О классификации базисов в P_k по разрешимости проблемы полноты для автоматов

Д. Н. БАБИН
Московский государственный университет им. М. В. Ломоносова
e-mail: babin@intsys.msu.ru

УДК 519.95

Ключевые слова: автоматные функции, проблема полноты, разрешимость, базисы в P_k.

Аннотация

Рассматривается проблема полноты систем автоматных функций вида $\Phi \cup \nu$, где $\Phi \subseteq P_k$, ν конечно. Ранее автор решил эту задачу в случае $k = 2$, а также показал, что для $[\Phi] = P_k$ существует алгоритм распознавания полноты систем $\Phi \cup \nu$. В статье рассматривается случай, когда $[\Phi]$ является максимальным (предполным) классом в P_k. Показано, что если класс Φ вложим в класс Слупецкого, то проблема полноты систем $\Phi \cup \nu$ неразрешима, а если Φ содержит класс сохранения всех констант, то имеет место алгоритмическая разрешимость указанной задачи. Тем самым возникает возможность классификации базисов в P_k, $k \geqslant 3$, по их способности в качестве добавки в автоматный базис обеспечивать алгоритмическую разрешимость проблемы полноты.

Abstract

D. N. Babin, On the classification of bases in P_k according to the decidability of the completeness problem for automata, Fundamentalnaya i prikladnaya matematika, vol. 15 (2009), no. 3, pp. 33—47.

The completeness problem for bases of the form $\Phi \cup \nu$, where $\Phi \subseteq P_k$ and ν is a finite system of automaton functions, is considered. Previously, the problem for $k = 2$ was solved by the author; it was also shown that there is an algorithm for determining the completeness of the system $\Phi \cup \nu$ when $[\Phi] = P_k$. The article is concerned with the case where $[\Phi]$ is the maximal (precomplete) class in P_k. The problem of completeness for systems $\Phi \cup \nu$ is shown to be undecidable if Φ is embedded in a Slupecki class and algorithmically decidable if Φ contains the preserving class of all constants. Thus, the bases in P_k, $k \geqslant 3$, can be classified according to their ability to guarantee the decidability of the completeness problem for automaton functions.

Введение

Решение задачи о полноте относительно операций суперпозиции и обратной связи для конечных систем автоматных функций наталкивается на существенные трудности. Здесь не применима классическая теория полноты, основанная на проверке вложимости тестируемой системы автоматов в максимальные

Фундаментальная и прикладная математика, 2009, том 15, № 3, с. 33—47.
© 2009 *Центр новых информационных технологий МГУ, Издательский дом «Открытые системы»*

классы, ввиду континуальности числа последних [5], а сама задача в общей постановке алгоритмически неразрешима [4].

Случаи алгоритмической разрешимости возникают при ограничении класса проверяемых систем. Первый пример такого рода был построен А. А. Летичевским [7]. Позднее автору удалось показать, что для систем автоматов над P_2, содержащих все булевы функции, задача о полноте алгоритмически разрешима [1]. Алгоритмическая разрешимость задачи полноты была получена и в классе линейных автоматов [9].

Решение задачи не упростилось при рассмотрении более слабого свойства аппроксимационной полноты (А-полноты), когда схема из базисных элементов заменяла автомат лишь до любого наперёд заданного момента времени. Проверка А-полноты для произвольных систем автоматов алгоритмически неразрешима, но есть алгоритм её проверки для систем автоматов, содержащих все булевы функции [3].

В этой ситуации академиком В. Б. Кудрявцевым было предложено использовать разрешимость проблемы автоматной полноты как инструмент для исследования базисов функций, а именно исследовать на полноту (А-полноту) системы вида $\Phi \cup \nu$, где Φ — замкнутый класс функций из P_k (его конечный базис), а ν — конечная система автоматных функций. Автором был полностью исследован случай $k = 2$ и построена классификация базисов в P_2 по их способности гарантировать разрешимость проблемы полноты конечных систем автоматов. Оказалось, что это свойство для класса функций выполнено в точности тогда, когда в классе содержится функция $x \oplus y \oplus z$ или функция $xy \cup xz \cup yz$ [2].

В этой статье указанная классификация продолжается на функции из P_k, $k > 2$, при этом уже на уровне максимальных (предполных) классов обнаружены противоположные случаи.

Основные результаты

Пусть $E_k = \{0, 1, \ldots, k-1\}$. Функции $g\colon E_k^n \to E_k^m$ называются функциями k-значной логики, их множество обозначается через P_k. Пусть

$$E_k^\infty = \{a(1)a(2)\ldots \mid a(j) \in E_k,\ j = 1, 2, \ldots\} -$$

множество всех сверхслов, а

$$E_k^\tau = \{a(1)a(2)\ldots a(\tau) \mid a(j) \in E_k,\ j = 1, 2, \ldots, \tau\} -$$

множество всех слов длины τ. Пусть

$$f\colon (E_k^\infty)^n \to (E_k^\infty)^m -$$

автоматная функция (а-функция), т. е. функция, задающаяся рекуррентно соотношениями

$$\begin{cases} q(1) = q_1, \\ q(t+1) = \varphi\big(q(t), a_1(t), \ldots, a_n(t)\big), \\ b_j(t) = \psi_j\big(q(t), a_1(t), \ldots, a_n(t)\big), \quad j = 1, \ldots, m, \end{cases} \tag{1}$$

