Math-Net.Ru

Общероссийский математический портал

А. В. Бабаш, Периоды выходных последовательностей автомата при заданной периодической входной последовательности, *Дискрет. матем.*, 2009, том 21, выпуск 4, 39–59

DOI: <https://doi.org/10.4213/dm1070>

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: 107.22.136.117

26 апреля 2023 г., 16:13:50

Периоды выходных последовательностей автомата при заданной периодической входной последовательности

© 2009 г. А. В. Бабаш

В работе оцениваются снизу периоды выходных последовательностей автоматов при заданной входной периодической последовательности.

1. Введение

Основным результатом по оценке снизу периода выходной последовательности конечного автомата, отвечающей его начальному состоянию и входной периодической последовательности, является результат, представленный теоремой 2.2 в [1] и состоящий в том, что минимальный период W выходной последовательности автомата не превосходит величины $|S|\omega$, где $|S|$ — число состояний автомата, а ω — минимальный период входной последовательности. В [2] и [3] приведены утверждения, суть которых состоит в том, что W является делителем числа $k\omega$ при некотором $k \leq |S|$.

В связи с большой сложностью проблемы оценки снизу периодов выходных последовательностей конечных автоматов при заданных начальных состояниях и входной периодической последовательности, естественным подходом к ее удовлетворительному решению является выделение тех или иных классов автоматов в качестве объектов исследований. Например, ряд работ посвящен вопросам периодичности выходных последовательностей линейных автономных автоматов, в частности, в этом классе выделяются работы, в которых указываются способы построения линейных рекуррентных последовательностей максимального периода в разнообразных алгебраических структурах. В данной работе используются другие подходы к решению обсуждаемой проблемы. Один из них заключается в установлении связей между наличием взаимной простоты периодов входной и выходной последовательностей автомата и различными обобщениями понятия автономности автомата.

Основные результаты работы могут быть сформулированы следующим образом.

- (1) Если приведенный автомат не имеет автономных состояний, то при периодической входной последовательности простого периода p , содержащей на своем периоде все k -граммы входного алфавита автомата для $k > |S|^2/2 + 3|S|/2 - 2$, где $|S|$ — число состояний автомата, период выходной последовательности автомата с любого начального состояния будет кратен p .

- (2) Класс так называемых перестановочных автоматов состоит из двух подклассов, подкласса автоматов с потерей информации и подкласса автоматов без потери информации. В статье доказано, что автоматы из первого подкласса таковы, что период выходной последовательности может сократиться по сравнению с периодом входной последовательности в любое число раз. Автоматы из второго подкласса таким свойством не обладают. Именно, для любого перестановочного автомата без потери информации при любой входной последовательности P периода $\omega(P)$ и любого состояния автомата период выходной последовательности будет не меньше $\omega(P)/|S|$.

Предложенные в работе подходы к получению нижних оценок периодов выходных последовательностей автоматов отличны от методики расчета мер приближенных периодов выходных последовательностей автомата, предложенной в [4]. Напомним, что в последней работе решена поставленная выше проблема, но для последовательностей состояний автомата и рассчитаны дополнительно меры приближенной периодичности этих последовательностей состояний. Ранее в работе [9] был указан широкий класс последовательных соединений автономного автомата с неавтономным автоматом с гарантированным обобщенным периодом выходных последовательностей (G -изопериодом в терминологии автора).

Приводимые результаты получены автором под руководством В. А. Башевым.

2. Обозначения, основные понятия, вспомогательные результаты

В статье используются следующие обозначения:

X, S, Y — произвольные непустые конечные множества с мощностями $|X| \geq 2, |S| \geq 2, |Y| \geq 2$;

$A = (X, S, Y, h, f)$ — конечный автомат с входным алфавитом X , множеством состояний S , выходным алфавитом Y , функцией перехода h и функцией выхода f ;

X^* — множество всех слов конечной длины в алфавите X ;

$A_M(s, P) = \{s_1, s_2, \dots, s_j, \dots\}$ — последовательность состояний автомата A , отвечающая его входной последовательности P и начальному состоянию $s = s_1 \in S$;

$A(s, P) = \{y_1, y_2, \dots, y_j, \dots\}$ — выходная последовательность автомата A ;

(ω, ω') — наибольший общий делитель чисел ω, ω' ;

$D \mid \omega$ обозначает, что D делит ω .

