

А. А. Летуновский, инженер-программист
ООО «ЭлЭсАй Интернешнел Ресерч», Москва

О ЗАДАЧЕ ВЫРАЗИМОСТИ АВТОМАТОВ ОТНОСИТЕЛЬНО СУПЕРПОЗИЦИИ ДЛЯ СИСТЕМ С ФИКСИРОВАННОЙ ДОБАВКОЙ

Рассматривается задача выразимости конечного группового автомата Медведева M суперпозициями систем вида $\Phi \cup R$, где Φ состоит из всех булевых функций и «задержки», R – произвольная конечная система автоматов. Ранее автор показал, что для группового автомата Медведева M , группа которого является разрешимой, существует алгоритм проверки $M \in [\Phi \cup R]$. В настоящей работе решается задача выразимости через системы $\Phi \cup R$ произвольных групповых автоматов Медведева.

Ключевые слова: конечный автомат, выразимости, алгоритм, группа

Введение

Известно, что решение задачи выразимости относительно операции суперпозиции для систем автоматных функций наталкивается на существенные трудности [1], а задача полноты не имеет смысла, так как все полные системы бесконечны. Тем не менее, в задаче полноты удалось понизить арность полных систем до 2 [2]. Для задачи выразимости в работе [3] установлена алгоритмическая неразрешимость для конечных систем автоматных функций. Ранее в задачах полноты относительно суперпозиции и обратной связи были получены результаты для алгоритмической разрешимости систем с фиксированной добавкой [5], поэтому имеет смысл решать задачу выразимости для систем с фиксированной добавкой. Автор в работах [4, 8] изучил алгоритмическую разрешимость задачи выразимости для автоматов с безусловными переходами. Ранее автор показал, что по системе автоматных функций, содержащей все булевы функции и «задержку» можно определить, выражима ли через эту систему конкретная автоматная функция, полугруппа которой является разрешимой группой [7]. В данной статье автор продолжает изучение случаев, где задача выразимости разрешима. В качестве выражаемой автоматной функции рассматривается автоматная функция Медведева группового автомата.

Основные понятия и результаты

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

Пусть E_2^∞ – множество всех сверхслов вида $a(1)a(2)\dots$, где $a(j) \in E_2$, $j = 1, 2, \dots$. Через N обозначим множество натуральных чисел. Для $k, l \in N$ будем обозначать через $k | l$ то, что k делит l .

Пусть $f : (E_2^\infty)^n \rightarrow (E_2^\infty)^m$ – автоматная функция (a -функция), т. е. она задается рекуррентно соотношениями (1)

$$\left\{ \begin{array}{l} q_1(1) = q0_1, \\ \dots \\ q_s(1) = q0_s \\ q_1(t+1) = \varphi_1(q_1(t), \dots, q_s(t), a_1, \dots, a_n), \\ \dots \\ q_s(t+1) = \varphi_s(q_1(t), \dots, q_s(t), a_1, \dots, a_n) \\ b_1(t) = \psi_1(q_1(t), \dots, q_s(t), a_1, \dots, a_n) \\ \dots \\ b_m(t) = \psi_m(q_1(t), \dots, q_s(t), a_1, \dots, a_n) \end{array} \right. \quad (1)$$

Вектор $q = (q_1, \dots, q_s)$ задает состояние a -функции f , $q0$ ее начальное состояние, буквы $a = (a_1, a_2, \dots, a_n)$ и $b = (b_1, \dots, b_m)$ называются входной и выходной буквами, а сверхслова $a(1)a(2)\dots$ и $b(1)b(2)\dots$ – 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 $A \subseteq E_2^n, Q \subseteq E_2^s, B \subseteq E_2^m$.

Автомат называется автоматом Медведева, если $B = Q, \psi(a, q) = q$.

Обычным образом доопределим функции φ и ψ на слова [1]:

$$\begin{aligned} \varphi(q, a(1)\dots a(t)) &= \varphi(\varphi(\dots \varphi(q, a(1)), \dots, a(t-1)), a(t)), \\ \psi(q, a(1), \dots, a(t)) &= \psi(\varphi(q, a(1)), \dots, a(t-1), a(t)) \end{aligned}$$

и определим рекурсивно функцию

$$\bar{\psi}(q, a(1), \dots, a(t)) = \bar{\psi}(q, a(1), \dots, a(t-1))\psi(\varphi(q, a(1)\dots a(t-1)), a(t)).$$

Класс всех a -функций обозначим через P_a . Класс всех a -функций с не более чем n состояниями обозначим P_a^n .

В этом классе обычным образом введем операции суперпозиции. Для суперпозиции будем использовать модификации операций из [6].

$$\left\{ \begin{array}{l} (\eta f)(x_1, x_2, \dots, x_n) = f(x_2, x_3, \dots, x_n, x_1), \\ (\varepsilon f)(x_1, x_2, \dots, x_n) = f(x_2, x_1, x_3, \dots, x_n), \\ (\varpi f)(x_1, x_2, \dots, x_n) = f(x_1, x_3, \dots, x_n), \\ (\delta f)(x_1, x_2, \dots, x_n) = f(x_1, x_2, \dots, x_{n+1}), \\ (f * g)(x_1, x_2, \dots, x_{m+n-1}) = f(g(x_1, \dots, x_m), x_{m+1}, \dots, x_{m+n-1}). \end{array} \right.$$

Пусть $R \subseteq P_a$, обозначим через $[R]$ – множество a -функций, получающихся из R с помощью операций суперпозиции. Рассматривая системы автоматов, будем считать без ограничения общности, что R 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

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

назовем автоматной функцией «задержки».

Обозначим $\langle R \rangle = [R \cup \{P_2, G_0\}]$.

Назовем автомат групповым, если все $\varphi_a(q) = \varphi(a, q), a \in A$ являются биекциями на Q .

