Выразимость линейных автоматов относительно расширенной суперпозиции

А. А. Летуновский

Доказана алгоритмическая разрешимость задачи выразимости линейных автоматов через произвольную конечную систему автоматов относительно расширенной суперпозиции.

Ключевые слова: автомат, линейный автомат, выразимость, суперпозиция, алгоритмическая разрешимость.

Введение

Известно, что решение задач полноты и выразимости относительно операции суперпозиции для систем автоматных функций наталкивается на существенные трудности [1]. Так в работе [2] установлена алгоритмическая неразрешимость задачи выразимости для конечных систем автоматных функций, а в [1] показана неполнота любой конечной системы автоматов. Ранее автор ввел понятие расширенной суперпозиции как суперпозиции для систем с обязательным наличием задержки и штриха Шеффера. Для расширенной суперпозиции автору удалось получить положительные результаты для выразимости константных автоматных функций, а также групповых автоматных функций [3, 4]. В данной работе изучается задача выразимости линейных автоматов. Доказана алгоритмическая разрешимость данной задачи.

Основные понятия и результаты

Пусть $E_2 = \{0, 1\}$, функции вида $g : E_2^n \to E_2$ называются булевыми функциями, их множество обозначается через P_2.

Пусть E_2^∞ — множество всех сверхслов вида $a(1)a(2)\ldots$, где $a(j) \in E_2$, $j = 1, 2, \ldots$. Через N обозначим множество натуральных чисел. Пусть

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

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

$$\begin{cases} q_1(1) = q0_1, \\ \ldots \\ q_s(1) = q0_s \\ q_1(t+1) = \varphi_1(q_1(t), \ldots, q_s(t), a_1, \ldots, a_n), \\ \ldots \\ q_s(t+1) = \varphi_s(q_1(t), \ldots, q_s(t), a_1, \ldots, a_n) \\ b_1(t) = \psi_1(q_1(t), \ldots, q_s(t), a_1, \ldots, a_n) \\ \ldots \\ b_m(t) = \psi_m(q_1(t), \ldots, q_s(t), a_1, \ldots, a_n) \end{cases} \tag{1}$$

Вектор $q = (q_1, \ldots, q_s)$ задает состояние a-функции f, $q0$ её начальное состояние, буквы $a = (a_1, a_2, \ldots, a_n)$ и $b = (b_1, \ldots, b_m)$ называют входной и выходной буквами, а сверхслова $a(1)a(2)\ldots$ и $b(1)b(2)\ldots$ — входными и выходными сверхсловами, соответственно. Вектор-функции φ и ψ называются функциями переходов и выходной функцией, соответственно, а шестерка

$$(E_2^n, E_2^s, E_2^m, \varphi, \psi, q0)$$

— автоматом, порождающим функцию f. Далее в тексте мы иногда будем использовать для автомата обозначение $(A, Q, B, \varphi, \psi, q0)$, при этом предполагая что $A \subseteq E_2^n, Q \subseteq E_2^s, B \subseteq E_2^m$.

В этом классе обычным образом введем операции суперпозиции. Для суперпозиции будем использовать модификации операций из [5].

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

Пусть $M \subseteq P$, обозначим через $[M]$ — множество a-функций, получающихся из M с помощью операций суперпозиции.

Автоматную функцию G_0, задаваемую уравнениями

$$\begin{cases} q(1) = 0, \\ q(t+1) = a(t), \\ b(t) = q(t), \end{cases}$$

назовём автоматной функцией задержки.

Будем называть автоматом Z_2 автомат, задаваемый рекуррентными соотношениями

$$\begin{cases} q(1) = 0, \\ q(t+1) = q(t) \oplus a(t), \\ b(t) = q(t), \end{cases}$$

Обозначим $<M> = [M \cup \{G_0, P_2\}]$ и назовем замыканием M относительно *расширенной суперпозиции.*

Автомат $A = (E_2^k, Q, E_2^l, \varphi, \psi, q0), Q \subset E_2^n$, называется *линейным*, если

$$\begin{cases} \varphi(x, q) = Aq \oplus Bx, \\ \psi(x, q) = Cq \oplus Dx, \\ q_0 = (0, 0, \ldots, 0), \end{cases}$$

где $A : E_2^n \to E_2^n, B : E_2^k \to E_2^n, C : E_2^n \to E_2^l, DB : E_2^k \to E_2^l$ — есть линейные операторы. Матрица A называется основной матрицей линейного атомата.

