

# О выразимости суперпозициями автоматов с разрешимыми группами

А. А. Летуновский

Рассматривается задача выразимости конечного автомата  $A$  суперпозициями системы  $\Phi \cup \nu$ , где  $\Phi$  состоит из всех функций  $k$ -значной логики и «задержки»,  $\nu$  — произвольная конечная система автоматов. Ранее автор показал, что для автомата  $A$  с безусловными переходами существует алгоритм проверки выразимости  $A$  через  $\{\Phi \cup \nu\}$ . В настоящей работе решается задача алгоритмической разрешимости задачи выразимости автомата с разрешимой группой через систему  $\Phi \cup \nu$ .

**Ключевые слова:** выразимость, конечный автомат, задержка, константный автомат, алгоритмическая разрешимость, разрешимая группа.

## Введение

Известно, что решение задачи выразимости относительно операции суперпозиции для систем автоматных функций наталкивается на существенные трудности [1], а задача полноты не имеет смысла, так как все полные системы бесконечны. Тем не менее, в задаче полноты удалось понизить арность полных систем до 2 [2]. Для задачи выразимости в работе [3] установлена алгоритмическая неразрешимость для конечных систем автоматных функций, а в работе [4] показана алгоритмическая неразрешимость определения бесконечности множества выразимых констант. Ранее в задачах полноты относительно суперпозиции и обратной связи удалось получить положительные результаты для алгоритмической разрешимости полноты систем с фиксированной добавкой [5]. В данной статье автор продолжает изучение

случаев, где задача выразимости разрешима. Показано, что по системе автоматных функций содержащей все функций  $k$ -значной логики и задержку можно определить, выразима ли через эту систему конкретная автоматная функция, «полугруппа» которой является разрешимой группой.

## 1. Основные понятия и результаты

Пусть  $E_k = \{0, 1, \dots, k-1\}$ , функции вида  $g : E_k^n \rightarrow E_k$  называются функциями  $k$ -значной логики, их множество обозначается через  $P_k$ . Пусть  $E_k^\infty$  — множество всех сверхслов вида  $a(1)a(2)\dots$ , где  $a(j) \in E_k$ ,  $j = 1, 2, \dots$ . Через  $\mathbb{N}$  обозначим множество натуральных чисел. Для  $m, n \in \mathbb{N}$  будем обозначать через  $m|n$  то, что  $m$  делит  $n$ . Пусть

$$f : (E_k^\infty)^n \rightarrow (E_k^\infty)^m$$

— автоматная функция ( $a$ -функция), то есть она задается рекуррентно соотношениями (1).

$$\left\{ \begin{array}{l} q_1(1) = q_0, \\ \dots \\ q_s(1) = q_0, \\ q_1(t+1) = \phi_1(q_1(t), \dots, q_s(t), a_1, \dots, a_n), \\ \dots \\ q_s(t+1) = \phi_s(q_1(t), \dots, q_s(t), a_1, \dots, a_n), \\ b_1(t) = \psi_1(q_1(t), \dots, q_s(t), a_1, \dots, a_n), \\ \dots \\ b_m(t) = \psi_m(q_1(t), \dots, q_s(t), a_1, \dots, a_n). \end{array} \right. \quad (1)$$

Вектор  $q = (q_1, \dots, q_s)$  задает состояние  $a$ -функции  $f$ ,  $q_0$  её начальное состояние, буквы  $a = (a_1, a_2, \dots, a_n)$  и  $b = (b_1, \dots, b_m)$  называют входной и выходной буквами, а сверхслова  $a(1)a(2)\dots$  и  $b(1)b(2)\dots$  — входными и выходными сверхсловами, соответственно. Вектор-функции  $\phi$  и  $\psi$  называются функциями переходов и выходной функцией, соответственно, а шестерка

$$(E_k^n, E_k^s, E_k^m, \phi, \psi, q_0)$$

— автоматом, порождающим функцию  $f$ . Далее в тексте мы иногда будем использовать для автомата обозначение  $(A, Q, B, \phi, \psi, q_0)$ , при этом предполагая что  $A \subseteq E_k^n, Q \subseteq E_k^s, B \subseteq E_k^m$ . Автомат  $M$  называется автоматом Медведева, если  $B = Q, \psi(a, q) = q$ . Назовем автомат автоматом с безусловными переходами, если  $\phi(q, a)$  не зависит от  $a$ .

