Math-Net.Ru

Общероссийский математический портал

А. В. Бабаш, О свойствах специальной композиции автоматов, *Дискрет. матем.*, 2003, том 15, выпуск 3, 66–75

DOI: <https://doi.org/10.4213/dm206>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.209.52.79

26 апреля 2023 г., 13:34:18

О свойствах специальной композиции автоматов

© 2003 г. А. В. Бабаш

Предлагаются способы построения моделей конечного автомата — новые автоматы, получаемые с помощью степеней исходного автомата и задания дополнительных функций на его выходных словах. Приложения результатов связываются с задачей определения состояния автомата по его входным и соответствующим выходным последовательностям.

1. Введение

В работе изучаются возможности построения для исследуемого автомата A его моделей-следствий, то есть новых автоматов, уравнения функционирования которых являются следствиями уравнений функционирования исходного автомата. Эти модели-следствия будут называться далее образами автомата A . Целью построения таких образов для A является разработка методов определения состояния автомата по его входным и соответствующим выходным последовательностям. С этой целью ниже исследуется вопрос получения моделей, являющихся неприведенными автоматами, приведенные формы которых имеют меньшее число состояний, чем у автомата A . Основные результаты работы были сформулированы в тезисах Второго Всероссийского симпозиума по прикладной и промышленной математике [1].

Будем использовать следующие обозначения:

$A = (X, S, Y, h, f)$ — конечный автомат с входным алфавитом X , множеством состояний S , $|S| \geq 2$, выходным алфавитом Y , функциями перехода h и выхода f ,

$$h: S \times X \rightarrow S, \quad f: S \times X \rightarrow Y;$$

$(h_x)_{x \in X}$ — частичные функции переходов автомата, $h_x: S \rightarrow S$, $h_x s = h(s, x)$ для $s \in S$, $x \in X$;

$(f_x)_{x \in X}$ — частичные функции выхода автомата, $f_x: S \rightarrow Y$, $f_x s = f(s, x)$ для $s \in S$, $x \in X$;

X^* — множество всех слов конечной длины алфавита X ;

$A(s, P)$ — выходное слово автомата A , соответствующее входному слову $P \in X^*$ и начальному состоянию $s \in S$;

$h(s, x(1), x(2), \dots, x(k))$ — заключительное состояние автомата при его начальном состоянии $s \in S$ и входном слове $(x(1), x(2), \dots, x(k)) \in X^k$;

$h_x(Z)$ — образ множества Z , $Z \subseteq S$, при отображении h_x ;

$|Z|$ — мощность множества Z .

Для автомата $A = (X, S, Y, h, f)$ в ряде случаев для удобства мы используем и обозначение $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$. Напомним основные необходимые нам понятия теории автоматов (см., например, [2, 3]).

Состояния s, s' автомата A называются k -неотличимыми, если

$$A(s, P) = A(s', P)$$

при любом входном слове $P \in X^k$. Состояния s, s' автомата A называются неотличимыми, если они k -неотличимы при любом k .

Аналогично вводится понятие неотличимости состояний s, s' автоматов

$$A = (X, S, Y, h, f), \quad A' = (X, S', Y, h', f').$$

Автоматы A, A' считаются неотличимыми, если для любого состояния $s \in S$ автомата A найдется неотличимое от него состояние $s' \in S'$ автомата A' и наоборот.

Автомат A называется приведенным, если он не имеет различных неотличимых состояний. Приведенной формой (с точностью до изоморфизма) автомата A называют любой неотличимый от него приведенный автомат.

Степенью различимости автомата A называется минимальное число $d = d(A)$, при котором для любых $s, s' \in S$ из равенств $A(s, P) = A(s', P)$ для всех $P \in X^d$ следуют равенства $A(s, P') = A(s', P')$ для всех $P' \in X^*$.

Полугруппой автомата A называют подгруппу преобразований $G = \langle (h_x)_{x \in X} \rangle$ множества S , порожденную частичными функциями переходов $(h_x)_{x \in X}$ автомата A .

