О выразимости константных автоматов суперпозициями

А. А. Летуновский

Показано, что для конечных систем автоматных функций, содержащих все истинностные функции и задержку, существует алгоритм выразимости константных автоматных функций. Множество выразимых константных автоматных функций явно описывается по первоначально заданной конечной системе автоматов. Также показано существование алгоритма выразимости автономных автоматов.

Введение

Известно, что решение задачи 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 работе [9] показана алгоритмическая неразрешимость определения бесконечности множества выразимых констант. Ранее в задачах полноты относительно суперпозиции и обратной связи удалось получить положительные результаты для систем функций, содержащих фиксированную добавку [3,5]. В статье показано, что по системе автоматных функций с фиксированной добавкой из всех истинностных функций и задержки можно определить выразима ли через неё конкретная константная автоматная функция, а также явно описать все выразимые константные автоматные функции. В качестве следствия показано существование алгоритма выразимости автономных автоматных функций для систем с той же добавкой.

1. Основные понятия и результаты

Пусть $E_k = \{0, 1, \ldots, k-1\}$, функции вида $g : E_k^n \to E_k$ называются функциями k- значной логики, их множество обозначается через P_k. Пусть E_k^∞- множество всех сверхслов вида $a(1)a(2)\ldots$, где $a(j) \in E_k$, $j = 1, 2, \ldots$. Через N обозначим множество натуральных чисел. Пусть

$$f : (E_k^\infty)^n \to (E_k^\infty)^m \text{ —}$$

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

$$\begin{cases} q_1(1) = q0_1, \\ \ldots \\ q_s(1) = q0_s \\ q_1(t+1) = \phi_1(q_1(t), \ldots, q_s(t), a_1, \ldots, a_n), \\ \ldots \\ q_s(t+1) = \phi_s(q_1(t), \ldots, q_s(t), a_1, \ldots, a_n) \\ b_1(t) = \psi_1(q_1(t), \ldots, q_s(t), a_1, \ldots, a_n) \\ \ldots \\ b_m(t) = \psi_m(q_1(t), \ldots, q_s(t), a_1, \ldots, a_n) \end{cases} \tag{1}$$

Вектор $q = (q_1, \ldots, q_s)$ задает состояние a-функции f, q_0 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

$$(E_k^n, E_k^s, E_k^m, \phi, \psi, q_0) \text{ —}$$

автоматом, порождающим функцию f. Далее в тексте мы иногда будем использовать для автомата обозначение $(A, Q, B, \phi, \psi, q_0)$, при этом предполагая что $A \subseteq E_k^n, Q \subseteq E_k^s, B \subseteq E_k^m$. Обычным образом доопределим функции ϕ и ψ на слова:
$\phi(q, a(1)\ldots a(t)) = \phi(\phi \ldots \phi(q, a(1)), \ldots, a(t-1)), a(t))$,
$\psi(q, a(1), \ldots, a(t)) = \psi(\phi(q, a(1)), \ldots, a(t-1)), a(t))$
и определим рекурсивно функцию

$\overline{\psi}(q, a(1), \ldots, a(t)) = \overline{\psi}(q, a(1), \ldots, a(t-1))\psi(\phi(q, a(1), \ldots, a(t-1)), a(t))$. Класс всех a-функций обозначим через P.

В этом классе обычным образом введем операции суперпозиции. Для суперпозиции будем использовать модификации операций из [7].

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

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

Автоматную функцию G_0, задаваемую уравнениями

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

назовём автоматной функцией задержки.

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

Автономной назовём автоматную функцию с функцией переходов, несущественно зависящей от входа. Класс автономных автоматных функций обозначим через U. Заметим, что $K \subset U$.

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

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

Определение 1. 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 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 $\Theta(\beta) = |\alpha|$.

Мы будем рассматривать следующие задачи: по конечному множеству автоматов $M \subset P$ и $\beta \in K$ проверить, верно ли что

$$1)\ \ \beta \in [M \cup \{G_0, P_k\}],$$
$$2)\ \ \mid \Theta([M \cup \{G_0, P_k\}] \cap K) \mid < \infty.$$

Также опишем множество $\Theta([M \cup \{G_0, P_k\}] \cap K)$.

Замечание 1. Для множеств автоматных функций, содержащих фиксированную добавку из задержки и всех булевых функций, получаем что мощность множества выразимых констант всегда равна бесконечности (за счет увеличения предпериода функцией задержки), поэтому для второй задачи мы рассматриваем мощность множества минимальных периодов.

