УДК 519.71

В. Г. Скобелев (Ин-т прикл. математики и механики НАН Украины, Донецк)

ПРЕДСТАВЛЕНИЕ АВТОМАТОВ ГРУППАМИ. II

We obtain necessary and sufficient conditions under which the representation of abstract automata in terms of finite groups is consistent with a function of automaton transitions. We obtain sufficient conditions under which the mapping of a free semigroup of automaton into a group performing by a component of the mapping is the homomorphism.

Одержано необхідні та достатні умови, при яких зображення абстрактних автоматів скінченними групами погоджено з функцією переходів автомата. Одержано достатні умови, при яких відображення вільної півгрупи автомата у групу, що здійснюється компонентою зображення, є гомоморфізмом.

Данная статья является продолжением работы [1], поэтому в ней сохранены введенные обозначения, предположения и продолжена нумерация формул и теорем.

В статье исследуется множество представлений абстрактных автоматов конечными группами, согласованных с функцией переходов. Получены необходимые и достаточные условия, при которых представление согласовано с функцией переходов автомата. Исследованы свойства компонент представления. Получены достаточные условия, при которых отображение, осуществляемое компонентой представления, является гомоморфизмом свободной входной полугруппы в группу. Понятия и обозначения в работе такие же, как и в [1 – 4].

Пусть $\mathfrak{G}_1 = (G_1, \circ)$ и $\mathfrak{G}_2 = (G_2, *)$ — заданные конечные группы. Обозначим через $F^c_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$ множество всех представлений $\Phi = (\varphi_1, \ldots, \varphi_G) \in$ $\in F_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$, согласованных с функцией переходов. В определении 2 свойство представления „быть согласованным с функцией переходов" сформулировано в терминах расширения отображения $\varphi_2 : X_m \to G_1$ на множество X^*_m. Именно свойства этого расширения и являются существенными для представлений $\Phi \in F^c_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$. Всюду в дальнейшем расширение отображения $\varphi_2 : X_m \to G_1$ на множество X^*_m будем обозначать через $\tilde{\varphi}_2$. В определениях представления, согласованного с функцией переходов, не фигурируют функция выходов автомата, выходной алфавит Y_n, группа $\mathfrak{G}_2$ и отображения φ_4, φ_5, φ_6. Поэтому все сформулированные ниже утверждения относительно представлений, согласованных с функцией переходов, справедливы при всех $n \geq 1$ и при любом выборе как группы $\mathfrak{G}_2$, так и отображений $\varphi_4 : Q_k \to G_2$, $\varphi_5 : X_m \to G_2$ и $\varphi_6 : G_2 \to Y_n$. Имеет место следующий критерий принадлежности представления $\Phi \in F_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$ множеству $F^c_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$.

Теорема 4. *Представление* $\Phi = (\varphi_1, \ldots, \varphi_6) \in F_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$ *согласовано с функцией переходов тогда и только тогда, когда существует такое расширение* $\tilde{\varphi}_2$ *отображения* $\varphi_2 : X_m \to G_1$ *на множество* X^*_m, *что для всех* $q \in$ $\in Q_k$, $p \in X^*_m$ *и* $x \in X_m$ *справедливы равенства*

$$\varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(px)) = \varphi_3(\varphi_1(\varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(p))) \circ \varphi_2(x)), \tag{14}$$

$$\varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(e)) = q. \tag{15}$$

Доказательство. Пусть $\Phi = (\varphi_1, \ldots, \varphi_6) \in F_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$. Из определения автомата B_Φ и из (10) следует, что для всех $q \in Q_k$, $p \in X^*_m$ и $x \in X_m$ справедливы равенства

$$\begin{aligned} \delta_\Phi(q,x) &= \varphi_3(\varphi_1(q)\circ\varphi_2(x)), \\ \delta_\Phi(q,e) &= q, \\ \delta_\Phi(q,px) &= \delta_\Phi(\delta_\Phi(q,p),x). \end{aligned} \tag{16}$$

