тоді, будучи префіксно замкненим, R унітарним зліва підмоноїдом. Таким чином, $R = Y^*$ для деякого суфіксного коду Y. З рівняння степеневого ряду отримуємо

$$\underline{A}^* = \underline{X}^*\underline{Y}^*.$$

Домноживши останній вираз на $1 - \underline{Y}$ справа, отримуємо рівність $\underline{X}^* = \underline{A}^* - \underline{A}^*\underline{Y}$. Таким чином, X^* є доповненням лівого ідеалу. Звідси випливає, що моноїд X^* є суфіксно замкненим. Отож, код X є $(1,0)$-граничним. □

Приклад 7.2.13. Код $X = (b^2b^*a)^*\{a, ba\}$ з прикладу 7.2.11 дає, для $R = A^* \setminus XA^*$, підмоноїд $R = \{b, b^2a\}^*$.

Ми закінчуємо цей розділ визначенням сім'ї кодів, яка є найбільш обмежуваною із розглянутих сімей. Підмножина $X \subset A^+$ називається *кодом без ком*, якщо для всіх слів $x \in X^+$, $u, v \in A^*$ виконується умова

$$uxv \in X^* \qquad \Longrightarrow \qquad u, v \in X^*. \tag{7.12}$$

Коди без ком є біфіксними кодами. Це ті коди, з якими найпростіше розшифрувати: якщо в слові $w \in X^*$, деякий множник може бути ідентифікований що він міститься в X, то цей множник є одним із членів єдиної X-факторизації слова w.

Твердження 7.2.14. *Код $X \subset A^+$ є кодом без ком тоді і лише тоді, коли він є (p,q)-граничним для всіх натуральних чисел p, q з $p+q = 3$ з якщо $A^+XA^+ \cap X = \varnothing$. Зокрема, код без ком є круговим.*

Доведення. Спочатку припустимо, що X кодом без ком. Нехай $u_0, u_1, u_2, u_3 \in A^*$ є такими, що u_0u_1, u_1u_2, $u_2u_3 \in X^*$. Якщо $u_1 = u_2 = 1$, то $u_0, u_3 \in X^*$. Інакше $u_1u_2 \in X^+$ і $u_0u_1u_2u_3 \in X^+$. Отже, за властивістю (7.12) отримуємо $u_0, u_3 \in X^*$. Позаяк код X є префіксним, то з $u_0, u_0u_1 \in X^*$ випливає, що $u_1 \in X^*$, і оскільки код X є суфіксним, то з $u_2u_3, u_3 \in X$ випливає, що слово u_2 міститься в моноїді X^*. Таким чином, маємо $u_0, u_1, u_2, u_3 \in X^*$. Отже, код X є (p,q)-граничним для всіх цілих $p, q \geqslant 0$ з $p+q = 3$. Крім того, $A^+XA^+ \cap X = \varnothing$. Справді, припустимо, що $uxv, x \in X$. Тоді за властивістю (7.12) отримуємо $u, v \in X^*$, звідки випливають рівності $u = v = 1$.

Навпаки, нехай слова $u, v \in A^*$ і $x \in X^+$ є такими, що $uxv \in X^*$. Позаяк $A^+XA^+ \cap X = \varnothing$, то існує факторизація $x = ps$ з $p, s \in A^*$ така, що $up, sv \in X^*$. З $up, ps, sv \in X^*$ за граничністю коду X маємо, що $u, p, s, r \in X^*$. Таким чином, виконується властивість (7.12). Останнє висловлення випливає з твердження 7.2.2. □

Твердження 7.2.15. *Нехай X, Z — композиційовні коди й $X = Y \circ Z$. Якщо Y і Z — коди без ком, то X — код без ком.*

Доведення. Нехай $u, v \in A^*$ та $x \in X^+$ — слова такі, що $uxv \in X^*$. Позаяк $X \subset Z^*$, то маємо $uxv \in Z^*$, $x \in Z*+$. Позаяк Z — код без ком, то звідси випливає, що $u, v \in Z^*$. З того, що Y — код без ком, отримуємо, що $u, v \in X^*$. Таким чином X — код без ком за умовою (7.12). □

Приклад 7.2.16. Нехай $A = \{a, b\}$ і $X = \{aab, bab\}$. Слова aab і bab мають єдине тлумачення. Це доводить, що X є кодом без ком.

7.3 Розподіли довжин

Тепер ми вивчаємо розподіли довжин кругових кодів. Нехай X — фіксований круговий код і $(u_n)_{n\geqslant 1}$ — його розподіл довжин. Для кожного натурального числа $n \geqslant 1$ через p_n позначимо кількість слів довжини n, які мають спряження в моноїді X^*.

Покладемо

$$u(z) = \sum_{n\geqslant 1} u_n z^n \qquad \text{і} \qquad p(z) = \sum_{n\geqslant 1} p_n z^n.$$

Таким чином, $u(z) = f_X(z)$ є породжуючим рядом коду X.

Твердження 7.3.1. *Наступні співвідношення виконуються для функцій $u(z)$ і $p(z)$:*

$$\exp \sum_{n\geqslant 1} \frac{p_n}{n} z^n = \frac{1}{1-u(z)}, \tag{7.13}$$

або еквівалентно

$$p(z) = \frac{zu'(z)}{1-u(z)}, \tag{7.14}$$

де через $u'(z)$ позначається похідна функції $u(z)$.

Доведення. Спочатку припустимо, що код X є скінченним.

Нехай $\mathcal{A}$ — квітковий автомат коду X, а N — матриця переходів графа автомата $\mathcal{A}$, тобто $N_{i,j}$ — кількість ребер від i до j в автоматі $\mathcal{A}$. Для кожного натурального числа $n \geqslant 0$ маємо

$$p_n = \mathrm{Tr}(N^n).$$

Справді, $\mathrm{Tr}(N^n) = \sum N^n_{i,i}$ і $N^n_{i,i}$ дорівнює кількості шляхів довжини n з i до i. З огляду на твердження 7.1.5 кожне слово w довжини n, яке має спряжене слово в моноїді X^* є міткою єдиного замкненого шляху в автоматі $\mathcal{A}$. Навпаки, кожен цикл містить початковий стан, а отже його мітка має спряжене слово в моноїді X^*. Це завершує доведення формули.

Тепер використаємо твердження 4.1.6. Присвоївши однаковий символ z для всіх літер рівняння (4.2)), матриця M з рівності (4.2)) стає Nz, а функція $\alpha(\underline{X})$ стає $u(z)$. Таким чином,

$$\det(I - Nz) = 1 - u(z).$$

Нехай $\lambda_1, \cdots, \lambda_k$ — власні значення матриці N, перелічені за їх кратністю. Тоді для кожного натурального числа $n \geqslant 1$, маємо

$$p_n = \mathrm{Tr}(N^n) = \lambda_1^n + \cdots + \lambda_k^n.$$

Далі, за елементарними обчисленнями, для будь-якого комплексного числа λ отримуємо

$$\exp\left(\sum_{n\geqslant 1} \frac{(\lambda z)^n}{n}\right) = \exp\left(\log \frac{1}{1-\lambda z}\right) = \frac{1}{1-\lambda z}.$$

А отже, отримуємо

$$\begin{aligned}\exp\sum_{n\geqslant 1}\frac{p_n}{n}z^n &= \exp\sum_{n\geqslant 1}\frac{\lambda_1^n+\cdots+\lambda_k^n}{n}z^n = \\ &= \exp\sum_{n\geqslant 1}\left(\frac{(\lambda_1 z)^n}{n}+\cdots+\frac{(\lambda_k z)^n}{n}\right) = \\ &= \frac{1}{1-\lambda_1 z}\cdot\ldots\cdot\frac{1}{1-\lambda_k z} = \\ &= \frac{1}{\det(I-Nz)}.\end{aligned}$$

Це доводить рівність (7.13) у випадку скінченних кодів. У загальному випадку для кожного додатнього цілого числа m розглянемо множину слів коду X довжини, що не перевищує m. Позаяк кожне значення p_n залежить лише від перших n членів послідовності (u_n), то рівність (7.13) виконується для всіх цілих, не перевищують числа m. Оскільки це справджується для всіх натуральних чисел m, то формула (7.13) є істинною також для нескінченних кодів.

Формула (7.14) випливає з рівності (7.13) з використанням логарифмічної похідної, тобто шляхом взяття похідних логарифмів. Справді, рівність $S = T$ двох рядів з постійним членом 1 еквівалентна рівності їх логарифмічних похідних. □

Приклад 7.3.2. Розглянемо круговий код $X = \{a, ba\}$ над алфавітом $A = \{a, b\}$. Маємо $u(z) = z + z^2$, а отже за формулою (7.14) отримуємо

$$p(z) = \frac{z+2z^2}{1-z-z^2}.$$

Автомат $\mathcal{A}$ зображено на рис. 7.5. Маємо

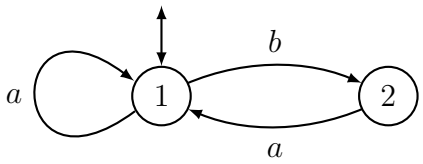


Рис. 7.5: Квітковий автомат кругового коду $X = \{a, ba\}$

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix},$$

а отже

$$\det(I - Mz) = 1 - z - z^2.$$

Власними значеннями матриці M є два корені φ і $\widehat{\varphi}$ многочлена $1-z-z^2$ і $p_n = \varphi^2+\widehat{\varphi}^2$.

За формулою (7.14) маємо $p(z) = zu'(z) + p(z)u(z)$, з якої ми отримуємо таке рекурентне співвідношення для p_n, яке використовується для числових обчислень і воно відоме під назвою *формулв Ньютона*:

$$p_n = nu_n + \sum_{i=1}^{n-1} p_i u_{n-i}. \tag{7.15}$$

Існує також близька формула для p_n. Для кожного цілого числа $i \geqslant 1$ покладемо $u^{(i)} = \left(u_n^{(i)}\right)_{n\geqslant 1}$ — розподіл довжин множини X^i. Еквівалентно, $u_n^{(i)}$ є коефіцієнтом степеня n многочлена $u(z)^i$. Тоді

$$\sum_{n\geqslant 1} \frac{p_n}{n} z^n = \log \frac{1}{1-u(z)} = \sum_{i\geqslant 1} \frac{u^{(i)}(z)}{i}.$$

Таким чином, для кожного цілого числа $n \geqslant 1$ явне значення чисел p_n у термінах чисел $u_n^{(i)}$ є

$$p_n = \sum_{i=1}^{n} \frac{n}{i} u_n^{(i)}.$$

Ми тепер дамо відношення з примітивними намистами. Нехай ℓ_n — кількість примітивних намист довжини n, які перетинають моноїд X^*. Ми почнемо з формули, яка використовується для обчислення чисел ℓ_n.

Твердження 7.3.3. *Для всіх цілих $n \geqslant 1$ виконується рівність*

$$p_n = \sum_{d|n} d\ell_d. \tag{7.16}$$

Доведення. Нехай u — примітивне слово довжини d яке має спряжене в моноїді X^*. Кожна степінь v слова u має рівно два d різних спряжень і має спряжене в моноїді X^*. Навпаки, нехай слово v має спряження v' в моноїді X^*, нехай u — єдине примітивне слово таке, що v' міститься в u^+. Оскільки моноїд X^* є чистим, то слово u міститься в X^*, а отже v само є степенем примітивного слова, яке має спряжене в моноїді X^*. Це доводить формулу (7.16). □

Використовуючи формулу Мьобіуса оберненого перетворення (твердження 1.3.4), ми отримуємо явну формулу

$$\ell_n = \frac{1}{n} \sum_{d|n} \mu(n/d) p_d.$$

Наступне твердження встановлює прямий зв'язок між послідовностями (u_n) і (ℓ_n).

Твердження 7.3.4. *Виконується таке співвідношення:*

$$\frac{1}{1-u(z)} = \prod_{n\geqslant 1} \frac{1}{(1-z^n)^{\ell_n}}. \tag{7.17}$$

Доведення. Оскільки для кожного натурального числа n виконується рівність

$$\frac{p_n}{n} = \sum_{d|n} \frac{d\ell_d}{n},$$

то маємо

$$\sum_{n\geqslant 1} \frac{p_n}{n} z^n = \sum_{d,k\geqslant 1} \ell_d \frac{z^{dk}}{k} = \sum_{d\geqslant 1} \ell_d \log \frac{1}{1-z^d} = \sum_{n\geqslant 1} \log \frac{1}{(1-z^n)^{\ell_n}}.$$

Взявши експоненту від обох боків рівності, отримуємо

$$\exp \sum_{n\geqslant 1} \frac{p_n}{n} z^n = \prod_{n\geqslant 1} \frac{1}{(1-z^n)^{\ell_n}}. \tag{7.18}$$

Складаючи разом формули (7.13) і (7.18), отримуємо формулу (7.17). □

З огляду на ряд $u(z) = \sum u_n z^n$, рівняння (7.14) визначає безпосередньо ряд $p(z)$, а рівняння (7.16) дозволяє обчислити послідовність (ℓ_n). Вони взагалі еквівалентні рівнянню (7.17). Щоб підкреслити ці залежності, ми пишемо $\ell_n(u)$ і $p - n(u)$ для послідовностей, заданих змінною u.

У спеціальному випадку ряду $u(z) = kz$ пишемо $\ell_n(k)$ замість $\ell_n(u)$. Це узгоджується з розділом 1 де через $\ell_n(k)$ позначається кількість примітивних намист довжиною n на k символах. Очевидно, що послідовність $(\ell_n(k))_{n\geqslant 1}$ відповідає коду $X = A$, і в цьому випадку тотожність (7.17) має вигляд

$$\frac{1}{1-kz} = \prod_{n\geqslant 1} \frac{1}{(1-z^n)^{\ell_n(k)}}. \tag{7.19}$$

Можна довести, якщо $u_n \leqslant v_n$ для всіх натуральних чисел n, то $\ell_n(u) \leqslant \ell_n(v)$ для всіх натуральних чисел n (вправа 7.4.9).

Приклад 7.3.5. Розглянемо знову круговий код $X = \{a, ab\}$ над алфавітом $A = \{a, b\}$. Маємо $u(z) = z + z^2$ і

$$p(z) = \frac{z + 2z^2}{1 - z - z^2}.$$

Перші значення p_n і ℓ_n наведено в таблиці 7.1.

n	1	2	3	4	5	6	7
p_n	1	3	4	7	11	18	29
ℓ_n	1	1	1	1	2	2	4

Табл. 7.1: Значення p_n і ℓ_n для коду $X = \{a, ab\}$

Тепер ми опишемо розподіли довжин кругових кодів.

Для цього, будемо говорити, що скінченна або нескінченна послідовність $(x_i)_{i\geqslant 1}$ слів у вільному моноїді A^+ є послідовністю Холла над алфавітом A, якщо вона отримується наступним чином:

Нехай $X_1 = A$. Тоді x_1 — довільно вибране слово в X_1. Якщо x_i та X_i визначені, то покладемо X_{i+1} визначається за формулою

$$X_{i+1} = x_i^*(X_i \setminus \{x_i\}),$$

і слово x_{i+1} — довільно вибраний елемент в коді X_{i+1}, який задовольняє умову

$$|x_{i+1}| \geqslant |x_i|.$$

Послідовність $(X_i)_{i\geqslant 1}$ називається послідовністю кодів, *асоційованих* із послідовністю $(x_i)_{i\geqslant 1}$.

Твердження 7.3.6. *Нехай $(x_i)_{i\geqslant 1}$ — послідовність Холла над алфавітом A та $(X_i)_{i\geqslant 1}$ — асоційована послідовність кодів. Тоді:*

(*i*) *для довільного натурального числа $i \geqslant 1$ кожен код X_i є $(i-1,0)$-граничним кодом;*

(*ii*) *кожне примітивне слово w таке, що $|w| > |x_i|$ має спряжене слово в моноїді X_{i+1}^*.*

Доведення. (*i*) Код $X_1 = A$ є $(0,0)$-граничним. Далі

$$X_{i+1} = T \circ X_i,$$

де T — код вигляду $b^*(B \setminus \{b\})$. Очевидно, що код T є $(1,0)$-граничним. Припустивши за індукцією, що X_i є $(i-1,0)$-граничним, отримуємо, що наше висловлення випливає з твердження 7.2.8.

(*ii*) Означимо $x_0 = 1$. Доведемо, що твердження істинним для всіх цілих чисел $i \geqslant 0$ індукцією по i. Для випадку $i = 0$ просто маємо, що будь-яке примітивне слово міститься у вільному моноїді A^*. Отже припускаємо, що $i \geqslant 1$, і нехай $w \in A^+$ — примітивне слово довжини $|w| > |x_i|$. Позаяк $|x_i| \geqslant |x_{i-1}|$, то маємо $|w| > |x_{i-1}|$. За припущенням індукції існує слово w', спряжене до слова w, яке міститься в моноїді X_i^*. Слово w' не міститься в моноїді x_i^*, оскільки слово w' примітивним і $|w'| > |x_i|$. Отже слово w' розкладається в добуток $w' = uxv$ для деяких $u, v \in X_i^*$ і $x \in X_i \setminus \{x_i\}$. Тоді спряжене слово $w'' = vux$ до слова w' міститься в $X_i^*(X_i \setminus \{x_i\}) \subset X_{i+1}^*$. Таким чином, спряжене слово до слова w міститься в моноїді X_{i+1}^*. □

Теорема 7.3.7. *Послідовність $u = (u_n)_{n\geqslant 1}$ є розподілом довжини кругового коду над k літерами тоді і лише тоді, коли $\ell_n(u) \leqslant \ell_n(k)$ для всіх натуральних чисел $n \geqslant 1$.*

Доведення. Нехай A — алфавіт з k літерами й X — круговий код з розподілом довжин $u = (u_n)$. Позаяк величина $\ell_n(u)$ дорівнює кількості примітивних намист довжини n, які перетинають моноїд X^*, то маємо $\ell_n(u) \leqslant \ell_n(k)$.

Для доведення оберненого твердження, побудуємо послідовність Холла. Зробимо це індукцією, припустимо визначено ціле число $m = m(n)$ та послідовність Холла $x_1, \ldots, x_m$ слів довжини не більше за n з послідовністю $X_1, \ldots, X_m$ асоційованих кодів, а отже з $X_{i+1} = x_i^*(X_i \setminus \{x_i\})$ такі, що розподіл довжин коду X_m збігається з послідовністю u на n перших членах. Позначимо для зручності $Y_n = X_{m(n)}$. Отже, поклавши $v_i = \mathrm{Card}(Y_n \cap A_i)$, маємо $v_i = u_i$ для $1 \leqslant i \leqslant n$. Ми доведемо, що

$$v_{n+1} - u_{n+1} = \ell_{n+1}(k) - \ell_{n+1}(u). \tag{7.20}$$

Приймемо це рівняння як належне. Покладемо $r = v_{n+1} - u_{n+1}$. Позаяк $0 \leqslant r$ ми можемо вибрати r слів $x_{m+1}, \ldots, x_{m+r}$ довжини $n+1$ в множині $Y_n = X_m$ для продовження побудови послідовності Холла для r кроків. У цьому випадку послідовність $x_1, \cdots, x_m, x_{m+1}, \ldots, x_{m+r}$ утворює загалом послідовність Холла. Поклавши $m(n+1) = m+r$, отримуємо код $Y_{n+1} = X_{m(n+1)}$ задовольняє рівність $\mathrm{Card}(Y_{n+1} \cap A_i) = u_i$ для $1 \leqslant i \leqslant n+1$. Це є очевидним для $i \leqslant n$. Далі, множина $Y_{n+1} \cap A_{n+1}$ отримується з $Y_n \cap A_{n+1}$, видаляючи r слова довжиною $n+1$. Це завершує індукцію, починаючи з $Y_0 = A$.

Тепер доведемо рівність (7.20). Позаяк $u_i = v_i$ для $i = 1, \ldots, n$, то за рівністю (7.15) маємо, що $p_i(u) = p_i(v)$ для $i = 1, \ldots, n$. Отже, знову за за рівністю (7.15) отримуємо, що

$$p_{n+1}(v) - p_{n+1}(u) = (n+1)(v_{n+1} - u_{n+1}).$$

Рівність (7.16) і рівності, доведені вище, показують, що $\ell_i(u) = \ell_i(v)$ для $i = 1, \ldots, n$. Звідси випливає, що

$$p_{n+1}(v) - p_{n+1}(u) = (n+1)(\ell_{n+1}(v) - \ell_{n+1}(u)),$$

що в свою чергу показує, що

$$\ell_{n+1}(v) - \ell_{n+1}(u) = v_{n+1} - u_{n+1}.$$

Позаяк $|x_m| \leqslant n$, то властивість послідовностей, викладена в твердженні 7.3.6(*ii*) стверджує, що кожне примітивне намисто довжини $n+1$ перетинає код X_m^*. Таким чином, $\ell_{n+1}(v) = \ell_{n+1}(k)$. Це доводить рівність (7.20). □

Приклад 7.3.8. Нехай $A = \{a, b\}$ і $u = (0, 1, 1, 3, \ldots)$. Конструкція доведення теореми 7.3.7 дає

$$\begin{aligned} X_1 &= \{a, b\}; \\ X_2 &= \{b, ab, aab, aaab, \ldots\}; \\ X_3 &= \{ab, aab, abab, aaab, baab, bbab, \ldots\}; \\ X_4 &= \{ab, bab, aaab, baab, bbab, \ldots\}, \end{aligned}$$

що відповідає послідовності Холла $x_1 = a$, $x_2 = b$, $x_3 = aab$. З цього отримуємо $Y_1 = X_3$ та $Y_2 = Y_3 = X_4$.

У таблиці 7.2 зображено покомпонетні максимальні розподіли довжин бінарних кругових кодів довжини, що не перевищує 4. Цей список викладений у спадному лексикографічному порядку. Останній стовпчик дає круговий код, який має зазначений розподіл побудований з використанням методу доведення теореми 7.3.7.

Наслідок 7.3.9. *Нехай A — алфавіт з $k \geqslant 1$ літерами. Для всіх натуральних чисел $m \geqslant 1$ існує круговий код $X \subset A^m$ такий, що* $\mathrm{Card}(X) = \ell_m(k)$.

Доведення. Нехай $u = (u_n)_{n \geqslant 1}$ — послідовність з усіма членами нулями, за вийнятком u_m, який дорівнює $\ell_m(k)$. За рівностями (7.15) і (7.16) маємо, що $\ell_n(u) = 0$ для $1 \leqslant n \leqslant m-1$ і $\ell_m(u) = u_m$. Отже, $\ell_n(u) \leqslant \ell_n(k)$ для $1 \leqslant n \leqslant m$. Згідно з доведенням теореми 7.3.7, цього достатньо, щоб забезпечити існування кругового коду X, що має слова u_m довжини m. Таким чином, множина $X \cap A^m$ задовольняє твердження. □

2	0	0	0	a, b
1	1	1	1	b, ab, a^2b, a^3b
1	1	0	0	b, ab, a^3b, a^2b^2
1	0	2	1	b, ab^2, a^2b, a^3b
1	0	1	2	b, a^2b, a^3b, ab^3
1	0	0	3	b, a^3b, ab^3, a^2b^2
0	1	2	3	$ab, a^2b, bab, a^3b, ba^2b, b^2ab$

Табл. 7.2: Список покомпонетних максимальних розподілів довжин бінарних кругових кодів довжини, що не перевищує 4

Наслідок 7.3.9 можна сформулювати так: *Можна вибрати систему X з представників примітивних класів суміжності слів довжиною m таким чином, що X — круговий код.* Наступний приклад дає більш точне описання таких кодів для $m = 2$.

Приклад 7.3.10. Нехай X — підмножина в $A^2 \setminus \{a^2 \colon a \in A\}$ і θ — відношення на алфавіті A, визначене так: $a\theta b$ тоді і тільки тоді, коли $ab \in X$. Тоді X є круговим кодом тоді і тільки тоді, коли рефлексивне та транзитивне замикання θ^* відношення θ є відношенням порядку.

Справді, припустимо спочатку, що θ^* не є частковим порядком. Тоді

$$a_1a_2, a_2a_3, \ldots, a_{n-1}a_n, a_na_1 \in X$$

для деяких натурального числа $n \geqslant 1$ і $a_1, \ldots, a_n \in A$. Якщо число n є парним, то поклавши $u = a_1$, $v = a_2 \cdots a_n$, маємо $uv, vu \in X^*$ й $u \notin X^*$. Якщо число n є непарним, то $(a_1a_2 \cdots a_n)^2 \in X^*$, але $a_1a_2 \cdots a_n \in X^*$. Отже, код X не є круговим.

Навпаки припустимо, що θ^* є частковим порядком на алфавіті A. Тоді A можна впорядкувати таким чином, що

$$A = \{a_1, a_2, \ldots, a_k\} \qquad \text{і} \qquad a_i\theta a_j \Longrightarrow i < j.$$

Тоді $X \subset \{a_ia_j \colon i < j\}$, і з огляду на приклад 7.2.7 множина X є круговим кодом.

Коди $X \subset A^m$ в наслідку 7.3.9 є круговими. Наступна теорема стверджує, що при непарному m код X може бути навіть обраний, як код без ком.

Теорема 7.3.11. *Для довільного алфавіту A з k літерами та для кожного непарного числа $m \geqslant 1$ існує код без ком $X \subset A^m$ такий, що*

$$\operatorname{Card}(X) = \ell_m(k).$$

З прикладу 7.3.10 випливає, що круговий код $X \subset A^2$ з $\ell_2(k) = k(k-1)/2$ елементами має вигляд $X = \{a_ia_j \colon i < j\}$ для деякої нумерації алфавіту A. Для $k = 4$ і $A = \{a, b, c, d\}$ отримуємо код $X = \{ab, ac, ad, bc, cd, bd\}$. Цей код не є кодом без ком, оскільки слово $abcd$ має факторизації $(ab)(cd)$ і $a(bc)d$. Отже, такий результат, як теорема 7.3.11 не виконується для парних цілих чисел m.

Для доведення теореми 7.3.11 ми побудуємо послідовність Холла $(x_i)_{i\geqslant 1}$ і послідовність $(X_i)_{i\geqslant 1}$ асоційованих кодів, поклавши

$$X_1 = A, \qquad X_{i+1} = x_i^*(X_i \setminus \{x_i\}), \qquad (i \geqslant 1), \tag{7.21}$$

де x_i — елемент коду X_i мінімальної непарної довжини. За побудовою $(x_i)_{i\geqslant 1}$ є насправді послідовністю Холла. Покладемо

$$U = \bigcup_{i\geqslant 1} X_i, \qquad Y = U \cap (A_2)^* \qquad \text{і} \qquad Z = U \cap A(A^2)^*.$$

Отже Y є множиною слів парної довжини в U та

$$Z = \{x_j \colon i \geqslant 1\}.$$

Для кожного слова $u \in U$ означимо

$$\nu(u) = \min\{i \in \mathbb{N} \colon u \in X_i\} - 1,$$
$$\delta(u) = \sup\{i \in \mathbb{N} \colon u \in X_i\}.$$

Таким чином, $\nu(u)$ позначає останній крок, перш ніж слово u появляється в деякому коді X_i, а $\delta(u)$ — останній раз, коли слово u появляється в деякому коді X_i. Зауважимо, що $Y = \{u \in U \colon \delta(u) = +\infty\}$. Далі, зауважимо, що $\delta(x_i) = i$, і якщо $\nu(u) = q$ для деякого слова $u \in U \setminus A$, то $u \in X_{1+q}$ і $u \notin X_q$. Отже, $u = x_q v$ для деякого слова $v \in X_{q+1}$. Далі для всіх $u \in U$ та $n \geqslant 1$ маємо

$$\nu(u) \leqslant n < \delta(u) \qquad \Longrightarrow \qquad x_n u \in U. \tag{7.22}$$

Доведемо пословністю лем, що для будь-якого непарного цілого числа m для коду $Z \cap A^m$ справджується твердження теореми 7.3.11.

Лема 7.3.12. *Для всіх непарних натуральних чисел m виконується рівність*

$$\mathrm{Card}(Z \cap A^m) = \ell_m(k).$$

Доведення. Нехай n — найменше натуральне число таке, що $|x_n| = m$. Нехай u — розподіл довжин коду X_n. Тоді за побудовою послідовності Холла (x_i) маємо

$$Z \cap A^m = \{x_n, x_{n+1}, \ldots, x_{n+p}\}$$

для деякого натурального числа p. Тоді $Z \cap A^m = X_n \cap A_m$, оскільки для всіх натуральних $k \geqslant 1$ слова в коді X_{n+k}, які не є в коді X_n мають довжину строго більшу за $|x_n|$. Таким чином, $\mathrm{Card}(Z \cap A^m) = u_m$.

Далі, за означенням числа n маємо $m > |x_{n-1}|$. За твердженням 7.3.6(ii) кожне примітивне слово довжини m має спряжене слово в X_n^*. Таким чином, отримуємо рівність $\ell_m(u) = \ell_m(k)$.

Нехай D — множина непарних чисел d таких, що $1 \leqslant d \leqslant m-2$. За побудовою послідовності Холла маємо, що $u_d = 0$ для кожного числа $d \in D$. Ми доведемо індукцією по d, що $p_d(u) = 0$ для $d \in D$. Ця рівність виконується для $d = 1$, оскільки $p_1 = u_1 = 0$. За рівністю (7.15) маємо

$$p_d = du_d + \sum_{i=1}^{d-1} p_i u_{d-i}.$$

Кожен член справа даної рівності дорівнює, оскільки $u_d = 0$ і або $p_i = 0$, або $u_{d-i} = 0$ оскільки i або $d-i$ є непарним. Таким чином, $p_d = 0$. Отже, за рівністю (7.16) маємо $\ell_d(u) = 0$ для $d \in D$, і на завершенні отримуємо $p_m(u) = mu_m$ і $\ell_m(u) = u_m$.

Ми отримуємо, таким чином, рівність $\mathrm{Card}(Z \cap A^m) = \ell_m(k)$. □

Лема 7.3.13. *Для кожного слова $w \in A^*$ існує єдина його факторизація*

$$w = yz_1z_2\cdots z_n \tag{7.23}$$

з $y \in Y^*$, $z_i \in Z$, $n \geqslant 0$ і $\delta(z_1) \geqslant \delta(z_2) \geqslant \cdots \geqslant \delta(z_n)$.

Доведення. Спочатку покажемо, що для кожного натурального числа $n \geqslant 1$ виконується рівність

$$X_n^* = X_{n+1}^* x_n^*.$$

Справді, за означенням маємо, що $X_{n+1} = x_n^*(X_n \setminus \{x_n\})$. Добуток вільного моноїда x_n^* з множиною $X_n \setminus \{x_n\}$ є однозначним, оскільки множина X_n є кодом. Таким чином, в термінах формальних степеневих рядів маємо

$$\underline{X_{n+1}} = x_n^*(\underline{X_n} - x_n). \tag{7.24}$$

Тому, отримуємо, що $\underline{X_{n+1}} = x_n^*\underline{X_n} - x_n^+$ і

$$\underline{X_{n+1}} - 1 = x_n^*\underline{X_n} - x_n^* = x_n^*(\underline{X_n} - 1).$$

Формула (7.24) випливає за інверсією.

Після послідовних підстановок у формулі (7.24), починаючи з $A^* = X_1^*$, отримуємо для всіх натуральних чисел $n \geqslant 1$ рівність

$$\underline{A^*} = \underline{X_{n+1}}^* x_n^* x_{n-1}^* \cdots x_1^*. \tag{7.25}$$

Тепер, нехай $w \in A^*$ і покладемо $p = |w|$. Нехай n — ціле число таке, що множина X_{n+1} не містить слів непарної довжини $\leqslant p$. З рівністю (7.25) існує факторизація слова w, як

$$w = yz_1z_2\cdots z_k$$

з $\delta(z_1) \geqslant \delta(z_2) \geqslant \cdots \geqslant \delta(z_k)$, $z_i \in Z$ і $y \in X_{n+1}^*$. Позаяк $|y| \leqslant p$, то з вибору числа n випливає, що y є добутком слів в множині X_{n+1} парної довжини. Звідси випливає, що $y \in Y^*$. Це доводить існування одної факторизації (7.23). Припустимо, що існує друга факторизація такого ж типу, скажемо нехай,

$$w = y'z_1'z_2'\cdots z_n'.$$

Нехай m — ціле число, більшим за $\delta(z_1)$ і $\delta(z_1')$, і є досить великим, щоб забезпечити умову $y, y' \in X_{m+1}^*$. Такий вибір є можливим, оскільки всі парні слова деякого коду X_l містяться також в кодах $X_{l'}$, для $l' \geqslant l$. Тоді за рівністю (7.25) обидві факторизації слова w однакові. □

Тепер ми охарактеризуємо послідовно форму факторизації (7.23), для слів, що є префіксами, і для слів, які є суфіксами слів у множині U.

Лема 7.3.14. *Для кожного власного префікса w слова в множині U існує факторизація (7.23) з $y = 1$.*

Доведення. Кожен з кодів X_n є максимальним префіксним кодом. Це випливає з багатократного застосування твердження 3.4.13. Отже, для натурального числа n, маємо

$$\underline{A^*} = \underline{X_{n+1}^*}\underline{P_{n+1}},$$

де $P_{n+1} = X_{n+1}A^-$ — множина власних префіксів слів коду X_{n+1}. Порівнюючи це рівняння з рівністю (7.25), отримуємо

$$P_{n+1} = x_n^* x_{n-1}^* \cdots x_1^*. \tag{7.26}$$

Нехай тепер w — власний префікс деякого слова u в множині U. Тоді $u \in X_{n+1}$ для деякого натурального числа n, а отже отримуємо $w \in P_{n+1}$. За рівнянням (7.25) слово w допускає факторизацію бажаної форми. □

Лема 7.3.15. *Для всіх натуральних чисел $n, p \geqslant 1$, маємо $x_n x_{n+p} \in Y^*$. Більше того, $zy \in Y^*Z$ для $z \in Z$ і $y \in Y$.*

Доведення. Першу формулу доведемо індукцією. Для $p = 1$ маємо $\nu(x_{n+1}) \leqslant n$, оскільки $x_{n+1} \in X_{n+1}$. Таким чином, врахувавши формулу (7.22) маємо, що $x_n x_{n+1} \in U$. Позаяк слово $x_n x_{n+1}$ має парну довжину, то $x_n x_{n+1} \in Y$.

Припустимо, що властивість виконується для всіх натуральних чисел, які не перевищують $p-1$, і покладемо $q = \nu(x_{n+p})$. Розрізняємо два випадки. Спочатку припустимо, що $q \leqslant n$. Тоді за імплікацією (7.22), коли x_{n+p} відіграє роль слова u, маємо $x_n x_{n+p} \in U$. Це слово має парну довжину. Отже, $x_n x_{n+p} \in Y$.

Далі припустимо, що $n \leqslant q$. Тоді $x_{n+p} \in U \setminus A$. Отже, $x_{n+p} = x_q u$ для деякого слова $u \in U$. Позаяк $q \leqslant n + p = \delta(x_{n+p})$, то маємо $x_n x_q \in Y^*$ за припущенням індукції. Далі слово u має парну довжину (оскільки числа $|x_n|$ і $|x_q|$ є обидва непарними). Таким чином, $u \in Y$, звідки випливає, що $x_n x_{n+p} \in Y^*$.

Тепер доведемо другу властивість. Покладемо $n = \delta(Z)$ і $q = \nu(y)$. Тоді $z = x_n$ і $y = x_q x_t$ для деякого натурального числа t. Якщо $n \leqslant q$, то $x_n x_q \in Y^*$ за попередніми аргументами, а отже $zy \in Y^*Z$. Припустимо протилежне, що $q \leqslant n$. Тоді за імплікацією (7.22) маємо $x_n x_q x_t = x_n y \in U$. Оскільки це слово має непарну довжину, то воно міститься в Z. □

Лема 7.3.16. *Будь-який суфікс w слова в U допускає факторизацію (7.23) з $n = 0$ або $n = 1$.*

Доведення. Для довільного вибраного слова $u \in U$, ми доведемо, що всі його суфікси містяться в $Y^*Z \cup Y^*$, індукцією по його довжині $|u|$. Випадок $|u| = 1$ є очевидним, і очевидно, що достатньо довести, твердження індукції для власних суфіксів слів у множині U.

Припустимо, що $|u| \geqslant 2$. Покладемо $n = \nu(u)$. Позаяк $u \in U \setminus A$, то маємо $u = x_n u'$ для деякого слова $u' \in U$.

Нехай w — власний правий множник слова u. Якщо слово w є суфіксом слова u', тоді за припущенням індукції слово w міститься в $Y^*Z \cup Y^*$. Отже, припустимо, що $w = w'u'$, з w' власним суфіксом слова x_n. За індукцією, слово w' міститься в множині $Y^*Z \cup Y^*$. Якщо $w' \in Y^*$, то $w'u' \in\in Y^*(Y \cup Z)$, і твердження індукції доведено. Таким чином, залишився випадок, коли $w' \in Y^*Z$. У цьому випадку, покладемо $w' = yx_k$ з $y \in Y^*$, $k \geqslant 1$. Зауважимо, що $k \leqslant n$, оскільки $|x_k| \leqslant |w'| \leqslant |x_n|$ (див. рис. 7.6).