где $q \in Q = \{q_1, \ldots, q_r\}$. Параметр q называется состоянием а-функции f, q_1 — её начальным состоянием, вектор-буквы $a = (a_1, \ldots, a_n)$ и $b = (b_1, \ldots, b_m)$ называются входной и выходной буквами, а сверхслова $a(1)a(2)\ldots$ и $b(1)b(2)\ldots$ — входным и выходным сверхсловами соответственно. Класс всех а-функций обозначим через P. В этом классе обычным образом введём операции суперпозиции и обратной связи. Для суперпозиции будем использовать модификации операций из [8]:

$$\begin{cases} (\eta f)(x_1, \ldots, x_n) = f(x_2, x_3, \ldots, x_n, x_1), \\ (\varepsilon f)(x_1, \ldots, x_n) = f(x_2, x_1, x_3, \ldots, x_n), \\ (\Omega f)(x_1, \ldots, x_{n-1}) = f(x_1, x_1, x_2, \ldots, x_{n-1}), \\ (\nabla f)(x_1, x_2, \ldots, x_{n+1}) = f(x_2, x_3, \ldots, x_{n+1}), \\ (f * g)(x_1, x_2, \ldots, x_{m+n-1}) = f(g(x_1, \ldots, x_m), x_{m+1}, \ldots, x_{m+n-1}). \end{cases}$$

Операция обратной связи, применённая к i-й входной и j-й выходной переменным а-функции $f(x_1, \ldots, x_n) = (y_1, \ldots, y_m)$, задаёт а-функцию

$$g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = (y_1, \ldots, y_{j-1}, y_{j+1}, \ldots, y_m),$$

вычисляемую следующим образом. Считаем, что операция обратной связи применима к f в состоянии q, если ψ_j в уравнении (1) фиктивно зависит от a_i при $q(t) = q$, а вычисление $b_s(t)$ осуществляется по схеме

$$\begin{cases} q(1) = q_1, \\ q(t+1) = \varphi\big(q(t), a_1(t), \ldots, a_{i-1}(t), \\ \quad \psi_j\big(q(t), a_1(t), \ldots, a_{i-1}(t), a_{i+1}(t), \ldots, a_n(t)\big), a_{i+1}(t), \ldots, a_n(t)\big), \\ b_s(t) = \psi_s\big(q(t), a_1(t), \ldots, a_{i-1}(t), \psi_j\big(q(t), a_1(t), \ldots, a_{i-1}(t), a_{i+1}(t), \ldots, a_n(t)\big), \\ \quad a_{i+1}(t), \ldots, a_n(t)\big), \quad s = 1, 2, \ldots, j-1, j+1, \ldots, m. \end{cases}$$

Считаем, что операция обратной связи применима к f, если она применима в начальном состоянии q_1 и из её применимости в состоянии $q(t)$ следует применимость в состоянии $q(t+1)$.

Пусть $\nu \subseteq P$, обозначим через $[\nu]$ множество всех а-функций, получающихся из ν с помощью операций суперпозиции и обратной связи. Множество ν называется полным, если $[\nu] = P$. Проблема полноты для P состоит в описании всех полных множеств ν.

Пусть τ — натуральное число, $f(x_1, \ldots, x_n)$ — некоторая автоматная функция, $f^\tau\colon (E_k^\tau)^n \to (E_k^\tau)^m$ — ограничение этой функции на множество слов длины τ. Скажем, что а-функции $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_n)$ τ-равны, если

$f^\tau = g^\tau$. Обозначим через $[\nu]_\tau$ множество всех а-функций, τ-равных получающимся из ν с помощью операций суперпозиции и обратной связи,

$$[\nu]_A = \bigcap_{\tau=1}^{\infty} [\nu]_\tau.$$

Известно [3], что результат применения операции обратной связи τ-равен τ применениям суперпозиции. Множество ν называется τ-полным, если $[\nu]_\tau = P$. Множество ν называется А-полным, если $[\nu]_\tau = P$ при всех τ. Проблема А-полноты для P состоит в описании всех А-полных множеств ν. Очевидно, что полное множество ν является А-полным.

Пусть $P^{(i)}$ — класс всех а-функций с не более чем i состояниями. Тогда

$$P = \bigcup_{i=1}^{\infty} P^{(i)}.$$

Известно [6], что

$$\left[P^{(2)}\right] = P, \quad \left[P^{(1)}\right] = P^{(1)}.$$

А-функции из $P^{(1)}$ называются истинностными, и мы будем отождествлять $P^{(1)}$ с множеством P_k функций k-значной логики, полагая

$$f(a(1)a(2)\ldots) = f\big(a(1)\big)f\big(a(2)\big)\ldots,$$

где $f\colon (E_k)^n \to (E_k)^m$, $f \in P_k$.

Множество функций $f\colon (E_k)^n \to E_k$, для которых выполнено одно из свойств: $n = 1$ или f не принимает всех значений из E_k, называется классом Слупецкого. Известно, что класс Слупецкого замкнут относительно суперпозиции, т. е. результат применения суперпозиции к функциям из этого класса — функция из этого же класса [10]. Будем обозначать класс Слупецкого через SLUP.

Для $l \in \{0, 1, \ldots, k-1\}$ функция $f \in P_k$, такая что $f(l, l, \ldots, l) = l$, называется сохраняющей константу l, а множество всех таких функций — классом сохранения константы l (это множество обозначается через U_l). Обозначим через

$$U = \bigcap_{i=0}^{k-1} U_l$$

класс сохранения всех констант. Известно, что классы U, U_l, $l = 1, 2, \ldots, k-1$, замкнуты относительно суперпозиции, т. е. результат применения суперпозиции к функциям из этих классов — функции из этих же классов [10].

Функция

$$\mathbf{w}(x, y) = \max(x, y) + 1 \bmod k$$

называется функцией Вебба. Известно, что $P_k = [\{\mathbf{w}\}]$, т. е. функция $\mathbf{w}$ образует полную систему в классе k-значных функций.