Продолжим отображение $\varphi_2 : X_m \to G_1$ до отображения $\tilde\varphi_2 : X_m^* \to G_1$. В силу определения 2 представление $\Phi = (\varphi_1, \ldots, \varphi_6) \in F_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$ согласовано с функцией переходов тогда и только тогда, когда для всех $q \in Q_k$ и $p \in X_m^*$ справедливо равенство

$$\delta_\Phi(q,p) = \varphi_3(\varphi_1(q)\circ\tilde\varphi_2(p)). \tag{17}$$

Из (16) и (17) вытекает, что представление $\Phi = (\varphi_1, \ldots, \varphi_6) \in F_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$ согласовано с функцией переходов тогда и только тогда, когда существует такое расширение $\tilde\varphi_2$ отображения φ_2 на множество X_m^*, что для всех $q \in Q_k$, $p \in X_m^*$ и $x \in X_m$

$$\begin{gathered} q = \delta_\Phi(q,e) = \varphi_3(\varphi_1(q)\circ\varphi_2(e)), \\ \varphi_3(\varphi_1(q)\circ\tilde\varphi_2(px)) = \delta_\Phi(q,px) = \delta_\Phi(\delta_\Phi(q,p),x) = \\ = \delta_\Phi(\varphi_3(\varphi_1(q)\circ\tilde\varphi_2(p)),x) = \varphi_3(\varphi_1(\varphi_3(\varphi_1(q)\circ\tilde\varphi_2(p)))\circ\varphi_2(x)), \end{gathered}$$

т. е. когда справедливы равенства (14) и (15). Теорема доказана.

В теореме 4, с одной стороны, определены необходимые и достаточные условия, при которых тройка отображений $(\varphi_1, \varphi_2, \varphi_3)$ может быть использована для конструирования представления $\Phi \in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2)$, а с другой — описано строение отображений φ_2, допустимых для представлений $\Phi \in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2)$. Это описание дано через свойства расширения $\tilde\varphi_2$ отображения φ_2 на множество X_m^*, определяемые с помощью равенств (14) и (15). В следующих трех предложениях описывается строение отображений φ_1 и φ_3, допустимых для представлений $\Phi \in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2)$.

Предложение 2. *Если* $\Phi = (\varphi_1, \ldots, \varphi_6) \in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2)$, *то* $\varphi_1 : Q_k \to G_1$ *— инъективное отображение.*

Доказательство. Пусть $\Phi = (\varphi_1, \ldots, \varphi_6) \in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2)$. В силу теоремы 4 для всех $q_1, q_2 \in Q_k$ справедливо равенство (15). Следовательно,

$$\varphi_3(\varphi_1(q_i)\circ\tilde\varphi_2(e)) = q_i, \quad i = 1, 2, \tag{18}$$

для всех $q_1, q_2 \in Q_k$. Предположим, что $q_1 \equiv q_2 \ (\ker\varphi_1)$. Тогда $\varphi_1(q_1) = \varphi_1(q_2)$. Из равенств (18) вытекает

$$q_1 = \varphi_3(\varphi_1(q_1)\circ\tilde\varphi_2(e)) = \varphi_3(\varphi_1(q_2)\circ\tilde\varphi_2(e)) = q_2.$$

Таким образом, показано, что для любых $q_1, q_2 \in Q_k$

$$q_1 \equiv q_2 \ (\ker\varphi_1) \Rightarrow q_1 = q_2. \tag{19}$$

Утверждение (19) эквивалентно утверждению о том, что $\varphi_1 : Q_k \to G_1$ — инъективное отображение. Предложение доказано.

Следствие 3. *Для любой группы* $\mathfrak{G}_1$ *порядка меньшего, чем* k,

$$F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2) = \varnothing.$$

Справедливость следствия 3 непосредственно следует из предложения 2, так как условие инъективности отображения φ_1 может быть выполнено тогда и только тогда, когда порядок группы $\mathfrak{G}_1$ не меньше, чем k.

Предложение 3. *Если* $\Phi = (\varphi_1, \ldots, \varphi_6) \in F^c_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$, *то* $\varphi_3 : G_1 \to$ $\to Q_k$ — *сюръективное отображение.*

Доказательство. Пусть $\Phi = (\varphi_1, \ldots, \varphi_6) \in F^c_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$. Поскольку $\varphi_3 : G_1 \to Q_k$, то $\mathrm{Val}\,\varphi_3 \subseteq Q_k$. В силу теоремы 4 для всех $q \in Q_k$ справедливо равенство (15). Следовательно, $q = \varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(e))$ для всех $q \in Q_k$. Итак, показано, что $q \in \mathrm{Val}\,\varphi_3$ для всех $q \in Q_k$. Это означает, что $Q_k \subseteq \mathrm{Val}\,\varphi_3$. Из включений $\mathrm{Val}\,\varphi_3 \subseteq Q_k$ и $Q_k \subseteq \mathrm{Val}\,\varphi_3$ вытекает $\mathrm{Val}\,\varphi_3 = Q_k$. Следовательно, $\varphi_3 : G_1 \to Q_k$ — сюръективное отображение. Предложение доказано.