Определим так называемые частичные функции переходов $(h_x)_{x \in X}$ и выходов $(f_x)_{x \in X}$ через h и f следующим образом:

$$\begin{aligned} h_x: S &\rightarrow S, & h_x(s) &= h(x, s); \\ f_x: S &\rightarrow Y, & f_x &= f(x, s). \end{aligned}$$

Для $P = \{x(1), x(2), \dots, x(j), \dots\}$ из X^* и $s \in S$ положим

$$s_j = h_{x(j-1)} \dots h_{x(1)} s_1, \quad y_j = f_j h_{x(j-1)} \dots h_{x(1)} s_1.$$

Через $h(s, x(1), \dots, x(k))$ обозначим заключительное состояние автомата A с начальным состоянием s при входном слове $x(1), \dots, x(k)$, то есть

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

Автомат A называется перестановочным, если $(h_x)_{x \in X}$ — биекции. Автомат A называется приведенным, если для любых различных состояний s_1 и s_2 из S найдется входное слово P (зависящее от s_1 и s_2), при котором $A(s_1, P) \neq A(s_2, P)$.

Слова $P_1, P_2, \dots, P_k \in X^*$ назовем сравнимыми, если они имеют конечную одинаковую длину или они бесконечные.

Назовем состояние $s \in S$ автомата A внешне k -автономным, если $A(s, P) = A(s, P')$ для любых $P, P' \in X^k$, и внешне автономным, если $A(s, P) = A(s, P')$ для любых сравнимых слов $P, P' \in X^*$. Автомат A называется внешне k -автономным, если каждое его состояние внешне k -автономно, и внешне автономным, если он внешне k -автономен при любом k , то есть каждое его состояние внешне автономно. Несложно доказывается, что автомат Мура внешне автономен тогда и только тогда, когда его приведенная форма внутренне автономна, то есть для любого $s \in S$

$$h_{x(k)}, \dots, h_{x(2)}, h_{x(1)} s = h_{x'(k)} \dots h_{x'(2)} h_{x'(1)} s$$

при любых сравнимых словах $x(1), \dots, x(k), x'(1), \dots, x'(k)$ из X^* .

Входная последовательность $P = x(1), \dots, x(k)$ автомата $A = (X, S, Y, h, f)$ называется установочной (для A), если для любых $s, s' \in S$ из условия $A(s, P) = A(s', P)$ вытекает равенство $h(s, P) = h(s', P)$.

Ниже под периодической последовательностью будет пониматься смешанно-периодическая последовательность. Использование ее частного случая — чисто периодической последовательности (смешанно-периодической последовательности без подхода) будет специально оговариваться. Периодом периодической последовательности P будем называть ее минимальный период.

В изучении периодов выходных последовательностей автомата при заданной периодической входной последовательности большое значение будут играть следующие понятия.

Определение 1. Система сравнимых входных слов $P_1, P_2, \dots, P_k$ (возможно $k = \infty$) автомата $A = (X, S, Y, h, f)$ называется слабо неотличимой относительно A (или, кратко, слабо неотличимой), если найдутся состояния $s_1, s_2, \dots, s_k$ из S , при которых

$$A(s_1, P_1) = A(s_2, P_2) = \dots = A(s_k, P_k).$$

В противном случае система слов $P_1, P_2, \dots, P_k$ называется сильно различимой относительно A (сильно различимой).

Определение 2. Автомат A называется слабо k -автономным, если система всех его входных слов длины k слабо неотличима (относительно A).

Определение 3. Степенью слабой автономности $\sigma(A)$ автомата A называется максимальное число k , если оно существует, при котором он слабо k -автономен. В противном случае полагаем $\sigma(A) = \infty$.

Определение 4. Полнотой $Q(P)$ последовательности $P = x(1), x(2), \dots, x(j), \dots$ назовем максимальное k , если оно существует, при котором все k -граммы алфавита X содержатся в P . В противном случае полагаем $Q(P) = \infty$.

В изучении периодичности функционирования конечных автоматов большую роль будет играть следующее вспомогательное утверждение.

Предложение 1. Для любых натуральных чисел a, b из условия $(a, b) = d$ следует, что существуют натуральные числа $n(1), n(2)$, при которых $an(1) - bn(2) = d$.