Обычным образом доопределим функции  $\phi$  и  $\psi$  на слова:

$$\begin{aligned} \phi(q, a(1), \dots, a(t)) &= \phi(\phi \dots \phi(q, a(1)), \dots, a(t-1)), a(t)), \\ \psi(q, a(1), \dots, a(t)) &= \psi(\phi(q, a(1)), \dots, a(t-1)), a(t)) \end{aligned}$$

и определим рекурсивно функцию

$$\bar{\psi}(q, a(1), \dots, a(t)) = \bar{\psi}(q, a(1), \dots, a(t-1))\psi(\phi(q, a(1), \dots, a(t-1)), a(t)).$$

Класс всех  $a$ -функций обозначим через  $P$ .

В этом классе обычным образом введем операции суперпозиции. Для суперпозиции будем использовать модификации операций из [6].

$$\left\{ \begin{aligned} (\eta f)(x_1, x_2, \dots, x_n) &= f(x_2, x_3, \dots, x_n, x_1), \\ (\varepsilon f)(x_1, x_2, \dots, x_n) &= f(x_2, x_1, x_3, \dots, x_n), \\ (\varpi f)(x_1, x_2, \dots, x_n) &= f(x_1, x_3, \dots, x_n), \\ (\delta f)(x_1, x_2, \dots, x_n) &= f(x_1, x_2, \dots, x_{n+1}), \\ (f * g)(x_1, x_2, \dots, x_{m+n-1}) &= f(g(x_1, \dots, x_m), x_{m+1}, \dots, x_{m+n-1}). \end{aligned} \right.$$

Пусть  $M \subseteq P$ , обозначим через  $[M]$  множество  $a$ -функций, получающихся из  $M$  с помощью операций суперпозиции. Рассматривая системы автоматов, будем считать без ограничения общности, что  $M$  состоит из одного автомата, так как задачу выразимости для нескольких автоматов можно свести к задаче для одного автомата, являющегося их параллельным соединением.

Автоматную функцию  $G_0$ , задаваемую уравнениями

$$\left\{ \begin{aligned} q(1) &= 0, \\ q(t+1) &= a(t), \\ b(t) &= q(t), \end{aligned} \right.$$

назовём автоматной функцией «задержки».

Обозначим  $\langle M \rangle = [M \cup \{P_k, G_0\}]$

Константной автоматной функцией назовем автоматную функцию, выдающую одно и тоже периодическое выходное сверхслово на всех входных сверхсловах. Класс константных автоматных функций обозначим через  $K$ .

Там, где это не приводит к недоразумению, будем одинаково обозначать автомат и его  $a$ -функцию.

**Определение 1.** Пусть  $M = (A, Q, B, \phi, \psi, q_0)$  — конечный автомат. Множество подстановок  $\{\phi_a : Q \rightarrow Q \mid a \in A\}$ , где  $\phi_a(q) = \phi(q, a)$ , порождает полугруппу подстановок  $S$  на множестве  $Q$ . Изоморфную  $S$  абстрактную полугруппу будем называть полугруппой автомата  $M$  и обозначать  $S_M$ .

**Определение 2.** Пусть  $S_1$  и  $S$  полугруппы. Скажем, что  $S_1$  делит  $S$  ( $S_1 \mid S$ ), если в  $S$  найдется такая подполугруппа  $S_2$ , что  $S_1$  является гомоморфным образом  $S_2$ .

**Определение 3.** Автоматом  $A_p$ ,  $p \in \mathbb{N}$  будем называть автомат Медведева вида

$$\begin{aligned} &(\{a, b\}, \{1, \dots, p\}, \{1, \dots, p\}, \phi, \psi, 1), \\ &\phi(i, b) = i, \phi(i, a) = (i + 1) \bmod p, \\ &\psi(i, a) = \psi(i, b) = i. \end{aligned}$$

Его диаграмма показана на рис. 1.

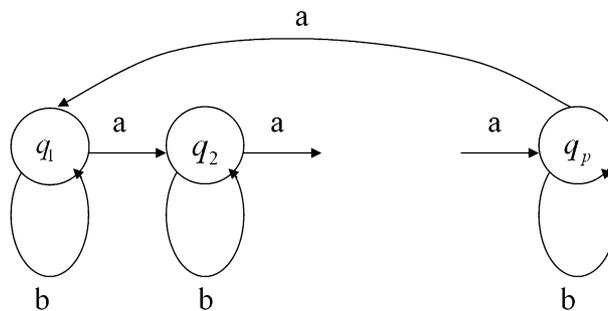


Рис. 1.