Будем называть автоматом Z_2 автомат, задаваемый рекуррентными соотношениями

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

Будем называть триггером (T) автомат Медведева с двумя входами и двумя состояниями со следующей функцией переходов:

$$\begin{aligned} \varphi(0, 00) &= 0, \varphi(1, 00) = 1, \\ \varphi(0, 01) &= 0, \varphi(1, 01) = 0, \\ \varphi(0, 10) &= 1, \varphi(1, 10) = 1, \\ \varphi(0, 11) &= 0, \varphi(1, 11) = 1. \end{aligned}$$

Теорема 1. Пусть R – произвольная система автоматов, M – произвольный групповой автомат Медведева, тогда задача определения $M \in \langle R \rangle$ является алгоритмически разрешимой.

Теорема 2. Пусть R – произвольная система автоматов, M – произвольный групповой автомат, тогда задача определения $M \in \langle R, Z_2 \rangle$ является алгоритмически разрешимой.

Теорема 3. Пусть R – произвольная система автоматов, тогда задача $\langle R, T \rangle \supseteq P_a^n$ является алгоритмически разрешимой.

Основные леммы и доказательство теоремы

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

Через β_M обозначим сверхслово, получающееся на выходе константного автомата M .

Для множества константных автоматных функций $K' \subseteq K$ обозначим через $\Theta(K')$ – множество длин минимальных периодов сверхслов $\{\beta_M : M \in K'\}$.

Из [8] известно, что для $R \subseteq P$ в случае $[R] \supseteq \{P_2, G_0\}, |R| < \infty$ задача выразимости константных автоматных функций является алгоритмически разрешимой, более того $\exists$ натуральные $b_R, q_R \in N$ такие, что

$$\Theta(<R>\cap K) = \{t : t \mid b_R q_R^i, i = 0, 1, \dots\}.$$

Число q_R называется главным цикловым индексом автомата R , b_R назовем частным цикловым индексом автомата R .

В работе [5] показано, что цикловые индексы b_R и q_R вычисляются по R . Заметим, что $q_R^2, q_R^3, \dots, q_R^i, \dots$ также являются главными цикловыми индексами, а $bq_R^2, bq_R^3, \dots, bq_R^i, \dots$ являются частными цикловыми индексами. Будем обозначать $q_R = q, b_M = b$.

Пусть $t \in N$, обозначим $M^t = (A^t, Q, B^t, \bar{\varphi}, \bar{\psi}, q0)$ – автомат M на словах длины t .

Обозначим φ_α – подстановку на множестве состояний автомата, задаваемую словом $\alpha \in A^*$, а через $\pi_\alpha = \{Q_1, \dots, Q_s\}$ – разбиение множества состояний автомата на классы эквивалентности по равенству выходных слов на входном слове α – такое, что $Q_1 \cup \dots \cup Q_s = Q$ и $\forall q_1, q_2 \in Q \quad q_1, q_2 \in Q_i \Leftrightarrow \bar{\psi}(q_1, \alpha) = \bar{\psi}(q_2, \alpha)$.

Пусть $\alpha \in A^*$. Обозначим $p_\alpha = (\varphi_\alpha, \pi_\alpha)$. Для $A' \in A^*$ обозначим $P_{A'} = \{p_\alpha : \alpha \in A'\}$.

Определение 1. Будем говорить, что автоматы

$$M_1 = (A_1, Q_1, B_1, \varphi_1, \psi_1), \quad M_2 = (A_2, Q_2, B_2, \varphi_2, \psi_2)$$

подобны ($M_1 \approx M_2$), если $Q_1 = Q_2$ и $P_{A_1} = P_{A_2}$.

Утверждение 1. Пусть автоматы M_1 и M_2 подобны, тогда $M_1 \in <M_2>$ и $M_2 \in <M_1>$.

Так как всего существует конечное число попарно неподобных автоматов с фиксированным числом состояний, то в последовательности $M^b, M^{bq}, M^{bq^2}, \dots$ найдется конечное число попарно неподобных автоматов. Значит, для некоторых $l_0 < l_1$ $M^{l_0} \approx M^{l_1}$. Без ограничения общности можно считать частным цикловым индексом автомата M число bq^{l_0} , а главным цикловым индексом число $q^{l_1-l_0}$.

Определение 2 [2]. Пусть f и g – автоматы с одинаковым числом входов и одинаковым числом выходов. Скажем, что автоматная функция g копирует автоматную функцию f , если найдутся такие натуральные n, j, k ($n \leq j$), что для любого $l = 0, 1, 2, \dots$ и любой входной последовательности достаточной длины значение автоматной функции g в момент $j + kl$ совпадает со значением автоматной функции f в момент $n + kl$, т. е. $f(n + kl) = g(j + kl)$.

Обозначим K_s – константный автомат $\underbrace{(1 \dots 0)}_s$.

Лемма 1 [2] (Лемма о копировании). Пусть f – автоматная функция Медведева и g копирует f с параметрами n, j, s , тогда $f \in <g \cup K_s>$.

Лемма 2. Пусть b, q – цикловые индексы автомата M , $q > 1$ и M^{bq} подобен автомату Медведева, тогда $M^{bq} \in <M>$.

Доказательство: Для доказательства леммы введем некоторые обозначения и приведем схему, копирующую автомат M^{bq} :

$f(x_1, \dots, x_{(bq)^2})$ – булева функция с $(bq)^2$ входами и bq выходами, такая, что $f(\bar{x}) = \bar{y}$ тогда и только тогда, когда $p(\bar{x}) = p(\bar{y})$, причем $y_1 = x_1$. Такое $\bar{y}$ всегда найдется по построению цикловых индексов;

w, w_1 – автоматные функции с bq входами и одним выходом, такие, что $w(t) = x_i$ при $t = i \bmod n_1$, $w_1(t) = x_i$ при $t = i \bmod n_1 + 1$;

w^{-1} – автоматная функция с bq входами и $(bq)^2$ выходами, такая, что $w^{-1}(t) = \overline{x(t - n_1 + 1)x(t - n_1 + 2) \dots x(t)}$ при $t = 0 \bmod n_1$, $w^{-1}(t) = 0$ иначе;

$S(x_1, x_2)$ – автоматная функция, такая, что при $t = 1, \dots, n_1$ $S(x_1, x_2) = x_1$, а при $t > n_1$ $S(x_1, x_2) = x_2$.

