

ПРЕДСТАВЛЕНИЕ АВТОМАТОВ ГРУППАМИ

Рассматривается задача представления абстрактных автоматов конечными группами. Доказана универсальность предложенного представления и исследуются его свойства.

Розглядається задача зображення абстрактних автоматів скінченними групами. Доведена універсальність запропонованого зображення та досліджуються його властивості.

Абстрактный автомат представляет собой три абстрактных конечных множества и два определенных на них абстрактных отображения. Такой объект задается таблицами, определяющими отображения, или, что эквивалентно, взвешенным мультиграфом. Поэтому основным методом решения задачи теории абстрактных автоматов является поиск ситуаций в пространстве, построенном с помощью указанных таблиц, или на графе. В то же время абстрактный автомат является конечной алгебраической системой. Детализация ее структуры позволяет "арифметизировать" вычисления, осуществляемые абстрактным автоматом. Это дает возможность, во-первых, классифицировать автоматы в зависимости от вычисляемых ими функций и, во-вторых, существенно использовать при решении задач теории автоматов аппарат современной алгебры. Именно на основе такого подхода и был выделен специальный, достаточно узкий класс автоматов — линейные последовательностные машины [1].

В настоящей статье предложен общий метод представления абстрактных автоматов конечными группами. Доказана универсальность этого представления и исследуются его свойства. Понятия и обозначения в работе такие же, как и в [2–4].

Пусть \mathcal{A}_{mnk} , $m \geq 1$, $n \geq 1$, $k \geq 2$, — множество всех автоматов $A = (Q_k, X_m, Y_n, \delta_A, \lambda_A)$, имеющих фиксированное множество состояний $Q_k = \{q_1, \dots, q_k\}$, входной $X_m = \{x_1, \dots, x_m\}$ и выходной $Y_n = \{y_1, \dots, y_n\}$ алфавиты ($\delta_A: Q_k \times X_m \rightarrow Q_k$ и $\lambda_A: Q_k \times X_m \rightarrow Y_n$ — функции переходов и выходов автомата A). Запись $A = A'$ ($A, A' \in \mathcal{A}_{mnk}$) означает, что автоматы A и A' равны друг другу как алгебраические системы, т.е. $\delta_A = \delta_{A'}$ и $\lambda_A = \lambda_{A'}$. Рассмотрим группы $\mathcal{G}_1 = (G_1, \circ)$ и $\mathcal{G}_2 = (G_2, *)$. Обозначим через $F_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$, $m \geq 1$, $n \geq 1$, $k \geq 2$, множество всех упорядоченных наборов $\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6)$ из шести отображений, где $\varphi_1: Q_k \rightarrow G_1$, $\varphi_2: X_m \rightarrow G_1$, $\varphi_3: G_1 \rightarrow Q_k$, $\varphi_4: Q_k \rightarrow G_2$, $\varphi_5: X_m \rightarrow G_2$, $\varphi_6: G_2 \rightarrow Y_n$. Каждому набору $\Phi \in F_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$ поставим в соответствие такой автомат $B_\Phi = (q_k, X_m, Y_n, \delta_\Phi, \lambda_\Phi)$, что

$$\begin{aligned}\delta_\Phi(q, x) &= \varphi_3(\varphi_1(q) \circ \varphi_2(x)), \\ \lambda_\Phi(q, x) &= \varphi_6(\varphi_4(q) * \varphi_5(x))\end{aligned}\quad (1)$$

для всех $q \in Q_k$ и $x \in X_m$. Положим $\mathcal{A}_{mnk}(\mathcal{G}_1, \mathcal{G}_2) = \{B_\Phi \mid \Phi \in F_{mnk}(\mathcal{G}_1, \mathcal{G}_2)\}$. Ясно, что для любых групп \mathcal{G}_1 и \mathcal{G}_2 при всех $m \geq 1$, $n \geq 1$ и $k \geq 2$ справедливо соотношение

$$\emptyset \neq \mathcal{A}_{mnk}(\mathcal{G}_1, \mathcal{G}_2) \subseteq \mathcal{A}_{mnk} \quad (2)$$

