

УДК 512.543

MINIMAL GENERATORS SYSTEMS FOR GROUPS OF AUTOMATIC PERMUTATIONS

МІНІМАЛЬНІ СИСТЕМИ ТВІРНИХ ГРУП АВТОМАТНИХ ПІДСТАНОВОК

Sikora V.S. / Сікора В.С.

c.ph.-math..sc., doc. / к.ф.-м..н., доц.

ORCID: 0000-0002-5283-8759

*Yurij Fedkovych Chernivtsi National University, Ukraine, Chernivtsi, vul. Universytetska, 28,
58000*

*Чернівецький національний університет імені Юрія Федьковича, Україна,
Чернівці, вул. Університетська, 28, 58000*

Анотація. У статті досліджується питання побудови системи твірних для групи фінітних автоматних підстановок, доведено теорему про можливість побудови незвідної системи твірних скінченної метасиметричної групи.

Ключові слова: система твірних, група автоматних підстановок, скінченна метасиметрична група.

Вступ. Деякі початкові відомості про групи всіх автоматних підстановок над заданим алфавітом можна знайти в роботах [1–4]. Зокрема, в [3] встановлено, що їх можна конструювати з симетричних груп, використовуючи операцію вінцевого добутку, тобто при вивченні груп автоматних підстановок можна застосовувати добре розвинену теорію вінцевих добутків.

Об'єктом дослідження даної праці є питання побудови системи твірних для групи фінітних автоматних підстановок.

Постановка задачі. Допоміжні твердження. Нехай задано два автомати

$$A_1 = \langle Q_1, X_1, Y_1, \delta_1, \lambda_1 \rangle, \quad A_2 = \langle Q_2, X_2, Y_2, \delta_2, \lambda_2 \rangle$$

такі, що вхідний алфавіт другого з цих автоматів збігається з вихідним алфавітом першого (тобто, що $X_2 = Y_1$).

Означення 1 [2]. Суперпозицією $A_1 \cdot A_2$ автоматів A_1 та A_2 називається автомат $B = \langle Q, X_1, Y_2, \delta, \lambda \rangle$, множина станів Q якого збігається з добутком $Q_2 \times Q_1$ множин станів автоматів A_1 та A_2 . При цьому для довільного стану $q = (q_2, q_1) \in Q$ та довільного вхідного сигналу $x \in X_1$ автомата B значення функцій переходів та виходів автомата B визначаються зі співвідношень:

$$\delta(q, x) = (\delta_2(q_2, \lambda_1(q_1, x)), \delta_1(q_1, x)), \quad \lambda(q, x) = \lambda_2(q_2, \lambda_1(q_2, x)).$$

Лема 1 [6]. Добуток автоматних відображень є автоматним відображенням. Обернене до бієктивного автоматного відображення також є автоматним.

Дане твердження впливає з того, що суперпозицію (добуток) автоматних перетворень γ_{A_1} та γ_{A_2} , які задаються відповідно автоматами A_1 і A_2 , можна задати композицією $A_1 \cdot A_2$ цих автоматів:

$$\gamma_{A_1} \cdot \gamma_{A_2} = \gamma_{A_1 \cdot A_2}.$$

Таким чином, всі автоматні бієктивні відображення над алфавітом X утворюють групу, яку називають *групою автоматних підстановок* над алфавітом X і позначають $A(X)$. Згідно з вищенаведеним, маємо

$$A(X) \simeq \text{Aut } T(X),$$

де символом $\text{Aut } T(X)$ позначено групу автоморфізмів дерева $T(X)$.

Оскільки композиція скінченних автоматів є скінченним автоматом і обернене до скінченного автоматного перетворення також є скінченним автоматним, то всі скінченно автоматні перетворення утворюють підгрупу в групі $A(X)$, яку позначають $K(X)$. Важливу роль при дослідженнях будови групи автоматних підстановок $A(X)$ відіграє також група $F(X)$ так званих фінітарних перетворень [7].

Означення 2 [5]. Перетворення $f: X^* \rightarrow X^*$ називається фінітарним, якщо існує таке натуральне число m , що для довільного слова $\omega \in X^*$ його образ $f(\omega)$ відрізняється від ω не більше, ніж першими m літерами.