Автомат A называют перестановочными, если $(h_x)_{x \in X}$ — биекции S в S .

Автомат A называют автоматом Медведева, если $f_x s = s$ при любых $s \in S, x \in X$, то есть выходной последовательностью автомата является его последовательность состояний. Для таких автоматов мы используем специальные обозначения $A(M) = (X, S, Y, h)$ или $A(M) = (X, S, Y, (h_x)_{x \in X})$.

Диагностической последовательностью автомата A называют последовательность $P \in X^*$, при которой $A(s, P) \neq A(s', P)$ при любых различных $s, s' \in S$. Автомат называют диагностируемым, если для него существует диагностическая последовательность.

2. Построение моделей-следствий автомата

Пусть $A = (X, S, Y, h, f)$ — конечный автомат. Под обработкой степени k будем понимать произвольное отображение $\Phi: X^k \times Y^k \rightarrow Y'$, где Y' — некоторый алфавит. Образом автомата A при обработке Φ назовем автомат $A_\Phi = (X^k, S, Y', h_\Phi, f_\Phi)$ с функциями перехода

$$h_\Phi(s, x(1), x(2), \dots, x(k)) = h(s, x(1), x(2), \dots, x(k)) = h_{x(k)} h_{x(k-1)} \dots h_{x(1)} s$$

и выхода

$$f_\Phi(s, x(1), x(2), \dots, x(k)) = \Phi(x(1), x(2), \dots, x(k), A(s, x(1), x(2), \dots, x(k))),$$

Рис. 1.

где $s \in S$, $(x(1), x(2), \dots, x(k))$ — входной символ A_Φ , $(x(1), x(2), \dots, x(k)) \in X^k$.

Указанный автомат A_Φ обладает следующим свойством. Если при входной последовательности

$$x(1), x(2), \dots, x(Lk) = P(1), P(2), \dots, P(L),$$

где $P(j) = x((j-1)k+1), \dots, x(jk)$, $j \in \{1, \dots, L\}$, и начальном состоянии $s \in S$ выходная последовательность автомата A есть

$$A(s, x(1), x(2), \dots, x(Lk)) = y_1, y_2, \dots, y_{Lk} = Y_1, Y_2, \dots, Y_L,$$

то выходная последовательность автомата A_Φ , соответствующая входной последовательности $P(1), P(2), \dots, P(L)$ и начальному состоянию $s \in S$, определяется равенством

$$A_\Phi(s, P(1), P(2), \dots, P(L)) = \Phi_{P(1)}(Y_1), \Phi_{P(2)}(Y_2), \dots, \Phi_{P(L)}(Y_L),$$

где

$$\Phi_{P(j)}(Y_j) = \Phi(P(j), Y_j), \quad Y_j = y_{(j-1)k+1}, \dots, y_{jk}, \quad j \in \{1, \dots, L\}.$$

Таким образом, функционирование автомата A_Φ представимо схемой, данной на рис. 1, где $H(k)$ — проходной накопитель на k пар знаков (x, y) , $S(k)$ — узел выборки шага k .

Определение 1. Автомат A называется слабо неприведенным автоматом, если для него существует обработка Φ , при которой его образ A_Φ является неприведенным автоматом с числом классов неотличимых состояний, большим единицы. В противном случае, автомат A называется сильно приведенным.

Очевидно следующее утверждение.

Предложение 1. Для автомата A тогда и только тогда найдется обработка $\Phi: X^k \times Y^k \rightarrow Y'$, при которой автомат A_Φ имеет гомоморфный приведенный образ с числом состояний $|S'|$, $2 \leq |S'| \leq |S| - 1$, когда автомат A слабо неприведен.

Ниже дается описание слабо неприведенных и сильно приведенных автоматов. Введем дополнительные понятия и обозначения.

