Коди й автомати

Олег Гутік

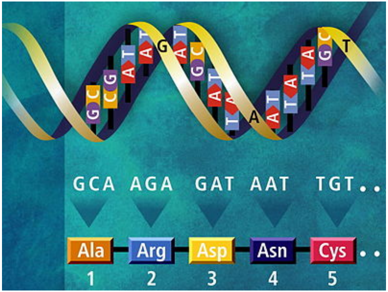
Львівський національний університет імені Івана Франка

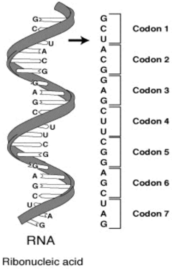
Перша зимова IT-школа DES 2020 Data Engineering and Security
28 січня 2020 р.

Теорія кодування — це вивчення властивостей кодів та їхньої придатності для специфічних задач. Коди використовуються для стиснення даних, криптографії, знаходження і виправлення помилок і від недавнього часу для мережевого кодування[en]. Коди вивчаються у теорії інформації, електротехніці, математиці і кібернетиці для створення ефективних і надійних методів перетворення даних. Це зазвичай передбачає прибирання надмірності коду та знаходження і виправлення помилок.

Генетичний код (Вікіпедія)

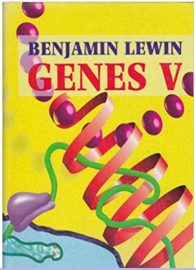
Генетичний код — певна відповідність між послідовністю нуклеотидів в молекулі ДНК (мРНК) і послідовністю амінокислот в молекулі білка, яка нею кодується. Ця система правил розташування нуклеотидів в молекулах нуклеїнових кислот (ДНК і РНК) надає всім живим організмам можливість кодування амінокислотної послідовності білків за допомогою послідовності нуклеотидів.
У ДНК використовується чотири нуклеотиди — аденін (A), гуанін (G), цитозин (C) і тимін (T), які в україномовній літературі також часто позначаються літерами А, Г, Ц і Т відповідно. Ці букви складають «алфавіт» генетичного коду. У РНК використовуються ті ж нуклеотиди, за винятком тиміну, який замінений схожим нуклеотидом, — урацилом, який позначається буквою U (або У в україномовній літературі). У молекулах ДНК і РНК нуклеотиди складають ланцюжки, а отже, інформація закодована у вигляді послідовності генетичних “літер”.

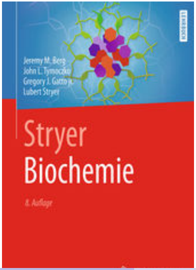


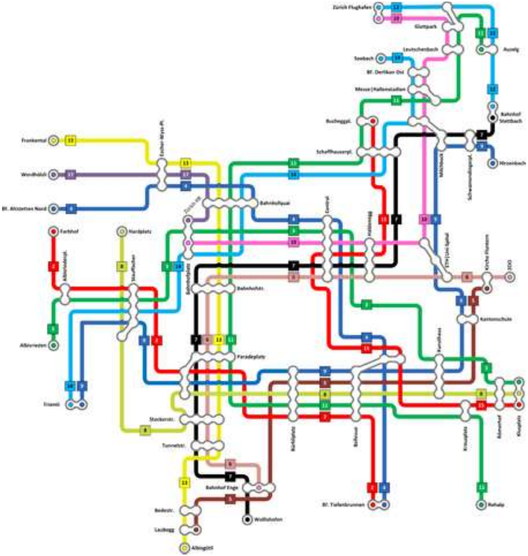


Генетичний код

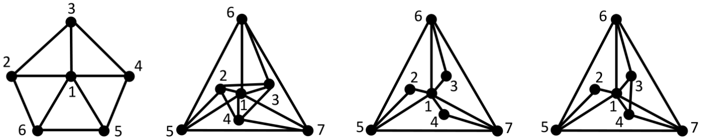
Коди без ком вперше зустрічаються статті [S.W. Golomb, D. Gordon, L.R. Welch, Comma-free codes, Can. J. Math. **10** (1958), 202–209]. Деякі математики в той час вважали, що біологічний код є кодом без ком (*гіпотеза Крика, Crick's hypothesis*). Кількість амінокислот, що появляються у білках, становить 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 з праць Нірнберга (Niernberg) виявилося, що біологічний код не є навіть кодом у сенсі алгебраїчного коду. Декілька трійок базисів можуть кодувати одну і ту ж кислоту (див. монографії [B. Lewin, Genes V, Oxford Univ. Press, 1994] або [L. Stryer, Biochemistry, Freeman, 1975]).





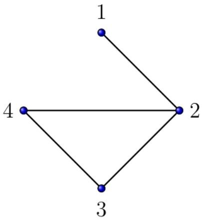


Простий граф $G = (V, E)$ називається *слово-зображуваним* (або *зображуваний словом*), якщо існує слово w над алфавітом $A(w) = V$ таке, що літери x й y чередуються в слові w тоді і лише тоді, коли $xy \in E$, тобто вершини x й y зв'язані ребром для всіх $x \neq y$. У цьому випадку ми будемо говорити, що слово w зображає граф G, і слово w називається а *словом-зображенням* для графа G.

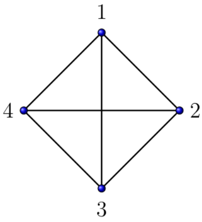


Графи на рис. не є слово-зображуваними.

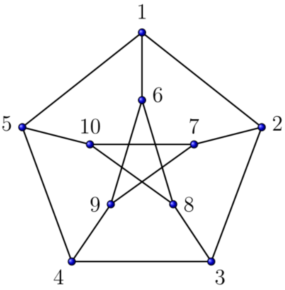
Графи, що зображаються словами



M



K_4



Граф Петерсона

Графи на рис. є слово-зображуваними. Справді, наприклад, 1213423 є словом-зображенням для графа M, 1234 – для повного графа K_4, і словом-зображенням для графа Петерсона є

$$1387296(10)7493541283(10)7685(10)194562.$$

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.

