УДК 512.54

А. В. Руссєв

ПРО СКІНЧЕННІ ТА АБЕЛЕВІ ГРУПИ, ПОРОДЖЕНІ СКІНЧЕННИМИ АВТОМАТАМИ

A. V. Russyev. *On finite and Abelian groups generated by finite automata*, Matematychni Studii, **24** (2005) 139–146.

We present a sufficient condition for finiteness of groups generated by a finite automaton. We provide a criterion when a group generated by a finite automaton over two-letter alphabet is Abelian.

А. В. Руссев. *О конечных и абелевых группах, порожденных конечными автоматами* // Математичні Студії. – 2005. – Т.24, №2. – С.139–146.

Приведено достаточное условие конечности группы, порожденной конечным автоматом. Дан критерий абелевости группы, порожденной конечным автоматом над двухэлементным алфавитом.

1. Вступ. В останні десятиріччя теорія автоматів отримала численні застосування в алгебраїчних дослідженнях. У статті [1] В. М. Глушков запропонував використовувати автомати-транслятори над скінченним алфавітом для визначення груп підстановок з тими чи іншими властивостями. А саме, зафіксувавши певний стан такого автомату над алфавітом X, одержимо деяке перетворення (чи підстановку) множини всіх слів над X. Тоді напівгрупою (яка в деяких випадках може бути і групою), породженою цим автоматом, назвемо напівгрупу перетворень, породжену всіма такими перетвореннями. Користуючись цим способом визначення груп, різні автори будували, зокрема, приклади нескінченних скінченно породжених груп, груп проміжного росту та інші цікаві приклади груп; було охарактеризовано всі групи, які можна породити двостановим автоматом над двоелементним алфавітом (див. статтю [2] і список літератури у ній). Досліджувались напівгрупи, породжені двостановими автоматами над двоелементним алфавітом (див., напр. [3]).

У даній статті дається достатня умова скінченності групи, визначеної скінченним автоматом над скінченним алфавітом. Доведено, що ця умова не є необхідною, причому ідея побудови контрприкладу у випадку двоелементного алфавіту належить Д. Савчуку, за що автор висловлює йому свою подяку.

Також охарактеризовано скінченні абелеві групи, породжені скінченними автоматами над двоелементним алфавітом. Наводиться критерій, коли група, породжена скінченним автоматом над двоелементним алфавітом, є абелевою.

2. Означення та допоміжні твердження. Зафіксуємо деяку непорожню скінченну множину X, яку називатимемо алфавітом.

2000 *Mathematics Subject Classification:* 20F99, 68Q70.

Означення 1. *Автоматом* над алфавітом X називається набір $A = \langle X, Q, \varphi, \lambda\rangle$, де Q — множина внутрішніх станів автомату, $\varphi\colon X \times Q \to Q$ — функція переходів, $\lambda\colon X \times Q \to X$ — функція виходів.

Нехай $A = \langle X, Q, \varphi, \lambda\rangle$ — деякий автомат.

Означення 2. *Потужністю автомату* A називається потужність множини його внутрішніх станів; для скінченного автомату A приймемо $|A| := |Q|$.

Позначимо $X^* := \bigcup_{n\geq 1} X^n \cup \{\Lambda\}$, де Λ — порожнє слово, та визначимо відображення $\varphi\colon X^* \times Q \to Q$ та $\lambda\colon X^* \times Q \to X^*$ за правилом: для $q \in Q$, $w \in X^*$ та $x \in X$

$$\begin{aligned} \varphi(wx, q) &= \varphi(x, \varphi(w, q)), & \varphi(\Lambda, q) &= q, \\ \lambda(wx, q) &= \lambda(w, q)\lambda(x, \varphi(w, q)), & \lambda(\Lambda, q) &= \Lambda, \end{aligned}$$

звідки легко отримати, що для всіх $w_1, w_2 \in X^*$ та для всіх $q \in Q$

$$\varphi(w_1 w_2, q) = \varphi(w_2, \varphi(w_1, q)), \tag{1}$$
$$\lambda(w_1 w_2, q) = \lambda(w_1, q)\lambda(w_2, \varphi(w_1, q)). \tag{2}$$

Кожному стану $q \in Q$ відповідають відображення $\pi_q := \lambda(\cdot, q)\colon X \to X$ та $f_q := \lambda(\cdot, q)\colon X^* \to X^*$. Відображення f_q можна розглядати як відображення X^ω — множини нескінченних слів $x_1x_2x_3\ldots$ в себе, де $x_1, x_2, \ldots \in X$. Причому $f_q(x_1x_2\ldots) = y_1y_2\ldots$, якщо $f_q(x_1x_2\ldots x_k) = y_1y_2\ldots y_k$ для кожного $k \in \mathbb{N}$.