Для произвольного автомата $A = (X, S, Y, h, f)$ разбиение $P(S)$ множества S

$$P(S) = \{Z_j: j \in \{1, \dots, t\}\}, \quad 2 \leq t \leq |S| - 1, \quad Z_j \cap Z_{j'} = \emptyset, \quad j \neq j', \quad j, j' \in \{1, \dots, t\},$$

назовем системой блоков импримитивности автомата A , или же системой блоков импримитивности полугруппы $G = \langle (h_x)_{x \in X} \rangle$ автомата A , если для любого $x \in X$ и любого $j \in \{1, \dots, t\}$ существует $j' \in \{1, \dots, t\}$, при котором $h_x(Z_j) \subseteq Z_{j'}$. Будем называть A примитивным автоматом, если он не обладает системой блоков импримитивности, в противном случае, назовем A импримитивным автоматом. Соответственно полугруппу автомата A назовем примитивной и импримитивной. Заметим, что введенные понятия корректны и для автоматов без выходов, в связи с чем они будут использоваться и для автоматов этого класса.

В дальнейшем в работе рассматриваются такие автоматы, у которых число состояний больше единицы и не все частичные функции выхода постоянны на всем множестве состояний.

Очевидно следующее утверждение.

Предложение 2. *Любой неприведенный автомат является и слабо неприведенным автоматом.*

Для автомата $A = (X, S, Y, h, f)$ и произвольного натурального числа n через $A^n(M)$ обозначим автомат Медведева

$$A^n(M) = (X^n, S, (h_p : P \in X^n)),$$

где $h_p = h_{x(n)}h_{x(n-1)} \dots h_{x(1)}$, $P = (x(n), x(n-1), \dots, x(1)) \in X^n$. При $n = 1$

$$A^1(M) = A(M) = (X, S, Y, (h_x)_{x \in X}).$$

Ниже будет использоваться следующее очевидное утверждение.

Лемма 1. *Если автомат A слабо неприведен, то существует натуральное число n , при котором автомат $A^n(M)$ импримитивен.*

Очевидно, что в качестве n в лемме можно взять k , при котором образ автомата A при обработке степени k является слабо неприведенным автоматом.

Ниже мы сужаем класс исследуемых автоматов до класса диагностируемых автоматов. Заметим, что в этот класс входят перестановочные автоматы. Полное описание слабо неприведенных диагностируемых автоматов дает следующая теорема.

Теорема 1. *Приведенный диагностируемый автомат A слабо неприведен тогда и только тогда, когда существует натуральное число n , при котором автомат Медведева $A^n(M)$ импримитивен.*

Доказательство. Необходимость условий теоремы следует из леммы 1. Докажем достаточность этих условий. Предположим сначала, что при $n = 1$ для автомата A выполнены условия теоремы. Обозначим $Z_1, Z_2, \dots, Z_t$ некоторую систему его блоков импримитивности. Выберем произвольное натуральное число k , не меньшее минимальной длины $K(A)$ диагностической последовательности автомата A , положим $Y' = \{1, 2, \dots, t\}$, отображение $\Phi: X^k \times Y^k \rightarrow Y'$ зададим с помощью функций $\Phi_P: Y^k \rightarrow Y'$, $P \in X^k$, следующим образом.

1. Для произвольного $P \in X^k$ на блоках $Z_1, Z_2, \dots, Z_t$ системы импримитивности автомата A введем бинарное отношение σ_P . Блоки Z, Z' находятся в отношении σ_P (в этом случае пишут $Z\sigma_P Z'$) тогда и только тогда, когда существуют состояния $s \in Z, s' \in Z'$, для которых $A(s, P) = A(s', P)$. Пусть σ_P^* — транзитивное замыкание этого бинарного

отношения на $\{Z_1, Z_2, \dots, Z_t\}$. Для каждого класса эквивалентности $Z^\wedge$ бинарного отношения эквивалентности σ_P^* определим минимальный номер блока из $\{Z_1, Z_2, \dots, Z_t\}$, принадлежащий классу $Z^\wedge$.