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 (обрізаною) частиною* автомата $\mathcal{A}$.

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

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 (обрізаною) частиною* автомата $\mathcal{A}$.

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

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 (обрізаною) частиною* автомата $\mathcal{A}$.

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

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

$$p \cdot uv = p \cdot u \cdot v. \tag{1}$$

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

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

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 $p \xrightarrow{a} q$.

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

$$p \cdot uv = p \cdot u \cdot v. \tag{1}$$

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

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

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

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.

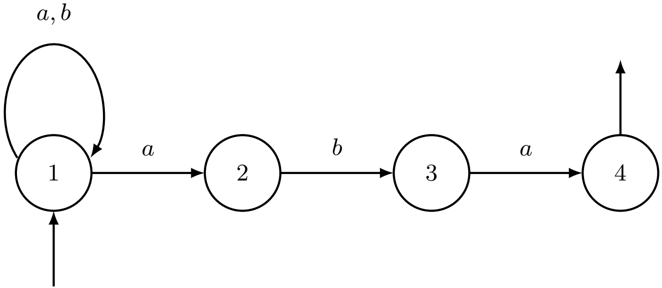


Рис.: Недетермінований автомат, який розпізнає множину слів $X = \{a, b\}^*aba$.

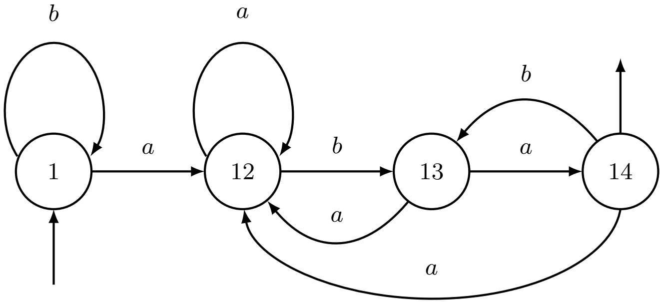


Рис.: Детермінований автомат, який розпізнає множину слів $X = \{a, b\}^*aba$.

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

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

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

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

Теорема

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.

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

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

Два стани $p, q \in Q$ називаються *невідокремлюваними*, якщо $L_p = L_q$ і *вілокремлюваними* в протилежному випадку. Детермінований автомат називається *зведеним* або *мінімальним*, якщо довільні два різні його стани є відокремлюваними.
Нехай X — підмножина вільного моноїда A^*. Синтаксичний моноїд множини X — це моноїд переходів мінімального автомата $\mathcal{A}(X)$.

Теорема

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.

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

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

Два стани $p, q \in Q$ називаються *невідокремлюваними*, якщо $L_p = L_q$ і *вілокремлюваними* в протилежному випадку. Детермінований автомат називається *зведеним* або *мінімальним*, якщо довільні два різні його стани є відокремлюваними.
Нехай X — підмножина вільного моноїда A^*. Синтаксичний моноїд множини X — це моноїд переходів мінімального автомата $\mathcal{A}(X)$.

Теорема

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.

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

$$x_1, \cdots, x_n = x'_1, \cdots, x'_m$$

випливає, що

$$n = m \qquad \text{і} \qquad x_i = x'_i \quad \text{для} \quad i = 1, \ldots, n.$$

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, порожній множина також кодом. Елемент коду іноді називається *кодовим словом*.

Приклад

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.

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

$$x_1, \cdots, x_n = x'_1, \cdots, x'_m$$

випливає, що

$$n = m \qquad \text{і} \qquad x_i = x'_i \quad \text{для} \quad i = 1, \ldots, n.$$

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, порожній множина також кодом. Елемент коду іноді називається *кодовим словом*.

Приклад

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.

Приклад

Над алфавітом, що складається з однієї літери a, непорожня підмножина вільного моноїда a^* є кодом тоді і тільки тоді, коли він є одноточковою та відмінною від одиниці 1 вільного моноїда a^*.

Приклад

Множина $X = \{aa, baa, ba\}$ над алфавітом $A = \{a, b\}$ є кодом.

Приклад

Множина $X = \{a, ab, ba\}$ над алфавітом $A = \{a, b\}$ не є кодом, оскільки слово $w = aba$ має дві різні факторизації

$$w = (ab)a = a(ba).$$

Твердження

Нехай A — алфавіт. Якщо підмножина X вільного моноїда A^* є кодом над A, то X^n є кодом над A для довільного додатного цілого числа n.

Приклад

Над алфавітом, що складається з однієї літери a, непорожня підмножина вільного моноїда a^* є кодом тоді і тільки тоді, коли він є одноточковою та відмінною від одиниці 1 вільного моноїда a^*.

Приклад

Множина $X = \{aa, baa, ba\}$ над алфавітом $A = \{a, b\}$ є кодом.

Приклад

Множина $X = \{a, ab, ba\}$ над алфавітом $A = \{a, b\}$ не є кодом, оскільки слово $w = aba$ має дві різні факторизації

$$w = (ab)a = a(ba).$$

Твердження

Нехай A — алфавіт. Якщо підмножина X вільного моноїда A^* є кодом над A, то X^n є кодом над A для довільного додатного цілого числа n.

Приклад

Над алфавітом, що складається з однієї літери a, непорожня підмножина вільного моноїда a^* є кодом тоді і тільки тоді, коли він є одноточковою та відмінною від одиниці 1 вільного моноїда a^*.

Приклад

Множина $X = \{aa, baa, ba\}$ над алфавітом $A = \{a, b\}$ є кодом.

