УДК 512.54

А. В. Руссєв

Групи автоматів без циклу з виходом

(Представлено членом-кореспондентом НАН України Ю. С. Самойленком)

Доведено, що клас груп, породжених автоматами над скінченним алфавітом, є замкненим відносно прямих степенів та деяких вінцевих добутків. Отримано точну оцінку порядків груп автоматів без циклу з виходом над бінарним алфавітом.

1. Клас груп, породжених автоматами-трансляторами над скінченними алфавітами, містить багато груп з цікавими та несподіваними властивостями. Серед них у першу чергу виділяються групи бернсайдового типу (скінченно породжені нескінченні періодичні групи) та групи проміжного росту (див. [1, 2] та наведену в них бібліогр.). Ряд робіт присвячено, зокрема, вивченню реалізацій тих чи інших груп як груп, породжених автоматами. Так, в [3] досліджувались абелеві групи, породжені скінченними автоматами над бінарним алфавітом, а в [4] побудовано скінченні автомати, що породжують деякі скінченно задані розв'язні групи. Відзначимо також приклади скінченних автоматів, що породжують вільну групу рангу 2 [2] та вільні добутки скінченної кількості циклічних груп порядку 2 [5]. Природно виникають такі питання. Які групи реалізуються як групи, породжені автоматом над заданим алфавітом? Яка найменша можлива кількість станів у такому автоматі? Зазначимо, що задача повної класифікації груп, породжених автоматами навіть над бінарним алфавітом, є надзвичайно складною. Так, повну класифікацію груп, породжених двостановими автоматами над бінарним алфавітом, наведено в [1], а результатам, отриманим при спробі класифікувати групи, породжені тристановими автоматами над цим же алфавітом, присвячено роботу [6].

У даній роботі встановлюється замкненість класу груп, породжених автоматами, відносно операції вінцевого добутку, активний множник якого є групою підстановок на алфавіті, та операції піднесення до прямого степеня. У класі груп, породжених автоматами, природно виділити підклас груп, породжених автоматами без циклу з виходом. Цей підклас містить лише скінченні групи [7]. Для класу груп, породжених автоматами без циклу з виходом над бінарним алфавітом, знайдена точна оцінка потужності групи, як функція кількості станів автомату.

2. Нехай X — деяка скінченна непорожня множина, яку будемо називати алфавітом, а її елементи — літерами.

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

Автомат $A = \langle X, Q, \varphi, \lambda\rangle$ можна зображати у вигляді поміченого орієнтованого графа, вершинами якого є стани автомата. Помітка в кожній вершині $q \in Q$ визначає функцію виходів $\lambda(q, \cdot)$. Функція переходів зображується за допомогою ребер. Для кожної пари $(q, x) \in Q \times X$ граф містить ребро з поміткою x, що виходить з вершини q і закінчується у вершині $\varphi(q, x)$.

Розглянемо автомат $A = \langle X, Q, \varphi, \lambda\rangle$.

Означення 2. Циклом в автоматі A називається послідовність попарно різних станів $q_1,\ q_2, \ldots, q_n \in Q,\ n \geqslant 1$, для яких існує послідовність літер $x_1,\ x_2, \ldots, x_n \in X$ така, що $\varphi(q_i, x_i) = q_{i+1}$ для $1 \leqslant i < n$ та $\varphi(q_n, x_n) = q_1$. При цьому число n називається довжиною циклу.

Означення 3. Цикл $q_1, q_2, \ldots, q_n \in Q$ в автоматі A називається циклом з виходом, якщо існує i, $1 \leqslant i \leqslant n$, та $x \in X$ такі, що $\varphi(q_i, x) \neq \{q_1, q_2, \ldots, q_n\}$. В іншому випадку кажуть, що цей цикл є циклом без виходу.

Означення 4. Стан $q \in Q$ називається циклічним, якщо він належить деякому циклу в автоматі A.