2. Пронумеруем этими номерами $\{j(1), j(2), \dots, j(t(P))\}$ классы отношения эквивалентности σ_P^* . Пусть $\{Z_{j(1)}^\wedge, Z_{j(2)}^\wedge, \dots, Z_{j(t(P))}^\wedge\}$ — классы эквивалентности отношения σ_P^* .

3. Для $s \in Z_j, Z_j \in Z_{j(v)}^\wedge$ положим

$$\Phi_P(A(s, P)) = j(v).$$

Таким образом, мы пока задали значения отображения Φ на всех парах вида

$$(P, A(s, P), \quad s \in S, \quad P \in X^k).$$

На парах $(P, Y_j) \in X^k \times Y^k$, не входящих в указанное множество пар, значение Φ выбираем произвольным образом. Ясно, что частичные функции выходов автомата A_Φ , являющегося образом автомата A при обработке Φ , постоянны на блоках $\{Z_1, Z_2, \dots, Z_t\}$ системы импримитивности автомата A . Заметим, что эти блоки в то же время являются блоками системы импримитивности автомата A_Φ , и для завершения доказательства теоремы в рассматриваемом частном случае $n = 1$ остается показать, что не все частичные функции выходов автомата A постоянны на множестве его состояний.

В силу диагностируемости приведенного автомата A для него существует диагностическая последовательность $\mathcal{P}$ длины $K(A) \leq k$. Рассмотрим фиксированную последовательность $\mathcal{P}$ длины k , начальное слово которой есть $\mathcal{P}$. Тогда выходные последовательности $(A(s, \mathcal{P}P : s \in S))$ автомата A попарно различны и по построению отношения эквивалентности $\sigma_{\mathcal{P}P}^*$ — классы этого отношения есть $Z_1, Z_2, \dots, Z_t$, то есть совпадают с блоками импримитивности автомата A_Φ и $\Phi(\mathcal{P}P, A(s, \mathcal{P}P) = j$, если $s \in Z_j, j \in \{1, \dots, t\}$. Следовательно, частичная функция выходов $f_{\Phi, \mathcal{P}P}$ автомата A_Φ не постоянна на S .

Рассмотрим теперь случай, когда n — произвольное натуральное число и автомат $A^n(M)$ импримитивен. Введем вспомогательный автомат

$$A^n = (X^n, S, Y^n, (h_P : P \in X^n), (f_P : P \in X^n))$$

с частичными функциями переходов

$$h_P = h_{x(n)}h_{x(n-1)} \dots, h_{x(1)}$$

при $P = (x(n), x(n-1), \dots, x(1)) \in X^n$ и частичными функциями выходов

$$f_P = f_{x(1)}s, f_{x(2)}h_{x(1)}s, \dots, f_{x(n)}h_{x(n-1)} \dots h_{x(1)}s, \quad s \in S.$$

Автомат A^n отличается от $A^n(M)$ наличием функций выхода. Выходная последовательность автомата $A^n(M)$ представляет собой последовательность n -грамм выходной последовательности автомата A .

Так как по условию автомат $A^n(M)$ импримитивен, импримитивен и автомат A^n , при этом он, очевидно, так же как и A , является диагностируемым автоматом. По доказанному ранее частному случаю, для автомата A^n найдется обработка

$$\Phi' : (X^n)^k \times (Y^n)^k \rightarrow Y'$$

некоторой степени k , при которой образ A_{Φ}^n автомата A^n является неприведенным автоматом с числом классов неотличимых состояний, большим единицы. Автомат $A_{\Phi'}^n$ имеет вид

$$A_{\Phi'}^n = (X^{kn}, S, Y', h'_{\Phi'}, f'_{\Phi'}).$$

Очевидно, функцию Φ' , определенную на словах длины k алфавита X^n , можно трактовать и как функцию Φ , определенную на словах длины kn алфавита X , принимающую те же значения, что и Φ' . Непосредственно проверяется, что образ A_{Φ} автомата A при обработке $\Phi: X^{nk} \times Y^{nk} \rightarrow Y'$ совпадает с автоматом $A_{\Phi'}^n$, и следовательно, автомат A слабо неприведен. Теорема доказана.

