ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель—июнь 2004. Серия 1. Том 11, № 2, 73–79

УДК 519.716

О ЧИСЛЕ МАКСИМАЛЬНЫХ ПОДГРУПП В ГРУППАХ АВТОМАТНЫХ ПОДСТАНОВОК*)

С. С. Марченков

Рассматриваются группы $\mathcal{D}_k, \mathcal{A}_k$ автоматных подстановок над k-буквенным алфавитом, реализуемых автоматами с бесконечным и конечным числом состояний. Доказано, что в группах $\mathcal{D}_k, \mathcal{A}_k$ и ряде других счетных подгрупп группы $\mathcal{D}_k$ мощность семейства максимальных подгрупп равна мощности семейства всех подгрупп соответствующей группы.

Пусть $N = \{0, 1, 2, \ldots, \}$, $k \in N$, $k \geqslant 2$, $E_k = \{0, 1, \ldots, k-1\}$, E_k^N — множество всех счетных последовательностей, составленных из элементов множества E_k. Элемент a множества E_k^N считаем функцией, отображающей N в E_k, и записываем в виде $a = a(0)a(1)a(2)\ldots$, где $a(t) \in E_k$ при $t \in N$.

В дискретной математике и математической кибернетике часто рассматриваются два класса функций, определенных на множестве E_k^N, — класс детерминированных (автоматных) и класс ограниченно-детерминированных (конечно-автоматных) функций [8]. Среди проблем, изучаемых для классов автоматных функций, одной из центральных является проблема полноты: каковы те необходимые и достаточные условия, которые обеспечивают полноту системы автоматных функций относительно выбранных операций. Распростаненный подход в решении проблемы полноты состоит в отыскании так называемых критериальных семейств. Критериальное семейство состоит из классов, замкнутых относительно рассматриваемых операций, причем произвольная система автоматных функций полна тогда и только тогда, когда она целиком не содержится ни в одном классе этого семейства.

Нетрудно видеть, что для произвольного замкнутого класса P всегда существует тривиальное критериальное семейство, состоящее из всех замкнутых подклассов класса P, отличных от P. Нетрудно также понять, что наименьшее критериальное семейство (если такое существует)

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 03-01-00783).

состоит только из предполных (максимальных) классов. Этим обстоятельством объясняется тот интерес, который проявляется к исследованию предполных классов автоматных функций.

В дальнейшем из операций, определенных на множестве автоматных функций, рассматриваем лишь операцию суперпозиции. Таким образом, под замкнутым классом будем понимать класс автоматных функций, замкнутый относительно операции суперпозиции.

Известно [3] (см. также [6]), что для класса всех конечно-автоматных функций мощность семейства предполных классов континуальна, т. е. равна мощности семейства всех замкнутых классов. Аналогичный эффект имеет место для класса всех детерминированных (автоматных) функций [6]. В связи с этим большой интерес представляет изучение замкнутых классов одноместных автоматных функций, осуществляющих взаимно однозначные отображения множества E_k^N на себя, т. е. подстановок на множестве E_k^N. Замкнутые классы подстановок естественно рассматривать в рамках теории групп. Таким образом, приходим к следующим задачам о группах автоматных подстановок.

Пусть $\mathcal{D}_k$ — группа подстановок на множестве E_k^N, осуществляемых детерминированными функциями (автоматами с бесконечным числом состояний), с групповой операцией композиции (суперпозиции) подстановок, $\mathcal{A}_k$ — подгруппа группы $\mathcal{D}_k$, соответствующая ограниченно-детерминированным (конечно-автоматным) функциям. Каково число максимальных подгрупп в группах $\mathcal{D}_k$ и $\mathcal{A}_k$?

Ниже мы устанавливаем, что в группах $\mathcal{D}_k, \mathcal{A}_k$ и ряде других счетных групп автоматных подстановок мощность семейства максимальных подгрупп равна мощности семейства всех подгрупп соответствующей группы. В частности, для групп $\mathcal{D}_k$ и $\mathcal{A}_k$ эти мощности суть 2^c и c, где c — мощность континуума. При получении этих результатов определяются мощности семейств максимальных подгрупп в некоторых бесконечных абелевых группах, связанных с группами автоматных подстановок [1].

Обозначим через G_2 группу $\langle E_2; \oplus\rangle$, где $\oplus$ есть сложение по модулю 2. Рассмотрим группу G_2^N — декартову сумму счетного числа экземпляров группы G_2. Группу G_2^N можно представить в виде $\langle E_2^N; \oplus\rangle$, где $\oplus$ представляет собой поразрядное сложение по модулю 2 бесконечных двоичных последовательностей. Отметим, что G_2^N есть периодическая абелева группа периода 2.