Группа автомата  $A_p$  есть  $Z_p$  — циклическая группа порядка  $p$ .

**Лемма 1.** Пусть  $C_p$  и  $B_p$  приведенные автоматы,  $C_p$  не является безусловным, причём  $S_{C_p} = S_{B_p} = Z_p$ . Тогда  $\langle C_p \rangle \supseteq \langle B_p \rangle$ .

Из леммы 1 прямо следует, что выразимость произвольного автомата с группой  $Z_p$  следует из выразимости автомата  $A_p$ .

Через  $\beta_{k_1}$  обозначим сверхслово, получающееся на выходе константного автомата  $k_1$ .

**Определение 4.** Любое периодическое сверхслово  $\beta$  можно представить в виде  $\beta = \gamma\alpha^\infty$ . Выберем из всех представлений такое, что  $\gamma$  и  $\alpha$  имеют наименьшую длину. Для выбранного представления назовем  $\gamma$  наименьшим предпериодом сверхслова  $\beta$ , а  $\alpha$  наименьшим периодом сверхслова  $\beta$ , а каждое слово вида  $\underbrace{\alpha\alpha\dots\alpha}_n$  будем называть периодом сверхслова  $\beta$ , здесь  $n \in \mathbb{N}$ . Обозначим  $|\alpha|$  длину слова  $\alpha$ .

Для множества константных автоматных функций  $K' \subseteq K$  обозначим через  $\Theta(K')$  множество длин минимальных периодов сверхслов  $\{\beta_{k_i} : k_i \in K'\}$ . Для случая одного сверхслова  $\beta = \gamma\alpha^\infty$  будем считать, что  $\Theta(\beta) = |\alpha|$ .

Если  $M$  — некоторое множество автоматов, обозначим через  $\Theta(M) = \Theta(\langle M \rangle \cap K)$  множество периодов его констант.

Из [7] известно, что для  $M \subseteq P$  в случае  $[M] \supseteq \{P_k, G_0\}$ ,  $|M| < \infty$  задача выразимости константных автоматных функций является алгоритмически разрешимой, более того  $\exists b, q \in \mathbb{N}$ , зависящие от  $M$ , такие что

$$\Theta(M) = \{t : t|bq^i, i = 0, 1, \dots\}.$$

Причем

$$\beta \in \langle M \rangle \Leftrightarrow \Theta(\beta) \in \Theta(M).$$

Число  $q$  назовем *главным цикловым индексом* замкнутого класса  $M$  и будем обозначать  $q(M)$ ,  $b$  назовем *безусловным цикловым индексом* замкнутого класса  $M$  и будем обозначать  $b(M)$ .

В работе [7] показано, что цикловые индексы  $b$  и  $q$  эффективно вычисляются по конечной системе автоматов  $M$ .

Опишем алгоритм вычисления цикловых индексов системы автоматов.

Пусть  $M = (A, Q, B, \phi, \psi, q_0)$

Для произвольного слова  $\alpha \in A^*$  обозначим через  $\phi_\alpha : Q \rightarrow Q$  отображение на множестве  $Q$ , задаваемое функцией переходов  $\phi$ ,

$\pi_\alpha$  — разбиение множества состояний  $Q$  на классы отличимости  $Q_1, \dots, Q_s$  словом  $\alpha$ . То есть, для  $\forall q_1 \in Q_1, q_2 \in Q_2, \psi(q_1, \alpha) \neq \psi(q_2, \alpha)$ .

Обозначим  $p_\alpha = (\phi_\alpha, \pi_\alpha)$ .

$P_l = \{p_\alpha, |\alpha| = l\}$ .

Рассмотрим последовательность  $N_1, N_2, \dots, N_k, \dots$  натуральных чисел, связанную с автоматом  $M$ , где  $N_{i+1}$  получается из  $N_i$  следующим рекурсивным способом.

Пусть  $C_i = \{\alpha_i\}$  — множество сверхслов во входном алфавите с длиной периода  $N_i$  (не обязательно минимальной). Рассмотрим множество сверхслов  $B_i = \{M(\alpha_i) | \alpha_i \in C_i\}$ . Пусть  $l_1, l_2, \dots, l_s$  — длины минимальных периодов сверхслов  $B_i$ . Положим  $N_{i+1} = \text{НОК}(l_1, \dots, l_s, N_i)$ .

По построению  $N_i | N_{i+1}$ . Пусть  $m_i = \frac{N_{i+1}}{N_i}$ .

