О некоторых задачах выразимости в группах автоматных перестановок

В.В. Макаров

Пусть n - целое число, $n \geq 2$. Пусть $E_n = \{0, 1, \cdots, n-1\}$. Кольцо вычетов, состоящее из всех элементов множества E_n, с операциями $\oplus, \otimes$, обозначается, как обычно, через $\mathbf{Z}_n$. Пусть S_n - полная симметрическая группа всех перестановок $f(x)$ на множестве E_n. Если $f, g \in S_n$, то обозначим $f(x)g(x) = g(f(x))$. Пусть $\tau(x)$ - перестановка из S_n такая, что $\tau(0) = 1, \tau(1) = 0, \tau(a) = a$ при $a \notin E_2$. Как известно, перестановки $\tau(x), x \oplus 1$ порождают группу S_n.

Группа AD_n автоматных перестановок состоит из всех одноместных детерминированных функций, заданных инициальными автоматами [1] A вида $A = (E_n, Q, E_n, \varphi, \psi, w)$, где E_n - алфавит входных и выходных символов, Q - не обязательно конечное множество состояний, $\varphi : Q \times E_n \to Q$ - функция переходов, $\psi : Q \times E_n \to E_n$ - функция выходов, w - начальное состояние, причем автомат A должен обладать свойством:

$$\forall q \in Q \exists m_q \in E_n (\psi(q, x) = x \oplus m_q).$$

Подгруппа в AD_n, состоящая из ограниченно - детерминированных функций [1], обозначается через AZ_n. Заметим, что AZ_n содержит бесконечную конечно - порожденную периодическую подгруппу [2].

Группа DS_n автоматных перестановок состоит из всех одноместных детерминированных функций, заданных инициальными автоматами A вида $A = (E_n, Q, E_n, \varphi, \psi, w)$, обладающими свойством:

$$\forall q \in Q \exists f_q(x) \in S_n (\psi(q, x) = f_q(x)).$$

Подгруппа в DS_n, состоящая из ограниченно - детерминированных функций, обозначается через AS_n [1].

Верны следующие групповые включения:

$$DS_n \supset AS_n \supset AZ_n, DS_n \supset AD_n \supset AZ_n.$$

Пусть $\mathcal{D}_n = \{A = (E_n, Q, E_n, \varphi, \psi, w) \in AS_n :$

$$\exists q \in Q \forall q_1 \in q((\psi(q, x) = x \oplus 1) \wedge ((q_1 = q) \vee (\psi(q_1, x) = x)))\}.$$

Таким образом, в систему $\mathcal{D}_n$ входят те автоматы из AS_n, на диаграмме Мура [1] которых лишь в единственном состоянии реализуется функция $x \oplus 1$, а в остальных состояниях реализуется тождественная функция входа.

Пусть $\mathcal{T}_n = \{A = (E_n, Q, E_n, \varphi, \psi, w) \in AS_n :$

$$\exists q \in Q \forall q_1 \in q((\psi(q, x) = \tau(x)) \wedge ((q_1 = q) \vee (\psi(q_1, x) = x)))\}.$$

Таким образом, в систему $\mathcal{T}_n$ входят те автоматы из AS_n, на диаграмме Мура [1] которых лишь в единственном состоянии реализуется функция $\tau(x)$, а в остальных состояниях реализуется тождественная функция входного значения.

Пусть также $S(n) = \mathcal{D}_n \cup \mathcal{T}_n$.

Через E_n^m мы обозначим множество всех слов длины m, состоящих из букв алфавита E_n. Через E_n^* мы обозначим множество всех слов конечной длины, составленных из элементов алфавита E_n. Суперпозицию автоматных отображений A и B обозначим как $A \circ B$ и будем считать: если $C = A \circ B$, то при любом $\alpha \in E_n^*$ имеет место $C(\alpha) = B(A(\alpha))$.