3. Периоды выходных последовательностей автомата без внешне автономных состояний при входной периодической последовательности заданной полноты

Через $W(s, P)$ обозначим период выходной последовательности $A(s, P)$ автомата A , полученной при его начальном состоянии $s \in S$ при входной периодической последовательности $P = \{x(1), x(2), \dots\}$. В дальнейшем удобно представлять периодическую последовательность P в виде конкатенации ZV конечного слова $Z = \{x(1), x(2), \dots, x(n)\}$, являющегося подходом P и ее чисто периодической части $V = \{x(n+1), x(2), \dots\}$. Если P — чисто периодическая последовательность, то Z — пустое слово. Заметим, что выходная последовательность $A(s, P)$ для произвольного автомата A (даже при чисто периодической последовательности P) вообще говоря, смешанно-периодическая.

Теорема 1. Пусть $P = ZV$ — входная периодическая последовательность автомата A периода $\omega(P)$.

- (1) Если $Q(V) > \sigma(A)$, то при любом начальном состоянии $s \in S$ автомата A $(\omega(P), W(s, P)) \neq 1$.
- (2) Если $\omega(P)$ — простое число и V содержит сильно различимую систему сравнимых мультиграмм относительно автомата A , то при любом начальном состоянии $s \in S$ период $W(s, P)$ кратен $\omega(P)$.
- (3) Если A — приведенный автомат Мили без внешне автономных состояний, $\omega(P)$ — простое число, $Q(V) > |S|^2/2 + 3|S|/2 - 2$, то при любом начальном состоянии $s \in S$ период $W(s, P)$ кратен $\omega(P)$.
- (4) Если A — приведенный автомат Мура без внешне автономных состояний, $\omega(P)$ — простое число, $Q(V) > |S|^2/2 + |S|/2$, то при любом начальном состоянии $s \in S$ период $W(s, P)$ кратен $\omega(P)$.

Доказательство. Для $P = \{x(1), x(2), \dots\}$ положим $P^j = \{x(j), x(j+1), \dots\}$. Через $A(s)$ обозначим связную компоненту автомата A , содержащую состояние $s \in S$. Доказательство теоремы 1 проведем с помощью следующих трех вспомогательных лемм.

Лемма 1. Пусть $P = \{x(1), x(2), \dots\}$ — входная чисто периодическая последовательность периода $\omega(P)$ автомата $A = (X, S, Y, h, f)$. Тогда система сравнимых мультиграмм вида

$$\begin{aligned} P^{kd+1} &= \{x(kd+1), x(kd+2), \dots\}, & k &\in \{0, 1, \dots\}, \\ P^{(1)} &= P, & d &= (\omega(P), W(s, P)), \end{aligned} \quad (1)$$

слабо неотличима относительно связной компоненты $A(s)$ автомата A , содержащей состояние $s \in S$.

Доказательство. Для произвольного состояния s_1 автомата A рассмотрим выходную (вообще говоря, смешанно-периодическую) последовательность $A(s_1, P) = \{y_1, y_2, \dots\}$ и последовательность состояний $A_M(s, P) = \{s_1, s_2, \dots\}$, отвечающих входной последовательности P и начальному состоянию $s_1 \in S$. Легко видеть, что существует t , при котором последовательность $y_t, y_{t+1}, \dots$ чисто периодическая, и она может быть получена при входной периодической последовательности P , то есть $A(s_t, P) = \{y_t, y_{t+1}, \dots\}$. При этом связная компонента $A(s_t)$ автомата A содержится в компоненте $A(s_1)$.

Для доказательства утверждения теоремы достаточно доказать, что множество слов (1) слабо неотлично относительно связной компоненты $A(s_t)$ автомата A , содержащей состояние $s_t \in S$.

Положим для краткости $s_t = s$, $\omega(P) = \omega$, $W(s_t, P) = W$. При $(\omega, W) = \omega$ утверждение теоремы очевидно. Предположим, что $(\omega, W) = d \neq \omega$. Пусть k — произвольное число. Существуют такие натуральные числа $n(1)$ и $n(2)$, что $kn(1)\omega - kn(2)W = kd$. Ясно, что

$$\begin{aligned} A(s, P) &= A(s, P') = A(s, P^{kd-kd+1}) \\ &= A(s, P^{d-kn(1)\omega+kn(2)W+1}) = A(s, P^{kd+kn(2)W+1}). \end{aligned} \quad (2)$$