Автоматная функция $B\colon E_k^\infty \to E_k^\infty$, задаваемая уравнениями

$$\begin{cases} q(1) = k-1, \\ q(t+1) = x(t), \\ b(t) = q(t), \end{cases}$$

называется а-функцией задержки. Известно [6], что

$$[\{B\} \cup \{\mathbf{w}\}] = P.$$

Имеют место следующие утверждения.

Теорема 1. *Пусть $\Phi \subseteq \mathrm{SLUP}$. Тогда не существует алгоритма, по конечному множеству $\nu \subseteq P$ решающего вопрос, верно ли, что $[\Phi \cup \nu] = P$.*

Теорема 2. *Пусть $\Phi \subseteq \mathrm{SLUP}$. Тогда не существует алгоритма, по конечному множеству $\nu \subseteq P$ решающего вопрос, верно ли, что $[\Phi \cup \nu]_A = P$.*

Теорема 3. *Для любого $\Phi \supseteq U$ существует алгоритм, по конечному множеству $\nu \subseteq P$ решающий, верно ли, что $[\Phi \cup \nu] = P$.*

Теорема 4. *Для любого $\Phi \supseteq U$ существует алгоритм, по конечному множеству $\nu \subseteq P$ решающий, верно ли, что $[\Phi \cup \nu]_A = P$.*

Замечание. Пусть $F_1 \subseteq F \subseteq P_k$. Если не существует алгоритма, по конечному множеству $\nu \subseteq P$ решающего вопрос о полноте (A-полноте) множества $F \cup \nu$, то не существует и алгоритма, решающего вопрос о полноте (A-полноте) множества $F_1 \cup \nu$.

Из замечания следует, что достаточно доказать теоремы 1—4 только для случая $\Phi = \mathrm{SLUP}$, $\Phi = U$.

Автор выражает благодарность академику В. Б. Кудрявцеву за постановку задачи и ценные указания.

1. Основные леммы и доказательство теорем

Тройка $T = \langle D, \rho, W\rangle$, где $D = \{d_1, \ldots, d_k\}$, $\rho\colon D \to D^*$, $\rho(d_i) = R_i$, W — натуральное число, называется системой однородных продукций Поста. Если $l \geqslant W$, то скажем, что T применима к слову

$$\xi = d_{i_1} d_{i_2} \ldots d_{i_l},$$

и назовём слово

$$\xi' = d_{i_{w+1}} \ldots d_{i_l} R_{i_1}$$

результатом применения T к слову ξ. У слова ξ «стираются» первые W букв и к нему приписывается слово R_{i_1}, которое соответствует букве d_{i_1}. Если $l < W$, то T не применима к слову ξ. Последовательность $\xi_1, \xi_2, \ldots$, в которой $\xi_1 = \xi$, а ξ_{i+1} — результат применения T к слову ξ_i, $i = 1, 2, \ldots$, назовём последовательностью продукций слова ξ. Последовательность продукций слова ξ конечна,

если последнее слово имеет длину, меньшую W. В этом случае будем говорить, что при применении к слову ξ система T останавливается через конечное число шагов. Для каждой однородной системы продукций T можно поставить вопрос о разрешимости «проблемы остановки» этой системы: существует ли алгоритм A_T, который по любому наперёд заданному слову ξ устанавливает, конечно или бесконечно множество T-продукций слова ξ, т. е. останавливается ли T при применении к слову ξ или нет. Известно [8], что существует система однородных продукций Поста, для которой не существует алгоритма, по слову $\xi \in D^*$ решающего вопрос о конечности последовательности продукций слова ξ. Сформулируем этот факт в виде леммы [8].

Лемма 1. *Существует система однородных продукций Поста $T = \langle D, \rho, W\rangle$, для которой не существует алгоритма, решающего проблему остановки.*

Обозначим через $\mathbb{N}_0$ множество натуральных чисел с нулём. Зафиксируем систему продукций Поста $T = \langle D, \rho, W\rangle$ с неразрешимой проблемой конечности последовательности продукций, и пусть $|D| = r$.

Пусть $\tilde{R}$ — множество сверхслов α, таких что

$$\{\alpha(t+1), \alpha(t+2), \ldots, \alpha(t+k)\} \neq E_k \quad \text{при всех} \quad t \geqslant t_\alpha.$$

Запишем $w, v \in E_k^k$ как

$$w = 0\,1 \ldots (k-1), \quad v = (k-1)(k-2)\ldots 0.$$

Определим сверхслова

$$w^\infty = w\,w\ldots, \quad 1^\infty = 1\,1\ldots, \quad 0^\infty = 0\,0\ldots$$

и функции

$$u\colon E_k^\infty \to E_k^\infty, \quad u_i\colon E_k^\infty \to E_k^\infty,$$
$$u(a\alpha) = aw^\infty, \quad u_i(a\alpha) = iw^\infty, \qquad i = 0, 1, \ldots, k-1, \quad a \in E_k, \quad \alpha \in E_k^\infty.$$

Через $\alpha]_t$ обозначим начало длины t сверхслова $\alpha \in E_k^\infty$, через $|\alpha'|$ — длину слова α'. Каждому элементу $d_i \in D$ поставим в соответствие слово

$$\tilde{d}_i = v^i w v^{r-i}, \quad \tilde{d}_i \in E_k^{k(r+1)}.$$

Для $\xi = d_{i_1} \ldots d_{i_s}$ обозначим $\tilde{\xi} = \tilde{d}_{i_1} \ldots \tilde{d}_{i_s}$.