Рассмотрим схему (рис. 1) и докажем, что она копирует автомат M^{bq} .

Действительно, пусть $a(0)a(1)a(2)\dots$ – произвольная входная последовательность автомата M^{bq} , $q(0)q(1)\dots$ и $b(0)b(1)b(2)\dots$ – соответствующие последовательность состояний и выходная последовательность. Посмотрим, как преобразует эту входную последовательность построенная схема. Обозначим $a(t) = \overline{a_1(t)a_2(t)\dots a_{bq}(t)}$, $q'(0)q'(1)\dots$, $b'(0)b'(1)\dots$ – последовательность состояний и выходная последовательность автомата M в схеме. В моменты времени $0..bq-1$ на вход автомата M последовательно попадают $a_1(0), a_2(0), \dots, a_{bq}(0)$. Таким образом, $q'(bq) = q(1)$, $b'(i) = b_i(0)$, $i = 1..bq$. По построению функций f, w^{-1}, w_1

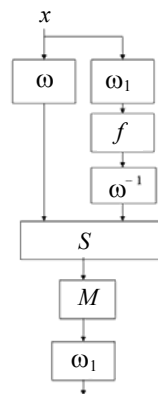
$$\begin{aligned} q'(2bq) &= \varphi(q'(bq), w_1(f(w^{-1}(a(1)a(2)\dots a(bq)))))) = \\ &= \varphi(q'(bq), w_1(f(a(1)a(2)\dots a(bq)))) = \varphi(q'(bq), f(a(1)a(2)\dots a(bq))) = \\ &= \varphi(q(1), a(1)a(2)\dots a(bq)) = q(bq). \end{aligned}$$


Рис. 1. Схема, копирующая автомат M^{bq}

Так как автомат M^{bq} подобен автомату Медведева, любые два состояния автомата M , достижимые словами длины кратной bq , отличимы любым словом длины bq . Таким образом, данная схема копирует автомат, подобный автомату M^{bq} с параметрами $bq, bq, 1$, а значит, по лемме о копировании и утверждению 1 $M^{bq} \in \langle M \rangle$. Лемма доказана.

Определение 3. Пусть $M = (A, Q, B, \varphi, \psi, q_0)$, $M' = (A', Q', B', \varphi', \psi', q'_0)$. M' называется n -подавтоматом M , если $\exists n$, так что $A' \subseteq A^n, Q' \subseteq Q, B' \subseteq B^n$ и $\varphi(A', Q') \subseteq Q'$.

Прямо из леммы 2 следует

Утверждение 2. Пусть b, q – цикловые индексы M , $M' - bq$ – подавтомат M и M' автомат Медведева, тогда $M' \in \langle M \rangle$.

Определение 4. Пусть $M = (A, Q, B, \varphi, \psi, q_0)$, $M' = (A', Q', B', \varphi', \psi', q'_0)$ – автоматы. Скажем, что автомат M' является гомоморфным образом автомата M , если найдутся такие отображения «на» $\chi: Q \rightarrow Q'$, $\eta: A \rightarrow A'$, $\varpi: B \rightarrow B'$, что диаграммы, изображенные ниже, коммутативны.

$$\begin{array}{ccccc} A_1 \times Q_1 & \xrightarrow{\varphi} & Q_1 & A_1 \times Q_1 & \xrightarrow{\psi} & B_1 \\ \eta \downarrow & \chi \downarrow & \chi \downarrow & \eta \downarrow & \chi \downarrow & \varpi \downarrow \\ A_2 \times Q_2 & \xrightarrow{\varphi'} & Q_2 & A_2 \times Q_2 & \xrightarrow{\psi'} & B_2 \end{array}$$

Несложно показать, что

Утверждение 3. Пусть автомат M' является гомоморфным образом автомата M , тогда $M' \in M >$.

Определение 5. Будем говорить, что $M'' | M$, если $\exists n$, $\exists M' - n$ – подавтомат M , так что M'' является гомоморфным образом M' .

Определение 6. Пусть $M = (A, Q, B, \varphi, \psi, q_0)$ – произвольный автомат. Множество подстановок $\{\varphi_a: Q \rightarrow Q \mid a \in A\}$, где $\varphi_a(q) = \varphi(q, a)$, порождает полугруппу подстановок S на множестве Q . Эту полугруппу подстановок будем называть полугруппой автомата M и обозначать S_M .

Определение 7. Будем называть простым автоматом, автомат Медведева с простой группой.

Будем называть автомат M групповым, если S_M – группа.

Лемма 3. Пусть $M = (A, Q, Q, \varphi, \varphi, q_0)$ – групповой неконстантный автомат Медведева, b, q – его цикловые индексы. Тогда $q > 1$.

Доказательство: Докажем утверждение от противного. Предположим, что $q = 1$. Тогда для всех слов $\gamma \in A^b$ период сверхслова $M(\gamma^\infty)$ равен b . Значит, что $\varphi(q_0, \gamma) = q_0$. Так как автомат групповой, то для любого $a \in A$ отображение $\varphi(q, a): Q \rightarrow Q$ – взаимно-однозначное, а значит, $|\varphi(Q, a)| \geq |Q|$. Так как для любого слова длины b отображение $|\varphi(q_0, \gamma)| = 1$, то для любого $a \in A$ $|\varphi(q_0, a)| = 1$, а значит, автомат M – константный, что противоречит условию леммы. Лемма доказана.

