Решение автоматных уравнений с двумя неизвестными

И. В. Лялин

Пусть имеется автоматная схема S, полученная из автоматов с помощью операции суперпозиции. Пусть в S несколько автоматов $x_1, x_2, \ldots, x_n$ разрешается заменять на любые подходящие по входам и выходам автоматы $x'_1, x'_2, \ldots, x'_n$. Рассматривается следующая задача: существует ли такая замена, чтобы полученная схема S' реализовывала автомат, эквивалентный наперед заданному автомату h. В статье доказывается алгоритмическая неразрешимость этой задачи, если $n \geqslant 2$. В работе [1] доказана алгоритмическая разрешимость этой задачи для случая $n = 1$.

Введение

Частный случай решаемой задачи был рассмотрен А. К. Григоряном в [2] и [3]. В этих работах решаются автоматные уравнения с одной неизвестной для 4 видов схем. Позже А. С. Подколзин и Ш. М. Ушчумлич в [4] ввели понятие автоматного уравнения, отличное от понятия автоматного уравнения, рассматриваемого в данной работе. В уравнениях из [4] ограничения накладываются на внутреннее устройство автомата, а не на его поведение, как в данной работе. В работе [5] рассмотрено уравнение с одной неизвестной произвольного вида, но без обратных связей. Приводится алгоритм, определяющий имеет ли такое уравнение решение, а также находящий это решение «в общем виде». Последний результат в [1] был обобщен для произвольного автоматного уравнения, в том числе и с обратными связями. В данной статье рассматриваются автоматные уравнения с более чем одной переменной и доказывается их алгоритмическая неразрешимость, то есть показывается несуществование алгоритма, который по произвольному автоматному уравнению с более чем одной переменной определяет имеет ли оно решение, или нет.

Автор выражает благодарность академику В. Б. Кудрявцеву и профессору Э. Э. Гасанову за ценные замечания и предложения при написании статьи.

1. Основные понятия и результаты

Абстрактным конечным инициальным автоматом, в соответствии с [6], называется шестерка $V = (A, Q, B, \phi, \psi, q^0)$, где A, Q, B — конечные множества, ϕ — функция, определенная на множестве $Q \times A$ и принимающая значения из Q, ψ — функция, определенная на множестве $Q \times A$ и принимающая значения из B, $q^0 \in Q$. Множества A, Q, B называются соответственно *входным алфавитом, алфавитом состояний* и *выходным алфавитом* автомата V. Функция ϕ называется *функцией переходов*, а функция ψ — *функцией выходов* автомата V. $q^0 \in Q$ называется *начальным состоянием.* Через A^* обозначим множество всех конечных слов в алфавите A. Абстрактный конечный инициальный автомат определяет автоматную функцию $f : A^* \to B^*$, которая задается рекуррентно соотношениями

$$\begin{cases} q(1) = q^0, \\ q(t+1) = \phi(q(t), a(t)), \\ f(t) = \psi(q(t), a(t)) \end{cases}$$

Множество автоматов с входным алфавитом A и выходным B обозначим $P(A, B)$.

Пусть $z_1 = (A_1, Q_1, B_1, \phi_1, \psi_1, q_1^0)$ и $z_2 = (A_2, Q_2, B_2, \phi_2, \psi_2, q_2^0)$. Будем говорить, что автомат z есть декартово произведение автоматов z_1 и z_2, или что автомат z раскладывается в декартово произведение автоматов z_1 и z_2, если $z = (A_1 \times A_2, Q_1 \times Q_2, B_1 \times B_2, \phi, \psi, (q_1^0, q_2^0))$. Здесь $\phi((q_1(t), q_2(t)), (a_1(t), a_2(t))) = (\phi_1(q_1(t), a_1(t)), \phi_2(q_2(t), a_2(t))) \in Q_1 \times Q_2$, а $\psi((q_1(t), q_2(t)), (a_1(t), a_2(t))) = (\psi_1(q_1(t), a_1(t)), \psi_2(q_2(t), a_2(t))) \in B_1 \times B_2$. Будем записывать это так: $z = z_1 \times z_2$.

Обозначим $G^{B_1,B_2,\dots,B_n}_{A_1,A_2,\dots,A_n}$ множество всех таких $z \in P(A_1 \times A_2 \times \ldots \times A_n, B_1 \times B_2 \times \ldots \times B_n)$, для которых найдутся такие автоматы $z_i \in P(A_i, B_i)$, $1 \leqslant i \leqslant n$, что $z = z_1 \times z_2 \times \ldots \times z_n$.

Пусть $V = (A, Q, B, \phi, \psi, q^0)$ и $z = (B, Q_z, C, \phi_z, \psi_z, q_z^0)$. Скажем, что автомат $\pi_B(V, z) = (A, Q \times Q_z, C, \phi_\pi, \psi_\pi, (q^0, q_z^0))$ получен из автоматов V и z с помощью *операции суперпозиции*, если $\phi_\pi((q, q_z), a) = (\phi(q, a), \phi_z(q_z, \psi(q, a)))$ и $\psi_\pi((q, q_z), a) = \psi_z(q_z, \psi(q, a))$. Понятно, что $\pi_B(V, z) \in P(A, C)$.

Если $V = (A \times A', Q, B \times B', \phi, \psi, q^0)$, то будем говорить, что V имеет два входа с алфавитами A и A' и два выхода с алфавитами B и B'. Договоримся входы автомата V обозначать x_1, x_2, а выходы y_1, y_2. Функции выхода на выходах y_1, y_2 обозначим соответственно ψ_1 и ψ_2.