Приклад

Множина $X = \{a, ab, ba\}$ над алфавітом $A = \{a, b\}$ не є кодом, оскільки слово $w = aba$ має дві різні факторизації

$$w = (ab)a = a(ba).$$

Твердження

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.

Приклад

Над алфавітом, що складається з однієї літери a, непорожня підмножина вільного моноїда a^* є кодом тоді і тільки тоді, коли він є одноточковою та відмінною від одиниці 1 вільного моноїда a^*.

Приклад

Множина $X = \{aa, baa, ba\}$ над алфавітом $A = \{a, b\}$ є кодом.

Приклад

Множина $X = \{a, ab, ba\}$ над алфавітом $A = \{a, b\}$ не є кодом, оскільки слово $w = aba$ має дві різні факторизації

$$w = (ab)a = a(ba).$$

Твердження

Нехай A — алфавіт. Якщо підмножина X вільного моноїда A^* є кодом над A, то X^n є кодом над A для довільного додатного цілого числа n.

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

$$x \leqslant x' \quad \Longrightarrow \quad x = x', \tag{2}$$

для всіх $x, x' \in X$, Це можна перефразувати так: довільні два різни елементи множини X є непорівняльними в префіксному порядку.

Безпосередньо з умови (2) 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

Кожна префіксна (суфіксна, біфіксна) множина слів $X \neq \{1\}$ є кодом.

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

$$x \leqslant x' \quad \Longrightarrow \quad x = x', \tag{2}$$

для всіх $x, x' \in X$, Це можна перефразувати так: довільні два різни елементи множини X є непорівняльними в префіксному порядку.

Безпосередньо з умови (2) 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

Кожна префіксна (суфіксна, біфіксна) множина слів $X \neq \{1\}$ є кодом.

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

$$x \leqslant x' \quad \Longrightarrow \quad x = x', \tag{2}$$

для всіх $x, x' \in X$, Це можна перефразувати так: довільні два різни елементи множини X є непорівняльними в префіксному порядку.

Безпосередньо з умови (2) 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

Кожна префіксна (суфіксна, біфіксна) множина слів $X \neq \{1\}$ є кодом.

Префіксним кодом (*суфіксним кодом*, *біфіксним кодом*) називається префіксна (суфіксна, біфіксна) множина слів, яка є кодом, тобто відрізняється від $\{1\}$.

Приклад

Однорідні коди є біфіксні. Множини $X = \{a, ba\}$ і $Y = \{a, ab\}$ над алфавітом $A = \{a, b\}$ є префіксним та суфіксним кодами, відповідно.

Приклад

Множини $X = a^*ba$ і $Y = \{a^n b^n : n > 0\}$ 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

Код Морзе (*азбука Морзе*) ототожнює з кожним алфавітно-цифровим символом послідовність точок і тире. Наприклад, літера А кодується "$\cdot -$", а Р кодується "$\cdot - - \cdot$". Якщо кожне кодове слово завершується додатковим символом (зазвичай пробілом, який називається "пауза"), код Морзе стає префіксним кодом.

Префіксним кодом (*суфіксним кодом*, *біфіксним кодом*) називається префіксна (суфіксна, біфіксна) множина слів, яка є кодом, тобто відрізняється від $\{1\}$.

Приклад

Однорідні коди є біфіксні. Множини $X = \{a, ba\}$ і $Y = \{a, ab\}$ над алфавітом $A = \{a, b\}$ є префіксним та суфіксним кодами, відповідно.

Приклад

Множини $X = a^*ba$ і $Y = \{a^n b^n : n > 0\}$ 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

Код Морзе (*азбука Морзе*) ототожнює з кожним алфавітно-цифровим символом послідовність точок і тире. Наприклад, літера А кодується “$\cdot -$”, а Р кодується “$\cdot - - \cdot$”. Якщо кожне кодове слово завершується додатковим символом (зазвичай пробілом, який називається “пауза”), код Морзе стає префіксним кодом.

Префіксним кодом (*суфіксним кодом*, *біфіксним кодом*) називається префіксна (суфіксна, біфіксна) множина слів, яка є кодом, тобто відрізняється від $\{1\}$.

Приклад

Однорідні коди є біфіксні. Множини $X = \{a, ba\}$ і $Y = \{a, ab\}$ над алфавітом $A = \{a, b\}$ є префіксним та суфіксним кодами, відповідно.

Приклад

Множини $X = a^*ba$ і $Y = \{a^n b^n : n > 0\}$ 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

Код Морзе (*азбука Морзе*) ототожнює з кожним алфавітно-цифровим символом послідовність точок і тире. Наприклад, літера A кодується “$\cdot -$”, а P кодується “$\cdot - - \cdot$”. Якщо кожне кодове слово завершується додатковим символом (зазвичай пробілом, який називається “пауза”), код Морзе стає префіксним кодом.

Префіксним кодом (*суфіксним кодом*, *біфіксним кодом*) називається префіксна (суфіксна, біфіксна) множина слів, яка є кодом, тобто відрізняється від $\{1\}$.

Приклад

Однорідні коди є біфіксні. Множини $X = \{a, ba\}$ і $Y = \{a, ab\}$ над алфавітом $A = \{a, b\}$ є префіксним та суфіксним кодами, відповідно.

Приклад

Множини $X = a^*ba$ і $Y = \{a^n b^n : n > 0\}$ 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

Код Морзе (*азбука Морзе*) ототожнює з кожним алфавітно-цифровим символом послідовність точок і тире. Наприклад, літера A кодується "$\cdot -$", а P кодується "$\cdot - - \cdot$". 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.

Приклад

Однорідні коди A^n є максимальними над алфавітом A.

Твердження

Кожен код X над алфавітом A міститься в максимальному коді над A.

Твердження

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.

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.

