УДК 512.54

Федорова М. В.

ВІЛЬНІ ДОБУТКИ СКІНЧЕННИХ ГРУП, ЗАДАНІ СКІНЧЕННИМИ АВТОМАТАМИ

Побудовано нове ізоморфне занурення вільного добутку скінченної кількості скінченних груп у групу скінченних автоматів над алфавітом, кількість елементів якого дорівнює найбільшому порядку вільних співмножників. Наведено приклад ініціальних автоматів, які задають вільний добуток двох циклічних груп третього порядку.

Ключові слова: автомат, вільний добуток, пінг-понг лема.

Розглянемо алфавіт $X = \{x_1, \ldots, x_n\}$, $n > 1$. Множини слів довжини m ($m \geq 0$), всіх скінченних слів та нескінченних слів (ω-слів) над X позначимо X^m, X^* та X^ω відповідно.

Автоматом над X називається трійка даних

$$A = \langle Q, \varphi, \psi \rangle,$$

у якій Q — непорожня множина внутрішніх станів автомата A, φ та ψ — його функції переходів та виходів, які діють з $Q \times X$ у Q та X відповідно. Зокрема, скінченним автоматом є автомат зі скінченною множиною станів.

Кожен такий автомат, знаходячись у деякому стані q_0, задає перетворення множин X^* та X^ω, яке називається автоматним перетворенням. Якщо це перетворення є бієкцією, то воно називається автоматною підстановкою. Автоматна підстановка, яка визначається деяким скінченним автоматом, називається скінченно автоматною підстановкою. Усі скінченно автоматні підстановки утворюють групу відносно суперпозиції, яка позначається $FGA(X)$ і називається групою скінченних автоматів над X (деталі див. напр. у [1; 2]).

Виникає природне питання про побудову занурень тих чи інших резидуально скінченних груп, зокрема вільних добутків скінченних груп у групи скінченних автоматів. У роботі [3] А. Олійник навів конструктивне доведення існування ізоморфного занурення вільного добутку скінченного числа скінченних груп у групу скінченних автоматів над певним алфавітом.

Найбільш цікавими і компактними є такі занурення, при яких заданий вільний добуток є групою деякого автомата, тобто породжується множиною автоматних підстановок, визначених у його станах. Приклади таких занурень вільних добутків для бінарного алфавіту будували Д. Савчук та Є. Мунтян (див. Theorem 1.10.2 в [1]) для вільного добутку трьох циклічних груп порядку 2, і Д. Савчук та Я. Воробець (див. Theorem 3.1 у [4]) для m ($m \geq 4$) циклічних груп порядку 2.

Залишається відкритим питання про існування інших прикладів вільних добутків скінченних груп, що породжуються всіма автоматними підстановками, визначеними в станах деякого скінченного автомата. Окремими задачами є дослідження властивостей заданих скінченно автоматних дій вільних добутків та побудова для вільних добутків скінченно автоматних дій з певними наперед заданими властивостями (наприклад, високо транзитивних дій).

Цю роботу присвячено побудові нових прикладів скінченно автоматних дій вільних добутків скінченних груп.

Розглянемо m ($m \geq 2$) груп $G_1, \ldots, G_m$, порядки яких дорівнюють $p_1, \ldots, p_m$ відповідно, $1 \leq p_1 \leq \ldots \leq p_m$, $n = p_m > 2$. Побудуємо скінченно автоматне зображення їх вільного добутку. Для цього розглянемо ряд відомих допоміжних тверджень.

Нехай Π_i — оператор, що витирає перші i символів слова, яке або є нескінченним, або його довжина не менша за i, $i \geq 0$. Позначимо символом $\omega[k, i]$ i-тий склад довжини k слова ω.

Твердження 1 ([3]). *Підстановка π на множині X^ω є автоматною в тому і лише тому випадку, коли для довільних u і v з X^ω та натурального k з рівності*

$$u[k, 1] = v[k, 1]$$

випливає рівність

$$\pi(u)[k, 1] = \pi(v)[k, 1].$$

Також для доведення нам знадобиться узагальнена пінг-понг лема.

