

Алгоритм полноты систем автоматных функций с полной булевой частью

Д.Н. Бабин

Рассматриваются автоматные базисы с полной булевой частью. Построен алгоритм для проверки полноты таких базисов и получены верхние оценки его сложности.

Введение

Известно, что решение задачи о полноте относительно операций суперпозиции и обратной связи для систем автоматных функций наталкивается на существенные трудности. Так в работе [1] установлена континуальность всякой критериальной системы для этой задачи, а позднее в работе [2] установлена ее алгоритмическая неразрешимость для конечных систем автоматных функций. Вместе с тем, для специальных систем автоматов, выдающих номер своего состояния (автоматов Медведева) и содержащих все булевы функции, указанная задача алгоритмически разрешима [3]. Ранее, в работе [4] автором было показано, что при наличии булевых функций алгоритмически разрешима проблема полноты и для произвольных систем автоматов, и даже не все булевы функции для этого нужны [5, 6, 7]. Возникший при этом аппарат сохраняемых предикатов на экспериментах с автоматами, позволил упростить доказательство работы [4]. Новый вариант доказательства приводится в настоящей работе.

1. Основные понятия и результаты

Пусть $E_2 = \{0, 1\}$, E_2^∞ — множество всех сверхслов $a(1)a(2)\dots$, где $a(j) \in E_2, j = 1, 2, \dots$; Пусть

$$f : (E_2^\infty)^n \rightarrow (E_2^\infty)^m$$

— автоматная функция (а.-функция), то есть она задается рекуррентно соотношениями, где $q \in Q = \{q_1, \dots, q_r\}$.

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

Параметр q называется состоянием а.-функции f , q_1 — ее начальным состоянием, вектор — буквы $a = (a_1, \dots, a_n)$ и $b = (b_1, \dots, b_m)$ называются входной и выходной буквами, а сверхслова $a(1)a(2)\dots$ и $b(1)b(2)\dots$ — входным и выходным сверхсловами, соответственно. Класс всех а.-функций обозначим через P_a . Если $|Q| = 1$, то автоматную функцию (1) можно отождествить с булевой вектор-функцией $\psi_j(q(t), a_1(t), \dots, a_n(t))$ и считать булевы функции частным случаем автоматных. Известно, что все булевы функции порождаются одной функцией $\bar{x} \vee \bar{y}$.

В классе автоматных функций введем операции суперпозиции и обратной связи. Для суперпозиции будем использовать операции:

$$\begin{cases} (\eta f)(x_1, \dots, x_n) = f(x_2, x_3, \dots, x_n, x_1), \\ (\epsilon f)(x_1, \dots, x_n) = f(x_2, x_1, x_3, \dots, x_n), \\ (\Omega f)(x_1, \dots, x_{n-1}) = f(x_1, x_1, x_2, \dots, x_{n-1}), \\ (\nabla f)(x_1, x_2, \dots, x_{n+1}) = f(x_2, x_3, \dots, x_{n+1}), \\ (f * g)(x_1, x_2, \dots, x_{l+n-1}) = f(g(x_1, \dots, x_l), x_{l+1}, \dots, x_{l+n-1}). \end{cases}$$

Операция обратной связи (о.с.), примененная к i -ой входной и j -ой выходной переменным а.-функции $f(x_1, \dots, x_n) = (y_1, \dots, y_m)$, задает а.-функцию

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

вычисляемую алгоритмически следующим образом. Считаем, что о.с. 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

$$\left\{ \begin{array}{l} q(1) = q_1, \\ q(t+1) = \varphi(q(t), a_1(t), \dots, a_{i-1}(t), \psi_j(q(t), a_1(t), \dots, a_{i-1}(t)), \\ \quad a_{i+1}(t), \dots, a_n(t)), a_{i+1}(t), \dots, a_n(t)), \\ b_s(t) = \psi_s(q(t), a_1(t), \dots, a_{i-1}(t), \psi_j(q(t), a_1(t), \dots, a_{i-1}(t)), \\ \quad a_{i+1}(t), \dots, a_n(t)), a_{i+1}(t), \dots, a_n(t)), \\ s = 1, 2, \dots, j-1, j+1, \dots, m. \end{array} \right.$$

Считаем, что о.с. применима к f , если она применима в начальном состоянии q_1 , и из ее применимости в состоянии $q(t)$ следует применимость в состоянии $q(t+1)$. Пусть $M \subseteq P_a$, обозначим через $[M]$ множество всех а.-функций, получающихся из M с помощью операций суперпозиции и обратной связи. Множество M называется полным, если $[M] = P_a$. Проблема полноты для P_a состоит в описании всех полных множеств M .

Имеет место теорема:

Теорема 1. *Для конечной системы $M \subset P_a$ равенство $[M \cup \{\bar{x} \vee \bar{y}\}] = P_a$ алгоритмически проверяемо, и число шагов проверки не превосходит $(2^{2^{|Q|^2+1}})!$.*

2. Основные леммы и доказательство теоремы

Обозначим через $\bar{X}, \mathbf{1}, \mathbf{0}, f_{\text{ш}}, f_{\&}, f_{\vee}$ автоматные интерпретации истинностных функций, соответственно, $\bar{x}, 1, 0, \bar{x}_1 \vee \bar{x}_2, x_1 \& x_2, x_1 \vee x_2$.

Для натуральных D, N автоматную функцию с уравнениями (1), где $m = n = D + N, Q = \{1, \dots, D + N\}$, и для любого $a \in E_2^{D+N}$ $\psi(i, a) = 0^{i-1} 10^{D+N-i}$,

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

назовем (D, N) -счетчиком и обозначим через $B_{D,N}$. $B_{D,N}$ выдает всегда одну и ту же последовательность с периодом N и предпериодом D . Если же при тех же условиях $\psi(i, (a_1, \dots, a_{D+N})) = a_i$, то назовем ее (D, N) -селектором и обозначим через $C_{D,N}$. Множество всех счетчиков обозначим через \mathbf{K} .

Без ограничения общности, будем исследовать на полноту системы вида $\{f_{\text{ш}}, f\}$, где f задается уравнениями (1).

Для $D, 0 \leq D \leq s$ последовательность (2),

$$(a(1), b(1)), (a(2), b(2)), \dots, (a(s), b(s)), \quad (2)$$

где $a(1), \dots, a(s) \in E_2^n; q(1), \dots, q(s+1) \in Q; b(1), \dots, b(s) \in E_2^m; b(i) = \psi(q(i), a(i)); q(i+1) = \varphi(q(i), a(i)), i = 1, \dots, s;$

$q(1) = q_1, \varphi(q(s), a(s)) = q(D+1)$, назовем (D, s) экспериментом с а.-функцией f .

Пусть i, j натуральные числа, $1 \leq i, j \leq s, j \neq i$. Скажем, что а.-функция f является (j, i) -зависимой, если для каждой последовательности (2) выполнено соотношение (3), а.-функция f допускает счетчик $B_{D,N}$, если для некоторого $s = D + kN$ и любых $i \neq j, 1 \leq i, j \leq s$ а.-функция f не является (j, i) -зависимой.

$$\psi(q(j), a(i)) = b(i). \quad (3)$$

Имеют место следующие леммы.