Лема 2 [5]. Кожне фінітарне перетворення є скінченно автоматним. Усі фінітарні перетворення утворюють підгрупу в групі $K(X)$ всіх скінченно автоматних підстановок, яку позначають $F(X)$.

Нехай $X^{(r)}$ — підмножина X^* , яка складається зі слів довжини точно r . Згідно з лемою 1.9 з [8], ця підмножина є інваріантною відносно перетворення $A(X)$, тобто можна розглянути групу перетворень $(A(X), X^{(r)})$. Якщо J_r —

ядро цього перетворення, то фактор-група $A^{(r)}(X) = A(X) / J_r$ діє на $X^{(r)}$ точно. Аналогічно, фактор-групи

$$K^{(r)}(X) = K(X) / J_r \cap K(X), \quad F^{(r)}(X) = F(X) / J_r \cap F(X)$$

також діють точно на $X^{(r)}$.

Лема 3. Для довільного $r \in \mathbf{N}$ мають місце рівності

$$K^{(r)}(X) = F^{(r)}(X) = A^{(r)}(X).$$

Доведення. Оскільки $F(X) \leq K(X) \leq A(X)$, то справджується включення

$$K^{(r)}(X) \leq F^{(r)}(X) \leq A^{(r)}(X). \quad (1)$$

З іншого боку, група $F(X)$ складається з усіх можливих таблиць вигляду

$$[g_1, g_2(x_1), g_3(x_1, x_2), \dots, g_k(x_1, x_2, \dots, x_{k-1}), \varepsilon, \varepsilon, \dots]$$

($k \in \mathbf{N}$). Початки довжини r таких таблиць пробігають множину всіх можливих таблиць довжини r , тобто $K^{(r)}(X) = A^{(r)}(X)$. Звідси, враховуючи включення (1), дістаємо потрібні рівності. Лему 3 доведено.

Далі, для довільного $r \in \mathbf{N}$ можна визначити природну проєкцію (епіморфізм) $\varphi_r : A^{(r+1)}(X) \rightarrow A^{(r)}(X)$, та природний мономорфізм $\psi_r : A^{(r)}(X) \rightarrow A^{(r+1)}(X)$. Тим самим задано два спектри груп: прямий $(A^{(r)}(X); \psi_r)_{r \in \mathbf{N}}$, та обернений $(A^{(r)}(X); \varphi_r)_{r \in \mathbf{N}}$. Отже, можна говорити про x граничні групи (означення див. [9]).

Лема 4. Мають місце такі співвідношення:

$$(i) \lim_{\rightarrow} (A^{(r)}(X), \psi_r) \simeq F(X);$$

$$(ii) \lim_{\leftarrow} (A^{(r)}(X), \varphi_r) \simeq A(X).$$

Доведення. (i) Група $G = \lim_{\rightarrow} (A^{(r)}(X), \psi_r)$ є граничною групою прямого спектру. Її елементами є нитки (нескінченні послідовності) вигляду $u_1 u_2 \dots u_r \dots$, де $u_1 \in A^{(1)}(X)$, $u_2 \in A^{(2)}(X), \dots$, при цьому виконується умова узгодженості, тобто

місце умова (і) із означення вінцевого добутку для r -членної послідовності. Тому умови автоматності й належності до вінцевого добутку симетричних груп підстановок на $X^{(r)}$ визначають одну і ту ж групу.

2) впливає з 1) та леми 4, оскільки існує природна проекція $\prod_{i=1}^{r+1} S(X)^{(i)}$ на

$\prod_{i=1}^r S(X)^{(i)}$, яка полягає у викреслюванні останньої координати таблиць із

$\prod_{i=1}^{r+1} S(X)^{(i)}$ і вінцевий добуток $\prod_{i=1}^{\infty} S(X)^{(i)}$ є граничною групою оберненого

спектру скінченно ітерованих вінцевих добутків з такими проекціями.

Твердження 3) впливає із наведеної Дж.Рені у [10] характеристизації скінченно автоматних перетворень, оскільки залишки таблиці природним чином відповідають залишкам перетворення в розумінні Рені.