Определение 8 [10]. Пусть S – некоторая абстрактная полугруппа с единицей, $|S| = r$ и n – наименьшее целое такое, что $n \geq \log_2 r$. Всякое отображение E_2^n на S будем называть кодированием. Если $\gamma: E_2^n \rightarrow S$ – кодирование, то для всякого элемента $s \in S$ найдется набор $a = (a_1, \dots, a_n) \in E_2^n$, такой, что $\gamma(a) = s$.

Зафиксируем такое кодирование γ и рассмотрим автомат $M = (E_2^n, S, E_2^n, \varphi, \psi)$ с n входами и n выходами, множество состояний которого совпадает с множеством элементов полугруппы S , начальное состояние – единичный элемент $e \in S$, а функция переходов соответствует умножению в полугруппе S

$$\varphi(s, a) = s * \gamma(a).$$

Функция выходов φ определена следующим образом:

$$\varphi(s, a) = \overline{\gamma^{-1}(s)},$$

где $\overline{\gamma^{-1}(s)}$ – произвольный набор из E_2^n , такой, что $\gamma(\overline{\gamma^{-1}(s)}) = s$.

Будем называть построенный автомат *автоматом полу группы* S .

Лемма 4. Пусть M – некоммутативный групповой автомат Медведева, S_M – группа автомата M , M' – автомат группы S_M . Тогда $M' \in \langle M \rangle$, $M \in \langle M' \rangle$.

Доказательство: В [10] показано, что существует r , такое, что любой элемент группы S_M может быть представлен словом длины r . По лемме 3 $q > 1$ и в качестве r можно взять $bq > r$ достаточно большой цикловый индекс автомата M . По лемме 2 $M^{bq} \in M$. Построим теперь по автомату M^{bq} автомат M' .

Так как автомат M^{bq} групповой и содержит всю группу S_M , любое состояние автомата M^{bq} достижимо словом длины bq . Обозначим γ_i – слово, переводящее начальное состояние автомата M^{bq} в состояние q_i .

Пусть d – число состояний автомата M . Рассмотрим схему, изображенную на рис. 2.

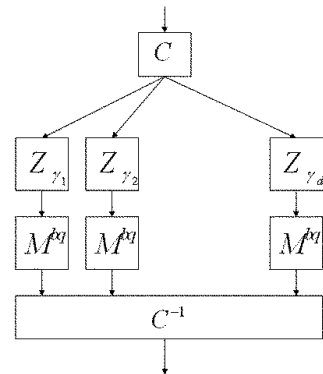


Рис. 2. Схема, выражающая автомат S_M

Здесь $C: S_M \rightarrow E_2^{bq}$ – функция кодирования, отображающая элементы группы S_M в слова во входном алфавите M^{bq} . Z_{γ_i} – задержка, выдающая в первые bq моментов времени γ_i . $C^{-1}: Q^d \rightarrow S_M$ – функция обратного кодирования, отображающая текущий вектор состояний M^{bq} в элемент группы S_M . Построенный автомат является автоматом группы S_M , что и требовалось доказать. Аналогично доказывается включение $M \in \langle M' \rangle$.

Лемма 5. Пусть M – групповой автомат Медведева, $R \subseteq P, |R| < \infty$, тогда $M \in \langle R \rangle \Leftrightarrow$ все простые автоматы, делящие M принадлежат $\langle R \rangle$.

Доказательство леммы 5 Необходимость. Пусть автомат $M \in \langle R \rangle$, докажем, что для произвольного простого P , такого, что $P | M$ $P \in \langle M \rangle \subseteq \langle R \rangle$. Случай

автомата P с коммутативной группой рассмотрен в [7]. Пусть теперь группа автомата P некоммутативна.

По условию делимости $\exists n$, и существует n -подавтомат M , такой, что P является гомоморфным образом этого подавтомата. Как обычно b и q – цикловые индексы автомата M . Докажем, что в качестве n можно взять $n = bq$, тогда утверждение леммы будет следовать из утверждения 2 и утверждения 3.

Для доказательства этого рассмотрим последовательность степеней автомата $M - M, M^2, M^3, \dots, M^i, \dots$. По определению подобия автоматов, найдутся такие p и p_0 , что для любого $j \geq p_0$ $M^j \approx M^{j+p}$. Более того, несложно показать, что для любого $j < p_0$ $M^j - (j+p)$ – подавтомат M .

Покажем, что $p \mid bq$. Для этого покажем, что bq также является периодом последовательности M^i . Действительно, взяв любое слово α длины bq q раз подряд, мы получим тождественную подстановку на некотором множестве состояний автомата M e_α , а значит, такая же тождественная подстановка α' есть и на длине bq . Значит, $\forall \alpha$ $p_{\alpha\alpha'} = p_\alpha$ и $P_{bq} \subseteq P_{2bq}$. Продолжая далее аналогичные рассуждения, получим цепочку $P_{bq} \subseteq P_{2bq} \subseteq \dots \subseteq P_{bq^2}$. Но мы знаем [7], что $P_{bq} = P_{bq^2}$ и таким образом $P_{bq} = P_{2bq} = \dots = P_{bq^2}$ и bq – период последовательности M^i .

Теперь вернемся к доказательству леммы. Как мы только что показали, $\exists i$, что $P \mid M^{bq+i}$. Рассмотрим автомат $M^{bq(bq+i)}$. Используя то же самое отображение, что и при делении A^{bq+i} , мы получим некоторый подавтомат P , так как P – простой автомат, то либо это P , либо константный автомат с одним состоянием. Второй случай невозможен, так как это противоречит некоммутативности P . Таким образом, $P \mid A^{bq(bq+i)} \approx A^{bq}$, и лемма доказана.