Определение. Пусть $A \in AD_n$. Пусть для $\alpha \in E_n^*$ через q_α обозначено состояние, в которое автомат A переходит из начального состояния w по входному слову α. Пусть $\psi(q_\alpha, x) = x \oplus m_{q_\alpha}$. Характеристической последовательностью $\{\chi_t^A : t \geq 0\}$ автомата А называется следующая последовательность чисел χ_t^A из E_n :

$$\chi_0^A = m_w,$$

а при $t \geq 1$

$$\chi_t^A = \sum_{\alpha \in E_n^t} m_{q_\alpha} \pmod{n}.$$

Если $A, B \in AD_n$ и $C = A \circ B$, то при любом $t \geq 0$ имеет место: $\chi_t^C = \chi_t^A \oplus \chi_t^B$, что нетрудно проверить непосредственно.

При $\alpha \in E_n^*$ через α^∞ обозначим сверхслово [1]: $\alpha\alpha\cdots\alpha\cdots$.

Определим систему $\Im_n$ в группе AD_n следующим образом:

$$\Im_n = \{A \in AD_n : \chi_t^A = 1 \qquad \text{при всех} \qquad t \geq 0\}.$$

Все элементы системы $\Im_n$ имеют бесконечный порядок (индукцией по N легко проверяется, что отображения из $\Im_n$ действуют на каждом множестве E_n^N как циклическая перестановка порядка n^N).

Лемма 1. *Пусть $A \in DS_n$. Пусть $W = \{\alpha 0^\infty : \alpha \in E_n^*\}$. Пусть существует ξ из множества сверхслов W, такое, что значение $A(\xi)$ отображения A на сверхслове ξ не принадлежит W, но для любого η из W имеет место $A^{-1}(\eta) \in W$, то есть обратное к A отображение A^{-1} сохраняет множество W. Тогда отображение A имеет бесконечный порядок.*

Теорема 1. *Группа AZ_n порождается элементами бесконечного порядка.*

Теорема 2. *Группа AD_n порождается элементами бесконечного порядка.*

Лемма 2. *Множество $S(n)$ является порождающей системой для группы AS_n.*

Теорема 3. *Группа AS_n порождается элементами бесконечного порядка.*

Доказательства приводятся в работе автора [3].

Заметим, что в [3] мы эффективным образом построили порождающую систему из элементов бесконечного порядка для групп AS_n, AZ_n (существует алгоритм, определяющий принадлежность произвольного автомата группы предложенным порождающим системам, состоящим из элементов бесконечного порядка).

Однако неизвестно, существует ли эффективная процедура определения порядка произвольного конечного автомата даже в группе AS_2.

Заметим также, что неизвестно, порождают ли все элементы порядка 2 группу AS_2.

Если рассматривать группу AD_p как функциональную систему с алгебраической операцией суперпозиции и топологической операцией замыкания (то есть с оператором А - полноты, [1]), то элементы порядка р порождают AD_p при простом числе р.

Отметим, что вопрос о том, автоматы каких порядков входят в систему $S(n)$, является открытым даже для случая $n = 2$ (в случае $n = 2$ множества $\mathcal{D}_n$ и $\mathcal{T}_n$ совпадают). В группе AS_2 все элементы конечного порядка имеют порядки, являющиеся степенями 2 [1]. Известно, что система $S(2)$ содержит элементы первого, второго, четвертого (результат автора [4]) и бесконечного порядка. Неизвестно, содержатся ли в системе $S(2)$ элементы каких - либо других порядков (например, восьмого).

Заметим, что если $A_1 \in S(2)$ и $A_1 \neq E$, где E - единица автоматной группы, $A_1 = (E_2, \{1, \cdots, n\}, E_2, \varphi, \psi, w), \psi(1, x) = x \oplus 1$, то автомат $A_0 = (E_2, \{1, \cdots, n\}, E_2, \varphi, \psi, 1)$ имеет порядок, равный порядку автомата A_1.

Пусть A_0 - элемент системы $S(2)$, 1 - начальное состояние A_0 и в этом состоянии реализуется нетождественная выходная функция $\psi(1, x) = x \oplus 1$. Предположим, что автомат A_0 имеет порядок, больший 2: $|A_0| > 2$. Очевидно, что для автомата $A_0 = (E_2, \{1, \cdots, n\}, E_2, \varphi, \psi, 1)$ выполнено следующее:

$$\exists \gamma \in E_2^* \exists \delta \in E_2 (q_{\delta\gamma} = 1, q_{A_0(\delta\gamma)} \neq 1).$$

Напомним, что для $\beta \in E_2^*$ через q_β обозначено состояние, в которое автомат A_0 переходит из начального состояния 1 по входному слову β.