Пусть дан автомат $V = (A \times B', Q, B \times B', \phi, \psi, q^0)$. Определим операцию обратной связи. Считаем, что обратная связь (о.с.) корректна в состоянии $q \in Q$, если ψ_2 фиктивно зависит от x_2 при $q(t) = q$, то есть для всех $a \in A$, $b_1, b_2 \in B'$ выполняется $\psi_2(q, (a, b_1)) = \psi_2(q, (a, b_2))$. Обозначим $\psi_2(q, a) = \psi_2(q, (a, b_1))$. Скажем, что автомат $o_{B'}(V) \in P(A, B)$ получен из автомата V с помощью *операции обратной связи (о.с.)*, если его функция выхода $\psi_o(t)$ вычисляется по схеме

$$\begin{cases} q(1) = q^0, \\ q(t+1) = \phi(q(t), (a(t), \psi_2(q(t), a(t)))), \\ \psi_o(t) = \psi_1(q(t), (a(t), \psi_2(q(t), a(t)))) \end{cases}$$

Считаем, что о.с. корректна, если она корректна в начальном состоянии q^0, и из её корректности в состоянии $q(t)$ следует корректность в состоянии $q(t+1)$.

Пусть $S = (A \times B', Q, B \times A', \phi, \psi, q^0)$ и $x = (A', Q_x, B', \phi_x, \psi_x, q_x^0)$. Рассмотрим оператор $R_S(x)$, определенный на автоматах $x \in P(A', B')$ и задаваемый соответственно $R_S(x) = o_{B'}(\pi_{A'}(S, x))$. $P_S(A', B')$ обозначим множество всех $x \in P(A', B')$, для которых инициальная обратная связь в R_S корректна. Понятно, что оператор R_S отображает множество $P_S(A', B')$ во множество $P(A, B)$.

Автоматным уравнением с одной неизвестной называется пара автоматов $S \in P(A \times B', B \times A')$ и $h \in P(A, B)$. Записывается автоматное уравнение так: $S(x) = h$. *Решением* автоматного уравнения $S(x) = h$ является каждый такой автомат $z \in P_S(A', B')$, что $R_S(z) = h$.

В работе [5] доказана алгоритмическая разрешимость задачи нахождения решения автоматного уравнения с одной неизвестной. В данной статье рассматривается решение автоматных уравнений для случая $A' = A'_1 \times A'_2 \times \ldots \times A'_n$ и $B' = B'_1 \times B'_2 \times \ldots \times B'_n$, а множество решений ищется среди автоматов $G^{B'_1, B'_2, \ldots, B'_n}_{A'_1, A'_2, \ldots, A'_n} \cap P_S(A', B')$. Доказывается алгоритмическая неразрешимость задачи нахождения решения такого уравнения.

Автоматным уравнением с n неизвестными называется такое автоматное уравнение с одной неизвестной $S(x) = h$, в котором $S \in P(A \times B'_1 \times B'_2 \times \ldots \times B'_n, B \times A'_1 \times A'_2 \times \ldots \times A'_n)$. *Решением* автоматного уравнения с n неизвестными является каждое решение уравнения с одной неизвестной, принадлежащее множеству $G^{B'_1, B'_2, \ldots, B'_n}_{A'_1, A'_2, \ldots, A'_n}$. Записывать автоматное уравнение с n неизвестными будем так: $S(x_1, x_2, \ldots, x_n) = h$, подразумевая, что x_i принимает значения автоматов из $P(A'_i, B'_i)$, и при этом $x = x_1 \times x_2 \times \ldots \times x_n$.

Содержательно автоматное уравнение представляет из себя произвольную схему S, в которой некоторые автоматы $x_1, x_2, \ldots, x_n$ являются «неизвестными». Вместо неизвестных нужно подставить такие автоматы $z_1, z_2, \ldots, z_n$, чтобы все обратные связи (если они есть в схеме) были корректны, и чтобы полученная схема $S(z_1, z_2, \ldots, z_n)$ была эквивалентна автомату h. Если такой набор автоматов $(z_1, z_2, \ldots, z_n)$ существует, то он называется решением уравнения $S(x_1, x_2, \ldots, x_n) = h$. Решить автоматное уравнение означает найти множество всех его решений.

В данной работе рассматривается задача нахождения решения автоматного уравнения с двумя неизвестными и доказывается её алгоритмическая неразрешимость. То есть несуществование алгоритма, который для любого автоматного уравнения с двумя неизвестными устанавливал бы, имеет оно решение или нет. Отсюда также следует неразрешимость задачи для любого количества переменных, больших чем две.

Теорема 1. *Проблема существования решения автоматных уравнений с двумя переменными алгоритмически неразрешима.*

2. Доказательство алгоритмической неразрешимости

Будем обозначать через h_0 константный автомат с одним выходом, всегда на выходе выдающий 0.

Утверждение 1. *Для любого уравнения* $S(x_1, x_2, \ldots, x_n) = h$ *существует такое уравнение* $S'(x_1, x_2, \ldots, x_n) = h_0$, *что множества их решений совпадают.*

Доказательство.

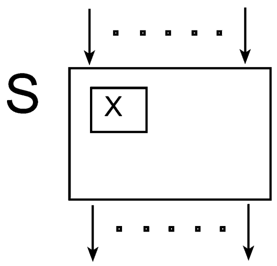

Рис. 1. $S(x_1, x_2, \ldots, x_n)$.