Таким образом, для диагностируемых автоматов задача описания слабо неприведенных или сильно приведенных автоматов сводится к проверке импримитивности или примитивности степеней $A^n(M)$, $n \in \{1, 2, \dots\}$, автомата A .

3. Изучение примитивности степеней автомата

Предварительно введем необходимые обозначения. Для полугруппы $G = \langle (h_x)_{x \in X} \rangle$ автомата

$$A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X}),$$

порожденной частичными функциями переходов $(h_x)_{x \in X}$, рассмотрим граф $\Gamma(G)$ — граф полугруппы G . Вершинами графа являются элементы $g \in G$. Из вершины g проводится ориентированная дуга в вершину g' с меткой $x \in X$ тогда и только тогда, когда $gh_x = g'$. Под элементарным контуром графа $\Gamma(G)$ будем понимать путь из некоторой выбранной вершины в эту вершину, не содержащий одинаковых вершин. Обозначим через D наименьшее общее кратное длин элементарных контуров. Через M_k обозначим k -й слой полугруппы $G = \langle (h_x)_{x \in X} \rangle$, то есть множество всех ее элементов, представимых положительными словами $h_{x(k)}h_{x(k-1)} \dots h_{x(1)}$ длины k из образующих $\langle (h_x)_{x \in X} \rangle$. Если G содержит тождественное преобразование S , то она представима в виде $G = G' \cup G''$, где G' — подполугруппа полугруппы G , не содержащая биективных отображений S в S , а G'' — подполугруппа G , состоящая из всех биективных отображений полугруппы G . Через $d(G'')$ будем обозначать ширину группы G'' , то есть минимальное число ее слоев, объединение которых дает G'' . Для полугруппы G с единицей через $L(G)$ обозначим минимальное натуральное число L , при котором $|M_L| = |M_{L+1}|$.

Теорема 2. *Справедливы следующие утверждения.*

- (1) При любом натуральном j

$$M_{|G|+j} \subseteq M_{|G|+j+D}.$$

- (2) Последовательность множеств $M_1, M_2, \dots, M_k, \dots$ смешанно периодическая с длиной подхода, не превышающей величины $|G| + L^*D$, где L^* — минимальное неотрицательное целое число, для которого $M_{|G|+L^*D+1} = M_{|G|+L^*D+1+D}$, период D' данной последовательности является делителем величины D .

- (3) Найдется натуральное число $h(G)$ такое, что

$$|G| + L^*D + 1 \leq h(G) \leq |G| + L^*D + D',$$

при котором слой $M_{h(G)}$ является подполугруппой полугруппы G , и кроме того,

$$M_{h(G)} = \bigcap_{h=1}^{\infty} G_h,$$

где G_h — полугруппа автомата $A^h(M) = ((X^h, S, Y^h, (h_P : P \in X^h)))$.

- (4) Если полугруппа G содержит тождественное преобразование S , то последовательность $M_1, M_2, \dots, M_k, \dots$ смешанно периодическая с длиной подхода $L(G) - 1$ и периодом $d(G'')$, найдется натуральное число $h(G)$ такое, что

$$L(G) \leq h(G) \leq L(G) + d(G') - 1,$$

при котором $M_{h(G)}$ является полугруппой и

$$G_{d(G'')} = M_{h(G)} = \bigcap_{h=1}^{\infty} G_h.$$

Доказательство. Рассмотрим произвольный элемент g из $M_{|G|+j}$, $j \in \{1, 2, \dots\}$. Он может быть представлен в виде $g = h_{x(1)}h_{x(2)} \dots h_{x(|G|+j)}$ при некоторых $x(k) \in X$, $k \in \{1, 2, \dots, |G| + j\}$. Тогда в графе $\Gamma(G)$ имеется путь вида

$$h_{x(1)} \rightarrow_{x(2)} h_{x(1)}h_{x(2)} \rightarrow_{x(3)} \dots \rightarrow_{x(|G|+j)} h_{x(1)}h_{x(2)} \dots h_{x(|G|+j)}.$$