Означення 3. Нехай $q_0 \in Q$. Стан $q \in Q$ називається *досяжним* зі стану q_0, якщо існує слово $w \in X^*$ таке, що $\varphi(w, q_0) = q$.

Твердження 1. *Нехай $q_0 \in Q$ та для довільного q досяжного з q_0 відображення π_q є перестановкою на X. Тоді f_{q_0} є бієкцією.*

Доведення. Доведемо, що f_{q_0} — ін'єкція. Припустимо, що для деяких $w_1, w_2 \in X^*$, $w_1 \neq w_2$ справджується рівність $f_{q_0}(w_1) = f_{q_0}(w_2)$. Нехай $w_1 = uxu_1$, $w_2 = uyu_2$, де $u, u_1, u_2 \in X^*$, $x, y \in X$, $x \neq y$. З рівності (2) випливає, що $\pi_q(x) = \pi_q(y)$, де $q = \varphi(u, q_0)$. Останнє суперечить умові. Отже, f_{q_0} — ін'єкція. Нехай $u = y_1y_2y_3\ldots y_n \in X^*$ — деяке слово. Побудуємо слово $w \in X^*$ таке, що $f_{q_0}(w) = u$. $f_{q_0}(\Lambda) = \Lambda$. Нехай $w_k = x_1x_2\ldots x_k \in X^*$ таке, що $f_{q_0}(w_k) = y_1y_2\ldots y_k$. За умою ми можемо вибрати літеру $x_{k+1} \in X$ так, що $\pi_q(x_{k+1}) = y_{k+1}$, де $q = \varphi(w_k, q_0)$. Тоді з рівності (2) випливає, що для слова $w_{k+1} = w_kx_{k+1}$ виконується $f_{q_0}(w_{k+1}) = y_1y_2\ldots y_{k+1}$. Отже, слово $w = w_n$ є шуканим словом. □

Означення 4. Автомат A називається *груповим*, якщо для кожного $q \in Q$ відображення π_q є бієкцією.

Означення 5. *Групою, породженою груповим автоматом* A, називається група підстановок множини X^ω, породжена функціями $f_q\colon X^\omega \to X^\omega$, де q пробігає всі стани з Q.

Означення 6. Автомат A називається *мінімізованим*, якщо відображення f_{q_1} та f_{q_2} різні для довільних двох різних станів $q_1, q_2 \in Q$.

Твердження 2. *Для групового автомату $A_1 = \langle X, Q_1, \varphi_1, \lambda_1\rangle$ існує мінімізований автомат A_2, що породжує ту ж саму групу, що й A_1.*

Доведення. На множині Q_1 визначимо відношення еквівалентності: $q_1 \sim q_2$, якщо $f_{q_1} = f_{q_2}$. Побудуємо відображення $i : Q_1 \to Q_1$, яке для кожного елемента з класу еквівалентності ставитиме у відповідність фіксованого для цього класу представника. Позначимо $Q_2 = i(Q_1)$. Нехай функція λ_2 є звуженням функції λ_1 на множину $X \times Q_2$. Функцію φ_2 визначимо за правилом $\varphi_2(x, q) = i(\varphi_1(x, q))$ для $x \in X$ та $q \in Q_2$. Отже, визначено автомат $A_2 = \langle X, Q_2, \varphi_2, \lambda_2\rangle$, що задовольняє умову: для кожного $q \in Q_1$ відображення $f_q = f_{i(q)}$, де $f_{i(q)}$ — відображення визначене автоматом A_2. Справді, $q \sim i(q)$, а тому $\lambda_1(\cdot, q) = \lambda_1(\cdot, i(q)) = \lambda_2(\cdot, i(q))$, та з умови $q_1 \sim q_2$ випливає $\varphi_1(\cdot, q_1) \sim \varphi_1(\cdot, q_2) \sim i(\varphi_1(\cdot, q_2)) = \varphi_2(\cdot, q_2)$ для $q_1 \in Q_1$ та $q_2 \in Q_2$. Отже, автомати A_1 та A_2 породжують одну і ту ж групу. Автомат A_2 є мінімізованим за побудовою. □

Нехай $A_1 = \langle X, Q_1, \varphi_1, \lambda_1\rangle$ та $A_2 = \langle X, Q_2, \varphi_2, \lambda_2\rangle$ — деякі автомати.