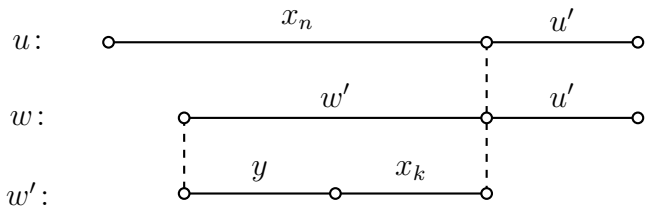


Рис. 7.6: Доведення леми 7.3.16

Зараз ми виділимо два випадки. Спочатку припустимо, що $u' \in Y$. Тоді за лемою 7.3.15 маємо $x_k u' \in Y^*Z$. Звідси випливає, що $w = yx_ku' \in Y^*Z$. Далі, припустимо, що $u' \in Z$. Тоді $u' = x_m$ для деякого натурального числа m. Маємо $x_m \in X_{n+1}$, звідки випливає, що $m > n$. Оскільки $k \leqslant n$, то маємо $k \leqslant m$ і за лемою 7.3.15, $x_k x_m \in Y^*$. Отже $w = yx_kx_m \in Y^*$. Це завершує доведення. □

Доведення теореми 7.3.11. Нехай m — непарне натуральне число, $X = Z \cap A_m$ і $x, x', x'' \in X$. Припустимо, що для деяких слів $u, v \in A^+$ виконується рівність

$$xx' = ux''v. \tag{7.27}$$

Тоді для деяких слів $w, t \in A^+$ маємо $x = uw$, $x'' = wt$ і $x' = tv$. Позаяк слово x'' має непарну довжину, то одне зі слів w або t мусить мати парну довжину. Припустимо, що довжина слова w є парною (див. рис. 7.7). Позаяк слово w є власним префіксом

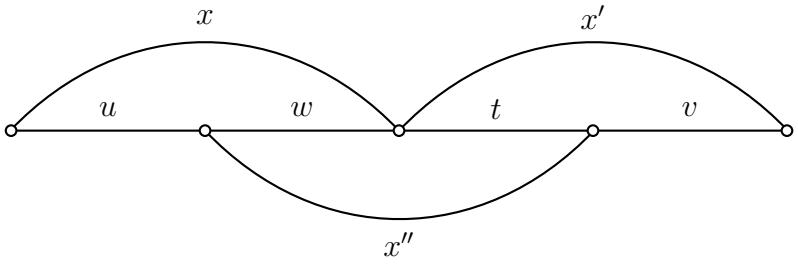


Рис. 7.7: Випадок, коли слово w має парну довжину

слова $x'' \in Z$, то за лемою 7.3.14 існує факторизація

$$w = z_1 z_2 \cdots z_n \qquad \text{з} \qquad z_1, z_2, \ldots, z_n \in Z \qquad \text{і} \qquad \delta(z_1) \geqslant \cdots \geqslant \delta(z_n).$$

З іншого боку, слово w є суфіксом слова $x \in Z$, і врахувавши лему 7.3.16, отримуємо, що $w \in Y^*Z \cup Y^*$. Позаяк слово w має парну довжину, то $w \in Y^*$. Таким чином, $n = 0$ і $w = 1$, а це доводить, що $u = x$, $x' = x''$ і $v = \varepsilon$. □

Приклад 7.3.17. Нехай $A = \{a, b\}$. Послідовність $(x_n)_{n \geqslant 1}$, яка відповідає умовам конструкції, наведеної вище, зображена в таблиці 7.3. У цій таблиці ми зобразили лише слова довжиною не більше за п'ять. Слова однакової довжини записуються у

стовпчик. Беручи слова довжини п'ять у X_5, ми отримуємо всі слова довжини п'ять у коді Z. Таким чином, наступний код є кодом без ком $X \subset A^5$:

$$X = \left\{a^4b, ba^3b, b^2a^2b, b^3ab, a^2bab, babab\right\}.$$

X_1	a, b				
X_2	b	ab	a^2b	a^3b	a^4b
X_3		ab	a^2b bab	a^3b ba^2b b^2ab	a^4b ba^3b b^2a^2b b^3ab
X_4		ab	a^2b bab	a^3b ba^2b b^2ab	a^4b ba^3b b^2a^2b b^3ab a^2bab
X_5		ab	a^2b bab	a^3b ba^2b b^2ab	a^4b ba^3b b^2a^2b b^3ab a^2bab $babab$

Табл. 7.3: Послідовність, яка задовольняє умови конструкції

Цей код має $\mathrm{Card}(X) = \ell_2(5) = 6$ елементів. Слова довжини три в X_3 утворюють код без ком з прикладу 7.2.16.

7.4 Вправи до розділу 7

Підрозділ 7.1

В. 7.4.1. Доведіть, що підмоноїд $\{ab, ba\}^*$ є чистим.

В. 7.4.2 (теорема Файна-Уілфа). Доведіть, якщо два степені слів x і y мають спільний префікс довжини

$$|x| + |y| - \mathbf{нсд}(|x|, |y|),$$

то слова x і y є степенями слова z.

Підрозділ 7.2

В. 7.4.3. Скінченний моноїд називається *аперіодичним*, якщо він не містить нетривіальних підгруп. Нехай $X \subset A^+$ — скінченний код і $\mathcal{A} = (Q, 1, 1)$ — однозначний обрізаний автомат, який розпізнає моноїд X^*. Нехай φ — його асоційоване зображення. Доведіть, що моноїд X^* є чистим тоді і тільки тоді, коли моноїд $\varpi(A^*)$ є аперіодичним.

В. 7.4.4. Множина $X \subset A^+$ називається (p, q)-*обмеженою* для для деяких $p, q \geqslant 0$, якщо для довільної послідовності $u_0, u_1, \ldots, u_{p+q}$ слів з умови $u_{i-1}u_i \in X$ для $1 \leqslant i \leqslant p + q$ випливає, що $u_p \in X^*$.

(1) Доведіть, що для $p + q \leqslant 2$, множина X є (p, q)-обмеженою тоді і тільки тоді, коли вона є (p, q)-граничною.
(2) Нехай $A = \{a, b\}$ і $X = \{a, ab\}$. Доведіть, що код X є $(3, 0)$-обмеженим, але не є $(3, 0)$-граничним.

В. 7.4.5. Доведіть, що розпізнаваний код є граничним тоді і тільки тоді, коли він є круговим.

(Підказка: Для розпізнаваного кругового коду X нехай $\varphi\colon A^* \to M$ — морфізм на синтактичному моноїді моноїда X^*. Доведіть, що X є (p, p)-граничним для $p = \mathrm{Card}(M) + 1$.)

Підрозділ 7.3

В. 7.4.6. Нехай A — k-літерний алфавіт і $s \in A^+$ — слово довжини p. Нехай

$$R = \{w \in A^*\colon sw \in A^*s, |w| < p\}$$

— скінченна множина. Нехай

$$X = A^*s \setminus A^*sA^+$$

— семафорний код. Використовуючи твердження 3.7.18, доведіть, що породжуючим рядом коду X є

$$f_X(t) = \frac{t^p}{t^p + (1 - kt)f_R(t)}.$$

Тепер, нехай

$$Z = (sA^+ \cap A^+s) \setminus A^+sA^+.$$

Доведіть, що виконується рівність

$$s + \underline{A}\,\underline{X} = \underline{X} + \underline{Z}.$$

Нехай $U = Zs^{-1}$. Доведіть, що для всіх натуральних чисел $n \geqslant p$ множина $U \cap A^n$ є кодом без ком і породжуючим рядом множини U є

$$f_U(t) = \frac{(kt-1)}{t^p + (1-kt)f_R(t)} + 1.$$

В. 7.4.7. Доведіть, що для будь-якої послідовності $(u_n)_{n\geqslant 1}$ p_n, визначена формулою (7.13), утворюється з від'ємних цілих чисел.

В. 7.4.8. Нехай $(u_n)_{n\geqslant 1}$ — послідовність невід'ємних цілих чисел. Нехай A — *ваговий алфавіт* з u_n літер ваги n для кожного натурального числа $n \geqslant 1$. Вагою слова називається сума ваг його літер. Доведіть, що $\ell_n(u)$ дорівнює кількості примітивних намист на алфавіті A з вагою n.

В. 7.4.9. Нехай $(u_n)_{n\geqslant 1}$ і $(v_n)_{n\geqslant 1}$ — дві послідовності цілих чисел таких, що

$$0 \leqslant u_n \leqslant v_n$$

для всіх натуральних чисел $n \geqslant 1$. Доведіть, що

$$l_n(u) \leqslant l_n(v)$$

для всіх натуральних чисел $n \geqslant 0$.

(Підказка: Використайте вправу 7.4.8.)

В. 7.4.10. Для довільної послідовності $(v_n)_{n\geqslant 1}$ комплексних чисел, означимо послідовність $(p_n)_{n\geqslant 1}$ наступним чином:

$$p_n = \sum_{d|n} dv_d^{n/d}.$$

Доведіть, що в термінах породжуючих рядів виконується рівність

$$\exp \sum_{n\geqslant 1} \frac{p_n}{n} z^n = \prod_{n\geqslant 1} (1 - v_n z^n)^{-1}.$$

Нотатки до розділу 7

Означення граничних кодів взято зі статті Шютценбергера [186], де граничні коди визначаються умовою, яка позначається через $\mathcal{U}_s(p,q)$ для $p \leqslant 0 \leqslant q$, що еквівалентна нашій умові $C(-p,q)$. Теорему 7.1.10 взято зі статті [138]. Див. також статтю [122], де вперше зустрічається термін "круговий код".

Існує близький зв'язок між формулами, які стосуються розподілу довжин кругових кодів і симетричними функціями. Власне, для скінченного коду числа u_n є, з точністю до знаку, елементарними симетричними функціями коренів многочлена $1-u(z)$ і p_n — суми степенів. Формула (7.13) э добре відомою в цьому контексті та формула (7.15) відома під назвою *формули Ньютона* (див., наприклад, [141]). Твердження 7.3.1 зустрічається в монографії Стенлі [196, 197].

Ліву частину формули (7.13) часто називають *зета-функцією*. У контексті символічної динаміки зета-функція підзсуву S визначається так

$$\zeta_S(z) = \exp \prod_{n\geqslant 1} \frac{p_n}{n} z^n,$$

де p_n — кількість точок періоду n (див. монографію [128]). Це відповідає нашій гіпотезі, враховуючи підзсув, утворений з усіх нескінченних слів, що мають факторизацію в словах кода X. У цьому контексті формула (7.13) є окремим випадком результату Меннінга [146], який полягає в наступному. Нехай S — підзсув породжений усіма двобічними нескінченними шляхами в графі G. Нехай M — матриця переходів графа G. Тоді

$$\zeta_S(z) = \frac{1}{\det(I - Mz)}.$$

Числа $l_n(k)$ називаються *числами Witt* (*Witt numbers*) і тотожність (7.19) називається *циклотомічною тотожністю*. Інші результати про зета-функції та кругові коди викладено в статті Келлера [104]. Книги Стенлі [196, 197] містять застосування цих понять до чисельної комбінаторики.

Теорему 7.3.7 доведено в статті Шутценбергера [186]. Для доведення використовується метод, відомий у контексті вільних алгебр Лі, як *метод усунення Лазарда*.

Пара (v,p), визначена у вправі 7.4.10 називається *вектором Witt* (*Witt vector*) (див. монографію [120] або статтю [152]). Зв'язок між векторами та кодами Вітта та конструкцією, наведеною у вправі 7.4.10, досліджується Луком та Тібоном у статті [139].

Історія кодів без ком цікава. Вперше вони зустрічаються статті [82]. Деякі математики в той час вважали, що біологічний код є кодом без ком (*гіпотеза Крика*). Кількість амінокислот, що появляються у білках, становить 20. Вони кодуються словами довжиною три над алфавітом базисів A, C, G, U. Тепер число $l_3(4)$, що є максимальною кількістю елементів у коді без ком (або круговому коді), що складається із слів довжиною три над чотири-літерним алфавітом, дорівнює в точності 20. На жаль для математики, через декілька років праці Нірнберга виявилося, що біологічний код не є навіть кодом у сенсі цієї книги. Декілька трійок базисів можуть кодувати одну і ту ж кислоту (див. монографії [198] або [127]). Ми вважаємо, що це розчарування не послаблює інтерес до кругових кодів.

Твердження теореми 7.3.11, як гіпотеза було висловлено в статті [82] і доведено Істманом в праці [65]. Ще одну побудову дав Шольц у статті [177], на якій ґрунтуються наведене нами доведення. Інші можливі конструкції описані в праці [57]. Для парної довжини не відома жодна формула, яка б надавала максимальну кількість елементів коду без коми (див. [101][1]). Подальші дослідження кодів без ком, включають відповідну проблему поповнення, розв'язану Ламом у праці [119], і вивчення більш загальної сім'ї кодів, так званої сім'ї *solid*-кодами (або кодів тіл) (див. [193] і [118]).

Вправа 7.4.2 належить Файну та Уілфу (див. [131, 132]). Вправа 7.4.3 взята зі статті [162] (див. також [89]). Ці твердження мають природне місце в рамках теорії різноманітностей моноїдів (див. [63] або [160]).

Вправа 7.4.6 взята з [86]. Коди введені в цій вправі визначені Ґілбертом у праці [75] і називаються *префіксно-синхронізованими*. Ґілберт сформулював гіпотезу, що $U \cap A^n$ має максимальни порядок, у випадку коли слово s вибирається необлямованим і має довжину $\log_k n$. Цю гіпотезу врегулювали Гібас та Одлізько в статті [86]. Вона виконується для $k = 2, 3, 4$, але не виконується для $k \geqslant 5$.

[1] B. H. Jiggs – це псевдонім автора Basil Gordon.

Розділ 8

Факторизації вільних моноїдів

У цьому розділі систематично досліджується поняття факторизації вільних моноїдів, яке вже було розглянуто в окремих випадках у розділі 7. Основний результат підрозділу 8.1 (теорема 8.1.2) охарактеризує факторизацію вільних моноїдів. Зокрема, це показує, що коди, які фігурують у цих факторизаціях, є круговими. Доведення ґрунтується на техніці перерахування. Для цього ми визначаємо логарифм у кільці формального степеневого ряду з некомутативниими змінними. Виведені властивості, необхідні для доведення. Ми проілюструємо теорему факторизації, розглядаючи дуже загальне сім'ї факторизацій, отримані з множин, що називаються *множинами Лазарда*.

Підрозділ 8.2 присвячений вивченню факторизацій в скінченнц кількість підмоноїдів. Ми спочатку розглянемо факторизації в два підмоноїди, які називаються *бісекціями*. Основний результат (твердження 8.2.4) дає метод для побудови всіх бісекцій. Далі ми вивчаємо трисекції, тобто такі факторизації в три підмоноїди. Ми доводимо складний результат (теорема 8.2.6), який показує, що кожну трисекцію можна побудувати шляхом "склеювання" разом факторизацій на чотири множники, отримані послідовними бісекціями.

8.1 Факторизації

Велику кількість разів в попередньому розділі ми використовували спеціальні випадки поняття факторизації, які будуть означені в цьому підрозділі. Ми побачимо в цьому підрозділі, що ці факторизації є замкнені стосовно кругових кодів. Нехай I — лінійно впорядкована множина та $(X_i)_{i\in I}$ — сім'я підмножин вільної напівгрупі A^+, індексована множиною I. *Впорядокованою факторизацією* слова $w \in A^*$ називається факторизація

$$w = x_1 x_2 \cdots x_n \tag{8.1}$$

з $n \geqslant 0$, $x_i \in X_{j_i}$ такими, що $j_1 \geqslant j_2 \geqslant \cdots \geqslant j_n$.

Сім'я $(X_i)_{i\in I}$ називається *факторизацією* вільного моноїда A^*, якщо кожне слово $w \in A^*$ має рівно одну впорядковану факторизацію.

Якщо $(X_i)_{i\in I}$ — факторизація, то кожна множина X_i є кодом, оскільки в протилежному випадку єдина факторизація не обов'язково виконується для слів у множині X_i^*. Ми покажемо далі (теорема 8.1.2), що множина X_i є насправді круговим кодом.

Тепер ми викладемо формулювання в термінах формальних степеневих рядів. Розглянемо сім'ю $(\sigma_i)_{i\in I}$ формальних степеневих рядів над алфавітом A з коефіцієнтами в напівкільці K, індексовану множиною I. Припустимо далі, що сім'я $(\sigma_i)_{i\in I}$ є локально скінченною. Нехай $J = \{j_1, j_2, \cdots, j_n\}$ — скінченна підмножина множини I, з $j_1 \geqslant j_2 \geqslant \cdots \geqslant j_n$. Покладемо

$$\tau_J = \sigma_{j_1}\sigma_{j_2}\cdots\sigma_{j_n}.$$

Тоді для всіх слів $w \in A^*$ означимо

$$(\tau_J, w) = \sum_{x_1x_2\cdots x_n=w} (\sigma_{j_1}, x_1)(\sigma_{j_2}, x_2)\cdots(\sigma_{j_n}, x_n). \tag{8.2}$$

Нехай $\mathcal{S}$ — множина всіх скінченних підмножин множини I. Тоді сім'я $(\tau_J)_{J\in\mathcal{S}}$ є локально скінченною. Справді, для кожного слова $w \in A^*$ множина $F(w)$ множників слова w є скінченною. Для кожного множника $x \in F(w)$ множина I_x індексів $i \in I$ таких, що $(\sigma_i, x) \neq 0$ є скінченною. З формули (8.2) випливає, якщо $(\tau_J, w) \neq 0$, то $J \subset \bigcup_{x\in F(w)} I_x$. Звідси випливає, що існує лише скінченна кількість множин J таких, що $(\tau_J, w) \neq 0$. Ці міркування дозволяють нам визначити добуток

$$\sigma = \prod_{i\in I}(1 + \sigma_i)$$

за формулою

$$\sigma = \sum_{J\in\mathcal{S}} \tau_J.$$

Якщо множина I є скінченною, то ми отримуємо звичайне поняття добутку послідовності формальних степеневих рядів, а останній вираз — це в точності розгорнута форма, отримана розподілом.

Розглянемо сім'ю $(X_i)_{i\in I}$ підмножин вільної напівгрупи A^+ індексовану лінійно впорядкованою множиною I. Якщо сім'я $(X_i)_{i\in I}$ є факторизацією вільного моноїда A^*, то справджується рівність

$$\underline{A^*} = \prod_{i\in I} \underline{X_i^*}. \tag{8.3}$$

І навпаки, якщо множини X_i є кодами і якщо напівгрупи X_i^+ є попарно диз'юнктними, то добуток $\prod_{i\in I} \underline{X_i^*}$ визначено і з формули (8.3) випливає, що сім'я $(X_i)_{i\in I}$ є факторизацією вільного моноїда A^*.

Приклад 8.1.1. Формула (7.25) стверджує, що сім'я

$$(X_{n+1}, \{x_n\}, \ldots, \{x_1\})$$

є факторизацією вільного моноїда A^* для всіх натуральних чисел $n \geqslant 1$. Лема 7.3.13 стверджує, що сім'я множин

$$(Y, \ldots, \{x_n\}, \{x_{n-1}\}, \ldots, \{x_1\})$$

є факторизацією вільного моноїда A^*.

Основним результатом цього розділу є наступна теорема.

Теорема 8.1.2 (Шютценбергер). *Нехай $(X_i)_{i\in I}$ — сім'я підмножин вільної напівгрупи A^+, індексована лінійно впорядкованою множиною I. Тоді з двох довільних наступних умов випливає третя:*

(*i*) *кожне слово $w \in A^*$ має щонайменше одну впорядковану факторизацію;*
(*ii*) *кожне слово $w \in A^*$ має щонайбільше одну впорядковану факторизацію;*
(*iii*) *кожна з множин X_i ($i \in I$) є круговим кодом і кожен клас спряженості непорожніх слів перетинає рівно один з моноїдів X_i^*.*

Доведення ґрунтується на техніці перерахування. Перш ніж надати доведення, нам будуть потрібні певні результати стосовно логарифму формального степеневого ряду з комутативними або некомутативними змінними. Далі ми розглянемо дещо більш загальну ситуацію, а саме формальний степеневий ряд, визначений над моноїдами, які є прямими добутками скінченної кількості вільних моноїдів. Нехай M — моноїд, який є прямим добутком скінченної кількості вільних моноїдів. Множина

$$S = \mathbb{Q}^M$$

функцій з моноїда M в поле $\mathbb{Q}$ раціональних чисел зі структурою напівкільця, як це робилося для формальних рядів над вільним моноїдом. Зокрема, якщо $\sigma, \tau \in S$, то добуток $\sigma\tau$ визначений за формулою

$$(\sigma\tau, m) = \sum_{uv=m} (\sigma, u)(\tau, v),$$

є коректно визначеним, оскільки множина пар (u, v), які задовольняють умову $uv = m$ є скінченною. Як і у випадку формальних степеневих рядів над вільним моноїдом, сім'я $(\sigma_i)_{i\in I}$ елементів множини S є локально скінченною, якщо для всіх $m \in M$ множина $\{i \in I \colon (\sigma_i, m) \neq 0\}$ є скінченною. Означимо

$$S^{(1)} = \{\sigma \in S \colon (\sigma, 1) = 0\}.$$

Для $\sigma \in S^{(1)}$ сім'я $(\sigma^n)_{n\geqslant 0}$ степенів елемента σ є локально скінченною. Справді, для кожного елемента $m \in M$ маємо, що $(\sigma^n, m) = 0$ для всіх натуральних чисел n більших за суму довжин компонент елемента m. Це дозволяє нам визначити

$$\log(1+\sigma) = \sigma - \frac{\sigma^2}{2} + \frac{\sigma^3}{3} - \cdots + \frac{(-1)^{n+1}\sigma^n}{n} + \cdots, \tag{8.4}$$

$$\exp(\sigma) = 1 + \sigma + \frac{\sigma^2}{2!} + \cdots + \frac{\sigma^n}{n!} + \cdots, \tag{8.5}$$

для всіх $\sigma \in S^{(1)}$.

Нехай M і N — моноїди, які є скінченними прямими добутками вільних мноїдів. Нехай $S = \mathbb{Q}^M$ і $T = \mathbb{Q}^N$. Морфізм

$$\gamma \colon M \to T$$

з моноїда M в мультиплікативний моноїд T називається *неперервним*, якщо сім'я $(\gamma(m))_{m\in M}$ є локально скінченною. У цьому випадку морфізм γ можна продовжити до морфізму, який також позначатимемо через γ, з алгебри S в алгебру T за формулою

$$\gamma(\sigma) = \sum_{m\in M} (\sigma, m)\gamma(m). \tag{8.6}$$

Ця сума є коректно визначеною, оскільки сім'я $(\gamma(m))_{m\in M}$ є локально скінченною. Продовжений морфізм γ також називається *неперервним морфізмом* з алгебри S в алгебру T. Для довільної локально скінченної сім'ї $(\sigma_i)_{i\in I}$ елементів алгебри S сім'я $\gamma(\sigma_i)_{i\in I}$ є також локально скінченною та виконується рівність

$$\sum_{i\in I} \gamma(\sigma_i) = \gamma\left(\sum_{i\in I} \sigma_i\right). \tag{8.7}$$

Відповідно до формули (8.7), неперервний морфізм $\gamma\colon S \to T$ цілком визначається його значенням на моноїді M, а отже, породжуючою множиною X моноїда M. Більше того, морфізм $\gamma\colon S \to T$ є неперервним тоді і тільки тоді, коли $\gamma(X \setminus \{1\}) \subset T^{(1)}$ і сім'я $(\gamma(x))_{x\in X}$ є локально скінченною. Це пов'язано з тим, що кожен елемент $m \in M$ має лише скіченну кількість множників $m = x_1x_2\cdots x_k$ з $x_1, x_2, \ldots, x_k \in X \setminus \{1\}$. З формули (8.6) випливає, якщо $\sigma \in S^{(1)}$, то $\gamma(\sigma) \in T^{(1)}$. З формули (8.7) отримуємо рівності

$$\log(1 + \gamma(\sigma)) = \gamma(\log(1 + \sigma)), \tag{8.8}$$

$$\exp(\gamma(\sigma)) = \gamma(\exp(\sigma)). \tag{8.9}$$

Враховуючи класичні результати з елементарного аналізу, ми отримуємо наступні формули в алгебрі $\mathbb{Q}[[s]]$ формальних степеневих рядів зі змінною s:

$$\exp(\log(1 + s)) = 1 + s, \qquad \log(\exp(s)) = s. \tag{8.10}$$

Більше того, в алгебрі $\mathbb{Q}[[s, t]]$ формальних степеневих рядів з двома комутуючими змінними s і t, маємо

$$\exp(s + t) = \exp(s)\exp(t), \qquad \log((1 + s)(1 + t)) = \log(1 + s) + log(1 + t). \tag{8.11}$$

Нехай M — моноїд, який є скінченним прямим добутком вільних моноїдів і $S = \mathbb{Q}^M$. Нехай $\sigma \in S^{(1)}$ і γ — неперервний гомоморфізм з алгебри $\mathbb{Q}[[s]]$ у S, означений за формулою $\gamma(s) = \sigma$. Тоді за формулами (8.8)–(8.10), маємо

$$\exp(\log(1 + \sigma)) = 1 + \sigma, \qquad \log(\exp(\sigma)) = \sigma, \tag{8.12}$$

а це доводить, шо функції exp і log є оберненими бієкціями між собою з множини S на множину

$$1 + S^{(1)} = \left\{1 + r\colon r \in S^{(1)}\right\}.$$

Тепер розглянемо два ряди $\sigma, \tau \in S^{(1)}$, які комутують, тобто є такими, що $\sigma\tau = \tau\sigma$. Позаяк підмоноїд алгебри S породжений рядами σ і τ є комутативним, то відображення γ з $s^* \times t^*$ в S, визначений за формулою

$$\gamma(s^p t^q) = \sigma^p \tau^q,$$

є неперервним морфізмом з $\mathbb{Q}[[s,t]]$ в S і за формулою (8.11) отримуємо

$$\exp(\sigma+\tau)=\exp(\sigma)\exp(\tau),\qquad \log((1+\sigma)(1+\tau))=\log(1+\sigma)+log(1+\tau). \quad (8.13)$$

Ці формули не виконуються у випадку, коли ряди σ і τ не комутують. Ми наведемо властивість різниці двох сторін формули (8.13) у загальному випадку. Ряд $\sigma\in\mathbb{Q}\langle A\rangle\rangle$ називається *циклічно нульовим*, якщо для кожного класу суміжності $C\in A^*$ виконується рівність

$$(\sigma,\underline{C})=\sum_{w\in C}(\sigma,w)=0.$$

Очевидно, що будь-яка сума циклічно нульового рядів все ще є циклічно нульовим рядом.

Твердження 8.1.3. *Нехай A — алфавіт $S=Q\langle\langle A\rangle\rangle$ і $\gamma\colon S\to S$ — неперервний морфізм. Для кожного циклічно нульового ряду $\sigma\in S$, ряд $\gamma(\sigma)$ є циклічно нульовим.*

Доведення. Нехай $T\subset A^*$ — множина представників класів спряжень вільного моноїда A^*. Позначимо через $C(t)$ клас спряженості елемента $t\in T$. Нехай

$$\tau=\sum_{t\in T}\left(\sum_{w\in C(t)}(\sigma,w)(w-t)\right).$$

Сім'я многочленів

$$\left(\sum_{w\in C(t)}(\sigma,w)(w-t)\right)_{t\in T}$$

є локально скінченною. Отже, ця сума є коректно визначеною. Далі

$$\tau=\sum_{t\in T}\sum_{w\in C(t)}(\sigma,w)w-\sum_{t\in T}\sum_{w\in C(t)}(\sigma,w)t=\sigma-\sum_{t\in T}(\sigma,C(t))t.$$

Оскільки ряд σ є циклічно нульовим, то другий ряд зникає а, отже, $\tau=\sigma$. Звідси випливає рівність

$$\gamma(\sigma)=\sum_{t\in T}\left(\sum_{w\in C(t)}(\sigma,w)\left(\gamma(w)-\gamma(t)\right)\right).$$

Для доведення твердження достатньо показати, що кожен ряд $\gamma(w)-\gamma(t)$ для $w\in C(t)$ є циклічно нульовим. Для цього розглянемо $w\in C(t)$. Тоді $t=uv$ і $w=vu$ для деяких слів $u,v\in A^*$. Поклавши $\mu=\gamma(u)$ і $\nu=\gamma(v)$, отримуємо $\gamma(w)-\gamma(t)=\nu\mu-\mu\nu$. Далі

$$\nu\mu=\sum_{x,y\in A^*}(\nu,x)(\mu,y)xy.$$

Отже,

$$\nu\mu-\mu\nu=\sum_{x,y\in A^*}(\nu,x)(\mu,y)(xy-yx).$$

Оскільки кожен многочлен $xy-yx$ очевидно є циклічно нульовим, то ряд $\nu\mu-\mu\nu$ є циклічно нульовим, а отже ряд $\gamma(\sigma)$ є таким, також. □

Твердження 8.1.4. *Нехай $A = \{a, b\}$ і C — клас суміжності вільного моноїда A^*. Тоді*

$$(\log((1+a)(1+b)), \underline{C}) = (\log(1+a), \underline{C}) + (\log(1+b), \underline{C}). \tag{8.14}$$

Іншими словами, ряд

$$\log((1+a)(1+b)) - \log(1+a) - \log(1+b)$$

є циклічно нульовим.

Доведення. Маємо

$$(1+a)(1+b) = 1 + a + b + ab$$

і

$$\log((1+a)(1+b)) = \sum_{m \geqslant 1} \frac{(-1)^{(m+1)}}{m}(a+b+ab)^m.$$

Нехай $w \in A^n$ і d — кількість входжень слова ab, як множник у слово w. Перевіримо, що

$$((a+b+ab)^m, w) = \binom{d}{n-m}. \tag{8.15}$$

Справді, величина $((a+b+ab)^m, w)$ дорівнює кількості факторизацій $w = x_1 x_2 \cdots x_m$ слова w на m слів, з $x_i \in \{a, b, ab\}$. Позаяк слово w має довжину n і кожне слово x_i має довжину 1 або 2, то існує рівно $n-m$ слів x_i, які збігаються зі словом ab. Кожна факторизація слова w що відповідає вибору $n-m$ множників слова w дорівнює ab серед d входжень слова ab. Таким чином, існує рівно $\binom{d}{n-m}$ факторизацій. Це доводить формулу (8.15).

Нехай тепер C — клас суміжності, n — довжина слів в класі C і p їх порядок. Тоді $\mathrm{Card}(C) = n/p$. Якщо $C \subset a^*$, то $C = \{a^n\}$. Тоді формула (8.15) доводить, що величина $((a+b+ab)^m, a^n)$ дорівнює 1 або 0 в залежності чи $n = m$, або ні. Отож, обидва боки формули (8.14) в цьому випадку дорівнюють $\dfrac{(-1)^n}{n}$. Аналогічне виконується якщо $C \subset b^*$. Таким чином, ми можемо припускати, що C не міститься в $a^* \cup b^*$. Тоді права частина формули (8.14) дорівнює 0. Розглянемо ліву частину формули (8.14). Оскільки кожне слово в класі C містить щонайменше одну літеру a, то існує слово w в класі C чиєю першою літерою є a. Нехай d — кількість входжень слова ab як множник у слово w. Серед n/p спряжень слова w існує d/p спряжень, які починаються з літери b і закінчуються літерою a. Справді, приймемо $w = vp$. Тоді слово v має d/p входжень множника ab. Кожне з d/p спряжень слова w в bA^*a отримане "різання" v в середині одним входженням слова ab. Кожне з цих d/p спряжень має лише $d-1$ входження слова ab в якості множника. Інші $\dfrac{n-d}{p}$ входжень слова w мають всі d входжень множника ab. За формулою (8.15) для кожного спряження u слова w маємо

$$((a+b+ab)^m, u) = \begin{cases} \binom{d-1}{n-m}, & \text{якщо } u \in bA^*a, \\ \binom{d}{n-m}, & \text{в іншому випадку.} \end{cases}$$

Підсумовування за елементами класу C дає рівність

$$((a+b+ab)^m, \underline{C}) = \frac{d}{p}\binom{d-1}{n-m} + \frac{n-d}{p}\binom{d}{n-m}.$$

Позаяк

$$\binom{d-1}{n-m} = \frac{d-n+m}{d}\binom{d}{n-m},$$

то отримуємо рівність

$$((a+b+ab)^m, \underline{C}) = \frac{m}{p}\binom{d}{n-m}.$$

Отже, маємо

$$(\log(1+a)(1+b), \underline{C}) = \frac{1}{p}\sum_{m\geqslant 1}(-1)^{m+1}\binom{d}{n-m}. \tag{8.16}$$

Оскільки $n > d$ і $d \neq 0$, то ця знакозмінна сума біноміальних коефіцієнтів дорівнює 0. □

Наступне твердження є розширенням твердження 8.1.4.

Твердження 8.1.5. *Нехай $(\sigma_i)_{i\in I}$ — локально скінченна сім'я елементів множини $\mathbb{Q}\langle\langle A\rangle\rangle$, індексована лінійно впорядкована множиною I така, що $(\sigma_i, 1) = 0$ для всіх $i \in I$. Тоді ряд*

$$\log\left(\prod_{i\in I}(1+\sigma_i)\right) - \prod_{i\in I}\log(1+\sigma_i) \tag{8.17}$$

є циклічно нульовим.

Доведення. Покладемо $S = \mathbb{Q}\langle\langle A\rangle\rangle$ і

$$S^{(1)} = \{\sigma \in S \colon (\sigma, 1) = 0\}.$$

Нехай $\sigma, \tau \in S^{(1)}$. Тоді ряд

$$\delta = \log((1+\sigma)(1+\tau)) - \log(1+\sigma) - \log(1+\tau)$$

є циклічно нульовим. Справді, або ряди σ і τ комутують і ряд δ є циклічно нульовим за умовою (8.13), або алфавіт A має щонайменше дві літери a і b. Розглянемо неперервний гомоморфізм γ такий, що $\gamma(a) = \sigma$ і $\gamma(b) = \tau$. Тоді ряд

$$d = \log((1+a)(1+b)) - \log(1+a) - \log(1+b)$$

є циклічно нульовим за твердженням 8.1.4. Оскільки $\delta = \gamma(d)$, то з твердження 8.1.3 випливає, що ряд δ є циклічно нульовим. Тепер, нехай $\tau_1, \tau_2, \ldots, \tau_n \in 1 + S^{(1)}$. Аргументуючи індукцією, припустимо, що ряд

$$\epsilon = \log(\tau_n \cdots \tau_2) - \sum_{i=2}^{n}\log\tau_i$$

є циклічно нульовим. З огляду на попередню дискусію маємо, що ряд

$$\epsilon' = \log(\tau_n \cdots \tau_2 \tau_1) - \log(\tau_n \cdots \tau_2) - \log \tau_1$$

є циклічно нульовим. Звідси випливає, що ряд

$$\epsilon + \epsilon' = \log(\tau_n \cdots \tau_1) - \sum_{i=1}^{n} \log \tau_i$$

є циклічно нульовим. Це доводить формулу (8.17) для скінченних множин I. Для загального випадку, ми розглянемо фіксований клас суміжності C. Нехай n — довжина слів в класі C і $B = \mathrm{alph}(C)$. Тоді множина B є скінченною та $C \subset B^n$. Означимо відношення еквівалентності на S поклавши: $\sigma \sim \tau$ тоді і тільки тоді, коли $(\sigma, w) = (\tau, w)$ для всіх $w \in B^{[n]}$[1]. Зауважимо спочатку, що з умови $\sigma \sim \tau$ випливає, що $\sigma^k \sim \tau^k$ для всіх $k \geqslant 1$. Отже з $\sigma \sim \tau$ та $\sigma, \tau \in S^{(1)}$ випливає, що

$$\log(1 + \sigma) \sim \log(1 + \tau).$$

Розглянемо сім'ю $(\tau_i)_{i \in I}$, яка задовольняє умови твердження. Нехай

$$I_0 = \{i \in I \colon \sigma_i \sim 0\} \qquad \text{і} \qquad I' = I \setminus I_0.$$

Тоді множина I' є скінченною. Справді, для кожного слова $w \in B^{[n]}$ існує лише скінченна кількість індексів i таких, що $(\sigma_i, w) \neq 0$. Позаяк множина B є скінченною, то множина $B^{[n]}$ є також скінченною, а отже I' — скінченна множина.

Далі зауважимо, що справджується відношення

$$\prod_{i \in I} (1 + \sigma_i) \sim \prod_{i \in I'} (1 + \sigma_i), \tag{8.18}$$

оскільки з огляду на формулу (8.2) маємо $(\tau_J, w) = 0$ для $w \in B^{[n]}$, за винятком випадків, коли $J \subset I'$. З формули (8.18) випливає, що

$$\log\left(\prod_{i \in I} (1 + \sigma_i)\right) \sim \log\left(\prod_{i \in I'} (1 + \sigma_i)\right).$$

Отже, отримуємо

$$\left(\log\left(\prod_{i \in I} (1 + \sigma_i)\right), \underline{C}\right) = \left(\log\left(\prod_{i \in I'} (1 + \sigma_i)\right), \underline{C}\right).$$

Далі, оскільки $\sigma_i \sim 0$ для $i \in I_0$, то маємо $\log(1+\sigma_i) \sim 0$ для $i \in I_0$. Отже виконується рівність

$$\left(\sum_{i \in I} \log(1 + \sigma_i), \underline{C}\right) = \left(\sum_{i \in I'} \log(1 + \sigma_i), \underline{C}\right)$$

[1] Нагадаємо, що $B^{[n]} = \{w \in B^* \colon |w| \leqslant n\}$.