Для $\alpha \neq \beta$, $\alpha, \beta \in E_k^\infty$, определим числовую функцию

$$c(\alpha, \beta) = \max_{\alpha]_t = \beta]_t} t.$$

Пусть

$$M_i^1 = \left\{w^n \tilde{d}_i \tilde{d}_{j_1} \ldots \tilde{d}_{j_l} w^\infty \mid n, l \in \mathbb{N}_0,\ j_1, \ldots, j_l \in \{1, \ldots, r\}\right\},$$
$$M_i^2 = \left\{w^n \tilde{d}_i \tilde{d}_{j_1} \tilde{d}_{j_2} \ldots \mid n \in \mathbb{N}_0,\ j_1, j_2, \ldots \in \{1, \ldots, r\}\right\}.$$

Для $\alpha \notin M_i^1 \cup M_i^2$ определим $c_i\colon E_k^\infty \to \mathbb{N}$, полагая

$$c_i(\alpha) = \max_{\beta \in M_i^1 \cup M_i^2} c(\alpha, \beta).$$

Пусть

$$\Delta = w^n \tilde{d}_i \tilde{d}_{j_1} \dots \tilde{d}_{j_l} w^\infty, \quad n \in \mathbb{N}_0.$$

Определим а-функции

$$f_i \colon E_k^\infty \to E_k^\infty, \quad i = 1, \dots, r,$$

соотношениями (a), (b), (c), (d):

(a) $f_i(a\Delta) = a w^{n+Wk(r+1)} \tilde{d}_{j_w} \dots \tilde{d}_{j_l} \tilde{R}_i w^\infty$ при $l > W-1$,

(b) $f_i(a\Delta) = a w^{n+Wk(r+1)} \tilde{R}_i w^\infty$ при $l = W-1$,

(c) $f_i(a\Delta) = a w^\infty$ при $l < W-1$,

(d) $f_i(a\beta) = a\beta' bb \dots$ при $\beta \notin M_i^1 \cup M_i^2$, где $|\beta'| = c_i(\beta) - 1$, $b \in E_k$.

Определим а-функции

$$f_i' \colon E_k^\infty \to E_k^\infty, \quad i = 1, \dots, r,$$

соотношениями (a), (b), (c'), (d):

(c') $f_i'(a\Delta) = a w^{n+lk(r+1)} 1\,1 \dots$ при $l < W-1$.

Определим а-функции G, E, I, f_ξ для $\alpha, \beta, \gamma \in E_k^\infty$, $a, b \in E_k$ следующим образом:

$$G(\alpha, a\gamma) = \begin{cases} a(k-1)(k-1)\dots \text{ при } a \neq k-1, \\ B(\alpha) \text{ при } a = k-1,\ \gamma = w^\infty, \\ (k-1)\alpha'\, b\, b \dots \text{ при } a = k-1,\ \gamma \neq w^\infty,\ |\alpha'| = c(\gamma, w^\infty) - 1, \end{cases}$$

$$E(\alpha, \beta, a\gamma) = \begin{cases} a\,\alpha(2) \oplus \beta(2)\alpha(3) \oplus \beta(3) \dots \text{ при } \gamma = w^\infty, \\ a\,\alpha'\, b\, b \dots \text{ при } \gamma \neq w^\infty,\ |\alpha'| = c(\gamma, w^\infty) - 1, \end{cases}$$

$$I(\alpha, \beta) = \alpha(1) \oplus \beta(1)\, 1\, 1 \dots, \quad f_\xi(a\alpha) = a\bar{\xi} w^\infty.$$

Через $\hat{g}_i(x, y)$, $i = 1, \dots, m_2$, обозначим двухместные функции из P_k, не принимающие всех значений из E_k, а через $\hat{h}_i(x)$, $i = 1, \dots, m_1$, обозначим одноместные функции из P_k, принимающие все значения. Нетрудно убедиться, что функции $\hat{g}_i(x, y)$, $i = 1, \dots, m_2$, $\hat{h}_i(x)$, $i = 1, \dots, m_1$, порождают класс Слупецкого, в котором также лежат все константные функции.

Имеют место следующие леммы.

Лемма 2. *Система*

$$\Sigma = \{\hat{g}_i(x, y),\ i = 1, \dots, m_2,\ \hat{h}_i(x),\ i = 1, \dots, m_1,\ I,\ E,\ f_1, \dots, f_r,\ f_\xi,\ G\}$$

полна тогда и только тогда, когда последовательность продукций слова ξ конечна.

Лемма 3. *Система*

$$\Sigma' = \{\hat{g}_i(x, y),\ i = 1, \dots, m_2,\ \hat{h}_i(x),\ i = 1, \dots, m_1,\ I,\ E,\ f_1', \dots, f_r',\ f_\xi,\ G\}$$

A-полна тогда и только тогда, когда последовательность продукций слова ξ бесконечна.

Доказательство теорем 1 и 2 следует из лемм 2 и 3 соответственно.

Известны следующие теоремы.

Теорема 5 [1]. *Существует алгоритм, по конечному множеству $\nu \subset P$ решающий, верно ли, что $[P_k \cup \nu] = P$.*

Теорема 6 [3]. *Существует алгоритм, по конечному множеству $\nu \subset P$ решающий, верно ли, что $[P_k \cup \nu]_A = P$.*

Теоремы 3 и 4 будут доказаны сведением к теоремам 5 и 6. Для этого необходимо указать алгоритм определения выразимости константных истинностных функций через а-функции из ν и U.