Пусть φ — автоматная подстановка на множества E_k^N, A_φ — инициальный автомат с множеством состояний Q (вообще говоря, бесконечным), реализующий подстановку φ. Следуя [1], поставим в соответствие подстановке φ некоторую двоичную последовательность из E_2^N.

Очевидно, что в каждом состоянии автомата A_φ реализуется некоторая подстановка на множестве E_k. Пусть Q_1 — множество всех состояний автомата A_φ, в которых реализуются нечетные подстановки. Для каждого $t \geqslant 0$ обозначим через p_t число путей (т. е. слов в алфавите E_k) длины t, ведущих из начального состояния автомата A_φ в состояния из множества Q_1. Последовательности $\{p_0, p_1, p_2, \ldots\}$ поставим в соответствие последовательность a_φ из E_2^N, где для любого $t \geqslant 0$ величина $a_\varphi(t)$ есть остаток от деления p_t на 2. Нетрудно убедиться в том, что последовательность a_φ зависит только от подстановки φ и не зависит от выбора автомата A_φ, реализующего подстановку φ.

Обозначим через H_k описанное выше отображение множества всех автоматных подстановок на E_k^N в множество бесконечных двоичных последовательностей E_2^N. В работе [1] установлено, что H_k является гомоморфизмом группы $\mathcal{D}_k$ на группу G_2^N. При этом образом множества всех конечно-автоматных подстановок на E_k^N является множество всех периодических (с предпериодами) последовательностей из E_2^N. Обозначим его через Per. Тогда $\langle \mathrm{Per}; \oplus \rangle$ — подгруппа группы G_2^N и ограничение гомоморфизма H_k на группу $\mathcal{A}_k$ есть гомоморфизм группы $\mathcal{A}_k$ на группу $\langle \mathrm{Per}; \oplus \rangle$.

Связь между максимальными подгруппами групп $\mathcal{D}_k$ и G_2^N, групп $\mathcal{A}_k$ и $\langle \mathrm{Per}; \oplus \rangle$, а также некоторых других групп будет вытекать из следующего почти очевидного утверждения.

Утверждение 1. *Пусть F_1, F_2 — группы, H — гомоморфизм группы F_1 на группу F_2, F' — максимальная подгруппа группы F_2. Тогда полный прообраз $H^{-1}(F')$ группы F' при отображении H является максимальной подгруппой группы F_1.*

Следствие. *Мощность семейства максимальных подгрупп группы F_2 не превосходит мощности семейства максимальных подгрупп группы F_1.*

Результаты о числе максимальных подгрупп в некоторых счетных подгруппах группы G_2^N будут получены ниже с использованием понятия $\mathcal{M}$-сжатого множества, которое обобщает понятие сжатого множества, введенного Р. Фридбергом [9] (см. также [5, 7]). Пусть $\mathcal{M}$ — произвольная совокупность подмножеств множества N. Множество $C \subseteq N$ назовем *$\mathcal{M}$-сжатым*, если оно бесконечно и для любого множества $M \in \mathcal{M}$ одно из множеств

$$M \cap C \quad \overline{M} \cap C,$$

где $\overline{M} = N \setminus M$, конечно (пустое множество также считаем конечным). Если $\mathcal{M}$ — совокупность всех рекурсивно перечислимых подмножеств множества N, то $\mathcal{M}$-сжатое множество является сжатым по Фридбергу.

Теорема 1. *Для любой счетной совокупности $\mathcal{M}$ подмножеств множества N существуют $\mathcal{M}$-сжатые множества.*

Доказательство. Пусть $\mathcal{M} = \{M_1, M_2, \ldots\}$. Зададим пошаговую процедуру построения $\mathcal{M}$-сжатого множества C. На каждом шаге n этой процедуры определяется конечная часть C_n множества C и вспомогательное бесконечное множество T_n. При этом выполняются соотношения

$$C_0 \subset C_1 \subset \ldots, \quad T_0 \supset T_1 \supset \ldots \tag{1}$$

Множество C будет совпадать с объединением $\bigcup\limits_{n \geqslant 0} C_n$.

Положим $C_0 = \varnothing,\ T_0 = N$.

Ш а г $n > 0$. Рассмотрим множество M_n. Если одно из множеств

$$M_n \cap T_{n-1}, \quad \overline{M}_n \cap T_{n-1} \tag{2}$$

конечно, то берем наименьший элемент a в множестве T_{n-1} и полагаем

$$C_n = C_{n-1} \cup \{a\}, \quad T_n = T_{n-1} \setminus \{a\}.$$

Пусть оба множества (2) бесконечны. Тогда берем наименьший элемент a в множестве $\overline{M}_n \cap T_{n-1}$ и полагаем

$$C_n = C_{n-1} \cup \{a\}, \quad T_n = (\overline{M}_n \cap T_{n-1}) \setminus \{a\}.$$

Переходим к шагу $n+1$.