Зі скінченного випадку отримуємо

$$\left(\log\left(\prod_{i\in I'}(1+\sigma_i)\right),\underline{C}\right)=\left(\sum_{i\in I'}\log(1+\sigma_i),\underline{C}\right)$$

Збираючи все це разом, маємо

$$\left(\log\left(\prod_{i\in I}(1+\sigma_i)\right),\underline{C}\right)=\left(\sum_{i\in I'}\log(1+\sigma_i),\underline{C}\right)=\left(\sum_{i\in I}\log(1+\sigma_i),\underline{C}\right),$$

що і завершує доведення твердження. □

Для доведення теореми 8.1.2 нам потрібна остаточна лема, яка є переформулюванням тверджень 7.1.7 і 7.1.8.

Твердження 8.1.6. *Нехай $X\subset A^+$ — код. Для кожного класу спряженості C, який перетинає моноїд X^* справджується нерівність $(\log\underline{X}^*,\underline{C})\geqslant(\log\underline{A}^*,\underline{C})$, і рівність виконується у випадку, коли X є круговим кодом. Навпаки, якщо $(\log\underline{X}^*,\underline{C})=(\log\underline{A}^*,\underline{C})$ для всіх класів спряженості, що перетинають моноїд X^*, то X є круговим кодом.*

Доведення. Маємо $X^*=(1-X)^{-1}$. Звідси випливає, що $\log(X^*(1-X))=0$. Позаяк ряди X^* і $1-X$ комутують, то отримуємо рівність $0=\log X^*+\log(1-X)$, а це доводить, що $\log X^*=-\log(1-X)$. Отже

$$\log X^*=\sum_{m\geqslant 1}\frac{1}{m}\underline{X^m}.$$

Зокрема, якщо $C\subset A^m$ — клас спряженості, то

$$(\log\underline{X}^*,\underline{C})=\sum_{m\geqslant 1}\frac{1}{m}\operatorname{Card}(X^m\cap C).$$

Для $X=A$ формула набуває вигляду

$$(\log\underline{A}^*,\underline{C})=\frac{1}{n}\operatorname{Card}(C).$$

Твердження є тепер безпосереднім наслідком тверджень 7.1.6 і 7.1.7. □

Доведення теореми 8.1.2. Припустимо спочатку, що умови (i) та (ii) виконуються, тобто, що сім'я $(X_i)_{i\in I}$ є факторизацією вільного моноїда A^*. Тоді множини X_i є кодами та за формулою (8.13) маємо

$$\underline{A}^*=\prod_{i\in I}\underline{X_i^*}. \tag{8.19}$$

Взявши логарифм від обох сторін рівності, отримуємо

$$\log\underline{A}^*=\log\left(\prod_{i\in I}\underline{X_i^*}\right). \tag{8.20}$$

За твердженням 8.1.5 ряд

$$\delta = \log \underline{A^*} - \sum_{i \in I} \log \underline{X_i^*} \tag{8.21}$$

є циклічно нульовим. Отже, для кожного класу спряженості C виконується рівність

$$(\log \underline{A^*}, \underline{C}) = \sum_{i \in I} \left(\log \underline{X_i^*}, \underline{C} \right). \tag{8.22}$$

За твердженням 8.1.6 маємо, що для кожного індексу $i \in I$ і для кожного класу спряженості C, що перетинає X_i^*, виконується нерівність

$$(\log \underline{A^*}, \underline{C}) \leqslant \left(\log \underline{X_i^*}, \underline{C} \right). \tag{8.23}$$

Формули (8.22) і (8.23) доводять, що для кожного класу спряженості C існує єдиний індекс $j \in I$ такий, що клас спряженості C перетинає моноїд X_j^*. Для цього індексу j виконується нерівність

$$(\log \underline{A^*}, \underline{C}) \leqslant \left(\log \underline{X_j^*}, \underline{C} \right). \tag{8.24}$$

Таким чином, якщо деякий моноїд X_j^* перетинає деякий клас спряженості, то жоден інший моноїд X_i^* $(i \in I \setminus \{j\})$ перетинає цей клас спряженості. Позаяк виконується рівність (8.24), то кожен з кодів X_i є круговим кодом за твердженням 8.1.6. Це доводить умову (iii).

Тепер припустимо, що виконується умова (iii). Нехай C — клас спряженості та $i \in I$ — єдиний індекс такий, що моноїд X_i^* перетинає C. Позаяк код X_i є круговим, то рівність (8.24) виконується за твердженням 8.1.6 і більше того $\left(\log \underline{X_j^*}, \underline{C} \right) = 0$ для всіх $j \neq i$. Підсумовуючи всі рівності (8.24), отримуємо рівняння (8.22). Це доводить, що ряд δ, визначений за формулою (8.21), є циклічно нульовим.

Нехай α — канонічний морфізм з алгебри $\mathbb{Q}\langle\langle A \rangle\rangle$ на алгебру $\mathbb{Q}[[A]]$ формальних степеневих рядів з комутативними змінними в алфавіті A. Множина слів у вільному моноїді A^*, які мають однакові образи стосовно морфізму α є об'єднанням класів спряженості, оскільки $\alpha(uv) = \alpha(vu)$. Позаяк формальний степеневий ряд δ є циклічно нульовим, то його образ $\alpha(\delta)$ є також циклічно нульовим рядом. Оскільки морфізм α є неперервним, застосувавши до обох боків формули (8.21) морфізм α, отримуємо рівність

$$0 = \log \alpha(\underline{A^*}) - \sum_{i \in I} \log \alpha(\underline{X_i^*}).$$

Таким чином, маємо, що

$$\log \alpha(\underline{A^*}) = \sum_{i \in I} \log \alpha(\underline{X_i^*}). \tag{8.25}$$

Далі, умова (iii) гарантує, що добуток $\prod_{i \in I} \underline{X_i^*}$ існує. За твердженням 8.1.5 ряд

$$\log \left(\prod_{i \in I} \underline{X_i^*} \right) - \sum_{i \in I} \log \underline{X_i^*}$$

є циклічно нульовим. Таким чином, його образ стосовно морфізму α є нульовим, а отже справджується рівність

$$\log\alpha\left(\prod_{i\in I}\underline{X_i^*}\right)=\sum_{i\in I}\log\alpha\left(\underline{X_i^*}\right).$$

Це разом з рівністю (8.25) доводить, що

$$\log\alpha(\underline{A^*})=\log\alpha\left(\prod_{i\in I}\underline{X_i^*}\right).$$

Позаяк функція log є взаємно однозначною, то з останньої рівності випливає, що

$$\alpha(\underline{A^*})=\alpha\left(\prod_{i\in I}\underline{X_i^*}\right).$$

Це доводить, що $\alpha(\epsilon)=0$, де

$$\epsilon=\underline{A^*}-\prod_{i\in I}\underline{X_i^*}.$$

Зауважимо, що умова (i) означає, що всі коефіцієнти ряду ϵ є від'ємними або нульовими. Умова (ii) стверджує, що всі коефіцієнти ряду ϵ є додатними або нульовими. Отож, в обох випадках всі коефіцієнти ряду ϵ мають однаковий знак. З цього разом з умовою $\alpha(\epsilon)=0$ випливає, що implies that $\epsilon=0$. Це доводить той факт, якщо умова (iii), чи одна з умов, або умова (i) або умова (ii) виконуються, то інша одна з умов (i) і (ii) також виконуються. □

Факторизація $(X_i)_{i\in I}$ вільного моноїда A^* називається *повною*, якщо кожен код X_i зводиться до до одноточкової множини x_i. Наступний результат є безпосереднім наслідком теореми 8.1.2. Нагадаємо з розділу 1, що через $\ell_n(k)$ позначається кількість примітивних намист довжини n на k-літерному алфавіті.

Наслідок 8.1.7. *Нехай $(x_i)_{i\in I}$ — повна факторизація вільного моноїда A^*. Тоді множина*

$$X=\{x_i\colon i\in I\}$$

є множиною представників примітивних спряжених класів. Зокрема, для всіх натуральних чисел $n\geqslant 1$ виконується рівність

$$\mathrm{Card}(X\cap A^n)=\ell_n(k),\tag{8.26}$$

де $k=\mathrm{Card}(A)$.

Доведення. Відповідно до умови (iii) теореми 8.1.2 кожен клас спряженості перетинає рівно один із підмоноїдів X_i^*. Зважаючи на ту ж умову, кожен код $\{x_i\}$ є круговим а, отже, кожне слово x_i є примітивним. Це доводить, що X — це множина представників примітивних класів спряженості. Формула (8.26) є прямим наслідком попередніх міркувань. □

Тепер ми опишемо систематичну процедуру отримання великого класу повних факторизацій вільних моноїдів. До таких факторизацій належить конструкція, що використовується в підрозділі 7.3.

Множиною Лазарда називається лінійно впорядкована підмножина Z вільної напівгрупи A^+, яка задовольняє таку властивість: для кожного натурального числа $n \geqslant 1$ множина $Z \cap A = \{z_1, z_2, \ldots, z_k\}$ з $z_1 < z_2 < \cdots < z_k$ такими, що

$$z_i \in Z_i \qquad \text{для} \qquad 1 \leqslant i \leqslant k, \qquad \text{і} \qquad Z_{k+1} \cap A^{[n]} = \varnothing,$$

де множини $Z_1, \ldots, Z_{k+1}$ визначаються так:

$$Z_1 = A, \qquad Z_{i+1} = z_i^* \left(Z_i \setminus \{z_i\}\right) \qquad (1 \leqslant i \leqslant k).$$

Приклад 8.1.8. Нехай $(x_n)_{n\geqslant 1}$ — послідовність Холла над алфавітом A й $(X_n)_{n\geqslant 1}$ — асоційована послідовність кодів. Припустимо, що для кожного натурального числа n слово x_n є словом мінімальної довжини в коді X_n, і нехай $Z = \{x_n \colon n \geqslant 1\}$ — підмножина вільної напівгрупи A^+, впорядкована індексами. Тоді Z є множиною Лазарда.

Приклад 8.1.9. Нехай $(x_n)_{n\geqslant 1}$ — послідовність використана в доведенні теореми 7.3.11. Нагадаємо, що ми починаємо з $X_1 = A$ та

$$X_{i+1} = x_i^*(X_i \setminus \{x_i\}) \qquad i \geqslant 1,$$

де x_i — слово в X_i мінімальної непарної довжини. Позначимо через Y множину слів парної довжини в множині $\bigcup_{i\geqslant 1} X_i$. Тепер множина $Y_1 = Y$ і для кожного натурального числа $i \geqslant 1$ покладемо

$$Y_{i+1} = y_i^* \left(Y_i \setminus \{y_i\}\right),$$

де слово $y_i \in Y_i$ вибрано з мінімальною довжиною. Нехай множина

$$T = \{x_i, y_i \colon i \geqslant 1\}$$

впорядкована наступним чином

$$x_1 < x_2 < \cdots < x_n < \cdots < y_1 < y_2 < \cdots .$$

Впорядкована множина T є множиною Лазарда. Справді, нехай $n \geqslant 1$ і

$$T \cap A^{[n]} = \{x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_s\}.$$

Покладемо

$$Z_i = X_i, \quad (1 \leqslant i \leqslant r+1), \qquad Z_{r+i+1} = y_i^*(Z_{r+i} \setminus \{y_i\}), \quad (1 \leqslant i \leqslant s).$$

Ми доведемо індукцією по i, що

$$Z_{r+i} \cap A^{[n]} = Y_i \cap A^{[n]} \qquad (1 \leqslant i \leqslant s+1). \tag{8.27}$$

Справді, слова в $X_{r+1} = Z_{r+1}$ довжини щонайбільше n всі мають парну довжину, оскільки словами непарної довжини є $x_1, x_2, \ldots, x_r$. Таким чином, усі ці слова містяться $Y = Y_1$. Звідси випливає, що кожне слово парної довжини $\leqslant n$ завжди міститься в X_{r+1}, оскільки $|x_{r+1}| > n$.

Далі, розглянемо $y \in Y_{i+1} \cap A^{[n]}$. Тоді $y = y_i^p y'$ для деякого слова $y' \in Y_i \setminus \{y_i\}$. Позаяк $|y'| \leqslant n$, то за припущенням індукції маємо, що $y' \in Z_{r+i}$, звідки випливає, що $y \in Z_{r+i+1}$. Обернене твердження доводиться аналогічним чином.

Рівняння (8.27) доводить, що $y_i \in Z_{r+i}$ для $1 \leqslant i \leqslant s$ і, що $Z_{r+s+1} \cap A^{[n]} = \varnothing$. Отож, T є множиною Лазарда.

Твердження 8.1.10. *Нехай $Z \subset A^+$ — множина Лазарда. Тоді сім'я $(z)_{z\in Z}$ є повною факторизацією вільного моноїда A^*.*

Доведення. Нехай $w \in A^*$ і $n = |w|$. Покладемо

$$Z \cap A^{[n]} = \{z_1, z_2, \ldots, z_k\}$$

з $z_1 < z_2 < \cdots < z_k$. Нехай $Z_1 = A$ та $Z_{i+1} = Z_i^*(Z_i \setminus \{z_i\})$ для $i = 1, 2, \ldots, k$. Тоді $z_i \in Z_i$ для $i = 1, 2, \ldots, k$ і $Z_{k+1} \cap A^{[n]} = \varnothing$. За аналогією, як і в доведенні леми 7.3.13 отримуємо для $1 \leqslant i \leqslant k$ рівність

$$\underline{Z_i^*} = \underline{Z_{i+1}^*} z_i^*,$$

звідки шляхом послідовних замін отримуємо

$$\underline{A^*} = \underline{Z_{k+1}^*} z_k^* \cdots z_1^*. \tag{8.28}$$

Отже, існує факторизація $w = y z_{i_1} z_{i_2} \cdots z_{i_n}$ з $y \in Z_{k+1}^*$ і $i_1 \geqslant i_2 \geqslant \cdots \geqslant i_n$. Позаяк $Z_{k+1} \cap A^{[n]} = \varnothing$, то ми маємо, що $y = 1$. Це доводить існування впорядковано факторизації. Припустимо, що існує інша факторизація, скажимо $w = t_1 t_2 \cdots t_m$ з $t_j \in Z$ і $t_1 \geqslant t_2 \geqslant \cdots \geqslant t_m$. Тоді $t_i \in Z \cap A^{[n]}$ для кожного натурального числа i. За рівністю (8.28) обидві факторизації збігаються. □

Ми закінчуємо цей підрозділ додатковим прикладом повної факторизації. Розглянемо лінійно впорядкований алфавіт A. Нагадаємо, що *лексикографічний* або *алфавітний* порядок, який позначається $\prec$, на вільному моноїді A^* визначається наступним чином: $u \prec v$ якщо слово u є власним префіксом слова v, або якщо $u = ras$, $v = rbt$, $a < b$ для $a, b \in A$ та $r, s, t \in A^*$. Нагадаємо також, що для алфавітного порядку справджується така властивість:

$$u \prec v \qquad \Longleftrightarrow \qquad wu \prec wv.$$

За означенням, *словом Линдона* (*Lyndon word*) називається примітивне слово, яке є мінімальним у його класі спряженості. Це еквівалентно тому, що слово $w \in A^+$ э словом Линдона тоді і тільки тоді, коли $w = uv$ з $u, v \in A^+$ випливає, що $w \in vu$. Нехай L — множина слів Линдона. Ми доведемо, що $(l)_{l\in L}$ є повною факторизацією вільного моноїда A^*. Для цього ми доведемо твердження, які цікаві самі по собі.

Твердження 8.1.11. *Слово w є словом Линдона тоді і тільки тоді, коли w є найменшим за всі його власні непорожні праві множники.*

Доведення. Умова є достатньою. Нехай $w = uv$ з $u, v \in A^+$. Позаяк $w \prec v$ і $v \prec vu$, то маємо $w \prec vu$. Звідси випливає, що $w \in L$. Навпаки, нехай $w \in L$ і розглянемо факторизацію $w = uv$ з $u, v \in A^+$. Спочатку ми доведемо, що слово v не є префіксом слова w. Припустимо протилежне. Тоді $w = vt$ для деякого слова $t \in A^+$. Позаяк $w \in L$, то маємо $w \prec tv$. Але з $w = uv$ випливає відношення $uv \prec tv$. Звідси в свою чергу випливає, що $u \prec t$ звідки, помноживши зліва на слово v, отримуємо

$$vu \prec vt = w,$$

протиріччя. Припустимо, що $v \prec uv$. Позаяк слово v не є префіксом слова w, то звідси випливає, що $vu \prec uv$ і $w \notin L$, протиріччя. Отже $uv \prec v$, і доведення завершено. □

Твердження 8.1.12. *Нехай l і m — слова Линдона. Якщо $l \prec m$, то lm є словом Линдона.*

Доведення. Спочатку доведемо, що $lm \prec m$. Якщо слово l є префіксом слова m, то приймемо $m = lm'$. Тоді $m \prec m'$ за твердженням 8.1.11. Отже $lm \prec lm' = m$. Якщо слово l не є префіксом слова m, то з нерівності $l \prec m$ безпосередньо випливає, що $lm \prec m$. Нехай v непорожній власний суфікс слова lm. Якщо слово v є суфіксом слова m, то за твердженням 8.1.11 отримуємо, що $m \prec v$. Таким чином, $lm \prec m \prec v$. У протилежному випадку маємо, що $v = v'm$ для деякого вдасного непорожнього суфікса v' слова l. Тоді $l \prec v'$ і звідси випливає, що $lm \prec v'm$. Таким чином, отримуємо, що у всіх випадках справджується нерівність $lm \prec v$. За твердженням 8.1.11 це доводить, що $lm \in L$. □

Теорема 8.1.13. *Сім'я $(l)_{l \in L}$ є повною факторизацією вільного моноїда A^*.*

Доведення. Ми доведемо, що справджуються умови (i) і (iii) теореми 8.1.2. Очевидно, що виконується умова (iii), оскільки L є системою представників примітивних класів спряження. Для доведення умови (i) припустимо, що $w \in A^+$. Тоді слово w має щонайменше одну факторизацію $w = l_1 l_2 \cdots l_n$ з $l_1, l_2, \ldots, l_n \in L$. Справді, кожна літера є завжди словом Линдона. Розглянемо факторизацію $w = l_1 l_2 \cdots l_n$ словами Линдона з найменшим числом n. Тоді ця факторизація є впорядкованою. Справді, в протилженому випадку, це був би якийсь індекс i такий, що $l_i \prec l_{i+1}$. Але тоді $l_i l_{i+1} \in L$ і слово w матимиме факторизацію з $n - 1$ слів Линдона. Таким чином, виконується умова (i) теореми 8.1.2. □

Можна довести (див. вправи 8.3.3 і 8.3.4), що L — це множина Лазарда.

8.2 Скінченні факторизації

У цьому підрозділі ми розглядатимемо факторизації $(X_i)_{i\in I}$ із скінченною множиною індексів I. Це є сім'ї $X_n, X_{n-1}, \dots, X_1$ підмножин вільної напівгрупи A^+ над алфавітом A такі, що

$$\underline{A^*} = \underline{X_n^*}\,\underline{X_{n-1}^*}\cdots\underline{X_1^*}. \tag{8.29}$$

За теоремою 8.1.2 кожна множина X_i є круговим кодом і кожен клас спряженості перетинає рівно один моноїд X_i^*. Мета цього підрозділу — уточнити ці властивості. Ми побачимо, що в деяких особливих випадках коди X_j є граничними. Питання про те, чи всі коди, що появляються у скінченних факторизаціях, є граничними, досі відкриті. Почнемо з дослідження *бісекцій*, тобто факторизацій вигляду (X, Y). У цьому випадку множина X називається *лівим множником*, а множина Y — *правим множником* бісекції (X, Y). Тоді

$$\underline{A^*} = \underline{X^*}\,\underline{Y^*}. \tag{8.30}$$

Приклад 8.2.1. Нехай $A = \{a, b\}$. Пара (a^*b, a) є бісекцією вільного моноїда A^*. Більш загально, якщо $A = A_0 \cup A_1$ є розбиттям алфавіта A, то пара $(A_0^*A_1, A_0)$ є бісекцією вільного моноїда A^*.

Формулу (8.30) можна записати так:

$$\underline{Y}\,\underline{X} + \underline{A} = \underline{X} + \underline{Y}. \tag{8.31}$$

Справді, рівність (8.30) еквівалентна рівності

$$1 - \underline{A} = (1 - \underline{Y})(1 - \underline{X}),$$

взявши інверсію від обох частин цієї рівності. Звідси випливає рівність (8.31). Рівності (8.30) і (8.31) показують, що пара (X, Y) підмножин вільної напівгрупи A^+ є бісекцією тоді і тільки тоді, коли виконуються такі умови:

$$A \subset X \cup Y, \tag{8.32}$$

$$X \cap Y = \varnothing, \tag{8.33}$$

$$YX \subset X \cup Y, \tag{8.34}$$

$$\begin{array}{l}\text{кожне слово} \quad z \in X \cup Y,\ z \notin A \quad \text{однозначно} \\ \text{факторизується } z = yx \quad \text{з} \quad x \in X,\ y \in Y.\end{array} \tag{8.35}$$

Ми побачимо далі (теорема 8.2.6), що для підмножин з такими властивостями підмножина вже достатньо для того, щоб пара (X, Y) була бісекцією.

Перед тим, як це зробити, ми доведемо, що для бісекції (X, Y) код X є $(1, 0)$-граничним і код Y є $(0, 1)$-граничним. Нагадаємо, що $(1, 0)$-граничний код є префіксним і, що за твердженням 7.2.12 префіксний код X є $(1, 0)$-граничним тоді і тільки тоді, коли множина $R = A^* \setminus XA^*$ є підмоноїдом вільного моноїда A^*. Симетрично, суфіксний код Y є $(0, 1)$-граничним тоді і тільки тоді, коли множина $S = A^* \setminus A^*Y$ є підмоноїдом в A^*.

Твердження 8.2.2. *Нехай X і Y — дві підмножини вільної напівгрупи A^+. Тоді такі умови є еквівалентними:*

(i) (X, Y) *є бісекцією вільного моноїда* A^**;*
(ii) X *і* Y *є кодами,* X *є* $(1,0)$*-граничним і* $Y^* = A^* \setminus XA^*$*;*
(iii) X *і* Y *є кодами,* Y *є* $(0,1)$*-граничним і* $X^* = A^* \setminus A^*Y$*.*

Доведення. $(i) \Rightarrow (ii)$ З рівності $\underline{A}^* = \underline{X}^*\underline{Y}^*$, домноживши її зліва на $1-\underline{X}$, отримуємо рівність $(1-\underline{X})\underline{A}^* = \underline{Y}^*$, з якої випливає, що $\underline{Y}^* = \underline{A}^* - \underline{X}\ \underline{A}^*$. Кількість префіксів у множині X довільного слова $w \in A^*$ дорівнює $(\underline{X}\ \underline{A}^*, w)$. Рівність доводить, що це число дорівнює 0 або 1, в залежності чи $w \in Y$, чи $w \notin Y^*$. Звідси випливає, що X є префіксним кодом, а також, що виконується рівність $Y^* = A^* \setminus XA^*$. Таким чином, множина $A^* \setminus XA^*$ є підмоноїдом в A^*, і за твердженням 7.2.12 код X є $(1,0)$-граничним.

$(ii) \Rightarrow (i)$ За наслідком 3.1.8 маємо, що $\underline{A}^* = \underline{X}^*\underline{R}$ з $R = A^* \setminus XA^*$. Оскільки $R = Y^*$ і множина Y є кодом, то $\underline{R} = \underline{Y}^*$. Таким чином, отримуємо рівність $\underline{A}^* = \underline{X}^*\underline{Y}^*$.

З вище викладеного випливає, що умови (i) and (ii) є еквівалентними. Еквівалентність умов (i) and (iii) доводиться аналогічно. □

Наслідок 8.2.3. *Ліві множники бісекцій є в точності* $(1,0)$*-граничні коди.*

Зауважимо, що для бісекції (X, Y) маємо, що або X є максимальним префіксним кодом, або Y є максимальним суфіксним кодом. Справді, маємо, що $Y^* = A^* \setminus XA^*$. Якщо моноїд Y^* не містить правого ідеалу, то множина XA^* є щільною справа, а отже код X є максимальним префіксним. У протилежному випадку, моноїд Y^* є щільним зліва, а отже множина Y є максимальним суфіксним кодом.

Твердження 8.2.4. *Нехай M і N — підмоноїди вільного моноїда A^* таке, що $\underline{A}^* = \underline{M}; \underline{N}$. Тоді M і N є вільними моноїдами та пара (X, Y) їх баз є бісекцією вільного моноїда A^*.*

Доведення. Нехай u і v — слова вільного моноїда A^* такі, що $uv \in M$. Покладемо $v = mn$ з $m \in M$ і $n \in N$. Аналогічно покладемо $um = m'n'$ для деяких слів $m' \in M$ і $n' \in N$ (див. рис. 8.1). Тоді $uv = m'(n'n)$. Оскільки $uv \in M$, то з єдиності

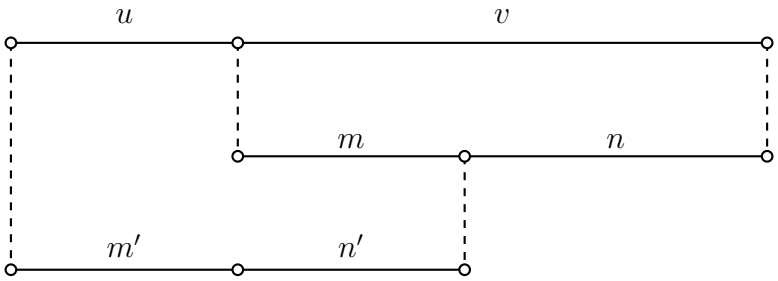


Рис. 8.1: Факторизації

факторизації випливає, що $n = n' = \varepsilon$, а отже $v \in M$. Це доводить, що моноїд

M задовольняє умову $C(1,0)$. Таким чином, моноїд M породжений $(1,0)$-граничним кодом X. Аналогічно доводиться, що моноїд N породжений $(0,1)$-граничним кодом Y. Очевидно, пара (X,Y) їх баз є бісекцією вільного моноїда A^*. □

Приклад 8.2.5. Нехай M і N — два підмоноїди вільного моноїда A^* такі, що

$$M \cap N = \{\varepsilon\} \qquad \text{і} \qquad M \cup N = A^*.$$

Ми поєднаємо спеціальну бісекцію вільного моноїда A^* з парою (M,N). Для цього нехай

$$R = \{r \in A^* \colon r = uv \;\Rightarrow\; v \in M\}$$

— множина слів в моноїді M, які мають всі свої суфікси в M. Симетрично означимо

$$S = \{s \in A^* \colon s = uv \;\Rightarrow\; u \in N\}\,.$$

Множина R є підмоноїдом вільного моноїда A^* оскільки M є підмоноїдом у A^*. Більше того, множина R є суфіксно замкненою. Звідси випливає, що база моноїда R, скажемо X, є $(1,0)$-граничним кодом. Подібно S є вільним підмоноїдом і його база, скажемо Y, є $(0,1)$-граничним кодом. Ми доведемо, що (X,Y) є бісекцією вільного моноїда A^*. З огляду на твердження 8.2.2 достатньо довести, що $Y^* = A^* \setminus XA^*$. Спочатку розглянемо слово $y \in Y^* = S$. Тоді всі його префікси містяться в моноїді N. таким чином, жоден префікс слова y не міститься в X. Це доводить, що $Y^* \subset A^* \setminus XA^*$.

Навпаки, нехай $w \in A^* \setminus XA^*$. Ми доведемо, що кожен префікс u слова w міститься в моноїді N індукцією за довжиною слова u. Очевидно, що дане твердження виконується для $|u| = 0$. Далі, якщо $|u| \geqslant 1$, то слово u не може міститися в $R = X^*$, оскільки в протилежному випадку слово w мало б префікс в моноїді X. Отож, існує факторизація $u = u'v'$ з $v' \notin M$. Таким чином, отримуємо, що $v' \in N$ і $v' \neq \varepsilon$. За припущенням індукції маємо, що $u' \in N$. Оскільки N є підмоноїдом у A^*, то $u = u'v' \in N$. Це доводить, що $w \in S = Y^*$.

Спеціальний випадок цієї конструкції отриманий розглядом морфізму $\varphi \colon A^* \to \mathbb{Z}$ в адитивний моноїд $\mathbb{Z}$ і поклавши

$$M = \{m \in A^* \colon \varphi(m) > 0\} \cup \{\varepsilon\} \qquad \text{і} \qquad N = \{n \in A^* \colon \varphi(n) \leqslant 0\}\,.$$

Для фіксованого слова $w \in A^*$, ми отримаємо факторизацію $w = rs$ з $r \in R$ і $s \in S$ наступним чином. Слово r є найкоротшим префіксом слова w таким, що значення $\varphi(r)$ є максимальним у множині значень морфізму φ на префіксах слова w (див. рис. 8.2).

Конструкцію, викладену в прикладі 8.2.5 можна розглядати як спеціальний випадок такого більш загального результату.

Теорема 8.2.6. *Нехай (P,Q) — розбиття вільної напівгрупи A^+. Існує єдина бісекція (X,Y) вільного моноїда A^* така, що $X \subset P$ і $Y \subset Q$. Ця бісекція отримується наступним чином.*

Нехай

$$X_1 = P \cap A, \qquad Y_1 = Q \cap A, \tag{8.36}$$

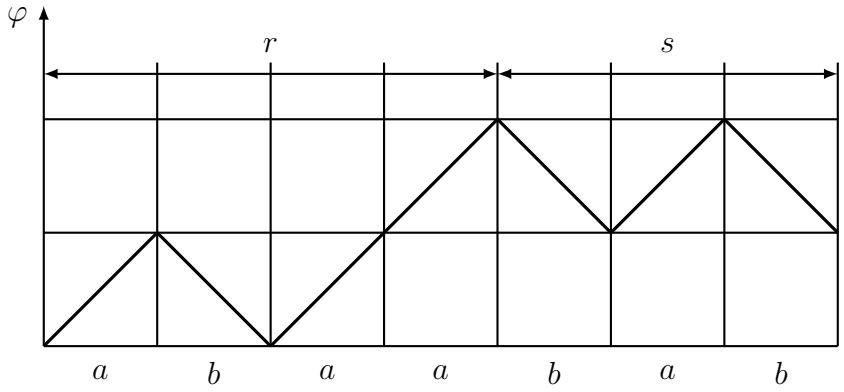


Рис. 8.2: Шлях значень морфізму φ для $\varphi(a) = 1$, $\varphi(b) = -1$ і $w = abaabab$

і

$$Z_n = \bigcup_{i=1}^{n} Y_i X_{n-i}, \tag{8.37}$$

$$X_n = Z_n \cap P, \qquad Y_n = Z_n \cap Q, \tag{8.38}$$

для $n \geqslant 2$. *Тоді*

$$X = \bigcup_{n\geqslant 1} X_n \qquad і \qquad Y = \bigcup_{n\geqslant 1} Y_n. \tag{8.39}$$

Доведення. Спочатку доведемо єдиність. Розглянемо бісекцію (X, Y) вільного моноїда A^* таку, що $X \subset P$ і $Y \subset Q$. Доведемо, що для натурального числа $n \geqslant 1$ маємо, що $X \cap A_n = X_n$, $Y \cap A_n = Y_n$, з X_n та Y_n визначеними за формулами (8.36) і (8.38). Доведення проведемо індукцією. Нехай $n = 1$. Тоді

$$X \cap A \subset P \cap A = X_1.$$

З формули (8.32) випливає, що $A \subset X \cup Y$ і $P \cap Y = \varnothing$. Звідси випливає, що $P \cap A \subset X$, а отже $X \cap A = X_1$. За припущенням індукції маємо, що $Z_n \subset YX \cap A_n$ для $n \geqslant 2$. Таким чином, за формулою (8.34) отримуємо, що $Z_n \subset (X \cup Y) \subset A_n$. Звідси випливає, що

$$Z_n \cap P \subset X \cap A_n \qquad \text{і} \qquad Z_n \cap Q \subset Y \cap A_n.$$

Навпаки, нехай $z \in (X \cup Y) \cap A_n$. Тоді за формулою (8.35) маємо, що $z = yx$ для деяких $y \in Y$, $x \in X$. За припущенням індукції $y \in Y_i$ і $x \in X_{n-i}$ для $i = |y|$. Використавши рівність (8.37) отримуємо, що $z \in Z_n$. Це доводить, що $(X \cup Y) \cap A_n \subset Z_n$. Отже, $X \cap A_n \subset Z_n \cap P$ та $Y \cap A_n \subset Z_n \cap Q$.

Для доведення існування бісекції розглянемо пару (X, Y) визначену у формулі (8.39). Доведення проведемо в декілька етапів. Означимо $Z_1 = A$ та приймемо $Z = \bigcup_{n\geqslant 1} Z_n$. Врахувавши формули (8.36) і (8.38), отримуємо, що $Z = X \cup Y$. Зауважимо спочатку, що за формулою (8.37) виконується рівність

$$YX \cup A = X \cup Y. \tag{8.40}$$

Очевидно, що з рівності (8.40) випливає включення $YX \subset X \cap Y$. За індукцією, отримуємо включення

$$Y^*X^* \subset X^* \cup Y^*. \tag{8.41}$$

Далі, маємо, що справджується рівність

$$A^* = X^*Y^*. \tag{8.42}$$

Справді, нехай $w \in A^*$. Оскільки $A \subset Z$, то слово w має щонайменше одну факторизацію $w = z_1 z_2 \cdots z_n$ з $z_1, z_2, \ldots, z_n \in Z$. Виберемо таку факторизацію, щоб число n було найменшим. Тоді ми не можемо мати $z_i \in Y$, $z_{i+1} \in X$ для деякого $1 \leqslant i \leqslant n-1$, оскільки з означення слова w випливає, що $z_j z_{j+1} \in Z$ за рівністю (8.40), а це суперечить мінімальності числа n. Звідси випливає, що існує деяке натуральне число $j \in \{1, \ldots, n\}$ таке, що $z_1, \ldots, z_j \in X$ і $z_{j+1}, \ldots, z_n \in Y$, а це доводить, що $w \in X^*Y^*$.

Далі доведемо, що моноїд X^* є суфіксно замкненою множиною. Для цього достатньо довести, що виконується умова

$$uv \in X \qquad \Longrightarrow \qquad v \in X^*. \tag{8.43}$$

Справді, припустивши (8.43), розглянемо слово $w = rs \in X^*$. Тоді $r = r'u$, $s = vs'$ для деяких $r', s' \in X^*$ і $uv \in X \cup \{\varepsilon\}$. За умовою (8.43) слово v міститься в моноїді X^*, а отже отримуємо, що $s \in X^*$, а це доводить, що моноїд X^* є суфіксно замкненою множиною. Ми доведемо виконання властивості (8.43) індукцією по довжині слова $x = uv$. Очевидно, що властивість (8.43) виконується для $|x| = 1$. Припустимо,що $|x| \geqslant 2$. Тоді за формулою (8.40) маємо, що $x = y_1 x_1$ для деяких $y_1 \in Y$, $x_1 \in X$. Якщо y_1 не є літерою, то знову за формулою (8.40) маємо, що $y_1 = y_2 x_2$ для деяких $y_2 \in Y$, $x_2 \in X$. Повторивши цю операцію декілька разів, отримуємо факторизацію

$$x = y_k x_k \cdots x_2 x_1$$

з $y_k \in Y_n \cap A$ і $x_1, \ldots, x_k \in X$.

Кожен суфікс v слова x має вигляд $v = v_p x_{p-1} \cdots x_1$ для деякого суфікса v_p слова x_p і $1 \leqslant p \leqslant k$. За припущенням індукції отримуємо, що $v_p \in X^*$. Звідси випливає, що $v \in X^*$. Це завершує доведення властивості (8.43). Аналогічно доводится, що моноїд Y^* є префіксно замкненою множиною.

Далі ми стверджуємо, що виконується рівність

$$X^* \cap Y^* = \{\varepsilon\}, \tag{8.44}$$

і доведемо цю рівність за індукцією, показавши, що множина $X^* \cap Y^*$ не містить слів довжини $n \geqslant 1$. Ця умова виконується для $n = 1$, оскільки $X \cap Y = \varnothing$. Припустимо, що для деякого слова $w \in A^n$ існує дві факторизації

$$x = x_1 x_2 \cdots x_p = y_1 y_2 \cdots y_q$$

з $x_1, x_2, \ldots, x_p \in X$, $y_1, y_2, \cdots, y_q \in Y$. Оскільки моноїд Y^* є префіксно замкненою множиною, то $x_1 \in Y^*$. Оскільки моноїд X^* є суфіксно замкненою множиною, то $y_q \in X^*$. Отже $x_1 \in X \cap Y^*$ і $y_q \in X^* \cap Y$. З припущення індукції випливає, що це є неможливим, якщо слова x_1 і y_q є коротшими за слово w. Таким чином, ми

отримуємо, що $p = q = \varepsilon$. Але тоді $w \in X \cap Y = \varnothing$, отримали протиріччя. Це доводить рівність (8.44). Тепер ми доведемо, що множина X є префіксною. Для цього ми покажемо індукцією по $n \geqslant 1$, що жодне слово в множині X довжини n не має власного префікса в X. Це твердження, очевидно, виконується для $n = 1$.