Для доказательства теорем 3, 4 введём следующие определения. Для натуральных D, N автоматную функцию с уравнениями (1), где

$$m = D + N + k, \quad n = 0, \quad Q = \{1, \dots, D + N\}$$

и для любых $i \in Q$, $a \in E_k^n$ выполнено

$$\psi(i,a) = \Big(\big(i, i \oplus 1, \dots, i \oplus (k-1)\big), (0, 0, \dots, 0, \overset{i}{1}, 0, \dots, 0)\Big),$$

$$\phi(i,a) = \begin{cases} i+1 & \text{при } i < D+N, \\ D+1 & \text{при } i = D+N, \end{cases}$$

назовём (D,N)-счётчиком и обозначим через $B_{D,N}$. Здесь $\oplus$ обозначает сложение по модулю k.

Заметим, что счётчик $B_{D,N}$ выдаёт всегда одну и ту же последовательность с периодом N и предпериодом D. Кроме того, в моменты, не сравнимые по модулю N, функция $B_{D,N}$ выдаёт разные буквы и ни в какой момент времени не сохраняет никаких констант. Множество всех счётчиков обозначим через K.

При доказательстве теорем 3, 4 без ограничения общности будем исследовать на полноту системы вида $\{f\} \cup U$, где f задаётся уравнениями (1). Для а-функции f, заданной соотношениями (1), и $D \leqslant s$ последовательность

$$\big(a(1), b(1)\big), \big(a(2), b(2)\big), \dots, \big(a(s), b(s)\big), \tag{2}$$

где

$$a(1), \dots, a(s) \in E_k^n, \quad q(1), \dots, q(s) \in Q,$$
$$b(1), \dots, b(s) \in E_k^m, \quad b(i) = \psi\big(q(i), a(i)\big),$$
$$q(t+1) = \phi\big(q(i), a(i)\big), \quad i = 1, \dots, s, \quad q(1) = q_1,$$

назовём (s)-экспериментом с а-функцией f. Если же ещё выполнено

$$q(D+1) = \phi\big(q(s), a(s)\big),$$

то назовём её (D,s)-экспериментом с а-функцией f.

Пусть i, j — натуральные числа, $1 \leqslant i, j \leqslant s$, $j \neq i$. Скажем, что а-функция f является (j,i)-зависимой на (D,s)-экспериментах ((s)-экспериментах), если для *каждой* последовательности (2) выполнено соотношение

$$\psi\big(q(j), a(i)\big) = b(i). \tag{3}$$

Скажем, что а-функция f сохраняет константу $l \in \{0, \ldots, k-1\}$ в j-й момент на (D,s)-экспериментах ((s)-экспериментах), если на *каждой* последовательности (2) выполнено

$$\psi\big(q(j), (l, l, \ldots, l)\big) = (l, l, \ldots, l).$$

Скажем, что а-функция f имитирует счётчик $B_{D,N}$ на циклических экспериментах, если для некоторого $s = D + pN$ и любых $1 \leqslant i, j \leqslant s$, $i \neq j \bmod N$, а-функция f не является (j,i)-зависимой и не сохраняет константу $l \in \{0, \ldots, k-1\}$ в j-й момент на (D,s)-экспериментах при всех l и j. Скажем, что а-функция f имитирует счётчик $B_{D,N}$ на простых экспериментах, если для некоторого $s = D + N$ и любых $i \neq j, 1 \leqslant i,\ j \leqslant s$, а-функция f не является (j,i)-зависимой и не сохраняет константу $l \in \{0, \ldots, k-1\}$ в j-й момент на (s)-экспериментах при всех l и j.

Имеют место следующие леммы.

Лемма 4. *Соотношение $[\{f\} \cup U] \supseteq K$ имеет место в точности тогда, когда для любых натуральных D, N функция f имитирует счётчик $B_{D,N}$ на циклических экспериментах.*

Лемма 5. *Свойство функции f для любых натуральных D, N имитировать счётчик $B_{D,N}$ на циклических экспериментах алгоритмически проверяемо.*

Лемма 6. *Соотношение $[\{f\} \cup U]_A \supseteq K$ имеет место в точности тогда, когда для любого натурального s функция f имитирует счётчик $B_{0,s}$ на простых экспериментах.*

Лемма 7. *Свойство функции f для любого натурального s имитировать счётчик $B_{0,s}$ на простых экспериментах алгоритмически проверяемо.*

Доказательство теорем 3 и 4 следует из теорем 5 и 6, лемм 4—7 и того факта, что $[K \cup U] \supseteq P_k$.

Доказательство лемм 2 и 3

Пусть S — схема над множеством а-функций Σ. Правым путём в схеме S назовём такую последовательность элементов $g_1, g_2, \ldots, g_n$ схемы S, что выход а-функции g_1 совпадает с выходом схемы, а выходы а-функций g_{i+1} для многоместных g_i соединены с правым входом g_i, а для одноместных g_i с их единственным входом. Элемент g_n называется начальным элементом пути.

Утверждение. *Пусть некоторая схема S над системой Σ реализует константную а-функцию с выходным сверхсловом $(k-1)w\,w\,\alpha$. Тогда в схеме S существует правый путь с начальным элементом $g \in \{I,\ \hat{g}_i(x,y),\ i = 1, \ldots, m_2\}$.*