Твердження 4) впливає безпосередньо з означення фінітарного перетворення і фінітарної таблиці.

Зауваження 1. Пункт 2) леми 5 є одним із основних результатів роботи [3], але його доведення в цій роботі є ускладненим, оскільки автор використовує інші модифікації вінцевого добутку.

На групі $A(X)$ природно вводиться метрика (див. [4, 6]). А саме, якщо перетворення із $A(X)$ задаються таблицями, то відстань між ними дорівнює η^k , де η , ($0 < \eta < 1$) — фіксоване число, а k — довжина спільного початку таблиць. Тим самим група $A(X)$ перетворюється в метричну групу і є повним метричним простором.

Лема 6. Підгрупа $F(X)$ є всюди щільною в підгрупі $A(X)$.

Доведення. Справді, кожна таблиця

$$[g_1, g_2(x_1), g_3(x_1, x_2), \dots]$$

є границею послідовності фінітарних таблиць

$$[g_1, \varepsilon, \varepsilon, \dots],$$

$$[g_1, g_2(x_1), \varepsilon, \varepsilon, \dots],$$

$$[g_1, g_2(x_1), g_3(x_1, x_2), \varepsilon, \varepsilon, \dots].$$

Звідси отримуємо, що всюди щільною в $A(X)$ буде також і підгрупа $K(X)$ (див. [7, 8]).

Основний результат. Згідно з лемою 4, група $A^{(r)}(X)$ ізоморфна вінцевому добутку r симетричних груп степеня n ($n = (X)$):

$$A^{(r)}(X) \simeq \underbrace{S_n \wr S_n \wr \dots \wr S_n}_r =: S(n, r).$$

Отже, $A^{(r)}(X)$ має степінь n^r і порядок $(n!)^{1+n+n^2+\dots+n^{r-1}}$, при цьому діє на множині слів довжини r транзитивно та імпримітивно. Для кожного цілого k ($1 \leq k \leq r$) група $A^{(r)}(X)$ містить підгрупу k -координатних таблиць, тобто таблиць вигляду $[\varepsilon, \dots, \varepsilon, g_k(x_1, x_2, \dots, x_{k-1}), \varepsilon, \dots, \varepsilon]$, яка ізоморфна n^{k-1} -му степеню симетричної групи S_n .

Розглянемо спочатку системи твірних групи $A^{(r)}(X)$, які складаються лише з координатних таблиць. Для цього в симетричній групі S_n фіксуємо деяку систему твірних $\Pi = \{\pi_1, \pi_2, \dots, \pi_s\}$ і розглянемо таблиці вигляду

$$u_r(\bar{x}_{k-1}^{0,l}, k, \pi_l) = [\varepsilon, \dots, \varepsilon, h_{k,l}(x_1, \dots, x_{k-1}), \varepsilon, \dots, \varepsilon], \quad (2)$$

в яких

$$h_{k,l}(x_1, \dots, x_{k-1}) = \begin{cases} \pi_l, & \text{якщо } (x_1, \dots, x_{k-1}) = \bar{x}_{k-1}^{0,l}, \\ \varepsilon & \text{у решті випадків} \end{cases} \quad (3)$$

де ε – одиничний елемент групи S_n , $\bar{x}_{k-1}^{0,l} = (x_{1,l}^0, \dots, x_{k-1,l}^0)$ — фіксований кортеж, $l = 1, 2, \dots, s$, $k = 1, 2, \dots, r$.

Має місце твердження.

Теорема 1. Система елементів, визначених формулами (2) та (3), є системою твірних групи $S(n, r)$ при довільному виборі кортежів $\bar{x}_k^{0,l}$ ($1 \leq k \leq r-1$, $1 \leq l \leq s$). Ця система буде незвідною тоді й тільки тоді, коли система Π буде незвідною.

Доведення. Покажемо спочатку, що система (2) є системою твірних групи

$S(n, r)$. Використаємо індукцію за r . Випадок $r=1$ – база індукції – є тривіальним. Нехай тепер при деякому $r \geq 2$ твердження теореми є правильним. Покажемо, що воно залишається правильним у випадку вінцевого добутку $S(n, r+1)$.