Означення 7. *Добутком автоматів A_1 та A_2* називається автомат $A = \langle X, Q, \varphi, \lambda\rangle$, де $Q = Q_1 \times Q_2$ та

$$\varphi(x, (q_1, q_2)) = (\varphi_1(x, q_1), \varphi_2(\lambda_1(x, q_1), q_2)), \quad \lambda(x, (q_1, q_2)) = \lambda_2(\lambda_1(x, q_1), q_2).$$

З означення випливає, що $f_{(q_1,q_2)} = f_{q_2}(f_{q_1}) = f_{q_1} \cdot f_{q_2}$ для $(q_1, q_2) \in Q_1 \times Q_2$. Далі розглядатимемо мінімізований добуток автоматів A_1 і A_2, тобто мінімізований автомат отриманий з добутку $A_1 \cdot A_2$ за допомогою процедури, описаної в доведенні твердження 2. Мінімізований добуток автоматів A_1 і A_2 також позначатимемо $A_1 \cdot A_2$. Надалі важатимемо, що автомат $A_1 \cdot A_2$ — мінімізований добуток автоматів A_1 та A_2.

Твердження 3. *Нехай A_1 та A_2 — мінімізовані групові автомати. Тоді для потужності добутку правильна нерівність $|A_1 \cdot A_2| \geq \max\{|A_1|, |A_2|\}$.*

Доведення. Нехай $q_2 \in Q_2$. Тоді для довільних $q_1', q_1'' \in Q_1$ умови $f_{(q_1',q_2)} \neq f_{(q_1'',q_2)}$ та $f_{q_1'} \neq f_{q_1''}$ еквівалентні. Звідки $|A_1 \cdot A_2| \geq |A_1|$. Подібно доводимо нерівність $|A_1 \cdot A_2| \geq |A_2|$. □

Теорема 1. *Нехай A — мінімізований автомат над алфавітом X такий, що $|A^2| = |A|$. Тоді для довільного $k \in \mathbb{N}$ виконується $|A^k| = |A|$.*

Доведення. Нехай $q_0 \in Q$ — фіксований стан автомату A. Тоді відображення $f_{(q_0,q)}$ попарно різні для $q \in Q$. З умови випливає, що для всіх $q_1, q_2 \in Q$ існує стан $q \in Q$ такий, що $f_{q_1} \cdot f_{q_2} = f_{(q_1,q_2)} = f_{(q_0,q)} = f_{q_0} \cdot f_q$. Розглянемо автомат A^4 та задане його станом відображення $f_{(q_1,q_2,q_3,q_4)}$, де $q_1, q_2, q_3, q_4 \in Q$, для якого за наведеною вище властивістю маємо $f_{(q_1,q_2,q_3,q_4)} = f_{q_1} \cdot f_{q_2} \cdot f_{q_3} \cdot f_{q_4} = f_{q_0} \cdot f_{q_2'} \cdot f_{q_3} \cdot f_{q_4} = f_{q_0} \cdot f_{q_0} \cdot f_{q_3'} \cdot f_{q_4} = f_{q_0} \cdot f_{q_0} \cdot f_{q_0} \cdot f_{q_4'} = f_{(q_0,q_0,q_0,q_4')}$, де $q_2', q_3', q_4' \in Q$ — деякі стани автомату A. Отже, $|A^4| = |A|$.

Нехай $|A| = |A^2| = \ldots = |A^{2^m}|$. Тоді, застосовуючи доведене до автомату $A^{2^{m-1}}$, маємо $|A^{2^{m+1}}| = |(A^{2^{m-1}})^4| = |A^{2^{m-1}}| = |A|$. Звідси отримуємо рівність $|A| = |A^2| = \ldots = |A^{2^m}| = \ldots$ Оберемо m так, щоб виконувалась нерівність $2^{m-1} \leq k < 2^m$. За твердженням 3 маємо нерівності $|A^k| = |A^{2^{m-1}} \cdot A^{k-2^{m-1}}| \geq |A^{2^{m-1}}| = |A|$ та $|A| = |A^{2^m}| = |A^k \cdot A^{2^m-k}| \geq |A^k|$, звідки випливає $|A^k| = |A|$. Тут під автоматом A^0 розуміємо автомат, який містить один стан, що задає тотожнє відображення. □

Наслідок 1. *Якщо додатково A містить стан $q_0 \in Q$ такий, що порядок f_{q_0} скінченний, то автомат A породжує скінченну групу.*