Предложение 4. *Если* $\Phi = (\varphi_1, \ldots, \varphi_6) \in F^c_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$, *то* $\varphi_3\,|_{(\mathrm{Val}\,\varphi_1) \circ \tilde{\varphi}_2(e)}$ — *инъективное отображение.*

Доказательство. Пусть $\Phi = (\varphi_1, \ldots, \varphi_6) \in F^c_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$. В силу предложения 2 φ_1 — инъективное отображение. Следовательно,

$$|\mathrm{Val}\,\varphi_1| = |Q_k| = k.$$

А так как $\mathfrak{G}_1$ — группа, то справедливо равенство

$$|(\mathrm{Val}\,\varphi_1) \circ \tilde{\varphi}_2(e)| = |\mathrm{Val}\,\varphi_1|.$$

Из последних двух равенств вытекает $|(\mathrm{Val}\,\varphi_1) \circ \tilde{\varphi}_2(e)| = k$. В силу теоремы 4 для всех $q \in Q_k$ справедливо равенство (15). Таким образом, $\varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(e)) =$ $= q$ для всех $q \in Q_k$. Следовательно,

$$\mathrm{Val}\left(\varphi_3\,|_{(\mathrm{Val}\,\varphi_1) \circ \tilde{\varphi}_2(e)}\right) = Q_k.$$

Итак, показано, что $\varphi_3\,|_{(\mathrm{Val}\,\varphi_1) \circ \tilde{\varphi}_2(e)}$ — отображение k-элементного множества $(\mathrm{Val}\,\varphi_1) \circ \tilde{\varphi}_2(e)$ на k-элементное множество Q_k. Последнее утверждение эквивалентно утверждению о том, что $\varphi_3\,|_{(\mathrm{Val}\,\varphi_1) \circ \tilde{\varphi}_2(e)}$ — инъективное отображение. Предложение доказано.

В силу следствия 3 $F^c_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2) = \varnothing$ для любой группы $\mathfrak{G}_1$ порядка меньшего, чем k. Как показано ниже, именно число k является таким наименьшим значением порядка группы $\mathfrak{G}_1$, что множество $F^c_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2)$ может быть непустым.

Теорема 5. *Для всех* $k \geq 2$ *и* $m \geq 1$ *существуют такие группы* $\mathfrak{G}_1$ *порядка* k, *что* $F^c_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2) \neq \varnothing$.

Доказательство. Зафиксируем числа $k \geq 2$ и $m \geq 1$. Выберем в качестве группы $\mathfrak{G}_1$ аддитивную группу $\mathfrak{Z}_k = (Z_k, +)$ вычетов по модулю k. Рассмотрим представление $\Phi = (\varphi_1, \ldots, \varphi_6) \in F_{mnk}(\mathfrak{Z}_k, \mathfrak{G}_2)$, удовлетворяющее следующим условиям:

1) $\varphi_1(q_i) = i - 1$ для всех $i = 1, \ldots, k$;
2) $\varphi_2(x) = 0$ для всех $x \in X_m$;
3) $\varphi_3(j) = q_{j+1}$ для всех $j = 0, 1, \ldots, k-1$.

Определим расширение $\tilde{\varphi}_2$ отображения φ_2 на множество X^*_m с помощью равенства

$$\tilde{\varphi}_2(p) = 0, \quad p \in X^*_m.$$

Выберем произвольные $q_i \in Q_k$, $p \in X_m^*$ и $x \in X_m$. Из определения отображений $\varphi_1, \varphi_2, \tilde{\varphi}_2$ и φ_3 вытекает

$$\varphi_3(\varphi_1(q_i) + \tilde{\varphi}_2(px)) = \varphi_3((i-1)+0) = \varphi_3(i-1) = q_{(i-1)+1} = q_i,$$

$$\varphi_3(\varphi_1(\varphi_3(\varphi_1(q_i) + \tilde{\varphi}_2(p))) + \varphi_2(x)) = \varphi_3(\varphi_1(\varphi_3((i-1)+0)) + 0) =$$
$$= \varphi_3(\varphi_1(\varphi_3(i-1))) = \varphi_3(\varphi_1(q_{(i-1)+1})) = \varphi_3(\varphi_1(q_i)) = \varphi_3(i-1) = q_i.$$