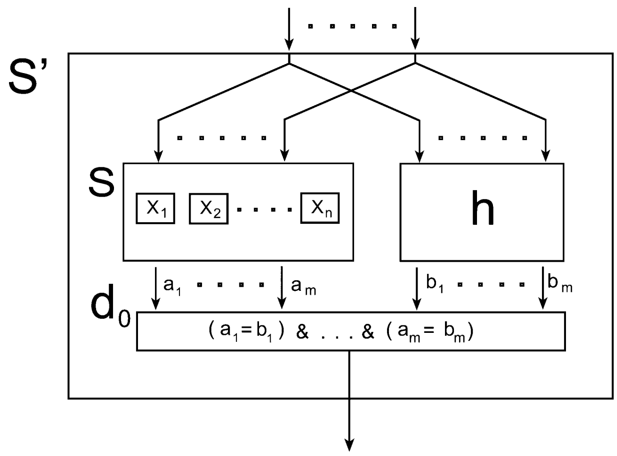

Рис. 2. $S'(x_1, x_2, \ldots, x_n)$.

Пусть схема S имеет m выходов $a_1, a_2, \ldots, a_m$ (см. рис. 1). Тогда h тоже имеет m выходов $b_1, b_2, \ldots, b_m$, так как количество входов и выходов у S и h совпадают. Пусть $d_0(a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_m)$ — такой автомат, что для произвольного момента времени $t \geqslant 1$ если $a_i(t) = b_i(t)$ для всех $i : 1 \leqslant i \leqslant m$, то d_0 в момент времени t выдаёт на выходе 0, иначе выдаёт на выходе 1.

Рассмотрим схему S', которая получается из схем S, автоматов h и d_0 так, как показано на рис. 2. Соответствующие входы автомата h и схемы S отождествляются и являются входами схемы S'. Выходы

$a_1, a_2, \ldots, a_m$ схемы S подключаются к одноименным входам автомата d_0. Выходы $b_1, b_2, \ldots, b_m$ автомата h подключаются к одноименным входам автомата d_0. Выход автомата d_0 есть выход схемы S'.

Нетрудно видеть, что уравнение $S(x_1, x_2, \ldots, x_n) = h$ имеет то же множество решений, что и $S'(x_1, x_2, \ldots, x_n) = h_0$. Действительно: пусть вместо переменных $x_1, x_2, \ldots, x_n$ стоят автоматы $c_1, \ldots, c_n$. Тогда если автомат $S(c_1, \ldots, c_n)$ эквивалентен автомату h, то для любых входов они всегда дают одинаковый выход. То есть для всех $t \geqslant 1$ и $i : 1 \leqslant i \leqslant m$ будет $a_i(t) = b_i(t)$. Значит для любого момента времени $t \geqslant 1$ d_0 выдаёт на выходе 0. Значит, $S'(c_1, \ldots, c_n) = h_0$. Обратно, если $S'(c_1, \ldots, c_n) = h_0$, то для любого момента времени $t \geqslant 1$ d_0 выдаёт на выходе 0, для любого входа схемы S'. По определению автомата d_0, это возможно только если для всех $t \geqslant 1$ и $i : 1 \leqslant i \leqslant m$ будет $a_i(t) = b_i(t)$. А это, в свою очередь, означает эквивалентность автоматов $S(c_1, \ldots, c_n)$ и h, то есть $S(c_1, \ldots, c_n) = h$. Утверждение доказано.

Утверждение 1 позволяет в дальнейшем рассматривать только уравнения вида $S(x_1, x_2, \ldots, x_n) = h_0$, тем самым упрощая изложение.

Системой автоматных уравнений с n неизвестными называется множество из m автоматных уравнений:

$$\left\{\begin{array}{lcl} S_1(x_1, x_2, \ldots, x_n) & = & h_0 \\ S_2(x_1, x_2, \ldots, x_n) & = & h_0 \\ \ldots & & \\ S_m(x_1, x_2, \ldots, x_n) & = & h_0 \end{array}\right.$$

Решением системы автоматных уравнений называется такой набор автоматов $c_1, c_2, \ldots, c_n$, который является решением каждого уравнения.

Утверждение 2. *Для любой системы из двух автоматных уравнений с двумя неизвестными*

$$\left\{\begin{array}{l} S_1(x, y) = h_0 \\ S_2(x, y) = h_0 \end{array}\right.$$

существует уравнение $S(x, y) = h_0$ с тем же множеством решений.

Доказательство.

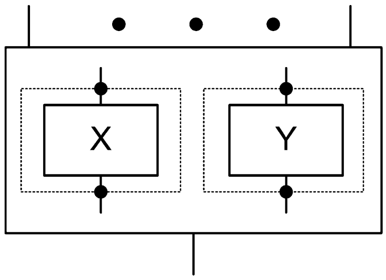

Рис. 3. $S_1(x, y), S_2(x, y)$.