Доведення. З умов теореми випливає, що для довільних $q_1, q_2 \in Q$ існують стани q_1^*, q_2^*, q_3^*, $q_4^* \in Q$ такі, що:

$$f_{q_1} \cdot f_{q_2} = f_{q_0} \cdot f_{q_1^*}, \qquad f_{q_1} \cdot f_{q_2} = f_{q_0} \cdot f_{q_1^*};$$
$$f_{q_2} \cdot f_{q_4^*} = f_{q_1} \cdot f_{q_0}, \qquad f_{q_1}^{-1} \cdot f_{q_2} = f_{q_0} \cdot f_{q_4^*}^{-1};$$
$$f_{q_0} \cdot f_{q_1} = f_{q_3^*} \cdot f_{q_2}, \qquad f_{q_1} \cdot f_{q_2}^{-1} = f_{q_0}^{-1} \cdot f_{q_3^*};$$
$$f_{q_2} \cdot f_{q_1} = f_{q_2^*} \cdot f_{q_0}, \qquad f_{q_1}^{-1} \cdot f_{q_2}^{-1} = f_{q_0}^{-1} \cdot f_{q_2^*}^{-1}.$$

Отже, довільний добуток двох твірних або обернених до них можна подати у вигляді $f_{q_0}^{\pm 1} \cdot f_q^{\pm 1}$ для деякого $q \in Q$. Звідси випливає, що довільний скінченний добуток твірних або обернених до них можна подати у вигляді $f_{q_0}^m \cdot f_q^{\pm 1}$, де $m \in \mathbb{Z}$ — деяке ціле число, а $q \in Q$ — деякий стан. Якщо порядок f_{q_0} дорівнює n, то кількість елементів в групі, породженій автоматом A, не перевищує $2n|A| < \infty$. □

3. Достатня умова скінченності групи, породженої автоматом. Нехай $A = \langle X, Q, \varphi, \lambda \rangle$ та $A_* = \langle X, Q_*, \varphi_*, \lambda_* \rangle$ — автомати над алфавітом X.

Означення 8. Говоритимемо, що автомат A_* містить автомат A ($A_* \supset A$), якщо існує відображення $i : Q \to Q_*$ таке, що для кожного $q \in Q$ виконуються рівності $\varphi_*(\cdot, i(q)) = i(\varphi(\cdot, q))$ та $\lambda_*(\cdot, i(q)) = \lambda(\cdot, q)$.

Надалі для $A \subset A_*$ вважатимемо, що $Q \subset Q_*$ та i — тотожнє відображення. Нам будуть потрібні наступні леми.

Лема 1. *Нехай $A_* \supset A$ та $\varphi_*(x, q) \in Q$ для кожних літери $x \in X$ та стану $q \in Q_* \setminus Q$. Тоді автомат A породжує скінченну групу тоді і тільки тоді, коли автомат A_* породжує скінченну групу.*

Доведення. Нехай автомати A та A_* породжують групи G та G_* відповідно. З умови випливає, що $G < G_*$. Якщо G_* скінченна, то очевидно, що G також скінченна.

Нехай G скінченна. Розглянемо автомат $A_0 = \langle X, Q_0, \varphi_0, \lambda_0 \rangle$, який містить всі можливі добутки станів автомату A. Побудуємо автомат $A^* = \langle X, Q^*, \varphi^*, \lambda^* \rangle$, додавши до автомату A_0 всі можливі стани q такі, що $\lambda^*(\cdot, q)$ — підстановка на X та $\varphi^*(x, q) \in Q_0$ для $x \in X$. Тоді $|A^*| = |A_0| + |X|! \cdot |A_0|^{|X|} < \infty$. Нехай автомат A^* породжує групу G^*. Доведемо, що $A^{*2} = A^*$. Для цього достатньо для $q_1, q_2 \in Q^*$ довести, що існує стан $q \in Q^*$ такий, що $f_{(q_1,q_2)} = f_q$. Для кожного $x \in X$: $\varphi^*(x, (q_1, q_2)) = (\varphi^*(x, q_1), \varphi^*(\lambda^*(x, q_1), q_2)) \in Q_0 \times Q_0$. Отже, існує стан $q_x \in Q_0$ такий, що $f_{\varphi^*(x,(q_1,q_2))} = f_{q_x}$. Стан q треба вибрати так, щоб $\pi_q = \pi_{(q_1,q_2)}$ та $\varphi^*(x, q) = q_x$. Звідси випливає, що $|G^*| < \infty$. За побудовою $A^* \supset A_*$, тому $G_* < G^*$ та $|G_*| < \infty$. □