Достаточность. Для доказательства воспользуемся полугрупповой теорией автоматов. Пусть $P_1, P_2, \dots, P_n$ – множество простых автоматов, делящих M . $H_1, H_2, \dots, H_n$ – соответствующие простые группы этих автоматов, G – группа автомата M . $P_1', P_2', \dots, P_n'$ – автоматы получившихся простых групп, M' – автомат группы G . По лемме 4 $P_1' \in P_1 >, P_2' \in P_2 >, \dots, P_n' \in P_n >, M \in M' >$.

Докажем, что автомат M' выразим через автоматы $P_1', P_2', \dots, P_n'$, тогда по лемме 4 автомат M будет выразим через автоматы $P_1, P_2, \dots, P_n$. Для этого рассмотрим первый автомат выражающей системы P_1' и представим функцию переходов автомата M' в виде композиции функции переходов автомата P_1' и еще одного группового автомата. Так как $P_1 \mid M$, то H_1 – подгруппа G . Значит, мы можем представить группу G в виде $G = H_1 + H_1c_1 + H_1c_2 + \dots + H_1c_k$, где элементы c_i – представители соответствующих классов смежности. Таким образом, каждый элемент группы G представляется в виде $g = h_1c$.

Если автомат M' находится в состоянии g , а на вход поступает элемент g_1 , то он переходит в новое состояние $g' = gg_1$. Пользуясь разложением состояний на

классы смежности, получаем соотношение $h_1 c' = h_1 c g_1$. Произведем это умножение следующим образом: во-первых, положим $c' = \overline{c g_1}$, где $\bar{x}$ обозначает представитель класса смежности, содержащего элемент x . Тогда получаем равенство $h_1 c' = h_1 c g_1 (\overline{c g_1})^{-1}$. Элемент $c g_1$ принадлежит группе, поэтому может быть переписан в виде $h_1 c$, откуда вытекает соотношение $c g_1 (\overline{c g_1})^{-1} = h_1$. Следовательно, элемент h_1 представляется как произведение элементов, принадлежащих подгруппе H . Процесс нахождения представителя нового смежного класса зависит только от представителя старого смежного класса и входного элемента, благодаря чему его можно изобразить как действие автомата, каждое состояние которого соответствует представителю смежного класса. Этот автомат будем называть начальным. Отображение переходов начального автомата при поступлении входного автомата, принадлежащего группе, соответствует переходу старого смежного класса в новый. Для выполнения приведенного ранее разложения элемента h_1 необходимы выходной элемент из начального автомата, а также элемент h_1 .

Для того, чтобы можно было построить соединение двух введенных автоматов, необходимо разрешить только один вопрос: выходной элемент начального автомата не воспринимается вторым автоматом, в него должен поступать элемент $c g_1 (\overline{c g_1})^{-1}$, который может быть найден с помощью кодирующей функции. Эта кодирующая функция зависит только от текущих элементов c и g_1 . Кодирующая функция представляет собой булеву функцию.

Выходной элемент схемы находится следующим образом: с помощью кодирующей функции из выходных элементов начального и подгруппового автомата формируется их произведение, являющееся элементом группы, затем этот групповой элемент кодируется в выход автомата.

Эквивалентность, имеющаяся между схемой автоматов и первоначальным групповым автоматом, заключается в том, что каждой паре элементов (c, h_1) , являющейся состоянием схемы, соответствует некоторое состояние группового автомата.

Приведенное разложение может быть продолжено. Таким образом возможно построение схемы, элементами которой являются автоматы M_i , а результирующий автомат M' . Лемма доказана.

Лемма 6. Пусть P – простой автомат Медведева, M – произвольный автомат, тогда $P \in M > \Leftrightarrow P | M^{bq}$.

Доказательство Леммы 6 Необходимость: Доказательство слово в слово повторяет доказательство необходимости в лемме 5 с той лишь разницей, что теперь автомат M не автомат Медведева. Но так как автомат P – автомат Медведева и $P | M^{bq}$, то найдется $M' - bq$ подавтомат автомата M , такой, что $P | M'$ и $M' \in M >$ по лемме 2.

Достаточность. Из теоремы Крона – Роудза и того факта, что $P \in M >$ следует, что $S_P | S_M$. Определение делимости для полугрупп следующее $S_1 | S$, если в S найдется подполугруппа S_2 , такая, что S_1 является гомоморфным образом S_2 .

Вообще говоря, из делимости полугрупп не следует делимость соответствующих автоматов. Для доказательства делимости автоматов в случае простого некоммутативного автомата Медведева нам понадобится Лемма 7.

Лемма 7. Пусть $M = (A, Q, B, \varphi, \psi, q_0)$ – произвольный автомат Медведева, (X, S) – простая некоммутативная подгруппа S полугруппы S_M с системой образующих $X = (s_1, \dots, s_k)$. Пусть $\alpha_1, \dots, \alpha_k$ – множество слов в алфавите A , таких, что $\varphi(q, \alpha_i) = s_i(q), i = 1, \dots, k$. Тогда в группе S существует система образующих $X' = (s'_1, \dots, s'_k)$, и множество слов в алфавите A – $\alpha'_1, \dots, \alpha'_k$, такие, что $\varphi(q, \alpha'_i) = s'_i(q), \alpha'_i$ и $l(\alpha'_1) = \dots = l(\alpha'_k)$.

Доказательство. Пусть $l_1 = l(\alpha_1), \dots, l_m = l(\alpha_m)$. Обозначим $d = NOD(l_1, \dots, l_m)$. Пусть $(e_1, \dots)$ – множество слов в алфавите A , таких, что $\varphi(q, e_i) = q, i = 1, \dots$. Обозначим $l(e_i) = d_i$. Обозначим $d_e = NOD(\{d_i\})$. Очевидно, что $d_e = Cd$ для некоторого C . Возможны два случая:

1. $C > 1$.