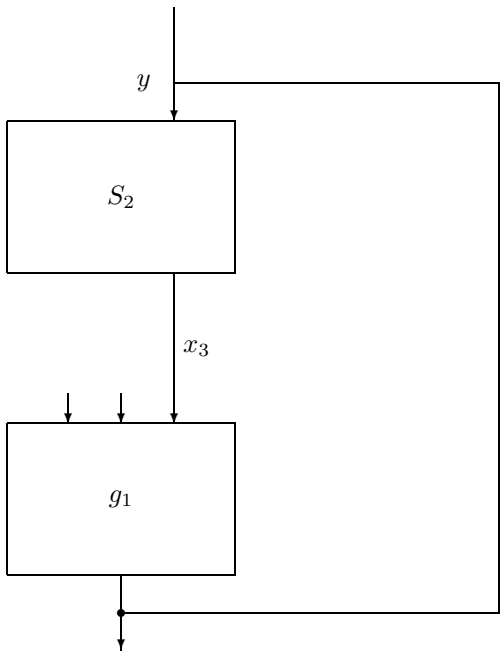

Рис. 1

Доказательство. Пусть схема S_1 над Σ получается из схемы S заменой а-функций на функции их начальных состояний. Схема S_1 реализует константу $k-1$ и состоит из функций начальных состояний

$$\{\hat{g}_i(x,y),\ i=1,\dots,m_2,\ \hat{h}_i(x),\ i=1,\dots,m_1,\ x\oplus y,\ z,\ x\dots x,\ y\}$$

системы

$$\Sigma=\{\hat{g}_i(x,y),\ i=1,\dots,m_2,\ \hat{h}_i(x),\ i=1,\dots,m_1,\ I,\ E,\ f_1,\dots,f_k,\ f_\xi,\ G\}.$$

Представим схему S_1 в виде, приведённом на рис. 1. Пусть g_1 — элемент схемы S_1, выход которого совпадает с выходом схемы, и пусть $g_1\notin \notin\{I,\ \hat{g}_i(x,y),\ i=1,\dots,m_2\}$. Тогда выходная функция его начального состояния взаимно-однозначна, а значит, схема S_2 имеет фиктивный вход y (который можно отбросить), а на выходе x_3 реализуется константа. Продолжая эту процедуру, мы получим искомый путь. Утверждение доказано. □

Доказательство леммы 2. Достаточность. Пусть последовательность продукций слова ξ конечна и имеет вид $\xi_1,\xi_2,\dots,\xi_s$, первая буква слова ξ_j есть d_{ij} и длина слова ξ_s меньше W. Тогда

$$u(x)=f_{i_s}\Big(f_{i_{s-1}}\big(\dots f_{i_1}\big(f_\xi(x)\big)\dots\big)\Big),\quad u(k-1)=u_{k-1}.$$

Непосредственной проверкой можно убедиться в том, что

$$E\Big(x, y, u\big(I(x,y)\big)\Big) = x \oplus y, \quad G(x, u_{k-1}) = B(x).$$

Существенная функция $x \oplus y$ вместе с функциями класса Слупецкого [10] порождает полную в P_k систему истинностных функций. Значит, система Σ полна.

Необходимость. Пусть система Σ полна и некоторой схемой S над Σ выразима константная а-функция с выходным сверхсловом $(k-1)\,w^\infty$. Из утверждения получаем, что в схеме S существует правый путь $g_1, \ldots, g_n$ с начальным элементом $g_n \in \{I,\ \hat{g}_i(x,y),\ i = 1, \ldots, m_2\}$. Среди $g_1, \ldots, g_{n-1}$ найдётся элемент типа f_ξ, в противном случае схема S будет выдавать сверхслово из $\tilde{R}$, что приводит к противоречию. Пусть g_{i_0} — элемент типа f_ξ с минимальным номером i_0, и пусть для определённости $\xi = d_i d_{j_1} \ldots d_{j_l}$. Тогда либо $\hat{g}_{i_0-1}$ — взаимно-однозначная одноместная функция, либо g_{i_0-1} — элемент типа f_i. В других случаях схема S обязана выдавать слово из $\tilde{R}$, что приводит к противоречию. Просмотрев таким образом всю цепочку $g_{i_0}, \ldots, g_1$, получим, что последовательность $g_n, \ldots, g_1$ содержит конечную подпоследовательность $f_\xi, f_i, \ldots, f_{i_s}$, соответствующую конечной последовательности продукций слова ξ. Лемма доказана. □

Доказательство леммы 3. Достаточность. Пусть система $\xi_1, \xi_2, \ldots$ продукций слова ξ бесконечна, первая буква слова ξ_j есть d_{ij}. Тогда для любого τ на всех словах δ длины τ $u(\delta)$ совпадает с $f'_{i_\tau}\Big(f'_{i_{\tau-1}}\big(\ldots f'_{i_1}\big(f_\xi(\delta)\big)\ldots\big)\Big)$ и $u\big((k-1)\,\delta\big)$ совпадает с $u_{k-1}(a\,\delta)$. Непосредственной проверкой можно убедиться в том, что

$$E\Big(x, y, u\big(I(x,y)\big)\Big) = x \oplus y, \quad G(x, u_{k-1}) = B(x).$$

Существенная функция $x \oplus y$ вместе с функциями класса Слупецкого порождает полную в P_k систему истинностных функций. Значит, система Σ' τ-полна при всех τ, т. е. она A-полна.

Необходимость. Пусть, от противного, система Σ' A-полна и при этом система продукций слова ξ конечна и имеет вид $\xi_1, \xi_2, \ldots, \xi_s$. Выберем $\tau = Wks(r+1) + k + 1$ и рассмотрим все а-функции из Σ' на словах длины τ.

Пусть схема S над Σ' реализует константную а-функция с выходным сверхсловом $(k-1)\,w^\infty]_\tau$. Из утверждения получаем, что в схеме S существует правый путь $g_1, \ldots, g_n$ с начальным элементом $g_n \in \{I,\ \hat{g}_i(x,y),\ i = 1, \ldots, m_2\}$. Обозначим через A_τ множество слов α длины τ, таких что

$$\big\{\alpha\big(\tau - (k-1)\big), \alpha\big(\tau - (k-2)\big), \ldots, \alpha(\tau)\big\} \neq E_k.$$

В словах из A_τ последние k букв неразнозначны.