Из построения легко следуют соотношения (1) и

$$C_n \cap T_n = \varnothing \quad (n \geqslant 0).$$

Кроме того, все элементы множества C, не вошедшие в множество C_n, принадлежат множеству T_n. Далее, если на шаге n построения множества C выясняется, что одно из множеств (2) конечно, то конечным будет и одно из множеств

$$M_n \cap C, \quad \overline{M}_n \cap C.$$

Если же не шаге n обнаруживается, что оба множества (2) бесконечны, то после шага n множество C определяется так, что за исключением конечного числа элементов (принадлежащих множеству C_n) оно будет состоять из элементов множества $\overline{M}_n$. Таким образом, в этом случае множество $M_n \cap C$ оказывается конечным. Теорема 1 доказана.

Следствие. *В условиях теоремы* 1 *существует континуальное число* $\mathcal{M}$*-сжатых множеств.*

Доказательство. Достаточно заметить, что любое бесконечное подмножество $\mathcal{M}$-сжатого множества является $\mathcal{M}$-сжатым.

Обозначим через G_2^d подгруппу группы G_2^N, которая состоит из всех элементов $a(0)a(1)\ldots$, у которых только конечное число компонент $a(t)$ равно 1. Группа G_2^d есть прямая сумма счетного числа групп G_2.

Теорема 2. *Пусть* G *— счетная подгруппа группы* G_2^N *и* $G_2^d \subseteq G$. *Тогда группа* G *имеет континуальное число максимальных подгрупп.*

Доказательство. Если $a \in G$, то пусть

$$M_a = \{n \mid n \in N,\ a(n) = 1\}, \quad \mathcal{M} = \{M_a \mid a \in G\}.$$

Обозначим через C некоторое $\mathcal{M}$-сжатое множество. Пусть G_C — множество всех таких элементов $a \in G$, что одно из множеств

$$M_a \cap C, \quad \overline{M}_a \cap C \tag{3}$$

конечно и содержит четное число элементов (случаи $M_a \cap C = \varnothing$ и $\overline{M}_a \cap C = \varnothing$ не исключаются). Нетрудно убедиться в том, что G_C — группа. Из условия $G_2^d \subseteq G$ и бесконечности множества C следует, что $G_C \neq G$. Докажем, что G_C максимальна в группе G.

Пусть $a \in G \setminus G_C$. Тогда одно из множеств (3) конечно и состоит из нечетного числа элементов. Если b — произвольный элемент из $G \setminus G_C$, то одно из множеств $M_b \cap C$, $\overline{M}_b \cap C$ также конечно и состоит из нечетного числа элементов. Значит, одно из множеств $M_{a\oplus b} \cap C$, $\overline{M}_{a\oplus b} \cap C$ конечно и состоит из четного числа элементов, т. е. $a \oplus b$ входит в группу G_C. Поскольку $b = (a \oplus b) \oplus a$, произвольный элемент из $G \setminus G_C$ можно получить сложением подходящего элемента группы G_C и фиксированного элемента a из $G \setminus G_C$. Следовательно, группа G_C максимальна в группе G.

Пусть теперь C_1, C_2 — два различных $\mathcal{M}$-сжатых множества и, например, $n \in C_1 \setminus C_2$. Обозначим через c такой элемент группы G_2^d, что $c(n) = 1$ и $c(m) = 0$ при $m \neq n$. Тогда $c \in G_{C_2}$, $c \notin G_{C_1}$. Поэтому группы G_{C_1} и G_{C_2} различны. Для завершения доказательства теоремы 2 остается применить следствие из теоремы 1.

Пусть $\mathcal{B}$ — булева алгебра всех подмножеств множества N с теоретико-множественными операциями объединения, пересечения и дополнения до множества N. Напомним, что фильтром булевой алгебры $\mathcal{B}$ называется такое непустое подмножество F элементов алгебры $\mathcal{B}$, что выполняются следующие условия:

1) если $A, B \in F$, то $A \cap B \in F$;

2) если $A \in F$ и $A \subseteq B$, то $B \in F$;

3) $\varnothing \notin F$.

Фильтр F алгебры $\mathcal{B}$ называется ультрафильтром, если F не содержится ни в каком другом фильтре алгебры $\mathcal{B}$, отличном от F. Известно (см., например, [2, 4]), что всякий фильтр алгебры $\mathcal{B}$ можно расширить до ультрафильтра. Кроме того, если U — ультрафильтр алгебры $\mathcal{B}$ и A — произвольное подмножество множества N, то ультрафильтру U принадлежит одно (и, очевидно, только одно) из множеств $A, \overline{A}$.