Означення 9. Автомат $A_{(k)} = \langle X^k, Q, \varphi_{(k)}, \lambda_{(k)} \rangle$ такий, що $\varphi_{(k)}(w, q) = \varphi(w, q)$, $\lambda_{(k)}(w, q) = \lambda(w, q)$ для кожних $w \in X^k$ та стану $q \in Q$, називається *k-прискореним автоматом для автомату A.*

Лема 2. *Групи, породжені автоматами A та $A_{(k)}$, ізоморфні.*

Доведення. Відповідні стани автоматів діють на слова з X^ω та $(X^k)^\omega = X^\omega$ однаково. Тому групи породжені цими автоматами ізоморфні. □

Означення 10. *Циклом* в автоматі A називається послідовність попарно різних станів $q_1, q_2, \ldots, q_n \in Q$, для яких існує послідовність літер $x_1, x_2, \ldots, x_n$ така, що $\varphi(x_i, q_i) = q_{i+1}$ для $1 \leq i < n$ та $\varphi(x_n, q_n) = q_1$, при цьому число n називається довжиною циклу.

Означення 11. Цикл $q_1, q_2, \ldots, q_n \in Q$ в автоматі A називається *циклом з виходом*, якщо існують i $(1 \leq i \leq n)$, та $x \in X$ такі, що $\varphi(x, q_i) \notin \{q_1, q_2, \ldots, q_n\}$. В іншому випадку кажуть, що цей цикл є циклом без виходу.

Достатню умову скінченності групи породженої автоматом дає наступна теорема.

Теорема 2. *Група породжена скінченним автоматом, який не містить циклу з виходом, скінченна.*

Доведення. Нехай скінченний автомат A не містить циклу з виходом. Позначимо символом k найменше спільне кратне довжин всіх циклів та кількості станів. Розглянемо k-прискорений автомат $A_{(k)}$. Всі стани останнього діляться на два класи: циклічні (q — циклічний, якщо для всіх $x \in X^k$ виконується $\varphi_{(k)}(x, q) = q$) та передциклічні (q — передциклічний, якщо він не є циклічним та для всіх $x \in X^k$ стан $\varphi_{(k)}(x, q)$ є циклічним). Нехай $A_{(k)} \supset A_0$, який складається з циклічних станів $A_{(k)}$ та G_0 — група породжена A_0. Легко бачити, що G_0 ізоморфна деякій підгрупі групи підстановок на X^k. Тому $|G_0| \leq |X^k|! < \infty$. За лемою 1 група, породжена $A_{(k)}$, скінченна, а за лемою 2 група, породжена A, скінченна. □

Обернене твердження, взагалі кажучи, є хибним. Для $|X| \geq 3$ розглянемо автомат, який складається з двох станів q та q_0, що задовольняють умови $\pi_q = (a, b)$, $\pi_{q_0} = e$, $\varphi(a, q) = \varphi(b, q) = q$, $\varphi(x, q) = q_0$ для решти літер та $\varphi(\cdot, q_0) = q_0$, де $a, b \in X$ — деякі фіксовані літери з X.

У випадку $|X| = 2$ контрприклад будуємо так. Автомат над $X = \{0, 1\}$ має три стани 1, a та c, для яких $\pi_1 = \pi_c = e$ та $\pi_a = (0, 1)$; $\varphi(0, 1) = \varphi(1, 1) = 1$, $\varphi(0, a) = \varphi(1, a) = c$, $\varphi(0, c) = 1$ та $\varphi(1, c) = a$. Він містить цикл з виходом. Доведемо, що цей автомат породжує скінченну групу. Легко бачити, що $f_a^2 = 1$ та $f_c^2 = 1$. Розглянемо добуток $(f_a \cdot f_c)^4 = f_{(a,c,a,c,a,c,a,c)}$. Для $w \in X^*$ правильні рівності $f_{(a,c,a,c,a,c,a,c)}(0w) = 0f_{(c,a,c,1,c,a,c,1)}(w) = 0w$ та $f_{(a,c,a,c,a,c,a,c)}(1w) = 1f_{(c,1,c,a,c,1,c,a)}(w) = 1w$, тобто $(f_a \cdot f_c)^4 = 1$. З вказаних рівностей випливає, що автомат визначає групу, яка містить не більше 8 елементів, а тому є скінченною. Безпосередніми обчисленнями можна перевірити, що він визначає групу, яка є підгрупою $\mathbb{D}_4$. Насправді він породжує $\mathbb{D}_4$, що випливає з теореми 4 наступного розділу, оскільки всі власні підгрупи $\mathbb{D}_4$ абелеві.