Розглянемо множину $X^* = \bigcup\limits_{n \geqslant 1} X^n \bigcup \{\Lambda\}$ усіх слів над алфавітом X; символом Λ будемо позначати порожнє слово. Функції переходів та виходів автомата A продовжуються на множину $Q \times X^*$ за правилом: для $q \in Q$, $w \in X^*$ та $x \in X$

$$\varphi(q, wx) = \varphi(\varphi(q, w), x), \qquad \varphi(q, \Lambda) = q,$$

$$\lambda(q, wx) = \lambda(q, w)\lambda(\varphi(q, w), x), \qquad \lambda(q, \Lambda) = \Lambda.$$

Кожному стану $q \in Q$ відповідає відображення $f_q = \lambda(q, \cdot)\colon X^* \to X^*$.

Далі будемо розглядати лише такі автомати, що для кожного стану $q \in Q$ відображення f_q є бієкцією.

Означення 5 [2, розділ 1.5.4]. Групою, породженою автоматом A, називається група, породжена перетвореннями f_q, де q пробігає всі стани автомата A.

Згідно з означенням, група, породжена автоматом, є групою підстановок на множині X^*.

Теорема 1 [7, теорема 2]. *Група, породжена скінченним автоматом, який не містить циклу з виходом, скінченна.*

Символом $S(X)$ будемо позначати симетричну групу підстановок на множині X.

3. Клас груп, породжених автоматами над алфавітом X, є замкненим відносно певних теоретико-групових операцій. А саме, має місце такий результат про замкненість відносно вінцевого множення:

Теорема 2. *Нехай G є групою, породженою (скінченним, без циклу з виходом) автоматом $A = \langle X, Q, \varphi, \lambda\rangle$ над алфавітом X, $P < S(X)$ та для кожного $q \in Q$ підстановка $\lambda(q, \cdot)$ належить групі P. Тоді група $P \wr G$ також є групою, породженою (скінченним, без циклу з виходом) автоматом над алфавітом X.*

Також клас груп, породжених автоматами над алфавітом X, є замкненим відносно піднесення до прямого степеня:

Теорема 3. *Нехай G є групою, породженою (скінченним, без циклу з виходом) автоматом над алфавітом X. Тоді група $\bigoplus\limits_{i=1}^{n} G$ для кожного натурального n також є групою, породженою (скінченним, без циклу з виходом) автоматом над алфавітом X.*

У загальному випадку з того, що G_1 і G_2 породжуються автоматами над алфавітом X, не випливає, що $G_1 \times G_2$ породжується автоматом над тим же алфавітом. Наприклад, група $\mathbb{Z} \oplus \mathbb{Z}_2$ не породжується автоматом над бінарним алфавітом [3, твердження 3.4], хоча групи $\mathbb{Z}$ та $\mathbb{Z}_2$ породжуються.

Якщо не накладати обмежень на алфавіт, то легко побудувати автомат, що буде породжувати групу $G_1 \times G_2$. Досить розглянути алфавіт вдвічі більшої потужності і автомат утворити з двох диз'юнктних частин, одна з яких буде діяти як автомат для G_1 на першій половині алфавіту і тотожно на другій половині, а інша, навпаки, тотожно на першій половині і як автомат для G_2 на другій.

З теорем 2 і 3 отримуємо такий результат про реалізацію груп як груп, породжених автоматами:

Наслідок 1. *Нехай група G породжується (скінченним, без циклу з виходом) автоматом над бінарним алфавітом. Тоді групи $\mathbb{Z}_2 \wr G$ та $\bigoplus\limits_{i=1}^{n} G$ породжуються (скінченним, без циклу з виходом) автоматом над бінарним алфавітом.*

Зауважимо, що доведення теорем 2 і 3 є конструктивними, а тому, як тільки відома конструкція автомата, що породжує групу G, відразу можна вказати автомати, які б породжували групи $\mathbb{Z}_2 \wr G$ та $\bigoplus\limits_{i=1}^{n} G$.

4. Надалі вважатимемо, що $X = \{0, 1\}$. Знайдемо точну оцінку порядку групи, породженої n-становим ($n \in \mathbb{N}$) автоматом без циклів з виходом.

Нехай автомат $A = \langle X, Q, \varphi, \lambda \rangle$ без циклу з виходом породжує групу G. Множину твірних групи G ототожнюємо з множиною станів автомата A. Легко бачити, що квадрати циклічних станів автомата A діють тотожно. Тому кожний циклічний стан A буде оберненим до себе. Крім того, усі ці стани попарно комутують. Будемо говорити, що множина циклічних станів автомата A є залежною, якщо серед них є стан, що діє тотожно або є добутком деяких інших циклічних станів.