Выберем натуральное число $n(3)$ так, чтобы $\omega|(n(2) + n(3))$ и продолжим равенство (2) следующим образом:

$$\begin{aligned} &A(s, P^{kd+kn(2)W+1}) \\ &= A(h_x(kd+kn(2)W+n(3)W) \dots h_x(kd+kn(2)W+1)s, P^{kd+kn(2)W+n(3)W+1}) \\ &= A(h_x(kd+kn(2)W+n(3)W) \dots h_x(kd+n(2)W+1)s, P^{kd+1}). \end{aligned}$$

Здесь было учтено, что $\omega(P^{kd+1}) = \omega$. Нетрудно также убедиться в том, что состояние $s_{kd+1}^* = h_x(kd+n(2)W+n(3)W) \dots h_x(kd+n(2)W+1)s$ принадлежит связной компоненте $A(s)$ автомата A .

Таким образом, доказано существование состояний $s_1^*, s_{d+1}^*, \dots, s_{kd+1}^*$ связной компоненты $A(s)$ автомата A , при которых

$$A(s_1^*, P) = A(s_{d+1}^*, P^{d+1}) = \dots = A(s_{kd+1}^*, P^{kd+1}),$$

что и доказывает лемму 1.

Из леммы 1 вытекает утверждение 2 теоремы 1. В качестве P в условиях леммы 1 надо рассмотреть чисто периодическую часть V последовательности RV .

Теперь нам необходимо выяснить связи понятий слабой k -автономности автомата и его внешней k -автономности. Отметим, что слабая k -автономность автомата A равносильна слабой автономности его приведенной формы, в связи с чем исследование слабо k -автономных автоматов можно проводить, ограничиваясь рассмотрением приведенных автоматов.

Отметим, что для приведенных автоматов всегда существуют установочные последовательности. Обозначим через $L(\tilde{A})_{\text{hom}}$ длину минимальной установочной последовательности для приведенной формы $\tilde{A}$ автомата A .

Обозначим через $D(A)$ диаметр автомата A , а через $d(A)$ его степень различимости.

Лемма 2. Слабо k -автономный автомат A при $k \geq L(\tilde{A})_{\text{hom}} + D(A) + d(A) + 1$ имеет внешне автономное состояние.

Доказательство. Без ограничения общности будем считать, что $A = \tilde{A}$. Покажем сначала, что слабо k -автономный автомат A при $k > L(A)_{\text{hom}}$ имеет внешне $(k - L(A)_{\text{hom}})$ -автономное состояние.

Пусть A слабо k -автономен, $k > L$, $L(A)_{\text{hom}} = L$. Это означает, что найдутся состояния $s_p \in S$, $P \in X^k$ и выходное слово $\{y_1, y_2, \dots, y_k\}$ автомата A , при которых $A(s_p, P) = \{y_1, y_2, \dots, y_k\}$ для каждого $P \in X^k$. В частности, для установочной последовательности $R \in X^L$ и произвольных слов $U \in X^{k-L}$

$$A(s_{RU}, RU) = \{y_1, y_2, \dots, y_k\}, \quad U \in X^{k-L}. \quad (3)$$

(RU — конкатенация слов R и U).

Так как R — установочная последовательность для A , то найдется $s \in S$, при котором $h(s_{RU}, R) = s$ при всех $U \in X^{k-L}$. Из последних равенств и равенств (3) вытекает, что $A(s, U) = \{y_1, y_2, \dots, y_k\}$ при всех $U \in X^{k-L}$, то есть состояние s внешне k -автономно.

Пусть теперь при $k \geq L(A)_{\text{hom}} + D(A) + d(A) + 1$ автомат A слабо k -автономен. По доказанному выше A имеет внешне $(k - L(A)_{\text{hom}})$ -автономное состояние $s \in S$. Из условий леммы следует, что $k' = (k - L(A)_{\text{hom}}) \geq D(A) + d(A) + 1$. Несложно доказать, что каждое состояние, достижимое из s является, по крайней мере, внешне $(d(A) + 1)$ -автономным. Для доказательства леммы 2 достаточно доказать, что автомат $A(s)$, порожденный состоянием s , является внешне автономным.