Лемма 1. *Имеет место включение $[\{f, f_{\text{ш}}\}] \supseteq \mathbf{K}$ точно тогда, когда для любого натурального N найдутся $D, s = D + kN$ такие, что f допускает счетчик $B_{D,N}$.*

Лемма 2. *Отношение включения $[\{f, f_{\text{ш}}\}] \supseteq \mathbf{K}$ алгоритмически проверяемо.*

Через $Q_i \subseteq Q$ обозначим множество состояний а.-функции f достижимых из начального за i тактов. Скажем, что а.-функция f с уравнениями (1) имеет память в j -тый момент, если для некоторого слова $\alpha \in E_2^n$ длины $j-1$ и некоторых букв $a, b, c \in E_2^n$ выполнено $\psi(\varphi(q_1, \alpha a), c) \neq \psi(\varphi(q_1, \alpha b), c)$, в противном случае скажем, что

а.-функция f не имеет памяти в j -тый момент. Обозначим множество всех а.-функций, не имеющих памяти в j -тый момент, через $U(j), j = 0, 1, \dots$

Автоматная функция $G: E_2^\infty \rightarrow E_2^\infty$ с уравнениями

$$q(1) = 0, \quad q(t+1) = a(t), \quad b(t) = q(t)$$

называется автоматной функцией «задержки» или «задержкой». Известно, что $[\{G, f_{\text{ш}}\}] = P_a$. Через λ обозначим пустую букву. Пусть $p, q, r, s \in Q$, определим бинарные отношения $\mathbf{2}, \mathbf{0}, \mathbf{1}$ на множестве $Q \times Q$.

$((p, q), (r, s))$ связаны отношением $\mathbf{2}, \mathbf{0}, \mathbf{1}$, если

$$\exists a, b ((\varphi(p, a) = r) \& (\varphi(q, b) = s) \& (\psi(p, a) \neq \psi(q, a)));$$

$$\exists a ((\varphi(p, a) = r) \& (\varphi(q, a) = s) \& (\psi(p, a) = \psi(q, a)));$$

$$\exists a, b ((\varphi(p, a) = r) \& (\varphi(q, b) = s) \& (\psi(p, a) = \psi(q, a)) \& (\psi(p, b) = \psi(q, b)));$$

соответственно, пусть $\mathbf{ALL} = \mathbf{2} \cup \mathbf{0} \cup \mathbf{1}$ и функция

$\eta: Q^2 \times Q^2 \rightarrow \{\lambda, 0, 1, 2\}$ определена как

$$\eta((p, q), (r, s)) = \begin{cases} \lambda, & \text{если } ((p, q), (r, s)) \notin \mathbf{ALL}, \\ 2, & \text{если } ((p, q), (r, s)) \in \mathbf{2}, \\ 0, & \text{если } ((p, q), (r, s)) \in \mathbf{0} \setminus \mathbf{2}, \\ 1, & \text{если } ((p, q), (r, s)) \in \mathbf{1} \setminus \{\mathbf{0} \cup \mathbf{2}\}. \end{cases}$$

Пусть $\overline{\max}$ обозначает максимум относительно порядка $\lambda \leq 1 \leq 0 \leq 2$, а \max — относительно порядка $0 \leq 1 \leq 2 \leq \lambda$.

Обозначим через I_f полный ориентированный граф с помеченными ребрами и множеством вершин $Q \times Q$, где η — функция отметок ребер и назовем I_f локальным информационным графом а.-функции f . Для $X_1, X_2 \in 2^{Q \times Q}, X_1 \neq \emptyset, X_2 \neq \emptyset$ обозначим через $E(X_1, X_2) \subseteq 2^{Q \times Q \times Q \times Q}$ всякую систему ребер графа I_f со свойством: всякое $x_1 \in X_1$ ($x_2 \in X_2$) соединено ребром из $E(X_1, X_2)$ с $x_2 \in X_2$ ($x_1 \in X_1$), а множество всех таких систем — через $\Upsilon(X_1, X_2)$. Определим функцию

$\Theta: 2^{Q \times Q} \times 2^{Q \times Q} \rightarrow \{\lambda, 0, 1, 2\}$ для $X_1 \neq \emptyset, X_2 \neq \emptyset$ соотношением

$$\Theta(X_1, X_2) = \overline{\max}_{\Upsilon(X_1, X_2)} \left(\max_{E \in \Upsilon(X_1, X_2)} (\eta(E)) \right).$$

Для $X_1 = \emptyset$ или $X_2 = \emptyset$ определим $\Theta(X_1, X_2) = \lambda$. Полный ориентированный граф \widehat{I}_f с помеченными ребрами и множеством вершин $2^{Q \times Q}$, где Θ функция отметок, назовем глобальным информационным графом а.-функции f . Если $q \in Q_i$, то цикл

$$\{(q, q)\} E_1 X_1 E_2 X_2 \dots X_{l-1} E_l \{(q, q)\}$$

в графе \widehat{I}_f (соответственно I_f) назовем i -тым циклом, здесь через E_1, \dots, E_l обозначены ребра. Если отметки ребер i -того цикла таковы, что

$$\Theta(E_1) = 1, \Theta(E_2) = 2, \Theta(E_3) \neq 1, \dots, \Theta(E_l) \neq 1,$$

$$(\eta(E_1) = 1, \eta(E_2) = 2, \eta(E_3) \neq 1, \dots, \eta(E_l) \neq 1),$$

то назовем его i -тым информационным циклом в графе \widehat{I}_f (соответственно I_f).

Имеет место следующая лемма.

Лемма 3. *Для системы $\{f, f_{\mathcal{U}}\}$ такой, что $[\{f, f_{\mathcal{U}}\}] \supseteq \mathbf{K}$ имеет место $[(\{f, f_{\mathcal{U}}\}) \ni G$ точно тогда, когда*

1) $f \notin U(i)$ при всех натуральных i ,

2) найдется натуральное $N \leq 2^{|Q|^2}$ такое, что для всех $i > N$ в графе \widehat{I}_f имеется i -тый информационный цикл.

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 . Обозначим через $Q_{pl}^t = Q_p^t \cap R_l$, тогда $Q_{pl}^{t+1} = \{\varphi(p, a) | a \in E_2^n, p \in Q_{pl}^t\} \cap R_l$. Последовательность $Q_{pl}^t, t = 1, 2, \dots$ будет детерминированной, а значит, и периодической. Можно выбрать период и предпериод этой последовательности равный, для простоты, одному и тому же числу ρ при всех $p, l \in Q$. Очевидна грубая оценка $\rho \leq (2^{|Q|})!$. Итак для любых $p, l \in Q$ $Q_{pl}^t = Q_{pl}^{t+\rho}$, при $t = 1, 2, \dots$.

Доказательство теоремы.

Без ограничения общности случай конечной системы $M = \{f_1, f_2, \dots, f_k\}$ сводится к случаю, когда M состоит из одного элемента $M = \{f\}$. Ввиду периодичности последовательности $Q_{q_1}^t, t = 1, 2, \dots$ проверка условия $f \notin U(i)$ сводится к перебору значений

$i < 2\rho$ и всех путей длины не большей $i + 1$, проходящих по состояниям а.-функции f . Число таких путей не превосходит $(2^n)^{2\rho}$. Общее число операций при переборе не превосходит $2\rho 2^{2n\rho}$, где $\rho < (2^{|Q|})!$. Таким образом, общее число операций не превосходит числа $2(2^{|Q|})!(2^{2n(2^{|Q|})!})$. В лемме 2 доказана алгоритмическая проверяемость включения $\{f, f_{\text{ш}}\}_K \supseteq \mathbf{K}$.