Слабку достатню умову для нескінченності групи, породженої автоматом, дає наступне твердження.

Твердження 4. *Нехай $|X| = 2$, автомат A, у якого існують стан $q \in Q$ та літера $x \in X$ такі, що $f_{\varphi(x,(q,q))} = f_q$. Тоді f_q має нескінченний порядок або f_q — тотожнє відображення.*

Доведення. Нехай f_q має скінченний порядок та не є тотожнім. Тоді за [2] порядок f_q дорівнює 2^n, $n \in \mathbb{N}$, тобто $\underbrace{f_q \cdot \ldots \cdot f_q}_{2^n} = f_{\underbrace{(q, q, \ldots, q)}_{2^n}} = 1$. Звідси

$$f_{\varphi(x,\underbrace{(q, q, \ldots, q)}_{2^n})} = \underbrace{f_{\varphi(x,(q,q))} \cdot \ldots \cdot f_{\varphi(x,(q,q))}}_{2^{n-1}} = \underbrace{f_q \cdot \ldots \cdot f_q}_{2^{n-1}} = 1.$$

Суперечність. □

4. Абелеві групи, породжені автоматами. У цьому розділі $X = \{0, 1\}$. Позначимо символом σ транспозицію (01), а символом e одиничну підстановку на X. Нехай $A = \langle X, Q, \varphi, \lambda\rangle$ — деякий автомат, можливо із нескінченною кількістю станів. Для кожного $q \in Q$ визначимо $s(q) := f_{\varphi(1,q)} \cdot f^{-1}_{\varphi(0,q)} = f^{-1}_{\varphi(0,q)}\left(f_{\varphi(1,q)}\right)$. Критерій абелевості групи, породженої автоматом, дає наступна теорема.

Теорема 3. *Автомат A породжує абелеву групу тоді і лише тоді, коли $s(q_1) = s(q_2)$ для всіх $q_1, q_2 \in Q$ таких, що $\pi_{q_1} = \pi_{q_2}$ та $s(q) = 1$ для всіх $q \in Q$ таких, що $\pi_q = e$.*

Доведення. Розглядатимемо відображення множини X^ω, визначені як станами автомату A, так і станами A^2.

Необхідність. Нехай $q_1, q_2 \in Q$ — довільні два стани, для яких $\lambda(\cdot, q_1) = \lambda(\cdot, q_2) = \sigma$. З абелевості випливає, що $f_{\varphi(0,q_1)} \cdot f_{\varphi(1,q_2)} = f_{\varphi(0,(q_1,q_2))} = f_{\varphi(0,(q_2,q_1))} = f_{\varphi(0,q_2)} \cdot f_{\varphi(1,q_1)}$. Звідси маємо

$$s(q_1) = f_{\varphi(1,q_1)} \cdot f^{-1}_{\varphi(0,q_1)} = f^{-1}_{\varphi(0,q_2)} \cdot f_{\varphi(0,q_1)} \cdot f_{\varphi(1,q_2)} \cdot f^{-1}_{\varphi(0,q_1)} = f_{\varphi(1,q_2)} \cdot f^{-1}_{\varphi(0,q_2)} = s(q_2).$$

Нехай додатково $q \in Q$ — довільний стан, для якого $\lambda(\cdot, q_1) = e$. З абелевості випливає, що $f_{\varphi(0,q_1)} \cdot f_{\varphi(1,q)} = f_{\varphi(0,(q_1,q))} = f_{\varphi(0,(q,q_1))} = f_{\varphi(0,q)} \cdot f_{\varphi(0,q_1)} = f_{\varphi(0,q_1)} \cdot f_{\varphi(0,q)}$. Звідси випливає $f_{\varphi(1,q)} = f_{\varphi(0,q)}$ та $s(q) = f_{\varphi(1,q)} \cdot f^{-1}_{\varphi(0,q)} = 1$.

Достатність. Потрібно довести, що для всіх $q_1, q_2 \in Q$ правильна рівність

$$f_{(q_1,q_2)} = f_{(q_2,q_1)} \text{ або еквівалентна до неї } f_{q_1} \cdot f_{q_2} = f_{q_2} \cdot f_{q_1}. \tag{3}$$

Доводитимемо індукцією за довжиною слова. База індукції (для слів довжини 1) випливає з рівності $\lambda(\cdot, (q_1, q_2)) = \lambda(\cdot, q_1) \cdot \lambda(\cdot, q_2) = \lambda(\cdot, q_2) \cdot \lambda(\cdot, q_1) = \lambda(\cdot, (q_2, q_1))$. Нехай умова (3) виконується для слів довжини k. Зафіксуємо стани $q_1, q_2 \in Q$ та доведемо, що для них виконується умова (3) для слів довжини $k + 1$. Розглянемо два випадки.

