Math-Net.Ru

Общероссийский математический портал

В. В. Макаров, Группа автоматных перестановок AS_n порождается элементами бесконечного порядка, *Дискрет. матем.*, 1997, том 9, выпуск 3, 117–124

DOI: <https://doi.org/10.4213/dm486>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 52.87.193.239

26 апреля 2023 г., 10:48:11

Группа автоматных перестановок AS_n порождается элементами бесконечного порядка

© 1997 г. В. В. Макаров

Для произвольного целого числа $n \geq 2$ изучается группа AS_n , состоящая из ограниченно-детерминированных функций одного переменного, задаваемых инициальными автоматами с конечным числом состояний на диаграмме Мура, с входным и выходным алфавитом $E_n = \{0, 1, \dots, n-1\}$, в каждом состоянии q которых реализуется выходная функция $\psi(q, x)$, равная некоторой перестановке $f_q(x)$ на множестве E_n , $f_q(x)$ — элемент полной симметрической группы S_n . Для AS_n в явном виде найдена порождающая система из элементов бесконечного порядка.

Пусть n — целое число, $n \geq 2$. Наибольший общий делитель целых чисел a и b обозначим через (a, b) . Пусть

$$E_n = \{0, 1, \dots, n-1\}, \quad M_1 = \{a \in E_n : (a, n) \neq 1\}.$$

Кольцо вычетов, состоящее из всех элементов множества E_n , с операциями сложения $\oplus$, вычитания $\ominus$ и умножения $\otimes$ по модулю n мы обозначим через Z_n , $Z_n = (E_n, \oplus, \ominus, \otimes)$. Пусть $Z_n^* = \{a \in E_n : (a, n) = 1\}$. Пусть S_n — полная симметрическая группа всех перестановок $f(x)$ на множестве E_n . Если $f, g \in S_n$ и $x \in E_n$, 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 $a \notin E_2$. Известно, что перестановки $\tau(x)$ и $x \oplus 1$ 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 — множество состояний (не обязательно конечное), $\varphi: Q \times E_n \rightarrow Q$ — функция переходов, $\psi: Q \times E_n \rightarrow E_n$ — 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 [1]. Заметим, что AZ_n содержит бесконечную конечнопорожденную периодическую подгруппу [2]. Группа DS_n автоматных перестановок состоит из всех одноместных детерминированных функций, заданных инициальными

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 $\eta \in W$ имеет место включение $A^{-1}(\eta) \in W$, то есть обратное к A отображение A^{-1} сохраняет множество W . Тогда автомат A имеет бесконечный порядок.

Доказательство. Если предположить, что $|A| < \infty$, то при некотором m имеет место равенство $A = (A^{-1})^m$ и для любого сверхслова η вида $\alpha 0^\infty$ для некоторого $\alpha \in E_n^*$ выходное сверхслово $A(\eta)$ имеет вид $\beta 0^\infty$ при некотором $\beta \in E_n^*$. Получили противоречие. Лемма доказана.

Теорема 1. Группа AZ_n порождается элементами бесконечного порядка.

Доказательство. Пусть $A \in AZ_n$. Пусть $\{\chi_t^A\}$ — характеристическая последовательность автомата A . Пусть A задан диаграммой Мура и имеет N состояний $1, \dots, N$. Пусть w — начальное состояние. Пусть при $1 \leq i, j \leq N$ определен a_{ij} — остаток от деления на n числа ориентированных ребер на диаграмме автомата A , направленных из состояния i в состояние j . Таким образом, определена матрица $M = \|a_{ij}\|$, $1 \leq i, j \leq N$, пусть M^t — t -я степень матрицы M над кольцом Z_n . Пусть $M^t = \|a_{ij}^{(t)}\|$, $1 \leq i, j \leq N$. Пусть при $1 \leq i \leq N$

$$\psi(i, x) = x \oplus m_i,$$

где ψ — функция выходов автомата A . Стандартным в теории графов методом (индукция по t) показывается, что при любом $t \geq 1$

$$\chi_t^A = \sum_{i=1}^N m_i a_{wi}^{(t)} \pmod{n}.$$

Таким образом, существуют $-1 \leq r \leq n^{N^2}$ и $T \geq 1$ такие, что при любых $a = 1, \dots, T-1$ и $m \geq 1$

$$\chi_{r+a}^A = \chi_{r+a+Tm}^A.$$

Пусть $D = \{0, 1, \dots, r\}$, при $r = -1$ полагаем D пустым. Определим при $d \in E_n$ и $d \neq 1$ множества

$$U_d = \{u \in D : \chi_u^A = d\},$$

пусть $U_d = \{u_{d,1}, \dots, u_{d,L_d}\}$,

$$V_d = \{v : 1 \leq v \leq T, \chi_{r+v}^A = d\},$$

пусть $V_d = \{v_{d,1}, \dots, v_{d,N_d}\}$.