Рассмотрим проверяемость условия 1 леммы 3. Ввиду периодичности последовательности $Q_{q_1}^t, t = 1, 2, \dots$ проверка условия $f \notin U(i)$, как это показано в теореме 1 занимает не более $2(2^{|Q|})!(2^{2n(2^{|Q|})!})$ операций. Оценим размеры графа \widehat{I}_f . Он имеет множество вершин мощности $R = 2^{|Q|^2}$. Для проверки наличия i -того информационного цикла необходимо проверить простые пути из вершин, достижимых из вершины $\{(q_1, q_1)\}$ за $i + 2$ такта. Число таких путей не превосходит $R!$. Вместо проверки счетного числа значений i , достаточно проверить состояния из множеств R_i — достижимых за i тактов вершин графа \widehat{I}_f . Если $\rho\rho$ — период и предпериод последовательности R_1, R_2, \dots , то необходимо проверить вершины из множеств $R_1, R_2, \dots, R_{2\rho\rho}$. Очевидно, что $\rho\rho \leq (2^R)!$. Таким образом, общее число операций при проверке условия 2) леммы 3 не превосходит числа

$$(2^{2^{|Q|^2+1}})!$$

Теорема доказана.

3. Доказательство лемм

Доказательство леммы 1. Необходимость.

Пусть $N \neq \rho$ и через а.-функции $f_{\text{ш}}, f$ выражена а.-функция g , равная $B_{0,N}$. Это значит, что найдутся $k, D, s = D + kN$ такие, что а.-функция g не является (j, i) -зависимой при $i \neq j \pmod{N}$. Зафиксируем для определенности $i, j, i < j \pmod{N}$.

Пусть а.-функция g получилась операцией обратной связи из а.-функции \tilde{g} . Покажем, что \tilde{g} также не является (j, i) -зависимой. В самом деле: пусть эксперимент (2), получившийся из эксперимента (4), нарушал (j, i) зависимость.

$$((a(1), e(1)), (b(1), e(1))), \dots ((a(s), e(s)), (b(s), e(s))). \quad (4)$$

Это означает, что $b = \psi(q(j), a(i)) \neq b(i)$. 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

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

По правилу применимости о.с. имеем $e = e'$ и, если есть сохранение (j, i) -зависимости для \tilde{g} , то $e' = e(i)$, откуда следует $b' = b = b(i)$, а это означает сохранение (j, i) -зависимости для g , что противоречит нашему предположению.

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

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

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 а.-функция $f_{\text{ш}}$ сохраняет (j, i) -зависимости на (D, s) -экспериментах.

Повторяя эти рассуждения, мы получим, что сама а.-функция f не сохраняет (j, i) -зависимость на (D, s) -экспериментах при $i \neq j \pmod{N}$.

Если для (D, s) -экспериментов выполнена (j, i) -зависимость, то будет выполнена (j_1, i) -зависимость, где $j_1 = j \pmod{\rho}$, $j_1 \neq i \pmod{N}$. В самом деле: это следует из того, что для каждого $p \in Q_D$ и для каждого $r \in Q_{p,p}^{i-D}$ имеем $Q_{r,p}^{j-i} = Q_{r,p}^{j_1-i}$. Так как $N \neq \rho$ для $i = j \pmod{N}$ а.-функция f также не будет (j, i) -зависимой. Получилось, что счетчик $B_{D,N}$ допустим системой $\{f_{\text{ш}}, f\}$. Очевидно, что из допустимости $B_{0,2\rho}$ следует допустимость $B_{0,\rho}$. 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 , допускающее счетчик $B_{D,N}$. 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 -тый эксперимент из P ,

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

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

Можно считать, что среди $a(1), a(2), \dots, a(s)$ нет равных (в противном случае можно добавить фиктивные входы и выбрать $a(1), a(2), \dots, a(s)$ попарно не равными). Рассмотрим (D, s) -эксперимент (2) с а.-функцией g_j . Для $a \in E_2^n$ определим булеву вектор-функцию $h_j : E_2^{m+n} \rightarrow E_2^m$,

$$h_j(x, y) = \begin{cases} a(i) & \text{для } x = a(i), y = b(i), i = 1, \dots, s \\ a(j) & \text{для } y = \psi(q(j), x), x \in E_2^n, y \in E_2^m. \end{cases}$$

Это можно сделать ввиду отсутствия (j, i) -зависимостей. В состоянии $q(j)$ выходная функция а.-функции $f_j(x) = h_j(x, g_j(x))$ принимает значение $a(j)$ для всех входных букв, то есть является константой. Рассмотрим а.-функцию $F_{N,D,k}(x) = f_s(\dots f_2(f_1(x)) \dots)$ с начальным состоянием $(q(1), q(1), \dots, q(1))$, она имеет n входов и n выходов. В состоянии $(q(j), q(j), \dots, q(j))$ реализуется константа $a(j)$. После n применений операции обратной связи от соответствующих выходов к соответствующим входам получится а.-функция, с точностью до булевой перекодировки, равная $B_{D,N}$. Достаточность доказана.

Доказательство леммы 2.

Возьмем такой случай расположения чисел $D < D + \rho < i < i + \rho < j < s - \rho < s$. Если для (D, s) -экспериментов выполнена (j, i) -зависимость, то для (D_1, s_1) -экспериментов, будет выполнена (j_1, i_1) -зависимость, где $D_1 < D_1 + \rho < i_1 < D + 2\rho < j_1 < s_1 < j_1 + \rho$, и $D_1, D; i_1, i; j_1, j; s_1, s$ попарно совпадают по модулю ρ . Это следует из того, что для каждого $p \in Q_{q_1,p}^D$ имеем $Q_{q_1,p}^D = Q_{q_1,p}^{D_1}$, $Q_{p,p}^i = Q_{p,p}^{i_1}$; для каждого $r \in Q_{p,p}^{i-D}$ имеем $Q_{r,p}^{j-i} = Q_{r,p}^{j_1-i_1}$; для каждого $l \in Q_{r,p}^{j-i}$ имеем $Q_{l,p}^{s-j} = Q_{l,p}^{s_1-j_1}$.

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

Таким образом, условие выразимости системой $\{f_{\text{ш}}, f\}$ всех константных а.-функций алгоритмически проверяемо. Лемма 2 доказана.

Пусть I_1, I_2 полные графы с множествами вершин P_1, P_2 и функциями отметок ребер

$$\chi_1: P_1 \times P_1 \rightarrow \{\lambda, 0, 1, 2\}, \chi_2: P_2 \times P_2 \rightarrow \{\lambda, 0, 1, 2\},$$

соответственно. Полный граф с множеством вершин $P_1 \times P_2$ и функцией отметок $\chi: (P_1 \times P_2) \times (P_1 \times P_2) \rightarrow \{\lambda, 0, 1, 2\}$, где

$$\chi(((p_1^1, p_1^2), (p_2^1, p_2^2))) = \overline{\max}(\chi_1((p_1^1, p_2^1)), \chi_2((p_1^2, p_2^2)))$$

назовем прямым произведением графов I_1, I_2 и обозначим через $I_1 \times I_2$. Граф $\underbrace{I \times \dots \times I}_l$ будем называть l -той степенью графа I и обозначать через I^l .

Утверждение 1. В графе \widehat{I}_f существует i -тый информационный цикл точно тогда, когда для некоторого натурального $l \leq 2^n |Q|^2 2^{|Q|^2}$ i -тый информационный цикл существует в графе $(I_f)^l$.

Доказательство. Пусть f а.-функция, определенная уравнениями (1), I_f — ее локальный информационный граф, \widehat{I}_f — ее глобальный информационный граф, $q \in Q_i, X_0 = \{(q, q)\}$,

$$X_0 \xrightarrow{x_0} X_1 \xrightarrow{x_1} \dots X_{s-1} \xrightarrow{x_{s-1}} X_0$$

i -тый информационный цикл в \widehat{I}_f . Длина s этого цикла не превосходит числа вершин графа \widehat{I}_f , которое не превосходит $2^{|Q|^2}$. Пусть $\Upsilon_j = \Upsilon(X_j, X_{j+1}), j = 0, 1, \dots, s-1$ система ребер графа I_f , по которым выбрана отметка $x_j = \max_{E \in \Upsilon_j} \chi(E)$ ребра X_j, X_{j+1} графа \widehat{I}_f . Пусть l число разных цепей, идущих по ребрам систем $\Upsilon_j, j = 0, 1, \dots, s-1$ из X_0 в X_0 , тогда для некоторого l в $(I_f)^l$ будет i -тый информационный цикл, составленный из указанных цепей. Заметим, что $l \leq |Q|^2 2^n s = 2^n |Q|^2 2^{|Q|^2}$.