2. $C = 1$.

1. Пусть $C > 1$. Рассмотрим множество элементов группы S , соответствующее словам длины, кратной Cd в алфавите A . Несложно показать, что это нормальная подгруппа группы S , что возможно только если это единица.

Таким образом, для любого элемента группы S имеем $s^C = e$. В этом случае это циклическая группа порядка C , а значит, не выполнено условие некоммутативности.

2. Пусть $C = 1$. Тогда найдутся два слова в алфавите A (e_1, e_2) , такие, что $\varphi(q, e_1) = \varphi(q, e_2) = q$ и $l(e_1) - l(e_2) = d$. Добавляя e_1 и e_2 к образующим, мы можем выровнять длины образующих элементов, при этом не меняя значений соответствующих элементов группы.

Лемма доказана.

Из леммы 7 и того факта, что $P \mid A$ следует, что существует n – подавтомат A' и отображения «на» $\chi: Q_{A'} \rightarrow Q_P$, $\eta: A_{A'} \rightarrow A_P$, что диаграмма, изображенная ниже, коммутативна

$$\begin{array}{ccc} A_{A'} \times Q_{A'} & \xrightarrow{\varphi} & Q_{A'} \\ \eta \downarrow & \chi \downarrow & \chi \downarrow \\ A_P \times Q_P & \xrightarrow{\varphi'} & Q_P \end{array}$$

Для доказательства делимости осталось показать, что существует отображение «на» $\varpi: B_{A'} \rightarrow B'$, что диаграмма, изображенная ниже, коммутативна

$$\begin{array}{ccc} A_{A'} \times Q_{A'} & \xrightarrow{\psi} & B_{A'} \\ \eta \downarrow & \chi \downarrow & \varpi \downarrow \\ A_P \times Q_P & \xrightarrow{\psi'} & B_P \end{array}$$

Рассмотрим схему, выражающую автомат P , состоящую из автомата M , булевых функций и задержек. Без ограничения общности будем считать, что схема, выражающая P , является суперпозицией двух автоматов M_1 – верхнего и M_2 – нижнего. По теореме Крона – Роудза либо M_1 , либо M_2 имеет гомоморфизм по переходам на автомат P .

Рассмотрим всевозможные случаи. 1. Автомат M_1 состоит из задержек и булевых функций и не имеет гомоморфизма по переходам на P . Тогда M_2 имеет гомоморфизм на P по переходам, а так как выход всей схемы совпадает с выходом P , то существует гомоморфизм и по выходам на P .

Пусть автомат M_1 не является автоматом из задержек и булевых функций. Так как вся схема имеет гомоморфизм по переходам на P , то такой гомоморфизм имеет и M_1 , так как состояние схемы – это пара (состояние M_1 , состояние M_2). Пусть M_2 имеет также гомоморфизм на P . Для дальнейшего доказательства нам понадобится

Лемма 8. Пусть автомат M имеет гомоморфизм по переходам на простой групповой автомат P , тогда существует M' – групповой приведенный подавтомат M , такой, что M' также имеет гомоморфизм на P .

Доказательство. Рассмотрим максимальное подмножество множества состояний Q' автомата M , такое, что $\forall \alpha \in A \quad \varphi(\alpha, Q') = Q'$. Очевидно, выбранное подмножество будет групповым подавтоматом автомата M . Докажем, что этот подавтомат будет иметь гомоморфизм на P . Понятно, что свойство коммутативности по переходам при выделении подавтомата исходного автомата сохраняется. Значит, нужно доказать, что для любого состояния автомата P найдется прообраз в автомате M' . Пусть это не так и существует $p \in Q_P$, так что любое $q \in Q_M$ – прообраз p , q не принадлежит Q' . В этом случае $Q_p \subseteq Q_M$ – прообраз p при гомоморфизме «склеивается» с некоторым другим прообразом при подаче подходящего слова. Так как это выполнено в автомате M , то будет выполнено и в автомате P , что невозможно, так как автомат P – групповой. Лемма доказана.

Лемма 8 позволяет без ограничения общности считать автомат M_1 групповым. Рассмотрим множество слов над входным алфавитом автомата P , которое переводит начальное состояние автомата M_1 в себя. Это множество слов образует нормальную подгруппу в группе автомата P . Так как P – автомат с простой группой, эта нормальная подгруппа является либо всей группой P , либо единичной подгруппой. В первом случае на выбранном множестве слов автомат M_2 работает синхронно с автоматом P , а следовательно, имеет гомоморфизм и по выходам на P . Во втором случае рассмотрим множество слов, переводящих выбранное состояние в некоторое другое состояние в автомате M_1 . Данное множество слов будет образовывать некоторый смежный класс в группе P по единичной подгруппе, а таким образом все множество слов будет образовывать всю группу P . Значит, автомат M_1 в точности автомат P . Так как автомат M_1 групповой, приведенный и имеет гомоморфизм по переходам на P , то он имеет гомоморфизм и по выходам на P .

Пусть теперь M_1 имеет гомоморфизм по переходам на P , а M_2 не имеет такого гомоморфизма. Выделим в автомате M_1 групповой подавтомат стандартным образом. Осуществим процедуру приведения неотличимых состояний автомата M_1 . Если автомат M_1 все еще имеет гомоморфизм на автомат P , то из того, что автомат M_1 групповой, приведенный и имеет гомоморфизм по переходам на автомат P следует, что он имеет гомоморфизм и по выходам на автомат P . Если же автомат M_1 после приведения не имеет гомоморфизма по переходам на P , то мы пришли к противоречию, так как получили из двух автоматов, не имеющих гомоморфизм по переходам на P схемой автомат P , что противоречит теореме Крона – Роудза.