Из всех слов γ, обладающих вышеприведенным свойством, выберем слово наименьшей длины (таких, вообще говоря, несколько) и обозначим его через α. Это слово α назовем разделяющим. Не ограничивая общности, можно считать, что $\delta = 0$.

Очевидно:

$$q_{0\alpha} = 1, q_{1\alpha} \neq 1, A_0(0\alpha) = 1\alpha, A_0(1\alpha) = 0\alpha.$$

Имеет место:

Лемма 3. *Если порядок автомата A_0 равен 4, то автомат A_0 имеет следующую орбиту мощности 4 из сверхслов $R_{00}, R_{01}, R_{10}, R_{11}$ для каждого разделяющего слова α :*

$$R_{ab} = (a \oplus b \oplus 1) \qquad \alpha \qquad (a\alpha_1 \qquad b\alpha_2) \qquad (a\alpha_3 \qquad b\alpha_4) \cdots$$

$$\cdots \qquad (a\alpha_{2k+1} \qquad b\alpha_{2k})\cdots,$$
$$a, b \in E_2,$$

где

$$\alpha_1, \alpha_2, \cdots, \alpha_n, \cdots$$

- некоторые начальные фрагменты слова α.

Используя вышеприведенную Лемму, можно построить элемент системы $S(2)$ четвертого порядка. Диаграмма этого автомата (минимальный по числу состояний на диаграмме Мура элемент 4 - го порядка системы $S(2)$ имеет 8 состояний) приводится в работе автора [4].

Теорема 4. *В группе AS_2 для произвольного натурального числа k существует автомат, имеющий ровно k отрицаний на диаграмме Мура порядка 2^{k+1}. (См. [5].)*

В заключение приведем одно интересное достаточное условие бесконечности порядка автомата из группы AS_2.

Пусть $A \in AS_2$ и задан диаграммой с алфавитом состояний $Q = \{1, \cdots, n\}$, причем в состояниях из множества $M_1 = \{1, \cdots, k\}$ реализуется отрицание входного значения, а в остальных состояниях - тождественная функция входного значения. Пусть 1 - начальное состояние. Пусть при произвольном $t \geq 2$ определено $M_t = \{i \in Q : \exists a_i \in E_2(\varphi(i, a_i) \in M_{t-1}, \varphi(i, a_i \oplus 1) \notin M_{t-1}.)\}$

Очевидно, что для любого t $M_t \subseteq Q$, следовательно, последовательность $\{M_t\}$ (называемая *гомологической*) является периодической.

Теорема 5. *Пусть гомологическая последовательность автомата A имеет вид:*
$$M_1, \cdots, M_T, M_1, \cdots, M_T, \cdots.$$
Тогда автомат A имеет бесконечный порядок.

Заметим, что в работе [5] также изучены топологические характеристики групп автоматных перестановок AS_2 и AD_2. Они бывают полезны при прояснении ряда автоматных и теоретико - групповых свойств автоматных групп. В определенной метрике дискретными подгруппами являются лишь конечные подгруппы AD_2, есть открыто - замкнутые множества, компактная группа AD_2 не является группой Ли (как локально компактная группа, в каждой окрестности единицы которой содержится нетривиальная подгруппа).

Автор выражает благодарность Алешину С.В. за руководство работой и Кудрявцеву В.Б. за ценные советы по представлению результатов и многочисленные консультации.

Список литературы

[1] Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Введение в теорию автоматов. - М. : Наука, 1985.

[2] Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. - М. : Наука, 1982.

[3] Макаров В.В. Группа автоматных перестановок AS_n порождается элементами бесконечного порядка//Дискретная математика. - 1997. - Том 9. - Вып.3.

[4] Макаров В.В. О порядках элементов группы автоматных перестановок// Вестник МГУ. Сер.1. Мат.,мех. - 1991. - Вып.4. - С. 86 - 87.

[5] Макаров В.В. О группах автоматных перестановок// Фундаментальная и прикладная математика. - 1996. - Том 2. - Вып.1. - С. 171 - 186.