Обратно. Пусть в $(I_f)^l$ имеется i -тый информационный цикл, $q \in Q_i$,

$$(p_1^0, \dots, p_l^0) \xrightarrow{x_0} \dots \rightarrow (p_1^{s-1}, \dots, p_l^{s-1}) \xrightarrow{x_{s-1}} (p_1^0, \dots, p_l^0),$$

$p_j^r \in Q \times Q, r = 1, \dots, s-1, j = 1, \dots, l, (p_1^0, \dots, p_l^0) = ((q, q), \dots, (q, q))$. Пусть $X_i = \{q_j^i | j = 1, 2, \dots, l\}$, тогда цикл $(X_0) \xrightarrow{y_0} (X_1) \xrightarrow{y_1} \dots \xrightarrow{y_{s-1}} (X_0)$ будет глобальным информационным циклом в \widehat{I}_f . В самом деле: $y_0 = x_0 = 1$; $y_1 = x_1 = 2$ не может измениться, так как она уже максимальна. Если $x_j = 0$ и возникла ситуация, когда для одной системы ребер отметка равна 0, а для другой — 1, тогда функция $\overline{\text{max}}$ выберет отметку 0. Отметка 1 возникнуть здесь не может. Утверждение 1 доказано.

Пусть $g(x) = y$ одноместная а.-функция с уравнениями (1), I_g ее локальный информационный граф. Путь

$$(p(1), q(1)) \xrightarrow{x_1} (p(2), q(2)) \xrightarrow{x_2} \dots \xrightarrow{x_{l-1}} (p(l), q(l))$$

в графе I_g , между отметками которого и функциями φ и ψ выполнено соотношение (5), назовем *приведенным* (см. рис. 1). Здесь $\psi_p(a) = \psi(p, a)$.

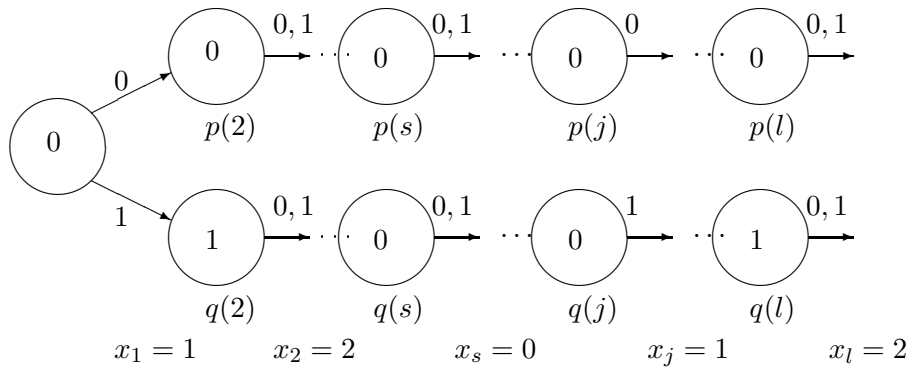


Рис. 1.

$$\begin{cases} \psi_{p(i)} \equiv \psi_{q(i)} \equiv 0, \text{ при } x_i \neq 2; \\ \psi_{p(i)} \equiv 0, \psi_{q(i)} \equiv 1, \text{ при } x_i = 2; \\ \varphi(p(i), 0) = \varphi(p(i), 1) = p(i+1), \text{ при } x_i \neq 1; \\ \varphi(q(i), 0) = \varphi(q(i), 1) = q(i+1), \text{ при } x_i \neq 1; \\ \varphi(p(i), 0) = p(i+1), \varphi(q(i), 1) = q(i+1) \text{ при } x_i = 1. \end{cases} \quad (5)$$

Утверждение 2. Пусть в графе I_f имеется i -тый цикл длины l с отметками x_1, x_2, \dots, x_l , тогда через $\{f, f_{\text{III}}\} \cup \mathbf{K}$ выразима одноместная α -функция g , в графе I_g которой имеется i -тый приведенный цикл с теми же отметками x_1, x_2, \dots, x_l .

Доказательство.

Пусть указанный цикл в графе I_f имеет вид (рис. 2). Состояния p_2, p_3, \dots, p_l образуют верхнюю ветвь, а состояния q_2, q_3, \dots, q_l — нижнюю ветвь цикла, $p_i, q_i \in Q, a_i, b_i \in E_2^n, c_i, d_i \in E_2^m$.

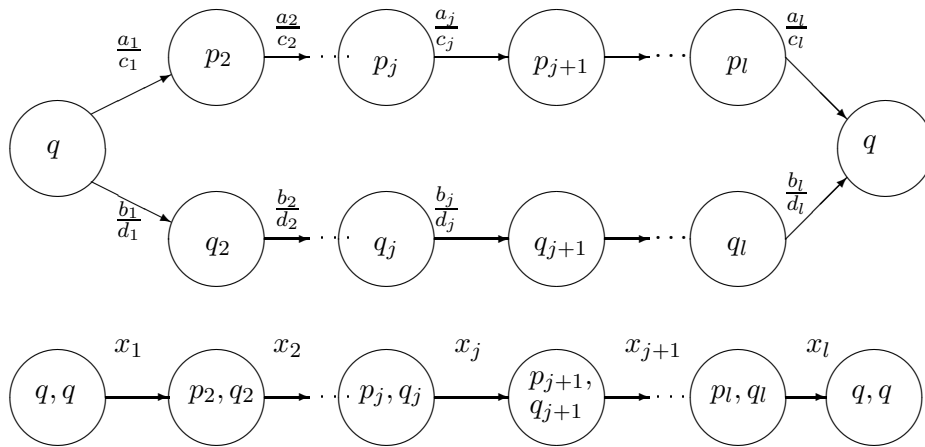


Рис. 2.

Определим функции

$$\gamma_j: E_2 \rightarrow E_2^n, \quad \delta_j: E_2^n \times E_2^m \rightarrow E_2$$

по a_j, b_j, c_j, d_j (см. рис. 1), $j = 1, 2, \dots, l$, следующим образом:

$$\gamma_j(z_1) = \begin{cases} a_j & \text{при } x_j = 0; \\ a_j & \text{при } x_j = 1, z_1 = 0; \\ b_j & \text{при } x_j = 1, z_1 = 1; \\ a_j & \text{при } x_j = 2, a_j = b_j, c_j \neq d_j; \\ a_j & \text{при } x_j = 2, z_1 = 0; \\ b_j & \text{при } x_j = 2, z_1 = 1; \end{cases}$$

$$\delta_j(z_2, y_1) = \begin{cases} 0 & \text{при } x_j = 0, x_j = 1; \\ 0 & \text{при } x_j = 2, a_j = b_j, c_j \neq d_j, z_2 = c_j, y_1 = a_j; \\ 1 & \text{при } x_j = 2, a_j = b_j, c_j \neq d_j, z_2 = d_j, y_1 = b_j; \\ 0 & \text{при } x_j = 2, a_j \neq b_j, e_j \neq c_j, z_2 = c_j, y_1 = a_j; \\ 1 & \text{при } x_j = 2, a_j \neq b_j, e_j \neq c_j, z_2 = e_j, y_1 = a_j; \\ 1 & \text{при } x_j = 2, a_j \neq b_j, e_j \neq c_j, y_1 = b_j. \end{cases}$$