Так как число вершин этого пути больше $|G|$, он содержит хотя бы один элементарный контур. Пусть этот контур имеет вид

$$h_{x(1)}h_{x(2)} \dots h_{x(k)} \rightarrow_{x(k+1)} h_{x(1)}h_{x(2)} \dots h_{x(k+1)} \rightarrow_{x(k+2)} \dots \rightarrow_{x(k+p)} h_{x(1)}h_{x(2)} \dots h_{x(k+p)},$$

где $h_{x(1)}h_{x(2)} \dots h_{x(k)} = h_{x(1)}h_{x(2)} \dots h_{x(k+p)}$. Элемент g можно представить положительным словом длины $|G| + j + D$ вида

$$h_{x(1)}h_{x(2)} \dots h_{x(k)}(h_{x(k+1)} \dots h_{x(k+p)})^{c+1}h_{x(k+p+1)} \dots h_{x(|G|+j)},$$

где $c = D/p$, следовательно, $g \in M_{|G|+j+D}$. Таким образом, $M_{|G|+j} \subseteq M_{|G|+j+D}$ при любом натуральном j . Следовательно,

$$M_{|G|+1} \subseteq M_{|G|+1+D} \subseteq \dots \subseteq M_{|G|+1+kD}, \quad k \in \{1, 2, \dots\}.$$

По определению величины L^*

$$M_{|G|+L^*D+1} = M_{|G|+L^*D+1+D}.$$

Используя эти соотношения, проверяем справедливость равенств

$$M_{|G|+L^*D+1} = M_{|G|+L^*D+1+kD}, \quad k \in \{0, 1, \dots\}.$$

Отсюда,

$$M_{|G|+L^*D+1+j} = M_{|G|+L^*D+1+j+kD}, \quad j, k \in \{0, 1, \dots\}.$$

Таким образом, доказано утверждение 2 теоремы.

Определим натуральное число $h(G)$, исходя из условий, что

$$|G| + L^* + 1 \leq h(G) \leq |G| + L^* D + D$$

и $h(G)$ кратно D' . Тогда очевидно, что $M_{h(G)} M_{h(G)} = M_{h(G)+h(G)} = M_{h(G)}$ (здесь $M_{h(G)} M_{h(G)}$ — произведение множеств подстановок). Следовательно, $M_{h(G)}$ — полугруппа и

$$G_{h(G)} = M_{h(G)}, \quad M_{h(G)} \supseteq \bigcap_{h=1}^{\infty} G_h, \quad G_h \supseteq G_{kh}, \quad k \in \{1, 2, \dots\}.$$

В частности, при $k(0)h \geq h(G)$ и $k(0)h$ кратном D' , $k(0) \in \{1, 2, \dots\}$, справедливо включение $G_h \supseteq M_{k(0)h}$ и $M_{k(0)h} = M_{h(G)}$, откуда получаем, что

$$M_{h(G)} = \bigcap_{h=1}^{\infty} G_h.$$

Перейдем к доказательству утверждения 4 теоремы. Если полугруппа G содержит тождественное преобразование S , то среди ее образующих $(h_x)_{x \in X}$ найдется биективное отображение $h(0): S \rightarrow S$, в связи с чем

$$|M_1| \leq |M_2| \leq \dots \leq |M_j| \leq \dots$$

Через $h_x M_{L(G)}$ обозначим множество $\{h_x m: m \in M_{L(G)}\}$, аналогично положим $M_{L(G)} h_x = \{m h_x: m \in M_{L(G)}\}$. Из определения параметра $L(G)$ вытекает, что $|M_{L(G)}| = |M_{L(G)} + 1|$, откуда

$$M_{L(G)+1} = \bigcup_{x \in X} M_{L(G)} h_x = \bigcup_{x \in X} h_x M_{L(G)} = h(0) M_{L(G)} = M_{L(G)} h(0),$$

$$M_{L(G)+j} = (h(0))^j M_{L(G)} = M_{L(G)} (h(0))^j, \quad j \in \{0, 1, \dots\}.$$