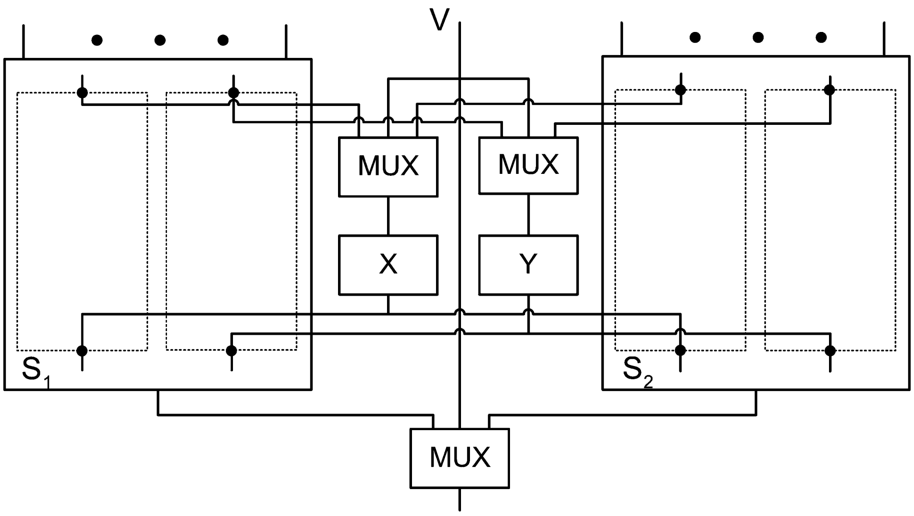

Рис. 4. $S(x, y)$.

Для упрощения понимания изложим доказательство для случая, когда неизвестные x и y имеют по одному двоичному входу и выходу. Случай с большим количеством входов и выходов доказывается аналогично.

Определим автомат MUX, который понадобится нам не только в этой схеме. У него 3 двоичных входа: a, b, c и один выход d. Если в первый момент времени на входе c будет 0, то для любого момента времени $t \geqslant 1$ будет $d(t) = a(t)$. Если же в первый момент времени на входе c будет 1, то для любого момента времени $t \geqslant 1$ будет $d(t) = b(t)$. Таким образом, автомат MUX работает как переключатель, выдавая на выходе одну из входных последовательностей $a(t)$ или $b(t)$ в зависимости от того, что в первый момент времени пришло на вход c.

На рис. 3 показаны (схематично) схемы $S_1(x, y)$ и $S_2(x, y)$. У них несколько входов(сверху) и один выход. Внутри их располагаются «неизвестные» автоматы x и y, имеющие каждый по две точки подключения к схеме: вход(сверху) и выход(снизу).

Теперь будем строить схему $S(x, y)$, как показано на рис. 4. $S(x, y)$ состоит из схем S_1, S_2 и 3 автоматов MUX: MUX_x, MUX_y, MUX_z. Входами S являются все входы схем S_1 и S_2, а также дополнительный вход c. Точку входа x в S_1 соединяем со входом a автомата MUX_x. Точку входа y в S_1 соединяем со входом a автомата MUX_y. Точку входа x в S_2 соединяем со входом b автомата MUX_x. Точку входа y в S_2 соединяем со входом b автомата MUX_y. Выход автомата MUX_x соединим со входом «неизвестной» x. Выход автомата MUX_y соединим со входом «неизвестной» y. Выход «неизвестной» x соединим с точками выхода этой неизвестной в обоих схемах S_1 и S_2. Выход «неизвестной» y соединим с точками выхода этой неизвестной в обоих схемах S_1 и S_2. Выход схемы S_1 соединим со входом a автомата MUX_z. Выход схемы S_2 соединим со входом b автомата MUX_z. Выход автомата MUX_z является выходом схемы S. Вход c схемы S соединим со входами c автоматов MUX_x, MUX_y и MUX_z.

Пусть на место «неизвестной» x подставлен автомат c_1, а на место «неизвестной» y подставлен автомат c_2. Как несложно увидеть, схема S работает следующим образом: если в начальный момент времени на вход c придет 0, то все автоматы MUX переключатся на схему S_1, и вся схема $S(c_1, c_2)$ будет эквивалентна схеме $S_1(c_1, c_2)$. Если же в начальный момент времени на вход c придет 1, то все автоматы MUX переключатся на схему S_2, и вся схема $S(c_1, c_2)$ будет эквивалентна схеме $S_2(c_1, c_2)$. Следовательно, $S(x, y) = h_0$ тогда и только тогда, когда $S_1(x, y) = h_0$ и $S_2(x, y) = h_0$. Утверждение доказано.

Сводить задачу решения автоматного уравнения будем к задаче распознавания сочетаемости, алгоритмическая неразрешимость которой доказана Постом. Напомним в чем она заключается.

Задача распознавания сочетаемости. Пусть $E_m = \{0, 1, \ldots, m-1\}$ — конечный алфавит. Пусть $A_0, \ldots, A_{p-1}$ и $B_0, \ldots, B_{p-1}$ — слова в этом алфавите. Данный набор слов назовём системой Поста. Обозначим данную систему Поста T. Система Поста называется сочетаемой, если существуют такие $i_1, \ldots, i_r \in E_p$, что слово $A_{i_1}A_{i_2}\ldots A_{i_{r-1}}A_{i_r}$ совпадает со словом $B_{i_1}B_{i_2}\ldots B_{i_{r-1}}B_{i_r}$. Данные $i_1, \ldots, i_r$ есть решение системы Поста. Количество индексов в решении не должно быть нулевым. Пост доказал, что для любого $m > 1$ задача сочетаемости алгоритмически неразрешима.

Обозначим $(E_{p+2})^\infty$ множество всех сверхслов над алфавитом $E_{p+2} = \{0, \ldots, p, p+1\}$. Обозначим $(\overline{p+1})^\infty$ сверхслово, составленное только из символа $\overline{p+1}$, а $(0)^\infty$ сверхслово, составленное только из символа 0.