Пусть а.-функции $D_1, D_2 \in [\{\mathbf{K}, f_{\text{ш}}\}]$ и имеют уравнения (6),(7), соответственно,

$$D_1: E_2^* \rightarrow (E_2^n)^*, \quad D_2: (E_2^m \times E_2^n)^* \rightarrow E_2^*.$$

S_1, S_2 множества состояний а.-функций D_1, D_2 , соответственно, и $S_1 = S_2 = \{1, 2, \dots, l\}$. Здесь $z_1 \in E_2, y_1 \in E_2^n, z_2 \in E_2^m, y_2 \in E_2, s_1 \in S_1, s_2 \in S_2$.

$$\begin{cases} s_1(1) = 1, \\ s_1(t+1) = s_1(t) + 1 \pmod{l}, \\ y_1(t) = \gamma_{s_1(t)}(z_1) \end{cases} \quad (6)$$

$$\begin{cases} s_2(1) = 1, \\ s_2(t+1) = s_2(t) + 1 \pmod{l}, \\ y_2(t) = \delta_{s_2(t)}(z_2, y_1) \end{cases} \quad (7)$$

В графе односторонней а.-функции $h = D_2(f(D_1(z_1)), D_1(z_1))$ будет «почти приведенный» цикл с такими же отметками x_1, \dots, x_l с той разницей, что для $x_i = 2$ могут быть два варианта переходов а) и б) (рис. 3).

Далее мы сведем случай б) к случаю а). Пусть а.-функция $H_j(u, v, z), H_j: (E_2^3)^* \rightarrow E_2^*$ имеет множество состояний $S =$

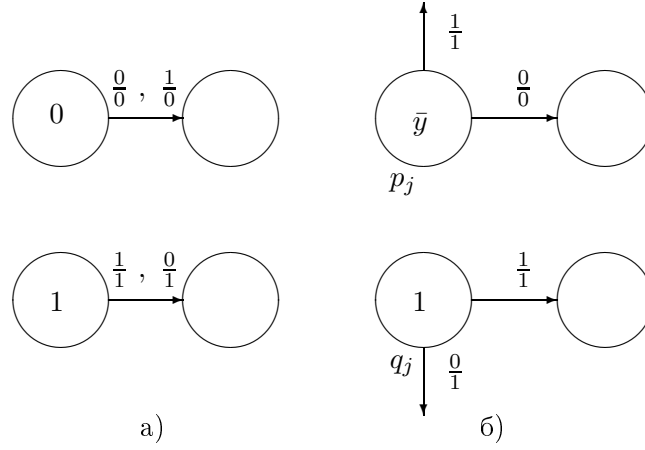


Рис. 3.

$\{1, 2, \dots, l\}$ и уравнения

$$\begin{cases} s(1) = 1, \\ s(t + 1) = s(t) + 1 \pmod{l}, \\ H_j(t) = \begin{cases} u(t) & \text{для } s(t) \neq j, \\ u(t) + v(t) + z(t) & \text{для } s(t) = j. \end{cases} \end{cases}$$

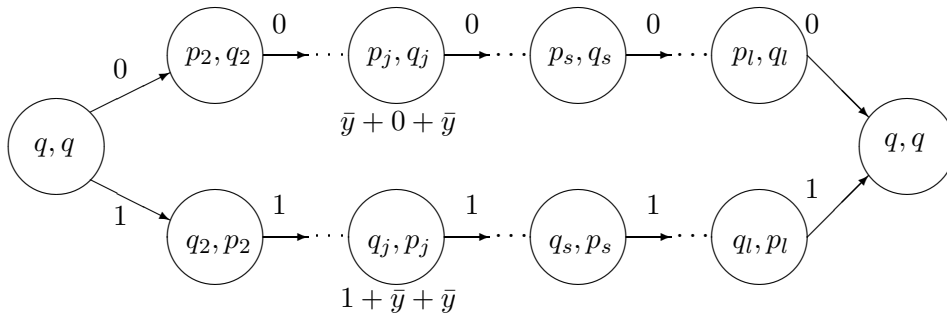


Рис. 4.

Если номер j соответствует случаю б), тогда а.-функция $F_j(y) = H_j(h(y), \overline{h(\bar{y})}, \bar{y})$, имеет фрагмент диаграммы, показанный на рис. 4, и приведенный цикл с теми же отметками x_1, x_2, \dots, x_l . В самом деле: для $s(t) \neq j$ выполнено $F_j \equiv h(y)$, а также условия (5). Если имеет

место этот случай, то выходная функция в состоянии (p_j, q_j) (рис. 4) будет такова: $\bar{y} + 0 + \bar{y} = 0$, а в состоянии (q_j, p_j) будет выходная функция $1 + \bar{y} + \bar{y} = 1$. Таким образом, для $F_j(y)$ будут выполнены все условия (5), кроме: $\varphi(p(j), 1) = p(j + 1)$, $\varphi(q(j), 0) = q(j + 1)$ в случае б). При помощи срабатывающей в j -тый момент обратной связи указанный недостаток исправляется, и фрагмент диаграммы приводится к виду рис. 1 схемой, изображенной на рисунке 5, где а.-функция $w_j(x, y)$

$$w_j : (E_2^2)^* \rightarrow E_2$$

имеет множество состояний S и уравнения

$$\begin{cases} s(1) = 1, \\ s(t + 1) = s(t) + 1 \pmod{l}, \\ w_j(t) = \begin{cases} x(t) & \text{для } s(t) \neq j, \\ y(j) & \text{для } s(t) = j. \end{cases} \end{cases}$$

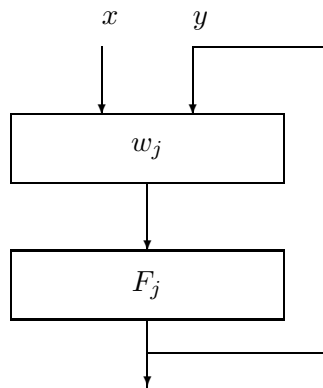


Рис. 5.

Утверждение 2 доказано.

Утверждение 3. Пусть а.-функция f равна «задержке» G , тогда найдется натуральное $N \leq |Q|^2$ такое, что для любого $i > N$, в графе I_f имеется i -тый информационный цикл.

Доказательство. Пусть f одноместная а.-функция с уравнениями (1), и f эквивалентна G . Последовательность $\{q_1\}, Q_1, Q_2, \dots$ имеет

предпериод ρ и период ρ . Пусть $i > \rho$ и $q \in Q_i$ — такое состояние, что для любого слова $\beta \in E_2^*$ найдется слово $\gamma \in E_2^*$ такое, что $\varphi(q, \beta\gamma) = q$ (q — состояние из сильносвязной компоненты). Пусть слова $\alpha, \bar{\alpha} \in E_2^*$ таковы, что $\alpha = a_1 a_2 \dots a_\rho$, $\bar{\alpha} = \bar{a}_1 \bar{a}_2 \dots \bar{a}_\rho$. Рассмотрим путь (рис. 6) в графе I_f . В состоянии p_j из q ведет путь $a_1 a_2 \dots a_{j-1}$, в состоянии q_j — путь $\bar{a}_1 \bar{a}_2 \dots \bar{a}_{j-1}$.