Следовательно, длина подхода рассматриваемой последовательности $M_1, M_2, \dots$ равна $L(G) - 1$, а ее период D' делит порядок подстановки $h(0)$.

Обозначим через $d = d(g'')$ ширину подгруппы G'' полугруппы G . Напомним, что шириной группы в фиксированных образующих называют минимальное количество слоев, покрывающих ее как множество. Известно, что, во-первых, ширина группы совпадает с периодом ее слоев, и, во-вторых, ширина группы совпадает с общим наибольшим делителем длин положительных определяющих слов (соотношений) группы. В силу последнего факта найдется натуральное число $k(0)$, при котором

$$k(0)d \geq L(G), \quad E \in M_{k(0)d}, \quad E \in M_{k(0)d+d},$$

где E — единица группы G'' . Тогда при любом $j \in \{0, 1, \dots\}$

$$M_{k(0)d+j} M_{k(0)d} = M_{k(0)d+j+k(0)d} = M_{k(0)d+j},$$

$$M_{k(0)d+j} M_{k(0)d+d} = M_{k(0)d+j+k(0)d+d} = M_{k(0)d+j}.$$

Следовательно, период D' рассматриваемой последовательности слоев делит величины $k(0)d$ и $(k(0) + 1)d$, и, таким образом, D' является делителем ширины d группы G'' .

Каждый слой M_j , $j \in \{1, 2, \dots\}$, полугруппы G можно представить в виде $M_j = M'_j \cup M''_j$, где M''_j — j -й слой подгруппы G'' полугруппы G , а M'_j — j -й слой подполугруппы G' полугруппы G . Ранее отмечалось, что период слоев группы совпадает с ее шириной. Поэтому период последовательности $M'_1, M''_2, \dots$ есть d . Учитывая, что D' должно делить d , а ранее было показано, что d делит D' , заключаем, что $D' = d$.

Определим натуральное число $h(0) = H(G)$, исходя из условий, что

$$L(G) \leq h(0) \leq L(G) + d - 1$$

и $E \in M_{h(0)}$. Очевидно, что $M_{h(0)}$ — полугруппа и $M_j \subseteq M_{h(0)+j}$, $j \in \{1, 2, \dots\}$. Поэтому

$$G_d = M_{h(0)} = \bigcap_{h=1}^{\infty} G_h.$$

Доказательство теоремы завершено.

Следствие 1. *Приведенный диагностируемый автомат*

$$A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$$

сильно приведен тогда и только тогда, когда примитивна полугруппа

$$G_d = M_{h(0)} = \bigcap_{h=1}^{\infty} G_h.$$

Для формулировки критерия сильной приведенности перестановочного автомата $A(M) = (X, S, Y, (h_x)_{x \in X})$ в терминах импримитивности групп автоматов, являющихся его степенями, приведем ряд следствий из теоремы 2 и ее доказательства. Данные результаты по описанию последовательности слоев $M_1, M_2, \dots$ группы $G = \langle (h_x)_{x \in X} \rangle$ получены ранее М. М. Глуховым в [4]. Подчеркнем, что импримитивность автомата, импримитивность его группы или его подгруппы G_n мы здесь трактуем в расширенном смысле, не требуя транзитивности рассматриваемых групп.