Таким образом,

$$\varphi_3(\varphi_1(q_i) + \tilde{\varphi}_2(px)) = \varphi_3(\varphi_1(\varphi_3(\varphi_1(q_i) + \tilde{\varphi}_2(p))) + \varphi_2(x)).$$

Кроме того,

$$\varphi_3(\varphi_1(q_i) + \tilde{\varphi}_2(e)) = \varphi_3((i-1)+0) = \varphi_3(i-1) = q_i.$$

Итак, показано, что для всех $q \in Q_k$, $p \in X_m^*$ и $x \in X_m$ справедливы равенства (14) и (15). В силу теоремы 4 $\Phi = (\varphi_1, \ldots, \varphi_6) \in F_{mnk}^c(\mathfrak{Z}_k, \mathfrak{G}_2)$, т. е. $F_{mnk}^c(\mathfrak{Z}_k, \mathfrak{G}_2) \neq \varnothing$. Теорема доказана.

Приведенное доказательство теоремы 5 является конструктивным. Используемый в этом доказательстве метод построения конечной группы, имеющей заданные свойства, допускает естественное обобщение на случай произвольной группы $\mathfrak{G}_1$ порядка k. Суть этого обобщения состоит в том, что множество Q_k наделяется структурой конечной группы порядка k, а множеству $\operatorname{Val}\tilde{\varphi}_2$ ставится в соответствие некоторое подмножество этой группы. Использование этого фактора дает возможность описать строение автоматов, принадлежащих множеству $\{ B_\Phi \in \mathfrak{A}_{mnk}(\mathfrak{G}_1, \mathfrak{G}_2) \mid \Phi \in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2) \}$.

Теорема 6. *Пусть $\mathfrak{G}_1$ — группа порядка k. Если $\Phi = (\varphi_1, \ldots, \varphi_6) \in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2)$, то автомат B_Φ состоит из $k/|\operatorname{Val}\tilde{\varphi}_2|$ компонент сильной связанности, каждая из которых содержит $|\operatorname{Val}\tilde{\varphi}_2|$ состояний.*

Доказательство. Пусть $\mathfrak{G}_1 = (G_1, \circ)$ — произвольная группа порядка k и $\Phi = (\varphi_1, \ldots, \varphi_6) \in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2)$.

Рассмотрим автомат $B_\Phi = (Q_k, X_m, Y_n, \delta_\Phi, \lambda_\Phi)$. Выберем произвольное состояние $q \in Q_k$. Множество S_q всех состояний, достижимых из состояния q, удовлетворяет равенству

$$S_q = \left\{ \delta_\Phi(q, p) \mid p \in X_m^* \right\}.$$

Поскольку $\Phi \in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2)$, то из определения 2 вытекает

$$S_q = \left\{ \varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(p)) \mid p \in X_m^* \right\}. \tag{20}$$

Кроме того, в силу предложения 2, $\varphi_1 : Q_k \to G_1$ — инъективное отображение k-элементного множества Q_k в k-элементное множество G_1. Следовательно, φ — сюръективное отображение, т. е. $\operatorname{Val}\varphi_1 = G_1$. Так как $\mathfrak{G}_1$ — группа, то справедливы равенства

$$\operatorname{Val}\varphi_1 \circ \tilde{\varphi}_2(e) = G_1 \circ \varphi_2(e) = G_1, \tag{21}$$

$$|\varphi_1(q) \circ \operatorname{Val}\tilde{\varphi}_2| = |\operatorname{Val}\tilde{\varphi}_2|. \tag{22}$$

Из равенств (20) – (22) и предложений 3 и 4 вытекает, что $\varphi_3|_{\operatorname{Val}\varphi_1 \circ \tilde{\varphi}_2(e)} = \varphi_3|_{G_1} = \varphi_3$ — биективное отображение множества G_1 на множество Q_k. Следовательно, в силу равенств (20) и (22)

$$\left|S_q\right| = \left|\mathrm{Val}\,\tilde{\varphi}_2\right|, \qquad q \in Q_k. \tag{23}$$

Покажем, что множество S_q, $q \in Q_k$, является компонентой сильной связанности автомата B_Φ.