Среди $g_1, \ldots, g_{n-1}$ найдётся элемент типа f_ξ, в противном случае схема S будет выдавать сверхслово из A_τ, что приводит к противоречию. В самом деле, начальный элемент пути $g_n \in \{I,\ \hat{g}_i(x,y),\ i = 1, \ldots, m_2\}$ всегда выдаёт слова из A_τ, однозначные функции их не выводят из A_τ, по определению функций

E, G, f'_i нарушение разнозначности на (правом) входе в кортеже из последних τ букв приводит к выдаче одной и той же буквы с предыдущего такта.

Пусть g_{i_0} — элемент типа f_ξ с минимальным номером i_0, и пусть для определённости $\xi = d_i d_{j_1} \dots d_{j_l}$. Тогда либо g_{i_0-1} — взаимно-однозначная одноместная функция, либо g_{i_0-1} — элемент f_i. В других случаях схема S обязана выдавать слово из A_τ, что приводит к противоречию. Просмотрев таким образом всю цепочку $g_{i_0}, \dots, g_1$, получим, что последовательность $g_n, \dots, g_1$ обязана содержать конечную подпоследовательность f_ξ, $f_i, \dots, f_{i_s}$, соответствующую конечной последовательности продукций слова ξ. Значит, по соотношению (c') на выходе f_{i_s} всё-таки получится слово из A_τ, что приводит к противоречию. Таким образом, предположение об A-полноте и одновременной конечности системы продукций слова ξ неверно. Лемма доказана. □

2. Доказательство лемм 4—7

Доказательство леммы 4. Необходимость. Предположим, что через а-функции из $\{f\} \cup U$ выражена а-функция g, равная $B_{D,N}$. Это значит, что найдутся натуральные p, D, $s = D + pN$, такие что а-функция g не является (j,i)-зависимой ни при каких $i \neq j \bmod N$ и не сохраняет констант в j-й момент ни при каких j. Зафиксируем для определённости $i < j$.

Если а-функция g получилась операцией обратной связи последнего выхода с последним входом из а-функции $\tilde{g}$, то $\tilde{g}$ также не будет (j,i)-зависимой. В самом деле, пусть при этом эксперимент (2) а-функции g нарушает (j,i)-зависимость и получился из эксперимента (4), который её сохранял:

$$\Big(\big(a(1),e(1)\big),\big(b(1),e(1)\big)\Big),\dots,\Big(\big(a(s),e(s)\big),\big(b(s),e(s)\big)\Big). \tag{4}$$

Это означает, что $b = \psi\big(q(j),a(i)\big) \neq b(i)$. Пусть входная буква $a(i)$ в диаграмме g в состоянии $q(j)$ получилась из входной буквы $(a(i),e)$ в диаграмме $\tilde{g}$ в состоянии $q(j)$. Тогда имеем

$$\psi_{\tilde{g}}\big(q(j),(a(i),e)\big) = (b,e), \quad \psi_{\tilde{g}}\Big(q(j),\big(a(i),e(i)\big)\Big) = (b',e').$$

По правилу применимости операции обратной связи имеем $e = e'$, если есть сохранение (j,i)-зависимости для $\tilde{g}$, то $e' = e(i)$. Тогда $b' = b = b(i)$, а это означает сохранение (j,i)-зависимости для g, что приводит к противоречию.

Если $\psi_{\tilde{g}}$ в некотором состоянии сохраняла константу l, то подача обратной связи на несущественный для неё вход не может изменить этого свойства.

Пусть теперь g получилась суперпозицией а-функций g_1 и g_2 и эксперимент (2) получился из экспериментов

$$\big(a(1),c(1)\big),\dots,\big(a(s),c(s)\big), \quad \big(c(1),b(1)\big),\dots,\big(c(s),b(s)\big),$$

а-функций g_1 и g_2 соответственно. Если предположить, что g_1 и g_2 сохраняют (j,i)-зависимость, то получим, что g также сохраняет (j,i)-зависимость. Значит, хотя бы одна из а-функций g_1 или g_2 не сохраняет (j,i)-зависимость на

(D,s)-экспериментах. Очевидно, что не сохраняющая константу функция не может быть получена суперпозицией функций, эту константу сохраняющих.

Заметим, что всякая истинностная а-функция сохраняет все (j,i)-зависимости на всех (D,s)-экспериментах. Повторяя эти рассуждения, мы получим, что сама базисная а-функция f не должна сохранять (j,i)-зависимость на (D,s)-экспериментах при $i \neq j \bmod N$ и не должна сохранять констант во все моменты. Значит, f имитирует счётчик $B_{D,N}$ при всех натуральных D, N на своих циклических экспериментах. Необходимость доказана.

Достаточность. Для фиксированных N, D, k, $s = D + kN$ и некоторого j рассмотрим множество всех (D,s)-экспериментов P с а-функцией f, имитирующей счётчик $B_{D,N}$. Пусть $|P| = t$ и g_j — параллельное соединение t копий а-функции f. Пусть g_j описывается уравнениями (1) и $\alpha_l \in P$ — l-й эксперимент из P:

$$\alpha_l = \big(a^{(l)}(1), b^{(l)}(1)\big), \big(a^{(l)}(2), b^{(l)}(2)\big), \ldots, \big(a^{(l)}(s), b^{(l)}(s)\big), \quad l = 1, 2, \ldots, t,$$

$$a(i) = \big(a^{(1)}(i), \ldots, (a^{(t)}(i)\big), \quad b(i) = \big(b^{(1)}(i), \ldots, (b^{(t)}(i)\big), \quad i = 1, 2, \ldots, s.$$

Можно считать, что среди $\alpha(1), \alpha(2), \ldots, \alpha(s)$ нет равных и нет наборов вида $(l, l, \ldots, l)$ (в противном случае можно добавить фиктивные входы и выбрать $\alpha(1), \alpha(2), \ldots, \alpha(s)$ попарно различными).