Константной автоматной функцией назовем автоматную функцию, выдающую одно и тоже периодическое выходное сверхслово на всех входных сверхсловах.

Через β_{K_1} обозначим сверхслово, получающееся на выходе константного автомата K_1.

Определение. Пусть сверхслово β можно представить в виде $\beta = \gamma\alpha^\infty$. Выберем из всех таких представлений такое, что γ и α имеют наименьшую длину. Для выбранного представления назовем γ — наименьшим предпериодом сверхслова β, а α наименьшим периодом сверхслова β, а всякое слово вида $\underbrace{\alpha\alpha\ldots\alpha}_{n}$ будем называть периодом сверхслова β, здесь $n \in N$. Обозначим $|\alpha|$ длину слова α.

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

Из [3] известно, что

$$\Theta(<M> \cap K]) = \{t : t|bq^i, i = 0, 1, \ldots\}.$$

Числа b и q называются *частным и главным цикловыми индексами* множества автоматов M.

Теорема 1. *Пусть M — произвольная конечная система автоматов, а L_1 — линейный автомат, тогда*

$$L_1 \in <M> \Leftrightarrow \Theta(<L_1> \cap K) \in \Theta(<M> \cap K).$$

Теорема 2. *Задача выразимости линейных автоматов через произвольное конечное множество автоматов относительно расширенной суперпозиции алгоритмически разрешима.*

Основные леммы и доказательство теорем

Лемма 1 ([7]). *Групповой линейный автомат выразим через групповой автономный автомат, Z_2 и задержку.*

Доказательство. Пусть L — линейный групповой автомат

$$L = (E_2^k, S, E_2^l, \varphi_1, \psi_1, 0), \quad S \subset E_2^n,$$
$$\begin{cases} q' = \varphi_1(x, s) = As \oplus Bx, \\ y = \psi_1(x, s) = Cs \oplus Dx, \\ s_0 = (0, 0, \ldots, 0), \end{cases}$$

где $A : E_2^n \to E_2^n, B : E_2^k \to E_2^k$ — линейные операторы. Так как L — групповой автомат, то $det(A) \neq 0$[7]. Найдется такое натуральное число t, что $A^t = I$, где I — тождественный линейный оператор и для всех $t' < t$ $A^t \neq I$. Возьмем автомат

$$G = (E_2^k, \{I, A, A^2, \ldots, A^{t-1}\} \times Q), E_2^l, \varphi_2, \psi_2, (I, 0)).$$

Для $(Q, q) \in \{I, A, A^2, \ldots, A^t\} \times Q, x \in Q, u \in E_2^l$

$$\begin{cases} (Q, q)' = \varphi_2(x, (Q, q)) = (Aq, q \oplus (AQ)^{-1}Bx), \\ u = \psi_2(x, (Q, q)) = \varphi_1(x, Qq) \\ q_0 = (0, 0, \ldots, 0), \end{cases}$$

Покажем, что автоматы L и G — эквивалентны. Пусть на входы автоматов L и G подана последовательность $x_1, x_2, \ldots, x_m$. Соответствующая ей последовательность состояний автомата L пусть $0, s_2, s_3, \ldots, s_m$, последовательность состояний автомата G $(I,0),(Q_2,q_2'),(Q_3,q_3'),\ldots,(Q_m,q_m')$, выходная последовательность автомата L $y_1, y_2, \ldots, y_m$, выходная последовательность автомата G $u_1, u_2, \ldots, u_m$.

Покажем,что последовательности состояний автоматов L и G связаны следующим соотношением:

$$Q_i q_i = s_i, i = 1, 2, \ldots, m.$$

Применим индукцию по длине входной последовательности. Первый шаг $I0 = 0$. Пусть $Q_i q_i = s_i$, из уравнений автомата L следует $Q_{i+1} = AQ_i, q_{i+1} = q_i + (AQ_i)^{-1}Bx_i$, тогда $Q_{i+1}q_{i+1} = AQ_i(q_i + (AQ_i)^{-1}Bx_i) = AQ_iq_i + Bx_i = As_i + Bx_i$. Из уравнений автомата G следует $s_{i+1} = As_i + Bx_i$, значит $Q_{i+1}q_{i+1} = s_{i+1}$. Теперь покажем, что выходные последовательности автоматов L и G одинаковы. В самом деле