Розглянемо слово $uv \in X \cap A^n$ з $n \geqslant 2$ і припустимо, що $u \in X$. З огляду на умову (8.40) маємо, що $uv = yx$ для деяких $y \in Y$ і $x \in X$. Слово u не може бути префіксом слова y, оскільки в протилежному випадку слово u мало б міститися в $X \cap Y^*$, бо моноїд Y^* є префіксно замкненою множиною та це є неможливим за умовою (8.44). Отже існує слово $u' \in A^+$ таке, що $u = yu'$ і $u'v = x$.

За умовою (8.43), $u' \in X^*$. Більше того $|x| \leqslant n$. За припущенням індукції з рівності $x = u'v$ випливає, що $v = \varepsilon$. Таким чином, маємо, що $u = uv$, а це доводить твердження індукції для n. Таким чином, множина X є префіксною. Аналогічне доведення показує, що множина Y є суфіксною.

Тепер ми в змозі довести, що (X, Y) є бісекцією. Рівність (8.42) доводить, що кожне слово у вільному моноїді A^* допускає факторизацію. Для доведення єдиності припутимо, що $xy = x'y'$ для $x, x' \in X^*$ і $y, y' \in Y^*$. Припустимо, що $|x| \geqslant |x'|$. Тоді $x = x'u$ і $uy = y'$ для деякого слова u. Оскільки моноїд X^* суфіксно замкненою множиною та моноїд Y^* є префіксно замкненою множиною, то маємо, що $u \in X^* \cap Y^*$. Отже $u = \varepsilon$ за рівністю (8.44). Звідси випливає, що $x = x'$ і $y = y'$. Оскільки множини X і Y є кодами, то це завершує доведення теореми. □

Теорема 8.2.6 показує, що наступний метод дозволяє нам побудувати всі бісекції.

(*i*) Розбиття алфавіта A на дві підмножини X_1 і Y_1.

(*ii*) Для кожного натурального числа $n \geqslant 2$ розбиття множини $Z_n = \bigcup_{i=1}^{n-1} Y_i X_{n-i}$ на дві підмножини X_n і Y_n.

(*iii*) Приймемо $X = \bigcup_{n \geqslant 1} X_n$ і $Y = \bigcup_{n \geqslant 1} Y_n$.

Іншими словами, під час обчислення можна поступово побудувати компоненти розбиття (P, Q). Зручним способом подання обчислень є відображення слів у множинах X і Y у двох стовпцях, коли вони отримані. Це проілюстровано наступним прикладом.

Приклад 8.2.7. Нехай $A = \{a, b\}$. Ми будуємо бісекцію вільного моноїда A^*, розподіляючи ітераційно добутки yx ($x \in X$, $y \in Y$) на два стовпчики, як це показано на рис. 8.3. Всі добутки, що залишилися, поміщають у множину R. Це дає визначальне рівняння для множини R, оскільки з рівностей

$$A \cup YX = X \cup Y \qquad \text{і} \qquad X = \{a, ba\} \cup R$$

отримуємо, що

$$R = \{b, b^2a\}\, R \cup b^2a\{a, ba\}.$$

Таким чином,

$$R = \{b, b^2a\}^*\, b^2a\{a, ba\},$$

або також

$$R = \left(b^2b^*a\right)^*\, b^2b^*a\{a, ba\}.$$

	X	Y
1	a	b
2	ba	
3		bba
$\geqslant 4$	R	

Рис. 8.3: Бісекція вільного моноїда A^*

Отже,

$$X = \left(b^2 b^* a\right)^* \{a, ba\},$$

і ця множина є кодом з прикладу 7.2.11.

Наступна домовленість буде використана для решти цього розділу. Для коду X над алфавітом A пара (U, V) підмножин вільного моноїда A^* буде називатися *бісекцією моноїда* X^*, якщо

$$\underline{X}^* = \underline{U}^* \underline{V}^*.$$

Щоб пристосуватися до звичайного означення бісекції, достатньо розглянути кодуючий морфізм для коду X.

Трисекцією вільного моноїда A^* називається трійка (X, Y, Z) підмножин вільної напівгрупи A^+, які утворюють факторизацію вільного моноїда A^*, тобто виконується рівність

$$\underline{A}^* = \underline{X}^* \underline{Y}^* \underline{Z}^*. \tag{8.45}$$

Доведемо наступний результат, який описує взаємозв'язок між бісекціями та трисекціями вільного моноїда.

Теорема 8.2.8. *Нехай (X, Y, Z) — трисекція вільного моноїда A^*. Існують бісекція (U, V) моноїда Y^* і бісекція (X', Z') вільного моноїда A^* такі, що (X, U) є бісекцією моноїда X'^* і (V, Z) є бісекцією моноїда Z'^*,*

$$\underline{A}^* = \underline{X}^* \underline{Y}^* \underline{Z}^* = \left(\underline{X}^* \underline{U}^*\right)\left(\underline{V}^* \underline{Z}^*\right) = \underline{X'}^* \underline{Z'}^*.$$

Перш ніж викласти доведення теореми 8.2.8, ми виведемо декілька корисних формул.

Твердження 8.2.9. *Нехай (X, Y, Z) — трисекція вільного моноїда A^*.*

1. *Множина X^*Y^* є суфіксно замкненою та множина Y^*Z^* є префіксно замкненою.*

2. Справджується одне з включень

$$Y^*X^* \subset X^* \cup Y^*Z^*, \tag{8.46}$$

$$Z^*Y^* \subset Z^* \cup X^*Y^*. \tag{8.47}$$

3. Коди X, Y і Z є $(2,0)$-, $(1,1)$- і $(0,2)$-граничними, відповідно.

Доведення. Спочатку доведемо твердження 1. Нехай $w \in X^*Y^*$ і v — суфікс слова w (див. рис. 8.4). Тоді $w = uv$ для деякого слова u. Покладемо $v = xyz$ з $x \in X^*$,

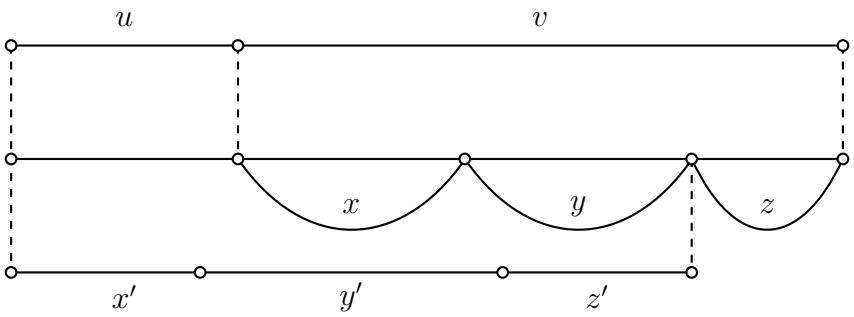


Рис. 8.4: Множина X^*Y^* є суфіксно замкненною

$y \in Y^*$ і $z \in Z^*$. Приймемо також $uxy = x'y'z'$ з $x' \in X^*$, $y' \in Y^*$ і $z' \in Z^*$. Тоді

$$w = uv = uxyz = x'y'(z'z).$$

З єдиності факторизації випливає, що $z' = z = \varepsilon$. Це доводить, що $v \in X^*Y^*$ і з останнього випливає, що множина X^*Y^* є суфіксно замкненою. Подібно отримуємо, множина Y^*Z^* є префіксно замкненою. Тепер перевіримо, чи виконується включення (8.46). Нехай $x \in X^*$ і $y \in Y^*$. Покладемо $yx = x'y'z'$ з $x' \in X^*$, $y' \in Y^*$ і $z' \in Z^*$. Якщо $x' = \varepsilon$, то $yx \in Y^*Z^*$. Отже, припускатимемо, що $x' \neq \varepsilon$. Слово x' не може бути префіксом слова y оскільки $y \in Y^*Z^*$ і множина Y^*Z^* є префіксно замкненою та $X^* \cap Y^*Z^* = \{\varepsilon\}$. Отже, існує слово u таке, що $x' = yu$ і $x = uy'z'$ (див. рис. 8.5). Оскільки слово u є суфіксом слова $x' \in X^*Y^*$, то воно міститься в множині X^*Y^*. Отже, $u = x''y''$ для деяких $x'' \in X^*$ і $y'' \in Y^*$. Це доводить, що $x = x''y''y'z'$. З єдиності факторизації випливає, $y'' = y' = z' = \varepsilon$. Таким чином, отримали, що $yx = x'y'z' = x' \in X^*$. Це завершує доведення включення (8.46). Включення (8.47) доводиться симетрично.

Код X є $(2,0)$-граничним. Справді, нехай $u, v, w \in A^+$ — слова такі, що $uv, vw \in X^*$. Оскільки слова v і w є суфіксами слів у вільному моноїді X^* і оскільки множина X^*Y^* э суфіксно замкненою, то слова v і w містяться в X^*Y^*. Отже, маємо

$$v = x'y' \qquad \text{і} \qquad w = xy$$

для деяких $x, x' \in X^*$, $y, y' \in Y^*$ (див. рис. 8.6). Слово $y'x$ є суфіксом слова $uvx \in X^*$. Аналогічними міркуваннями р=отримуємо, що слово $y'x$ міститься в множині X^*Y^*, а отже $y'x = x''y''$ для деяких слів $x'' \in X^*$ і $y'' \in Y^*$, звідси випливає, що $vw =$

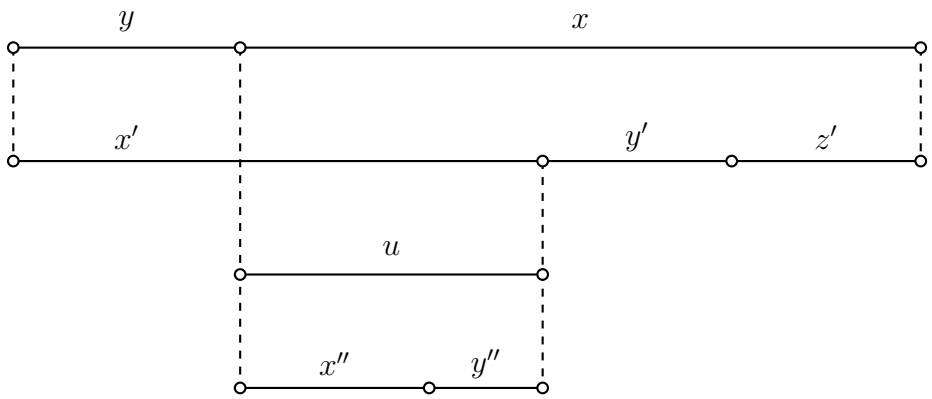


Рис. 8.5: $Y^*X^* \subset X^* \cup Y^*Z^*$

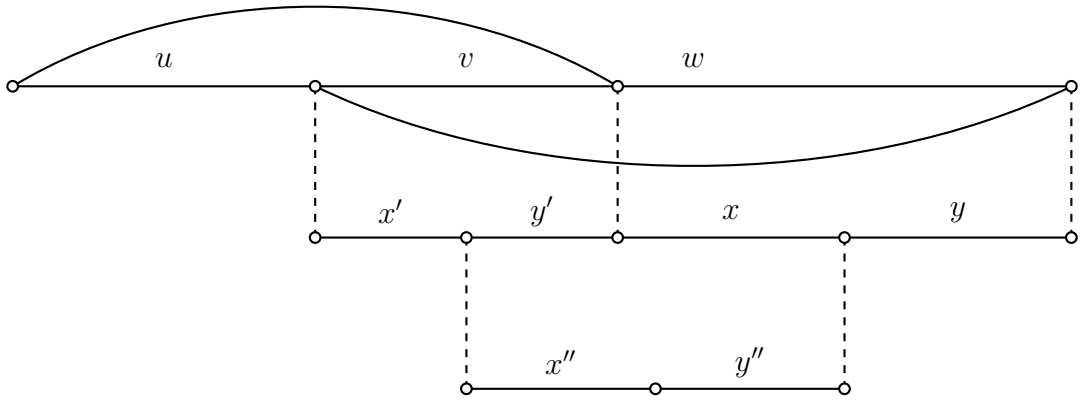


Рис. 8.6: Код X є $(2,0)$-граничним

$x'x''y''y$. Оскільки за припущенням $vw \in X^*$, то з єдиності факторизації випливає, що $y'' = y = \varepsilon$. Отож, $w = x \in X^*$. Це доводить, що X є $(2,0)$-граничним кодом. Аналогічно доводиться, що Z є $(0,2)$-граничним кодом.

Для доведення того, що код Y є $(1,1)$-граничним, розглянемо слова $u, v, w \in A^*$ такі, що $uv, vw \in Y^*$. Тоді $v \in X^*Y^*$, оскільки слово v є суфіксом слова uv в множині X^*Y^*, а також $v \in Y^*Z^*$, як лівий множник слова vw у множині Y^*Z^*. Отож, $v \in X^*Y^* \cap Y^*Z^*$. З єдиності факторизації випливає, що $v \in Y^*$. Це завершує доведення твердження. □

Доведення теореми 8.2.8. Покладемо

$$S = \{s \in Y^* \colon sX^* \subset X^*Y^*\}.$$

Спочатку зауважимо, що

$$S = \{s \in Y^* \colon sX^* \subset X^* \cup Y^*\}. \tag{8.48}$$

Справді, розглянемо слово $s \in Y^*$. Якщо $sX^* \subset X^* \cup Y^*$, то, очевидно, що $sX^* \subset X^*Y^*$. Припустимо протилежне, тобто, що $sX^* \subset X^*Y^*$. Оскільки $s \in Y^*$, то маємо $sX^* \subset Y^*X^*$ і використавши включення (8.46) отримуємо, що $sX^* \subset X^* \cup Y^*Z^*$. Отже,

$$sX^* \subset X^*Y^* \cap (X^* \cup Y^*Z^*) = (X^*Y^* \cap X^*) \cup (X^*Y^* \cap Y^*Z^*) = X^* \cup Y^*$$

за єдиністю факторизації. Це доводить рівність (8.48). Далі, S є підмоноїдом вільного моноїда A^*. Справді, $\varepsilon \in S$ і якщо $s, t \in S$, то $stX^* \subset sX^*Y^* \subset X^*Y^*$. Ми доведемо, що моноїд S, розглянутий як моноїд на алфавіті Y, задовольняє умову $C(1,0)$. Іншими словами, з $s, t \in Y^*$ і $st \in S$ випливає, що $t \in S$. Справді, розглянемо слово $x \in X^*$. Оскільки слово tx є суфіксом слова $stx \in X^*Y^*$ і оскільки множина X^*Y^* є суфіксно замкненою, то $tx \in X^*Y^*$. Отже, $t \in S$. Це доводить, що S є вільним підмоноїдом моноїда Y^*, породжений деяким $(1,0)$-граничним кодом U^*Y^+. Зауважимо, що код U є $(1,0)$-граничним, як код над алфавітом Y. За твердженням 8.2.2 код U є лівим множником деякої бісекції (U,V) вільного моноїда Y^*, з $V^* = Y^* \setminus UY^*$. Ми дамо інше означення множини V. Для цього покладемо

$$R = \{r \in Y^* \colon rX^* \cap Z^* \neq \varnothing\}.$$

Очевидно, що $R \cap S = \varepsilon$. Ми доведемо, що

$$R^* = V^*. \tag{8.49}$$

Спочатку доведемо, що $R \subset V^*$. Нехай $r \in R \setminus \{\varepsilon\}$. Приймемо $r = st$ з $s \in Y^+$ і $t \in Y^*$. Оскільки $r \in R$, то $stx \in Z^*$ для деякого слова $x \in X^*$. За включенням (8.46) маємо, що $tx \in X^* \cup Y^*Z^*$. Якщо $tx \in Y^*Z^*$, то $st \in Y^+Z^*$, що є неможливим, оскільки $stx \in Z^*$. Звідси випливає, що $tx \in X^*$. Отже $s \in R$. Оскільки $R \cap S = \{\varepsilon\}$, то $s \notin S$. Це доводить, що немає префікса $s \in Y^+$ слова r, який міститься в S. Іншими словами, жоден префікс слова r не міститься в коді U. Це доводить, що слово r міститься в моноїді V^*.

Далі ми доведемо, що $V^* \subset R^*$. Ми проведемо це доведення індукцією по довжині слів у множині V. Випадок порожнього слова є тривіальним. Нехай $v \in V^+$. Оскільки (U,V) є факторизацією, то $U^* \cap V^* = \{\varepsilon\}$. Звідси випливає, що $v \in U^* = S$. Отже за рівністю (8.48) існує деяке слово $x \in X^*$ таке, що $vx \in X^* \cup Y^*$. Оскільки $v \in Y^*$, то за включенням (8.46) маємо $vx \in Y^*Z^*$, і за попереднім зауваженням маємо навіть $vx \in Y^*Z^+$. Приймемо $vx = yz$ з $y \in Y^*$ і $z \in Z^+$. Тоді слово z не може бути суфіксом слова x, оскільки би в цьому випадку слово z мало б міститися в множині $X^*Y^* \cap Z^+$, що є неможливим. Таким чином існує деяке слово $w \in A^+$ таке, що $v = yw$ і $wx = z$. Оскільки слово w є суфіксом слова $v \in X^*Y^*$, то $w \in X^*Y^*$. Аналогічно слово w є префіксом слова $z \in Y^*Z^*$. Звідси випливає, що $w \in Y^*Z^*$. З єдиності факторизації випливає, що $w \in Y^*$. Слово y міститься в моноїді V^*. Справді, слово $y \in Y^*$ є префіксом слова v, і оскільки моноїд V^* є префіксно замкненою множиною, як підмножина вільного моноїда Y^*, то $y \in V^*$. Оскільки $|y| \leqslant |v|$, то з припущення індукції випливає, що $y \in R^*$. З іншого боку, з $w \in Y^*$ і $wx = z \in Z^*$ випливає, що $w \in R$. Отже, $v = yw \in R^*$. Це завершує доведення рівності (8.49). До цього ми це довели рівність

$$\underline{A}^* = \underline{X}^*\underline{U}^*\underline{V}^*\underline{Z}^*, \tag{8.50}$$

з $Y^* = U^*V^*$, $S = U^*$ і $R^* = V^*$. Для завершення доведення, достатньо показати, що добутки $M = X^*U^*$ і $N = V^*Z^*$ є підмоноїдами. Справді, оскільки добуток (8.50) є однозначним, то $M = X^*U^*$ і $N = V^*Z^*$, звідки випливає, що $A^* = MN$. За твердженням 8.2.4 моноїди M і N є вільними, а їх бази складають бажану бісекцію (X', Y'). Для доведення того, що множина X^*U^* є підмоноїдом, достатньо показати, що $U^*X^* \subset X^* \cup U^*$. Отже, розглянемо слова $x \in X^*$ і $s \in U^* = S$. Тоді за (8.48) маємо $sx \in X^* \cup Y^*$. Але з $sx \in Y^*$ випливає $sx \in S$, оскільки

$$sxX^* \subset sX^* \subset X^* \cup Y^*.$$

Отже, $sx \in X^* \cup S$, а це доводить, що X^*U^* є підмоноїдом в A^*. На завершенні доведемо, що V^*Z^* є підмоноїдом в A^*. Для цього покажемо, що виконується включення

$$Z^*R \subset R \cup Z^*. \tag{8.51}$$

З цього випливатиме, що $Z^*R^* \subset R^* \cup Z^*$, що в свою чергу доводить наше твердження з огляду на (8.49). Для доведення включення (8.51), зафіксуємо довільні $z \in Z^*$ і $r \in R$. Оскільки $r \in Y^*$, то з включення (8.47) випливає, що $zr \in Z^* \cup X^*Y^*$. З означення множини R випливає, що $rx \in Z^*$ для деякого слова $x \in X^*$, а це доводить, що $zrx \in Z^*$. Оскільки множина Y^*Z^* є префіксно замкненою, то $z \in Y^*Z^*$. З єдиності факторизації отримуємо, що $zr \in Z^* \cup Y^*$. Якщо $zr \in Y^*$, то $zr \in R$, оскільки $zrx \in Z^*$. Отже, $zr \in Z^* \cup R$ і це доводить включення (8.51). □

Теорема 8.2.8 показує, що всі трисекції можуть бути побудовані шляхом "склеювання" разом квадросекцій, отриманих послідовністю бісекцій. З наступного прикладу випливає, що навпаки, трисекцію не завжди можна отримати двома бісекціями.

Приклад 8.2.10. Нехай $A = \{a, b\}$. Суфіксний код

$$Z' = \left\{b, ba, ba^2\right\}$$

є $(0,1)$-граничним. Отже код Z' є правим множником бісекції (X', Z') вільного моноїда A^* з

$$X'^* = A^* \setminus A^*Z'.$$

Застосувавши рівність

$$\underline{Z'}\,\underline{X'} + \underline{A} = \underline{Z'} + \underline{X'},$$

отриману з рівності (8.31), маємо

$$\underline{A} - \underline{Z'} = (1 - \underline{Z'})\,\underline{X'},$$

а отже

$$\underline{X'} = \underline{Z'}^* (\underline{A} - \underline{Z'}).$$

Звідси випливає, що

$$\begin{aligned}
\underline{X'} &= \underline{Z'}^* \left(a - ba - ba^2\right) = \\
&= \left(\underline{Z'}^* - \underline{Z'}^* b - \underline{Z'}^* ba\right) a = \\
&= \left(1 + \underline{Z'}^* \left(b + ba + ba^2\right) - \underline{Z'}^* b - \underline{Z'}^* ba\right) a = \\
&= \left(1 + \underline{Z'}^* ba^2\right) a.
\end{aligned}$$

Отже,

$$X' = Z'^* ba^3 \cup \{a\}.$$

Далі означимо

$$U = (ba)^* ba^3, \qquad V = ba \qquad \text{і} \qquad Z = \left\{b, ba^2\right\} (ba)^*.$$

Пара (V, Z) є, очевидно, бісекцією моноїда Z'^*. Більше того, очевидно, що

$$U \subset X^*.$$

Це включення показує, що над алфавітом X' множина U є правим множником бісекції (X, U) моноїда X'^* з

$$X = U^* \left(X' \setminus U\right).$$

Більше того,

$$U^* V^* = \left\{ba, ba^3\right\}^*.$$

Тоді, поклавши

$$Y = \left\{ba, ba^3\right\},$$

отримуємо, що (U, V) є бісекцією моноїда Y^*. Таким чином, ми отримали

$$\underline{A}^* = \underline{X'^*}\,\underline{Z'^*} = \underline{X^*}\,\underline{U^*}\,\underline{V^*}\,\underline{Z^*} = \underline{X^*}\,\underline{Y^*}\,\underline{Z^*},$$

і (X, Y, Z) є трисекцією вільного моноїда A^*. Ні множина X^*Y^*, ні множина Y^*Z^* не є підмоноїдом вільного моноїда A^*. Справді, $ba \in Y$ і $a \in X$, оскільки $a \in X' \setminus U$. Однак, $ba^2 \in Z$, а отже

$$ba^2 \notin X^*Y^*.$$

Аналогічно $b \in Z$ і $ba^3 \in Y$, але $b^2a^3 \in X$ звідки випливає, що

$$b^2a^3 \notin Y^*Z^*.$$

Це означає, що трисекцію (X, Y, Z) неможливо отримати двома бісекціями.

8.3 Вправи до розділу 8

Підрозділ 8.1

В. 8.3.1. Нехай $A = \{1, 2, \ldots, n\}$ і $X_j = j\{j+1, \ldots, n\}^*$ для $j \in A$. Доведіть, що сім'я $(X_j)_{1 \leqslant j \leqslant n}$ є факторизацією вільного моноїда A^*.

В. 8.3.2. Нехай $\varphi\colon A^* \to \mathbb{R}$ — морфізм в адитивний моноїд. Для $r \in \mathbb{R}$ покладемо

$$C_r = \{v \in A^+ \colon \varphi(v) = r|v|\} \qquad \text{і} \qquad B_r = C_r \setminus \left(\bigcup_{s \geqslant r} C_s\right) A^+.$$

Доведіть, що сім'я $(B_r)_{r \in \mathbb{R}}$ зі звичайним природним порядком на $\mathbb{R}$ є факторизацією вільного моноїда A^*.

В. 8.3.3. (Ліва) *стандартна факторизація* слова Линдона $w \in L \setminus A$ визначається як пара

$$\pi(w) = (l, m)$$

слів у вільній напівгрупі A^+ таких, що $w = lm$ і l є найдовший власний префікс слова w, який міститься в множині L. Доведіть, що $m \in L$ і $l \prec m$.

(Підказка: Розгляньте факторизацію слова m як незростаючий добуток слів Линдона.)

Доведіть, якщо $\pi(w) = (l, m)$ і $\pi(m) = (p, q)$, то $p \preccurlyeq l \prec m$.

В. 8.3.4. Доведіть, що множина L слів Линдона над алфавітом A є множиною Лазарда.

(Підказка: Покладемо $L \cap A^n = \{z_1, z_2, \ldots, z_k\}$ з $z_1 \leqslant z_2 \leqslant \cdots \leqslant z_k$. Доведіть, що $z_i \in Z_i$ для $1 \leqslant i \leqslant k$, де

$$\begin{aligned} Z_1 &= A, \\ Z_{i+1} &= Z_i^*(Z_i \setminus \{z_i\}) \quad (1 \leqslant i \leqslant k). \end{aligned}$$

Доведіть, що множина Z_i містить усі слова z_r такі, що $\pi(z_r) = (z_s, z_t)$ з $s \leqslant i \leqslant r$.)

В. 8.3.5. Доведіть, що множина L_n слів Линдона довжини n над k-літерним алфавітом є круговим кодом. Доведіть, що L_n є кодом без ком тоді і тільки тоді, коли $n = 1$ або ($n = 2$, $k \leqslant 3$), або ($n = 3, 4$ і $k \leqslant 2$).

В. 8.3.6 (**теорема Линдона–Шутценбергера**)**.** Доведіть, якщо три слова x, y, z задовольняють рівність $x^m y^n = z^p$ з $m, n, p \geqslant 2$, то ці слова x, y, z належать до одного циклічного підмоноїда t^*.

(Підказка: Спочатку доведіть, що висновок виконується якщо $p \geqslant 3$, розглянувши спряження z' слова z, яке є словом Линдона. Тоді розв'яжіть випадок $p = 2$, використавши факто, що для деякого спряження x' слова x, рівність $x'^m = u^2 y^n$ виконується для деякого слова u.)

В. 8.3.7. Нехай $X = \{x, y\}$ — код з двома елементами. Доведіть, якщо моноїд X^* не є чистим, то множина $x^*y \cup y^*x$ містить слово, яке не є примітивним.

(Підказка: Розгляньте найменше натуральне число $i \geqslant 1$ таке, що $w^2 \in X^*xy^ixX^*$. Замінивши слово w його X-спряженим, припустіть, що слово y^ix є префіксом слова w і слово x є суфіксом слова w. Нехай слово w' є X-спряженим словом слова w таким, що $wh = hw'$ і з h коротшим за слово $z \in X$ таким, що $w' \in X^*z$. Охарактеризуйте три випадки:

(1) $w' \in yX^*x$,
(2) $w' \in xX^*x$,
(3) $w' \in X^*y$ і $|hx| > |y^i|$.

Обговоріть випадки (2) та (3) відповідно до того, чи виконується умова $|hx| > |y^i|$, чи ні.)

В. 8.3.8. Виведіть з вправи 8.3.7, якщо $x = uv$ і $y = vu$ є спряженими примітивними словами, то моноїд $X^* = \{x, y\}^*$ є вільним.

В. 8.3.9. Доведіть, що коефіцієнт перед z^n у ряді рівності (7.13) дорівнює кількості множин примітивних намист, що перетинають моноїд X^*, чий *лінійний степінь* (що дорівнює сумі довжин намист) дорівнює n. Запропонуєте два доведення, одне, яке використовує рівність (7.17), а друге застосування до вільного моноїда X^* властивості повних факторизацій викладеної в наслідку 8.1.7, використавши той факт, що X^* є дуже чистим підмоноїдом.

В. 8.3.10. Візьміть позначення вправи 7.4.10, з елементами p_n які визначені на початку підрозділу 7.3. Доведіть, що елементи v_n є невід'ємними цілими числами.

(Підказка: Вони є завжди цілими числами і це випливає з рівності (7.13). Ітерацією фундаментальної бісекції твердження 8.2.2, доведіть існування кодів X_n і C_n, які визначаються наступним чином:

$$\begin{aligned} X_1 &= X, \\ C_n &= \{x \in X_n \colon |x| = n\}, \\ X_{n+1} &= (X_n \setminus C_n)C_n^* \end{aligned}$$

такі, що вільний моноїд X^* має факторизацію $X^* = C_1^*C_2^* \cdots C_n^*X_{n+1}^*$. Доведіть, що число v_n дорівнює потужності коду C_n.)

В. 8.3.11. Підмножина L вільного моноїда A^* називається *циклічною*, якщо виконуються такі умови:

(*i*) для довільних слів $u, v \in A^*$ умова $uv \in L$ виконується тоді і лише тоді, коли $vu \in L$;
(*ii*) для кожного слова $w \in A^*$ та для кожного додатнього цілого числа n умова $w \in L$ виконується тоді і лише тоді, коли $w^n \in L$.

Дзета-функція визначається як лівий бік рівності (7.13), де p_n — кількість слів довжини n у множині L.

Доведіть наступні твердження:

(*i*) якщо X є круговим кодом, то замикання стосовно спряження моноїда X^* є циклічною множиною;
(*ii*) якщо код X є раціональним, то замикання стосовно спряження моноїда X^* є раціональною множиною;
(*iii*) дзета-функція коду X дорівнює породжуючій функції моноїда X^*;
(*iv*) дзета-функція циклічної множини L має розширення виражене правою частиною рівності (7.17), де через l_n позначається кількість примітивних намист довжини n, які містяться в L.

Підрозділ 8.2

В. 8.3.12. Доведіть, якщо факторизація

$$A^* = X_n^* X_{n-1}^* \cdots X_1^*$$

отримана композицією бісекцій, то X_i є $(i-1, n-i)$-граничним кодом.

(Підказка: Використайте індукцію по n.)

В. 8.3.13. Нехай X — $(2,0)$-граничний код над алфавітом A. Нехай $M \subset A^*$ — підмоноїд, породжений суфіксами слів у коді X. Доведіть, що моноїд M є унітарним справа. Нехай U — префіксний код породжуючий моноїд M. Доведіть, що існує бісекція вільного моноїда A^* вигляду (U, Z). Доведіть, що множина X, яка розглядається як код над множиною U є $(1,0)$-граничним кодом. Виведіть з цього, що (X, Y, Z) є трисекцією вільного моноїда A^*. Це доводить, що кожен $(2,0)$-граничний код є лівим множником деякої трисекції.

В. 8.3.14. Нехай

$$A = \{a, b, c, d, e, f, g\} \qquad \text{і} \qquad Y = \{d, eb, fa, ged, dac\}.$$

Доведіть такі твердження:

(*i*) код Y є $(1,1)$-граничним;
(*ii*) не існує трисекції вільного моноїда A^* вигляду (X, Y, Z).

(Підказка: Використайте твердження 8.2.9.)

В. 8.3.15. Нехай $y \in A^+$ — необлямоване слово. Доведіть такі твердження:

(*i*) існує трисекція вільного моноїда A^* вигляду $(X, \{y\}, Z)$;
(*ii*) префікс (відп., суфікс) слова y міститься в моноїді Z^* (відп., в моноїді X^*).

(Підказка: Спочатку побудуйте бісекцію (X', Z) вільного моноїда A^* таку, що X'^* є підмоноїдом в A^*, породженим суфіксами слова y.)

Нотатки до розділу 8

Поняття факторизації було введено Шютценбергером в статті [184], де він і довів теорему 8.1.2. Факторизація вільних моноїдів дуже тісно пов'язана з розкладами у прямі суми вільних алгебр Лі. Повне описання цього зв'язку можна знайти в монографіях [131, 132] і [204]. Твердження 8.1.4 є особливим випадком судження, відомого як формула Бейкера–Кемпбелла–Гаусдорфа (див., наприклад, [131,132]). Поняття множини Лазарда вперше введено В'єно в монографії [204]. Ряд прикладів інших факторизацій та бібліографію з цього напрямку можна знайти у монографіях [131, 132]. Скінченні факторизації вивчалися Шютценбергером і В'єно. Твердження 8.2.4 взято зі статті Шютценбергера [184], а теорема 8.2.6 належить В'єно [203]. Дисертація В'єно [203] містить інші результати про скінченні факторизації. Серед них існує необхідна та достатня умова з точки зору побудови твердження 8.2.4, щоб множники бісекції були розпізнаваними. Квадросекції вивчалися Кробом в статті [114].

Факторизація прикладу 8.1.8 належить Шпітцеру (див. [131, 132]). Вправа 8.3.6 є теоремою зі статті [140]. Доведення, викладені в розв'язку цієї вправи випливає з результатів праці [87]. Вправи 8.3.7 і 8.3.8 взяті зі статті Льонта та Шютценбергера [124]. Доведення, викладені в розв'язках випливають з результатів праці [23].

Дзета-функції циклічних множин вперше були введені в статті [35]. У цій статті доведено, що дзета-функція раціональної циклічної множини є раціональною функцією (див. також [27]). Вправа 8.3.11 доводить, що це твердження є істинним, якщо циклічна множина є замиканням стосовно спряження раціонального коду. В статті [167] доведено, що кожна раціональна циклічна множина є диз'юнктним об'єднанням замикання стосовно спряження раціональних дуже чистих моноїдів. Звідси випливає, що дзета-функція є $\mathbb{N}$-раціональною.

Вправи 8.3.13 і 8.3.14 взяті зі статті В'єно [203].

Розділ 9

Однозначні моноїди відношень

Кожному однозначному автоматові відповідає моноїд відношень, який також називається однозначним. Відношенню на цьому моноїді відповідає кожному слову та обчислення на словах замінено обчисленнями на відношеннях.

Головний результат цього розділу (теорема 9.4.1) стверджує, що дуже тонкі коди є в точності коди, для яких асоційований моноїд задовольняє умову скінченності: *він містить відношення скінченного додатнього рангу*. Цей результат пояснює, чому тонкі коди є природною сім'єю, що містить розпізнавані коди. Це дозволяє довести властивості тонких кодів міркуванням у скінченних структурах. Як наслідок, наведемо, для прикладу, альтернативне доведення максимальності тонких повних кодів, яке не використовує ймовірностних методів.

Основний результат також дозволяє визначити для кожного тонкого коду деякі важливі параметри: степінь і групу коду. Групою тонкого коду є скінченна група підстановок. Степенем коду є кількість елементів на яких ця група діє. Ці параметри відображають властивості слів за допомогою "Інтерпретацій". Наприклад, синхронізовані коди у розумінні розділу 3 — це такі коди, що мають степінь 1.

Цей розділ організовано наступним чином. У підрозділі 9.1 доведено основні властивості однозначних моноїдів відношень. Ці моноїди постійно появляються у тому, як виникають, оскільки кожен однозначний автомат породжує однозначний моноїд відношень. У підрозділі 9.2 визнача.nmcz два зображення однозначних моноїдів відношень, які називаються $\mathcal{R}$- і $\mathcal{L}$-зображеннями, або зображеннями Шютценбергера. Ці зображення є відносними стосовно фіксованого ідемпотента, вибраного в моноїді, і вони описують спосіб дії елементів моноїда шляхом правого чи лівого множення на $\mathcal{R}$-клас і $\mathcal{R}$-клас ідемпотента.

Поняття рангу відношення визначено в підрозділі 9.3. Найважливіший результат у цьому підрозділі стверджує, що мінімальний ідеал однозначного моноїда відношень утворюється з відношень, що мають мінімальний ранг, за умови, що ранг є скінченним (теорема 9.3.10). Більше того, у цьому випадку мінімальний ідеал має коректно організовану структуру.

У підрозділі 9.1 ми повертаємося до кодів. Ми означуємо поняття дуже тонкого коду, який є деталізацією поняття тонкого коду. Це два поняття збігаються у випадку повних кодів. Далі ми доведемо фундаментальну теорему: код X є дуже тонким толі і лише тоді, коли асоційований неоднознапчний моноїд відношень містить елементи скінченного додатнього рангу (теорема 9.4.1). Викладено різні наслідки цього

результату про структуру кодів.

Підрозділ 9.5 містить означення групи та степеня коду. Визначення дається через квітковий автомат, а потім доведено, що воно не залежить від розглянутого автомата. Ми також показуємо, як степінь може бути вираженим у термінах інтерпретації слів.