Определение 1. Представлением автомата $A \in \mathcal{A}_{mnk}$ группами \mathcal{G}_1 и \mathcal{G}_2

назовем такой упорядоченный набор отображений $\Phi_A = (\varphi_1^A, \varphi_2^A, \varphi_3^A, \varphi_4^A, \varphi_5^A, \varphi_6^A) \in F_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$, что $A = B_{\Phi_A}$ ($B_{\Phi_A} \in \mathcal{U}_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$).

Зафиксируем группы $\mathcal{G}_1 = (G_1, \circ)$ и $\mathcal{G}_2 = (G_2, *)$, а также значения $m \geq 1$, $n \geq 1$ и $k \geq 2$. Предположим, что для автомата $A \in \mathcal{U}_{mnk}$ существует его представление $\Phi_A \in F_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$ группами \mathcal{G}_1 и \mathcal{G}_2 . Так как $A = B_{\Phi_A}$, то $\delta_A = \delta_{\Phi_A}$ и $\lambda_A = \lambda_{\Phi_A}$. Из последних двух равенств и из (1) вытекает справедливость следующих утверждений:

$$(\forall q, q' \in Q_k)((\exists x \in X_m)(\delta_A(q, x) \neq \delta_A(q', x) \Rightarrow q \notin q'(\ker \varphi_1^A))),$$

$$(\forall q, q' \in Q_k)((\exists x \in X_m)(\lambda_A(q, x) \neq \lambda_A(q', x) \Rightarrow q \notin q'(\ker \varphi_4^A))),$$

$$(\forall q, x' \in X_m)((\exists q \in Q_k)(\delta_A(q, x) \neq \delta_A(q, x') \Rightarrow x \notin x'(\ker \varphi_2^A))),$$

$$(\forall q, x' \in X_m)((\exists q \in Q_k)(\lambda_A(q, x) \neq \lambda_A(q, x') \Rightarrow x \notin x'(\ker \varphi_5^A))).$$

Из этих утверждений, в частности, следует, что как число попарно различных строк, так и число попарно различных столбцов таблицы переходов (соответственно таблицы выходов) любого автомата $A \in \mathcal{U}_{mnk}$ принадлежащего множеству $\mathcal{U}_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$, не превышает $|G_1|$ (соответственно $|G_2|$). Следующая теорема указывает естественный способ расширения множества представлений автоматов $A \in \mathcal{U}_{mnk}$ при фиксированных значениях параметров $m > 1$, $n \geq 1$ и $k \geq 2$.

Теорема 1. Если группы $\mathcal{G}_1, \mathcal{G}'_1$ и $\mathcal{G}_2, \mathcal{G}'_2$ удовлетворяют условиям

$$\mathcal{G}_i \leq \mathcal{G}'_i, \quad i = 1, 2, \quad (3)$$

то включение

$$\mathcal{U}_{mnk}(\mathcal{G}_1, \mathcal{G}_2) \subseteq \mathcal{U}_{mnk}(\mathcal{G}'_1, \mathcal{G}'_2) \quad (4)$$

справедливо для всех $m \geq 1, n \geq 1$ и $k \geq 2$.

Доказательство. Пусть группы $\mathcal{G}_1 = (G_1, \circ), \mathcal{G}_2 = (G_2, *)$, $\mathcal{G}'_1 = (G'_1, \circ)$ и $\mathcal{G}'_2 = (G'_2, *)$ удовлетворяют условиям (3). Зафиксируем значения $m \geq 1, n \geq 1$ и $k \geq 2$. Выберем произвольный автомат $B_\Phi = (Q_k, X_m, Y_n, \delta_\Phi, \lambda_\Phi) \in \mathcal{U}_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$, где $\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6) \in F_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$. Из условий (3) вытекает, что справедливы включения $G_i \subseteq G'_i, i = 1, 2$. Поэтому существует упорядоченный набор отображений $\Phi' = (\varphi'_1, \varphi'_2, \varphi'_3, \varphi'_4, \varphi'_5, \varphi'_6) \in F_{mnk}(\mathcal{G}'_1, \mathcal{G}'_2)$, удовлетворяющий следующим трем условиям:

$$1) \varphi'_1(q) = \varphi_1(q) \text{ и } \varphi'_4(q) = \varphi_4(q) \text{ для всех } q \in Q_k;$$

$$2) \varphi'_2(x) = \varphi_2(x) \text{ и } \varphi'_4(x) = \varphi_4(x) \text{ для всех } x \in X_m;$$

$$3) \varphi'_3|_{G_1} = \varphi_3 \text{ и } \varphi'_6|_{G_2} = \varphi_6.$$

Рассмотрим автомат $B_{\Phi'} = (Q_k, X_m, Y_n, \delta_{\Phi'}, \lambda_{\Phi'}) \in \mathcal{U}_{mnk}(\mathcal{G}'_1, \mathcal{G}'_2)$. В силу (1) для всех $q \in Q_k$ и $x \in X_m$

$$\delta_{\Phi'}(q, x) = \varphi'_3(\varphi'_1(q) \circ \varphi'_2(x)) = \varphi'_3(\varphi_1(q) \circ \varphi_2(x)),$$

$$\lambda_{\Phi'}(q, x) = \varphi'_6(\varphi'_4(q) * \varphi'_5(x)) = \varphi'_6(\varphi_4(q) * \varphi_5(x)).$$

А так как \mathfrak{G}_1 и \mathfrak{G}_2 — группы, то справедливы следующие утверждения:

$$\varphi_1(q), \varphi_2(x) \in G_1 \Rightarrow \varphi_1(q) \circ \varphi_2(x) \in G_1,$$

$$\varphi_4(q), \varphi_5(x) \in G_2 \Rightarrow \varphi_4(q) * \varphi_5(x) \in G_2.$$

Поэтому для всех $q \in Q_k$ и $x \in X_m$

$$\delta_{\Phi'}(q, x) = \varphi'_3|_{G_1}(\varphi_1(q) \circ \varphi_2(x)) = \varphi_3(\varphi_1(q) \circ \varphi_2(x)) = \delta_{\Phi}(q, x),$$

$$\lambda_{\Phi'}(q, x) = \varphi'_6|_{G_2}(\varphi_4(q) * \varphi_5(x)) = \varphi_6(\varphi_4(q) * \varphi_5(x)) = \lambda_{\Phi}(q, x).$$

Это означает, что $B_{\Phi} = B_{\Phi'}$. Итак, для каждого автомата $B_{\Phi} \in \mathcal{U}_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$ существует равный ему автомат $B_{\Phi'} \in \mathcal{U}_{mnk}(\mathfrak{G}'_1, \mathfrak{G}'_2)$. Следовательно, включение (4) справедливо. Теорема доказана.

Следствие 1. Пусть последовательности групп $\{\mathfrak{G}_1^{(j)} \mid j \in N\}$ и $\{\mathfrak{G}_2^{(j)} \mid j \in N\}$ удовлетворяют условиям

$$\mathfrak{G}_i^{(1)} \leq \mathfrak{G}_i^{(2)} \leq \dots \leq \mathfrak{G}_i^{(j)} \leq \dots, \quad i = 1, 2.$$

Тогда

$$\emptyset \neq \mathcal{U}_{mnk}(\mathfrak{G}_1^{(1)}, \mathfrak{G}_2^{(1)}) \subseteq \dots \subseteq \mathcal{U}_{mnk}(\mathfrak{G}_1^{(j)}, \mathfrak{G}_2^{(j)}) \subseteq \dots \subseteq \mathcal{U}_{mnk}.$$

Справедливость следствия 1 непосредственно вытекает из (2) и (4).