**Лемма 2.** ([7]) Пусть для некоторых  $l, m$   $P_l = P_m$ , тогда для любого  $k \in \mathbb{N}$   $P_{lk} = P_{mk}$ .

**Лемма 3.** ([7])  $m_i$  периодична.

Приведем здесь алгоритм определения цикловых индексов  $b$  и  $q$  по системе автоматов  $M$ .

1 шаг. Строим последовательность  $N_i$  до тех пор, пока не найдутся  $N_i$  и  $N_j$ , такие, что  $P_{N_i} = P_{N_j}$ .

2 шаг. Положим  $b = N_i, q = \frac{N_j}{N_i}$ .

**Определение 5.** ([2]) Пусть  $f$  и  $g$  — автоматы с одинаковым числом входов и одинаковым числом выходов. Скажем, что автоматная функция  $g$  копирует автоматную функцию  $f$ , если найдутся такие натуральные  $n, j, k$  ( $n \leq j$ ), что для любого  $l = 0, 1, 2, \dots$  и любой входной последовательности достаточной длины значение автоматной функции  $g$  в момент  $j + kl$  совпадает со значением автоматной функции  $f$  в момент  $n + kl$ , то есть  $f(n + kl) = g(j + kl)$ .

**Лемма 4 (Лемма о копировании).** ([2]) Пусть  $g$  — автоматная функция Медведева и  $g$  копирует  $f$  с параметрами  $n, j, l$ , тогда  $f \in [g \cup \{G_0, P_k, (\underbrace{1 \dots 0}_l)^\infty\}]$

**Определение 6.** ([8]) Пусть  $G_1$  и  $G_2$  — группы, если группа  $G$  такова, что  $\exists f : G \rightarrow G_1$  — гомоморфизм,  $\text{Ker } f = G_2$ . Назовем  $G$  расширением  $G_1$  с помощью  $G_2$ . Множество групп, полученных расширениями конечных циклических групп назовем множеством разрешимых групп.

**Теорема 1.** Пусть  $M$  — конечное множество автоматных функций, тогда  $A_p$  выразим через  $\langle M \rangle$  тогда и только тогда, когда  $p$  делит некоторую степень главного циклового индекса множества  $M$ .

**Теорема 2.** Пусть  $M$  — конечное множество автоматных функций, тогда существует алгоритм, позволяющий проверить свойство выразимости  $A_p$  через  $\langle M \rangle$ .

**Теорема 3.** Пусть  $M$  — конечное множество автоматных функций,  $B$  — некоторый автомат Медведева, причем  $S_B$  — разрешимая группа. Тогда  $B$  выразим через  $\langle M \rangle$  точно тогда, когда для всех  $Z_p | S_B$  автомат  $A_p$  выразим через  $\langle M \rangle$ .

**Теорема 4.** Пусть  $M$  — конечное множество автоматных функций,  $B$  — некоторый автомат Медведева, причем  $S_B$  — разрешимая группа. Тогда существует алгоритм, позволяющий проверить свойство выразимости  $B$  через  $\langle M \rangle$ .

## 2. Доказательство теорем

### Доказательство теоремы 1

Необходимость: Пусть  $A_p \in \langle M \rangle$ , тогда

$$\Theta(M) \supseteq \Theta(A_p) = \{p^i, i = 0, 1, \dots\},$$

так как очевидно  $\Theta(A_p) = \{p^i, i = 0, 1, \dots\}$ , но тогда  $p | q_M^i$  для некоторого  $i$ .

Достаточность: Докажем сначала, что выразим автомат  $A_{q_M}$ . Автомат  $A_p$  выразим через  $A_{q_M}$  «навешиванием» на выход автомата  $A_{q_M}$  функции  $h(q) = q \bmod p$ .

Для доказательства выразимости  $A_{q_M}$  построим схему из автоматов  $\langle M \rangle$ , которая «копировала» бы автомат  $A_{q_M}$ . Для построения этой схемы воспользуемся алгоритмом построения цикловых индексов, а также несколькими вспомогательными функциями.

По построению  $b_M$  и  $q_M$  существует слово  $\alpha$  длины  $b_M$  и схема  $\Sigma$  автоматов из  $\langle M \rangle$  такие, что период  $\beta = \Sigma(\alpha)$  равен  $b_M q_M$ . Из этого следует, что  $\alpha$  задает на состояниях схемы  $\Sigma$  подстановку  $s_1 \rightarrow s_2, s_2 \rightarrow s_3, \dots, s_{q_M} \rightarrow s_1$ , при этом состояние  $s_1$  является достижимым в схеме. Без ограничения общности будем считать, что  $s_1$  — начальное состояние.