Приклад

Однорідні коди A^n є максимальними над алфавітом A.

Твердження

Кожен код X над алфавітом A міститься в максимальному коді над A.

Твердження

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.

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.

Приклад

Однорідні коди A^n є максимальними над алфавітом A.

Твердження

Кожен код X над алфавітом A міститься в максимальному коді над A.

Твердження

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.

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.

Приклад

Однорідні коди A^n є максимальними над алфавітом A.

Твердження

Кожен код X над алфавітом A міститься в максимальному коді над A.

Твердження

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.

Означення мінімального автомата

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

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

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

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

Таким чином, отримуємо, що $L_Y = Y$.
Автомат $\mathcal{A}(X)$ називається *мінімальним автоматом* підмножини X слів вільного моноїда A^*.

Означення мінімального автомата

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

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

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

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

Таким чином, отримуємо, що $L_Y = Y$.

Автомат $\mathcal{A}(X)$ називається *мінімальним автоматом* підмножини X слів вільного моноїда A^*.

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

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

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

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

Таким чином, отримуємо, що $L_Y = Y$.
Автомат $\mathcal{A}(X)$ називається *мінімальним автоматом* підмножини X слів вільного моноїда A^*.

Означення мінімального автомата

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

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

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

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

Таким чином, отримуємо, що $L_Y = Y$.

Автомат $\mathcal{A}(X)$ називається *мінімальним автоматом* підмножини X слів вільного моноїда A^*.

Означення мінімального автомата

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

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

Таким чином, отримуємо, що $L_Y = Y$.

Автомат $\mathcal{A}(X)$ називається *мінімальним автоматом* підмножини X слів вільного моноїда A^*.

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

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

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

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

Таким чином, отримуємо, що $L_Y = Y$.
Автомат $\mathcal{A}(X)$ називається *мінімальним автоматом* підмножини X слів вільного моноїда A^*.

Означення мінімального автомата

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

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

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

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

Таким чином, отримуємо, що $L_Y = Y$.

Автомат $\mathcal{A}(X)$ називається *мінімальним автоматом* підмножини X слів вільного моноїда A^*.

Означення мінімального автомата

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

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

Таким чином, отримуємо, що $L_Y = Y$.
Автомат $\mathcal{A}(X)$ називається *мінімальним автоматом* підмножини X слів вільного моноїда A^*.

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

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

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

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

Таким чином, отримуємо, що $L_Y = Y$.

Автомат $\mathcal{A}(X)$ називається *мінімальним автоматом* підмножини X слів вільного моноїда A^*.

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

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

Таким чином, отримуємо, що $L_Y = Y$.

Автомат $\mathcal{A}(X)$ називається *мінімальним автоматом* підмножини X слів вільного моноїда A^*.

Означення мінімального автомата

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

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

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

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

Таким чином, отримуємо, що $L_Y = Y$.

Автомат $\mathcal{A}(X)$ називається *мінімальним автоматом* підмножини X слів вільного моноїда A^*.

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

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

Таким чином, отримуємо, що $L_Y = Y$.

Автомат $\mathcal{A}(X)$ називається *мінімальним автоматом* підмножини X слів вільного моноїда A^*.

Твердження 1

Нехай $A \neq \varnothing$ і X — підмножина вільного моноїда A^*. Тоді такі умови є еквівалентними:

(i) множина X є префіксною;

(ii) мінімальний автомат $\mathcal{A}(X)$ або 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 $T \cdot A = \varnothing$.

Властивості

Твердження 1

Нехай $A \neq \varnothing$ і X — підмножина вільного моноїда A^*. Тоді такі умови є еквівалентними:

(i) множина X є префіксною;

(ii) мінімальний автомат $\mathcal{A}(X)$ або 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 $T \cdot A = \varnothing$.

Твердження 1

Нехай $A \neq \varnothing$ і X — підмножина вільного моноїда A^*. Тоді такі умови є еквівалентними:

(i) множина X є префіксною;

(ii) мінімальний автомат $\mathcal{A}(X)$ або 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 $T \cdot A = \varnothing$.

Твердження 1

Нехай $A \neq \varnothing$ і X — підмножина вільного моноїда A^*. Тоді такі умови є еквівалентними:

(i) множина X є префіксною;

(ii) мінімальний автомат $\mathcal{A}(X)$ або 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 $T \cdot A = \varnothing$.

Твердження 1

Нехай $A \neq \varnothing$ і X — підмножина вільного моноїда A^*. Тоді такі умови є еквівалентними:

(i) множина X є префіксною;

(ii) мінімальний автомат $\mathcal{A}(X)$ або 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 $T \cdot A = \varnothing$.

Твердження 1

Нехай $A \neq \varnothing$ і X — підмножина вільного моноїда A^*. Тоді такі умови є еквівалентними:

(i) множина X є префіксною;

(ii) мінімальний автомат $\mathcal{A}(X)$ або 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 $T \cdot A = \varnothing$.

Твердження 1

Нехай $A \neq \varnothing$ і X — підмножина вільного моноїда A^*. Тоді такі умови є еквівалентними:

(i) множина X є префіксною;

(ii) мінімальний автомат $\mathcal{A}(X)$ або 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 $T \cdot A = \varnothing$.

Властивості

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.

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.

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.

Властивості

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

$$u \cdot a = \begin{cases} ua, & \text{якщо } ua \in XA^- \cup X; \\ \varnothing, & \text{в протилежному випадку.} \end{cases}$$

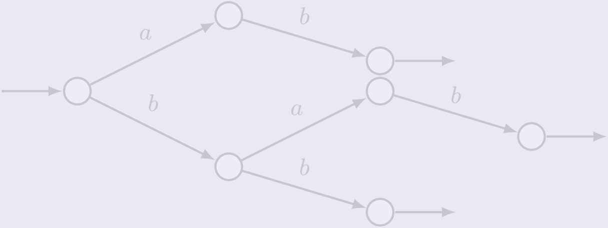
Позаяк множина $XA^- \cup X$ є префіксно замкненою, то відразу бачимо, що $1 \cdot u \in X$ тоді і тільки тоді, коли $u \in X$, тобто $L(\mathcal{A}) = X$. Наочне зображення літерного автомата відповідає, звичайно, літерному зображенню кода.