Итак, пусть автомат $A(s)$ является внешне k -автономным при $k = (d(A) + 1)$ и s^* — произвольное его состояние, а $\{x(1), \dots, x(d+t+1)\}, \{x'(1), \dots, x'(d+t+1)\}$, $d = d(A)$, $t \geq 1$, — произвольная пара его входных слов. Предположим, что $A(s)$ является внешне $(d+1)$ -автономным при некотором натуральном t . В этом случае, очевидно, состояния $h(s^*, x(1)), h(s^*, x'(1))$ будут $d+t-1$ неотличимы и, следовательно, неотличимы. Используя внешне $(d+t)$ -автономность автомата $A(s)$ и неотличимость указанных состояний, получаем, что

$$\begin{aligned} f_{x(d+t+1)} h_{x(d+t)} \dots h_{x(2)} (h_{x(1)} s^*) &= f_{x(d+t+1)} h_{x(d+t)} \dots h_{x(2)} (h_{x'(1)} s^*) \\ &= f_{x'(d+t+1)} h_{x'(d+t)} \dots h_{x'(2)} (h_{x'(1)} s^*). \end{aligned}$$

Таким образом, доказано, что из внешне $(d+t)$ -автономности автомата A следует его внешне $(d+t+1)$ -автономность, $t \geq 1$, откуда и вытекает внешне автономность автомата $A(s)$. Утверждение леммы 2 доказано.

Лемма 3. Для приведенных автоматов A , не имеющих внешне автономных состояний,

$$\sigma(A) \leq \frac{|S|^2}{2} + \frac{3|S|}{2} - 2,$$

если A — автомат Мили, и

$$\sigma(A) \leq \frac{|S|^2}{2} + \frac{3|S|}{2},$$

если A — автомат Мура.

Доказательство. В работе [5] показано, что для любого приведенного автомата Мили

$$L(A)_{\text{hom}} \leq \frac{|S|(|S| - 1)}{2},$$

а для приведенных автоматов Мура

$$L(A)_{\text{hom}} \leq \frac{|S|(|S| - 1)}{2} - |S| + 2,$$

причем эти оценки как функции от числа состояний $|S|$ не могут быть понижены. Известно также (см., например, [5, 6]), что

$$D(A) \leq |S| - 1$$

для любого автомата A . Поэтому

$$L(A)_{\text{hom}} + D(A) + d(A) \leq \frac{|S|(|S| - 1)}{2} + 2|S| - 2$$

для автомата Мили и

$$L(A)_{\text{hom}} + D(A) + d(A) \leq \frac{|S|^2}{2} + \frac{|S|}{2}$$

для автоматов Мура. Следовательно, по лемме 2 при $k \geq |S|(|S| - 1)/2 + 2|S| - 1$ слабо k -автономный автомат Мили имеет внешне автономное состояние. По этой причине для автоматов Мили без внешне автономных состояний

$$\sigma(A) \leq \frac{|S|^2}{2} + \frac{3|S|}{2} - 2.$$

Аналогично доказывается, что для автоматов Мура без внешне автономных состояний

$$\sigma(A) \leq \frac{|S|^2}{2} + \frac{|S|}{2}.$$

Продолжим доказательство теоремы 1. Докажем теперь утверждение 1 теоремы 1. Пусть $P = ZV$ — входная периодическая последовательность автомата A . Предположим, что существует $s_0 \in S$, при котором $(\omega(P), W(s_0), P) = 1$. Очевидно, найдется состояние $s \in S$, при котором $W(s, V) = W(s_0, P)$. По лемме 1 система сравнимых мультиграмм вида V^{k+1} , $k \in \{0, 1, \dots\}$, $V^1 = V$ слабо неотличима относительно связной компоненты $A(s)$ автомата A , содержащей состояние $s \in S$. В частности, автомат $A(s)$ слабо $Q(V)$ -автономен. Поэтому его степень слабой автономности удовлетворяет неравенству $\sigma(A(s)) \geq Q(V)$. Но $\sigma(A) \geq \sigma(A(s))$, в связи с чем $\sigma(A) \geq Q(V)$, что противоречит условию первого утверждения теоремы.

Пусть теперь A — приведенный автомат без внешне автономных состояний, $\omega(P)$ — простое число, $Q(V) > |S|^2/2 + 3|S|/2 - 2$. Предположим, что $(\omega(P), W(s_0, P)) = 1$. Тогда согласно первому утверждению теоремы должно выполняться неравенство $\sigma(A) \geq Q(V)$. По лемме 3 $|S|^2/2 + 3|S|/2 - 2 \geq \sigma(A)$. Следовательно, $|S|^2/2 + 3|S|/2 - 2 \geq Q(V)$, что противоречит условиям утверждения 3 теоремы 1. Аналогично доказывается четвертое утверждение теоремы 1.