Лема 1. *Нехай множина циклічних станів автомата A є залежною. Якщо $|Q| = n$, то має місце нерівність $|G| \leqslant 2^{2^{n-1}-1}$.*

Доведення. Доводимо індукцією за кількістю станів n. База індукції $n = 1$. Єдиний стан такого автомата буде циклічним. Оскільки множина циклічних станів є залежною, то цей стан є тотожним і група G є одиничною.

Крок індукції. Розіб'ємо множину станів автомата A на дві частини $Q = Q_1 \bigsqcup Q_2$, де $Q_1 = \operatorname{im} \varphi$ — множина станів, в які можна прийти по ребру з деякого іншого, а $Q_2 = Q \backslash Q_1$ — множина станів, в які не входять ребра. Якщо Q_2 порожня, то автомат A містить лише циклічні стани. Вони мають порядок не вище за 2 та комутують. Враховуючи залежність множини циклічних станів, маємо

$$|G| \leqslant 2^{n-1} \leqslant 2^{2^{n-1}-1}.$$

Нехай тепер Q_2 не порожня. Позначимо через $\widetilde{G}$ групу, породжену автоматом з множиною станів Q_1. Усі циклічні стани A належать множині Q_1. Тому за припущенням індукції маємо $|\widetilde{G}| \leqslant 2^{2^{n-2}-1}$, оскільки $|Q_1| \leqslant n - 1$. Група G є підгрупою $\mathbb{Z}_2 \wr \widetilde{G}$, а тому

$$|G| \leqslant |\mathbb{Z}_2 \wr \widetilde{G}| = 2 \cdot |\widetilde{G}|^2 \leqslant 2 \cdot \left(2^{2^{n-2}-1}\right)^2 = 2^{2^{n-1}-1}.$$

Твердження леми випливає з принципу математичної індукції.

Лема 2. *Нехай слово w, що складене з твірних G, має непарну довжину та дорівнює 1 у групі G. Тоді множина циклічних станів A є залежною.*

Доведення. Слово w можна вважати станом автомата $(A \bigcup A^{-1})^{|w|}$. Цей стан є одиничним. Тому довільний стан w також одиничний. Розглянемо стан $\widetilde{w} = w|_u$, де u — деяке слово довжини $|Q|$, в який перейде автомат зі стану w, одержавши слово u. Кожний стан автомата $A \bigcup A^{-1}$ з добутку w, одержавши $|Q|$ літер, перейде в циклічний стан автомата

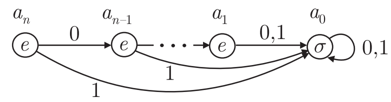

Рис. 1

$A \bigcup A^{-1}$. Але множини циклічних станів автоматів A^{-1} та A збігаються. Отже, стан $\widetilde{w}$ є добутком $|w|$ циклічних станів автомата A і його можна скоротити до вигляду, де кожний циклічний стан зустрічається не більше одного разу. Одержаний добуток буде містити непарну кількість циклічних станів автомата A. Звідси випливає залежність циклічних станів A.

Лема 3. *Нехай слова w_1, w_2 складені з твірних G та $w_1 = w_2$ у групі G. Якщо множина циклічних станів A є незалежною, то довжини слів w_1 та w_2 мають однакову парність.*

Доведення. Розглянемо слово $w = w_1 w_2^{-1}$. Якщо воно має непарну довжину, то за лемою 2 множина циклічних станів A є залежною.

Нехай множина циклічних станів автомата A є незалежною. Елемент групи G будемо називати парним, якщо він є добутком парної кількості твірних групи. Лема 3 обгрунтовує коректність введення поняття парності на елементах G. Нехай $g \in G$ — деякий твірний групи G. Відображення групи G в себе, задане правилом $x \mapsto gx$, є ін'єктивним та переводить непарні елементи в парні і навпаки. Тому кількість парних і непарних елементів однакова.