Автомат, имеющий один вход с алфавитом E_{p+2} и один выход с алфавитом E_{p+2}, назовем *повторителем*, если он любое входное сверхслово вида

$$\underbrace{p\,p\ldots p\; i_1\; p\,p\ldots p\; i_2\; p\,p\ldots p\ldots\; i_r\; p\,p\ldots p}_{R}\;\overline{p+1}\;\tilde{\alpha}, \qquad (1)$$

где $0 \leqslant i_k \leqslant p-1$ и $\tilde{\alpha}$ — произвольное сверхслово из $(E_{p+2})^\infty$, преобразует в выходное сверхслово

$$\underbrace{p\;p\;\ldots\;p}_{R}\;i_1\;i_2\;\ldots\;i_r\;(\overline{p+1})^\infty \qquad (2)$$

или в выходное сверхслово вида

$$\underbrace{p\;p\;\ldots\;p}_{T<R}\;(\overline{p+1})^\infty \qquad (3)$$

Ситуацию, когда повторитель выдаёт сверхслово последнего вида, будем называть *отказ в момент времени* $T+1$, или просто *отказ.*

t-повторителем будем называть такой повторитель, который для любого слова вида (1) не выдает отказ, если $v \leqslant t$, и выдает отказ, если $v > t$.

Обозначим $M(x, y)$ схему, изображенную на рис. 5. У неё два входа v_1 и v_2 с алфавитами $\{0, 1, \ldots, p+1\}$ и один выход v_6 с алфавитом $\{0, 1\}$. Выходы v_7, v_8 и v_9 «неизвестной» x ни к чему не подключены.

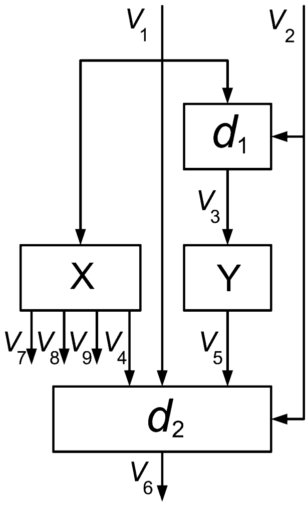

Рис. 5. $M(x, y)$.

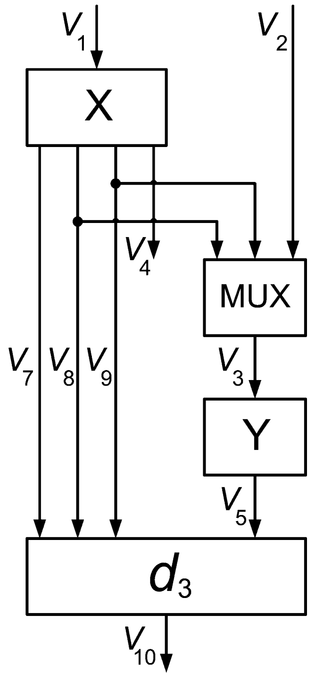

Рис. 6. $P_T(x, y)$.

Автомат d_1 работает следующим образом: любое сверхслово вида

$$\underbrace{p\,p\ldots p}_{u_0} i_1 \underbrace{p\,p\ldots p}_{u_1}\ i_2 \underbrace{p\,p\ldots p}_{u_2}\ \ldots\ i_r \underbrace{p\,p\ldots p}_{u_r}\ \overline{p+1}\ \ldots,$$

поданное на вход v_1, отображает в выходное сверхслово

$$\underbrace{p\,p\ldots p}_{u_0} j_1 \underbrace{p\,p\ldots p}_{u_1}\ j_2 \underbrace{p\,p\ldots p}_{u_2}\ \ldots\ j_r \underbrace{p\,p\ldots p}_{u_r}\ \overline{p+1}\ \ldots, \tag{4}$$

где $j_1 j_2 \ldots j_r = i_1 i_2 \ldots i_r$, если $v_2(1) \geqslant p$, и $j_1 j_2 \ldots j_r = v_2(1) i_1 i_2 \ldots i_{r-1}$ если $v_2(1) < p$. $v_2(1)$ будем называть подсадным символом.

Автомат d_2 работает следующим образом. Пусть на вход v_1 поступило произвольное сверхслово вида (1).
1) Если при этом на входах v_4 и v_5 одно и то же сверхслово вида (3), то d_2 на выходе выдает сверхслово $(0)^\infty$.
2) Если одновременно выполняются следующие условия:

а) на входе v_4 сверхслово

$$\underbrace{p\,p\dots p}_{R}\ i'_1\ i'_2\ \dots\ i'_s\ \overline{p+1}\ \overline{p+1}\ \dots \tag{5}$$

б) на входе v_5 сверхслово

$$\underbrace{p\,p\dots p}_{R}\ j'_1\ j'_2\ \dots\ j'_s\ \overline{p+1}\ \overline{p+1}\ \dots \tag{6}$$

в) $i'_s = i_r$
г) если $v_2(1) \geqslant p$, то $i'_n = j'_n$ для всех n от 1 до s
д) если $v_2(1) < p$, то $j'_1 = v_2(1)$
е) если $v_2(1) < p$, то $i'_n = j'_{n+1}$ для всех n от 1 до $s-1$,

то d_2 на выходе выдает сверхслово $(0)^\infty$.
3) В иных случаях d_2 на выходе выдает любое сверхслово, кроме $(0)^\infty$.

Утверждение 3. *Если автомат c является t-повторителем, то пара автоматов (c, c) является решением уравнения $M(x, y) = h_0$ (к первому c добавляются 3 несущественных выхода, которые в схеме никуда не подсоединяются (см. рис. 5)).*

Доказательство. Пусть на вход v_1 подали произвольное сверхслово, представим его в виде (1).