Властивості

Приклад 2

Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$. Код X має літерне зображення, яке зображене на рис.

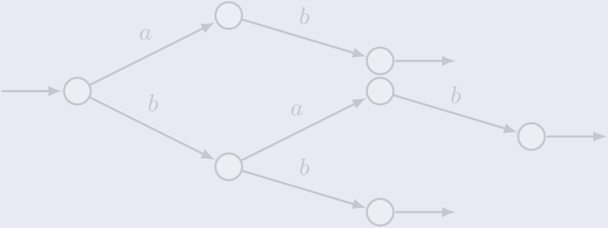
і літерний автомат, який зображений на рис.



Приклад 2

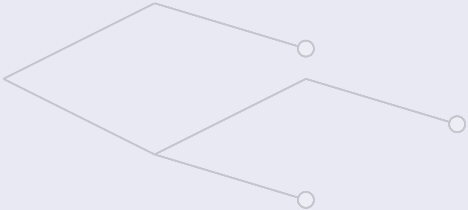
Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$. Код X має літерне зображення, яке зображене на рис.

і літерний автомат, який зображений на рис.

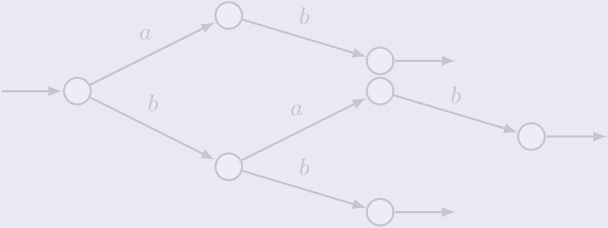


Приклад 2

Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$. Код X має літерне зображення, яке зображене на рис.

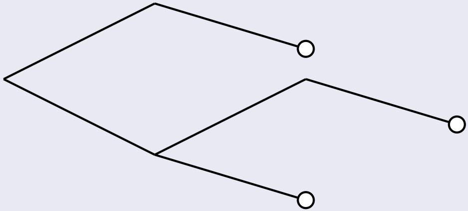


і літерний автомат, який зображений на рис.

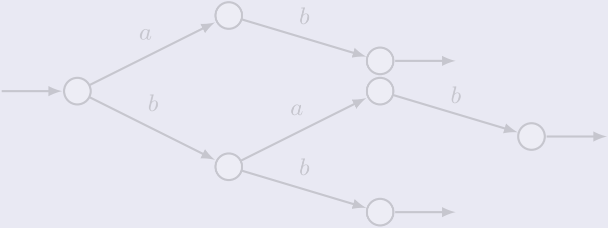


Приклад 2

Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$. Код X має літерне зображення, яке зображене на рис.

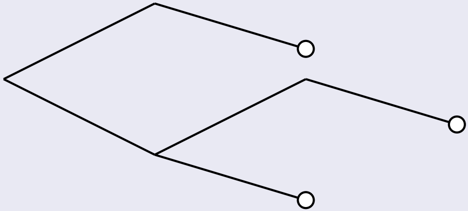


і літерний автомат, який зображений на рис.

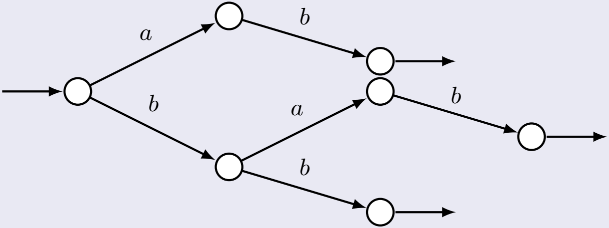


Приклад 2

Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$. Код X має літерне зображення, яке зображене на рис.



і літерний автомат, який зображений на рис.



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, 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 наступних прикладах.

Властивості

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, 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 наступних прикладах.

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, 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 наступних прикладах.

Властивості

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, 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 наступних прикладах.

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, 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 наступних прикладах.

Властивості

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, 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 наступних прикладах.

Властивості

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, 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 наступних прикладах.

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, 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 наступних прикладах.

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, 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 наступних прикладах.

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, 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 наступних прикладах.

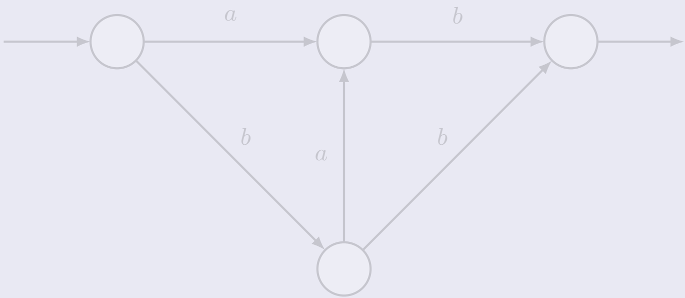
Літерний автомат $\mathcal{A}$ префіксного коду X є впорядкованим автоматом, але не є мінімальним в цілому. Для нескінченних кодів він завжди є нескінченним. Розглянемо два стани автомата $\mathcal{A}$. Еквівалентно розглянути два префікси слів з множини X, скажемо u і v, що входять в ці стани. Ці два 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, 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 наступних прикладах.