9.1 Однозначні моноїди відношень

Відношенням m над P і Q називається підмножина декартового добутку $P \times Q$. Якщо $P = Q$, то будемо говорити, що m є *відношенням* (*бінарним відношенням*) над P. Якщо $(p, q) \in m$, то ми записуватимемо еквівалентно

$$(p,q) \in m \iff (p,m,q) = 1 \iff pmq \iff p \xrightarrow{m} q \iff m_{p,q} = 1. \tag{9.1}$$

Кожне з цих позначень стосується специфічного погляду на відношення. Четверте дозволяє розглядати відношення як граф, третє імітує відношення порядку, останнє стосується погляду на відношення як на матрицю. Очевидно, що заперечення перебування у відношенні можемо записати одним з еквівалентних виглядів:

$$(p,q) \notin m \iff (p,m,q) = 0 \iff m_{p,q} = 0. \tag{9.2}$$

У цих виразах 0 і 1 приписуються елементи булевого напівкільця. Зокрема, розглянуті як матриці, відношення є булевими матрицями. Оскільки 0 і 1 є елементами кожного напівкільця, то кожне відношення також можна розглядати як матрицю над цим напівкільцем. Аналогічно, рядок або стовпець відношення — це рядок або стовпець відповідної матриці. Отже,

$$m_{p*} = \{q \in Q \colon m_{pq} = 1\} \qquad \text{і} \qquad m_{*q} = \{p \in Q \colon m_{pq} = 1\}.$$

Кожне часткове відображення з P в Q є зокрема відношенням над P і Q. Зокрема, підстановка на множині Q є відношенням на Q.

Добутком (або *композицією*) відношення m над P і Q та відношення n над Q і R називається відношення mn, яке визначається наступним чином

$$(p,r) \in mn \quad \iff \quad \exists q \in Q \colon (p,q) \in m \quad \text{і} \quad (q,r) \in n.$$

Множина $\mathfrak{P}(Q \times Q)$ відношень над множиною Q є моноїдом стосовно операції добутку відношень. Добуток mn відношень називається *однозначним*, якщо для довільних $(p, r) \in mn$ існує щонайбільше один лемент $q \in Q$ такий, що $(p, q) \in m$ і $(q, r) \in n$.

Якщо відношення розглядати як графи, це становить єдиність шляхів довжиною 2, тобто з

$$p \xrightarrow{m} q \xrightarrow{n} r, \qquad p \xrightarrow{m} q' \xrightarrow{n} r,$$

випливає рівність $q = q'$. Розглядаючи як матриці, означення еквівалентно властивості, що значення добутку m і n має однакове значення в будь-якому напівкільці. Зокрема, розглядаючи як матриці над множиною натуральних чисел $\mathbb{N}$, суми $\sum_{q \in Q} m_{p,q} n_{q,r}$ набувають лише значення 0 або 1. Ще один спосіб переконатися в цьому — це побачити, якщо $\mathbf{r}$ — рядок матриці m і $\mathbf{l}$ — стовпчик матриці n, то існує щонайбільше один елемент $q \in Q$ такий, що $\mathbf{r}_q = \mathbf{l}_q = 1$.

Приклад 9.1.1. Нехай m і n — відношення, що визначаються в матричній формі наступним чином:

$$m = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}, \qquad n = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

Безпосередньо звичайним множенням матриць над кільцем цілих чисел отримуємо

$$mn = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix},$$

а отже добуток відношень m і n є однозначним.

Моноїд M відношень над множиною Q називається *однозначним*, якщо для всіх $m, n \in M$ добуток mn є однозначим. Як підмоноїд моноїда $\mathfrak{P}(Q \times Q)$ моноїд M містить одиницю id_Q, що є тотожним відображенням множини Q.

Приклад 9.1.2. Кожне моноїд відношень над множиною Q, який складається з часткових перетворень є однозначним.

Приклад 9.1.3. Легко перевіряється, що моноїд, породжений матрицями з прикладу 9.1.1 є однозначним і має дев'ять елементів.

Нагадаємо, що моноїд M відношень над множиною Q називається *транзитивним*, якщо для довільних $p, q \in Q$ існує відношення $m \in M$ таке, що $(p, q) \in m$.

Нехай $\mathcal{A} = (Q, I, T)$ — автомат над алфавітом A. Нагадаємо, що для кожного слова $w \in A^*$ через $\varphi_{\mathcal{A}}(w)$ позначається відношення на множині Q, яке визначається наступним чином:

$$(p, q) \in \varphi_{\mathcal{A}}(w) \qquad \Longleftrightarrow \qquad p \xrightarrow{w} q.$$

Як це випливає з означення відображення $\varphi_{\mathcal{A}}$ є морфізмом з вільного моноїда A^* в моноїд відношень над множиною Q.

Наступне твердження стосується однозначних моноїдів відношень і однозначних автоматів.

Твердження 9.1.4. *Нехай $\mathcal{A}$ — автомат над алфавітом A. Тоді автомат $\mathcal{A}$ є однозначним тоді і тільки тоді, коли моноїд $\varphi_{\mathcal{A}}(A^*)$ є однозначним. Більше того, якщо $\mathcal{A} = (Q, 1, 1)$, то автомат $\mathcal{A}$ є обрізаним тоді і тільки тоді, коли моноїд $\varphi_{\mathcal{A}}(A^*)$ є транзитивним.*

Доведення. Припустимо, що існують шляхи

$$p \xrightarrow{u} r \xrightarrow{v} q, \qquad p \xrightarrow{u} r' \xrightarrow{v} q$$

в автоматі $\mathcal{A}$. Якщо $r \neq r'$, то добуток елементів $\varphi_{\mathcal{A}}(u)$ і $\varphi_{\mathcal{A}}(v)$ є неоднозначним, і очевидно, що виконується обернене твердження.

Далі, нехай $\mathcal{A} = (Q, 1, 1)$ — обрізаний автомат. Нехай $p, q \in Q$. Нехай $u, v \in A^*$ — такі слова, що $p \xrightarrow{u} 1$ і $1 \xrightarrow{v} q$ є шляхами в автоматі $\mathcal{A}$. Тоді $p \xrightarrow{uv} q$ є шляхом в автоматі $\mathcal{A}$, а отже $p\varphi_{\mathcal{A}}(uv)q$. Обернене твердження є очевидним. □

Відношення m на множині Q називається *оборотним*, якщо існує відношення n на Q таке, що $mn = nm = \mathrm{id}_Q$, де id_Q — відношення рівності на Q.

Твердження 9.1.5. *Відношення є оборотним тоді і тільки тоді, коли воно є підстановкою.*

Доведення. Нехай m — оборотне відношення на Q і n — відношення на Q таке, що $mn = nm = \mathrm{id}_Q$. Для кожного $p \in Q$ існує елемент $q \in Q$ такий, що pmq, оскільки з відношення $pmnp$ маємо $pmqnp$ для деякого $q \in Q$. Такий елемент q — єдиний: якщо pmq', то $qnpmq' = q\,\mathrm{id}_Q\,q'$, а отже $q = q'$. Звідси випливає, що m є відображенням. Тепер, якщо pmq і $p'mq$, то $pmqnp$ і $p'mqnp$, звідки випливає, що $p' = p$. Таким чином, відображення m є ін'єктивним. Оскільки $nm = \mathrm{id}_Q$, то відображення m є також сур'єктивним. Отже, m є підстановкою.

Обернене твердження є очевидним. □

Нехай m — відношення над множиною Q. *Фіксованою точкою* відношення m називається елемент $q \in Q$ такий, що qmq. У матричній формі фіксованими точками є індекси q такі, що $m_{q,q} = 1$, іншими словами такими є індекси, для яких існує одиниця 1 на діагоналі. Через $\mathrm{Fix}(m)$ позначатимемо *множину нерухомих точок відношення* m.

Твердження 9.1.6. *Нехай M — однозначний моноїд відношень над множиною Q. Нехай $e \in M$ і $S = \mathrm{Fix}(e)$. Наступні умови є еквівалентними:*

(*i*) *e є ідемпотентом;*

(*ii*) *для довільних $p, q \in Q$, маємо $p \xrightarrow{e} q$ тоді і лише тоді, коли існує елемент $s \in S$ такий, що $p \xrightarrow{e} s$ і $s \xrightarrow{e} q$;*

(*iii*) *виконується умова*

$$e = \mathbf{lr} \qquad i \qquad \mathbf{rl} = \mathrm{id}_S, \tag{9.3}$$

де $\mathbf{l} \subset Q \times S$ і $\mathbf{r} \subset S \times Q$ є звуженнями відношення e на добутки $Q \times S$ і $S \times Q$, відповідно.

Якщо e є ідемпотентом, то більше того в матричній формі

$$\mathbf{l} = \begin{bmatrix} \mathrm{id}_S \\ \mathbf{l}' \end{bmatrix}, \qquad \mathbf{r} = \begin{bmatrix} \mathrm{id}_S & \mathbf{r}' \end{bmatrix}, \qquad e = \begin{bmatrix} \mathrm{id}_S & \mathbf{r}' \\ \mathbf{l}' & \mathbf{l}'\mathbf{r}' \end{bmatrix},$$

з $\mathbf{l}' \subset (Q \setminus S) \times S$ і $\mathbf{r}' \subset S \times (Q \setminus S)$ і $\mathbf{r}'\mathbf{l}' = 0$. Зокрема, відношення e є тотожним відношенням на $\mathrm{Fix}(e)$.

Розклад (9.3) ідемпотентного відношення називається *стовпчико-рядковим розкладом відношення*. Зауважимо, що

$$e\mathbf{l} = \mathbf{l} \qquad \text{і} \qquad \mathbf{r}e = \mathbf{r}, \tag{9.4}$$

оскільки

$$e\mathbf{l} = \mathbf{lrl} = \mathbf{l}\,\mathrm{id}_S = \mathbf{l} \qquad \text{і} \qquad \mathbf{r}e = \mathbf{rlr} = \mathrm{id}_S\,\mathbf{r} = \mathbf{r}.$$

Доведення твердження 9.1.6. $(i) \Rightarrow (ii)$ Нехай елементи $p, q \in Q$ є такими, що peq. Тоді pe^3q. Звідси випливає, що існують $s, t \in Q$ такі, що $peseteq$. Отож отримуємо, що $peseq$ і $peteq$. Оскільки моноїд M є однозначним, то $s = t$, а отже ses і $s \in S$. Обернене висловлення є очевидним.

$(ii) \Rightarrow (iii)$ Нехай $\mathbf{l} \subset Q \times S$ і $\mathbf{r} \subset S \times Q$ є звуженнями відношення e на добутки $Q \times S$ і $S \times Q$, відповідно. Якщо peq, то існує елемент $s \in S$ такий, що pes і seq. Тоді $p\mathbf{l}s$ і $s\mathbf{r}q$. Таким чином, якщо $p\mathbf{l}s$ і $s\mathbf{r}q$, то маємо $peseq$, а отже peq. Оскільки така фіксована точка s єдина, то $e = \mathbf{lr}$.

Тепер нехай $r, s \in S$ з $r\mathbf{rl}s$. Тоді $r\mathbf{rq}\mathbf{l}s$ для деякого елемента $q \in Q$. Отже, req і qes. Більше того, rer і ses, звідки випливає, що

$$rereqes \qquad \text{і} \qquad reqeses.$$

З однозначності моноїда M випливає, що $r = q = s$. І навпаки маємо $s\mathbf{rl}s$ для всіх $s \in S$.

$(iii) \Rightarrow (i)$ Маємо

$$e^2 = (\mathbf{lr})(\mathbf{lr}) = \mathbf{l}(\mathbf{rl})\mathbf{r} = \mathbf{lr} = e.$$

Отже, елемент e є ідемпотентом.

Припустимо тепер, що елемент e є ідемпотентом. Звуження відношення e на $S \times S$ є відношенням рівності. Справді відношення ses виконується для всіх $s \in S$, і якщо ser з $s, r \in S$, то $seser$ і $serer$, звідки однозначності моноїда M випливає, що $s = r$. Це доводить, що відношення l і r мають вказану форму. Не завершенні добуток $\mathbf{rl}$ дорівнює

$$\mathbf{rl} = \mathrm{id}_S + \mathbf{r}'\mathbf{l}'.$$

Оскільки $\mathbf{rl} = \mathrm{id}_S$, то звідси випливає рівність $\mathbf{r}'\mathbf{l}' = 0$, що і завершує доведення твердження. □

Нехай M — однозначний моноїд відношень над множиною Q і $e \in M$ — ідемпотент. Тоді eMe є моноїдом і e є одиничним елементом в eMe, оскільки $em = me = eme = m$ для всіх $m \in eMe$. Напівгрупа eMe є найбільший моноїд, який міститься в M і має e в якості одиничного елемента. Напівгрупа eMe називається моноїдом локалізованим в e (див. підрозділ 1.2). $\mathscr{H}$-клас $H(e)$ ідемпотента e є групою одиниць моноїда eMe (твердження 1.12.4).

Твердження 9.1.7. *Нехай M — однозначний моноїд відношень над множиною Q, e — ідемпотент в M і $S = \mathrm{Fix}(e)$ — множина нерухомих точок відношення e. Звуження γ елементів моноїда eMe на $S \times S$ є ізоморфізмом моноїда eMe на однозначний моноїд відношень над множиною S. Якщо $e = \mathbf{lr}$ — стовпчико-рядковий розклад відношення e, цей ізоморфізм визначається за формулою*

$$\gamma \colon m \to \mathbf{r}m\mathbf{l}. \tag{9.5}$$

Множина $\gamma(H(e))$ є групою підстановок над множиною S. Далі, якщо моноїд M є транзитивним, то образ $\gamma(eMe)$ також є транзитивним моноїдом.

Однозначний моноїд відношень $\gamma(eMe)$ будемо позначати через M_e, а групу підстановок $\gamma(H(e))$ — через G_e.

Доведення твердження 9.1.7. Нехай γ — відображення, означене за формулою (9.5). Якщо $m \in eMe$, то

$$(s, \gamma(m), t) = (s, \mathbf{r}m\mathbf{l}, t) = (s, m, t),$$

для $s, t \in S$, оскільки $s\mathbf{r}s$ і $t\mathbf{l}t$. Таким чином, відношення $\gamma(m)$ є звуженням елементів в eMe на множину $S \times S$. Далі, відображення γ є морфізмом, оскільки

$$\gamma(e) = \mathbf{r}e\mathbf{l} = \mathrm{id}_S$$

і

$$\gamma(mn) = \gamma(men) = \mathbf{r}(men)\mathbf{l} = \mathbf{r}m\mathbf{l}\mathbf{r}n\mathbf{l} = \gamma(m)\gamma(n)$$

для $m, n \in eMe$. На завершенні, відображення γ є ін'єктивним, оскільки якщо $\gamma(m) = \gamma(n)$ для деяких $m, n \in eMe$, то також $\mathbf{l}\gamma(m)\mathbf{r} = \mathbf{l}\gamma(n)r$. Але

$$\mathbf{l}\gamma(m)\mathbf{r} = \mathbf{l}\mathbf{r}m\mathbf{l}\mathbf{r} = eme = m.$$

Тоді $m = n$. Моноїд

$$M_e = \gamma(eMe)$$

є моноїдом відношень над множиною S, оскільки він містить відношення id_S. Він також є однозначним, як довільне звуження однозначного моноїда відношень.

На завершенні, множина $G_e = \gamma(H(e))$ складається з оборотних відношень. За твердженням 9.1.5, $G_e = \gamma(H(e))$ є групою підстановок над множиною S.

Припустимо, що моноїд M є транзитивним. Для довільних $s, t \in S$ існує елемент $m \in M$ такий, що smt. Тоді також $semet$. Взявши звуження на множину S, отримуємо $s\gamma(eme)t$. Оскільки $\gamma(eme) \in M_e$, то це доводить, що моноїд M_e є транзитивним. □

Приклад 9.1.8. Розглянемо відношення m, яке визначається в матричній формі наступним чином:

$$m = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

Тоді

$$m^2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \text{і} \quad m^3 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

Отже, m^2 є ідемпотеним відношенням. Моноїд $M = \{1, m, m^2\}$ є однозначним моноїдом відношень. Нерухомими точками відношення $e = m^2$ є 1 і 2, і стовпчикорядковим розкладом відношення e є

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \mathbf{l}\mathbf{r}.$$

Маємо

$$m = \mathbf{l}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\mathbf{r},$$

і звуження відношення m на множину $\{1, 2\}$ є транспозицією (12). Моноїд M_e збігається з групою G_e, яка ізоморфна фактор-групі $\mathbb{Z}/2\mathbb{Z}$.

Нехай M — довільний моноїд. Ми порівняємо зараз локалізовані моноїди двох ідемпотентів $\mathscr{D}$-класу. Нехай e і e' — два $\mathscr{D}$-еквівалентні ідемпотенти моноїда M. Оскільки, за означенням, $\mathscr{D} = \mathscr{R}\mathscr{L}$, то існує елемент $d \in M$ такий, що $e\mathscr{R}d\mathscr{L}e'$. За означенням цих відношень існує впорядкована четвірка

$$(a, a', b, b') \tag{9.6}$$

елементів моноїда M така, що

$$ea = d, \qquad da' = e, \qquad bd = e' \qquad \text{і} \qquad b'e' = d, \tag{9.7}$$

(див. рис. 9.1). Впорядкована четвірка (9.6) називається *системою переходу* з e до

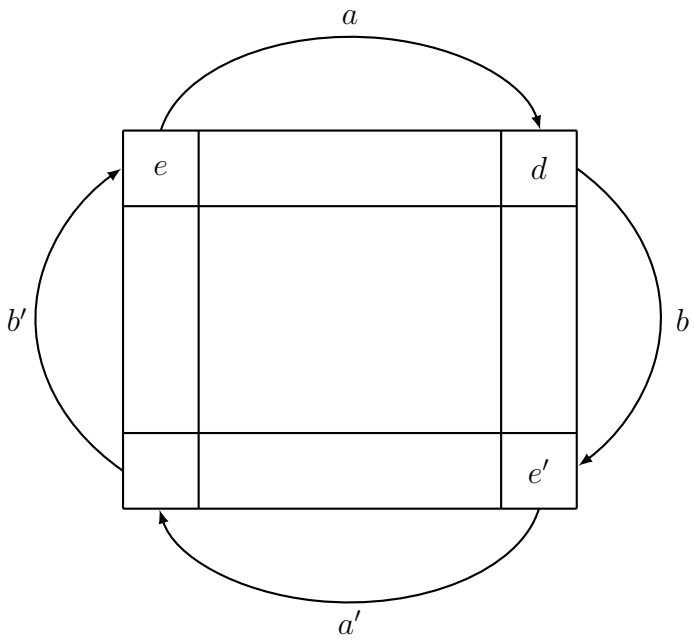


Рис. 9.1: Система переходу

e'. На рис. 9.1 множення справа на a або a' зображена горизонтальною стрілкою, а множення зліва на b або b' зображено вертикальною стрілкою.

Наступні формули легко вивести з формули (9.7). Більше того, зауважимо, що більшість з цих рівностей зустрічаються в підрозділі 1.12:

$$eaa' = e, \qquad bea = e', \qquad ea = b'e', \tag{9.8}$$

і

$$bb'e' = e', \qquad b'e'a' = e, \qquad be = e'a', \tag{9.9}$$

причому остання рівність отримується так

$$be = bb'e'a' = e'a'.$$

Оскільки e і e' є ідемпотентами, то справджуються наступні рівності:

$$eabe = e, \qquad e'a'b'e' = e'. \tag{9.10}$$

Справді, за рівностями (9.8) маємо, що

$$e' = e'e' = beabea.$$

Отже

$$b'e'a' = b'beabeaa'.$$

Оскільки

$$be = e'a'$$

за рівностями (9.9), то маємо

$$b'be = b'e'a' = e.$$

Аналогічно, позаяк рівностями (9.8) маємо, що

$$eaa' = e,$$

то отримуємо рівність

$$b'e'a' = e = eabe.$$

Це доводить першу рівність. Доведення другої рівності є аналогічним.

Два моноїди відношень M над Q і M' над Q' називаються *еквівалентними*, якщо існує відношення $\theta \in \mathfrak{P}(Q \times Q')$, яке є бієкцією з Q на Q' таке, що відображення

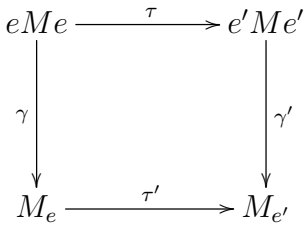
$$m \mapsto \theta^t m \theta$$

є ізоморфізмом з M на M' (відношення θ^t є транспонуванням відношення θ). Оскільки відношення θ є бієкцією, то маємо $\theta^t = \theta^{-1}$. Таким чином, у випадку де M і M' є групами підстановок, це означення збігається з означенням викладеним у підрозділі 1.13.

Твердження 9.1.9. *Нехай M — однозначний моноїд відношень над множиною Q і $e, e' \in M$ — два $\mathscr{D}$-еквівалентні ідемпотенти. Тоді моноїди eMe і $e'Me'$ є ізоморфними, моноїди M_e і $M_{e'}$ є еквівалентними та групи G_e і $G_{e'}$ є еквівалентними групами підстановок. Точніше, нехай $S = \mathrm{Fix}(e)$, $S' = \mathrm{Fix}(e')$, $e = \mathbf{lr}$, $e' = \mathbf{l}'\mathbf{r}'$ — їх стовпчико-рядкові розклади, γ і γ' — звуження на $S \times S$ і $S' \times S'$, і (a, a', b, b') — система переходу з e до e'. Тоді*

(*i*) *відображення $\tau\colon m \mapsto bma$ є ізоморфізмом з eMe на $e'Me'$;*
(*ii*) *відношення $\theta = \mathbf{r}a\mathbf{l}' = \mathbf{r}b'\mathbf{l}' \in \mathfrak{P}(S \times S')$ є бієктивним відображенням з S на S';*
(*iii*) *відображення $\tau'\colon n \mapsto \theta^t n \theta$ є ізоморфізмом з M_e на $M_{e'}$;*

(*iv*) *діаграма*



є комутативною.

Доведення. (*i*) Нехай $m \in eMe$. Тоді

$$\tau(m) = bma = bemea = e'a'mb'e',$$

оскільки $be = e'a'$ і $b'e' = ea$ за формулами (9.8) і (9.9). З цього випливає, що $\tau(m) \in e'Me'$. Далі

$$\tau(e) = bea = e'$$

за формулою (9.8). Для $m, m' \in eMe$ за формулою (9.10) маємо

$$\tau(m)\tau(m') = bmabm'a = bmeabem'a = bmem'a = bmm'a = \tau(mm').$$

Таким чином, відображення τ є морфізмом. На завершенні, легко бачити, що відображення $m' \mapsto b'm'a'$ є оберненим до τ, а отже τ є ізоморфізмом з eMe на $e'Me'$.

(*ii*) Маємо $eae' = eb'e'$. Звідси випливає, що $\mathbf{r}eae'\mathbf{l}' = \mathbf{r}eb'e'\mathbf{l}'$. Оскільки за (9.4) маємо $\mathbf{r}e = \mathbf{r}$ і $e'\mathbf{l}' = \mathbf{l}'$, то отримуємо, що

$$\theta = \mathbf{r}a\mathbf{l}' = \mathbf{r}b'\mathbf{l}'.$$

Відношення θ оборотним зліва, оскільки

$$(\mathbf{r}'b\mathbf{l})\theta = \mathbf{r}\mathbf{l}b'\mathbf{r}a\mathbf{l}' = \mathbf{r}'bea\mathbf{l}' = \mathbf{r}'e'\mathbf{l}' = \mathrm{id}_{S'},$$

і θ оборотним справа, оскільки маємо

$$\theta(\mathbf{r}'a'\mathbf{l}) = \mathbf{r}b'\mathbf{l}'\mathbf{r}'a'\mathbf{l} = \mathbf{r}b'e'a'\mathbf{l}' = \mathbf{r}e\mathbf{l} = \mathrm{id}_S\,.$$

Таким чином, відображення θ є оборотним, а отже є бієкцією, і $\theta^t = \mathbf{r}'a\mathbf{l}' = \mathbf{r}'b\mathbf{l}$.

(*iv*) Для $m \in eMe$ маємо

$$\tau'\gamma(m) = (\mathbf{r}'b\mathbf{l})(\mathbf{r}m\mathbf{l})(\mathbf{r}a\mathbf{l}') = \mathbf{r}'bemea\mathbf{l}' = \mathbf{r}'(bma)\mathbf{l}' = \gamma'\tau(m),$$

що доводить комутативність діаграми.

(*iii*) Висловлення випливає з комутативності діаграми і з того факту, що відображення γ, τ і γ' є ізоморфізмами. □

Приклад 9.1.10. Розглянемо матриці

$$u = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \text{і} \quad v = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Вони породжують однозначний моноїд відношень (це можна перевірити використанням, наприклад, метод твердження 4.2.5). Матриця

$$uv = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

є матрицею m з прикладу 9.1.8. Елемент

$$e = (uv)^2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

є ідемпотентом. Маємо $\mathrm{Fix}(e) = \{1, 2\}$, і стовпчико-рядковим розкладом є

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \mathbf{lr}.$$

Матриця

$$e' = (vu)^2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

є також ідемпотентом. Маємо $\mathrm{Fix}(e') = \{3, 4\}$, і стовпчико-рядковим розкладом є

$$e' = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \mathbf{l}'\mathbf{r}'.$$

Ідемпотенти e і e' лежить в одному $\mathscr{D}$-класі. Справді, можемо взяти в якості системи переходу з e до e' елементи

$$a = b' = u \qquad \text{і} \qquad a' = b = vuv.$$

Бієкція $\theta = \mathbf{r}a\mathbf{l}'$ з множини $\mathrm{Fix}(e) = \{1, 2\}$ на множину $\mathrm{Fix}(e') = \{3, 4\}$ визначається за формулою

$$\theta\colon 1 \mapsto 4,\ 2 \mapsto 3.$$

9.2 Зображення Щютценбергера

Тепер опишемо корисний метод для обчислення групи підстановок G_e для ідемпотента e в однозначному моноїді відношень. Цей метод вимагає від нас зробити вибір між "лівим" і "правим". Ми спочатку представляємо правобічний випадок.

Нехай M — однозначний моноїд відношень і e — довільний ідемпотент моноїда M. Нехай R — $\mathscr{R}$-клас елемента e, Λ — множина $\mathscr{H}$-класів класу R і $G = H(e)$ — $\mathscr{H}$-клас ідемпотента e. Для кожного $H \in \Lambda$ виберемо два елементи a_H, $a'_H \in M$ такі, що

$$ea_H \in H, \qquad ea_H a'_H = e,$$

з умовою, що

$$a_G = a'_G = e$$

(див. рис. 9.2). Така множина пар $(a_H, a'_H)_{H\in\Lambda}$ називається *системою координат* кла-

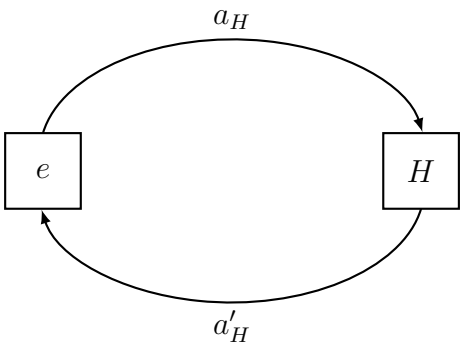


Рис. 9.2: Дві координати. Пара (a_H, a'_H) задовольняє умови $ea_H \in H$ і $ea_H a'_H = e$

су R стосовно ідемпотента e. За твердженням 1.12.2 маємо, що $Ga_H = H$ і $Ha'_H = G$, оскільки елементи a_H, a'_H реалізуються правим множенням двома оборотними бієкціями з G на H.

Нехай $e = \mathbf{lr}$ — стовпчико-рядковий розклад ідемпотента e та приймемо

$$\mathbf{r}_H = \mathbf{r}a_H \qquad \text{і} \qquad \mathbf{l}_H = a'_H\mathbf{l} \qquad \text{для} \qquad H \in \Lambda. \tag{9.11}$$

Зауважимо, що рівність $r_H = \mathbf{r}ea_H$ випливає з рівності $\mathbf{r} = \mathbf{r}e$, яка є рівністю (9.4).

Кожен елемент $m \in M$ визначає часткову праву дію на множині Λ, яка визначається

$$H \cdot m = \begin{cases} Hm, & \text{якщо } Hm \in \Lambda; \\ \varnothing, & \text{в іншому випадку,} \end{cases} \tag{9.12}$$

для всіх $H \in \Lambda$. Тепер визначимо часткове відображення з $\Lambda \times M$ в G прийнявши

$$H * m = \begin{cases} \mathbf{r}_H m \mathbf{l}_{H_m} & \text{якщо } Hm \in \Lambda; \\ \varnothing, & \text{в іншому випадку.} \end{cases} \tag{9.13}$$

Спочатку зауважимо, що з умови $H\cdot m \neq \varnothing$ випливає $H*m \in G_e$. Справді, покладемо $H' = Hm$. З умови $ea_H \in H$ отримуємо $ea_H m \in H'$, а це доводить, що

$$ea_H m a_{H'} \in G.$$

Звідси випливає, що

$$\begin{aligned} H * m &= \mathbf{r}_H m \mathbf{l}_{H'} = \\ &= (\mathbf{r} e a_H) m \, (a'_{H'} \mathbf{l}) = \\ &= \mathbf{r} \, (e a_H m a'_{H'}) \, \mathbf{l} \in G_e. \end{aligned}$$

Зауважимо також, що

$$H \cdot 1 = H \qquad \text{і} \qquad H * 1 = e, \tag{9.14}$$

для всіх $H \in \Lambda$. Далі,

$$(H * m)(H \cdot m * n) = H * mn. \tag{9.15}$$

для всіх $m, n \in M$. Остання формула показує, що відображення $(H, m) \mapsto H \cdot m$ і $(H, m) \mapsto H * m$ є аналогічні тим, які пов'язані з детермінованим перетворювачем, як визначено в розділі 4.

Для перевірки формули (9.15) припустимо, що $H' = Hm$ і $H'' = Hmn$, оскільки випадки $H \cdot m = \varnothing$ або $H \cdot mn = \varnothing$ є простими (див. рис. 9.3). Використавши (9.4),

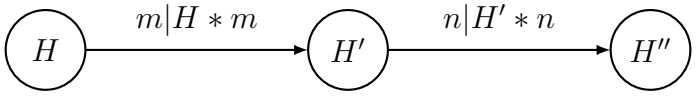


Рис. 9.3: Композиція виходів. Міткою ребра із стану H в стан $H' = H \cdot m$ є пара $(m, H * m)$, і вона позначається через $m|H * m$

маємо

$$\begin{aligned} (H * m)(H' * n) &= \mathbf{r}_H m \mathbf{l}_{H'} \mathbf{r}_{H'} n \mathbf{l}_{H''} = \\ &= \mathbf{r}_H m a'_{H'} \mathbf{l} \mathbf{r} a_{H'} n \mathbf{l}_{H''} = \\ &= \mathbf{r} a_H m a'_{H'} e a_{H'} n a'_{H''} \mathbf{l} = \\ &= \mathbf{r} \, ((e a_H m a'_{H'}) \, e) \, a_{H'} n a'_{H''} \mathbf{l}. \end{aligned}$$

Оскільки $e a_H m a'_{H'} \in G$, то маємо $e a_H m a'_{H'} e = e a_H m a'_{H'}$. Отже,

$$(H * m)(H' * n) = \mathbf{r} \, ((e a_H m) \, a'_{H'} a_{H'}) \, n a'_{H''} \mathbf{l}.$$

Оскільки $e a_H m \in H'$ і множення справа на $a'_{H'} a_{H'}$ є тотожним відображенням на H', то отримуємо

$$(H * m)(H' * n) = \mathbf{r} e a_H m n a'_{H''} \mathbf{l} = \mathbf{r}_H m n \mathbf{l}_{H''} = H * mn.$$

Це доводить формулу (9.15). Як наслідок, маємо такий результат.

Твердження 9.2.1. *Нехай M — однозначний моноїд відношень, породжений множиною T. Нехай e — ідемпотент моноїда M, R — його $\mathcal{R}$-клас, λ — множина $\mathcal{H}$-класів класу R і нехай $(a_H, a'_H)_{H \in \Lambda}$ — система координат класу R стосовно до ідемпотента e. Тоді група підстановок G_e породжується елементами вигляду $H * t$, для $H \in \Lambda$, $t \in T$ і $H * t \neq \varnothing$.*

Доведення. Елементи $H * t$ для $H \in \Lambda$ і $t \in T$ є, або $\varnothing$, або містяться в G_e. Тепер, нехай g — елемент групи $H(e)$. Тоді існують $t_1, t_2, \ldots, t_n \in T$ такі, що

$$g = t_1 t_2 \cdots t_n,$$

оскільки T породжує моноїд M. Нехай $G = H(e)$ і

$$H_i = G t_1 t_2 \cdots t_i$$

для $1 \leqslant i \leqslant n$. З рівності $Gg = G$ випливає, що $H_i t_{i+1} \cdots t_n = G$. Отже, $H_i \in \Lambda$ і $G \cdot t_1 \cdots t_i = H_i$. За рівністю (9.15) отримуємо

$$G * g = (G * t_1)(H_1 * t_2) \cdots (H_{n-1} * t_n).$$

Але $G * g = \mathbf{r}g\mathbf{l}$. Це доводить наше твердження. □

Пара часткових відображень з $\Lambda \times M$ в Λ і в G_e визначених формулами (9.12) і (9.13) називається *правим зображенням Шютценбергера* або *$\mathscr{R}$-зображенням* моноїда M стосовно ідемпотента e та координатної системи $(a_H, a'_H)_{H \in \Lambda}$.

Нехай 0 — новий елемент такий, що $0g = g0 = 00 = 0$ для всіх $g \in G_e$. Відображення

$$\mu \colon M \to (G_e \cup \{0\})^{\Lambda \times \Lambda},$$

яке ставить у відповідність кожному елементові $m \in M$ $\Lambda \times \Lambda$-матрицю, визначену за формулою

$$(\mu m)_{H,H'} = \begin{cases} H * m, & \text{якщо } Hm = H'; \\ \varnothing, & \text{в іншому випадку,} \end{cases}$$

є морфізмом з моноїда M у моноїд $\Lambda \times \Lambda$-матриць таких, що кожен рядок містить не більше одного ненульового елемента з $G_e \cup \{0\}$ (надалі такі матриці ми будемо називати *рядково-мономіальними* $\Lambda \times \Lambda$-*матрицями* над $G_e \cup \{0\}$). Це ж насправді еквівалентне формулювання формули (9.15).

Симетрично означимо *ліве зображення Шютценбергера* або *$\mathscr{L}$-зображення* моноїда M стосовно ідемпотента e наступним чином. Нехай L — $\mathscr{L}$-клас ідемпотента $e \in M$ і Γ — множина $\mathscr{H}$-класів, які містяться в L. Для кожного $H \in \Gamma$ виберемо два елемента $b_H, b'_H \in M$ такі, що

$$b_H e \in H \qquad \text{і} \qquad b'_H b_H e = e,$$

з $b_G = b'_G = e$. Така множина пар $(b_H, b'_H)_{H \in \Gamma}$ називається *системою координат* класу L стосовно ідемпотента e. к і в умові (9.11), покладемо

$$\mathbf{l}_H = b_H c \qquad \text{і} \qquad \mathbf{r}^H = \mathbf{r} b'_H \qquad \text{для} \qquad H \in \Gamma.$$

Для кожного елемента $m \in M$ означимо часткову ліву дію на Γ, поклавши

$$m \cdot H = \begin{cases} mH, & \text{якщо } mH \in \Gamma; \\ \varnothing, & \text{в іншому випадку,} \end{cases} \tag{9.16}$$

для $H \in \Gamma$, і часткове відображення з $M \times \Gamma$ в G_e, поклавши

$$m * H = \begin{cases} \mathbf{r}^{mH} m \mathbf{l}^H, & \text{якщо } mH \in \Gamma; \\ \varnothing, & \text{в іншому випадку.} \end{cases} \tag{9.17}$$

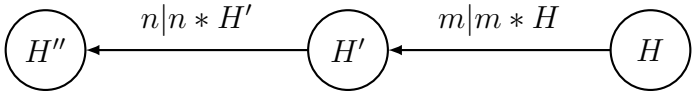


Рис. 9.4: Композиція виходів. Міткою ребра із стану H в стан $H' = m \cdot H$ є пара $(m, m*H)$, і вона позначається через $m|m*H$. Зауважте, що вхід зчитується справа наліво і, що вихід записується справа наліво

Тоді аналогом формули (9.15) стає

$$(n * m \cdot H)(m * H) = nm * H, \tag{9.18}$$

і твердження 9.2.1 виконується з урахуванням відповідних змін (див. рис. 9.4).

Зауважимо, що для обчислення $\mathscr{L}$-класів і $\mathscr{R}$-класів однозначного моноїда відношень ми можемо використати таке спостереження, перевірка якого простою та безпосередньою: якщо $m\mathscr{L}n$ (відп., якщо $m\mathscr{R}n$), то кожен рядок (відп., стовпець) матриці m — це сума рядків (відп., стовпців) матриці n і навпаки. Це дає простий тест для визначення, що два елементи містяться в різних $\mathscr{L}$-класах (відп., $\mathscr{R}$-класах).