Лема 4. *Нехай множина циклічних станів автомата A є незалежною. Якщо $|Q| = n$, то має місце нерівність $|G| \leqslant 2^{2^{n-1}}$.*

Доведення. Доводимо індукцією за кількістю станів n. База індукції $n = 1$. Єдиний стан такого автомата буде циклічним. Оскільки множина циклічних станів є незалежною, то цей стан має порядок 2 та $|G| = 2$.

Крок індукції. Розіб'ємо множину станів автомата A на дві частини $Q = Q_1 \bigsqcup Q_2$, де $Q_1 = \operatorname{im} \varphi$ — множина станів, в які можна прийти по ребру з деякого іншого, а $Q_2 = Q \setminus Q_1$ — множина станів, в які не входять ребра. Якщо Q_2 порожня, то автомат A містить лише циклічні стани, що мають порядок 2 та комутують. Звідси

$$|G| \leqslant 2^n \leqslant 2^{2^{n-1}}.$$

Нехай тепер Q_2 не порожня. Позначимо через $\widetilde{G}$ групу, породжену автоматом з множиною станів Q_1. За припущенням індукції маємо $|\widetilde{G}| \leqslant 2^{2^{n-2}}$, оскільки $|Q_1| \leqslant n-1$. Група G є підгрупою $\mathbb{Z}_2 \wr \widetilde{G}$. Елементи групи G мають вигляд $[\pi; g_1, g_2]$, де $\pi \in \mathbb{Z}_2$, g_1, $g_2 \in \widetilde{G}$ однакової парності. Тому

$$|G| \leqslant \frac{1}{2} \cdot |\mathbb{Z}_2 \wr \widetilde{G}| = \frac{1}{2} \cdot 2 \cdot |\widetilde{G}|^2 \leqslant \left(2^{2^{n-2}}\right)^2 = 2^{2^{n-1}}.$$

Твердження леми випливає з принципу математичної індукції.

Теорема 4. *Нехай автомат $A = \langle X, Q, \varphi, \lambda \rangle$ без циклу з виходом породжує групу G. Якщо $|Q| = n$, то $|G| \leqslant 2^{2^{n-1}}$.*

Доведення. Твердження теореми є наслідком лем 1 та 4.

Зауважимо, що оцінка в теоремі 4 є точною. Як приклад можна розглянути автомат, зображений на рис. 1. Він має $n+1$ стан і породжує групу $G \simeq \mathbb{Z}_2 \oplus \wr_{i=1}^{n} \mathbb{Z}_2$ порядку 2^{2^n}.

1. *Григорчук Р. И., Некрашевич В. В., Сущанский В. И.* Автоматы, динамические системы и группы // Тр. Мат. ин-та им. В. А. Стеклова. – 2000. – **231**. – С. 134–214.
2. *Nekrashevych V. V.* Self-similar groups. – Providence, RI: Amer. Math. Soc., 2005. – 231 p.

3. *Nekrashevych V., Sidki S.* Automorphisms of the binary tree: state closed subgroups and dynamics of 1/2-endomorphisms // Groups: Topological, Combinatorial and Arithmetic Aspects / Ed. T. W. Müller. – Cambridge: Cambridge Univ. Press, 2004. – **311**. – P. 375–404.
4. *Bartholdi L., Šunić Z.* Some solvable automaton groups // Contemp. Math. – 2006. – **394**. – P. 11–29.
5. *Savchuk D., Vorobets Ya.* Automata generating free products of groups of order 2, 2008. – (available at http://arxiv.org/abs/0806.4801).
6. *Bondarenko I., Grigorchuk R., Kravchenko R. et al.* Classification of groups generated by 3-state automata over a 2-letter alphabet // Algebra and Discrete Mathematics. – 2008. – **1**. – P. 1–163.
7. *Руссєв А. В.* Про скінченні та абелеві групи, породжені скінченними автоматами // Мат. студії. – 2005. – **24**, № 2. – С. 139–146.

Київський національний університет
ім. Тараса Шевченка

Надійшло до редакції 15.05.2009

A. V. Russyev

Groups of automata without cycles with exit

It is proved that the class of groups generated by automata over a finite alphabet is closed with respect to direct powers and some wreath products. Orders of groups of automata without cycles with exit over a binary alphabet are precisely estimated.