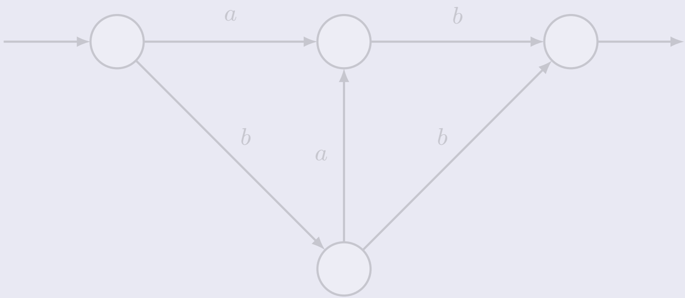
Приклад 3

Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$. 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.



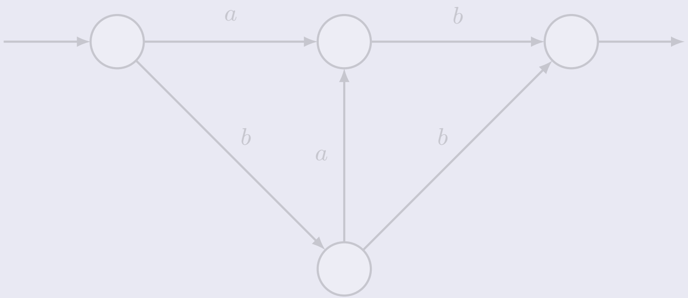
Приклад 3

Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$. 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.



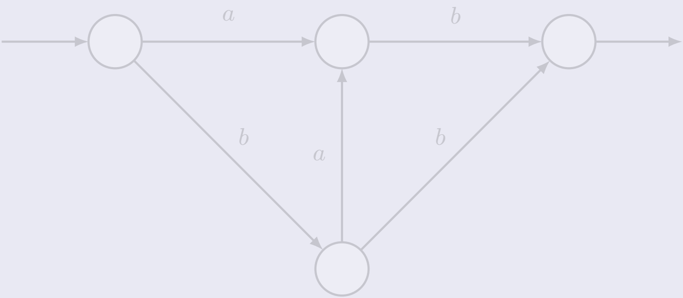
Приклад 3

Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$. 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.



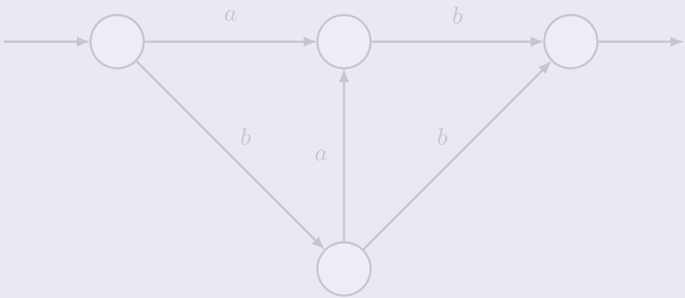
Приклад 3

Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$. 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.



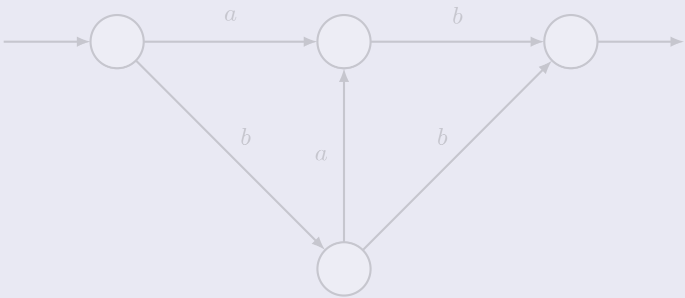
Приклад 3

Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$. 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.



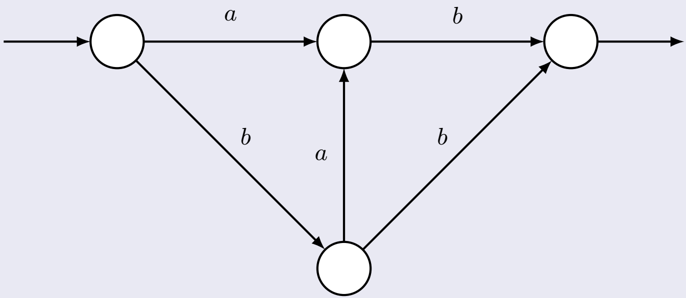
Приклад 3

Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$. 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.



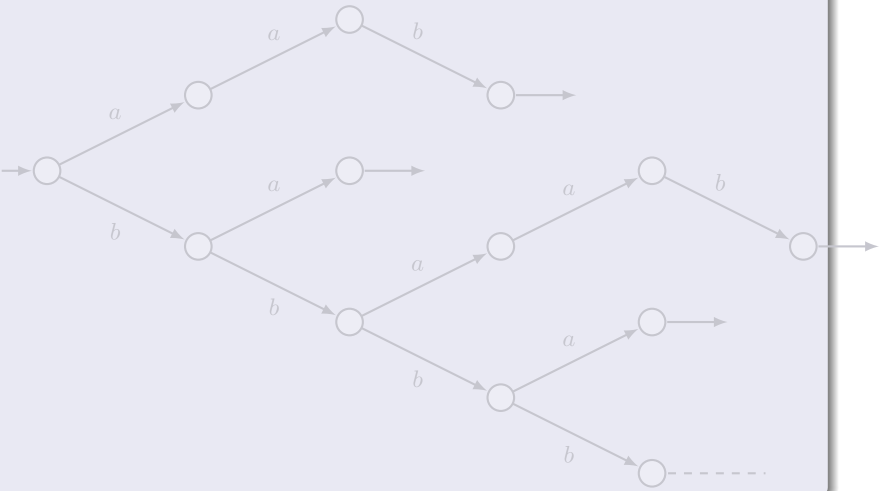
Приклад 3

Нехай $X = \{ab, bab, bb\}$ — код над алфавітом $A = \{a, b\}$. 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.