$\check{\alpha} = \underbrace{\alpha\alpha\dots\alpha}_{q_M}$  является словом, попарно отличающим состояния  $(s_1, s_2, \dots, s_{q_M})$ . Действительно, пусть это не так и состояния  $s_i$  и  $s_j$  неотличимы словом  $\check{\alpha}$ , тогда период  $\beta$  равен  $b_M(j-i)$ , что неверно. Таким образом  $\check{\alpha} = \underbrace{\alpha\alpha\dots\alpha}_{q_M}$  — слово, задающее единичную подстановку на  $s_1, \dots, s_{q_M}$  и отличающее все эти состояния.

Из алгоритма построения цикловых индексов следует, что  $P_{b_M} = P_{b_M * q_M}$ . А значит для любого слова  $\alpha$  длины  $b_M$  существует слово  $\beta$  длины  $b_M * q_M$ , такое, что  $\phi_\alpha = \phi_\beta$  для любого автомата из  $M$ , причём  $\alpha^\infty$  и  $\beta^\infty$  выразимы через  $\langle M \rangle$ .

Рассмотрим слова  $\bar{\alpha} = \underbrace{\check{\alpha}\check{\alpha}\dots\check{\alpha}}_{q_M}$  и  $\bar{\beta} = \underbrace{\check{\alpha}\check{\alpha}\dots\check{\alpha}}_{q_M-1}\beta$ . Заметим, что слова  $\bar{\alpha}$  и  $\bar{\beta}$  задают соответственно единичную подстановку и циклическую подстановку порядка  $q_M$  на состояниях  $s_1, s_2, \dots, s_{q_M}$ , при этом состояния попарно отличимы словами  $\bar{\alpha}$  и  $\bar{\beta}$ . Заметим также, что  $|\bar{\alpha}| = |\bar{\beta}| = b_M * q_M^2$ .

Обозначим  $e$  — единичную подстановку на состояниях автомата  $A_{q_M}$  (она задается буквой  $b$ ),  $t$  — подстановку  $(q_2, q_3, \dots, q_n, q_1)$  (она задается буквой  $a$ ). Обозначим  $\bar{a} = \underbrace{bb\dots b}_{b_M q_M^2}$ ,  $\bar{b} = \underbrace{bb\dots b}_{b_M q_M^2 - 1} a$ . Заметим, что  $\bar{a}$  задает подстановку  $e$ ,  $\bar{b}$  — подстановку  $t$ .

Теперь построим несколько вспомогательных функций, позволяющих отобразить входные слова в алфавите  $\{a, b\}$  в нужные нам входные слова в алфавите  $\bar{\alpha}, \bar{\beta}$ .

Пусть  $\gamma$  — произвольное слово длины  $b_M * q_M^3$ . На состояниях автомата  $A_{q_M}$  слово  $\gamma$  задаёт одну из  $q_M$  подстановок —  $(e, t, t^2, \dots, t^{q_M-1})$ . Пусть  $\gamma$  задает подстановку  $t^i$ . Тогда  $\overline{f(\gamma)} = \underbrace{\overline{bb \dots b}}_i \underbrace{\overline{aa \dots a}}_{q_M-i}$ . Заметим,

что  $\overline{f(\gamma)}$  задает ту же подстановку, что и  $\gamma$  на состояниях  $A_{q_M}$ .

$g$  — функция  $k$ -значной логики, такая что  $g(\bar{a}) = \bar{\alpha}, g(\bar{b}) = \bar{\beta}$ .

$G_0^i$  — задержка на  $i$  тактов, в первые  $i$  тактов выдающая 0.

$G_{\check{\alpha}}^i$  — задержка на  $i$  тактов, в первые  $i$  тактов выдающая  $\check{\alpha}$ .

Обозначим через  $S$  автомат с  $b_M q_M^3$  входами — переключатель входов. В первые  $b_M q_M^3$  тактов времени он выдаёт по циклу буквы слова  $\check{\alpha}$ , а после по циклу с периодом  $b_M q_M^3$  передает  $i$ -й вход на выход.

Несложно понять, что автомат  $S$  может быть получен суперпозицией счетчиков по модулю  $b_M q_M^3$ , булевых функций и задержек.