Приклад 9.2.2. Розглянемо знову однозначний моноїд з прикладу 9.1.10, породжений матрицями

$$u = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \text{і} \quad v = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Розглянемо ідемпотент

$$e = (uv)^2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

$\mathscr{R}$-клас R ідемпотента e складається з трьох $\mathscr{H}$-класів, які занумеруємо $0, 1, 2$. На рис. 9.5 викладено зображення для кожного з цих $\mathscr{H}$-класів. Те, що $\mathscr{L}$-класи є різними, перевіряється шляхом огляду рядків e, eu і eu^2. Далі, зауважимо, що

$$eu^3 = eu^2v = e,$$

а це доводить, що ці елементи є $\mathscr{R}$-еквівалентними. Далі,

$$euv = (uv)^3 \mathscr{H} e.$$

На завершенні, елемент

$$ev = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

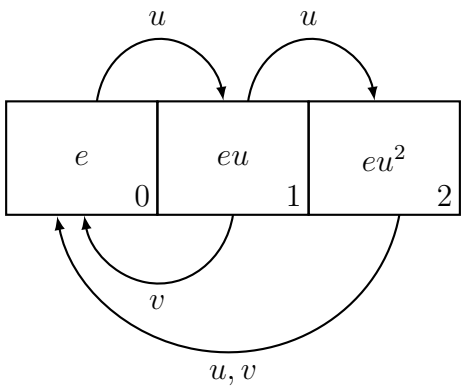


Рис. 9.5: $\mathscr{R}$-клас ідемпотента e

має лише один ненульовий рядок (стовпчик), а отже не може бути елементом $\mathscr{D}$-класу ідемпотента e. На рис. 9.5 показано про вплив правого множення на елементи u і v.

Виберемо систему координат класу R, поклавши

$$\begin{aligned} a_0 &= a'_0 = e, \\ a_1 &= u, \quad a'_1 = vuv, \\ a_2 &= u^2, \quad a'_2 = u. \end{aligned}$$

Тоді

$$\mathbf{r}_0 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \qquad \mathbf{l}_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 1 \end{bmatrix},$$

$$\mathbf{r}_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}, \qquad \mathbf{l}_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$\mathbf{r}_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad \mathbf{l}_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Позначимо через $H \xrightarrow{t|g} H'$ той факт, що виконуються рівності $H \cdot t = H'$ і $H * t = g$. Тоді $\mathscr{R}$-зображення моноїда M стосовно ідемпотента e і до цієї системи координат отримано, поповненням рис. 9.5 і подано на рис. 9.6 з

$$i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \text{і} \qquad j = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Група G_e, очевидно, ізоморфна групі підстановок $\mathfrak{S}_2$.

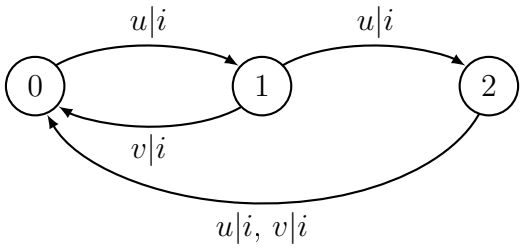


Рис. 9.6: $\mathscr{R}$-зображення моноїда M стосовно ідемпотента e

Поняття, введені в цьому пункті, значно спрощуються, коли ми розглядаємо випадок моноїда (повного) відображення з Q в себе замість однозначного моноїда відношень.

Для $a \in M$ записуватимемо $pa = q$ замість $(p, a, q) = 1$.

Образом часткового відображення a, позначатимемо через $\mathrm{Im}(a)$, називається підмножина в $q \in Q$ така, що $pa = q$ для деякого $p \in Q$. *Ядерною еквіваленцією* часткового відображення a, позначатимемо через $\mathrm{Ker}(a)$, називається відношення еквівалентності на Q, визначене так:

$$p \equiv q \mod \mathrm{Ker}(a) \qquad \text{тоді і тільки тоді, коли} \qquad pa = qa.$$

Якщо $b \in Ma$, то $\mathrm{Im}(b) \subset \mathrm{Im}(a)$. Якщо $b \in aM$, то $\mathrm{Ker}(a) \subset \mathrm{Ker}(b)$.

Відображення $e \in M$ є ідемпотентним тоді і тільки тоді, коли його звуження на його образ є тотожним відображенням. Отже, образ відображення в цьому випадку дорівнює його множині нерухомих точок: $\mathrm{Im}(e) = \mathrm{Fix}(e)$.

Як результат попередніх результатів отримуємо: якщо $a\mathscr{L}b$, то $\mathrm{Im}(a) = \mathrm{Im}(b)$, і якщо $a\mathscr{R}b$, то $\mathrm{Ker}(a) = \mathrm{Ker}(b)$. Це дає достатню умову для того, щоб два елементи містилися в різних $\mathscr{L}$-класах (відп., $\mathscr{R}$-класах).

Для обчислення $\mathscr{R}$-класу ідемпотентного відображення e над скінченною множиною, ми можемо використати наступне спостереження, де $S = \mathrm{Fix}(e)$. Якщо звуження відображення m на S є підстановкою на S, то $e\mathscr{H}em$. Справді, звуження відображення m на S є підстановкою на S, а отже $em^p = e$ для деякого натурального числа p. Звідки випливає рівність $emm^{p-1} = e$, а отже $em\mathscr{H}e$.

Приклад 9.2.3. Нехай M — моноїд відображень з множини

$$Q = \{1, 2, \ldots, 8\}$$

в себе, породжений двома відображеннями u і v, які визначені в таблиці:

	1	2	3	4	5	6	7	8
u	4	5	4	5	8	1	8	1
v	2	3	4	5	6	7	8	1

де кожен стовпець містить образи u і v елемента множини Q, розміщеного у верхній частині стовпця. Відображення $e = u^4$ є ідемпотентним і має

$$S = \{1, 4, 5, 8\}$$

в якості множини нерухомих точок,

	1	2	3	4	5	6	7	8
u^4	1	4	1	4	5	8	5	8

Отримуємо шаблон, зображений на рис. 9.7 для $\mathscr{R}$-класу R ідемпотента e. Ці чотири

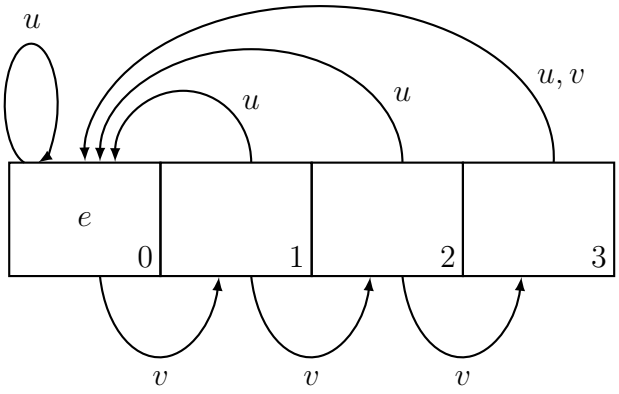


Рис. 9.7: $\mathscr{R}$-клас ідемпотента e

$\mathscr{H}$-класи є різними, оскільки образи елементів

$$e, ev, ev^2, ev^3$$

є різними. Для ребер, що повертаються до $\mathscr{H}$-класу елемента e, ми використовуємо спостереження, зазначене вище; достатньо перевірити, що звуження на множину S відображень

$$u, vu, v^2u, v^3u, v$$

є підстановками. Виберемо систему координат класу R, взявши

$$\begin{aligned} a_0 &= a'_0 = e, \\ a_1 &= v, \quad & a'_1 &= v^7, \\ a_2 &= v^2, \quad & a'_2 &= v^6, \\ a_3 &= v^3, \quad & a'_3 &= v^5. \end{aligned}$$

Для обчислення $\mathscr{R}$-зображення моноїда M стосовно ідемпотента e ми поступаємо наступним чином: якщо $H \cdot m = H'$, то підстановка $H * m$ на S не обчислюється обчисленням матричного добутку $H * m = \mathbf{r}_H m \mathbf{l}_{H'}$ формули (9.13), але, зауважуючи, що $H * m$ є звуженням на S відношення $ea_H ma'_{\cdot}$, оцінюючи цю функцію на S. Таким

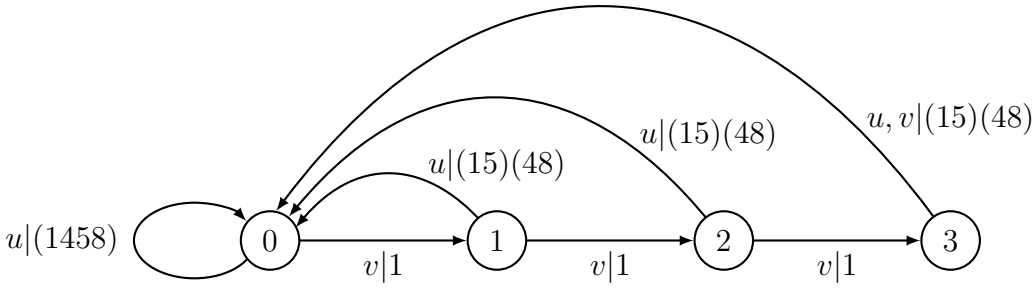


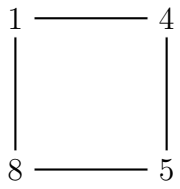
Рис. 9.8: $\mathscr{R}$-зображення

чином, ми уникаємо зайвих матричних обчислень при роботі з відображеннями. На рис. 9.8 представлено таке $\mathscr{R}$-зображення.

За твердженням 9.2.1 група G_e породжена підстановками

$$(1458), \qquad (15)(48) \qquad \text{і} \qquad (14)(58).$$

Група G_e ізоморфна *діедральній групі* D_4, є групою всіх симетрій квадрата.



Ця група містить вісім елементів.

9.3 Ранг і мінімальний ідеал

Нехай m — відношення між множинами P і Q. *Рангом відношення* m називається найменша потужність множин R таких, що існують два відношення $\mathbf{l} \in \mathfrak{P}(P \times R)$ і $\mathbf{r} \in \mathfrak{P}(R \times Q)$ з властивістю

$$m = \mathbf{lr} \tag{9.19}$$

і такі, що добуток $\mathbf{lr}$ є однозначним. Ранг відношення m позначається через $\operatorname{rank}(m)$. Ранг відношення m є невід'ємним цілим числом, або набуває значення $+\infty$. Пара $(\mathbf{l}, \mathbf{r})$, яка задовольняє умову (9.19) називається *мінімальним розкладом*, якщо не існує однозначної факторизації $m = \mathbf{l}'\mathbf{r}'$ такої, що $\mathbf{l}' \in \mathfrak{P}(P \times R')$, $\mathbf{r}' \in \mathfrak{P}(R' \times Q)$ і $R' \subsetneq R$. Якщо величина $\operatorname{rank}(m)$ є скінченною, то це еквівалентно висловленню, що величина $\operatorname{Card}(R)$ є мінімальною.

Приклад 9.3.1. Відношення

$$m = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

має ранг щонайбільше 2 з огляду на вище викладений розклад. Ранг відношення m не дорівнює 1, оскільки воно має різні ненульові стовпці. Таким чином, $\operatorname{rank}(m) = 2$.

Наступні властивості часто використовуються. По-перше, якщо добуток nmn' є однозначним, то

$$\operatorname{rank}(nmn') \leqslant \operatorname{rank}(m). \tag{9.20}$$

Справді, кожен розклад $(\mathbf{l}, \mathbf{r})$ відношення m індукує розклад $(n\mathbf{l}, \mathbf{r}n')$ відношення nmn'. Якщо

$$p \xrightarrow{n} s \xrightarrow{\mathbf{l}} t \xrightarrow{\mathbf{r}} u \xrightarrow{n} q \qquad \text{і} \qquad p \xrightarrow{n} s' \xrightarrow{\mathbf{l}} t' \xrightarrow{\mathbf{r}} u' \xrightarrow{n} q,$$

то $s = s'$ і $u = u'$ за однозначністю добутку nmn'. З однозначності добутку $\mathbf{lr}$ випливає $t = t'$. По-друге

$$\operatorname{rank}(m) \leqslant \min\{\operatorname{Card}(P), \operatorname{Card}(Q)\}.$$

Якщо $(\mathbf{l}, \mathbf{r})$ є мінімальним розкладом відношення m, то

$$\operatorname{rank}(m) = \operatorname{rank}(\mathbf{l}) = \operatorname{rank}(\mathbf{r}).$$

Далі

$$\operatorname{rank}(m) = 0 \qquad \Longleftrightarrow \qquad m = 0.$$

Якщо $P' \subset P$, $Q' \subset Q$ і якщо m' є звуженням відношення m на $P' \times Q'$, то

$$\operatorname{rank}(m') \leqslant \operatorname{rank}(m). \tag{9.21}$$

Ми отримуємо з першої нерівності, що два $\mathscr{J}$-еквівалентні елементи однозначного моноїда відношень мають однаковий ранг. Таким чином, ранг є сталою величиною на $\mathscr{D}$-класі.

Розглянемо два відношення $m \in \mathfrak{P}(P \times S)$ і $n \in \mathfrak{P}(S \times Q)$. Пара відношень (m, n) називається *обрізаною*, якщо відношення m не містить нульових стовпчиків і відношення n не містить нульових рядків. Це означення еквівалентне тому, що для всіх $s \in S$ існує хоча б одна пара $(p, q) \in P \times Q$ таке, що

$$p \xrightarrow{m} s \qquad \text{і} \qquad s \xrightarrow{n} q.$$

Твердження 9.3.2. *Кожен мінімальний розклад відношення є обрізаним.*

Доведення. Нехай $\mathbf{lr}$ — мінімальний розклад відношення m. Припустимо, що $\mathbf{l}$ містить стовпчик, який є нульовим. Тоді ми можемо видалити цей стовпчик і рядок того ж індексу r без зміни значення добутку. Але звідси випливає, що пара відношень $(\mathbf{l}, \mathbf{r})$ не є мінімальним розкладом. Таким чином, жодна колонка відношення $\mathbf{l}$ не є нульовою, і симетрично жоден рядок відношення $\mathbf{r}$ не є нульовим. Звідси випливає, що пара відношень $(\mathbf{l}, \mathbf{r})$ є обрізаною. □

Твердження 9.3.3. *Для довільної множини Q виконується рівність*

$$\operatorname{rank}(\mathrm{id}_Q) = \operatorname{Card}(Q).$$

Доведення. Нехай $\mathrm{id} = \mathbf{lr}$ — мінімальний розклад відношення тотожності id_Q такий, що $\mathbf{l} \in \mathfrak{P}(Q \times P)$ і $\mathbf{r} \in \mathfrak{P}(P \times Q)$. Нехай $p \in P$. Оскільки пара $(\mathbf{l}, \mathbf{r})$ є обрізаною, то існують $q, q' \in Q$ такі, що

$$q \xrightarrow{\mathbf{l}} p \xrightarrow{\mathbf{r}} q'.$$

Оскільки $\mathbf{lr} = \mathrm{id}_Q$, то маємо $q = q'$ і не існує елемента $q'' \neq q$ такого, що

$$p \xrightarrow{\mathbf{r}} q''.$$

Отже, відношення $\mathbf{r}$ визначає відображення з множини P в Q. Це відображення є сюр'єктивним, оскільки відношення id_Q є сюр'єктивним. Звідси випливає рівність $\operatorname{Card}(P) = \operatorname{Card}(Q)$. □

Твердження 9.3.4. *Підстановка на множині Q має ранг* $\operatorname{Card}(Q)$.

Доведення. Нехай m — підстановка на множині Q і n — обернена до неї підстановка. Тоді за твердженням 9.3.3 і рівністю (9.20) маємо

$$\operatorname{Card}(Q) = \operatorname{rank}(\mathrm{id}_Q) = \operatorname{rank}(mn) \leqslant \operatorname{rank}(m).$$

Отже, $\operatorname{rank}(m) = \operatorname{Card}(Q)$. □

Приклад 9.3.5. Ранг часткового відображення m з множини P в множину Q дорівнює

$$\operatorname{rank}(m) = \operatorname{Card}(\operatorname{Im}(m)).$$

Нехай m' — звуження відношення m на $P \times \operatorname{Im}(m)$. Тоді $m = m'\mathbf{r}$, де r — звуження відношення тотожності id_Q на множину $\operatorname{Im}(m)$. Звідси випливає нерівність

$$\operatorname{rank}(m) \leqslant \operatorname{Card}(\operatorname{Im}(m)).$$

Часткове відображення m' містить бієкцію n перерізу відношення m на $\operatorname{Im}(m)$, отриману шляхом вибору одного елемента в множині P для кожної множини $m^{-1}(q)$, з $q \in \operatorname{Im}(m)$. За твердженням 9.3.4 і рівністю (9.21) отримуємо

$$\operatorname{rank}(m) \geqslant \operatorname{rank}(n) = \operatorname{Card}(\operatorname{Im}(m)).$$

Отже, поняття рангу, яке було введено в підрозділі 3.5 збігається з одноіменним поняттям, означеним у цьому підрозділі.

Зауважимо, що ранг відношення m над скінченною множиною Q має сильні зв'язки зі звичайним поняттям рангу матриці, яке означене в лінійній алгебрі. Нехай K — полем, яке містить множину натуральних чисел $\mathbb{N}$. *Рангом* матриці m з коефіцієнтами в полі K, який позначається через $\operatorname{rank}_K(m)$, називається максимальна кількість рядків (або стовпчиків), які є лінійно незалежними над K. Можемо зауважити (вправа 9.7.8), що це число можна означити методом, аналогічним до означення рангу відношення. Зокрема,

$$\operatorname{rank}_K(m) \leqslant \operatorname{rank}(m).$$

Легко бачити (вправа 9.7.9), що в загальному випадку ця нерівність строгою. Проте, у випадку відношень, які є відображеннями, ці два поняття збігаються.

Наступне твердження дає простий метод для обчислення рангу ідемпотентного відношення.

Твердження 9.3.6. *Нехай e — ідемпотент однозначного моноїда відношень на множині Q. Тоді*

$$\operatorname{rank}(e) = \operatorname{Card}(\operatorname{Fix}(e)).$$

Доведення. Позначимо $S = \operatorname{Fix}(e)$. Стовпчиково-рядковий розклад відношення e доводить, що

$$\operatorname{rank}(e) \leqslant \operatorname{Card}(S).$$

Більше того, з огляду на твердження 9.1.6 матриця e містить одиничну матрицю I_S. Таким чином,

$$\operatorname{Card}(S) = \operatorname{rank}(I_S) \leqslant \operatorname{rank}(e)$$

за рівністю (9.21). □

Наступне твердження дає описання відношень скінченного рангу.

Твердження 9.3.7. *Для будь-якого відношення m наступні умови є еквівалентними:*

(*i*) *m має скінченний ранг;*
(*ii*) *множина рядків матриці m скінченна;*
(*iii*) *множина стовпців матриці m скінченна.*

Доведення. (*i*) $\Longrightarrow$ (*ii*) Нехай $m = \mathbf{lr}$ з $\mathbf{l} \in \mathfrak{P}(P \times S)$ і $\mathbf{r} \in \mathfrak{P}(S \times Q)$ — мінімальний розклад відношення m. Якщо два рядки відношення $\mathbf{l}$, скажемо з індексами p і q, є рівними, то відповідні рядки m_{p*} і m_{q*} відношення m також є рівними. Оскільки множина S є скінченною, то матриця $\mathbf{l}$ має щонайбільше $2^{\operatorname{Card}(S)}$ різних рядків. Отже, множина рядків відношення m є скінченною.

(*ii*) $\Longrightarrow$ (*i*) Нехай $(m_{s*})_{r \in S}$ — множина зображень рядків відношення m. Тоді $m = \mathbf{lr}$, де $\mathbf{r}$ — звуження відношення m на $S \times Q$, і $\mathbf{l} \in \mathfrak{P}(Q \times S)$ визначається за формулою

$$\mathbf{l}_{qr} = \begin{cases} 1, & \text{якщо } m_{q*} = m_{s*}; \\ 0, & \text{в інших випадках.} \end{cases}$$

Це доводить еквіваленцію (*i*) $\Longleftrightarrow$ (*ii*).

Доведення еквіваленції (*i*) $\Longleftrightarrow$ (*iii*) є аналогічним. □

Твердження 9.3.8. *Нехай m — відношення на множині Q скінченного рангу. Тоді напівгрупа породжена відношенням m є скінченною.*

Доведення. Нехай $m = \mathbf{lr}$ — мінімальний розклад відношення m такий, що

$$\mathbf{l} \in \mathfrak{P}(Q \times R) \qquad \text{і} \qquad \mathbf{r} \in \mathfrak{P}(R \times Q).$$

Нехай u — відношення над множиною R, означене $u = \mathbf{rl}$. Тоді для всіх натуральних n маємо

$$m^{n+1} = \mathbf{l}(\mathbf{rl})^n\mathbf{r} = \mathbf{l}u^n\mathbf{r}.$$

Оскільки множина R — скінченна, то множина відношень u^n є скінченною, а отже напівгрупа $\{m^n \colon n \geqslant 1\}$ є скінченною. □

Зокрема, з цього твердження випливає, що для будь-якого відношення скінченного рангу зручний степінь є ідемпотентним відношенням.

Нехай M — однозначний моноїд відношень над множиною Q. *Мінімальним рангом* моноїда M, позначається через $r(M)$, називається найменший з рангів елементів з M відмінних від нуль-відношення,

$$r(M) = \min\{\operatorname{rank}(m) \colon m \in M \setminus \{0\}\}.$$

Якщо M не містить нуль-відношення над множиною Q, то це є звичайно найменшим з рангів елементів моноїда M. Маємо $r(M) > 0$ якщо $Q \neq \varnothing$ і $r(M) < \infty$ тоді і лише тоді, коли моноїд M містить відношення скінченного додатнього рангу.

Тепер ми вивчаємо моноїди, що мають скінченний мінімальний ранг, і побачимо, що вони мають регулярну структуру. Ми маємо розрізняти два випадки: випадок, коли моноїд містить нульове відношення, і простіший випадок, коли цього немає.

Зауважимо, що нульове відношення відіграє роль нуля з огляду на наступне, більш точне твердження.

Твердження 9.3.9. *Якщо транзитивний однозначний моноїд відношень над непорожньою множиною Q містить нуль, то нуль є нульовим відношенням.*

Доведення. Нульове відношення завжди є нулем. Навпаки, якщо моноїд M містить нуль z, то ми доведемо, що z є нульовим відношенням. Якщо $\operatorname{Card}(Q) = 1$, то $z = 0$. Отже припускатимемо, що $\operatorname{Card}(Q) \geqslant 2$ і $z \neq 0$. Нехай $p, q \in Q$ такі, що $z_{p,q} = 1$. Нехай $r, s \in Q$. З транзитивності моноїда M випливає, що існують $m, n \in M$ такі, що

$$m_{rp} = n_{qs} = 1.$$

З рівності $mzn = z$ випливає, що $z_{rs} = 1$. Отже $z_{rs} = 1$ для всіх $r, s \in Q$, що суперечить однозначності моноїда M. □

Нехай M — однозначний моноїд відношень над непорожньою множиною Q. Для кожного елемента $q \in Q$ *стабілізатором* елемента q називається підмоноїд

$$\operatorname{Stab}(q) = \left\{m \in M \colon q \xrightarrow{m} q\right\}$$

моноїда M.

Теорема 9.3.10. *Нехай M — транзитивний однозначний моноїд відношень над непорожньою множиною Q, який містить порожнє відношення 0 і має скінченний мінімальний ранг. Нехай K — множина елементів моноїда M мінімального рангу $r(M)$. Тоді:*

(*i*) *моноїд M містить єдиний 0-мінімальний ідеал J, який збігається з $K \cup \{0\}$;*
(*ii*) *множина K є регулярним $\mathscr{D}$-класом, чиї $\mathscr{H}$-класи є скінченними;*
(*iii*) *кожен елемент $q \in Q$ є нерухомою точкою щонайменше одного ідемпотента e в K, тобто $e \in K \cap \mathrm{Stab}(q)$;*
(*iv*) *для кожного ідемпотента $e \in K$ група G_e є транзитивною групою степеня $r(M)$;*
(*v*) *групи G_e, для ідемпотентів $e \in K$, є еквівалентними.*

Перш ніж приступити до доведення, ми встановимо декілька необхідних результатів.

Твердження 9.3.11. *Нехай M — однозначний моноїд відношень над непорожньою множиною Q і $e \in M$ — ідемпотент. Якщо e має скінченний ранг, то локалізований моноїд eMe є скінченним.*

Доведення. Нехай S — множина нерухомих точок відношення e. За твердженням 9.3.6 множина S є скінченною. Отже моноїд M_e, який є однозначним моноїдом відношень над множиною S, є скінченним. Оскільки за твердженням 9.1.9 моноїд eMe ізоморфний моноїдові M_e, то він є скінченним. □

Тепер ми перевіримо технічну лему, корисну для "уникнення" нульового відношення.

Лема 9.3.12. *Нехай M — транзитивний однозначний моноїд відношень над непорожньою множиною Q.*

1. *Для кожного $m \in M \setminus \{0\}$ існують $n \in M$ і $q \in Q$ такі, що $mn \in \mathrm{Stab}(q)$ (відп., $nm \in \mathrm{Stab}(q)$). Отже, зокрема $mn \neq 0$ (відп., $nm \neq 0$).*
2. *Для всіх $m \in M \setminus \{0\}$ і $q \in Q$ існують $n, n' \in M$ такі, що $mnn' \in \mathrm{Stab}(q)$.*
3. *Для всіх $m, n \in M \setminus \{0\}$ існує елемент $u \in M$ такий, що $mun \neq 0$. Іншими словами, моноїд M є первинним.*

Доведення. 1. Нехай $q, r \in Q$ — такі елементи, що $(q, m, r) = 1$. Оскільки моноїд M є транзитивним, то існує елемент $n \in M$ такий, що $(r, n, q) = 1$. Отже, $(q, mn, q) = 1$.

2. Існують елементи $p, r \in Q$ такі, що $(p, m, r) = 1$. Нехай $n, n' \in M$ — такі елементи, що $(q, n, p) = 1$ і $(r, n', q) = 1$. Тоді $(q, nmn', q) = 1$.

3. Існують елементи $p, r, s, q \in Q$ такі, що

$$(p, m, r) = (s, n, q) = 1.$$

Візьмемо елемент $u \in M$ такий, що $(r, u, s) = 1$. Тоді $(p, mun, q) = 1$. □

Твердження 9.3.13. *Нехай M — транзитивний однозначний моноїд відношень над непорожньою множиною Q, який має скінченний мінімальний ранг. Тоді кожен правий ідеал $R \neq 0$ (відп., кожен лівий ідеал $L \neq 0$) моноїда M містить ненульовий ідемпотент.*

Доведення. Нехай $r \in R \setminus \{0\}$. За лемою 9.3.12 існують елементи $n \in M$ і $q \in Q$ такі, що $rn \in \mathrm{Stab}(q)$. Нехай $m \in M$ — такий елемент, що $\mathrm{rank}(m) = r(M)$. Знову, за лемою 9.3.12 існують елементи $u, v \in M$ такі, що $umv \in \mathrm{Stab}(q)$. Розглянемо елемент $m' = rnumv$. Тоді $m' \in R$ і $m' \in \mathrm{Stab}(q)$.

Оскільки $\mathrm{rank}(m') \leqslant \mathrm{rank}(m)$, то ранг елемента m' є скінченним. За твердженням 9.3.8 напівгрупа, породжена елементом m' є скінченною. Тоді існує натуральне число $k \geqslant 1$ таке, що елемент $e = (m')^k$ є ідемпотентом. Тоді $e \in R$ і $e \neq 0$, оскільки $e \in \mathrm{Stab}(q)$. □

Твердження 9.3.14. *Нехай M — транзитивний однозначний моноїд відношень над непорожньою множиною Q, який містить порожнє відношення 0 і має скінченний мінімальний ранг. Тоді для кожного елемента $m \in M$ наступні умови є еквівалентними:*

(*i*) $\mathrm{rank}(m) = r(M)$;
(*ii*) *правий ідеал mM є 0-мінімальним;*
(*iii*) *лівий ідеал Mm є 0-мінімальним.*

Доведення. (*i*) $\Longrightarrow$ (*ii*) Нехай $R \neq \{0\}$ — правий ідеал, який міститься в mM. Ми доведемо, що $R = mM$. За твердженням 9.3.13 ідеал R містить ідемпотент $e \neq 0$. Оскільки $e \in R \subset mM$, то існує елемент $n \in M$ такий, що $e = mn$. Оскільки $\mathrm{rank}(e) \leqslant \mathrm{rank}(m)$ і величина $\mathrm{rank}(m)$ є мінімальною, то маємо $\mathrm{rank}(e) \leqslant \mathrm{rank}(m)$. Нехай $m = \mathbf{lr}$ — мінімальний розклад відношення m з

$$\mathbf{l} \in \mathfrak{P}(Q \times S) \qquad \text{і} \qquad \mathbf{r} \in \mathfrak{P}(S \times Q).$$

Тоді

$$e = (\mathbf{lr})n = \mathbf{l}(\mathbf{r}n).$$

Добуток $\mathbf{l}(\mathbf{r}n)$, очевидно, можна вибрати так, щоб він був однозначним. Оскільки

$$\mathrm{rank}(e) = r(M) = \mathrm{Card}(S),$$

то пара $(\mathbf{l}, \mathbf{r}n)$ є мінімальним розкладом відношення e. Для всіх $k \geqslant 0$ маємо, що

$$e = e^{k+1} = \mathbf{l}(\mathbf{r}n\mathbf{l})^k\mathbf{r}n$$

з усіма однозначними добутками. Оскільки множина S є скінченною, то існує натуральне число $i \geqslant 1$ таке, що $(\mathbf{r}n\mathbf{l})^i$ є ідемпотентним елементом однозначного моноїда відношень на множині S, складених зі степенів добутку $\mathbf{r}n\mathbf{l}$. Оскільки

$$\mathrm{rank}((\mathbf{r}n\mathbf{l})^i) = \mathrm{Card}(S),$$

то кожен елемент в множині S нерухомою точкою відношення $(\mathbf{r}n\mathbf{l})^i$. Звідси випливає, що $(\mathbf{r}n\mathbf{l})^i = \mathrm{id}_S$. Отже,

$$em = e^i m = (\mathbf{r}n\mathbf{l})^i m = (\mathbf{r}n\mathbf{l})^i\mathbf{lr} = \mathbf{l}(\mathbf{r}n\mathbf{l})^i\mathbf{r} = \mathbf{lr} = m.$$

Рівність $em = m$ доводить, що $m \in R$, а отже $R = mM$. Отже mM є 0-мінімальним правим ідеалом.

$(ii) \Longrightarrow (i)$ Нехай $n \in M$ — такий елемент, що $\operatorname{rank}(n) = r(M)$. За лемою 9.3.12 існує елемент $u \in M$ такий, що $mun \neq 0$. З включення $munM \subset mM$ отримуємо рівність $munM = mM$, звідки випливає, що $m \in munM$. Отже, $\operatorname{rank}(m) \leqslant \operatorname{rank}(n)$, а це доводить рівність

$$\operatorname{rank}(m) = \operatorname{rank}(n).$$

Доведення еквіваленції $(i) \Longleftrightarrow (iii)$ є аналогічним. □

Доведення теореми 9.3.10. (i) За лемою 9.3.12 моноїд M є первинним. Згідно твердження 9.3.14 моноїд M містить 0-мінімальний лівий і 0-мінімальний правий ідеали. З огляду на наслідок 1.12.10 моноїд M містить єдиний 0-мінімальний ідеал J, який є об'єднанням 0-мінімальних правих ідеалів (відп., 0-мінімальних лівих ідеалів). Ще раз за твердженням 9.3.14 ідеал J є об'єднанням нуля 0 і множини K елементів мінімального додатнього рангу. Це завершує доведення висловлення (i).

(ii) З огляду на наслідок 1.12.10 множина K є регулярним $\mathscr{D}$-класом. Усі $\mathscr{H}$-класи множини K мають однакову потужність за твердженням 1.12.3. Скінченність цих $\mathscr{H}$-класів випливає з висловлення (iv).

(iii) Нехай $q \in Q$ і $k \in K$. З леми 9.3.12 випливає, що $nkn' \in \operatorname{Stab}(q)$ для деяких $n, n' \in M$. Оскільки за твердженням 9.3.8 напівгрупа, породжена елементом $m = nkn'$ є скінченною, то вона містить ідемпотент e. Тоді $e \in K \cap \operatorname{Stab}(q)$.

(iv) Нехай e — ідемпотент з множини K. Тоді $\mathscr{H}$-клас елемента e з приєднаним нулем є

$$H \cup \{0\} = eM \cap Me = eMe = H(e) \cup \{0\}.$$

Перша рівність є результатом того факту, що $\mathscr{R}$-клас ідемпотента e збігається з множиною $eM \setminus \{0\}$. Далі $eMe \subset eM \cap Me$, і навпаки, якщо $n \in eM \cap Me$, то $en = ne = n$, а отже $n = ene \in eMe$. Це доводить другу рівність. На завершенні, $H(e) = H$ оскільки множина H є групою.

За твердженням 9.1.7 маємо $M_e = G_e \cup \{0\}$ і моноїд M_e є транзитивним. Отже, G_e є транзитивною групою підстановок. Її степінь дорівнює $r(M)$.

Висловлення (v) є безпосереднім наслідком твердження 9.1.9. □

Тепер нехай M — однозначний моноїд відношень, який не містить порожнього (нульового) відношення. Теорема 9.3.10 допускає формулювання, яке є повністю аналогічним, і висловлюється так.

Теорема 9.3.15. *Нехай M — транзитивний однозначний моноїд відношень над множиною Q, який не містить нульового відношення і має скінченний мінімальний ранг. Нехай K — множина елементів мінімального рангу $r(M)$. Тоді:*

- (i) *множина K є мінімальним ідеалом моноїда M;*
- (ii) *множина K є регулярним $\mathscr{D}$-класом і вона є об'єднанням скінченних груп;*
- (iii) *кожна точка $q \in Q$ є нерухомою точкою щонайменше одного ідемпотента $e \in K$ такого, що $e \in K \cap \operatorname{Stab}(q)$;*
- (iv) *для кожного ідемпотента $e \in K$ група G_e є транзитивною групою степеня $r(M)$, і всі такі групи є еквівалентними.*

Доведення. Нехай M_0 — однозначний моноїд відношень

$$M_0 = M \cup \{0\}.$$

Маємо $r(M) = r(M_0)$. Отже, теорему 9.3.10 застосуємо до моноїда M_0. Для всіх елементів m моноїда M маємо

$$mM_0 = mM \cup \{0\}.$$

Очевидно, звідси випливає, що множина mM є мінімальним правим ідеалом моноїда M тоді і тільки тоді, коли mM_0 є 0-мінімальним правим ідеалом моноїда M_0. Аналогічне виконується для лівих і двобічних ідеалів. Зокрема, 0-мінімальний ідеал J моноїда M_0 є об'єднанням нуля 0 та мінімального ідеалу K моноїда M. Це доводить твердження (i).

Далі множина K є $\mathscr{D}$-класом моноїда M_0, а також вона є $\mathscr{D}$-класом моноїда M. Оскільки добуток двох елементів моноїда M ніколи не дорівнює нулю 0, то кожен $\mathscr{H}$-клас ідеала K є групою. Це доводить твердження (ii).

Інші твердження не потребують доведень. □

Нехай M — транзитивний однозначний моноїд відношень над непорожньою множиною Q скінченного мінімального рангу і

$$K = \{m \in M\colon \operatorname{rank}(m) = r(M)\}.$$

Групи G_e, для кожного ідемпотента e ідеала K, є еквівалентними транзитивними групами підстановок. *Групою Сушкевича* моноїда M є за означенням одна з таких груп.

9.4 Дуже тонкі коди

Код $X \subset A^+$ називається *дуже тонким*, якщо існує слово x в моноїді X^*, яке не множником слова в коді X. Нагадаємо, що через $F(X)$ позначається множина множників слів в коді X і, що $\overline{F}(X) = A^* \setminus F(X)$. З цими позначеннями код X є дуже тонким тоді і лише тоді, коли

$$X^* \cap \overline{F}(X) \neq \varnothing.$$

Кожен дуже тонкий код є тонким (тобто, він задовольняє умову $\overline{F}(X) \neq \varnothing$). Навпаки, тонкий код не є завжди дуже тонким (див. приклад 9.4.13). Проте, тонкий повний код X є дуже тонким. Справді, розглянемо слово $w \in \overline{F}(X)$. Оскільки код X є повним, то існують $u, v \in A^*$ такі, що $uwv \in X^*$. Тоді $uwv \in X^* \cap \overline{F}(X)$.

Мета цього розділу — довести наступний результат. Зокрема, він показує, що розпізнаваний код є дуже тонкий. Це є більш точніше, ніж твердження 2.5.20, яке лише стверджує, що розпізнаваний код є тонким.

Для простоти описання ми використовуємо наступне означення. Для фіксованого автомата $\mathcal{A}$ *рангом слова* w в $\mathcal{A}$ називається ранг відношення $\varphi_{\mathcal{A}}(w)$. Це узгоджується з визначенням рангу, наведеним у підрозділі 3.6 для детермінованих автоматів, як це показано в прикладі 4.2.6.

Теорема 9.4.1. *Нехай $X \subset A^+$ — код і $\mathcal{A} = (Q, 1, 1)$ — неоднозначний обрізаний автомат, який розпізнає моноїд X^*. Наступні умови є еквівалентними:*

(i) X є дуже тонким кодом;
(ii) моноїд $\varphi_{\mathcal{A}}(A^*)$ має скінченний мінімальний ранг.

Доведення цього результату складається з декількох етапів. Почнемо з наступної властивості, яка використовується для доведення того факту, що з умови (i) випливає умова (ii).