Твердження 2 ([3]). *Нехай G — група підстановок на множині Ω, яка породжується своїми власними підгрупами $G'_1, \ldots, G'_m$, $m \geq 2$, і порядок хоча б однієї з цих підгруп більший за 2. Якщо існують непорожні підмножини $\Omega_1, \ldots, \Omega_m$ в Ω, попарні перетини котрих тривіальні і такі, що для кожного натурального $1 \leq i, j \leq m$, $i \neq j$, виконується*

умова

$$\text{для } \omega \in \Omega_j \text{ та } g \in G_i' : \omega^g \in \Omega_i,$$

то група G розкладається у вільний добуток своїх підгруп $G_1', \ldots, G_m'$:

$$G = G_1' * \cdots * G_m'.$$

На алфавіті $X = \{x_1, \ldots, x_n\}$ задамо лінійний порядок $x_1 < \ldots < x_n$. Виділимо підмножину $X_i \subset X$, яка складається з перших p_i символів алфавіту X:

$$X_i = \{x_1, \ldots, x_{p_i}\}, \quad 1 \le i \le m.$$

Нехай зафіксована регулярна дія групи G_i на X_i. Продовжимо її на весь алфавіт X. А саме, для всіх $j > i$, $j \le m$, покладемо $g(x_j) = x_j$, $g \in G_i$. Тоді дія групи G_i на X^m матиме такий вигляд: $(x_{j_1} \ldots x_{j_m})^g = x_{j_1}^g \ldots x_{j_i}^g x_{j_i+1} \ldots x_{j_m}$.

Лема 3 ([3]). *Якщо два слова u та v довжини m над алфавітом X відрізняються l-тою буквою для деякого номера $1 \le l \le m$, то для довільної дії $g \in G_i$ слова u^g і v^g також відрізняються l-тою буквою.*

Позначимо $\overline{x_1}$ слово $x_1 \ldots x_1 \in X^m$. У X^m для $1 \le i \le m$ визначимо підмножини:

$$M_i = \{\underbrace{x \ldots x}_{i} x_1 \ldots x_1 : x \in X, x \ne x_1\}.$$

Зауваження 1. Врахуємо, що $|M_i| = p_i - 1$, $M_i \ne \varnothing$, для $i \ne j$ $M_i \cap M_j = \varnothing$, $\bar{x_1} \notin M_i$, $1 \le i, j \le m$.

Визначимо $D_i = \bigcup\limits_{j \ne i} M_j^{G_i}$, де

$$M_j^{G_i} = \{\omega^g : \omega \in M_j, g \in G_i\}, \quad 1 \le i, j \le m,$$
$$D_i = \{\overline{x_1}^{hg} : h \in G_j, g \in G_i, h \ne e_j, j \ne i\}.$$

Лема 4 ([3]). *D_i є об'єднанням орбіт визначеної вище групи G_i на множині слів довжини m над алфавітом X, $1 \le i \le m$.*

Зауваження 2. Звернемо увагу на те, що $\overline{x_1} \notin D_i$, $D_i \cap M_i = \varnothing$ для довільного $1 \le i \le m$.

Визначимо на $G_i, 1 \le i \le m$ функцію φ_i, котра кожному елементу $g \in G_i$ ставить у відповідність перетворення $\varphi_i(g)$ множини X^∞ всіх нескінченних слів над X. Для всіх $k \in \mathbb{N}$ довільне нескінченне слово $\omega \in X^\infty$ можна розглянути як добуток своїх складів довжини k:

$$\omega = \omega[k,1]\omega[k,2]\ldots$$

Як наслідок, для довільних $g \in G_i$, $u \in X^\infty$ визначимо $v = (\varphi_i(g))(u)$ таким чином:

$$v[2m,1] = u[2m,1],$$

а для всіх $j \ge 3$

$$v[m,j] = \begin{cases} (u[m,j])^g, & \text{якщо } u[m,j-2] \in D_i; \\ u[m,j], & \text{інакше.} \end{cases} \quad (1)$$

Ми задали скрізь визначене перетворення множини нескінченних слів над X. Зауважимо, що перетворення $\varphi_i(e_i)$ є тотожним.

Лема 5. *Для кожного елемента $g \in G_i$ і перетворення $\varphi_i(g)$ простору X є скінченно автоматною підстановкою над алфавітом X.*

Доведення. Розіб'ємо доведення на два етапи. Спочатку доведемо, що $\varphi_i(g)$ є автоматною, а потім — скінченно автоматною підстановкою.