Снизить данные в п. 3, 4 ограничения на величину $Q(V)$, понижая приведенные верхние оценки степени слабой автономности автоматов, не удастся. Следующие примеры показывают, что для автоматов Мили приведенная в лемме 3 оценка их степени слабой автономности достижима, а для автоматов Мура почти достижима.

Пример 1. Положим $X = \{1, \dots, |S|\}$, $S = \{s^{(1)}, s^{(2)}, \dots, s^{(|S|)}\}$, $Y = \{0, 1\}$, $h_x s^{(x)} = s^{(x+1)}$, $x \neq |S|$; $h_{|S|} s^{(|S|)} = s^{(|S|)}$; $h_x s^{(x+1)} = s^{(x)}$, $x \neq |S|$; $h_x s^{(j)} = s^{(j)}$, $x \neq j$, $j \neq x + 1$; $f_x s^{(j)}$ при $x = j = |S|$, и $f_x s^{(j)} = 0$ в противном случае.

Введенный автомат $A = (X, S, Y, h, f)$ является перестановочным автоматом, кроме того, он не имеет внешне автономных состояний. Покажем, что автомат A слабо k -автономен при $k = |S|^2/2 + |S|/2 - 1$. Пусть слово $P = \{x(1), x(2), \dots, x(k)\}$ таково, что

$A(s(x), P) \neq 0$ (не является словом, состоящим сплошь из нулей) для всех $s^{(x)}$ из S . Для каждой пары (i, j) , $1 \leq i \leq j \leq |S|$, очевидно, найдется целое число $L = L(i, j)$, $1 \leq L \leq k$, при котором $h_{x(L-1)}h_{x(L-2)} \dots h_{x(1)}s^{(i)} = s^{(j)}$, $x(L) = j$.

Здесь мы положили $h_{x(0)}s^{(i)} = s^{(i)}$. Для различных пар (i, j) , (i', j') величины $L(i, j)$, $L(i', j')$ различны. Действительно, если $L(i, j) = L(i', j')$, то

$$j = i(L(i, j)) = i'(L(i', j')) = j'.$$

Поэтому, в силу перестановочности автомата A , и $i = i'$. Таким образом, число различных чисел $L(i, j)$ совпадает с числом различных пар (i, j) , $1 \leq i \leq j \leq |S|$, которое в свою очередь, очевидно, равно $|S|^2/2 + |S|/2$. Учитывая, что $L(i, j) \leq k$, получаем неравенство

$$k \geq \frac{|S|^2}{2} + \frac{|S|}{2}.$$

Из этой оценки непосредственно вытекает, что для любой последовательности P длины меньшей, чем $|S|^2/2 + |S|/2$, найдется состояние $s^{(i)} \in S$ автомата A , при котором $A(s^{(i)}, P)$ есть последовательность, состоящая из нулей. То есть автомат A оказывается по крайней мере слабо k -автономным при $k = |S|^2/2 + |S|/2 - 1$.

Пример 2. Положим $X = \{1, 2, \dots, |S|\}$, а S, Y и частичные функции переходов $(h_x)_{x \in X}$, определим, как и в примере 1. Кроме того, положим $f_x = \lambda$ для всех $x \in X$. Рассматриваемый автомат A является перестановочным автоматом Мура без внешне автономных состояний. Аналогично тому, как показывается в примере 1, показывается, что автомат A является слабо k -автономным для $k = |S|^2/2 - |S|/2$.