1) Если $r > t$, то оба автомата на местах x и y выдадут отказ. В этом случае на входах v_4 и v_5 будет сверхслово вида (3), и тогда d_2 выдаст на выходе сверхслово $(0)^\infty$.

2) Если $r \leqslant t$ и $v_2(1) \geqslant p$, то на входах v_4 и v_5 будет сверхслово

$$\underbrace{p\,p\dots p}_{R}\ i_1\ i_2\ \dots\ i_r\ \overline{p+1}\ \overline{p+1}\ \dots \tag{7}$$

Несложно проверить выполнение всех условий случая 2) из определения автомата d_2, при котором d_2 выдаст на выходе сверхслово $(0)^\infty$.

3) Если $r \leqslant t$ и $v_2(1) < p$, то на входе v_4 будет сверхслово (7), а на входе v_5 сверхслово

$$\underbrace{p\, p \ldots p}_{R}\; v_2(1)\; i_1\; i_2\; \ldots\; i_{r-1}\; \overline{p+1}\; \overline{p+1}\; \ldots \tag{8}$$

Несложно проверить выполнение всех условий случая 2) из определения автомата d_2, при котором d_2 выдаст на выходе сверхслово $(0)^\infty$.

Итак, d_2 во всех случаях на выходе выдает сверхслово $(0)^\infty$. Значит пара автоматов (c, c) является решением уравнения $M(x, y) = h_0$. Утверждение доказано.

Утверждение 4. *Если (c_1, c_2) есть решение уравнения $M(x,y) = h_0$, то автоматы c_1 и c_2 являются повторителями (c_1 является повторителем для своего выхода v_4).*

Доказательство. Поскольку (c_1, c_2) есть решение уравнения $M(x, y) = h_0$, то при любом сверхслове (1) на входе схемы автомат d_2 на выходе должен выдать сверхслово $(0)^\infty$. Значит, на выходе c_1 должно быть сверхслово (5), или сверхслово (3). Предположим, что c_1 на входном сверхслове (1) ведет себя не как повторитель. Тогда на его выходе может быть только сверхслово (5) (причем $i'_1\; i'_2\; \ldots\; i'_s \neq i_1\; i_2\; \ldots\; i_r$), поскольку в остальных случаях c_1 ведет себя как повторитель. Будем i_n называть n-ным входным элементом, а i'_n — n-ным выходным элементом. Если $i'_n \neq i_n$, то будем говорить, что автомат c_1 обманывает в n-ном элементе, если $s < r$ — автомат c_1 сокращает, если $s > r$ — автомат c_1 удлиняет. Если для всех входных сверхслов автомат c_1 не обманывает, не сокращает и не удлиняет, то он является повторителем.

Аналогично, на выходе c_2 должно быть сверхслово (6), или сверхслово (3). Предположим, что c_2 на сверхслове (1) ведет себя не как повторитель. Тогда на его выходе может быть только сверхслово (6) (причем $j'_1\; j'_2\; \ldots\; j'_s \neq j_1\; j_2\; \ldots\; j_r$), поскольку в остальных случаях c_2 ведет себя как повторитель. Будем j_n называть n-ным входным элементом, а j'_n — n-ным выходным элементом. Если $j'_n \neq j_n$, то будем говорить, что автомат c_2 обманывает в n-ном элементе, если $s < r$ — автомат c_2 сокращает, если $s > r$ — автомат c_2 удлиняет. Если для всех входных сверхслов автомат c_2 не обманывает, не сокращает и не удлиняет, то он является повторителем.

1) Ни для какого входного сверхслова автомат c_2 не может обмануть в первом элементе, иначе в случае когда в начале стоит подсадной символ, не пройдет условие 2д) определения автомата d_2.

2) Если автомат c_2 не может обмануть в n-ном элементе ($n \leqslant s$) ни для какого входного сверхслова, то автомат c_1 тоже не может обмануть в n-ном элементе ни для какого входного сверхслова. Предположим, что это не так и для какого-то входного сверхслова автомат c_1 обманывает в n-ном элементе, $i'_n \neq i_n$. Пусть подсадного символа нет, тогда $j_n = i_n$. А в соответствии с условием 2е) автомата d_2 имеем $j'_n = i'_n$. Итак, $j'_n = i'_n \neq i_n = j_n$. Получается, что для данного входного сверхслова автомат c_2 обманывает в n-ном элементе. Противоречие.

3) Если автомат c_1 не может обмануть в n-ном элементе ни для какого входного сверхслова ($n \leqslant s-1$), то автомат c_2 не может обмануть в $n+1$-ом элементе ни для какого входного сверхслова. Предположим, что это не так и для какого-то входного сверхслова автомат c_2 обманывает в $n+1$-ом элементе, $j'_{n+1} \neq j_{n+1}$. Пусть в начале стоит подсадной символ, тогда $j_{n+1} = i_n$. А в соответствии с условием 2е) автомата d_2 имеем $j'_{n+1} = i'_n$. Итак, $i'_n = j'_{n+1} \neq j_{n+1} = i_n$. Получается, что для данного входного сверхслова автомат c_1 обманывает в n-ном элементе. Противоречие.

Из пунктов 1), 2), 3) следует, что автоматы c_1 и c_2 не могут обманывать ни в каком элементе.

Предположим, что автомат c_2 может сокращать. Тогда, в соответствии с условиями 2а) и 2б) автомата d_2, c_1 тоже сокращает. Пусть в начале стоит подсадной символ, и $i_r \neq i_s$. Поскольку автомат c_1 не может обманывать, то $i'_s = i_s$. Выходит, что $i'_s \neq i_r$ и не проходит условие 2в) автомата d_2. Противоречие.