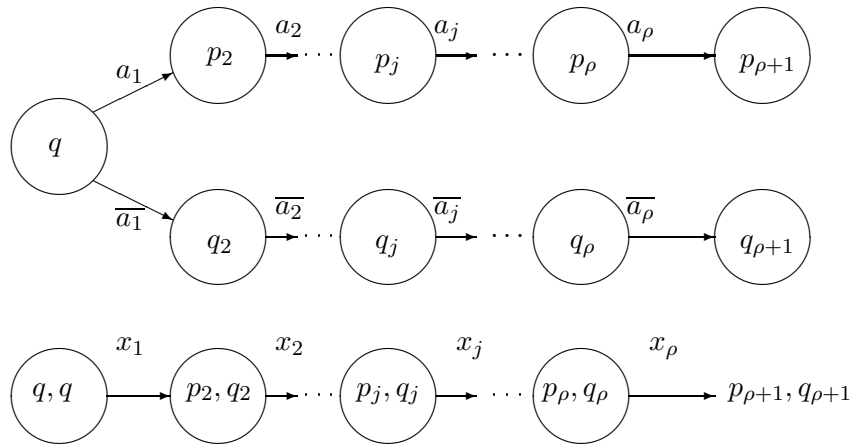


Рис. 6.

Так как в а.-функции $f = G$, в состоянии p_j реализуется константа a_{j-1} , а в состоянии q_j — константа \bar{a}_{j-1} , получаем, что $x_1 = 1$, $x_2 = x_3 = \dots = x_\rho = 2$. Из того, что $Q_i = Q_{i+\rho}$, имеем $p_{\rho+1}, q_{\rho+1} \in Q_i$. Для натурального s рассмотрим множество $H_s = \{\alpha^{s-l}(\bar{\alpha})^l \mid l = 1, 2, \dots, s\} \subset E_2^*$ слов длины $s\rho$, составленных из слов α и $\bar{\alpha}$. Пусть $\gamma, \beta \in H_s$ таковы, что $\gamma = \alpha^l(\bar{\alpha})^{s-l}$, $\beta = \alpha^j(\bar{\alpha})^{s-j}$, где $l < j$, состояния $r_\beta, r_\gamma, p \in Q$, такие что $r_\beta = \varphi(q, \beta)$, $r_\gamma = \varphi(q, \gamma)$, $p = \varphi(q, \alpha^l)$. В графе I_f из пары (q, q) в пару (r_β, r_γ) ведет путь (рис. 7), определяемый парой слов (β, γ) с отметками $y_1 = \dots = y_{l\rho} = 0, y_{l\rho+1} = 1, y_{l\rho+2} = \dots = y_{j\rho+1} = 2, y_{j\rho+2} = \dots = y_{s\rho} = 0$.

Если предположить, что для любого s и любых $\gamma, \beta \in H, \gamma \neq \beta$ выполнено, что $r_\beta \neq r_\gamma$, то получим противоречие с конечностью множества состояний а.-функции f . Следовательно, найдется такое s и такие слова $\gamma, \beta \in H, \gamma \neq \beta$ длины $s\rho$, что выполнено $r_\beta = r_\gamma$. Заметим, что $r_\beta, r_\gamma, p, q \in Q_i$. Пусть δ такое слово, что $\varphi(r_\beta, \delta) = q$, то-

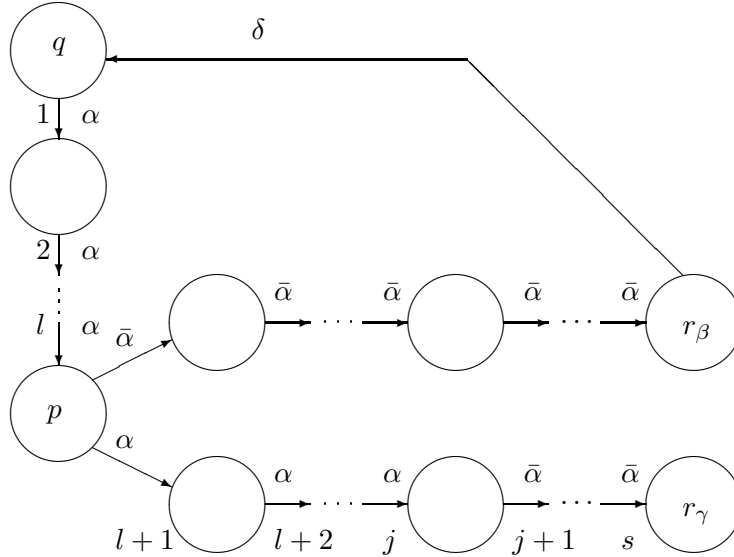


Рис. 7.

гда из пары (p, p) начинается искомый i -тый информационный цикл (рис. 7). Очевидно, что всякое состояние достижимо словом длины не большей $|Q|^2$. Утверждение 3 доказано.

Утверждение 4. Пусть a -функция h получается суперпозицией a -функций h_1, h_2 , при этом в графах I_h, I_{h_1}, I_{h_2} , соответственно, есть ребра с отметками $((p_1, p_2), (q_1, q_2)) \xrightarrow{x} ((r_1, r_2), (s_1, s_2))$,

$$(p_1, q_1) \xrightarrow{y} (r_1, s_1), (p_2, q_2) \xrightarrow{z} (r_2, s_2),$$

тогда отметки x, y, z связаны соотношениями:

$$(x = 2) \rightarrow ((y = 2) \vee (z = 2)),$$

$$(x = 0) \rightarrow ((y = 2) \vee (y = z = 0)).$$

Доказательство. Рассмотрим фрагмент диаграммы a -функции h (рис. 8), где показаны выходы a -функций h_1, h_2 . Пусть $x = 2$ и $c \neq e$, тогда, если $c'' \neq c'$, то $y = 2$, если $c'' = c'$, то $z = 2$. Пусть $x = 0, a =$

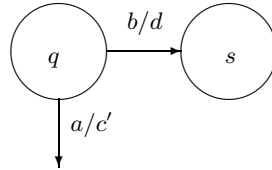
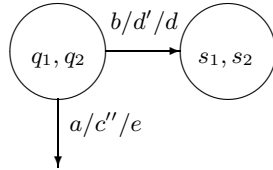
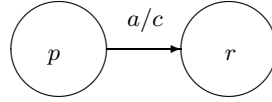
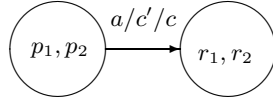


Рис. 8.

Рис. 9.

$b, c = d$, тогда при $c' \neq d'$ имеем $y = 2$, а при $c' = d'$ имеем $y = z = 0$. Утверждение 4 доказано.

Утверждение 5. Пусть a -функция h получена из a -функции g при помощи операции обратной связи, и в графе I_h есть ребро $(p, q) \xrightarrow{x} (r, s)$, тогда в графе I_g есть ребро $(p, q) \xrightarrow{y} (r, s)$, и при этом отметки ребер связаны соотношениями:

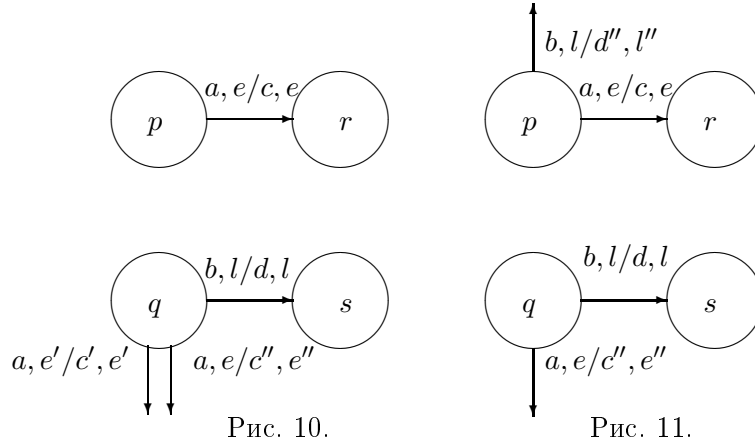
$$(x = 2) \rightarrow (y = 2); (x = 0) \rightarrow (y \neq 1).$$

Доказательство. Пусть a -функция h получена из a -функции g с уравнениями (1) операцией обратной связи, примененной от последнего выхода к последнему входу. На рисунке 9 изображен фрагмент диаграммы a -функции h , на рисунке 10 — соответствующий ему фрагмент диаграммы a -функции g , где $e, l, e', e'' \in E_2, a, b \in E_2^{n-1}, c, d, c', c'' \in E_2^{m-1}$.