Теорема 1. *Пусть M — конечное множество автоматных функций и β — константная автоматная функция, тогда существует алгоритм, позволяющий проверить свойство*

$$\beta \in [M \cup \{G_0, P_k\}].$$

Теорема 2. *Пусть M — конечное множество автоматных функций, тогда существует алгоритм, позволяющий проверить свойство*

$$\mid \Theta([M \cup \{G_0, P_k\}] \cap K) \mid < \infty.$$

Теорема 3. $\Theta([M \cup \{G_0, P_k\}] \cap K)$ *представимо в конечном автомате, который эффективно строится по M.*

Следствие 1. *Пусть M — конечное множество автоматных функций и u — автономная автоматная функция, тогда существует алгоритм, позволяющий проверить свойство*

$$u \in [M \cup \{G_0, P_k\}].$$

2. Основные леммы и доказательства теорем

Лемма 1. *Пусть $K_1, K_2 \in K$, причем $\Theta(K_2)$ делит $\Theta(K_1)$. Тогда $K_2 \in [K_1 \cup \{G_0, P_k\}]$.*

Доказательство. Обозначим $n = \Theta(K_1), n_1 = \Theta(K_2)$. Пусть $\beta_{K_1} = \delta_1\delta_2 \ldots \delta_n(\beta^1_{K_1} \ldots \beta^n_{K_1})^\infty$. Рассмотрим схему Σ' (рис. 1), где f — булева функция.

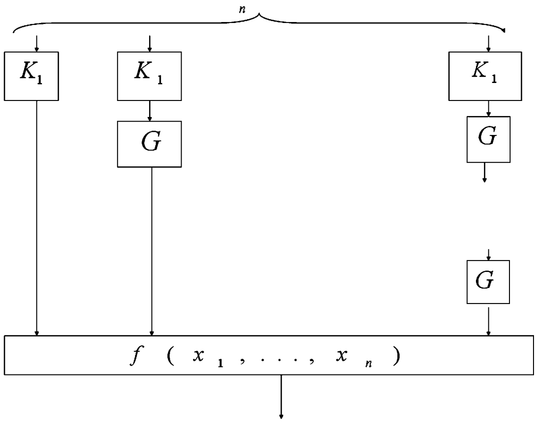

Рис. 1.

При подходящем выборе f Σ' реализует константный автомат K_2 с любым периодом n_1 выходного сверхслова $\beta^1_{K_2} \ldots \beta^{n_1}_{K_2}$, таким, что $n_1|n$ и предпериодом длины $2n$. Действительно для любого $t > 2n$ в моменты времени $t, t+1, \ldots, t+n$ на входе f появляются разные входные наборы, поэтому всегда можно так выбрать f, чтобы схема Σ' реализовывала наперед заданный константный автомат с наперед заданным периодом длины n.

От предпериода мы можем избавиться, рассмотрев константные автоматы

$K_3 = \beta^1_{K_2} \dots \beta^n_{K_2} \beta^1_{K_2} \dots \beta^n_{K_2} 00 \dots$, $Z = \underbrace{11 \dots 1}_{2n} 00 \dots$ и булеву функцию $f(x, y, z) = xy + \overline{x}z$. Подав на первый её вход Z, на второй K_3, на третий K_2 получим необходимый автомат.

Таким образом, имея в замыкании константу периода n мы можем получить подходящими схемами все константы периода $n_1|n$ с любым предпериодом. Лемма доказана.

Лемма 1 фактически позволяет нам работать не с множеством констант, выразимых через данную систему автоматов, а с множеством длин констант, выразимых данной системой автоматов.

Для $M \subset P$ обозначим через $R(M)$ подмножество натуральных чисел вида $R(M) = \Theta([M \cup \{G_0, P_k\}] \cap K)$ — это и есть множество длин периодов констант, выразимых множеством автоматов M, G_0, P_k.

Имеет место

Замечание 2. Пусть $|R(M)| < \infty$, тогда

$$R(M) = \{l \in N : l| \max(R(M))\}.$$

Замечание 3. Пусть $K_1, K_2 \in K$. Тогда

$$\max(R(\{K_1\} \cup \{K_2\})) = \text{НОК}(\max(R(K_1)), \max(R(K_2))).$$

Из известной леммы об удлинении периода констант автоматом [8] получаем, что длина периода константы, выразимой автоматом, имеет вид $2^{l_1} 3^{l_2} \dots p_i^{l_{i-1}}$, где p_i - простые числа, $p_i \leqslant |Q|$, а l_i — натуральные числа.