Предположим, что автомат c_1 может сокращать. Тогда, в соответствии с условиями 2а) и 2б) автомата d_2, c_2 тоже сокращает. Противоречие.

Предположим, что автомат c_2 может удлинять. Тогда, в соответствии с условиями 2а) и 2б) автомата d_2, c_1 тоже удлиняет. Пусть в начале стоит подсадной символ, и $i_r \neq j'_{r+1}$. Поскольку автомат c_1 не может обманывать, то $i'_r = i_r$. Выходит, что $i'_r \neq j'_{r+1}$ и не выполняется условием 2е) автомата d_2. Противоречие.

Предположим, что автомат c_1 может удлинять. Тогда, в соответствии с условиями 2а) и 2б) автомата d_2, c_2 тоже может удлинять. Противоречие.

Поскольку автоматы c_1 и c_2 не могут ни обманывать, ни укорачивать, ни удлинять, то они являются повторителями. Утверждение доказано.

Пусть дана произвольная система Поста T ($E_m = \{0, 1, ..., m-1\}$ — конечный алфавит, $A_0, \ldots, A_{p-1}$ и $B_0, \ldots, B_{p-1}$ — слова в этом алфавите).

Построим по ней схему $P_T(x, y)$, изображенную на рис. 6. У $P_T(x, y)$ два входа: v_1 с алфавитом $E_{p+2} = \{0, 1, \ldots, p+1\}$ и v_2 с двоичным алфавитом $E_2 = \{0, 1\}$. У $P_T(x, y)$ один двоичный выход с алфавитом $E_2 = \{0, 1\}$. Выход v_4 «неизвестной» x никуда не присоединен.

Автомат d_3 осуществляет следующие проверки:

1) Проверяет, что на вход v_8 подается сверхслово вида

$$\underbrace{i_1 \underbrace{p\, p \ldots p}_{|A_{i_1}|}\; i_2 \underbrace{p\, p \ldots p}_{|A_{i_2}|}\; \ldots\; i_r \underbrace{p\, p \ldots p}_{|A_{i_r}|}}_{R_1}\; \overline{p+1}\; \overline{p+1}\; \ldots$$

2) Проверяет, что на вход v_9 подается сверхслово вида

$$\underbrace{j_1 \underbrace{p\, p \ldots p}_{|B_{j_1}|}\; j_2 \underbrace{p\, p \ldots p}_{|B_{j_2}|}\; \ldots\; j_s \underbrace{p\, p \ldots p}_{|B_{j_s}|}}_{R_2}\; \overline{p+1}\; \overline{p+1}\; \ldots$$

3) Проверяет, что $R_1 = R_2$

4) Проверяет, что $A_{i_1} A_{i_2} \ldots A_{i_r} = B_{j_1} B_{j_2} \ldots B_{j_s}$

5) Сверхслово вида (3) не должно появиться на входе v_5 (то есть если на месте y стоит повторитель, то y не выдает отказ до момента времени R_1).

6) Сверхслова на входах v_5 и v_7 совпадают.

Если результаты всех проверок положительны, то d_3 на выходе выдает сверхслово $(0)^\infty$. Иначе выдает любое другое сверхслово.

Утверждение 5. *Система Поста T сочетаема тогда и только тогда, когда имеет решение система уравнений*

$$\begin{cases} M(x,y) = h_0 \\ P_T(x,y) = h_0 \end{cases}$$

Доказательство. Пусть система Поста T сочетаема и её решением является набор индексов $i_1 i_2 \dots i_r$.

Пусть автомат c_1 работает как r-повторитель для входа v_1 и выхода v_4, а на остальных трех выходах выдает следующие константные последовательности: на выходе v_8 последовательность

$$\underbrace{i_1 \underbrace{p\,p \dots p}_{|A_{i_1}|}\; i_2 \underbrace{p\,p \dots p}_{|A_{i_2}|}\; \dots\; i_r \underbrace{p\,p \dots p}_{|A_{i_r}|}}_{R}\; \overline{p+1}\; \overline{p+1}\; \dots$$

на выходе v_9 последовательность

$$\underbrace{i_1 \underbrace{p\,p \dots p}_{|B_{i_1}|}\; i_2 \underbrace{p\,p \dots p}_{|B_{i_2}|}\; \dots\; i_r \underbrace{p\,p \dots p}_{|B_{i_r}|}}_{R}\; \overline{p+1}\; \overline{p+1}\; \dots$$

на выходе v_7 последовательность

$$\underbrace{p\,p \dots p}_{R}\; i_1\; i_2\; \dots\; i_r\; \overline{p+1}\; \overline{p+1}\; \dots$$

Пусть автомат c_2 является r-повторителем. Тогда (c_1, c_2) является решением уравнения $M(x,y) = h_0$ по утверждению 3. Кроме того, проходят все проверки у автомата d_3. Значит, (c_1, c_2) является решением и уравнения $P_T(x,y) = h_0$.