Пусть $x = 2, c' \neq c$, и предположим противное $y = 2$, то есть выполнено $(c'', e'') = (c, e)$. Так как последний выход a -функции g не зависит от ее последнего входа, а первая компонента у букв (a, e') и (a, e) одна и та же, значит (см. рис. 10 состояние q) выполнено $e'' = e' = e$. Но тогда $(a, e') = (a, e)$ это один и тот же входной сигнал и $(c', e') = (c'', e'') = (c, e)$. Получилось противоречие с тем, что $c' \neq c$, значит $y = 2$.

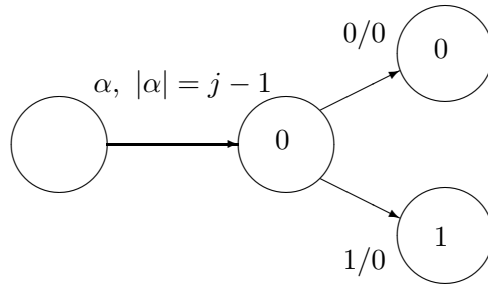
Пусть теперь $x = 0, a = b, c = d$ (см. рис. 11), предположим противное, что $y = 1$, и $(a, e) \neq (b, e)$, тогда выполнено

$$e'' = e, c'' = c, d'' = d, l'' = l.$$



Так как (по определению обратной связи) последний выход не зависит от последнего входа, имеем соотношение: $e'' = l, l'' = e$, значит $e = l$, откуда получаем противоречивое равенство $(a, e) = (b, l)$, значит $y \neq 1$. Утверждение 5 доказано.

Пусть $g(x) = y$ одноместная а.-функция с уравнениями (1), имеющая память в j -тый момент. Фрагмент диаграммы g вида (рис. 12) назовем j -тым приведенным фрагментом.



Здесь в состояниях помеченных **0**, **1** реализуются выходные функции 0, 1, соответственно.

Утверждение 6. Пусть а.-функция h получается суперпозицией а.-функций h_1, h_2 , и для некоторого i выполнено $h \notin U(i)$, тогда $h_1 \notin U(i)$ или $h_2 \notin U(i)$.

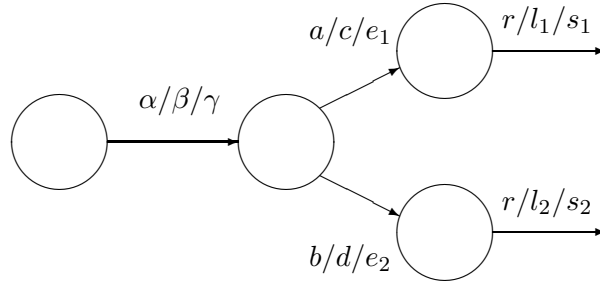


Рис. 13.

Доказательство. Рассмотрим фрагмент а.-функции h (см. рис. 13), на котором нарушается свойство $h \in U(i)$. Здесь $s_1 \neq s_2$. Если $l_1 \neq l_2$, то $h_1 \notin U(i)$; если $l_1 = l_2$, то $h_2 \notin U(i)$. Утверждение 6 доказано.

Утверждение 7. Пусть а.-функция h получена из а.-функции g операцией обратной связи, и для некоторого i выполнено $h \notin U(i)$, тогда $g \notin U(i)$.

Доказательство. Пусть фрагмент а.-функции h (см. рис. 3) получился при операции обратной связи из фрагмента а.-функции g (см. рис. 14).

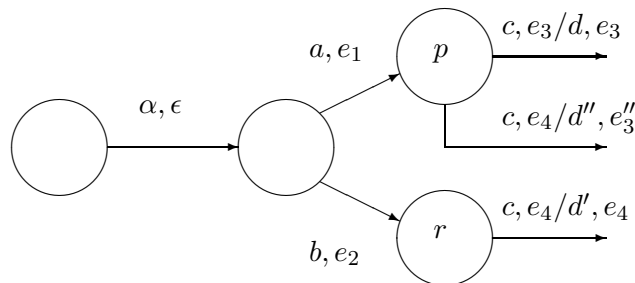


Рис. 14.

Здесь $d \neq d'$. Если $e_3 = e_4$, то $g \notin U(i)$. Предположим, что $e_3 \neq e_4$, тогда по определению обратной связи $e_3 = e_3''$, и значит, по сигналу (c, e_4) в состояниях p и r будут получаться разные выходные буквы (d'', e_3) и (d', e_4) . Значит, $g \notin U(i)$. Утверждение 7 доказано.

Доказательство леммы 3. Достаточность.

Зафиксируем $i > N$. Выберем в графе \widehat{I}_f i -тый информационный цикл длины p . По утверждению 1 в графе $(I_f)^l$ для некоторого l существует i -тый информационный цикл длины p , j -тая проекция которого имеет отметки

$$x_{ij}^1, \dots, x_{ij}^p, \quad j = 1, 2, \dots, l$$

$$\max_j x_{ij}^1 = 1, \quad \max_j x_{ij}^2 = 2, \quad \max_j x_{ij}^s \neq 1, \quad s = 3, 4, \dots, p.$$

По утверждению 2 найдется одноместная а.-функция

$$g_{ij} \in [\mathbf{K} \cup \{f, f_{\text{ш}}\}],$$

в информационном графе которой существует приведенный цикл с теми же отметками $x_{ij}^1, \dots, x_{ij}^p$, $j = 1, 2, \dots, l$ (см. рис. 1). Пусть $\{j | x_{ij}^s = 1\} = \epsilon_i(s)$, $1 \leq s \leq p$. Из определения информационного цикла следует, что при $s > 2$, $\epsilon_i(s) \neq \emptyset$, или при $s = 2$ существует натуральное $\xi_i(s)$ такое, что $x_{i, \xi_i(s)}^s = 2$. Рассмотрим схему (рис. 15), где H_1 и H_2 — булевы вектор-функции

$$H_1(z_1, z_2, s) = (x_1, x_2, \dots, x_l); \quad H_2(y_1, y_2, \dots, y_l, s) = (u, v);$$

$$u = \begin{cases} y_{\xi_i(2)}, & \text{при } s = 2; \\ y_{\xi_i(s)}, & \text{при } \epsilon_i(s) \neq \emptyset; \\ 0, & \text{при } \epsilon_i(s) = \emptyset; \end{cases}$$

$$v = \begin{cases} y_{\xi_i(2)} & \text{при } s = 2; \\ 0 & \text{при } s \neq 2; \end{cases}$$

$$x_j = \begin{cases} z_1 & \text{при } j = \xi_i(2), s = 2; \\ z_1 & \text{при } j \in \epsilon_i(s), s > 2, \epsilon_i(s) \neq \emptyset; \\ z_2 & \text{при } j \in \epsilon_i(s), s = 1; \\ 0 & \text{в остальных случаях.} \end{cases}$$

А.-функции $B_{0,p}, g_{ij}, j = 1, 2, \dots, l$, — муровские, следовательно применима операция обратной связи. Каждая из а.-функций g_{ij} имеет диаграмму (рис. 16) с той лишь разницей, что для отметки $x_{ij}^s = 1$ переход не является безусловным. Схема (рис. 15) реализует а.-функцию $f_{p,i}$ с диаграммой (рис. 16). Без ограничения общности можно выбрать длину цикла p не зависящую от i . В самом деле:

к каждой ветви i -того цикла можно добавить верхнюю ветвь, взятую произвольное число раз, тем самым, выбрать p кратным длинам всех i -тых информационных циклов, где $\rho \leq i \leq 2\rho$. Для каждого $i < N$ по условию леммы 3 $f \notin U(i)$, значит по утверждению 2 найдется а.-функция $g_i \in [\{f, f_{\text{ш}}, \mathbf{K}]$, имеющая i -тый приведенный фрагмент.