$$y_1 = \varphi_q(x_1, 0), u_1 = \varphi_2(x_1, (I,0)) = \varphi_1(x_1, I0) = y_1,$$
$$y_2 = \varphi_q(x_2, s_2), u_2 = \varphi_2(x_2, (Q_2, q_2)) = \varphi_1(x_2, Q_2q_2) = y_2,$$
$$y_m = \varphi_q(x_m, s_m), u_m = \varphi_2(x_m, (Q_m, q_m)) = \varphi_1(x_m, Q_mq_m) = y_m.$$

Таким образом, на произвольной входной последовательности автоматы L и G дают одинаковые выходные последовательности, значит, L и G эквивалентны. Автомат G можно представить в виде схемы, изображенной на рис. 1.

Здесь β — автономный автомат $\beta = (\{I, A, \ldots, A^t\}, E_2^r, \gamma_1, \delta_1, I)$, где r — наименьшее натуральное число такое, что $t \leqslant 2^r$. Для $Q, Q' \in \{I, A, \ldots, A^t\}, z \in E_2^r$ $Q' = \gamma_1(Q) = AQ, z = \delta_1(Q)$. Функция δ_1 на A^i принимает значение $\delta_1(A^i) = a_1a_2\ldots a_r$, где $a_1a_2\ldots a_r$ — двоичная запись числа i.

$F_1 \in P_2$. $F_1 : E_2^r \times E_2^k \to E_2^n$, если $a_1a_2\ldots a_r$ — двоичная запись числа i, а $x \in E_2^k$, то $F_1(a_1a_2\ldots a_r, x) = (AA^i)^{-1}Bx$.

$F_2 \in P_2$. $F_2 : E_2^r \times E_2^n \times E_2^k \to E_2^l$. $F_1(a_1a_2\ldots a_r, v, x) = \varphi_1(x, A^i, v)$.

Лемма 2 ([7]). *Произвольный линейный автомат выразим через групповой линейный автомат и задержку.*

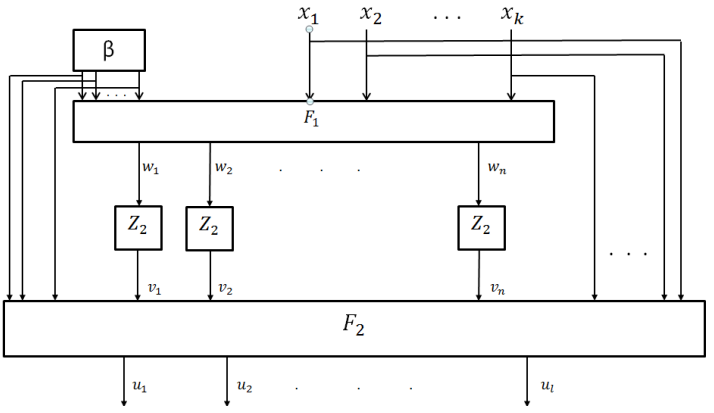

Рис. 1.

Доказательство. Пусть $L = (E_2^k, Q, E_2^l, \varphi, \psi, q_0)$, $Q \subset E_2^n$, $q_0 = 00\ldots0$ — линейный автомат и его уравнения

$$\begin{cases} q_1 = \varphi(x,q) = Aq \oplus Bx, \\ y_1 = \psi(x,q) = Cq \oplus Dx. \end{cases}$$

Можно выбрать такую систему координат в E_2^n, что в ней основная матрица A имеет клеточный вид[7]

$$\begin{pmatrix} A_1 & 0 & \ldots & 0 \\ 0 & A_2 & \ldots & 0 \\ . & . & . & . \\ 0 & 0 & \ldots & A_t \end{pmatrix}, \tag{2}$$

где либо $detA_i \neq 0$, либо $A_i = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ . & . & . & . & . \\ 0 & 0 & . & . & 1 \\ 0 & 0 & . & . & 0 \end{pmatrix}, i = 1, 2, \ldots, t.$