Пусть $q_1 \in S_q$ и $p \in X_m^*$ — такое входное слово, что $\delta_\Phi(q, p) = q_1$. Из равенства (10) вытекает

$$S_{q_1} = \left\{\delta_\Phi(q_1, p_1) \mid p_1 \in X_m^*\right\} = \left\{\delta_\Phi(q, pp_1) \mid p_1 \in X_m^*\right\} \subseteq S_q.$$

Покажем, что $S_q \subseteq S_{q_1}$. Для этого достаточно показать, что состояние q достижимо из состояния q_1.

Предположим противное, т. е. что состояние q не достижимо из состояния q_1. Из равенства (20) вытекает $\left|S_{q_1}\right| = \left|\mathrm{Val}\,\varphi_2\right| = \left|S_q\right|$. Следовательно, существует такое состояние $q_2 \in Q_k$, что $q_2 \in S_{q_1}$ и $q_2 \notin S_q$. Пусть $p_2 \in X_m^*$ — такое входное слово, что $\delta_\Phi(q, p_2) = q_2$. В силу равенства (10)

$$\delta_\Phi(q, pp_2) = \delta_\Phi(\delta_\Phi(q, p), p_2) = \delta_\Phi(q_1, p_2) = q_2,$$

т. е. $q_2 \in S_q$. Полученное противоречие показывает, что предположение неверно. Следовательно, $q \in S_{q_1}$, что и требовалось показать.

Из включений $S_{q_1} \subseteq S_q$ и $S_q \subseteq S_{q_1}$ вытекает, что $S_{q_1} = S_q$ для всех $q_1 \in$ $\in S_q$. Последнее утверждение эквивалентно утверждению о том, что S_q — компонента сильной связанности автомата B_Φ.

Итак, показано, что при всех $q \in Q_k$ множество S_q является компонентой сильной связанности автомата B_Φ, содержащей, в силу равенства (23), $|\mathrm{Val}\,\tilde{\varphi}_2|$ состояний. Число таких компонент сильной связанности равно $|Q_k|/|\mathrm{Val}\,\tilde{\varphi}_2| =$ $= k/|\mathrm{Val}\,\tilde{\varphi}_2|$, что и требовалось показать. Теорема доказана.

Выше предполагалось, что $\tilde{\varphi}_2 : X_m^* \to G_1$ — произвольное отображение, удовлетворяющее равенствам (14) и (15). Особый интерес представляет случай, когда $\tilde{\varphi}_2 : X_m^* \to G_1$ — гомоморфизм свободной полугруппы $\mathfrak{X}_m = (X_m^*, \cdot)$ (где $\cdot$ — операция конкатенации слов) в группу $\mathfrak{G}_1$. Известно, что каждое отображение $\varphi_2 : X_m \to G_1$ единственным образом продолжается до гомоморфизма $\tilde{\varphi}_2$ свободной полугруппы $\mathfrak{X}_m$ в группу $\mathfrak{G}_1$ с помощью равенств

$$\tilde{\varphi}_2(e) = 1_{G_1}, \tag{24}$$

$$\tilde{\varphi}_2(px) = \tilde{\varphi}_2(p) \circ \varphi_2(x), \quad p \in X_m^*, \; x \in X_m. \tag{25}$$

Исследуем условия, при которых для представлений, согласованных с функцией переходов, отображение φ_2 может быть продолжено до гомоморфизма $\tilde{\varphi}_2$ свободной полугруппы $\mathfrak{X}_m$ в группу $\mathfrak{G}_1$.

Предложение 5. *Пусть* $\Phi = (\varphi_1, \ldots, \varphi_6) \in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2)$. *Отображение* $\varphi_2 : X_m \to G_1$ *может быть так продолжено до отображения* $\tilde{\varphi}_2 : X_m^* \to G_1$, *что* $\tilde{\varphi}_2(e) = 1_{G_1}$ *тогда и только тогда, когда* $\varphi_3\varphi_1 : Q_k \to Q_k$ — *тождественное отображение.*

Доказательство. Пусть $\Phi = (\varphi_1, \ldots, \varphi_6) \in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2)$. Предположим, что отображение φ_2 может быть продолжено до отображения $\tilde{\varphi}_2$ так, что $\tilde{\varphi}_2(e) = 1_{G_1}$. Так как $\Phi \in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2)$, то в силу равенства (15)

$$q = \varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(e)) = \varphi_3(\varphi_1(q) \circ 1_{G_1}) = \varphi_3(\varphi_1(q)) = (\varphi_3\varphi_1)(q)$$

для всех $q \in Q_k$. Следовательно, $\varphi_3 \varphi_1$ — тождественное отображение множества Q_k на себя, что и требовалось показать.