Твердження 9.4.2. *Нехай $X \subset A^+$ — код і $\mathcal{A} = (Q, 1, 1)$ — неоднозначний обрізаний автомат, який розпізнає моноїд X^*. Для всіх слів $w \in \overline{F}(X)$ ранг слова w в автоматі $\mathcal{A}$ є скінченним.*

Доведення. Для кожного стану $p \in Q$ нехай $\Phi(p)$ — множина префіксів слова w, які є мітками шляхів зі стану p у стан 1:

$$\Phi(p) = \{u \in A^* \colon u \leqslant w \quad \text{і} \quad p\varphi_{\mathcal{A}}(u)1\}.$$

Далі ми доведемо, якщо $\Phi(p) = \Phi(p')$ для деяких станів $p, p' \in Q$, то рядки індексів p і p' в $\varphi_{\mathcal{A}}(w)$ є рівними. Розглянемо стан $q \in Q$ такий, що

$$p\varphi_{\mathcal{A}}(w)q.$$

Оскільки автомат $\mathcal{A}$ є обрізаним, то існують слова $v, v' \in A^*$ такі, що $1\varphi_(v)p$ і $q\varphi_(v')1$. Таким чином, $1\varphi_{\mathcal{A}}(vwv')1$, звідки випливає, що $vwv' \in X^*$. Оскільки $w \in \overline{F}(X)$, то шлях $p \xrightarrow{w} q$ не є простим. Тоді існують слова $u, u' \in A^*$ такі, що $w = uu'$ і $vu, u'v' \in X^*$. Звідси випливає, що існує в автоматі $\mathcal{A}$ шлях

$$1 \xrightarrow{v} p \xrightarrow{u} 1 \xrightarrow{u'} q \xrightarrow{v'} 1.$$

За означенням $u \in \Phi(p)$, звідки випливає, що $u \in \Phi(p')$. З цього отримуємо, що $p'\varphi_(u)1\varphi_(u')q$, а отже $p'\varphi_(w)q$. Це доводить наше висловлення.

Кількість множин $\Phi(p)$ для стану $p \in Q$ є скінченною. Згідно до висловлення, яке тільки, що було доведено, множина рядків відношення $\varphi_{\mathcal{A}}(w)$ також є скінченною. За твердженням 9.3.7 звідси випливає, що слово w має скінченний ранг. □

Приклад 9.4.3. Нехай $X = \{a^n ba^n : n \geqslant 0\}$ — код над алфавітом $A = \{a, b\}$. X є дуже тонким кодом, оскільки $b^2 \in X^* \cap \overline{F}(X)$. Автомат, який розпізнає моноїд X^* зображено на рис. 9.9. Образ стосовно відношення e слова b^2 в асоційованому

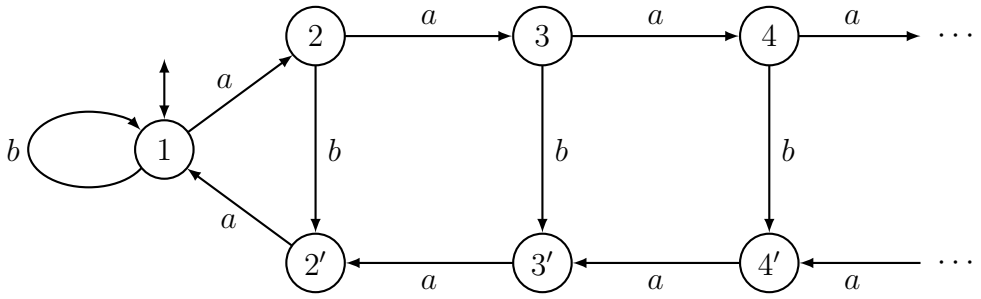


Рис. 9.9: Автомат, який розпізнає моноїд X^*

моноїді відношень M є ідемпотентом ранга 1. Скінченність рангу також випливає з твердження 9.4.2, оскільки слово b^2 не є множником слова в коді X. Локалізований моноїд eMe зведений до e і 0 (який є образом слова b^2ab^2, для прикладу). Моноїд M має елементи нескінченного рангу: це виконується для образу слова a. Справді, очевидно, що жоден степінь цього елемента не може бути ідемпотентом. а отже за твердженням 9.3.8, цей елемент має нескінченний ранг. Більше того, моноїд M має елементи скінченного рангу n для кожного цілого числа $n \geqslant 0$: слово ba^nba^nb має ранг $n + 1$, і це читач може легко перевірити.

Твердження 9.4.4. *Нехай X — код над алфавітом A, $\mathcal{A} = (Q, 1, 1)$ — неоднозначний обрізаний автомат, який розпізнає моноїд X^*, φ — асоційоване зображення та $M = \varphi(A^*)$.*

Для кожного ідемпотента $e \in \varphi(X^*)$ зі скінченним рангом такий, що група G_e є транзитивною, виконуються наступні висловлення:

(*i*) *існують слова $v_1, v_2, \ldots, v_{n+1} \in \varphi^{-1}(H(e))$ з такою властивістю: для всіх слів $y, z \in A^*$ таких, що*

$$yv_1v_2 \cdots v_{n+1}z \in X^*$$

існує натуральне число i $(1 \leqslant i \leqslant n)$ таке, що:

$$yv_1v_2 \cdots v_i, v_{i+1} \cdots v_{n+1}z \in X^*;$$

(*ii*) *множина $\varphi^{-1}(e) \cap \overline{F}(X)$ є непорожньою.*

Доведення. Нехай $e = \mathbf{lr}$ — стовпчико-рядковий розклад відношення e, S — множина його нерухомих точок і $G = H(e)$. За твердженням 9.1.9 звуження $\gamma\colon eMe \to M_e$ є ізоморфізмом визначеним $m \mapsto \mathbf{r}m\mathbf{l}$ і його обернене відображення визначається так $n \mapsto \mathbf{l}n\mathbf{r}$.

Множина S містить елемент 1, оскільки $e \in \varphi(X^*)$. Покладемо $S = \{1, 2, \ldots, n\}$. Спочатку виключаємо випадок, коли $\varphi^{-1}(e) = \{1\}$. Тоді e є одиничним елементом моноїда M і $S = Q$. Оскільки $H(e) = \{1\}$ і за припущенням група G_e є транзитивною, то отримуємо, що $A = X$. Таким чином, результат виконується тривіально.

Тепер припустимо, що $\varphi^{-1}(e) \neq \{1\}$. Виберемо елементи $g_2, g_3, \ldots, g_n \in G_e$ такими, що

$$2g_2 = 1, \quad 3g_2g_3 = 1, \quad \ldots, \quad ng_2g_3\cdots g_n = 1.$$

Такі елементи існують, оскільки G_e є транзитивною групою підстановок. Підстановки $g_2, g_3, \ldots, g_n$ є звуженнями на S елементів $h_2, h_3, \ldots, h_n$ групи $H(e)$ і виконуються рівності $h_i = \mathbf{l}g_i\mathbf{r}$. Отже $g_i = \mathbf{r}h_i\mathbf{l} = \gamma(h_i)$. Нехай $v_1, v_2, \ldots, v_{n+1} \in A^+$ є такими словами, що

$$\varphi(v_1) = \varphi(v_{n+1}) = e, \quad \varphi(v_2) = h_2, \quad \ldots, \quad \varphi(v_n) = h_n.$$

Покладемо $w = v_1v_2\cdots v_{n+1}$. Розглянемо слова $y, z \in A^*$ такі, що $ywz \in X^*$. Тоді існують стани $p, q \in Q$ такі, що

$$1 \xrightarrow{y} p \xrightarrow{w} q \xrightarrow{z} 1.$$

Зауважимо, що

$$\varphi(w) = \mathbf{lr}h_2\cdots h_n\mathbf{lr} = \mathbf{l}\gamma(h_2\cdots h_n)\mathbf{r} = \mathbf{l}g_2\cdots g_n\mathbf{r}.$$

Оскільки $p\varphi(w)q$, то існують $r, s \in S$ такі, що $p \xrightarrow{\mathbf{l}} r$, $rg_2\cdots g_n = s$ і $s \xrightarrow{\mathbf{r}} q$. Тоді $rg_2\cdots g_r = 1$ (з $g_2\cdots g_r = \mathrm{id}_S$ у випадку $r = 1$). Оскільки елементи $g_2, \ldots, g_r$ є підстановками, то звідси випливає рівність

$$1g_{r+1}\cdots g_n = s.$$

Отже, отримуємо, що $r \xrightarrow{h_2\cdots h_r} 1$, $1 \xrightarrow{h_{r+1}\cdots h_n} s$, і оскільки $\mathbf{l}_{p,r} = e_{p,r}$, $\mathbf{r}_{s,q} = e_{s,q}$, то маємо

$$p \xrightarrow{eh_2\cdots h_r} 1 \qquad \text{і} \qquad 1 \xrightarrow{h_{r+1}\cdots h_ne} q.$$

Звідси випливає, що

$$yv_1v_2\cdots v_r, v_{r+1}\cdots v_{n+1}z \in X^*.$$

отож, слова $v_1, \cdots, v_{n+1}$ задовольняють умову (i).

Для доведення того, що виконується умова (ii), перевіримо спочатку, що слово $w = v_1v_2\cdots v_{n+1}$ міститься в множині $\overline{F}(X)$. Справді, припустимо, що $ywz \in X$ для деяких слів $y, z \in A^*$. Тоді існує таке ціле число i $(1 \leqslant i \leqslant n)$, що

$$yv_1\cdots v_i, v_{i+1}\cdots v_{n+1}z \in X^*.$$

Оскільки $v_1, \ldots, v_{n+1} \in A^+$, то ці два слова містяться насправді в моноїді X^+, а це суперечить тому факту, що множина X є кодом. Отож, $w \in \overline{F}(X)$.

Нехай h' — інверсний елемент до $h = \varphi(w)$ в $H(e)$, і нехай w' — таке слово, що $\varphi(w') = h'$. Тоді $ww' \in \varphi^{-1}(e)$, а також маємо, що $ww' \in \overline{F}(X)$. Це завершує доведення твердження. □

Доведення теореми 9.4.1. $(i) \Rightarrow (ii)$ Нехай $x \in X^* \cap \overline{F}(X)$. За твердженням 9.4.2 ранг елемента $\varphi(x)$ скінченний. Оскільки $x \in X^*$, то маємо, що $(1, \varphi_{\mathcal{A}}(X), 1) = 1$, а отже $\varphi_{\mathcal{A}}(x) \neq 0$. Це доводить, що моноїд $\varphi_{\mathcal{A}}(A^*)$ має скінченний ранг.

$(ii) \Rightarrow (i)$ Напівгрупа $M = \varphi_{\mathcal{A}}(A^*)$ є транзитивним однозначним моноїдом відношень, що має скінченний мінімальний ранг $r(M)$. Нехай

$$K = \{m \in M \colon \operatorname{rank}(m) = r(M)\}.$$

За теоремами 9.3.10 і 9.3.15 існує ідемпотент $e \in K \cap \operatorname{Stab}(1)$, і група підстановок G_e є транзитивною степеня $r(M)$. За твердженням 9.4.4 множина $\varphi_{\mathcal{A}}^{-1}(e) \cap \overline{F}(X)$ непорожня. Оскільки $\varphi_{\mathcal{A}}^{-1}(e) \subset X^*$, то код X є дуже тонким. □

Тепер ми викладемо ряд наслідків теореми 9.4.1.

Наслідок 9.4.5. *Нехай X — повний код і $\mathcal{A} = (Q, 1, 1)$ — однозначний обрізаний автомат, який розпізнає вільний моноїд X^*. Наступні умови еквівалентні:*

(i) X є тонким кодом;
(ii) моноїд $\varphi_{\mathcal{A}}(A^*)$ містить елементи скінченного рангу.

Доведення. Оскільки код X є повним, то моноїд $\varphi_{\mathcal{A}}(A^*)$ не містить нульового відношення за твердженням 2.5.28. Отож, еквівалентність тверджень (i) та (ii) безпосередньо випливає з теореми 9.4.1. □

Іншим наслідком теореми 9.4.1 є алгебраїчне доведення теореми 2.5.13, яке не залежить від доведення цієї теореми, викладеного за допомогою теорії мір.

Наслідок 9.4.6. *Якщо X — тонкий повний код, то X є максимальним кодом.*

Доведення. Нехай $\mathcal{A} = (Q, 1, 1)$ — однозначний обрізаний автомат, який розпізнає вільний моноїд X^* і φ — асоційоване зображення. Нехай $x \in X^*$ — слово таке, що $e = \varphi(x)$ є ідемпотентом мінімального ідеала J моноїда $\varphi(A^*)$. Такий демпотент існує за теоремою 9.3.15(iii).

Нехай $y \notin X$. Тоді $e\varphi(y)e = \varphi(xyx)$ міститься в $\mathscr{H}$-класі ідемпотента e. Цей $\mathscr{H}$-клас є скінченною групою. Отож, існує натуральне число n таке, що $(\varphi(xyx))^n = e$. Звідси випливає, що $(xyx)^n \in X^*$, а отже отримуємо, що множина $X \cup \{y\}$ не є кодом. □

Нехай $X \subset A^+$ — код і $\mathcal{A} = (Q, 1, 1)$ — однозначний обрізаний автомат, який розпізнає вільний моноїд X^*. Ми довели, що код X є дуже тонким тоді і лише тоді, коли моноїд $M = \varphi_{\mathcal{A}}(A^*)$ має елементи скінченного додатного рангу. Нехай r — найменший з цих ненульових рангів, і нехай K — множина елементів моноїда M, які мають ранг r. Покладемо $\varphi = \varphi_{\mathcal{A}}$. Корисно мати на увазі такі факти.

Теорема 9.4.7.

Лема 9.4.8. *Нехай X — повний тонкий код. Тоді для довільного слова $u \in X^*$ існує слово $w \in X^* u X^*$, яке задовольняє таку умову: якщо $ywz \in X^*$, то існує факторизація $w = fug$ така, що $yf, gz \in X^*$.*

Доведення. □

Твердження 9.4.9.

Доведення. □

Твердження 9.4.10.

Доведення. □

Приклад 9.4.11.

Приклад 9.4.12.

Приклад 9.4.13.

9.5 Група та порядок кода

Твердження 9.5.1.

Доведення. □

Твердження 9.5.2.

Доведення. □

Приклад 9.5.3.

9.6 Інтерпретації

Твердження 9.6.1.

Доведення. □

9.7 Вправи до розділу 9

Підрозділ 9.1

В. 9.7.1.

В. 9.7.2.

В. 9.7.3.

В. 9.7.4.

В. 9.7.5.

Підрозділ 9.2

В. 9.7.6.

Підрозділ 9.3

В. 9.7.7.

В. 9.7.8.

В. 9.7.9.

В. 9.7.10.

В. 9.7.11.

В. 9.7.12.

В. 9.7.13.

В. 9.7.14.

В. 9.7.15.

В. 9.7.16.

В. 9.7.17.

В. 9.7.18.

В. 9.7.19.

Підрозділ 9.4

В. 9.7.20.

В. 9.7.21.

В. 9.7.22.

В. 9.7.23.

Підрозділ 9.5

В. 9.7.24.

В. 9.7.25.

В. 9.7.26.

В. 9.7.27.

В. 9.7.28.

Нотатки до розділу 9

Розділ 10

Синхронізація

10.1 Синхронізовані пари

10.2 Одноріжно синхронізовані коди

Приклад 10.2.1.

Твердження 10.2.2.

Доведення. □

Приклад 10.2.3.

Твердження 10.2.4.

Доведення. □

Приклад 10.2.5.

Приклад 10.2.6.

Теорема 10.2.7. *Нехай X — скінченний код. Тоді наступні умови є еквівалентними:*

(*i*) *X є круговим;*
(*ii*) *X є граничним;*
(*iii*) *X є однорідно синхронізованим.*

Твердження 10.2.8.

Доведення. □

Доведення теореми 10.2.7. □

Приклад 10.2.9.

Приклад 10.2.10.

Теорема 10.2.11.

Доведення. □

Приклад 10.2.12.

10.3 Локально синтаксично алалізоівні коди та локальні автомати

10.4 Дорожнє фарбування

10.5 Вправи до розділу 10

Підрозділ 10.2

В. 10.5.1.

В. 10.5.2.

В. 10.5.3.

В. 10.5.4.

В. 10.5.5.

Підрозділ 10.3

В. 10.5.6.

В. 10.5.7.

В. 10.5.8.

В. 10.5.9.

Нотатки до розділу 10

Розділ 11

Групи кодів

11.1 Групи та композиція кодів

11.2 Синхронізація семаформних кодів

11.3 Групові коди

11.4 Автомати біфіксних кодів

11.5 Глибина

11.6 Групи скінченних біфіксних кодів

Теорема 11.6.1. *Нехай G — примітивна група підстановок степеня d, яка містить d-цикл. Тоді або G є регулярною групою, або групою Фробеніуса, або є 2-транзитивною.*

11.7 Приклади

11.8 Вправи до розділу 11

Підрозділ 11.1

В. 11.8.1.

Підрозділ 11.3

В. 11.8.2.

В. 11.8.3.

Підрозділ 11.4

В. 11.8.4.

Підрозділ 11.5

В. 11.8.5.

В. 11.8.6.

В. 11.8.7.

В. 11.8.8.

В. 11.8.9.

Підрозділ 11.6

В. 11.8.10.

В. 11.8.11.

В. 11.8.12.

В. 11.8.13.

В. 11.8.14.

В. 11.8.15.

Підрозділ 11.7

В. 11.8.16.

В. 11.8.17.

В. 11.8.18.

В. 11.8.19.

Нотатки до розділу 11

Розділ 12

Факторизації циклічних груп

12.1 Факторизації циклічних груп

12.2 Багнети

12.3 Гаки

Твердження 12.3.1. *Нехай $L, R \subseteq \mathbb{N}$ з $0 \in L \cap R$ і $n \geqslant 1$ — такі, що пара (L, R) є прямою по модулю n і $\mathrm{Card}(L), \mathrm{Card}(R) \geqslant 2$. Якщо n — первинне число, то $X = \{a^n\} \cup a^L b \cup b a^R$ є кодом, який не міститься в скінченному максимальному коді.*

Доведення. □

12.4 Вправи до розділу 12

Підрозділ 12.1

В. 12.4.1.

В. 12.4.2.

В. 12.4.3.

Підрозділ 12.2

В. 12.4.4.

В. 12.4.5.

Підрозділ 12.3

В. 12.4.6.

В. 12.4.7.

В. 12.4.8.

В. 12.4.9.

В. 12.4.10.

Нотатки до розділу 12

Розділ 13

Щільності

13.1 Імовірність

13.2 Щільності

13.3 Ентропія

13.4 Імовірності над моноїдом

13.5 Строгі контексти

13.6 Вправи до розділу 13

Підрозділ 13.1

В. 13.6.1.

Підрозділ 13.2

В. 13.6.2.

Підрозділ 13.3

В. 13.6.3.

Підрозділ 13.4

В. 13.6.4.

В. 13.6.5.

Підрозділ 13.5

В. 13.6.6.

В. 13.6.7.

В. 13.6.8.

Нотатки до розділу 13

Розділ 14

Поліноми скінченних кодів

14.1 Додатні факторизації

14.2 Теорема про факторизацію

14.3 Некомутативні поліноми

14.4 Доведення теореми про факторизацію

14.5 Застосування

14.6 Комутативна еквівалентність

14.7 Повна зведеність

14.8 Вправи до розділу 14

Підрозділ 14.1

В. 14.8.1.

В. 14.8.2.

В. 14.8.3.

В. 14.8.4.

В. 14.8.5.

В. 14.8.6.

В. 14.8.7.

В. 14.8.8.

В. 14.8.9.

Підрозділ 14.3

В. 14.8.10.

В. 14.8.11.

В. 14.8.12.

В. 14.8.13.

Підрозділ 14.4

В. 14.8.14.

В. 14.8.15.

Підрозділ 14.5

В. 14.8.16.

Підрозділ 14.6

В. 14.8.17.

В. 14.8.18.

Підрозділ 14.7

В. 14.8.19.

В. 14.8.20.

В. 14.8.21.

В. 14.8.22.

Нотатки до розділу 14

Бібліоґрафія

[1] Ф. Р. Гантмахер, *Теория матриц*, Наука, Москва, 1967.

[2] Ф. Р. Гантмахер, *Теория матриц*, 5-е изд. Физматлит, Москва, 2004.

[3] И. М. Гельфанд, В. С. Ретах, *Детерминанты матриц над некоммутативными кольцами*, Функц. анализ и его прил. **25** (1991), no. 2, 13–25 (див. англ. пер. [74]).

[4] А. Клиффорд, Г. Престон, *Алгебраическая теория полугрупп*, Том 1, Пер. с англ. В. А. Баранского и В. Г. Житомирского. Под ред. Л. Н. Шеврина. М., Мир, 1972.

[5] Ж. Лаллеман, *Полугруппы и комбинаторные приложения*, Пер. с англ. И. О. Корякова; Под ред. Л. Н. Шеврина, Мир, Москва, 1985.

[6] В. И. Левенштейн, *О некоторых своствах кодирования и самонастраивающихся автоматах для декодирования сообщений*, Проблемы кибернетики **11** (1964), 63–121.

[7] В. Магнус, А. Каррас, Д. Солитэр, *Комбинаторная теория групп*, Наука, Москва, 1974.

[8] Г. С. Маканин, *О ранге бескоэффициентных уравнений с четырьмя неизвестными в свободной полугруппе*, Матем. сб. **100**(**142**) (1976), no. 2(6), 285–311.

[9] Ал. А. Марков, *Об алфавитном кодировании*, Докл. АН СССР **132** (1960), no. 3. 521–523.

[10] Ал. А. Марков, *Об алфавитном кодировании II*, Докл. АН СССР **139** (1961), no. 3. 560–561.

[11] А. Саломаа, *Жемчужины теории формальных языков*, пер. з англ. Мир, Москва, 1986.

[12] Л. Н. Шеврин, *О подполугруппах свободных полугрупп*, Докл. АН СССР **133** (1960), no. 3, 537–539. (англ. перекл. в [192])

[13] R. Adler, D. Coppersmith, and M. Hassner, *Algorithms for sliding block codes. An application of symbolic dynamics to information theory*, IEEE Trans. Inf. Theory **29** (1983), no. 1, 5–22.

[14] A. V. Aho and M. J. Corasick, *Efficient string matching: An aid to bibliographic search*, Communications of the ACM, **18** (1975), no. 6, 335–340.

[15] A. V. Aho, J. E. Hopcroft, and J. D. Ullman, The design and analysis of computer algorithms. Addison-Wesley, 1974.

[16] R. Ahlswede, B. Balkenhol, and L. H. Khachatrian, *Some properties of fix-free codes*, In Proc. 1st Int. Sem. on Coding Theory and Combinatorics, Thahkadzor, Armenia, pp. 20–33, 1996.

[17] A. Apostolico and R. Giancarlo, *Pattern-matching implementation of a fast test for unique decipherability*, Inform. Process. Lett. **18** (1984), no. 3, 155–158.

[18] R. B. Ash, *Information theory*, Dover Publ. Inc. 1965.

[19] R. B. Ash, *Information theory*, Dover Publ. Inc. 1990.

[20] R. B. Ash, *Information theory*, Dover Publ. Inc. 2012.

[21] J. Ashley, B. Marcus, D. Perrin, and S. Tuncel, *Surjective extensions of sliding block codes*, SIAM J. Discrete Math. **6** (1993), no. 4, 582–611.

[22] G. Bandyopadhyay, *A simple proof of the decipher ability criterion of Sardinas and Patterson*, Inf. Control **6** (1963), no. 4, 331–336.

[23] E. Barbin-Le Rest et M. Le Rest, *Sur la combinatoire des codes à deux mots*, Theor. Comput. Sci. **41** (1985), 61–80.

[24] F. Bassino, M.-P. Béal, and D. Perrin, *A finitestateversion of the Kraft-McMillan theorem*, SIAM J. Comput. **30** (2000), no. 4, 1211–1230.

[25] M.-P. Béal, *Codage symbolique*, Masson, 1993.

[26] M.-P. Béal, J. Berstel, B. H. Marcus, D. Perrin, Ch. Reutenauer, and P. H. Siegel, *Variable length-codes and finite automata*, In Isaac Woungang, editor, Selected Topicsin Information and Coding Theory. World Scientific, 2009.

[27] M.-P. Béal, O. Carton, and Ch. Reutenauer, *Cyclic languages and strongly cyclic languages*, Puech, Claude (ed.) et al., STACS 96. 13th annual symposium on theoretical aspects of computer science. Grenoble, France, February 22–24, 1996. Proceedings. Berlin: Springer-Verlag. Lect. Notes Comput. Sci. **1046** (1996), 49–59.

[28] M.-P. Béal, S. Lombardy, and J. Sakarovitch, *On the equivalence of $\mathbb{Z}$-automata*, In ICALP'05, Springer-Verlag, Lect. Notes Comput. Sc. **3580** (2005), 397–409.

[29] M.-P. Béal and D. Perrin, *Codes and sofic constraints*, Theor. Comput. Sci. *340* (2005), no. 2, 381–393.

[30] M.-P. Béal and D. Perrin, *Complete codes in a sofic shift*, In STACS 2006, Lect. Notes Comput. Sci. **3884** (2006), 127–136. Springer-Verlag.

[31] J. Berstel, *Transductions and context-free languages*, Vieweg and Teubner Verlag, 1979.

[32] J. Berstel and D. Perrin, *The origins of combinatorics on words*, European J. Combin. **28** (2007), no. 3, 996–1022.

[33] J. Berstel, D. Perrin, J. Perrot, and A. Restivo, *Sur le théorème du défaut*, J. Algebra **60** (1979), no. 1, 169–180.

[34] J. Berstel and Ch. Reutenauer, *Rational series and their languages*, Springer-Verlag, 1988.

[35] J. Berstel and Ch. Reutenauer, *Zeta functions of formal languages*, Trans. Amer. Math. Soc. **321** (1990), no. 2, 533–546,

[36] M. T. Biskup, *Shortest synchronizing strings for Huffman codes*, In E. Ochmanski and J. Tyszkiewicz, eds., Mathematical Foundations of Computer Science 2008, Torun, Poland, August 25–29, 2008, Springer-Verlag of Lect. Notes in Comput. Sc. **5162** (2008), 120–131.

[37] E. K. Blum, *Free subsemigroups of a free semigroup*, Michigan Math. J. **12** (1965), no. 2, 179–182.

[38] J.-M. Boë, A. de Luca, and A. Restivo, *Minimal complete sets of words*, Theor. Comput. Sci. **12** (1980), no. 3, 325–332.

[39] Ph. G. Bradford, M. J. Golin, L. L. Larmore, and W. Rytter, *Optimal prefix-free codes for unequal letter costs: dynamic programming with the Monge property*, J. Algorithms **42** (2002), no. 2, 277–303.

[40] V. Bruyère, *Maximal prefix products*, Semigroup Forum **36** (1987), no. 1, 147–157.

[41] V. Bruyère, *Automata and codes with bounded deciphering delay*, LATIN'92 (São Paulo, 1992), Springer-Verlag, Lect. Notes Comput. Sci. **583** (1992), 99–107.

[42] V. Bruyère and M. Latteux, *Variable-length maximal codes*, In ICALP'96, Springer-Verlag, Lect. Notes Comput. Sci. **1099** (1996), 24–47.

[43] V. Bruyère and D. Perrin, *Maximal bifix codes*, Theor. Comput. Sci. **218** (1999), no. 1, 107–121.

[44] V. Bruyère, L. M. Wang, and L. Zhang, *On completion of codes with finite deciphering delay*, European J. Combin. **11** (1990), no. 6, 513–521.

[45] J. A. Brzozowski, *Roots of star events*, J. Assoc. Comput. Mach. **14** (1967), no. 3, 466–477.

[46] R. M. Capocelli, A. A. De Santis, L. Gargano, and U. Vaccaro, *On the construction of statistically synchronizable codes*, IEEE Trans. Inf. Theory **38** (1992), no. 2, 407–414.

[47] R. M. Capocelli and Ch. M. Hoffmann, *Algorithms for factorizing and testing subsemigroups*, Combinatorial algorithms on words, Proc. NATO Adv. Res. Workshop, Maratea/Italy 1984, NATO ASI Ser., Ser. F **12** (1985), 59–81.

[48] J. Černý. *Poznamka k homogenym s konecnymi automati*, Mat.-fyz. cas. SAV. **14** (1964), 208–215.

[49] Y. Césari, *Sur un algorithme donnant les codes bipréfixes finis*, Math. Syst. Theory **6** (1972), no. 1–2, 221–225.

[50] Y. Césari, *Propriétes combinatoires des codes bipréfixes*, In D. Perrin, editor, Théorie des Codes (actes de la septième École de Printemps d'Informatique Théorique), LITP, (1979), pp. 20–46.

[51] Chr. Choffrut, *Une caractérisation des codes à délai borné par leur fonction de décodage*, In D. Perrin, editor, Théorie des Codes (actes de la septième École de Printemps d'Informatique Théorique), LITP, (1979), pp. 47–56.

[52] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*, Vol. 1, Providence, R.I.: Amer. Math. Soc. 1961.

[53] P. M. Cohn, *On subsemigroups of free semigroups*, Proc. Amer. Math. Soc. **63** (1962), no. 3, 347–351.

[54] P. M. Cohn, *Free rings and their relations*, Acad. Press, 1971.

[55] P. M. Cohn, *Free rings and their relations*, London Math. Math. Soc. Monogr. **19**, Academic Press, 2nd ed., 1985.

[56] Ch. Deppe and H. Schnettler, *On q-ary fix-free codes and directed de Brujin graphs*, In IEEE International Symposium on Information Theory, 2006, p. 1482–1485.

[57] J. S. Devitt and D. M. Jackson, *Comma-free codes: an extension of certain enumerative techniques to recursively defined sequences*, J. Comb. Theory, Ser. A **30** (1981), no. 1, 1–18.

[58] V. Diekert and A. Muscholl, Code problems on traces. In: Penczek W., SzaE,as A. (eds) Mathematical Foundations of Computer Science 1996. MFCS 1996. Springer, Berlin, Heidelberg, Lect. Notes Comput. Sci. **1113** (1996), 2–17.

[59] D. Derencourt, *A three-word code which is not prefix-suffix composed*, Theor. Comput. Sci. **163** (1996), 145–160.

[60] A. Ehrenfeucht and G. Rozenberg, *Elementary homomorphisms and a solution to the D0L sequence equivalence problem*, Theor. Comput. Sci. **7** (1978), no. 2, 169–183.

[61] A. Ehrenfeucht and G. Rozenberg, *Each regular code is included in a regular maximal code*, RAIRO Inf. Théor. 20 (1986), no. 1, 89–96.

[62] S. Eilenberg, *Automata, languages and machines*, Vol. **A**, Academic Press. 1974.

[63] S. Eilenberg, *Automata, languages and machines*, Vol. **B**, Academic Press. 1976.

[64] P. Elias, *Universal codeword sets and representations of the integers*, IEEE Trans. Inf. Theory **21** (1975), no. 2, 194–203.

[65] W. L. Eastman, *On the construction of comma-free codes*, IEEE Trans. Inf. Theory **11** (1965), no. 2, 263–267.

[66] W. Feller, *An introduction to probability theory and its applications*, Wiley, 3rd ed., 1968.

[67] D. Foata and Guo Niu Han, *Nombres de Fibonacci et polynômes orthogonaux*, In M. Morelli and M. Tangheroni, eds, Leonardo Fibonacci: il tempo, le opere, l'eredità scientifica, Pisa, 23–25 March. Pacini Editore (Fondazione IBM Italia). (1994), pp. 179–200,

[68] C. F. Freiling, D. S. Jungreis, F. Theberge, and K. Zeger, *Almost all complete binary prefix codes have a self-synchronizing string*, IEEE Trans. Inf. Theory **49** (2003), no. 9, 2219–2225.

[69] Z. Galil, *Open problems in stringology*. In A. Apostolico and Z. Galil, eds., Combinatorial Algorithms on Words (Maratea, 1984), NATO Adv. Sci. Inst. Ser. F, Springer-Verlag **12** (1985), pp. 1–8.

[70] R. G. Gallager and D. C. van Voorhis, *Optimal source codes for geometrically distributed integer alphabets*, IEEE Trans. Inf. Theory **21** (1975), no. 2, 228–230,

[71] F. R. Gantmacher, *The theory of matrices*, Vols 1, 2. Chelsea. Translated from the Russian original, 1959.

[72] F. R. Gantmacher, *The theory of matrices*, AMS Chelsea Publishing, Reprinted by American Mathematical Society, 2000.

[73] A. M. Garsia and M. L. Wachs, *A new algorithm for minimum cost binary trees*, SIAM J. Comput. **6** (1977), no. 4, 622–642.

[74] I. M. Gel'fand and V. S. Retakh, *Determinants of matrices over noncommutative rings*, Funct. Anal. Appl. **25** (1991), no. 2, 91–102 (Russian version of [3]).

[75] E. N. Gilbert, *Synchronization of binary messages*, IRE Trans.Inform. Theory **6** (1960), no. 4, 470–477,

[76] E. N. Gilbert and E. F. Moore, *Variable length binary encodings*, Bell System Tech. J. **38** (1959), no. 4, 933–967.

[77] D. Gillman and R. L. Rivest, *Complete variable-length "fix-free" codes*, Des. Codes Cryptography **5** (1995), no. 2, 109–114.

[78] B. Girod, Bidirectionally decodable streams of prefix code words, IEEE Communications Letters **3** (1999), no. 8, 245–247.

[79] M. J. Golin and G. Rote, *A dynamic programming algorithm for constructing optimal prefix-free codes with unequal letter costs*, IEEE Trans. Inf. Theory **44** (1998), no. 5, 1770–1781.

[80] M. J. Golin, C. Kenyon, and N. E. Young, *Huffman coding with unequal letter costs*, In Proc. of the Thirty-Fourth Annual ACM Symposium on 12479 Theory of Computing, 2002, pp. 785–791.

[81] S. W. Golomb, *Run-length encodings*, IEEE Trans. Inf. Theory, **12** (1966), no. 3, 399–401.

[82] S. W. Golomb, D. Gordon, and L. R. Welch, *Comma-free codes*, Can. J. Math. **10** (1958), 202–209.

[83] I. P. Goulden and D. M. Jackson, *Combinatorial enumeration*, Dover Publ. Inc., 1983.

[84] I. P. Goulden and D. M. Jackson, *Combinatorial enumeration*, Dover Publ. Inc. Reprint of the 1983 original, 2004.

[85] J. A. Green, *On the structure of semigroups*, Ann. Math. (2) **54** (1951), no. 1, 163–172.

[86] L. J. Guibas and A. M. Odlyzko, *Maximal prefix synchronized codes*, SIAM J. Appl. Math. **35** (1978), no. 2, 401–418.

[87] T. Harju and D. Nowotka, *The equation $x^i = y^j z^k$ in a free semigroup*, Semigroup Forum, 68 (2004), no. 3, 488–490.

[88] K. Hashiguchi and N. Honda, *Homomorphisms that preserve star-height*, Inf. Control **30** (1976), no. 3, 247–266.

[89] K. Hashiguchi and N. Honda, *Properties of code events and homomorphisms over regular events*, J. Comput. System Sci. **12** (1976), no. 3, 352–367.

[90] T. Head and A. Weber, *Deciding code related properties by means of finite transducers*, In R. Capocelli, A. De Santis, and U. Vaccaro, editors, Sequences, II (Positano, 1991), Springer-Verlag. (1993), pp. 260–272.

[91] T. Head and A. Weber, *Deciding multiset decipherability*, IEEE Trans. Inform. Theory, **41** (1) (1995), 291–297.

[92] Ch. M. Hoffmann, *A note on unique decipherability*, In Math. Foundations Comput. Sci. (MFCS), Springer-Verlag. Lect, Notes Comput. Sci. **176** (1984), 50–63.

[93] T. C. Hu and A. C. Tucker, *Optimal computer search trees and variable-length alphabetical codes*, SIAM J. Appl. Math. **21** (1971), 514–532.

[94] T. C. Hu and Paul A. Tucker, *Optimal alphabetic trees for binary search*, Inform. Process. Lett. **67** (1998), no. 3, 137–140,

[95] T. C. Hu and M.-T. Shing, *Combinatorial algorithms*, Dover Publ. Inc., 2nd ed., 2002.

[96] D. A. Huffman, *A method for the construction of minimum redundancy codes*. Proc. of the Institute of Electronics and Radio Engineers **40** (1952), no. 10, 1098–1101.

[97] D. A. Huffman, *Notes on information-lossless finite-state automata*, Nuovo Cimento, **13** (1959), Suppl. 2, 397–405.

[98] A. Itai, *Optimal alphabetic trees*, SIAM J. Comput. **5** (1976), no. 1, 9–18,

[99] M. Ito, H. Jürgensen, H. J. Shyr, and G. Thierrin, *Outfix and infix codes and related classes of languages*, J. Comput. Syst. Sci. **43** (1991), no. 3, 484–508.

[100] M. Ito and G. Thierrin, *Congruences, infix and cohesive prefix codes*, Theor. Comput. Sci. 136 (1994), no. 2, 471–485

[101] B. H. Jiggs, *Recent results in comma-free codes*, Can. J. Math. **15** (1963), 178–187.

[102] J. Karhumäki, *A property of three element codes*, In: M. Fontet, K. Mehlhorn (eds), STACS 84. Springer-Verlag, Lect. Notes Comput. Sci. **166** (1984), 305–313.

[103] R. M. Karp, *Minimum-redundancy coding for the discrete noiseless channel*, IRE Trans. Inform. Theory IT **7** (1961), 27–38.