Автоматність. За означенням $\varphi_i(g)$ з рівності початкових складів деякої довжини двох нескінченних слів випливає рівність складів такої ж довжини і в їх образів під дією $\varphi_i(g)$. Це означає, що $\varphi_i(g)$ задовольняє умову твердження 1. Отже, $\varphi_i(g)$ індукує перетворення множини X^*, котре позначимо також $\varphi_i(g)$:

$$(\varphi_i(g))(u) = ((\varphi_i(g))(u\omega))[|u|, 1],$$

де $u \in X^*, \omega \in X^\infty$ — довільні. Тепер для доведення взаємної однозначності перетворення $\varphi_i(g)$ на множині X^∞ досить довести ін'єктивність $\varphi_i(g)$. Оскільки $\varphi_i(g)$ зберігає довжини слів з цієї множини, перевіримо, що образи $u \in X^m$ та $v \in X^m$, $u \ne v$, під дією перетворення $\varphi_i(g)$ не можуть бути рівними. Справді, нехай найменшим номером букви, котрою відрізняються слова u та v, є l: для всіх $1 \le i \le l-1$: $u[1,i] = v[1,i]$, а $u[1,l] \ne v[1,l]$. Для довільного слова $\omega \in X^\infty$ розглянемо ω-слова $u\omega$ та $v\omega$. Склади довжини m, що містять l-ту букву цих слів, під дією $\varphi_i(g)$ одночасно або змінюються під дією g, або залишаються незмінними, а отже різними. Якщо на склад довжини m з l-тою буквою діє g, застосуємо лему 3, і ці слова також будуть відрізнятись l-тою буквою. Отже, $\varphi_i(g)$ — взаємно однозначне перетворення. За твердженням 1 перетворення $\varphi_i(g)$ є автоматною підстановкою над X.

Скінченна автоматність. Розглянемо довільне слово $u : |u| \ge 3m$. Тоді для деяких $l, j \in \mathbb{N}^0$, $l \ge 2$, $0 \le j \le m-1$ виконується

$$|u| = ml + j.$$

З визначення перетворення $\varphi_i(g)$ випливає, що її u-залишок $(\varphi_i(g))_u = (\varphi_i(g))_{\Pi_{(l-2)m}(u)}$. Оскільки $|\Pi_{(l-2)m}(u)| < 3m$ і для довільного слова u знайдеться таке слово u_1, що: $|u_1| < 3m$ і $(\varphi_i(g))_u = (\varphi_i(g))_{u_1}$, а слів довжини менше $3m$ над алфавітом X скінченна кількість, то підстановка $\varphi_i(g)$ має скінченну кількість різних залишків, а отже є скінченно автоматною.

Лема 6. *Функція φ_i є мономорфізмом з групи G_i в групу скінченно автоматних підстановок $FGA(X)$.*

Доведення. Розіб'ємо доведення на два етапи. Спочатку доведемо, що $\varphi_i(g)$ є гомоморфізмом, а потім — мономорфізмом.

Гомоморфізм. Розглянемо довільні $g_1, g_2 \in G_i$ та $u \in X^\infty$. Введемо такі позначення: $v = (\varphi_i(g_1g_2))(u)$, $\vartheta = (\varphi_i(g_1))(u)$, $\omega = (\varphi_i(g_2))(\vartheta)$. Для доведення, що $\varphi_i(g)$ є гомоморфізмом, за означенням необхідно перевірити, чи $v = \omega$. Достатньо показати, що відповідні склади довжини m цих ω-слів будуть рівними. За означенням $\varphi_i(g)$ для перших складів довжини $2m$ слів v, u, ϑ, ω можна записати такі рівності:

$$v[2m,1] = u[2m,1],$$
$$\omega[2m,1] = \vartheta[2m,1] = u[2m,1].$$

А отже $v[2m,1] = \omega[2m,1]$. Для довільного $j \geq 3$ розглянемо чотири випадки залежно від того, чи належить $(j-2)$-й склад слова u множині D_i, та яке представлення має $(j-2)$-й склад слова ϑ.