Если r_i — порядок квадратной матрицы A_i и $q_i \in E_2^r, i = 1, 2, \ldots, t$, то уравнения автомата L можно записать в следующем виде:

$$\begin{cases} q_1' = A_1 q_1 + B_1 x, \\ q_2' = A_2 q_2 + B_2 x, \\ \ldots \\ q_t' = A_t q_t + B_t x, \\ y = \psi(x, q_1, q_2, \ldots, q_t), \end{cases}$$

откуда видно, что автомат L изображается схемой, изображенной на рисунке 2, где $T_i = (E_2^k, Q_i, E_2^{r_i}, \varphi_i, \psi_i, q_0^{(i)})$, $Q_i \in E_2^{r_i}, q_0^{(i)} = 00\ldots0$,

$$\begin{cases} q_i' = A_i q_i + B_i x, \\ u_i = \psi(x, q_i), \end{cases} \quad i = 1, 2, \ldots, t.$$

$F \in P_2$. $F : E_2^{r_1} \times E_2^{r_1} \times \ldots \times E_2^{r_t} \times E_2^k \to E_2^l$. $F(u_1, u_2, \ldots, u_t, x) = \psi(x, u_1, u_2, \ldots, u_t)$.

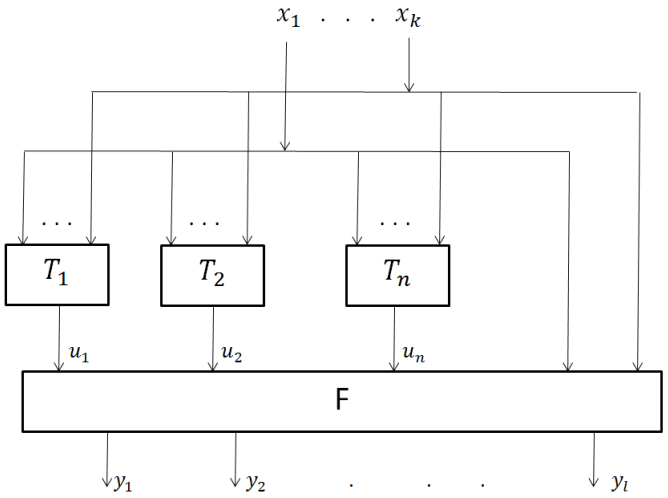

Рис. 2.

Если $detA_i \neq 0$, то автомат T_i — групповой.

Пусть $A_j = \underbrace{\begin{pmatrix} 0 & 1 & \ldots & 0 \\ . & . & \ldots & . \\ 0 & 0 & \ldots & 1 \\ 0 & 0 & \ldots & 0 \end{pmatrix}}_{r_j}$

Уравнения автомата T_j можно записать в виде

$$\begin{cases} q_1 = q_2 + B_j^{(1)} x \\ q_2 = q_3 + B_j^{(2)} x \\ \ldots \\ q_{r_j - 1} = q_{r_j} + B_j^{(r_j - 1)} x \\ q_{r_j} = B_j^{(r_j)} x \\ u_j = (q_1, q_2, \ldots, q_{r_j}), \end{cases}$$

откуда видно, что автомат T_j может быть реализован схемой, изображенной на рис. 3.

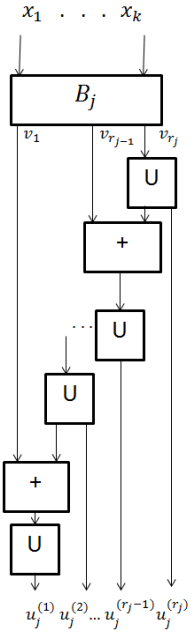

Рис. 3.

$B_j \in P_2$. $B_j : E_2^k \to E_2^{r_j}$. $B_j(x) = (B_j^(1)x, B_j^(2)x, \ldots, B_j^(r_j)x)$. G_0 — автомат задержка. $\oplus$ — двоичное сложение. Лемма доказана.

Лемма 3. *Пусть частный цикловый индекс линейного автономного автомата L равен b, K_b — все константные автоматы с длиной периода b, тогда если главный цикловый индекс равен 2, то:*
1. $L \in <K_b, Z_2>$,
2. $K_b \in <L>$,
3. $Z_2 \in <L>$.
Если главный цикловый индекс равен 1, то $L \in <K_b>$.