Рассмотрим (D,s)-эксперимент (2) с а-функцией g_j. Для $a \in E_k^n$ определим функцию $h_j \in U$:

$$h_j \colon E_k^{m+n} \to E_k^n,$$

$$h_j(x,y) = \begin{cases} a(i) & \text{для } x = a(i),\ y = b(i),\ i = 1, \ldots, s, \\ a(j) & \text{для } x \in E_k^n,\ y = \psi(q(j), x). \end{cases}$$

Это можно сделать из-за отсутствия (j,i)-зависимостей и несохранения констант. В состоянии $q(j)$ выходная функция а-функция $f_j(x) = h_j\big(x, q_j(x)\big)$ принимает значение $a(j)$ для всех входных букв, т. е. является константой. Рассмотрим а-функцию

$$F_{N,D,k}(x) = f_s\big(\ldots f_2\big(f_1(x)\big)\ldots\big)$$

с начальным состоянием $\big(q(1), q(1), \ldots q(1)\big)$, имеющую n входов и n выходов. В состоянии $\big(q(j), q(j), \ldots q(j)\big)$ реализуется константа $a(j)$. После n применений операции обратной связи от соответствующих выходов к соответствующим входам получится а-функция, с точностью до перекодировки функциями из U равная $B_{D,N}$. Достаточность доказана. □

Доказательство леммы 5. Пусть ${Q_p}^T \subseteq Q$ — множество состояний а-функции f, достижимых из состояния p за T тактов, а R_L — множество состояний, из которых достижимо состояние L. Пусть

$$Q_{p,L}^T = {Q_p}^T \cap R_L.$$

Тогда

$$Q_{p,L}^{T+1} = \{\phi(p,a) \mid a \in E_k^m,\ p \in Q_{p,L}^T\} \cap R_L.$$

Последовательность $Q^T_{p,L}$, $T = 1, 2, \ldots$, будет детерминированной, а значит, и периодической.

Выберем период и предпериод этой последовательности, равный, для простоты, одному и тому же числу ρ при всех $p, L \in Q$. Очевидна грубая оценка

$$\rho \leqslant \left(k^{|Q|}!\right).$$

Для любых $p, L \in Q$ и любого натурального T выполнено

$$Q^T_{p,L} = Q^{T+\rho}_{p,L}.$$

Возьмём, к примеру, следующий случай расположения чисел D, s, i, j:

$$D < D + \rho < i < i + \rho < j < s - \rho < s.$$

Если для (D, s)-экспериментов выполнена (j, i)-зависимость, то для (D_1, s_1)-экспериментов будет выполнена (j_1, i_1)-зависимость, где

$$D_1 < D_1 + \rho < i_1 < D + 2\rho < j_1 < s_1 < j_1 + \rho,$$

D_1, D, i_1, i, j_1, j, s_1, s попарно совпадают по модулю ρ. Это следует из того, что для каждого $p \in Q^D_{q_1,p}$ имеем $Q^D_{q_1,p} = Q^{D_1}_{q_1,p}$ и $Q^i_{p,p} = Q^{i_1}_{p,p}$; для каждого $r \in Q^{i-D}_{p,p}$ имеем $Q^{j-i}_{r,p} = Q^{j_1-i_1}_{r,p}$; для каждого $l \in Q^{j-i}_{r,p}$ имеем $Q^{s-j}_{l,p} = Q^{s_1-j_1}_{l,p}$.

В случае другого расположения чисел D, j, i мы таким же способом сократим интервалы между числами 1, D, j, i. Следовательно, наличие или отсутствие (j, i)-зависимости на (D, s)-экспериментах (а также сохранение констант) равносильно соответственно наличию или отсутствию (j_1, i_1)-зависимости (а также сохранению констант) на (D_1, s_1)-экспериментах при $D_1 \leqslant s_1 \leqslant 5\rho$. Последний факт проверяется перебором всех (D_1, s_1)-экспериментов. Лемма 5 доказана. □

Леммы 6 и 7 доказываются аналогично леммам 4 и 5 соответственно.

Литература

[1] Бабин Д. Н. Разрешимый случай задачи о полноте автоматных функций // Дискрет. мат. — 1992. — Т. 4, № 4. — С. 41—56.

[2] Бабин Д. Н. О классификации автоматных базисов Поста по разрешимости свойств полноты и А-полноты // Докл. РАН. — 1999. — Т. 367, № 4. — С. 439—441

[3] Буевич В. А. Условия А-полноты для автоматов. — М.: Изд-во Моск. ун-та, 1986.

[4] Кратко М. И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // ДАН СССР. — 1964. — Т. 155, № 1. — С. 35—37.

[5] Кудрявцев В. Б. О мощностях множеств предполных классов некоторых функциональных систем, связанных с автоматами // ДАН СССР. — 1963. — Т. 151, № 3. — С. 493—496.

[6] Кудрявцев В. Б., Алёшин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

[7] Летичевский А. А. Условия полноты для конечных автоматов // ЖВМ и МФ. — 1961. — № 4. — С. 702—710.

[8] Мальцев А. И. Алгоритмы и рекурсивные функции. — М.: Наука, 1986.

[9] Часовских А. А. О полноте в классе линейных автоматов // Мат. вопросы кибернетики. — 1995. — № 3. — С. 140—166.

[10] Яблонский С. В. Функциональные построения в k-значной логике // Тр. Мат. ин-та им. В. А. Стеклова АН СССР. — 1958. — Т. 51. — С. 5—142.