Обозначим через $\mathfrak{Z} = (Z_l, +)$, $l \geq 2$, аддитивную группу вычетов по модулю

l . Следующая теорема показывает, что при соответствующем выборе групп \mathfrak{G}_1 и \mathfrak{G}_2 достигается верхняя граница, устанавливаемая соотношением (2).

Теорема 2. Пусть $m \geq 1$, $n \geq 1$ и $k \geq 2$ — фиксированные числа. Если группы \mathfrak{G}_1 и \mathfrak{G}_2 удовлетворяют условиям

$$\mathfrak{Z}_{l_1} \leq \mathfrak{G}_i, \quad i = 1, 2, \quad (5)$$

$$\min\{l_1, l_2\} \geq mk, \quad (6)$$

то справедливо равенство

$$\mathcal{U}_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2) = \mathcal{U}_{mnk}. \quad (7)$$

Доказательство. Покажем, что из (5) и (6) вытекает справедливость включения

$$\mathcal{U}_{mnk}(\mathfrak{Z}_{l_1}, \mathfrak{Z}_{l_2}) \supseteq \mathcal{U}_{mnk} \quad (8)$$

Выберем произвольный автомат $A = (Q_k, X_m, Y_n, \delta_A, \lambda_A) \in \mathcal{U}_{mnk}$. В силу (6) существует такой набор $\Phi_A = (\varphi_1^A, \varphi_2^A, \varphi_3^A, \varphi_4^A, \varphi_5^A, \varphi_6^A) \in F_{mnk}(\mathfrak{Z}_{l_1}, \mathfrak{Z}_{l_2})$, что: 1) $\varphi_1^A(q_i) = \varphi_4^A(q_i) = i - 1$ для всех $i \in \{1, \dots, k\}$; 2) $\varphi_2^A(x_j) = \varphi_5^A(x_j) = (j - 1)k$ для всех $j \in \{1, \dots, m\}$; 3) отображения $\varphi_3^A: \mathfrak{Z}_{l_1} \rightarrow Q_k$ и $\varphi_6^A: \mathfrak{Z}_{l_2} \rightarrow Y_n$ удовлетворяют условиям

$$\varphi_3^A(r) = \delta_A(q_{R_k(r) + 1}, x_{\lfloor r/k \rfloor + 1}),$$

$$\varphi_6^A(r) = \lambda_A(q_{R_k(r) + 1}, x_{\lfloor r/k \rfloor + 1})$$

для всех $r \in \{0, 1, \dots, mk - 1\}$, где $R_b(a)$ — остаток от деления a на b , $a \lfloor c$ — целая часть числа c . Рассмотрим автомат $B_{\Phi_A} = (Q_k, X_m, Y_n, \delta_{\Phi_A}, \lambda_{\Phi_A}) \in \mathcal{U}_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$. В силу (1) для всех $q_i \in Q_k$ и $x_j \in X_m$

$$\delta_{\Phi_A}(q_i, x_j) = \varphi_3^A(\varphi_1^A(q_i) + \varphi_2^A(x_j)) = \varphi_3^A(i - 1 + (j - 1)k),$$

$$\lambda_{\Phi_A}(q_i, x_j) = \varphi_6^A(\varphi_4^A(q_i) + \varphi_5^A(x_j)) = \varphi_6^A(i - 1 + (j - 1)k).$$

Так как $i \in \{1, \dots, k\}$, то $R_k(i - 1 + (j - 1)k) = i - 1$ и $\lfloor (i - 1 + (j - 1)k) / k \rfloor = j - 1$.

Поэтому для всех $q_i \in Q_k$ и $x_j \in X_m$

$$\delta_{\Phi_A}(q_i, x_j) = \delta_A(q_{(i-1)+1}, x_{(j-1)+1}) = \delta_A(q_i, x_j),$$

$$\lambda_{\Phi_A}(q_i, x_j) = \lambda_A(q_{(i-1)+1}, x_{(j-1)+1}) = \lambda_A(q_i, x_j),$$

т.е. $A = B_{\Phi_A}$. Итак, для каждого автомата $A \in \mathcal{U}_{mnk}$ существует такой автомат

$B_{\Phi_A} \in \mathcal{U}_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$, что $A = B_{\Phi_A}$. Следовательно, включение (8) справедливо.