Якщо $\lambda(\cdot, q_1) = e$, то $\varphi(0, q_1) = \varphi(1, q_1)$ та $\varphi(x, (q_1, q_2)) = (\varphi(x, q_1), \varphi(\lambda(x, q_1), q_2)) = (\varphi(x, q_1), \varphi(x, q_2))$ і $\varphi(x, (q_2, q_1)) = (\varphi(x, q_2), \varphi(\lambda(x, q_2), q_1)) = (\varphi(x, q_2), \varphi(x, q_1))$. Рівність (3) виконується для слів довжини 1 та для кожного $x \in X$ рівність $f_{\varphi(x,(q_1,q_2))} = f_{(\varphi(x,q_1),\varphi(x,q_2))} = f_{(\varphi(x,q_2),\varphi(x,q_1))} = f_{\varphi(x,(q_2,q_1))}$ — для слів довжини k. Звідси випливає, що (3) виконується для слів довжини $k + 1$. У випадку $\lambda(\cdot, q_2) = e$ доведення здійснюємо подібно.

Нехай тепер $\lambda(\cdot, q_1) = \lambda(\cdot, q_2) = \sigma$. Тоді $s(q_1) = s(q_2) =: f$ та $f_{\varphi(1,q_i)} = f \cdot f_{\varphi(0,q_i)}$ або $f_{\varphi(0,q_i)} = f^{-1} \cdot f_{\varphi(1,q_i)}$. Рівність (3) виконується для слів довжини 1. Крім того,

$$\begin{aligned} f_{\varphi(0,(q_1,q_2))} = f_{\varphi(0,q_1)} \cdot f_{\varphi(1,q_2)} = f^{-1} \cdot f_{\varphi(1,q_1)} \cdot f_{\varphi(1,q_2)} = f^{-1} \cdot f_{\varphi(1,q_2)} \cdot f_{\varphi(1,q_1)} = \\ = f_{\varphi(0,q_2)} \cdot f_{\varphi(1,q_1)} = f_{\varphi(0,(q_2,q_1))} \end{aligned}$$

та

$$\begin{aligned} f_{\varphi(1,(q_1,q_2))} = f_{\varphi(1,q_1)} \cdot f_{\varphi(0,q_2)} = f \cdot f_{\varphi(0,q_1)} \cdot f_{\varphi(0,q_2)} = \\ = f \cdot f_{\varphi(0,q_2)} \cdot f_{\varphi(0,q_1)} = f_{\varphi(1,q_2)} \cdot f_{\varphi(0,q_1)} = f_{\varphi(1,(q_2,q_1))} \end{aligned}$$

для слів довжини k. Тому в цьому випадку (3) також виконується для слів довжини $k + 1$. □

Означення 12. Для автомату A, що породжує абелеву групу, визначимо *зсув* $sh(A)$ за допомогою рівності $sh(A) = s(q)$ для деякого $q \in Q$ такого, що $\lambda(\cdot, q) = \sigma$.

Оберненою до теореми 2 у випадку абелевої групи є наступна теорема.

Теорема 4. *Нехай мінімізований автомат A, $|A| < \infty$, породжує абелеву групу. Тоді наступні умови еквівалентні:*

(1) $sh(A) \neq 1$;

(2) A має цикл з виходом;

(3) A породжує нескінченну групу.

Доведення. (3)⇒(2). Випливає з теореми 2.

(2)⇒(1). Нехай умова (1) не виконується, тобто $sh(A) = 1$. Тоді для кожного стану $q \in Q$ функція $\varphi(\cdot, q)$ є сталою. Звідси випливає, що циклу з виходом не існує.

(1)⇒(3). Припустимо, що A породжує скінченну групу та містить добутки всіх своїх станів. Нехай h — стан автомату такий, що $f_h = sh(A) \neq 1$, а m — порядок f_h. Розглянемо послідовність, першим членом якої є h та кожний наступний є значенням функції $\varphi(0, \cdot)$ від попереднього. Позначимо $\tilde{h}$ перший стан послідовності, для якого $\lambda(\cdot, \tilde{h}) = \sigma$. Очевидно, що порядок $f_{\tilde{h}}$ також дорівнює m. Розглянемо стан $g_1 = \varphi(0, \tilde{h})$. З рівності $f^m_{\tilde{h}} = 1$ випливає, що $(f^2_{g_1} f_h)^{\frac{m}{2}} = f^m_{g_1} f_h^{\frac{m}{2}} = 1$. Звідси маємо $f^m_{g_1} \neq 1$ та $f^m_{g_1} = f_h^{\frac{m}{2}}$.