Для некоторого автомата A и произвольного слова $\alpha \in A^*$ обозначим через $s_\alpha = \phi_\alpha, (\phi_\alpha(q) = \phi_(q, \alpha))$ — подстановку на множестве состояний, задаваемую этим словом, π_α - разбиение множества состояний Q на классы отличимости этим словом. Состояния q_i и q_j принадлежат одному классу отличимости, если $\overline{\psi}(q_i, \alpha) = \overline{\psi}(q_j, \alpha)$.

Обозначим $p_\alpha = (s_\alpha, \pi_\alpha)$. $P_l = \{p_\alpha, |\alpha| = l\}$.

Рассмотрим последовательность $n_1, n_2, \dots, n_k, \dots$ натуральных чисел, связанную с автоматом А, где n_{i+1} получается из n_i следующим рекурсивным способом.

Пусть $c_i = \{\alpha_i\}$ — множество сверхслов с длиной периода n_i (не обязательно минимальной). Рассмотрим множество выходных сверхслов автомата A после подачи на него слов из c_i. Обозначим его через $A(c_i)$. Очевидно, что $A(c_i)$ — конечно. Тогда положим $n_{i+1} = HOK(\Theta(A(c_i)))$. Из замечаний 2, 3 следует, что n_i — максимальная длина периода констант, выразимых схемой глубины i (глубина схемы учитывается без учета истинностных функций и задержек), а длина периода произвольной константы, выразимой схемой глубины i, является делителем n_i.

По построению $n_i|n_{i+1}$. Далее мы докажем, что $m_i = \frac{n_{i+1}}{n_i}$ — периодическая последовательность.

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

Доказательство. Без ограничения общности докажем $P_{lk} \subseteq P_{mk}$.

Для этого докажем, что $\forall \alpha, |\alpha| = lk\ \exists \alpha_1, |\alpha_1| = mk$, такое что $p_{lk} = p_{mk}$.

Пусть $\alpha = \beta_1 \dots \beta_k$, где $|\beta_i| = l$. Тогда $s_\alpha = s_{\beta_1} * \dots * s_{\beta_k}$, а π_α будет получаться сначала как разбиение, задаваемое β_1, затем как измельчение этого разбиения разбиением, задаваемым словом $\beta_1\beta_2$ и т. д. Для $\forall p_{\beta_i} \in P_l\ \exists p_{\gamma_i} \in P_m$, такое что $p_{\beta_i} = p_{\gamma_i}$. Рассмотрим слово $\alpha_1 = \gamma_1 \dots \gamma_k$. Докажем, что для него выполнено

$p_\alpha = p_{\alpha_1}$. Действительно

$s_{\alpha 1} = s_{\gamma 1} * \dots * s_{\gamma k}$,

а $\pi_{\alpha 1}$ будет получаться сначала как разбиение, задаваемое γ_1, затем как измельчение этого разбиения разбиением $\gamma_1\gamma_2$ и т. д.

Таким образом $P_{lk} \subset P_{mk}$, обратное включение доказывается аналогично и лемма доказана.

Лемма 3. *m_i — периодична.*

Доказательство. Пусть нашлись n_i, n_j, такие, что $P_{n_i}{=}P_{n_j}$. Из построения m_i следует, что m_i — это фактически длина максимального удлинения, получаемого при подаче слов длины n_i на автомат A и затем взятия НОК этих удлинений. Очевидно, что множество удлинений однозначно задается множеством P_{n_i}. Таким образом $m_i = m_j$

и из леммы 2 следует, что $P^{n_{i+1}}{=}P^{n_{j+1}}$, а таким образом $m_{i+1} = m_{j+1}$ и лемма доказана.

Теперь перейдем к описанию алгоритма определения множества констант, выразимых через данную систему автоматов.
Алгоритм A
1 шаг. Строим последовательность n_i до тех пор, пока P_i не найдутся n_i и n_j, такие, что $P_{n_i} = P_{n_j}$. Такие i и j найдутся, так как P_{n_i} является подмножеством прямого произведения множества всех подстановок на Q и 2^Q, а данное произведение конечно.
2 шаг. Описание всех констант. Множеством длин периодов констант, выразимых системой автоматов, является множество делителей натуральных чисел вида $L = n_i * (\frac{n_j}{n_i})^t$, где t натуральное.