На рис. 1 изображена диаграмма автомата $B(m; T; h)$ при $m \geq 0$, $T \geq 1$, $h \in E_n$, $h \neq 0$, необходимого нам далее. На рис. 2 приводится диаграмма автомата $B^{-1}(m; T; h)$, обратного к $B(m; T; h)$. В силу леммы 1 (в качестве ξ взять 0^∞) автоматы $B(m; T; h)$ имеют бесконечный порядок. Рассмотрим также автоматы $C(m; h)$ при $m \geq 0$, $h \in E_n$, $h \neq 0$, их диаграммы приводятся на рис. 3. Определим автоматы T_i равенством

$$T_i = C(u_{i,1}; 1 \oplus i) \circ \dots \circ C(u_{i,L_i}; 1 \oplus i), \quad i \in E_n, \quad i \neq 1.$$

Рис. 1.

Рис. 2.

Рис. 3.

Определим также автоматы H_i при $i \in E_n, i \neq 1$, равенством

$$H_i = B(v_{i,1} + r; T; 1 \ominus i) \circ \dots \circ B(v_{i,N_i} + r; T; 1 \ominus i).$$

Пусть

$$T = T_0 \circ T_2 \circ \dots \circ T_{n-1}, \quad H = H_0 \circ H_2 \circ \dots \circ H_{n-1}.$$

Рассмотрим автомат R , равный $T \circ H \circ A$. Очевидно, что $R \in \mathfrak{B}_{n,1}$, и, следовательно, автомат R имеет бесконечный порядок. Очевидно, что $A = H^{-1} \circ T^{-1} \circ R$.

Рассмотрим при $m \geq 0$ и $h \in E_n, h \neq 0$, автоматы $F(m; h)$ и $G(m; h)$, их диаграммы приводятся на рис. 4. В силу леммы 1 (взять $\xi = 0^\infty$) автомат $F(m; h)$ бесконечного порядка, также очевидно, что автомат $G(m; h)$ имеет бесконечный порядок (порядок автомата $G(m; h)$ равен порядку автомата I , имеющего ту же диаграмму, что и автомат $G(m; h)$, но другое начальное состояние: с выходной нетождественной функцией, автомат I действует на каждом множестве E_n^t как циклическая перестановка порядка n_1^t при некотором $n_1, n_1 > 1$). Очевидно, что $C(m; h) = F(m; h) \circ G(m; h)$. Теорема 1 доказана.

Теорема 2. Группа AD_n порождается элементами бесконечного порядка.

Доказательство. Пусть $A \in AD_n$ и определена $\{\chi_t^A\}$. Пусть $U = \{u: \chi_u^A \neq 1\}$. Если множество U конечно, рассуждения аналогичны вышеприведенным. Пусть U бесконечно. Определим B из AD_n посредством задания его информационного дерева [1]. На дереве автомата B рассмотрим пути вида $0 \dots 0$ (u раз, где $u \in U$) с началом в корне дерева и расположим в их концах q с выходной функцией $\psi(q, x)$, равной $x \oplus (1 \ominus \chi_u^A)$. В остальных вершинах дерева расположим состояния с тождественной выходной функцией. В силу леммы 1 (взять $\xi = 0^\infty$) порядок отображения B бесконечен. Заметим, что $B \circ A \in \mathfrak{B}_n$ и $|B \circ A| = \infty$. Очевидно, $A = B^{-1} \circ (B \circ A)$. Теорема 2 доказана.

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

Доказательство. Рассмотрим произвольный автомат A из AS_n . Пусть

$$A = (E_n, Q, E_n, \varphi_1, \psi_1, 1),$$

где $Q = \{1, \dots, N\}$. Пусть

$$\psi_1(i, x) = \pi_i(x) \in S_n, \quad i \in Q.$$

Найдутся натуральные числа m_i и найдутся при $1 \leq j \leq m_i$ перестановки $\rho_{i,j}(x) \in \{\tau(x), x \oplus 1\}$ такие, что имеют место представления

$$\pi_i(x) = \rho_{i,1}(x) \dots \rho_{i,m_i}(x).$$

При $t \in Q$ и $r = 1, \dots, m_t$ определим автоматы $A_{t,r}$ вида

$$A_{t,r} = (E_n, Q, E_n, \varphi_{t,r}, \psi_{t,r}, 1)$$

следующим образом:

$$\begin{aligned} \psi_{t,r}(t, x) &= \rho_{t,r}(x), \\ \psi_{t,r}(i, x) &= x, & i \neq t, \\ \varphi_{1,1}(i, x) &= \varphi_1(i, x), & i \in Q, \\ \varphi_{t,r}(i, (\rho_{i,1} \dots \rho_{i,m_i})(x)) &= \varphi_{1,1}(i, x), & 1 \leq i < t, \\ \varphi_{t,r}(i, x) &= \varphi_{1,1}(i, x), & t < i \leq N, \\ \varphi_{t,r}(t, (\rho_{t,1} \dots \rho_{t,r-1})(x)) &= \varphi_{1,1}(t, x), & 2 \leq r \leq m_t, \\ \varphi_{t,1}(t, x) &= \varphi_{1,1}(t, x). \end{aligned}$$

Пусть при $1 \leq i \leq N$

$$B_i = A_{i,1} \circ \dots \circ A_{i,m_i}.$$

Тогда имеет место равенство $A = B_1 \circ \dots \circ B_N$. Очевидно, что $A_{t,r} \in \mathfrak{D}_n \cup \mathfrak{F}_n$. Лемма доказана.

Лемма 3. Система $\mathfrak{F}_n$ содержится в подгруппе группы AS_n , порожденной всеми элементами бесконечного порядка группы AS_n .

Доказательство. Пусть $A \in \mathfrak{F}_n$. Пусть B — сужение отображения A на множество E_2^* . Так как при $n = 2$ имеем равенство групп $AZ_2 = AS_2$, определена характеристическая последовательность $\{\chi_t^B\}$. Рассмотрим в случае $n = 2$ автоматы $B(m; T; h)$, $C(m; h)$, $F(m; h)$, $G(m; h)$. Определим автомат $F'(m; h)$ вида $(E_n, Q, E_n, \varphi, \psi, w)$ с условием $F'(m; h)(\alpha) = F(m; h)(\alpha)$ при $\alpha \in E_2^*$, и $\varphi(q, x) = q$ и $\psi(q, x) = x$ при $x \notin E_2$, $q \in Q$. Аналогично определим автоматы $B'(m; T; h)$, $C'(m; h)$, $G'(m; h)$. Очевидно, что $C'(m; h) = F'(m; h) \circ G'(m; h)$, а $B'(m; T; h)$, $F'(m; h)$, $G'(m; h)$ имеют бесконечный порядок. Аналогично теореме 1 строим автомат R . Очевидно, что $|R| = \infty$ (если бы при некотором P имело место равенство $|R| = P$, то сужение автомата R^P на E_2^* давало бы тождественное отображение). Аналогично теореме 1 строится схема из автоматов

$$R, (B'(m; T; h))^{-1}, (F'(m; h))^{-1}, (G'(m; h))^{-1}$$

бесконечного порядка, реализующая отображение A . Лемма доказана.

Легко видеть, что система $\mathfrak{D}_n$ лежит в группе AZ_n . Из теоремы 1 и лемм 2, 3 сразу получается следующее утверждение.

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

В заключение заметим, что вопрос о том, автоматы каких порядков входят в систему $S(n)$, является открытым даже для случая $n = 2$ (в случае $n = 2$ множества $\mathfrak{D}_n$ и $\mathfrak{F}_n$ совпадают). Известно, что система $S(2)$ содержит элементы первого, второго, четвертого (результат автора) и бесконечного порядков. Неизвестно, содержатся ли в системе $S(2)$ элементы других порядков, например, восьмого порядка.

Заметим также, что мы эффективным образом построили порождающую систему из элементов бесконечного порядка для группы AZ_n (существует алгоритм, определяющий принадлежность произвольного автомата группы AZ_n предложенной нами порождающей системе из элементов бесконечного порядка). Однако неизвестно, существует ли эффективная процедура определения порядка произвольного конечного автомата из группы AZ_n . Заметим также, что неизвестно, порождают ли все элементы порядка p группу AZ_p (даже для $p = 2$) в случае простого p . Если рассматривать группу AD_p как функциональную систему с алгебраической операцией суперпозиции и топологической операцией замыкания (то есть с оператором A -полноты [1]), то элементы порядка p порождают AD_p при простом натуральном p .

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. *Введение в теорию автоматов*. Наука, Москва, 1985.
2. Каргаполов М. И., Мерзляков Ю. И. *Основы теории групп*. Наука, Москва, 1982.

Статья поступила 02.06.1993.

Переработанный вариант поступил 05.01.1995.