$H$  — функция  $k$ -значной логики, которая по выходу автомата  $\Sigma$  после подачи слова  $\check{\alpha}$  определяет состояние автомата  $\Sigma$  после подачи слова  $\check{\alpha}$ . А затем по состоянию и входному слову длины  $b_M(q_M^3 - q_M)$  определяет состояние автомата  $\Sigma$  через  $b_M(q_M^3 - q_M)$  тактов времени, а затем осуществляет отображение  $s_1 \rightarrow q_1, s_2 \rightarrow q_2, s_{q_M} \rightarrow q_{q_M}$ .

Рассмотрим следующую схему  $\Sigma_K$  (рис.2) и докажем, что автоматная функция, реализуемая этой схемой копирует автоматную функцию  $A_{q_M}$ .

Рассмотрим  $j = 0, n = 2q_M b_M, k = q_M^3 b_M$  и докажем, что схема  $\Sigma_K$  копирует автомат  $A_{q_M}$  с параметрами  $j, n, k$ . Для этого рассмотрим произвольное входное слово  $\gamma = \gamma_1 \gamma_2 \dots \gamma_{q_M^3 b_M} r$  длины  $q_M^3 b_M r$  для некоторого  $r$ . Докажем, что выход автомата  $\Sigma_K$  в момент времени  $q_M^3 b_M r + 2q_M b_M$  совпадает с выходом автомата  $A_{q_M}$  в момент времени  $q_M^3 b_M r$  при подаче на оба автомата слова  $\gamma$ .

Докажем это утверждение по индукции.

1. В момент времени 0 выход автомата  $A_{q_M}$   $q_1$ . В момент времени  $2q_M b_M$  автомат  $\Sigma$  находится в состоянии  $s_1$ , так как на его вход поступает входное слово  $\check{\alpha}$ , а  $\phi_{\Sigma}(s_1, \check{\alpha}) = s_1$ .  $H(s_1, \underbrace{\check{\alpha}, \dots, \check{\alpha}}_{b_M(q_M^3 - q_M)}) = q_1$ , так

как функция  $H$  по выходу функции  $\Sigma$  после подачи слова  $\check{\alpha}$  опре-

деляет, что автомат  $\Sigma$  находится в состоянии  $s_1$  и по определению функции  $H$ , на выходе у неё  $q_1$ .

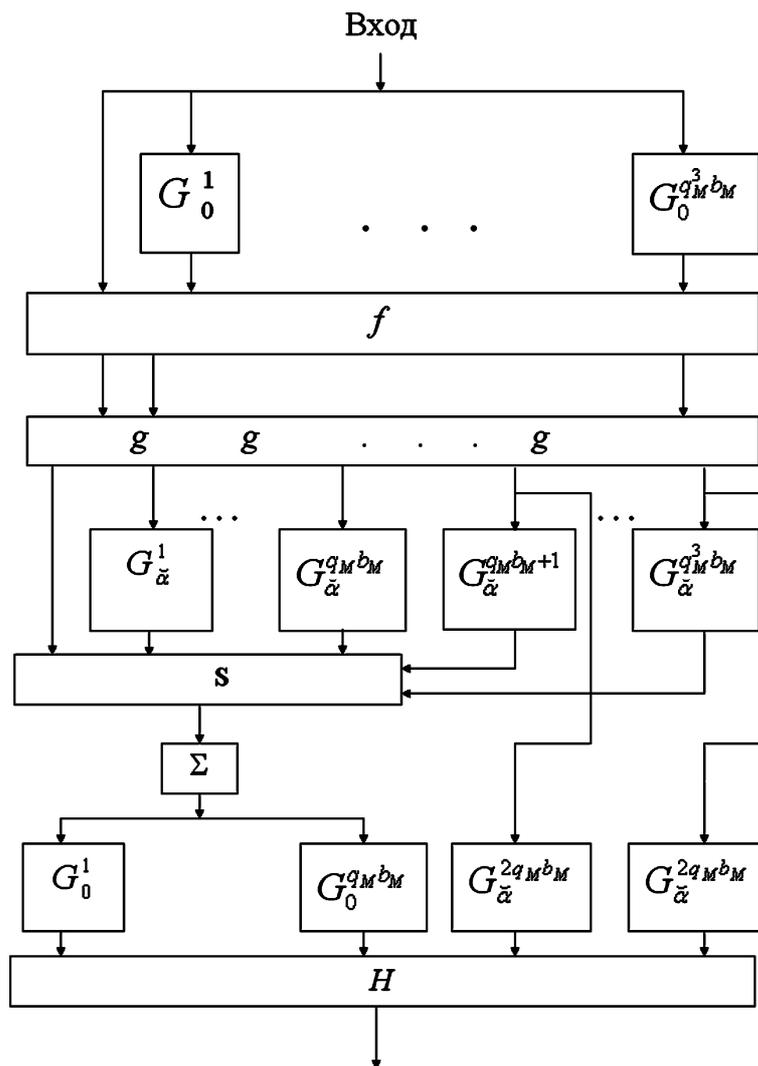


Рис. 2.