Перший випадок. Нехай $u[m, j-2] \in D_i$. Тоді за визначенням перетворення $\varphi_i(g)$ j-тий склад слова u буде змінюватися під дією g_1g_2 та g_1 для слів v та ϑ відповідно: $v[m,j] = (u[m,j])^{g_1g_2}$, $\vartheta[m,j] = (u[m,j])^{g_1}$. Припустимо, що $(j-2)$-й склад слова ϑ не змінювався: $\vartheta[m, j-2] = u[m, j-2]$. Тоді $\vartheta[m, j-2]$ також належить множині D_i і $\omega[m,j] = (\vartheta[m,j])^{g_2} = ((u[m,j])^{g_1})^{g_2} = v[m,j]$.

Другий випадок. Нехай $u[m, j-2] \in D_i$. Тоді $v[m,j] = (u[m,j])^{g_1g_2}$, $\vartheta[m,j] = (u[m,j])^{g_1}$. Припустимо, що $(j-2)$-й склад слова ϑ теж змінювався: $\vartheta[m, j-2] = (u[m, j-2])^{g_1}$. Тоді за лемою 4 склад $u[m, j-2]$ під дією g_1 залишається в об'єднанні орбіт D_i, тобто $\vartheta[m, j-2] = (u[m, j-2])^{g_1} \in D_i$ та $\omega[m,j] = (\vartheta[m,j])^{g_2} = ((u[m,j])^{g_1})^{g_2} = v[m,j]$.

Третій випадок. Нехай $u[m, j-2] \notin D_i$. Тоді за визначенням перетворення $\varphi_i(g)$ j-тий склад слова u не буде змінюватись при переході до слів v та ϑ: $v[m,j] = u[m,j]$, $\vartheta[m,j] = u[m,j]$. Припустимо, що $(j-2)$-й склад слова ϑ не змінювався: $\vartheta[m, j-2] = u[m, j-2]$. Тоді $\vartheta[m, j-2]$ теж не належить множині D_i і $\omega[m,j] = \vartheta[m,j] = u[m,j] = v[m,j]$.

Четвертий випадок. Нехай $u[m, j-2] \notin D_i$. Тоді $v[m,j] = u[m,j]$, $\vartheta[m,j] = u[m,j]$. Припустимо, що $(j-2)$-й склад слова ϑ змінювався: $\vartheta[m, j-2] = (u[m, j-2])^{g_1}$. Тоді за лемою 4 склад $u[m, j-2]$ під дією g_1 не належить D_i, тому $\omega[m,j] = \vartheta[m,j] = u[m,j] = v[m,j]$.

Отже, перетворення $\varphi_i(g)$ є гомоморфізмом.

Мономорфізм. Враховуючи, що множина D_i не порожня, з означення цього гомоморфізму випливає, що для довільного елемента $g \in G_i$, $g \neq id$, перетворення $\varphi_i(g)$ не є тотожним, тому $\varphi_i(g)$ є мономорфізмом.

Нехай G_i' — образ групи G_i під дією перетворення $\varphi_i(g)$. Застосувавши леми 5 і 6, отримаємо, що група G_i' є підгрупою групи скінченно автоматних підстановок $FGA(X)$ та $G_i' \simeq G_i$ для всіх $1 \leq i \leq m$. Позначимо G підгрупу групи $FGA(X)$, породжену підгрупами $G_1', \ldots, G_m'$.

Основним результатом є така

Теорема 7. *Група G розкладається у вільний добуток своїх підгруп $G_1', \ldots, G_m'$:*