Теорема 3. *Мощность семейства максимальных подгрупп группы* G_2^N *равна* 2^c.

Доказательство. Пусть U — ультрафильтр алгебры $\mathcal{B}$. Ультрафильтру U поставим в соответствие подмножество G_U группы G_2^N:

$$G_U = \{a \mid a \in G_2^n,\ \overline{M}_a \in U\}.$$

Из первых двух условий определения фильтра следует, что множество G_U замкнуто относительно операции $\oplus$ группы G_2^N и содержит нуль группы G_2^N, т. е. G_U — подгруппа группы G_2^N. Из условия 3) вытекает, что группе G_U не принадлежит элемент $11\ldots$ Таким образом, G_U — собственная подгруппа группы G_2^N.

Докажем, что группа G_U максимальна в группе G_2^N. Пусть $a \in G_2^N \setminus G_U$. Тогда множество $\overline{M}_a$ не принадлежит ультрафильтру U. Следовательно, ему принадлежит множество M_a. Пусть b — такой элемент из G_U, что $\overline{M}_b = M_a$. Элемент $a \oplus b$ входит в группу, порожденную множеством $G_U \cup \{a\}$, и $M_{a\oplus b} = N$. Если теперь c — произвольный элемент множества $G_2^N \setminus G_U$, то $\overline{M}_c \notin U$ и потому $M_c \in U$. Значит, в группе G_U имеется такой элемент d, что $\overline{M}_d = M_c$. Тогда группе, порожденной множеством $G_U \cup \{a\}$, принадлежит элемент $a \oplus b \oplus d$. Нетрудно видеть, что этот элемент совпадает с элементом c.

Пусть U_1, U_2 — различные ультрафильтры алгебры $\mathcal{B}$ и, например, $M \in U_1 \setminus U_2$. Так как ультрафильтру U_2 принадлежит хотя бы одно из множеств $M, \overline{M}$, то $\overline{M} \in U_2$. Очевидно также, что $\overline{M} \notin U_1$. Обращаясь к определению группы G_U, видим, что в группу G_{U_1} входит элемент a такой, что $M_a = \overline{M}$, и не входит элемент b такой, что $M_b = M$. Напротив, группе G_{U_2} принадлежит элемент b и не принадлежит элемент a. Таким образом, группы G_{U_1}, G_{U_2} различны. Остается воспользоваться тем фактом (см., например, [6]), что мощность семейства ультрафильтров булевой алгебры $\mathcal{B}$ равна 2^c. Теорема доказана.

Из утверждения 1, следствия из него и теорем 2, 3 вытекают следующие основные результаты.

Теорема 4. *Пусть G — счетная подгруппа группы G_2^N и $G_2^d \subseteq G$. Тогда мощность семейства максимальных подгрупп группы $H_k^{-1}(G)$ континуальна. В частности, континуальной является мощность семейства максимальных подгрупп группы $\mathcal{A}_k$.*

Теорема 5. *Мощность семейства максимальных подгрупп группы $\mathcal{D}_k$ равна 2^c.*

ЛИТЕРАТУРА

1. **Алёшин С. В.** О базисах в группах автоматных подстановок // Дискретный анализ. Сб. научн. тр. Вып. 17. Новосибирск: Ин-т математики СО АН СССР, 1970. С. 3–8.
2. **Кон П.** Универсальная алгебра. М.: Мир, 1968.
3. **Кудрявцев В. Б.** О мощности множеств предполных множеств некоторых функциональных систем, связанных с автоматами // Проблемы кибернетики. Вып. 13. М.: Наука, 1965. С. 45–74.
4. **Мальцев А. И.** Алгебраические системы. М.: Наука, 1970.
5. **Мальцев А. И.** Алгоритмы и рекурсивные функции. М.: Наука, 1986.
6. **Марченков С. С.** О классах Слупецкого для детерминированных функций // Дискретная математика. 1998. Т. 10, вып. 2. С. 128–136.
7. **Роджерс Х.** Теория рекурсивных функций и эффективная вычислимость. М.: Мир, 1972.
8. **Яблонский С. В.** Введение в дискретную математику. М.: Наука, 1986.
9. **Friedberg R. M.** Three theorems on recursive enumeration. I. Decomposition. II. Maximal set. III. Enumeration without duplication // J. Symbolic Logic. 1958. V. 23, N 3. P. 309–316.

Адрес автора:

МГУ, факультет ВМиК,
Воробьевы горы,
119992 Москва,
Россия.
E-mail: mathcyb@cs.msu.su

Статья поступила
1 сентября 2003 г.