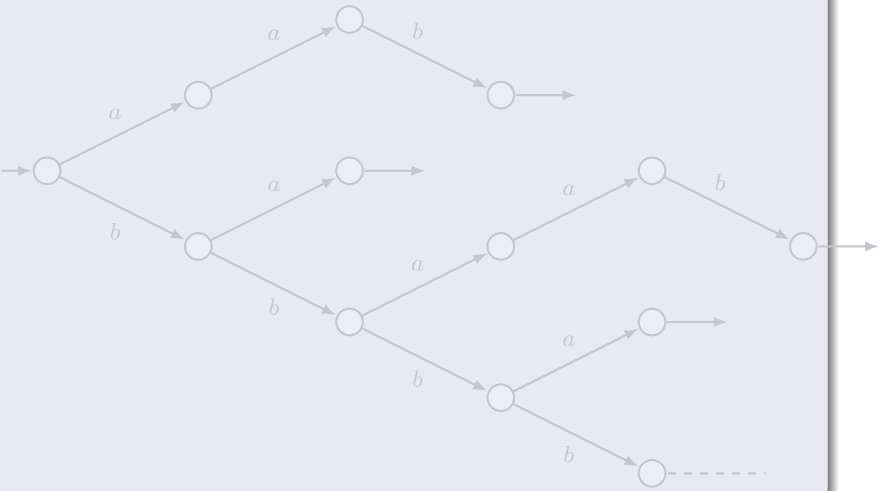
Приклад 4

Літерний автомат множини $X = (b^2)^*(a^2b \cup ba)$ зображено на рис.



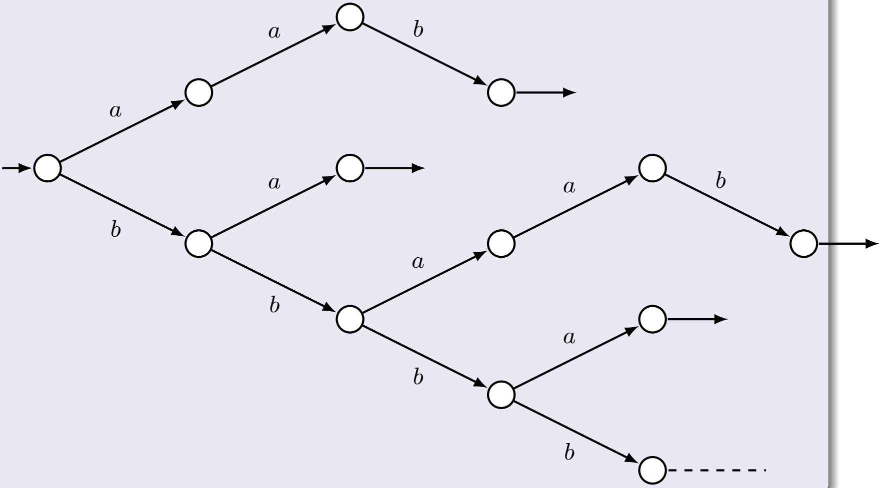
Приклад 4

Літерний автомат множини $X = (b^2)^*(a^2b \cup ba)$ зображено на рис.



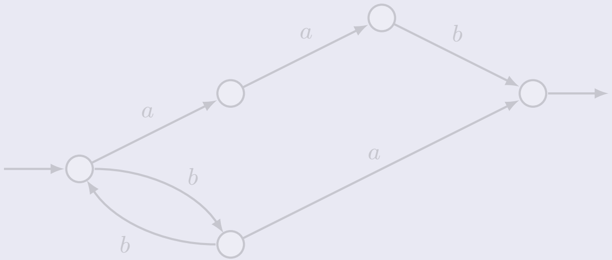
Приклад 4

Літерний автомат множини $X = (b^2)^*(a^2b \cup ba)$ зображено на рис.



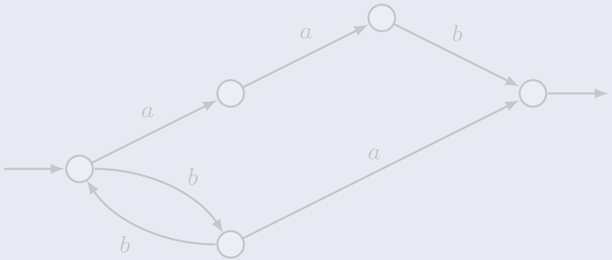
Приклад 4 (продовження)

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 коду $X = (b^2)^*(a^2b \cup ba)$ з рис.



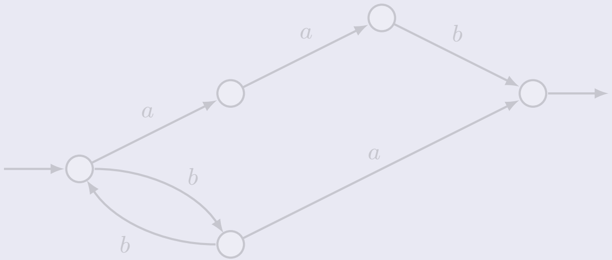
Приклад 4 (продовження)

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 коду $X = (b^2)^*(a^2b \cup ba)$ з рис.



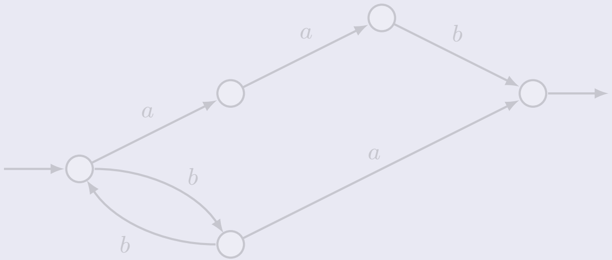
Приклад 4 (продовження)

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 коду $X = (b^2)^*(a^2b \cup ba)$ з рис.