Таким образом, либо P делит M_1 , либо P делит M_2 . Продолжая данную процедуру вглубь схемы, получим на каком-то уровне, что P делит M , так как очевидно, P не делит штрих Шеффера и задержку.

Лемма доказана.

Определение 9. Пусть $M = (A, Q, B, \varphi, \psi, q_0) \in P_a$ – произвольный автомат.

Назовем слово $\alpha \in A^*$ единым тестом для автомата M , если

$$\forall q_1, q_2 \in Q \quad \bar{\psi}(q_1, \alpha) \neq \bar{\psi}(q_2, \alpha).$$

Определение 10. Пусть $\dot{M} = (A, Q, B, \varphi, \psi, q_0)$ – произвольный автомат. Будем говорить, что $M' = (A, Q, Q, \varphi, \psi', q_0)$ – автомат Медведева автомата M , если $\psi'(a, q) = q$.

Утверждение 4. 1. Частный цикловый индекс автомата Z_2 равен 1.

2. Главный цикловый индекс автомата Z_2 равен 2.

3. $|\Theta(< Z_2 >)| = \infty$.

Без доказательства.

Лемма 9. Пусть $M = (A, Q, B, \varphi, \psi, q_0) \in P_a$ – произвольный приведенный групповой автомат. Тогда $\exists k \in N$ такое, что для любого $\alpha \in A^{2^k}$ существует $\alpha' \in A^{2^k}$ – такое, что:

1. $\varphi(\alpha, q) = \varphi(\alpha', q)$ для любого q ;

2. α' – единый тест для автомата M .

Доказательство: Так как у автомата M все состояния отличимы, для любой пары состояний q_i, q_j найдется слово α_{ij} , такое, что $\psi(q_i, \alpha_{ij}) \neq \psi(q_j, \alpha_{ij})$.

Обозначим через α_{ij}^{-1} слово в алфавите A такое, что слово $\varphi(\alpha_{ij} \alpha_{ij}^{-1}, q) = q$ для любого q . Тогда слово $\beta = \alpha_{12} \alpha_{12}^{-1} \alpha_{13} \alpha_{13}^{-1} \dots \alpha_{d-1d} \alpha_{d-1d}^{-1}$, $|Q| = d$ будет отличать любую пару состояний автомата M . Тогда произвольное слово вида $\beta \hat{\beta}$, такое, что $|\beta \hat{\beta}| = 2^k$ также будет отличать все состояния автомата M .

Докажем теперь, что для произвольных α и β ($|\alpha| = 2^k$, $|\beta| = l < 2^k$), существует β' ($|\beta'| = 2^k - l$), такое, что α и $\beta \beta'$ порождают одинаковые подстановки на множестве состояний автомата M или что то же самое – одинаковые элементы группы G автомата M .

Рассмотрим последовательность подмножеств элементов группы G :

$$\begin{aligned} G_1 &= \{\pi_a, a \in A\}, \\ G_2 &= \{\pi_{ab}, a, b \in A\}, \\ &\dots \\ G_k &= \{\pi_{a_1 a_2 \dots a_k}, a_i \in A\}, \\ &\dots \end{aligned}$$

В силу конечности группы G эта последовательность, начиная с некоторого t , периодическая, т. е.

$$\Gamma = \{G_t, G_{t+1}, \dots, G_{t+s}, G_t, \dots\}.$$

Мощности G_i совпадают, так как $|G_i| \leq |G_{i+1}| \leq |G_i|$. Если $|G_i| < |G|$, то G действует на элементах последовательности Γ как циклическая группа порядка s , а следовательно, $G_i \cong G/Z_s$, и G_i не допускает подобного разложения. Таким образом каждый элемент группы G представим в виде $g = zg_i$, где $z \in Z_s, g_i \in G_i$. Так как G_i не допускает дальнейшего разложения, все элементы группы G_i представлены словами длины i .

Пусть теперь у нас есть слово α ($|\alpha| = 2^k$) и β ($|\beta| = l$). Пусть $g_\alpha = z_{s_1} g_1$, $g_\beta = z_{s_2} g_2$, тогда, взяв $\beta' = z_{(s_1 - s_2) \bmod s} g_1^{-1} * g_2^{-1}$, получим необходимый элемент группы. Лемма доказана.

Лемма 10. Пусть $M \in P_a$ – произвольный групповой автомат. M' – его автомат Медведева. Тогда

1. $M' \in \langle M, Z_2 \rangle$;
2. $M \in \langle M', Z_2 \rangle$.

Доказательство: Доказательство пункта 2 элементарно, достаточно «навесить» на выход автомата Медведева функции выходов, реализуемые в состояниях автомата M и соединить с ними вход автомата M' .

Для доказательства пункта 2 воспользуемся леммой 5 и покажем, что все простые автоматы, делящие M' , выразимы через M .

Из леммы 2 и леммы 9 несложно показать, что подавтомат Медведева автомата M^{2^k} для достаточно большого k выразим через $\langle M \rangle$, поэтому достаточно показать, что простые автоматы выразимы через M^{2^k} для достаточно большого k .

Простые автоматы делятся на три типа:

- а) коммутативные константные автоматы;
- б) коммутативные неконстантные автоматы;
- в) некоммутирующие автоматы с простыми группами.

Пусть константный автомат K_s делит автомат M' . Возможны два случая: s делит 2^k и s не делит 2^k . В первом случае очевидно: константный автомат выразим. Во втором случае автомат K_s не является делителем автомата M'' для $s \mid l$, но так как s не делит 2^k , а автоматы Медведева M^{2^k} и M'^{2^k} совпадают по лемме 9, то $K_s \mid M^{2^k}$ и по лемме 6 автомат K_s выразим через M^{2^k} .