В силу теоремы 1 из (5) и (8) вытекает

$$\mathcal{U}_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2) \supseteq \mathcal{U}_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2) \supseteq \mathcal{U}_{mnk} \quad (9)$$

Из (2) и (9) непосредственно следует справедливость равенства (7). Теорема доказана.

Распространим функции переходов и выходов автомата $A = (Q_k, X_m, Y_n, \delta_A, \lambda_A) \in \mathcal{U}_{mnk}$ на множество $Q_k \times X_m^*$ обычным образом в соответствии с равенствами

$$\delta_A(q, e) = q, \quad \lambda_A(q, e) = e,$$

$$\delta_A(q, px) = \delta_A(\delta_A(q, p), x), \quad (10)$$

$$\lambda_A(q, px) = \lambda_A(q, p)\lambda_A(\delta_A(q, p), x),$$

где $q \in Q_k, p \in X_m^*, x \in X_m$, а e — пустое слово.

Из (1) и (10) вытекает, что для любых групп \mathfrak{G}_1 и \mathfrak{G}_2 представление Φ_A автомата $A \in \mathcal{U}_{mnk}$ на каждом такте осуществляет вычисления в соответствии со схемой: кодирование \rightarrow групповая операция \rightarrow декодирование.

При исследовании поведения автомата на множестве $Q_k \times X_m^*$ естественным является требование о том, чтобы для функции переходов кодирование осуществлялось только в начале функционирования, а декодирование — только в его конце. Выделим класс представлений, удовлетворяющих этому требованию.

Определение 2. Представление $\Phi_A = (\varphi_1^A, \varphi_2^A, \varphi_3^A, \varphi_4^A, \varphi_5^A, \varphi_6^A) \in \mathcal{U}_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$ автомата $A \in \mathcal{U}_{mnk}$ группами \mathfrak{G}_1 и \mathfrak{G}_2 назовем согласованным с функцией переходов, если

$$\delta_{\Phi_A}(q, p) = \varphi_3(\varphi_1(q) \circ \varphi_2(p))$$

при всех $q \in Q_k$ и $p \in X_m^*$.

Обозначим через $F_{mnk}^{(0)}(\mathcal{G}_1, \mathcal{G}_2)$ множество всех таких наборов $\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6) \in F_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$, что

$$\text{Val}\varphi_1 \circ \text{Val}\varphi_1 = \text{Val}\varphi_1, \quad (11)$$

$$(\forall q \in Q_k)(\varphi_3\varphi_1(q) = q' \Leftrightarrow q \equiv q'(\ker\varphi_1)). \quad (12)$$

Предложение 1. Если $\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6) \in F_{mnk}^{(0)}(\mathcal{G}_1, \mathcal{G}_2)$, то $(\varphi_1\varphi_3)|_{\text{Val}\varphi_1}$ — тождественное отображение.

Доказательство. Предположим, что $\Phi \in F_{mnk}^{(0)}(\mathcal{G}_1, \mathcal{G}_2)$. Выберем произвольное $q \in Q_k$. Пусть $\varphi_3\varphi_1(q) = q'$. Тогда $\varphi_1\varphi_3\varphi_1(q) = \varphi_1(q')$. Так как $\varphi_3\varphi_1(q) = q'$, то в силу (12) $\varphi_1(q) = \varphi_1(q')$. Следовательно, $\varphi_1\varphi_3\varphi_1(q) = \varphi_1(q)$ для всех $q \in Q_k$, т.е. $\varphi_1\varphi_3(\varphi_1(q)) = \varphi_1(q)$ для всех $\varphi_1(q) \in \text{Val}\varphi_1$. А это означает, что $(\varphi_1\varphi_3)|_{\text{Val}\varphi_1}$ — тождественное отображение. Предложение доказано.