Обратно, пусть система автоматных уравнений имеет решение (c_1, c_2). Тогда по утверждению 4 c_2 является повторителем. Кроме того, должны выполняться все проверки автомата d_3. Пусть на выходе v_8 последовательность

$$\underbrace{i_1 \underbrace{p\,p \dots p}_{|A_{i_1}|}\; i_2 \underbrace{p\,p \dots p}_{|A_{i_2}|}\; \dots\; i_r \underbrace{p\,p \dots p}_{|A_{i_r}|}}_{R}\; \overline{p+1}\; \overline{p+1}\; \dots,$$

на выходе v_9 последовательность

$$\underbrace{j_1\,\underbrace{p\;p\ldots p}_{|B_{j_1}|}\;j_2\,\underbrace{p\;p\ldots p}_{|B_{j_2}|}\;\ldots\;j_s\,\underbrace{p\;p\ldots p}_{|B_{j_s}|}}_{R}\;\overline{p+1}\;\overline{p+1}\;\ldots$$

Другого вида эти последовательности быть не могут, чтобы выполнялись проверки 1 и 2 автомата d_3. Возможен один из трех случаев:

1) Предположим, что $i_1\ i_2\ \ldots\ i_r \neq j_1\ j_2\ \ldots\ j_s$. Если $v_2(1) = 0$, то по определению автомата MUX $v_3 = v_8$. А поскольку c_2 является повторителем и в процессе работы схемы c_2 не должен выдать отказ (проверка 5 автомата d_3), то на выходе автомата c_2 будет сверхслово

$$\underbrace{p\;p\ldots p}_{R}\;i_1\;i_2\;\ldots\;i_r\;\;\overline{p+1}\;\overline{p+1}\;\ldots \tag{9}$$

Если же $v_2(1) = 1$, то по определению автомата MUX $v_3 = v_9$. А поскольку c_2 является повторителем и в процессе работы схемы c_2 не должен выдать отказ (проверка 5 автомата d_3), то на выходе автомата c_2 будет сверхслово

$$\underbrace{p\;p\ldots p}_{R}\;j_1\;j_2\;\ldots\;j_s\;\;\overline{p+1}\;\overline{p+1}\;\ldots \tag{10}$$

Схема $P_T(x, y)$ построена таким образом, что автомат c_1 не имеет никакой информации о входе v_2. Значит, его поведение никаким образом не зависит от сверхслова v_2. Пусть автомат c_1 на выходе v_7 выдает сверхслово (9). Тогда если $v_2(1) = 1$, то на v_5 будет сверхслово (10). А поскольку $i_1\ i_2\ \ldots\ i_r \neq j_1\ j_2\ \ldots\ j_s$, то $v_5 \neq v_7$, и значит не будет выполняться проверка 6 автомата d_3. Если же автомат c_1 на выходе v_7 выдает любое другое сверхслово, отличное от (9), а $v_2(1) = 0$, то на v_5 будет сверхслово (9). И опять $v_5 \neq v_7$. Получается, то бы автомат c_1 ни выдал на своём выходе v_7, найдется такой вход схемы, что не будет выполняться проверка 6 автомата d_3. В этом случае на выходе схемы будет сверхслово, отличное от $(0)^\infty$. То есть данная пара автоматов (c_1, c_2) не являются решением уравнения $P_T(x, y)$. Противоречие. Значит, этот случай не возможен.

2) Предположим, что $r = s = \infty$. В этом случае автомат c_2 рано или поздно должен выдать отказ (так как не бывает автоматов с бесконечной памятью), и будет нарушена проверка 5 автомата d_3. Тогда на выходе P_T будет последовательность, отличная от $(0)^\infty$, и (c_1, c_2) не будут решением уравнения $P_T(x, y) = h_0$. Противоречие.

3) Остается последний случай — $i_1\ i_2\ \ldots\ i_r = j_1\ j_2\ \ldots\ j_s$. Отсюда и из проверки 4 автомата d_3 следует, что система Поста T сочетаема. Утверждение доказано.

Утверждение 6. *Для любой системы Поста можно конструктивно построить автоматное уравнение с двумя неизвестными, которое будет иметь решение если и только если имеет решение соответствующая система Поста.*

Доказательство. Произвольная система Поста T сочетаема тогда и только тогда когда имеет решение система

$$\begin{cases} M(x,y) = h_0 \\ P_T(x,y) = h_0 \end{cases}$$

(по утверждению 5). Далее, для этой системы существует автоматное уравнение $S_T(x, y)$ с двумя неизвестными, которое имеет решение тогда и только тогда, когда и система (по утверждению 2). Значит, уравнение $S_T(x, y)$ имеет решение тогда и только тогда, когда система Поста T сочетаема. Утверждение доказано.

Доказательство теоремы 1. Предположим, что алгоритм существует. Тогда с помощью утверждения 6 пользуясь этим алгоритмом мы смогли бы решить комбинаторную проблему Поста. Противоречие.

Замечание. Несложно заметить (см. рис. 4, рис. 5 и рис. 6), что в полученном уравнении $S_T(x, y)$ не будет обратных связей. Следовательно, задача решения автоматных уравнений с двумя неизвестными без обратной связи тоже алгоритмически неразрешима.

Список литературы

[1] Лялин И. В. Решение автоматных уравнений с одной неизвестной // Интеллектуальные системы. Т. 12. 2008.

[2] Григорян А. К. Метод декомпозиции конечных автоматов // Автоматика и телемеханика. № 5. 1968.

[3] Григорян А. К. Метод декомпозиции кончных автоматов с выделением выходного и входного автоматов // Автоматика и телемеханика. № 10. 1968.

[4] Подколзин А. С., Ушчумлич Ш. М. О решении систем автоматных уравнений // Дискретная математика. Т. 2, вып. 1. 1990.

[5] Лялин И. В. О решении автоматных уравнений // Дискретная математика. Т. 16, вып. 2. С. 104–116. 2004.

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