2. Пусть утверждение выполнено для  $n = r$ , докажем, что оно выполнено для  $n = r + 1$ .

Пусть в момент времени  $b_M q_M^3 r$  автомат  $A_{q_M}$  находится в состоянии  $q_i$ , докажем, что тогда автомат  $\Sigma$  в момент времени  $b_M q_M^3 (r + 1)$  находится в состоянии  $s_i$ . Действительно, по построению функций  $f$ ,  $g$  и  $S$  суммарное входное воздействие на автомат  $A_{q_M}$  за  $b_M q_M^3$  тактов времени равно входному воздействию на автомат  $\Sigma$ , только применительно к состояниям  $s_1, \dots, s_{q_M}$ . Плюс изначальная задержка на  $b_M q_M^3$  тактов.

Пусть по входному слову длины  $b_M q_M^3$  автомат  $\Sigma$  из состояния  $q_i$  переходит в состояние  $q_j$ , тогда функция  $H$ , фактически моделирующая работу функции переходов автомата  $\Sigma$  в момент времени  $b_M q_M^3 (r + 1) + 2b_M q_M$  выдает  $q_j$  и копирование доказано.

Из копирования следует теорема 1. Теорема 1 доказана.

Теорема 2 следует из теоремы 1 и из [7].

### Доказательство теоремы 3

**Лемма 5.** Пусть  $M = (A, Q, B, \phi, \psi, q_0)$  — произвольный автомат Медведова,  $(X, S)$  — простая подгруппа  $S$  полугруппы  $S_M$  с системой образующих  $X = (s_1, \dots, s_k)$ . Пусть  $\alpha_1, \dots, \alpha_k$  — множество слов в алфавите  $A$ , таких, что  $\phi(q, \alpha_i) = s_i(q), i = 1, \dots, k$ . Тогда в группе  $S$  существует система образующих  $X' = (s'_1, \dots, s'_k)$ , и множество слов в алфавите  $A$  —  $\alpha'_1, \dots, \alpha'_k$ , такие что  $\phi(q, \alpha'_i) = s'_i(q), \alpha'_i$  некоторая конкатенация слов  $\alpha_i, i = 1, \dots, k$  и  $l(\alpha'_1) = \dots = l(\alpha'_k)$ .

**Доказательство.** Пусть  $l_1 = l(\alpha_1), \dots, l_m = l(\alpha_m)$ . Обозначим  $d = NOD(l_1, \dots, l_m)$ . Пусть  $(e_1, \dots)$  — множество слов в алфавите  $A$ , таких что  $\phi(q, e_i) = q, i = 1, \dots$ . Обозначим  $l(e_i) = d_i$ . Обозначим  $d_e = NOD(\{d_i\})$ . Очевидно, что  $d_e = Cd$  для некоторого  $C$ . Возможно 2 случая

1.  $C > 1$ .

2.  $C = 1$ .

1. Пусть  $C > 1$ . Рассмотрим множество элементов группы  $S$ , соответствующее словам длины кратной  $Cd$  в алфавите  $A$ . Несложно показать, что это нормальная подгруппа группы  $S$ , что возможно только если это единица.

Таким образом для любого элемента группы  $S$  имеем  $s^C = e$ . При чем  $s^i \neq e$  для  $i < C$ . Рассмотрим новые образующие группы  $S$   $X' = (s'_1, \dots, s'_k)$  такие, что  $s'_1(q) = \phi(q, \underbrace{s_1 \dots s_1}_{l_2 \dots l_m}), \dots, s'_k(q) = \phi(q, \underbrace{s_k \dots s_k}_{l_1 \dots l_{k-1}})$ .

Очевидно, что  $\{s_i, s_i^2, \dots, s_i^{C-1}\} = \{s'_i, s_i'^2, \dots, s_i'^{C-1}\}$ . Поэтому  $X'$  образующие группы  $S$ , удовлетворяющие условиям леммы.