Кожну таблицю $u_r(\bar{x}_{k-1}^{0,l}, k, \pi_l)$ ($1 \leq k \leq r$) довжини r продовжимо до таблиці $u_{r+1}(\bar{x}_{k-1}^{0,l}, k, \pi_l)$ довжини $r+1$, дописуючи в кінці одиничну координату. Система $u_{r+1}(\bar{x}_{k-1}^{0,l}, k, \pi_l)$ породжує у вінцевому добутку $S(n, r+1)$ підгрупу всіх можливих таблиць вигляду $[a_1, a_2(x_1), \dots, a_r(\bar{x}_{r-1})]$. Тому досить переконатися, що довільна таблиця вигляду

$$[\varepsilon, \dots, \varepsilon, a_{r+1}(\bar{x}_r)] \quad (4)$$

також породжується елементами із системи (2).

Кожну таку таблицю можна розкласти на добуток елементів вигляду

$$[\varepsilon, \dots, \varepsilon, h_{r+1,l}(\bar{x}_r)], \quad (5)$$

де $h_{r+1,l}(\bar{x}_r)$ набуває неединичного значення тільки в деякій одній точці (\bar{z}_r) . Вінцевий добуток $S(n, r)$ для довільного r діє на множині кортежів транзитивно. Тому для кортежа (\bar{z}_r) при довільному l ($1 \leq l \leq s$) знайдеться підстановка $v_l \in S(n, r)$ така, що $(z_1, \dots, z_r) = (x_{1,l}^0, \dots, x_{r,l}^0)^{v_l}$. За припущенням індукції, кожна з підстановок v_l ($1 \leq l \leq s$) можна розкласти на добуток твірних із систем (2), (3). Отже, таблиця \tilde{v}_l із $S(n, r+1)$, отримана з v_l дописуванням одиничної координати, також розкладається на добуток таких твірних. Виконуючи спряження таблиці (5) за допомогою \tilde{v}_l , отримаємо:

$$\tilde{v}_l \cdot [\varepsilon, \dots, \varepsilon, h_{r+1,l}(\bar{x}_r)] \cdot \tilde{v}_l^{-1} = [\varepsilon, \dots, \varepsilon, h_{r+1,l}(\bar{x}_r^{v_l})].$$

Функція $h_{r+1,l}(\bar{x}_r^{v_l})$ набуває неединичного значення тільки в одній точці $(x_{1,l}^0, \dots, x_{r,l}^0)$. Отже, можна розкласти на добуток функцій вигляду $h_{r+1,l}(\bar{x}_r)$, які визначаються рівністю (3). Звідси випливає, що кожна таблиця вигляду (4) є добутком елементів системи (2), тобто система (2) є системою твірних групи

$S(n, r + 1)$.

Переконаємося тепер, що система (2) є незвідною. Для цього досить показати, що при виключенні з неї хоча б одного елемента, вона перестане бути системою твірних. А це дійсно так, оскільки якщо ми зафіксуємо деякі номери k, l та відкинемо твірну $u(\bar{x}_{k-1}^{0,l}, k, \pi_l)$, то таблицю

$$[\varepsilon, \dots, \varepsilon, g_k(\bar{x}_{k-1}), \varepsilon, \dots, \varepsilon],$$

де $g_k(\bar{x}_{k-1})$ має неединичне значення, що дорівнює π_l , тільки в одній точці $\bar{x}_{k-1}^{0,l}$, вже не можна буде виразити через твірні, які залишилися.

Теорему 1 доведено.

Зауваження 2. Оскільки симетрична група S_n породжується двома підстановками – такими, наприклад, будуть пари $(1, 2)$, $(1, 2, \dots, n)$ або $(1, 2, \dots, n-1)$, $(1, 2, \dots, n)$ – то група $S(n, r)$, а отже і $A^{(r)}(X)$, має незвідні системи твірних вигляду (2), які містять $2r$ підстановок.