Предположим, что $\varphi_3 \varphi_1$ — тождественное отображение множества Q_k на себя, а $\tilde{\varphi}$ — произвольное расширение отображения φ_2 на множество X_m^*, удовлетворяющее равенствам (14) и (15). Рассмотрим расширение $\tilde{\varphi}_2 : X_m^* \to$ $\to G_1$ отображения φ_2, определяемое следующим образом:

$$\tilde{\varphi}_2(p) = \begin{cases} \tilde{\varphi}(p), & \text{если} \quad p \in X_m^+; \\ 1_{G_1}, & \text{если} \quad p = e. \end{cases}$$

Поскольку $\varphi_3 \varphi_1$ — тождественное отображение, то

$$\varphi_3(\varphi_1(q) \circ \varphi_2(e)) = \varphi_3(\varphi_1(q) \circ 1_{G_1}) = \varphi_3(\varphi_1(q)) = (\varphi_3 \varphi_1)(q) = q$$

для всех $q \in Q_k$, т. е. для расширения $\tilde{\varphi}_2$ справедливо равенство (15). А так как для расширения $\tilde{\varphi}$ справедливо равенство (14), $\tilde{\varphi}_2(p) = \tilde{\varphi}(p)$ для всех $p \in X_m^*$ и для $\tilde{\varphi}_2$ справедливо равенство (15), то для $\tilde{\varphi}_2$ также справедливо и равенство (14). Следовательно, отображение φ_2 может быть так продолжено до отображения $\tilde{\varphi}_2 : X_m^* \to G_1$, что $\tilde{\varphi}_2(e) = 1_{G_1}$, что и требовалось показать. Предложение доказано.

Теорема 7. *Если для представления* $\Phi = (\varphi_1, \ldots, \varphi_6) \in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2)$ *выполнены условия*:

1) $\tilde{\varphi}_2(e) = 1_{G_1}$;

2) $\operatorname{Val} \varphi_1 \circ \operatorname{Val} \tilde{\varphi}_2 = \operatorname{Val} \varphi_1$,

то расширение $\tilde{\varphi}_2 : X_m^* \to G_1$ *отображения* $\varphi_2 : X_m \to G_1$ *является гомоморфизмом свободной полугруппы* $\mathfrak{X}_m$ *в группу* $\mathfrak{G}_1$.

Доказательство. Пусть $\Phi = (\varphi_1, \ldots, \varphi_6) \in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2)$ и выполнены условия 1 и 2. В силу условия 1 для расширения $\tilde{\varphi}_2$ справедливо равенство (24). Следовательно, в силу предложения 5, $\varphi_3 \varphi_1$ — тождественное отображение. Из предложения 4 вытекает, что

$$\varphi_3 |_{(\operatorname{Val} \varphi_1) \circ \tilde{\varphi}_2(e)} = \varphi_3 |_{(\operatorname{Val} \varphi_1) \circ 1_{G_1}} = \varphi_3 |_{\operatorname{Val} \varphi_1}$$

— инъективное отображение. Так как $\varphi_3 \varphi_1$ — тождественное отображение, а φ_1 и $\varphi_3 |_{\operatorname{Val} \varphi_1}$ — инъективные отображения, то $\varphi_1 \varphi_3 |_{\operatorname{Val} \varphi_1}$ — тождественное отображение. Покажем, что для расширения $\tilde{\varphi}_2$ справедливо равенство (25). В силу условия 2 $\varphi_1(q) \circ \tilde{\varphi}_2(p) \in \operatorname{Val} \varphi_1$ для всех $q \in Q_k$ и $p \in X_m^*$. Поскольку $\varphi_1 \varphi_3 |_{\operatorname{Val} \varphi_1}$ — тождественное отображение, а $\varphi_3 |_{\operatorname{Val} \varphi_1}$ — инъективное отображение, то из равенства (14) вытекает

$$\varphi_1(q) \circ \tilde{\varphi}_2(px) = \varphi_1(q) \circ \tilde{\varphi}_2(p) \circ \varphi_2(x)$$

для всех $q \in Q_k$, $p \in X_m^*$ и $x \in X_m$. Так как $\mathfrak{G}_1$ — группа, то из последнего равенства следует

$$\tilde{\varphi}_2(px) = \tilde{\varphi}_2(p) \circ \varphi_2(x)$$

для всех $p \in X_m^*$ и $x \in X_m$, т.е. для расширения $\tilde{\varphi}_2$ справедливо равенство (25), что и требовалось показать. Теорема доказана.