Лемма 4. *Описанный алгоритм перечесляет те и только те константы, которые содержатся в замыкании исходного множества.*

Доказательство. Достаточность. Пусть константа содержится в замыкании нашего множества, тогда длина её периода делит n_i для некоторого i. Действительно, длина константы в замыкании множества получается последовательным увеличением с помощью умножения на делители чисел m_i, а так как $n_i = m_1 * m_2 * \ldots m_{i-1}$, то длина периода константы является делителем n_i для некотрого i. Докажем, что множество L содержит все n_i. При построении L мы перечисляли n_i до тех пор, пока для некоторых i, j $P_{n_i}{=}P_{n_j}$. Из равенства $P_{n_i}{=}P_{n_j}$ следует равенство $m_i = m_j$. Таким образом существует натуральное число $N = m_i * m_{i+1} * \ldots * m_{j-1}$, такое что $n_j = n_i * N$, $n_{j+1} = n_{i+1} * N$,... Отсюда, очевидным образом следует необходимое утверждение.

Необходимость фактически следует из того, что $L = \bigcup_{i=1}^{\infty}\{n'_i : n'_i|n_i\}$. Лемма доказана.

Доказательство теоремы 1 следует из леммы 4.

Доказательство теоремы 2 следует из того, что константных автоматов в замыкании множества бесконечно много тогда и только тогда когда множество L — бесконечно.

Доказательство теоремы 3. Алгоритм A следует описывает дерево о.д.-функции (ввиду периодичности последовательности m_i), значит множество длин констант, выразимых множеством автоматов с добавкой является регулярным множеством.

Определение 2. Назовем длиной периода автономного автомата длину периода его функции переходов.

Для доказательства следствия 1 нам понадобится

Лемма 5. *Пусть u_l — некоторый приведенный автономный автомат с минимальной длиной периода l, k_l — константный автомат с минимальной длиной периода l, тогда для произвольного конечного множества автоматов M выполнено*

$$k_l \in \{M, P_K, G_0\} \Leftrightarrow u_l \in \{M, P_K, G_0\}.$$

Доказательство. Для доказательства достаточности построим явно автомат u_l через k_l, булевы функции и задержки. Пусть в разных состояниях $q_1, \ldots, q_n$ автоматной функции u_l реализуются разные булевы функции $\psi_1, \ldots, \psi_n$, причем $\psi_1, \ldots, \psi_l$ повторяются в периоде. По лемме 1 выразимы константные автоматные функции

$K_1 = (\underbrace{10\ldots0}_{l})^\infty$, $K_2 = (\underbrace{01\ldots0}_{l})^\infty \ldots, K_l = (\underbrace{00\ldots1}_{l})^\infty$.

Тогда u_l выразима формулой

$u_l = \bigvee_1^m((K_i \& \psi_i))$.

Для доказательства необходимости применим метод доказательства от противного. Без ограничения общности будем считать, что автомат u_l имеет один вход. Докажем, что возможно получить схему, на выходе которой будет реализовываться константа периода l. Пусть это невозможно. Рассмотрим параллельное соединение двух автоматов u_l. На вход первого подадим 0^∞, на вход второго 1^∞.На выходе получим последовательность пар (x, y), где $x, y \in \{0, 1\}$. Пусть эта последовательность имеет период, меньший, чем l, без ограничения общности $l/2$. Тогда $\psi_1 = \psi_{l/2+1}, \psi_2 = \psi_{l/2+2}, \ldots, \psi_{l/2} = \psi_l$, а это противоречит приведенности автомата u_l. Лемма доказана.

Следствие 1 следует из теоремы 1 и из леммы 5.

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

Список литературы

[1] Кудрявцев В. Б. О мощностях множеств предполных классов некоторых функциональных систем, связанных с автоматами // ДАН СССР. Т. 151. № 3. 1963. 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] Буевич В. А. Об алгоритмической неразрешимости распознавания А-полноты для о.д.-функций // Математические заметки. Т. 12. № 6. 1972. С. 687–697.

[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 классификации автоматных базисов Поста по разрешимости свойств полноты и А-полноты // Доклады Академии наук. № 4. Т. 367. 1999. С. 439–441.

[6] Буевич В. А. Условия А-полноты для автоматов. М.: Изд. МГУ, 1986.

[7] Мальцев А. И. Итеративные алгебры и многообразие Поста // Алгебра и логика. 1966. Т. 5. № 2. С. 5–24.

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

[9] Летуновский А. А. О выразимости константных автоматнов // Интеллектуальные системы. Т. 9, вып. 1–4. 2005. С. 457–469.