Розглянемо послідовність, першим членом якої є g_k та кожний наступний є значенням функції $\varphi(0, \cdot)$ від попереднього. Позначимо $\tilde{g}_k$ перший стан послідовності, для якого $\lambda(\cdot, \tilde{g}_k) = \sigma$; n_k — його номер, рахуючи від нуля. Очевидно, що порядки f_{g_k} та $f_{\tilde{g}_k}$ однакові. Крім того, для довільних слів $u \in X^{n_k}$, $w \in X^*$ маємо $f_{g_k}(uw) = u f_{\tilde{g}_k}(w)$. Розглянемо стан $g_{k+1} = \varphi(0, \tilde{g}_k)$. Легко отримати рівність $f^2_{\tilde{g}_k}(xw) = x(f^2_{g_{k+1}} \cdot f_h)(w)$, яка виконується для довільних літери $x \in X$ та слова $w \in X^*$.

Для $k \geq 1$, довільних слів $u \in X^{n_k}$, $w \in X^*$ та для довільної літери $x \in X$ правильні рівності $f^m_{g_k}(uw) = u f^m_{\tilde{g}_k}(w)$ та $f^m_{\tilde{g}_k}(xw) = x(f^m_{g_{k+1}} \cdot f_h^{\frac{m}{2}})(w) = x(f^m_{g_{k+1}} \cdot f^m_{g_1})(w)$. Тому, для довільних $k \geq 1$ і слів $u \in X^{n_k+1}$, $w \in X^*$ виконується $f^m_{g_k}(uw) = u(f^m_{g_{k+1}} \cdot f^m_{g_1})(w)$, тобто відображення $f^m_{g_k}$ не змінює перших $n_k + 1 \geq 1$ літер, а на решту слова діє відображення $f^m_{g_{k+1}} \cdot f^m_{g_1}$. Для кожного множника міркуємо подібно. Звідси випливає, що відображення $f^m_{g_k}$ діє на слова нейтрально, тобто $f^m_{g_k} = 1$, що суперечить умові $f^m_{g_1} \neq 1$. □

Наступний наслідок характеризує всі скінченні абелеві групи, що можуть бути породжені автоматом над двоелементним алфавітом.

Наслідок 2. *Нехай A породжує скінченну абелеву групу. Тоді ця група для деякого $n \in \mathbb{N}$ ізоморфна до $\underbrace{C_2 \times \ldots \times C_2}_{n}$.*

Доведення. За теоремою 4 зсув $sh(A) = 1$, тобто для кожного стану $q \in Q$ функція переходу $\varphi(\cdot, q)$ стала. Тоді порядки всіх елементів не більші за 2. Справді, якщо $\varphi(\cdot, q_1) = q_2$, то $\varphi(\cdot, (q_1, q_1)) = (q_2, q_2)$. Крім того, для кожного стану $q \in Q$ відображення $\pi_{(q,q)}$ є тотожнім. Тому стани (q, q) діють нейтрально, тобто збігаються з одиницею групи.

Абелева група розкладається в добуток циклічних. Наявність в розкладі групи, породженої автоматом A, циклічної групи порядку відмінного від 2, суперечить тому, що порядки всіх елементів не перевищують 2. □

Наслідок 3. *Нехай $|X| = 2$. Не існує автомату над X, який породжує циклічну групу порядку більшого за 2.*

ЛІТЕРАТУРА

1. Глушков В. М. *Абстрактная теория автоматов* // УМН. – 1961. – Т.16, №5. – С.3–62.
2. Григорчук Р. И., Некрашевич В. В., Сущанский В. И. *Автоматы, динамические системы и группы* // Труды Мат. ин-та им. В.М. Стеклова. – 2000. – Т.231. – С.134–214.
3. Резников И.И., Сущанский В.И. *Функции роста автоматов с двумя состояниями над двухэлементным алфавитом* // Доп. НАН України. – 2002. – №2. – С.76–81.

Київський національний університет імені Тараса Шевченка,
механіко-математичний факультет,
Володимирська, 60, Київ, 01033

Надійшло 14.02.2005