Следствие 2. Если $\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6) \in F_{mnk}^{(0)}(\mathcal{G}_1, \mathcal{G}_2)$, то $\varphi_3|_{\text{Val}\varphi_1}$ и $\varphi_1|_{\text{Val}\varphi_3}$ — инъективные отображения.

Справедливость следствия 2 непосредственно вытекает из предложения 1. Положим

$$\mathcal{U}_{mnk}^{(0)}(\mathcal{G}_1, \mathcal{G}_2) = \{B_\Phi \in \mathcal{U}_{mnk}(\mathcal{G}_1, \mathcal{G}_2) \mid \Phi \in F_{mnk}^{(0)}(\mathcal{G}_1, \mathcal{G}_2)\}$$

Теорема 3. Функция переходов каждого автомата $B_\Phi \in \mathcal{U}_{mnk}^{(0)}(\mathcal{G}_1, \mathcal{G}_2)$ ($\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6) \in F_{mnk}^{(0)}(\mathcal{G}_1, \mathcal{G}_2)$) удовлетворяет равенству

$$\delta_\Phi(q, p) = \varphi_3(\varphi_3(q) \circ \varphi_3(p)) \quad (13)$$

при всех $q \in Q_k$ и $p \in X_m^+$.

Доказательство. Рассмотрим произвольный автомат $B_\Phi \in \mathcal{U}_{mnk}^{(0)}(\mathcal{G}_1, \mathcal{G}_2)$. Доказательство осуществим индукцией по длине входного слова.

Пусть $p \in X^+$ и $|p| = 1$. Тогда $p \in X_m$ и равенство (13) справедливо в силу (1).

Предположим, что (13) справедливо для всех $q \in Q_k$ и всех таких $p \in X_m^+$, что $|p| \leq l, l \geq 1$.

Пусть $p \in X_m^+$ и $|p| = l + 1$. Тогда $p = p'x$, где $|p'| = l$ и $x \in X_m$. Следовательно, $\delta_\Phi(q, p) = \delta_\Phi(q, p')x = \delta_\Phi(\delta_\Phi(q, p'), x) = \varphi_3(\varphi_1(\delta_\Phi(q, p'))) \circ \varphi_2(x)$ для всех $q \in Q_k$. В силу предположения индукции $\delta_\Phi(q, p') = \varphi_3(\varphi_1(q) \circ \varphi_2(p'))$. Поэтому $\delta_\Phi(q, p) = \varphi_3(\varphi_1\varphi_3(\varphi_1(q) \circ \varphi_2(p'))) \circ \varphi_2(x)$ для всех $q \in Q_k$. Так как $B_\Phi \in \mathcal{U}_{mnk}^{(0)}(\mathcal{G}_1, \mathcal{G}_2)$, то $\Phi \in F_{mnk}^{(0)}(\mathcal{G}_1, \mathcal{G}_2)$ и в соответствии с предположением 1 $(\varphi_1\varphi_3)|_{\text{Val}\varphi_1}$ — тождественное отображение. Отсюда вытекает, что $\delta_\Phi(q, p) = \varphi_3((\varphi_1(q) \circ \varphi_2(p')) \circ \varphi_2(x)) = \varphi_3(\varphi_1(q) \circ (\varphi_2(p') \circ \varphi_2(x))) = \varphi_3(\varphi_1(q) \circ \varphi_2(p))$ для всех $q \in Q_k$, что и требовалось доказать. Теорема доказана.

1. Гилл А. Линейные последовательностные машины. — М.: Наука, 1974. — 287с.
2. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. — М.: Наука, 1977. — 239с.
3. Мальцев А. И. Алгебраические системы. — М.: Наука, 1970. — 392с.
4. Трахтенброт Б. А., Барздин Я. М. Конечные автоматы (Поведение и синтез). — М.: Наука, 1970. — 400 с.

Получено 01.04.92