Пусть d — ширина группы $G = \langle (h_x)_{x \in X} \rangle$, заданной системой образующих элементов $\langle (h_x)_{x \in X} \rangle$ и некоторой системой положительных определяющих слов (соотношений) и $G_n = \langle (h_p : P \in X^n) \rangle$ — подгруппа группы G , порожденная всеми возможными положительными словами $h_{x(n)} h_{x(n-1)} \dots h_1$ длины n . Тогда найдется $n(0)$, при котором

$$G_d = M_{n(0)} = \bigcap_{n=1}^{\infty} G_n,$$

группа G_d — нормальный делитель группы G , по которому образующие $(h_x)_{x \in X}$ лежат в одном классе смежности G по G_d , причем фактор группа G/G_d циклическая порядка d . Любая группа $G_n = \langle (h_p : P \in X^n) \rangle$ является нормальным делителем группы G , по которой образующие $\langle (h_x)_{x \in X} \rangle$ лежат в одном классе смежности по G_n , при $(n, d) = d'$ группа G_n совпадает с группой $G_{d'}$, фактор группа G/G_n циклическая порядка d' . Используем это утверждение для решения нашей задачи. Если существует n , при котором группа $G_n = \langle (h_p : P \in X^n) \rangle$ импримитивна, то из представления

$$G_d = M_{n(0)} = \bigcap_{n=1}^{\infty} G_n$$

следует, что импримитивна и группа G_d . Если не существует n , при котором группа $G_n = \langle (h_p : P \in X^n) \rangle$ импримитивна, то G_d примитивна. Из примитивности G_d вытекает примитивность всех групп G_n , $n \in \{1, 2, \dots\}$. Следовательно (см. теорему 1), справедливо следующее утверждение.

Теорема 3. Следующие условия эквивалентны:

- (1) перестановочный автомат $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$ является сильно приведенным;
- (2) примитивен минимальный нормальный делитель группы $G = \langle (h_x)_{x \in X} \rangle$ автомата A , по которому все образующие элементы $(h_x)_{x \in X}$ содержатся в одном смежном классе;
- (3) примитивен соответствующий автомату A автомат $A^d(M)$, где d — ширина группы G .

Таким образом, для установления сильной приведенности перестановочного автомата A достаточно, используя порядки некоторых элементов его группы G и известные определяющие соотношения, найти множество чисел $\{d(1), d(2), \dots, d(m)\}$, среди которых должен содержаться параметр d группы G , и установить примитивность групп $G_{d(1)}, G_{d(2)}, \dots, G_{d(m)}$. Если при этом хотя бы одна из указанных групп окажется импримитивной, то импримитивна и группа

$$M_{n(0)} = \bigcap_{n=1}^{\infty} G_n,$$

и автомат A слабо неприведен.

Отметим еще одну возможность. Обозначим через $\langle (h_x h_{x'}^{-1})_{x, x' \in X} \rangle$ подгруппу группы G перестановочного автомата A , порожденную элементами $(h_x h_{x'}^{-1})_{x, x' \in X}$. Очевидно, что $(h_x h_{x'}^{-1})_{x, x' \in X}$ является подгруппой группы $M_{n(0)}$, в связи с чем достаточным условием примитивности группы $M_{n(0)}$, а вместе с ней и сильной приведенности автомата A , является примитивность группы $\langle (h_x h_{x'}^{-1})_{x, x' \in X} \rangle$.

Список литературы

1. Бабаш А. В., Неотличимость состояний конечного автомата относительно функции, заданной на его входных и выходных словах. *Обзорные прикладной и промышленной математики* (2001) 8, №1, 94–95.
2. Гилл А., *Введение в теорию конечных автоматов*. Наука, Москва, 1986.
3. Кудрявцев В. Б., Алешин С. В., Подколзин А. С., *Введение в теорию автоматов*. Наука, Москва, 1985.
4. Глухов М. М., О числовых параметрах, связанных с заданием конечных групп системами образующих элементов. *Труды по дискретной математике* (1997) 1, 43–66.

Статья поступила 10.07.2002.