В заключение работы отметим следующее. В теореме 6 установлено, что если порядок группы $\mathfrak{G}_1$ равен k, то множество автоматов B_Φ ($\Phi \in$ $\in F_{mnk}^c(\mathfrak{G}_1, \mathfrak{G}_2)$) состоит из перестановочных автоматов, у которых все компоненты сильной связанности имеют одно и то же число состояний. Естественно возникает задача о возможности представления таких автоматов в виде композиции автоматов, у которых множество состояний наделено структурой хорошо изученных групп. Приведем схематическое решение этой задачи для случая $m = 1$, т. е. для автономных автоматов. Поскольку представления согласованы с функцией переходов, то для упрощения обозначений будем рассматривать автоматы без выхода.

Автомат $A = (Z_k, \{x\}, \delta)$ $(Z_k = \{0, 1, \ldots, k-1\},\ k \geq 2)$ назовем счетчиком, если $\delta(z, x) = z + 1 \pmod k$ для всех $z \in Z_k$. Пусть $\mathcal{S}$ — множество всех конечных последовательностей счетчиков, а $\mathcal{A} = \bigcup_{n=1}^{\infty} \mathcal{A}_n$, где

$$\mathcal{A}_n = \left\{ A = \left(\mathop{\times}_{i=1}^{n} Z_{k_i}, \{x\}, \delta \right) \,\middle|\, k_i \geq 2 \quad \text{для всех} \quad i = 1, \ldots, n \right\}, \qquad n \in N.$$

Рассмотрим отображение $\chi : \mathcal{S} \to \mathcal{A}$, переводящее каждую конечную последовательность $A_i = (Z_{k_i}, \{x\}, \delta_i)$, $i = 1, \ldots, n$, счетчиков в такой автомат

$$\chi(A_1, \ldots, A_n) = \left(\mathop{\times}_{i=1}^{n} Z_{k_i}, \{x\}, \delta \right),$$

что функция переходов δ определена равенством $\delta((z_1, \ldots, z_n), x) = (\delta_1(z_1, x), \ldots, \delta_n(z_n, x))$. Автомат $\chi(A_1, \ldots, A_n)$ представляет собой декартово произведение счетчиков $A_1, \ldots, A_n$ с отождествлением их входов. Можно доказать, что его структура полностью определяется следующим образом.

Теорема 8. *Для любой конечной последовательности* $A_i = (Z_{k_i}, \{x\}, \delta_i)$, $i = 1, \ldots, n$, *счетчиков*:

1) *автомат* $\chi(A_1, \ldots, A_n)$ *состоит из НОД* $(k_1, \ldots, k_n)$ *компонент сильной связанности, каждая из которых содержит НОК* $(k_1, \ldots, k_n)$ *состояний;*

2) *состояния* $(z_1, \ldots, z_n), (z_1', \ldots, z_n') \in \mathop{\times}_{i=1}^{n} Z_{k_i}$ *принадлежат одной и той же компоненте сильной связанности автомата* $\chi(A_1, \ldots, A_n)$ *тогда и только тогда, когда совместна система сравнений*

$$l \equiv z_i' - z_i \pmod{k_i}, \quad i = 1, \ldots, n. \tag{26}$$

Пусть $A_i = (Z_{k_i}, \{x\}, \delta_i)$, $i = 1, \ldots, n$, — произвольная конечная последовательность счетчиков, $B = \chi(A_1, \ldots, A_n)$, а $X_B(q, q')$ — множество всех входных слов, переводящих B из состояния q в состояние q'. Из теоремы 8 вытекает, что для любых состояний $q = (z_1, \ldots, z_n)$ и $q' = (z_1', \ldots, z_n')$ автомата B справедливо равенство

$$X_B(q, q') = \{ x^l \mid l \text{ — решение системы (26)} \}.$$

Из определения отображения $\chi : \mathcal{S} \to \mathcal{A}$ и из теоремы 8 вытекает, что χ инъективно, причем $\varnothing \neq \operatorname{Val} \chi \subset \mathcal{A}$. Пусть

$$\mathcal{A}_n(m) = \left\{ A = \left(\mathop{\times}_{i=1}^{n} Z_{k_i}, \{x\}, \delta \right) \in \mathcal{A}_n \mid k_1 \ldots k_n \leq m \right\}, \qquad m, n \in N.$$