2. Пусть  $C = 1$ . Тогда найдутся 2 слова в алфавите  $A$   $(e_1, e_2)$ , такие что  $\phi(q, e_1) = \phi(q, e_2) = q$  и  $l(e_1) - l(e_2) = d$ . Добавляя  $e_1$  и  $e_2$  к образующим мы можем выровнять длины образующих элементов при этом не меняя значений соответствующих элементов группы. Лемма доказана.

**Лемма 6.** Пусть  $M$  — групповой автомат Медведева и известно, что  $Z_p | S_M$ . Тогда  $p | q(M)$ .

**Доказательство.** Рассмотрим множество  $P_t$  подстановок на множестве состояний автомата  $M$ , соответствующих словам длины  $t$ . Последовательность  $P_t$  является периодической с некоторого момента. Действительно, множество подстановок ограничено множеством подмножеств всех подстановок и найдутся индексы  $i$  и  $j$ , такие что  $P_i = P_j$ . Отсюда, очевидно следует, что  $P_{i+1} = P_{j+1}$  а следовательно и периодичность. Обозначим период последовательности  $S_t$  через  $n$ .

Докажем, что  $n | b$ . Действительно по построению цикловых индексов  $P_b = P_{bq} \Rightarrow n | b(q - 1)$ .

С другой стороны заметим, что единица в группе  $S_M$  может соответствовать только словам длины, кратной  $n$ . Действительно, пусть это не так и существует слово длины  $k < n$ , задающее единицу в группе  $S_M$ . Тогда последовательность  $S_t, S_{t+k}, S_{t+2k}, \dots$  является последовательностью вложенных множеств. Так как она возрастает и ограничена, то с какого-то момента она стабилизируется, но тогда  $n | k$ , что неверно. Но мы знаем, что взяв слово длины  $b$   $q$  раз мы получим слово, соответствующее единице. Таким образом существуют единицы длины  $bq$ . Таким образом  $n | bq$ .

Из последних двух утверждений следует, что  $n | b$ . Отсюда очевидно, что  $P_{qb} = P_{2qb} = P_{3qb} = \dots = P_{lqb} = P_{bq^2}$  для  $\forall l$ .

Из леммы 5 и из строения группы  $Z_p$  очевидно, что  $\exists l$  и слова  $\alpha, \beta$  ( $l(\alpha) = l(\beta) = l$ ), такие, что  $\alpha$  задает на некотором множестве

состояний  $q_1, \dots, q_p$  автомата  $M$  единичную подстановку, а  $\beta$  на этом же множестве состояний циклическую перестановку. Но в этом случае то же самое верно и для всех длин, кратных  $l$ , в том числе и  $bql$ , а значит и для  $bq^*$ . Таким образом мы показали, что в множестве  $P_{bq^*}$  всегда есть циклическая подстановка ранга  $p$ , а отсюда следует утверждение леммы. Лемма доказана.

Необходимость теоремы 3 следует из леммы 5 и теоремы 1.

Достаточность: техника синтеза автомата из автоматов с группами, являющимися делителями группы исходного автомата достаточно полно описана в [9].

Теорема 4 прямо следует из теоремы 3 и теоремы 2.

Автор выражает благодарность академику Кудрявцеву В. Б. и проф. Бабину Д. Н. за ценные замечания и внимание к работе.

## Список литературы

- [1] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. М.: Наука, 1985.
- [2] Бабин Д. Н. О полноте двухместных автоматных функций относительно суперпозиции // Дискретная математика. Т. 1, вып. 4. 1989. С. 423–431.
- [3] Кратко М. И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // ДАН СССР. 1964. Т. 155. № 1. С. 35–37.
- [4] Летуновский А. А. О выразимости константных автоматов // Интеллектуальные системы. Т. 9, вып. 1–4. 2005. С. 457–469.
- [5] Бабин Д. Н. О классификации автоматных базисов Поста по разрешимости свойств полноты и А-полноты // ДАН. Т. 367. № 4. 1999. С. 439–441.
- [6] Мальцев А. И. Итеративные алгебры и многообразие Поста // Алгебра и логика. 1966. Т. 5. № 2. С. 5–24.
- [7] Летуновский А. А. Разрешимый случай задачи выразимости автоматных функций относительно суперпозиции // Интеллектуальные системы. Т. 11, вып. 1–4. 2007. С. 769–771.

- [8] Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. М.: Наука, 1982.
- [9] Арбиб М. Алгебраическая теория автоматов языков и полугрупп. М.: Статистика, 1975.