$$G = G_1' * \cdots * G_m'.$$

Доведення. Застосуємо твердження 2. Нехай G діє на множині $\Omega = X^\infty$. Визначимо підмножини $\Omega_i, 1 \leq i \leq m$, множини Ω таким чином: $\omega = \omega[m,1]\omega[m,2]\omega[m,3]\ldots \in \Omega_i$ тоді і тільки тоді, коли існує номер $j \in \mathbb{N}$ такий, що склад $\omega[m,j] \in M_i$, склад $\omega[m,j+1]$ — довільний над X, а для всіх наступних номерів $l > j+1$ виконується рівність $\omega[m,l] = \bar{x_1}$. Розглянемо довільні $1 \leq i, j \leq m$. Враховуючи зауваження 1, можемо стверджувати, що $\Omega_i \neq \varnothing$, $\Omega_i \cap \Omega_j = \varnothing$, $i \neq j$. У групі G_i оберемо довільний елемент g, $g \neq id$, а в множині Ω_j довільне ω-слово ω. Доведемо, що $v = (\varphi_i(g))(\omega) \in \Omega_i$. Оскільки $\omega \in \Omega_j$, то існує натуральне r таке, що склад $\omega[m,r] \in M_j$, а для всіх наступних номерів $l > r$ виконується рівність $\omega[m,r] = \bar{x_1}$. За визначенням D_i виконується включення $M_j \in D_i$. Отже, $\omega[m,r] \in D_i$. Враховуючи зауваження 2, $\omega[m,l] \notin D_i$ для всіх номерів l більших за r. За означенням множини M_i та перетворення φ_i можемо записати, що $v[m,r+2] = (\omega[m,r+2])^g = \bar{x_1}^g \in M_i$, а для всіх номерів $l > r+2$ виконується $v[m,l] = \omega[m,l] = \bar{x_1}$.

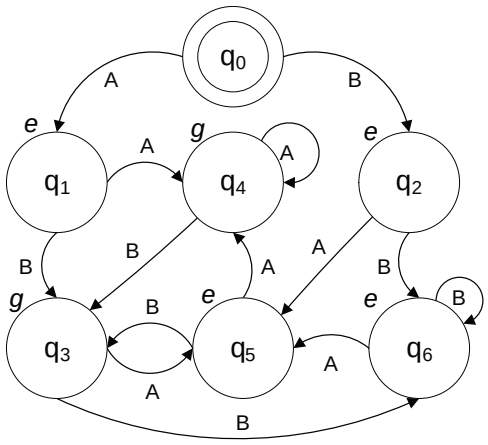

Рис. 1. Автомат, що задає твірні вільного добутку двох циклічних груп третього порядку

Отже, ω-слово v належить Ω_i. Застосувавши твердження 2, завершимо доведення теореми.

Приклад 1. Розглянемо вільний добуток двох циклічних груп третього порядку. Для такого добутку, як і вище, побудуємо множини M_i та D_i, $1 \leq i \leq 2$, які вважатимемо підмножинами алфавіту

$$X = \{0 = 00; 1 = 01; 2 = 02; 3 = 10; \\ 4 = 11; 5 = 12; 6 = 20; 7 = 21; 8 = 22\}.$$

Тоді твірні вільного добутку двох циклічних груп $C_3 * C_3$ можна задати за допомогою двох автоматів (рис. 1), для котрих функції переходів та виходів визначаються залежно від вибору множин M_i та D_i. А саме: для першого твірного ми використовуємо позначення A для множини D_1, позначення B — для множини $X \backslash D_1$, позначення g — для дії підстановки $\pi = (0, 1, 2)$ на перший символ у поточному складі. Для другого твірного ми використовуємо позначення таким чином: $A = D_2$, $B = x \backslash D_2$, g — дія підстановки $\pi = (0, 1, 2)$ на кожен символ у поточному складі.

Список літератури

1. Nekrashevych V. V. Self-similar groups / V. V. Nekrashevych. — Vienna, Chapman : Amer. Math. Soc., Providence, ROI, 2005. — 231+xi p.
2. Григорчук Р. И. Автоматы, динамические системы и группы / Р. И. Григорчук, В. В. Некрашевич, В. И. Сущанский // Труды мат. института им. Стеклова. — М. : МАИК «Наука/ Интерпериодика», 2000. — С. 134–214.
3. Олийнык А. С. Свободные произведения конечных групп и группы конечно автоматных подстановок / А. С. Олийнык // Труды мат. института им. Стеклова. — М. : МАИК «Наука/ Интерпериодика», 2000. — С. 323–331.
4. Savchuk D. Automata generating free products of groups of order 2 / D. Savchuk, Y. Vorobets // Journal of Algebra. — 2011. — Vol. 336, no. 1. — P. 53–66.

M. Fedorova

FREE PRODUCTS OF FINITE GROUPS DEFINED BY FINITE AUTOMATA

It is constructed new isomorphic embedding of the free product of finite number of finite groups into the group of finite automata over the alphabet which number of elements equals to the largest order of free multipliers. The example of initial automata defining the free product of two cyclic groups of order three is presented.

Keywords: automaton, free product, ping-pong lemma.

Матеріал надійшов 15.09.2014