Нетрудно убедиться в том, что

$$\frac{\sum_{n=1}^{\infty} |\operatorname{Val} \chi \cap \mathcal{A}_n(m)|}{\sum_{n=1}^{\infty} |\mathcal{A}_n(m)|} \to 0, \qquad m \to \infty.$$

Это означает, что почти все автоматы, принадлежащие множеству A, не принадлежат множеству $\operatorname{Val}\chi$, т. е. $\operatorname{Val}\chi$ является весьма „узким" подмножеством множества $\mathscr{A}$. Можно доказать, что справедливы следующие критерии, характеризующие общие (абстрактные) свойства отображения χ.

Теорема 9. *Если* $A_i = (Z_{k_i}, \{x\}, \delta_i)$, $i = 1, \ldots, n$, *и* $A_j' = (Z_{k_j'}, \{x\}, \delta_j')$ — *две произвольные конечные последовательности счетчиков,* $B = \chi(A_1, \ldots, A_n)$ *и* $B' = \chi(A_1', \ldots, A_n')$, *то*:

1) *автомат* B' *является гомоморфным образом автомата* B *тогда и только тогда, когда* $HOK\ (k_1', \ldots, k_{n'}') \mid HOK\ (k_1, \ldots, k_n)$;

2) *автоматы* B *и* B' *изоморфны тогда и только тогда, когда справедливы равенства*

$$\prod_{i=1}^{n} k_i = \prod_{j=1}^{n'} k_j'$$

и $HOK\ (k_1, \ldots, k_n) = HOK\ (k_1', \ldots, k_{n'}')$.

Из теоремы 9 вытекает, что фактор-множество множества $\operatorname{Val}\chi$ по отношению изоморфизма автоматов является счетным. Кроме того, подмножество $\mathscr{A}'$ множества $\operatorname{Val}\chi$, упорядоченное отношением гомоморфизма автоматов, образует верхнюю полуструктуру тогда и только тогда, когда для любых автоматов $B_1, B_2 \in \mathscr{A}'$ $(B_1 \neq B_2)$, у которых компоненты сильной связанности имеют соответственно m_1 и m_2 состояний, существует такой автомат $B \in \mathscr{A}'$, у которого компонента сильной связанности имеет m состояний, что $\text{НОК}\ (m_1, m_2) \mid m$. Можно показать, что имеет место следующий критерий, определяющий условия вложимости произвольного множества автономных автоматов как в множество $\mathscr{A}_n \cap \operatorname{Val}\chi$, так и в множество $\operatorname{Val}\chi$.

Теорема 10. *Пусть автомат* $B = (Q, \{x\}, \delta)$ *состоит из* d *компонент сильной связанности, каждая из которых содержит* m *компонент сильной связанности, а канонические разложения чисел* d *и* m *на сомножители имеют вид* $d = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, $m = p_1^{\beta_1} \ldots p_r^{\beta_r}$. *Последовательность счетчиков* $A_1, \ldots, A_n$, $n \in N$, *для которой автоматы* B *и* $\chi(A_1, \ldots, A_n)$ *изоморфны, существует тогда и только тогда, когда система*

$$\sum_{i=1}^{n} \gamma_{ij} = \alpha_j + \beta_j, \quad j = 1, \ldots, r,$$

$$\max\{\gamma_{ij} \mid i = 1, \ldots, n\} = \beta_j, \quad j = 1, \ldots, r,$$

$$\alpha_j,\ \beta_j,\ \gamma_{ij} \in Z_+, \quad i = 1, \ldots, n; \quad j = 1, \ldots, r,$$

имеет хотя бы одно решение.

1. *Скобелев В. Г.* Представление автоматов группами // Укр. мат. журн. – 1992. – **44**, № 10. – С. 1412 – 1416.
2. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. – М.: Наука, 1977. – 239 с.
3. *Мальцев А. И.* Алгебраические системы. – М.: Наука, 1970. – 392 с.
4. *Трахтенброт Б. А., Барздинь Я. М.* Конечные автоматы (поведение и синтез). – М.: Наука, 1970. – 400 с.

Получено 10.04.95