Пункты «б» и «в» непосредственно следуют из леммы 6, а также из того факта, что если неконстантный простой автомат делит автомат Медведева, то он делит и все степени этого автомата. Так как автоматы M'^{2^k} и M^{2^k} подобны, то простые автоматы, делящие M'^{2^k} , делят и автомат M^{2^k} . Лемма доказана.

Доказательство теоремы 2 непосредственно следует из леммы 10 и теоремы 1, так как для выразимости произвольного группового автомата достаточно проверить выразимость его автомата Медведева.

Теорема 3 прямо следует из теоремы 1, а также факта, показанного Кроном и Роудзом [9] в работе $\langle R \rangle \supseteq P_a^n$ тогда и только тогда, когда $\langle R \rangle \ni T$ и $\langle R \rangle$ содержит все специальные автоматы с простыми группами. Так как первое свойство по условию выполнено, а второе проверяемо по теореме 1, то верна и теорема 3.

Автор выражает благодарность проф. Д. Н. Бабину за ценные замечания и внимание к работе.

Библиографические ссылки

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. – М. : Наука. Гл. ред. физ.-мат. лит., 1985. – 320 с.
2. Бабин Д. Н. О полноте двухместных автоматных функций относительно суперпозиции // Дискрет. математика. – 1989. – Т. 1, вып. 4. – С. 423–431. – URL: <http://rc.dgu.ru/res/mat/intsys.msu.ru/staff/babin/gilbert.pdf> (дата обращения: 17.05.2012).
3. Кратко М. И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // Докл. АН СССР. – 1964. – Т. 155, № 1. – С. 35–37.
4. Летуновский А. А. О выразимости константных автоматов // Интеллектуал. системы. – 2005. – Т. 9, вып. 1–4. – С. 457–469. – URL: <http://intsys.msu.ru/magazine/archive/v9%281-4%29/letunovskiy-457-468.pdf> (дата обращения: 17.05.2012).
5. Бабин Д. Н. О классификации автоматных базисов Поста по разрешимости свойств полноты и А-полноты // Докл. Акад. наук. – 1999. – Т. 367, № 4. – С. 439–441.
6. Мальцев А. И. Итеративные алгебры и многообразие Поста // Алгебра и логика. – 1966. – Т. 5, № 2. – С. 5–24.
7. Летуновский А. А. О выразимости суперпозициями автоматов с разрешимыми группами (в печати).
8. Летуновский А. А. О выразимости константных автоматов суперпозициями // Интеллектуал. системы. – 2009. – Т. 13, вып. 1–4. – С. 397–406. – URL: <http://intsys.msu.ru/magazine/archive/v13%281-4%29/letunovskiy-397-406.pdf> (дата обращения: 17.05.2012).
9. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. – 3-е изд., перераб. и доп. – М. : Наука, 1982. – 288 с. – URL: <http://depositfiles.com/files/a8dtsfceb> (дата обращения: 17.05.2012).
10. Алгебраическая теория автоматов, языков и полугрупп / под ред. М. А. Арбиба ; пер. с англ. Н. И. Осетинского. – М. : Статистика, 1975. – 336 с. – URL: <http://bookfi.org/dl/437779/03ddc1> (дата обращения: 17.05.2012).
11. Алешин С. В. Об одном следствии теоремы Крона – Роудза // Дискрет. математика. – 1999. – Т. 11, вып. 4. – С. 101–109.

A. A. Letunovskiy, Programming Engineer, LSI International Research LLC, Moscow

Problem of automata expressability realtive to superposition for systems with fixed additive

The paper considers expressibility problem of finite group Medvedev automaton M relative to superposition of systems $\Phi \cup R$, where Φ consists of all Boolean functions and delay, R is the arbitrary finite system of automata. The author showed previously, that there is the testing algorithm $M \in [\Phi \cup R]$ for group Medvedev automaton M with the solvable group. The present paper is devoted to solution of expressibility problem relative to system $\Phi \cup R$ of arbitrary group automata.

Keywords: finite automaton, expressibility, algorithm, group

Получено: 10.05.12

УДК 531.8+692.522.3

С. И. Сачкова, аспирант;

А. Э. Пушкарев, доктор технических наук, профессор

Ижевский государственный технический университет имени М. Т. Калашникова

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КОЛЕБАНИЙ КАРКАСНЫХ СТРОИТЕЛЬНЫХ КОНСТРУКЦИЙ ПРИ ВОЗДЕЙСТВИИ ДВУХ ИСТОЧНИКОВ ВИБРАЦИИ

Рассмотрено влияние двух источников вибрации на новые строительные конструкции из термоструктурных панелей. Выявлено, что собственные частоты панелей близки к частотам бытовых машин, насосов и вентиляторов, а динамические прогибы панелей могут превышать допустимые значения.

Ключевые слова: колебания, строительные конструкции, термоструктурные панели

В последнее время нередко случаи разрушения зданий, сооружений и их конструктивных элементов из-за воздействия внешних и внутренних техногенных факторов, в большинстве случаев связанных с вибрацией. Шум и вибрации сопровождают человека не только на производстве, но и в быту, что приводит к негативным последствиям, начиная от утомления и снижения работоспособности и кончая разрушениями и человеческими жертвами. Чем больше источников вибрации, тем интенсивнее их негативное воздействие. Наряду с возникновением технических новшеств, появляются инновации и в области строительных материалов и конструкций, здания из которых в будущем будут эксплуатироваться в условиях предельной автоматизации быта, т. е. совместного действия многих приборов, что часто не принимается во внимание при проектировании новых зданий. Одна из все более широко применяемых современных строительных конструкций – это конструкции из термоструктурных панелей, состоящих из несущих металлических профилей, монолитно связанных с внутренним заполнением из теплоизоляционного материала.

Для изучения динамического воздействия вибрации на конструкции из термоструктурных панелей необходимо определить их собственную частоту и коэффициент затухания колебаний.