[104] G. Keller, *Circular codes, loop counting, and zeta-functions*, J. Comb. Theory, Ser. A **56** (1991), no. 1, 75–83.

[105] J. H. Kingston, *A new proof of the Garsia-Wachs algorithm*, J. Algorithms **9** (1988), no. 1, 129–136.

[106] B. Kitchens, *Continuity properties of factor maps in ergodic theory*, Ph.D. Thesis, University of North Carolina, Chapel Hill (1981).

[107] D. E. Knuth, *Optimum binary search trees*, Acta Informatica **1** (1971), 14–25.

[108] D. E. Knuth, *Dynamic Huffman coding*, J. Algorithms, **6** (1985), no. 2, 163–180.

[109] D. E. Knuth, *The art of computer programming*, Vol. **III**: Sorting and Searching. Addison-Wesley, 2nd ed., 1998.

[110] Z. Kohavi, *Switching and finite automata theory*, McGraw-Hill, 1970.

[111] Z. Kohavi, *Switching and finite automata theory*, 2nd. ed., McGraw-Hill, 1978.

[112] Z. Kohavi, *Switching and finite automata theory*, 2nd. ed., McGraw-Hill, 1979.

[113] Z. Kohavi and N. K. Jha, *Switching and finite automata theory*, 3rd. ed., McGraw-Hill, 2010.

[114] D. Krob, *Codes limites et factorisations finies du monoïde libre*, RAIRO, Inf. Théor. Appl. **21** (1987), no. 4, 437–467.

[115] M. Kunc, *Undecidability of the trace coding problem and some decidable cases*, Theor. Comput. Sci. **310** (2004), no. 1–3, 393–459.

[116] G. Lallement, *Semigroups and combinatorial applications*, Wiley, 1979.

[117] N. H. Lam, *Finite maximal infix codes*, Semigroup Forum **61** (2000), no. 3, 346–56.

[118] N. H. Lam, *Finite maximal solid codes*, Theor. Comput. Sci. **262** (2001), no. 1-2, 333–347.

[119] N. H. Lam, *Completing comma-free codes*, Theor. Comput. Sci. 301 (2003), no. 1-3, 399–415.

[120] S. Lang, *Algebra*, Addison-Wesley, 1965.

[121] J.-L. Lassez, *Prefix codes and isomorphic automata*, Int. J. Computer Math. **3** (1973), no. 1–4, 309–314.

[122] J.-L. Lassez, *Circular codes and synchronization*, Int. J. Comput. Inform. Sci. **5** (1976), no. 2, 201–208.

[123] A. Lentin, *Equations dans les monoïdes libres*, Gauthier-Villars, 1972.

[124] A. Lentin and M.-P. Schützenberger, *A combinatorial problem in the theory of free monoids*, In Combinatorial Mathematics and its Applications (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967), Univ. North Carolina Press, Chapel Hill, N.C., 1969, pp. 128–144.

[125] M. Léonard, *A property of biprefix codes*, RAIRO, Inf. Théor. Appl. **22** (1988), no. 3, 311–318.

[126] F. W. Levi, *On semigroups*, Bull. Calcutta Math. Soc. **36** (1944), 141–146.

[127] B. Lewin, *Genes V*, Oxford University Press, 1994.

[128] D. A. Lind and B. H. Marcus, An introduction to symbolic dynamics and coding, Cambridge Univ. Press, 1995.

[129] J. H. van Lint, *Introduction to coding theory*, Springer-Verlag, 1982.

[130] D. Long, *On group codes*, Theor. Comput. Sci. **163** (1996), no. 1-2, 259–267.

[131] M. Lothaire, *Combinatorics on words*, Cambridge University Press, 1983.

[132] M. Lothaire, *Combinatorics on words*, 2nd ed., Cambridge University Press, 1997.

[133] M. Lothaire, Algebraic combinatorics on words, Encyclopedia Math. Appl. **90** Cambridge Univ. Press, 2002.

[134] M. Lothaire, *Applied combinatorics on words*, Encyclopedia of Math. and its Appl. **90**. Cambridge Univ. Press, Cambridge, 2002.

[135] M. Lothaire, *Applied combinatorics on words*, Encyclopedia of Math. and its Appl. **105**. Cambridge Univ. Press, Cambridge, 2005.

[136] M. Lothaire, *Applied combinatorics on words*, Encyclopedia of Math. and its Appl. **90**. Cambridge Univ. Press, Cambridge, 2011.

[137] A. de Luca, *A note on variable length codes*, Inf. Control **32** (1976), no. 3, 263–271.

[138] A. de Luca and A. Restivo, *On some properties of very pure codes*, Theor. Comput. Sci. **10** (1980), no. 2, 157–170.

[139] J.-G. Luque and J.-Y. Thibon, *Noncommutative symmetric functions associated with a code, Lazard elimination, and Witt vectors*, Discrete Math. Theor. Comput. Sci. **9** (2007), no. 2, 59–72.

[140] R. C. Lyndon and M.-P. Schützenberger, *The equation $a^m = b^n c^p$ in a free group*, Michigan Math. J. **9** (1962) no. 4, 289–298.

[141] I. G. Macdonald, *Symmetric functions and Hall polynomials*, Oxford University Press, 1995.

[142] F. J. MacWilliams and N. J. Sloane, *The theory of error correcting codes*, North-Holland, 1977.

[143] W. Magnus, A. Karrass, and D. Solitar, *Combinatorial group theory*, Dover Publ. Inc., Mineola, NY, 1976.

[144] W. Magnus, A. Karrass, and D. Solitar, *Combinatorial group theory*, 2nd ed., Dover Publ. Inc., Mineola, NY, 2004.

[145] G. S. Makanin, *On the rank of equations in four unknowns in a free semigroup*, Math. USSR-Sb. **29** (1976), no. 2, 257–280.

[146] A. Manning, *Axiom A diffeomorphisms have rational zeta functions*, Bull. London Math. Soc. **3** (1971), no. 2, 215–220.

[147] S. Mantaci and A. Restivo, *Codes and equations on trees*, Theor. Comput. Sci. **255** (2001), no. 1–2, 483–509.

[148] B. Marcus, *Factorsand extensions of full shifts*, Monatsh. Math. **88** (1979), no. 3, 239–247.

[149] A. A. Markov, *On alphabet coding*, Soviet. Phys. Dokl. **6** (1962), 553–554.

[150] R. J. McEliece, *The theory of information and coding*, Encyclopedia Math. Appl. **86** Cambridge Univ. Press, 2004.

[151] B. McMillan, *Two inequalities implied by unique decipherability*, IRE Trans. Inform. Theory **IT-2** (1956), 115–116.

[152] N. Metropolis and G.-C. Rota, *Witt vectors and the algebra of necklaces*, Adv. Math. **50** (1983), no. 2, 95–125.

[153] E. F. Moore, *Gedanken-experiments on sequential machines*, In C. E. Shannon and J. McCarthy, eds, Automata Studies, Vol. **34** of Ann. of Math. Stud., 1956, pp. 129–153.

[154] M. Nivat, *Éléments de la théorie générale des codes*, Automata theory, Academic Press, New York, (1966), pp. 278–294.

[155] M. Nivat, *Binary tree codes*, In M. Nivat and A. Podelski, editors, Tree Automata and Languages, North-Holland, (1992), pp. 1–20.

[156] Y. Perl, M. R. Garey, and S. Even, *Efficient generation of optimal prefix codes: equiprobable words using unequal cost letters*, J. Assoc. Comput. Mach. **22** (1975), no. 2, 202–214,

[157] D. Perrin, *Codes asynchrones*, Bull. Soc. Math. France, **105** (1977), 385–404.

[158] J.-F. Perrot, *Contribution Γ l'étude des monoïdes syntaxiques et de certains groupes associés aux automates finis.* Thèse d'État, Université de Paris, 1972.

[159] J.-É. Pin, *Le problème de la synchronisation et la conjecture de Černý*, PhD thesis, Université Paris 6, 1978.

[160] J.-É. Pin, *Varieties of formal languages.* Foundations of Computer Science. Plenum Publishing Corp., 1986. With a preface by M.-P. SchΓjtzenberger, Translated from the French by A. Howie

[161] V. S. Pless, W. C. Huffman, and R. A. Brualdi (eds), Handbook of coding theory, Vol. I, II. North-Holland, 1998.

[162] A. Restivo, *On a question of McNaughton and Pappert*, Inf. Control **25** (1974), no. 1, 93–101.

[163] A. Restivo, *On codes having no finite completions*, Discrete Math. **17** (1977), no. 3, 309–316.

[164] A. Restivo, *Codes and local constraints*, Theor. Comput. Sci. **72** (1990), no. 1, 55–64.

[165] A. Restivo, S. Salemi, and T. Sportelli, *Completing codes*, RAIRO Inform. Théor. Appl. 23 (1989), 135–147.

[166] Ch. Reutenauer, *Ensembles libres de chemins dans un graphe*, Bull. Soc. Math. France **114** (1986), no. 2, 135–152.

[167] Ch. Reutenauer, $\mathbb{N}$-*rationality of zeta functions*, Adv. Appl. Math. **18** (1997), no. 1, 1–17.

[168] R. F. Rice, *Some practical universal noiseless coding techniques*, Technical report, Jet Propulsion Laboratory (1979) pp. I–X, 1–119.

[169] I. Richardson, *H.264 and MPEG-4 video compression: video coding for next-generation multimedia,* Wiley, 2003.

[170] J. A. Riley, *The Sardinas/Patterson and Levenshtein theorems,* Inf. Control **10** (1967), no. 2, 120–136.

[171] M. Rodeh, *A fast test for unique decipherability based on suffix trees*, IEEE Trans. Inform. Theory **IT-28** (1982), 648–651.

[172] J. Sakarovitch, *Éléments de théorie des automates*, Vuibert Informatique, Paris, 2003.

[173] J. Sakarovitch, *Elements of automata theory*, transl. from French, Cambridge Univ. Press, Cambridge, 2009.

[174] A. Salomaa, *Jewels of formal language theory*, Computer Science Press, 1981. (Russian version in [11])

[175] D. Salomon, *Variable-length codes for data compression*, Springer, 2007.

[176] A. A. Sardinas and G. W. Patterson, *A necessary and sufficient condition for the unique decomposition of coded messages*, IRE Internat. Conv. Rec. **8** (1953), 104–108.

[177] R. A. Scholtz, *Maximal and variable length comma-free codes*, IEEE Trans. Inf. Theory **15** (1969), no. 2, 300–306.

[178] M.-P. Schützenberger, *Une théorie algébrique du codage*, Séminaire Dubreil. Algébre et théorie des nombres, **9** (1955–1956), Talk no. 15, pp. 1–24.

[179] M.-P. Schützenberger, *On an application of semi groups methods to some problems in coding*, IRE Trans. Inform. Theory **2** (1956), no. 3, 47–60.

[180] M.-P. Schützenberger, *On a special class of recurrent events*, Ann. Math. Statist. **32** (1961), no. 4, 1201–1213.

[181] M.-P. Schützenberger, *On a family of submonoids*, Publ. Math. Inst. Hung. Acad. Sci., Ser. A **6** (1961), 381–391.

[182] M.-P. Schützenberger, *A remark on finite transducers*, Inf. Control **4** (1961), no. 2–3, 185–196.

[183] M.-P. Schützenberger, *On the synchronizing properties of certain prefix codes*, Inf. Control **7** (1964), no. 1, 23–36.

[184] M.-P. Schützenberger, *On the definition of a family of automata*. Inf. Control **4** (1965), no. 2–3, 245–270.

[185] M.-P. Schützenberger, *Sur certains sous-monoïdes libres*, Bull. Soc. Math. Fr. **93** (1965), 209–223.

[186] M.-P. Schützenberger, *Sur une question concernant certains sous monoïdes libres*, C. R. Acad. Sci. Paris **261** (1965), 2419–2420.

[187] M.-P. Schützenberger, *On a question concerning certain free submonoids*, J. Comb. Theory **1** (1966), no. 4, 437–422.

[188] M.-P. Schützenberger, *On synchronizing prefix codes*, Inf. Control **11** (1967), no. 4, 396–401.

[189] C. E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J. **27** (1948), no. 3, 379–423.

[190] C. E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J. **27** (1948), no. 4, 623–666.

[191] L. W. Shapiro, *A combinatorial proof of a Chebyshev polynomial identity*, Discrete Math. **34** (1981), no. 2, 203–206.

[192] L. N. Shevrin, *On subsemigroups of free semigroups*, Soviet. Math. Dokl. **1** (1960), 892–894.

[193] H.-J. Shyr and S.-Sh. Yu, *Solid codes and disjunctive domains*, Semigroup Forum, **41** (1990), no. 1, 23–37.

[194] J.-C. Spehner, *Quelques constructions et algorithmes relatifs aux sous-monoïdes d'un monoïde libre*, Semigroup Forum, **9** (1975), no. 1, 334–353.

[195] J.-C. Spehner, *Quelques problèmes d'extension, de conjugaison et de présentation des sous-monoïdes d'un monoïde libre*, PhD thesis, Université Paris 7, 1976.

[196] R. P. Stanley, *Enumerative Combinatorics*, Vol. 1, Cambridge Stud. Adv. Math. **49**, Cambridge Univ. Press, 1986.

[197] R. P. Stanley, *Enumerative Combinatorics*, Vol. 1, Cambridge Stud. Adv. Math. **49**, Cambridge Univ. Press, 1997.

[198] L. Stryer, *Biochemistry*, Freeman, 1975.

[199] Y. Takishima, M. Wada, and H. Murakami, *Reversible variable length codes*, IEEE Trans. Commun. **43** (1995), no. 2–4, 158–162.

[200] J. Teuhola, *A compression method for clustered bit-vectors*, Inf. Process. Lett. **7** (1978), no. 6, 308–311.

[201] B. Tilson, The intersection of free submonoids is free, Semigroup Forum **4** (1972), no. 1, 345–350.

[202] B. Varn, *Optimal variable length codes (arbitrary symbol cost and equal code word probabilities)*, Inf. Control **19** (1971), 289–301.

[203] G. Viennot, *Algèbres de Lie et monoïdes libres*, PhD thesis, Université Paris 7, 1974

[204] G. Viennot, *Algèbres de Lie et monoïdes libres*, Lect. Notes Math. **691**, Springer-Verlag, 1978.

[205] Ch. Ye and R. W. Yeung, *Some basic properties of fix-free codes*, IEEE Trans. Inf. Theory **47** (2001), no. 1, 72–87.

[206] S. Yekhanin, *Improved upper bound for the redundancy of fix-free codes*, IEEE Trans. Inf. Theory **50** (2004), no. 11, 2815–2818,

[207] L. Zhang and Zh. H. Shen, *Completion of recognizable bifix codes*, Theor. Comput. Sci. **145** (1995), no. 1-2, 345–355.

Предметний покажчик

Словник-мінімум англо-українських термінів

A

accessible ∼ доступний

accessible state ∼ доступний стан (автомата)

adjacent ∼ суміжний

adjacency matrix ∼ матриця переходів (суміжності)

adjacency matrix of an automaton ∼ матриця переходів (суміжності) автомата

adjacency matrix of a graph ∼ матриця суміжності графа

admit ∼ допускати

allow ∼ вважати, видавати, визнавати, враховувати, давати, давати дозвіл, дозволяти, допускати, надавати, погоджуватися

alphabet ∼ алфавіт

alphabetic order ∼ лексикографічний (алфавітний) порядок

ambiguous ∼ неоднозначний

appropriate ∼ відповідний

approximate ∼ наближений

approximate eigenvector of a nonnegative matrix ∼ наближений власний вектор невід'ємної матриці

associated ∼ асоційованbq

associated representation ∼ асоційоване зображення

asynchronous ∼ асинхронний

asynchronous automaton ∼ асинхронний автомат

automaton ∼ автомат

average ∼ середнє, середній

average length ∼ середня довжина

B

backward ∼ обернений, напрямлений в оберненому напрямкові

backward boundary edge ∼ обернене граничне ребро

balance of an automaton ∼ баланс автомата

base ∼ база

behavior ∼ поведінка, режим, характеристики

behavior of an automaton ∼ поведінка автомата

Bernoulli distribution ∼ розподіл Бернуллі

bideterministic automaton ∼ бідетермінований автомат

bifix code ∼ біфіксний код

bifix subset ∼ біфіксна підмножина (вільного моноїда)

bijection ∼ бієкція

bijective map ∼ бієктивне відображення

bisection ∼ бісекція

biunitary ∼ біунітарний

boundary ∼ межа, край, межовий, крайовий

boundary edge ∼ граничне ребро

C

case ∼ випадок

chain ∼ ланцюг (для частково впорядкованих множин)

channel ∼ канал

channel alphabet ∼ алфавіт каналу

characteristic ∼ характеристичний

characteristic series ∼ характеристичний ряд

characterization ∼ характеристика, характеризація, описання

circular code ∼ круговий код

coaccessible state ∼ кодоступний стан (автомата)

code ∼ код

codeword ∼ кодове слово

coding morphism ∼ кодуючий морфізм, морфізм кодування

coefficient ∼ коефіцієнт

coherence ∼ когерентність

coherence condition ∼ умова когерентності

column ∼ стовпець

column of a matrix ∼ стовпець матриці

combination ∼ комбінація

companion ∼ супутник

comparable ∼ порівняльний
completable ∼ поповнювальний
completable element ∼ поповнювальний елемент
completable word ∼ поповнювальне слово
complete ∼ повний
complete automaton ∼ повний автомат
complete ordered semiring ∼ повне впорядковане напівкільце
complete semiring ∼ повне напівкільце
complete subset ∼ повна підмножина
composable codes ∼ композиційовні коди
composition ∼ композиція
comprehensive ∼ всебічний, всеосяжний
concatenation ∼ конкатенація (дописування літер або слів)
concave ∼ увігнутий
conclude ∼ завершувати, закінчувати, робити висновок
conclusion ∼ висновок
congruence ∼ конгруенція
conjecture ∼ гіпотеза
conjugacy ∼ спряженість
conjugacy class ∼ клас спряженості
conjugate ∼ спряжений
conjugate word ∼ спряжені слова
consecutive ∼ послідовний
constant term ∼ постійний терм
constrained ∼ обмежений, скутий
(p, q)**-constrained set** ∼ (p, q)-обмежена множина
context ∼ контекст
context of a word ∼ контекст слова
continuous ∼ неперервний
continuous morphism ∼ неперервний морфізм
convenience ∼ зручність
convenient ∼ зручний
converge ∼ збігатися, збіжний
coprime integers ∼ взаємно первинні цілі числа
coset of a subgroup in the group ∼ суміжний клас підгрупи в групі
cost ∼ вартість, ціна
count ∼ брати до уваги, враховувати, перелічувати
cross-section ∼ переріз, поперечний переріз
crossing ∼ перетин, перехрещення, схрещування
crossing edge ∼ ребро схрещування
cutting ∼ розрізання
cutting point ∼ точка розрізання
cycle ∼ цикл
cyclically ∼ циклічно
cyclotomic ∼ круговий, циклотомічний
cyclotomic identity ∼ циклотомічна тотожність

D
dash ∼ тире
decide ∼ визначатися, приймати рішення
deciphering ∼ дешифрування
decoding ∼ декодування
decoding function ∼ функція декодування
decompose ∼ розкладати
decomposition ∼ розклад, розбиття
deduce ∼ виводити, робити висновок
degree ∼ степінь, порядок
degree of a group of permutations ∼ порядок групи підстановок
degree of a polynomial ∼ степінь полінома (многочлена)
delay ∼ затримка, затримувати
denominator ∼ знаменник
dense ∼ щільний
dense subset ∼ щільна підмножина
derivation ∼ виведення, диференціювання, операція взяття похідної, взяття похідної
derive ∼ виводити, отримувати, брати похідну
derived ∼ похідний, виведений
descending ∼ низхідний
description ∼ опис, описання
deserve ∼ заслуговувати
deterministic automaton ∼ детермінований автомат
dihedral group ∼ діедральна група
difference ∼ відмінність
different ∼ різний
disappear ∼ зникати
discover ∼ виявляти, знаходити
discuss ∼ дискутувати, обговорювати
disjoint ∼ диз'юнктний
disjoint double factorization ∼ диз'юнктна подвійна факторизація (слова)
distinguish ∼ розрізняти, характеризувати, розпізнати
distribution ∼ розподіл
diverge ∼ розбігатися, розбіжний
double ∼ підвійний
doubly transitive permutation group ∼ подвійно транзитивна група підстановок
Dyck code ∼ код Дика
Dyck code over n **letters** ∼ код Дика над n літерами
Dyck-prime ∼ первинне число за Диком
Dyck set ∼ множина Дика

E
ease ∼ простота
edge ∼ ребро, перехід (в автоматі)
eigenvalue ∼ власне значення

eigenvector ∼ власний вектор
Elias code ∼ код Еліа
elimination ∼ ліквідація, очищення, усунення
empty word ∼ порожнє слово
encoder ∼ кодувальний пристрій, кодер, шифратор
encoding ∼ кодування, шифрування
end of a path ∼ кінець шляху
end state of a path ∼ кінцевий стан шляху (автомата)
enough ∼ достатньо, доволі
ensure ∼ гарантувати
entropy ∼ ентропія
equality ∼ рівність
equivalence ∼ еквівалентність, еквіваленція
equivalence relation ∼ відношення еквівалентності
equivalent ∼ еквівалентний
erase ∼ викреслити, викреслювати, стирати
establish ∼ стверджувати
even ∼ парний
even permutation ∼ парна підстановка
event ∼ подія
evidently ∼ очевидно
except ∼ окрім, за винятком, виключати
existence ∼ існування
expansion ∼ розширення
explain ∼ пояснювати, тлумачити
exponent ∼ показник, показник степені, степінь, порядок, екпонента
exponent of a word ∼ порядок слова
expression ∼ вираз, зображення

F

factor ∼ множник (слова)
factorization ∼ факторизація (слова)
failure function ∼ функція відмови
family ∼ сім'я
family of rational subsets of a monoid ∼ сім'я раціональних підмножин моноїда
Fibonacci automaton ∼ автомат Фібоначчі
Fibonacci number ∼ число Фібоначчі
fill ∼ заповнювати
finite automaton ∼ скінченний автомат
finite deterministic automaton ∼ скінченний детеміністичний автомат
finite transducer ∼ скінченний перетворювач
flat ∼ плоский
flat tree ∼ плоске дерево
forbidden ∼ заборонений
formal ∼ формальний
formal series ∼ формальний ряд
formal sum ∼ формальна сума
forward boundary edge ∼ пряме граничне ребро
free ∼ вільний
free commutative monoid ∼ вільний комутативний моноїд
free group ∼ вільна група
free hull ∼ вільна оболонка
free monoid ∼ вільний моноїд
free semigroup ∼ вільна напівгрупа

G

gap ∼ діра, пробіл, прогалина,
gcd ∼ найбільший спільний дільник
generating series ∼ породжуючий ряд
generator ∼ породжуючий елемент
greatest common divisor ∼ найбільший спільний дільник
Green's relations ∼ відношення Гріна
group ∼ група
group code ∼ груповий код
group induced by a group on a class ∼ група, індукована групою на клас
group of units ∼ група одиниць

H

Hadamard product ∼ добуток Адамара
height ∼ висота
hidden Markov chain ∼ прихований ланцюг Маркова
homomorphism ∼ гомоморфізм
however ∼ все-таки, однак, проте

I

ideal ∼ ідеал
idempotent ∼ ідемпотент
identity element ∼ одиничний елемент, одиниця
identity relation ∼ відношення рівності
implement ∼ реалізовувати
implementation ∼ реалізація
imprimitivity equivalence of a group ∼ еквівалентність імпримітивності групи
imprimitivity quotient of a group ∼ фактор імпримітивності групи
imprimitivity partition ∼ розбиття імпримітивності
incident ∼ інцидентний
incident edge ∼ інцидентне ребро
inclusion ∼ вкладення, занурення
inclusion conjecture ∼ гіпотеза про вкладення (для скінченного коду)
inclusion problem ∼ проблема про вкладення (для скінченного коду)
incomparable ∼ непорівняльний
incomparable elements ∼ непорівняльні елементи
incompletable ∼ непоповнювальний
incompletable word ∼ непоповнювальне слово

indecomposable ∼ нерозкладний
indecomposable code ∼ нерозкладний код
indegree ∼ порядок входу, напівпорядок входу
index ∼ індекс
index of a subgroup in a group ∼ індекс підгрупи в групі
indicator ∼ індикатор, характеристична функція
induced ∼ індукований
inequality ∼ нерівність
infix code ∼ інфіксний код
information lossless machine ∼ інформаційна машина без втрат
information lossless machine of finite order ∼ інформаційна машина без втрат скінченного порядку
initial ∼ початковий
initial part ∼ початкова частина (підмножини вільного моноїда)
initial state ∼ початковий стан (автомата)
input automaton ∼ вхідний автомат
input label ∼ вхідна мітка
input-simple transducer ∼ перетворювач з простим входом
inseparable ∼ невідокремлюваний, несепарабельний
inseparable states ∼ невідокремлювані стани
inspection ∼ інспекція, ревізія, огляд
instantaneous ∼ миттєвий
insufficient ∼ недостатній, непридатний
integer ∼ ціле число
internal ∼ внутрішній
interpretation ∼ інтерпретація, тлумачення
invertible ∼ оборотний
invertible matrix ∼ оборотна матриця
irreducible ∼ незвідний, нерозкладний
irreducible nonnegative matrix ∼ незвідна невід'ємна матриця
isomorphism ∼ ізоморфізм

K

k-approximate eigenvector of a nonnegative matrix ∼ k-наближений власний вектор невід'ємної матриці
K-rational series ∼ K-раціональний ряд
k-transitive permutation group ∼ k-транзитивна група підстановок
kernel ∼ ядро

L

label ∼ мітка, мітити
label of a path ∼ мітка шляху
leaf ∼ листок (дерева)
least upper bound ∼ точна верхня грань, супремум
leaves ∼ листя (дерева)
left ∼ лівий
left ideal ∼ лівий ідеал
left residual ∼ ліва частка (множини)
left unitary ∼ унітарний зліва
length ∼ довжина
length distribution of the set ∼ розподіл довжини множини
length of a path ∼ довжина шляху
length of a word ∼ довжина слова
letter ∼ літера, буква
lexicographic order ∼ лексикографічний порядок
linear order ∼ лінійний порядок
literal ∼ літерний
literal automaton ∼ літерний автомат (префіксного коду)
literal deciphering delay ∼ літерна затримка дешифрування
literal transducer ∼ літерний перетворювач
literal representation ∼ літерне зображення (вільного моноїда)
locally finite family ∼ локально скінченна сім'я
longer ∼ довший
lookahead ∼ дивитися вперед, переглядати

M

map ∼ відображення, відображати
mapping ∼ відображення
Markov chain ∼ ланцюг Маркова
matrices ∼ матриці
matrix ∼ матриця
maximal ∼ максимальний
maximal code over an alphabet ∼ максимальний код над алфавітом
maximal free submonoid of a free monoid ∼ максимальний вільний підмоноїд вільного моноїда
merging ∼ злиття, ототожнення, склеєння
minimal ∼ мінімальний
minimal decomposition ∼ мінімальний розклад
minimal ideal ∼ мінімальний ідеал
modulus ∼ модуль
molecule ∼ молекула
monoid ∼ моноїд
morphism ∼ морфізм
morphism recognizes a subset ∼ морфізм розпізнає підмножину
Morse code ∼ код (азбука) Морзе
Möbius function ∼ функція Мьобіуса
Möbius inversion formula ∼ формула Мьобіуса оберненого перетворення
multigraph ∼ мультиграф
multiple ∼ кратне, кратне число

mutually prime integers ~ взаємно первинні цілі числа

N

namely ~ а саме
natural number ~ натуральне число
necessarily ~ неминуче, неодмінно, обов'язково
necklace ~ намисто
neutral element ~ нейтральний елемент, одиниця
next-state function of an automaton ~ функція переходів автомата
node ~ вузол (графа)
nonnegative ~ невід'ємний
normalized weighted automaton ~ нормалізовний зважений автомат
notations ~ позначення
null relation ~ порожнє відношення, нульвідношення
number ~ число

O

occurrence ~ входження, екземпляр, поява, виникнення
occurrence of a letter ~ входження літери (в слово)
odd ~ непарний
offset ~ зміщення
operation ~ операція
order ~ порядок
ordered semiring ~ впорядковане напівкільце
ordinary ~ звичайний, ординарний
origin ~ початок, джерело
origin of a path ~ початок шляху
origin state of a path ~ початковий стан шляху (автомата)
output label ~ вихідна мітка
output ~ вихід
over ~ над

P

palindrome ~ паліндром
palindrome prime ~ паліндромний первинний елемент
palindrome word ~ паліндромне слово
parity ~ парність
parse ~ граматичний (синтаксичний) аналіз, розклад
parsing ~ робити граматичний (синтаксичний) аналіз
partial order ~ частковий порядок
partially ordered set ~ частково впорядкована множина
partition ~ розбиття
path ~ шлях
pass ~ прохід, проходити
passing ~ перехід, проходження
passing system ~ система переходу
pattern matching machine ~ машина, яка розпізнає шаблони
period ~ період
permutation ~ підстановка
permutation group ~ група підстановок
persistent ~ стійкий, постійний, стійкий
persistent event ~ постійна подія
point ~ точка
point in a word ~ точка в слові
polynomial ~ поліном, многочлен
poset ~ частково впорядкована множина
position ~ позиція, розташування, місце, розряд
positive integer ~ натуральне число відмінне від нуля
power series ~ степеневий ряд
prefix ~ префікс
prefix-closed set ~ префіксно замкнена множина
prefix code ~ префіксний код
prefix coding problem ~ задача префіксного кодування
prefix graph ~ префіксний граф (множини слів)
prefix order ~ префіксний порядок
prefix subset ~ префіксна підмножина (вільного моноїда)
preliminary ~ попередній
prime ~ первинний
prime monoid ~ первинний моноїд
primitive ~ примітивний
primitive transitive group of permutations ~ примітивна транзитивна група підстановок
primitive word ~ примітивне слово
probability distribution ~ імовірнісний розподіл
probability generating series of a set ~ породжуючий ряд ймовірностей множини (вільного моноїда)
product ~ добуток
proper ~ власний
proper factor ~ власний множник
proper prefix ~ власний префікс
prove ~ доводити

Q

quotient automaton ~ фактор-автомат

R

radius ~ радіус
radius of convergence ~ радіус збіжності (степеневого ряду)
radix order ~ розрядний порядок

rank ~ ранг
rank of a word in an automaton ~ ранг слова в автоматі
rational ~ раціональний
rational expression ~ раціональне зображення
rational fraction ~ раціональний дріб
rational number ~ раціональне число
rational operation ~ раціональна операція
rational subset of a monoid ~ раціональна підмножина моноїда
reach ~ досягти
real ~ дійсний
real number ~ дійсне число
recognize ~ впізнавати, розпізнавати, розрізняти
recognizable subset ~ розпізнавана множина
recurrent ~ рекурентний, зворотній
recurrent state ~ зворотній стан (детермінованого автомата)
reduced ~ зведений, редукований
reduced automaton ~ зведений (мінімальний) автомат
reducible ~ звідний, розкладний
reducible nonnegative matrix ~ звідна невід'ємна матриця
reduction ~ редукція (автомата на автомат)
refinement ~ уточнення, деталізація
reflexive closure of a relation ~ рефлексивне замикання відношення
regular ~ регулярний
regular $\mathscr{D}$-class ~ регулярний $\mathscr{D}$-клас
regular expression ~ регулярне зображення
regular subset ~ регулярна підмножина
regular transitive group of permutations ~ регулярна транзитивна група підстановок
relation ~ відношення
relatively prime integers ~ взаємно первинні цілі числа
remainder ~ залишок, лишок, остача, наріст
representation ~ зображення
representative ~ представник
residual ~ частка
reversal set ~ обернена множина
reversal word ~ обернене (розвернуте) слово
reversible ~ оборотний
right ~ правий
right completable element ~ поповнювальний справа елемент (в множині)
right complete subset ~ повна справа підмножина (моноїда)
right dense subset ~ щільна справа підмножина (моноїда)
right ideal ~ правий ідеал
right coset of a subgroup ~ правий суміжний клас підгрупи
right unitary ~ унітарний справа
ring ~ кільце
root ~ корінь
root of a word ~ корінь слова
row ~ рядок
row of a matrix ~ рядок матриці
rule ~ виключяти
run-length encoding ~ кодування довжин рядів
run-length limited code ~ код з обмеженням довжини запису

S

scope ~ область дії, контекст
semaphore ~ семафорний
semaphore code ~ семафорний код
semigroup ~ напівгрупа
semiring ~ напівкільце
separable ~ відокремлюваний, сепарабельний
separable states ~ відокремлювані стани
sequence ~ послідовність
series ~ ряд
set ~ множина
set of edges ~ множина переходів (автомата)
set of states ~ множина станів (автомата)
set recognized by automaton ~ множина розпізнувана автоматом
shorthand ~ стенографія
sibling ~ елемент одного рівня, "брат"
sign ~ знак
significance ~ важливість, значення
simple ~ простий
simple graph ~ простий граф
simple path ~ простий шлях
simplifying ~ спрощення
simplifying word ~ спрощуване слово
simultaneously ~ одночасно
singleton set ~ одноелементна множина
source ~ джерело
source alphabet ~ вихідний алфавіт
spectral ~ спектральний
spectral radius ~ спектральний радіус
square ~ квадрат
stabilizer ~ стабілізатор
stabilizer of a point of a set ~ стабілізатор точки множини
stabilizer of a state ~ стабілізатор стану (в автоматі)
stable submonoid ~ стійкий підмоноїд
star ~ зірка
star of an automaton ~ зірка автомата

star operation ∼ зірка-операція, $*$-операція
starting ∼ початок (слова)
state ∼ стан (автомата)
stochastic ∼ стохастичний
stochastic automaton ∼ стохастичний автомат
stochastic matrix ∼ стохастична матриця
straightforward ∼ прямий, простий
strictly ∼ строго
strongly connected automaton ∼ сильно зв'язний автомат
strongly connected graph ∼ сильно зв'язний граф
submonoid ∼ підмоноїд
subset ∼ підмножина
successful ∼ успішній, вдалий
successful path ∼ успішний шлях
successive ∼ послідовний
submonoid ∼ підмоноїд
subsemigroup ∼ піднапівгрупа
substitute ∼ заміняти, заміщати
substitution ∼ заміна
substituting ∼ заміна, заміщення
successively ∼ підряд, послідовно
suffix ∼ суфікс
suffix-closed set ∼ суфіксно замкнена множина
summable family ∼ сумовна сім'я
support ∼ носій
support of a series ∼ носій ряду
symmetric ∼ симетричний
symmetric group ∼ симетрична група
symmetric relation ∼ симетричне відношення
synchronized ∼ синхронізований
synchronized code ∼ синхронізований код
synchronizing ∼ синхронізація
synchronizing for a code ∼ синхронізація коду
syntactic monoid ∼ синтаксичний моноїд

T

target ∼ мета
telegraph channel ∼ телеграфний канал
term ∼ терм, член
terminal ∼ кінцевий
terminal state ∼ кінцевий стан
thin ∼ тонкий, худий
thin set ∼ тонка множина
total order ∼ лінійний порядок
totally ordered semiring ∼ лінійно впорядковане напівкільце
tower ∼ башта
transducer ∼ перетворювач
transient ∼ перехідний
transient event ∼ перехідна подія
transitive ∼ транзитивний
transitive permutation group ∼ транзитивна група підстановок
transition function of an automaton ∼ функція переходів автомата
transition monoid of an automaton ∼ моноїд переходів автомата
transmission ∼ передання, передача, пересилка, проходження, трансляція, трансмісія
transmit ∼ передача
transmit data ∼ передача даних
transposed ∼ транспонований
transposed matrix ∼ транспонована матриця
transposition ∼ транспозиція, підстановка
treatment ∼ трактування
trie ∼ навантажене дерево
trim ∼ впорядкований, обрізаний
trim automaton ∼ впорядкований (обрізаний) автомат
trim part of an automaton ∼ впорядкована (обрізана) частина автомата
trim weighted automaton ∼ впорядкований (обрізаний) ваговий автомат
trimmed ∼ обрізаний
triple ∼ трійка
two-sided ideal ∼ двобічний ідеал
tuple ∼ набір

U

unambiguity ∼ однозначність
unambiguous ∼ однозначний
unambiguous automaton ∼ однозначний автомат
unbordered ∼ необлямований
unbordered word ∼ необлямоване слово
unfolded ∼ розгорнутий
unfolded automatun ∼ розгорнутий автомат
uniform ∼ однорідний
uniform Bernoulli distribution ∼ однорідний розподіл Бернуллі
uniform code ∼ однорідний код
uniform word ∼ однорідне слово
uniformly ∼ однорідно
uniformly synchronized code ∼ однорідно синхронізований код
uniquely decipherable code ∼ єдино розшифрований код
unit ∼ одиниця
unitary ∼ унітаний

V

value ∼ значення
variable ∼ змінна
vector ∼ вектор
verbal ∼ вербальний, словесний

vertex ∼ вершина
vice versa ∼ навпаки

W
weakly ∼ слабко
weight ∼ вага
weighted automaton ∼ ваговий автомат
weighted cost ∼ вагова вартість (коду)
whence ∼ звідки
word ∼ слово

Z
zero ∼ нуль
zero constant term ∼ нульовий постійний терм (коефіцієнт)