Нагадаємо, що комутатор елементів a, b групи G визначається як $(a, b) = a \cdot b \cdot a^{-1} \cdot b^{-1}$, а підгрупа, породжена всіма комутаторами, називається *комутантом* G і позначається G' . Оскільки група G' є найменшою за включенням підгрупою такою, що фактор-група G/G' — абелева, то цю останню називають *абелізацією* групи G [7,8]. Зокрема, комутантом симетричної групи S_n є знаковмінна група A_n , тобто абелізацією S_n буде циклічна група другого порядку.

Для того, щоб описати абелізацію групи $S(n, r)$, охарактеризуємо спочатку комутант цієї групи.

Нехай $\sigma = \prod f(\bar{x}_r)$ – добуток всіх значень деякої координатної функції, взятих у певному порядку. Підстановка σ є або парною, або непарною і ця властивість не залежить від порядку множників.

Із означення оператора \prod випливає:

(і) якщо $\prod f(\bar{x}_r) \in A_n$, то для довільної таблиці $u \in S(n, r)$ маємо

$$\prod f(\bar{x}_r^u) \in A_n;$$

(ii) якщо $\prod f(\bar{x}_r) \in A_n$ та $\prod g(\bar{x}_r) \in A_n$, то

$$\prod f(\bar{x}_r)g(\bar{x}_r) \in A_n,$$

де A_n – знаковмінна група порядку n .

Теорема 2. Комутант $S'(n, r)$ містить ті й тільки ті таблиці

$$[g_1, g_2(x_1), \dots, g_r(\bar{x}_{r-1})], \quad (6)$$

для яких виконується співвідношення:

$$g_1 \in A_n, \quad \prod g_i(\bar{x}_{i-1}) \in A_n \quad (1 \leq i \leq r).$$

Доведення. Нехай U — множина таблиць вказаного вигляду (6).

Очевидно, що підгрупа $S'(n, r)$ породжується таблицями $[g, \varepsilon, \dots, \varepsilon]$, $g \in A_n$, та всеможливими комутаторами таблиць вигляду

$$u = [g_1, \dots, g_k(\bar{x}_{k-1}), \varepsilon, \dots, \varepsilon],$$

$$v = [\varepsilon, \dots, \varepsilon, g_{k+1}(\bar{x}_k), \varepsilon, \dots, \varepsilon],$$

$$1 \leq k \leq r-1.$$

Зокрема, комутатор $(u, v) \in (k+1)$ -координатною таблицею, причому його $(k+1)$ -а координата дорівнює $|(u, v)|_{k+1} = g_{k+1}(\bar{x}_k^u) \cdot g_{k+1}^{-1}(\bar{x}_k)$. Функції $g_{k+1}(\bar{x}_k^u)$ та $g_{k+1}^{-1}(\bar{x}_k)$ набувають взаємно обернених значень у точках \bar{x}_k^u та \bar{x}_k . Тому в добутку всіх значень функції $|(u, v)|_{k+1}$ буде парне число непарних множників, тобто $|(u, v)|_{k+1} \in A_n$. Отже, всі такі комутатори (u, v) містяться в U . Звідси, завдяки властивостям (i), (ii) оператора \prod отримуємо, що $S'(n, r) \subseteq U$.

З іншого боку, довільну таблицю з U можна розкласти в добуток координатних таблиць. Досить буде довести, що кожен співмножник лежить у $S'(n, r)$.

Нехай $[\varepsilon, \dots, \varepsilon, f(\bar{x}_k), \varepsilon, \dots, \varepsilon]$ – така координатна таблиця, що $\prod f(\bar{x}_k) \in A_n$.

Якщо функція $g(\bar{x}_k)$ набуває тільки двох неединичних значень, причому вони є взаємно оберненими, то існує таблиця $w \in S(n, r)$ така, що $g(x_k) = h(\bar{x}_k^w)h^{-1}(\bar{x}_k)$, де $h(\bar{x}_k)$ має тільки одне неединичне значення, яке співпадає з неединичним значенням $g(\bar{x}_k)$. Звідси одержуємо, що

$$[\varepsilon, \dots, \varepsilon, g(\bar{x}_k), \varepsilon, \dots, \varepsilon] = (w, [\varepsilon, \dots, \varepsilon, h(\bar{x}_k), \varepsilon, \dots, \varepsilon]) \in S'(n, r).$$