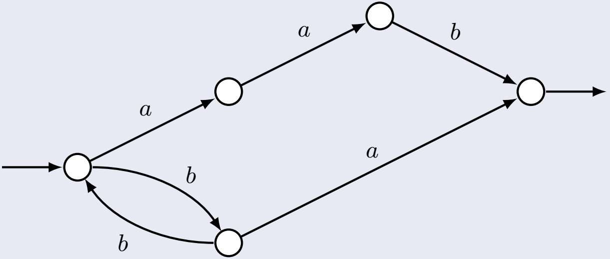
Приклад 4 (продовження)

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 коду $X = (b^2)^*(a^2b \cup ba)$ з рис.



Приклад 4 (продовження)

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 коду $X = (b^2)^*(a^2b \cup ba)$ з рис.



Підмножина P моноїда M називається *щільною* в M, якщо всі елементи множини M є поповнювальними в P, тобто P перетинає всі (двобічні) ідеали в моноїді M. Очевидно, що кожна надмножина щільної множини є щільною.

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 $MmM \cap P = \varnothing$.

Підмножина P моноїда M називається *повною* в M, якщо підмоноїд, що породжується множиною P є щільним. Кожна щільна множина також є повною.

Теорема

Кожен максимальний код є повною множиною.

Теорема

Кожен тонкий і повний код є максимальним.

Теорема

Нехай X — код над алфавітом A. Тоді X є повним тоді і лише тоді, коли X є щільним або максимальним.

Підмножина P моноїда M називається *щільною* в M, якщо всі елементи множини M є поповнювальними в P, тобто P перетинає всі (двобічні) ідеали в моноїді M. Очевидно, що кожна надмножина щільної множини є щільною.

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 $MmM \cap P = \varnothing$.

Підмножина P моноїда M називається *повною* в M, якщо підмоноїд, що породжується множиною P є щільним. Кожна щільна множина також є повною.

Теорема

Кожен максимальний код є повною множиною.

Теорема

Кожен тонкий і повний код є максимальним.

Теорема

Нехай X — код над алфавітом A. Тоді X є повним тоді і лише тоді, коли X є щільним або максимальним.

Підмножина P моноїда M називається *щільною* в M, якщо всі елементи множини M є поповнювальними в P, тобто P перетинає всі (двобічні) ідеали в моноїді M. Очевидно, що кожна надмножина щільної множини є щільною.

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 $MmM \cap P = \varnothing$.

Підмножина P моноїда M називається *повною* в M, якщо підмоноїд, що породжується множиною P є щільним. Кожна щільна множина також є повною.

Теорема

Кожен максимальний код є повною множиною.

Теорема

Кожен тонкий і повний код є максимальним.

Теорема

Нехай X — код над алфавітом A. Тоді X є повним тоді і лише тоді, коли X є щільним або максимальним.

Підмножина P моноїда M називається *щільною* в M, якщо всі елементи множини M є поповнювальними в P, тобто P перетинає всі (двобічні) ідеали в моноїді M. Очевидно, що кожна надмножина щільної множини є щільною.

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 $MmM \cap P = \varnothing$.

Підмножина P моноїда M називається *повною* в M, якщо підмоноїд, що породжується множиною P є щільним. Кожна щільна множина також є повною.

Теорема

Кожен максимальний код є повною множиною.

Теорема

Кожен тонкий і повний код є максимальним.

Теорема

Нехай X — код над алфавітом A. Тоді X є повним тоді і лише тоді, коли X є щільним або максимальним.

Підмножина P моноїда M називається *щільною* в M, якщо всі елементи множини M є поповнювальними в P, тобто P перетинає всі (двобічні) ідеали в моноїді M. Очевидно, що кожна надмножина щільної множини є щільною.
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 $MmM \cap P = \varnothing$.
Підмножина P моноїда M називається *повною* в M, якщо підмоноїд, що породжується множиною P є щільним. Кожна щільна множина також є повною.

Теорема

Кожен максимальний код є повною множиною.

Теорема

Кожен тонкий і повний код є максимальним.

Теорема

Нехай X — код над алфавітом A. Тоді X є повним тоді і лише тоді, коли X є щільним або максимальним.

Підмножина P моноїда M називається *щільною* в M, якщо всі елементи множини M є поповнювальними в P, тобто P перетинає всі (двобічні) ідеали в моноїді M. Очевидно, що кожна надмножина щільної множини є щільною.

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 $MmM \cap P = \varnothing$.

Підмножина P моноїда M називається *повною* в M, якщо підмоноїд, що породжується множиною P є щільним. Кожна щільна множина також є повною.

Теорема

Кожен максимальний код є повною множиною.

Теорема

Кожен тонкий і повний код є максимальним.

Теорема

Нехай X — код над алфавітом A. Тоді X є повним тоді і лише тоді, коли X є щільним або максимальним.

Властивості

Твердження

Кожен розпізнуваний код є тонким.

Приклад

Код $X = \{a^n b^n : n \geqslant 1\}$ є тонким (для прикладу, елемент ba не є множником коду X), але код X не є розпізнуваним.

Твердження

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.

Твердження

Кожен розпізнуваний код є тонким.

Приклад

Код $X = \{a^n b^n : n \geqslant 1\}$ є тонким (для прикладу, елемент ba не є множником коду X), але код X не є розпізнуваним.

Твердження

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.

Властивості

Твердження

Кожен розпізнуваний код є тонким.

Приклад

Код $X = \{a^n b^n : n \geqslant 1\}$ є тонким (для прикладу, елемент ba не є множником коду X), але код X не є розпізнуваним.

Твердження

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.

Ура!! Закінчилося!!!!