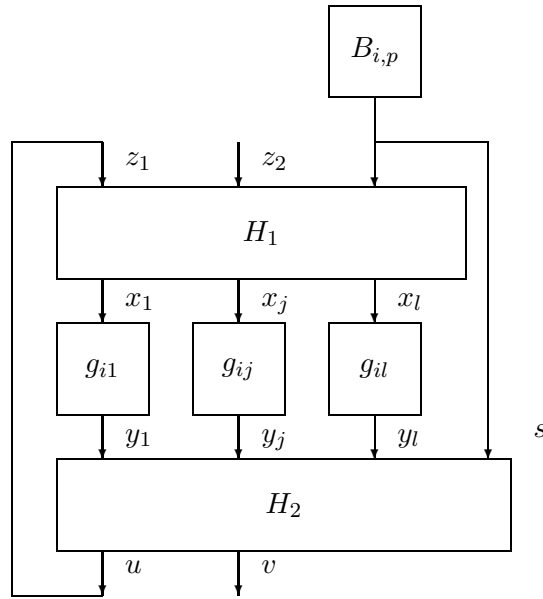


Рис. 15.

Тогда схема (рис. 17) равна «задержке» G . Здесь а.-функция $D: (E_2^{N+p})^* \rightarrow E_2^*$, имеет диаграмму, изображенную на рисунке 18.

Достаточность доказана.

Необходимость.

Пусть $[\{f, f_{\text{ш}}\}] \supseteq \mathbf{K}$ и $[\{f, f_{\text{ш}}\}] \ni G$. Покажем, что $f \notin U(i)$ для любого натурального i . В самом деле: $G \notin U(i)$, и если G получена некоторой схемой h , последняя операция которой суперпозиция двух функций h_1, h_2 , то по утверждению 7 $h_1 \notin U(i)$ или $h_2 \notin U(i)$. Если последняя операция указанной схемы — операция обратной связи, то а.-функция g , из которой получена G , по утверждению 7 обладает тем же свойством: $g \notin U(i)$. Применяя эти рассуждения к одной из подхо-

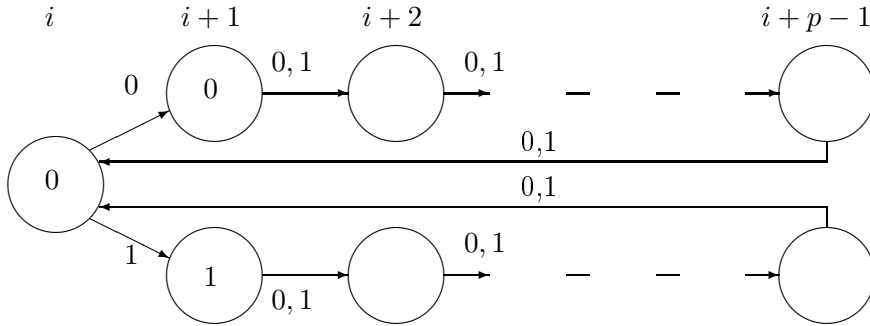


Рис. 16.

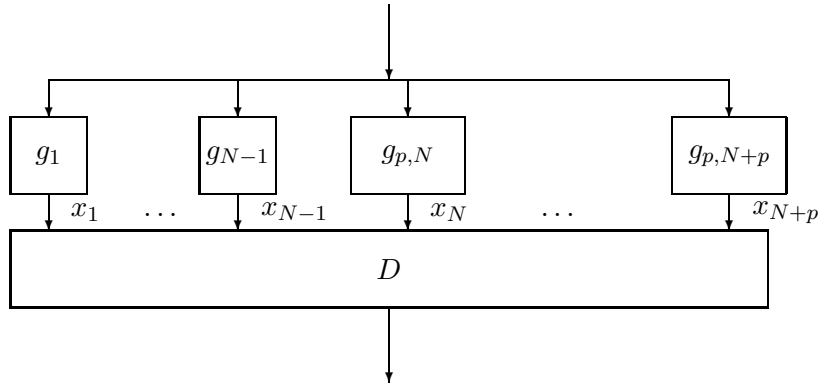


Рис. 17.

дящих а.-функций g, h_1, h_2 , мы через конечное число шагов (равное числу операций в указанной схеме) придем к тому, что $f \notin U(i)$, потому что $f_{III} \in U(i)$, при всех i .

По утверждению 3 найдется такое N , что в схеме h , где $h = g$, для любого $i > N$ в графе I_h имеется i -тый информационный цикл. Если h получилась операцией суперпозиции из а.-функций h_1, h_2 , то, согласно утверждению 4, в графе $I_{h_1} \times I_{h_2}$ имеется i -тый информационный цикл. Если h получилась из g операцией обратной связи, то согласно утверждению 5, в I_g имеется i -тый информационный цикл. Поскольку в графе $I_{f_{III}}$ нет i -тых информационных циклов при всех i , получаем, что i -тый информационный цикл найдется в графе $(I_f)^l$ для некоторого l . По утверждению 1 следует, что в графе \widehat{I}_f так-

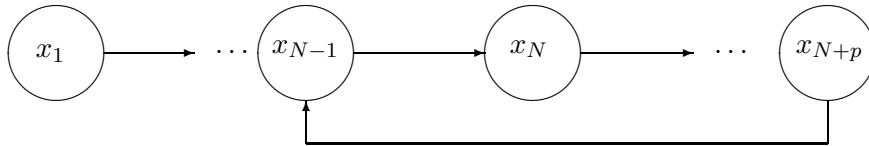


Рис. 18.

же имеется i -тый информационный цикл. Необходимость доказана. Лемма 3 доказана.

Список литературы

- [1] Кудрявцев В.Б. О мощностях множеств предполных классов некоторых функциональных систем, связанных с автоматами // ДАН СССР. 1963. Т. 151. № 3. С. 493–496.
- [2] Кратко М.И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // ДАН СССР. 1964. Т. 155. № 1. С. 35–37.
- [3] Летичевский А.А. Условия полноты для конечных автоматов // Вычислительная математика и математическая физика. № 4. 1961. С. 702–710.
- [4] Бабин Д.Н. Разрешимый случай задачи о полноте автоматных функций // Дискретная математика. Т. 4. 1992. Вып. 4. С. 41–56.
- [5] Бабин Д.Н. О разрешимости проблемы полноты для специальных систем автоматных функций // Дискретная математика. Т. 8. 1996. Вып. 4. С. 79–91.
- [6] Бабин Д.Н. Алгоритмическая разрешимость свойств полноты и A -полноты конечных систем автоматных функций с линейной истинностной частью // Интеллектуальные системы. Т. 3. 1998. С. 51–69.
- [7] Бабин Д.Н. Конечность множества автоматных базисов Поста с разрешимой проблемой полноты // Дискретная математика. Т. 10. 1998. Вып. 3. С. 57–64.