Якщо тепер $f(\bar{x}_k)$ набуває неединичного значення тільки в точках $\bar{x}_{k-1}^{(1)}$, $\bar{x}_{k-1}^{(2)}$, ..., $\bar{x}_{k-1}^{(s)}$, і ці значення дорівнюють $\alpha_1, \alpha_2, \dots, \alpha_s$ відповідно, тоді поклавши

$$g_i(\bar{x}_k) = \begin{cases} \alpha_i^{-1}, & \text{якщо } \bar{x}_{k-1} = \bar{x}_{k-1}^{(i)}, \\ \alpha_i, & \text{якщо } \bar{x}_{k-1} = \bar{x}_{k-1}^{(i+1)}, \\ \varepsilon & \text{в решті випадків,} \end{cases}$$

ми приходимо до рівності

$$g_{s-1} \cdot g_{s-2} \cdot \dots \cdot g_1 \cdot f = b,$$

де

$$b(\bar{x}_{k-1}) = \begin{cases} \alpha_1 \dots \alpha_s, & \text{якщо } \bar{x}_{k-1} = \bar{x}_{k-1}^{(s)}, \\ \varepsilon & \text{в решті випадків.} \end{cases}$$

Оскільки кожна з таблиць $[\varepsilon, \dots, \varepsilon, g_i(\bar{x}_{k-1}), \varepsilon, \dots, \varepsilon]$ ($1 \leq i \leq s$) і таблиця $[\varepsilon, \dots, \varepsilon, b(\bar{x}_{k-1}), \varepsilon, \dots, \varepsilon]$ належать до $S'(n, r)$, тоді й таблиця $[\varepsilon, \dots, \varepsilon, f, \varepsilon, \dots, \varepsilon]$ також належить до $S'(n, r)$. Звідси отримуємо, що $U \subseteq S'(n, r)$.

Теорему 2 доведено.

Висновки. Досліджено системи твірних груп автоматних підстановок, які діють на множині всіх слів над даним алфавітом або на множині слів довжини r ($r \in \mathbf{N}$) над цим алфавітом. Результати, одержані в роботі, можна застосувати для подальшого дослідження груп, індукованих автоматними підстановками на множині слів довжини r , а також нових серій систем твірних груп автоматних підстановок.

Abstract. The problem of construction of the system of generators for group of finitary automatic permutations is investigated. Theorem about construction of irreducible system of generators for finitary metasymmetric group is proved.

Key words: system of generators, automatic permutations, finitary metasymmetric group.

Література

1. Холл М. Теория групп. – М.: Изд-во иностр. лит., 1962. – 468 с.
2. Глушков В.М. Абстрактная теория автоматов // Успехи мат. наук. – 1961. – 16, №5. – С.3–63.

3. Заровный В.П. Автоматные подстановки и сплетения групп // Кибернетика.– 1965.– №1.– С.29–36.
4. Чекань Б., Гечеч Ф. О группе автоматных подстановок // Кибернетика.– 1965.– №1.– С.29–36.
5. Суцанський В.І. Групи автоматних підстановок // Доповіді НАН України.– 1998.– №6.– С.47–50.
6. Chillag D., Herzog M., Mann A. On the Diameter of a Graph Related to Conjugacy Classes of Groups // Bull. London Math. Soc.– 1993.– Vol.25.– P.255–262.
7. Сикора В.С., Суцанский В.И. Системы порождающих групп автоматных подстановок // Кибернетика и системный анализ.– 2000.– №3.– С.121–133.
8. Сікора В.С. Мінімальні системи твірних скінченних гіпероктаедральних, номіальних, метасиметричних та автоматних груп підстановок. Монографія.– Чернівці: Технодрук, 2018.– 168 с.
9. Курош А.Г. Теория групп.– М.: Наука, 1967.– 648 с.
10. Рэни Дж.Н. Последовательностные функции // Кибернетический сборник.– 1961.– Вып. 3.– С.142–146.

Стаття відправлена: 04.03.2021 г.

© Сікора В.С.