Доказательство. Из лемм 1, 2 следует, что главный цикловый индекс линейного автомата всегда либо 1 либо 2, так как линейный автомат выразим через константы, Z_2, задержки и булевы функции.

Рассмотрим представление линейного автомата в виде (2) и соответствующую рисунок 2.

Если ни один из автоматов T_i не является групповым, то для выразимости этого автомата достаточно булевых функций и задержек. Его главный цикловый индекс в этом случае равен 1.

Пусть хотя бы один из автоматов T_i — групповой. Если все групповые автоматы автономные, то в соответствующих схемах 1 булева функция F_2 не зависит от входов $v_1, v_2, \ldots, v_n$ и такие автоматы выразимы через автомат β.

Теперь предположим, что хотя бы один групповой автомат не автономный. Обозначим его T_1 и переставим его на первый вход в схеме 2. Функция F при этом существенно зависит от 1-го входа. Докажем тогда, что главный цикловый индекс автомата L не может быть равен 1. Действительно, пусть частный цикловый индекс автомата L равен b, а главный цикловый индекс равен 1. Тогда все константы периода 1 переходят после подачи на автомат L в константы периодов делителей b. Пусть автомат L задается уравнениями

$$\begin{cases} q(t+1) = Aq(t) + Bx(t) \\ y(t) = Cq(t) + Dx(t), \end{cases}$$

тогда, взяв в качестве константы периода 1 нулевое сверхслово, получим $Cq = CA^bq$ для любого q.

Докажем теперь, что $A^bq \sim q$. Так как $CA^iq = CA^{b+i}q$, то $C(A^iq + A^{i-1}B\alpha_1 + \ldots + B\alpha_i) = C(A^{b+i}q + A^{i-1}B\alpha_1 + \ldots + B\alpha_i)$ для любых q и $\alpha_1\alpha_1 \ldots \alpha_i$ и состояние $A^bq \sim q$. По условию $Cq = C(A^bq + A^{b-1}B\alpha_1 + \ldots + B\alpha_b)$, а значит $C(A^{b-1}B\alpha_1 + \ldots + B\alpha_b) = 0$ для всех слов длины b. Значит автомат по всем словам длины b переходит в начальное состояние. Такой автомат не является групповым. Получили противоречие.

Для доказательства утверждения 1 заметим, что в леммах 1, 2 мы построили линейный автомат из задержек, булевых функций, Z_2 и константы периода t такого, что $A_G^t = I$, где A_G — невырожденная часть в разложении (2). Ранее в доказательстве мы показали, что если частный цикловый индекс автомата равен b, причем $b|t$, то состояния q и A^bq — неотличимы. А значит групповой автомат можно заменить на эквивалентный такой, что $A_G'^b = I$, а значит и константу можно заменить на частный цикловый индекс.

Доказательство теоремы 1. Пусть $L \in M$, тогда возможны 3 случая.

1. $L \in <\varnothing>$

2. $L \in <K_b>$. Тогда L выразим тогда и только тогда когда выразимы все константы периода b.
3. $L \in <K_b, Z_2>$. Тогда L выразим тогда и только тогда, когда выразимы все константы периода b и Z_2. А Z_2 выразим тогда и только тогда, когда главный цикловый индекс M делится на 2, а значит тогда и только тогда, когда выразимы все константы периода степени 2. Теорема доказана.

Теорема 2 непосредственно следует из теоремы 1.

Работа выполнена на кафедре МаТИС механико-математического факультета МГУ им. Ломоносова под руководством профессора Д. Н. Бабина.

Список литературы

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

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

[3] Летуновский А. А. О выразимости константных автоматов суперпозициями // Интеллектуальные системы. — 2009. Т. 13, вып. 1–4. — С. 397–406.

[4] Летуновский А. А. О задаче выразимости автоматов относительно суперпозиции для систем с фиксированной добавкой // Интеллектуальные системы. — 2011. Т. 15, вып. 1–4. — С. 401–412.

[5] Мальцев А. И. Алгоритмы и рекурсивные функции. — М.: Наука, 1965.

[6] Бабин Д. Н. Задача выразимости в некоторых классах автоматов // Комбинаторно-алгебраические методы в прикладной математике. — 1982. — С. 21–45.

[7] Гилл А. Линейные последовательностные машины. Анализ, синтез и применение / Пер. с англ. А. С. Бернштейна. — М.: Наука, 1974.