Отличие доказательства состоит в том, что множество чисел вида $L(i, j)$ необходимо рассматривать при $1 \leq i \leq j \leq |S| - 1$. Число таких пар (i, j) равно $|S|^2/2 - |S|/2$. Поэтому

$$k \geq \frac{|S|^2}{2} - \frac{|S|}{2} + 1,$$

и следовательно,

$$\sigma(A) \geq \frac{|S|^2}{2} - \frac{|S|}{2}.$$

Как видно из приведенных общих утверждений, оценки параметра $\sigma(A)$ слабой автономности автоматов в классе автоматов без внешне автономных состояний не могут быть существенно улучшены, например, по порядку. Поэтому естественно возникает вопрос, нельзя ли в общем случае оценку $\sigma(A)$ существенно понизить, если искать ее для почти всех автоматов. Из приведенных результатов работ [7, 8] по оценкам диаметра $D(A)$, степени различимости $d(A)$ и длины $L(A)_{\text{hom}}$ установочного эксперимента для почти всех автоматов следует, что для почти всех приведенных автоматов $A = (X, S, Y, h, f_x)$, $|X| \geq 2$, $|Y| \geq 2$, без внешне автономных состояний

$$\sigma(A) \leq 5 \log_{|Y|} |S| + \frac{1}{6} \log_{|X|} |S|.$$

Для практического использования утверждения теоремы 1 необходимо выделить классы автоматов с наибольшей степенью слабой автономности. Поэтому представляют интерес оценки слабой автономности приводимых ниже линейных векторных автоматов.

4. Периоды выходных последовательностей линейного векторного автомата при заданной входной периодической последовательности

Ниже мы уточним утверждение леммы 3 и утверждения 1, 2 теоремы 1 для некоторых классов линейных автоматов.

Пусть $A = (X, V_n(q) \setminus 0, F_q, (B_x)_{x \in X}, (C_x)_{x \in X})$ — линейный автомат с входным алфавитом X , множеством состояний $V_n(q) \setminus 0$, являющимся векторным пространством $V_n(q)$ над полем F_q с исключенным нулевым вектором, выходным алфавитом F_q , частичными функциями переходов $(B_x)_{x \in X}$, являющимися линейными преобразованиями векторного пространства $V_n(q)$, частичными функциями выхода $(C_x)_{x \in X}$, осуществляющими линейные отображения $V_n(q)$ в F_q .

Лемма 4. Если $s \in V_n(q) \setminus 0$ — внешне k -автономное состояние, $k \geq 2n$, автомата $A = (X, V_n(q) \setminus 0, F_q, (B_x)_{x \in X}, (C_x)_{x \in X})$, то оно внешне автономно.

Доказательство. Рассмотрим систему векторов $CB(j)$ ранга r_j

$$\begin{aligned} &\{B_{x(1)}s: x(1) \in X\}, \\ &\{B_{x(2)}B_{x(1)}s: x(1) \in X^2\}, \\ &\dots \\ &\{B_{x(j)} \dots B_{x(1)}s: x(j) \dots x(1) \in X^j\}. \end{aligned}$$

Легко видеть, что $1 \leq r_1 \leq \dots \leq r_j \leq r_{j+1} \leq \dots$, кроме того, из равенства $r_j = r_{j+1}$ для некоторого j следует, что $r_j = r_{j+k}$ при любом $k \geq 0$. Поэтому $r_{n-1} = r_n \leq n$.

Выберем $r = r_{n-1}$ линейно независимых векторов $s, s_1, \dots, s_{r-1}$ в $CB(n-1)$. Если теперь предположить, что состояние s внешне k -автономно, $k \geq 2n$, то, очевидно, должны быть внешне $(k-n+1)$ -автономными состояния $s, s_1, \dots, s_{r-1}$. Используя свойство линейности автомата, заключаем, что все достижимые из s состояния автомата A внешне $(k-n+1)$ -автономны, то есть внешне $(k-n+1)$ -автономен автомат $A(s)$, порожденный состоянием s . Так как степень различимости $d(A)$ любого автомата A не превосходит его размерности n , степень различимости $d(A(s))$ его подавтомата $A(s)$ не превосходит n . Итак, $A(s)$ является $(k-n+1)$ -автономным, $k \geq 2n$ и $d(A) \leq n$. Следовательно, $A(s)$ является k -автономным при некотором $k \geq d(A(s)) + 1$. Теперь несложно доказывается, что из этого факта следует внешне автономность состояния s линейного автомата A .

Напомним, что диагностической последовательностью произвольного автомата (X, S, Y, h, f) называется любое его входное слово P (если оно существует), при котором для любых $s, s' \in S$ из условия $A(s, P) = A(s', P)$ вытекает, что $s = s'$.

Отметим, что диагностическая последовательность автомата является одновременно и установочной. Обозначим $L(A)_{\text{diag}}$ минимальную длину диагностической последовательности автомата A .

Легко доказывается, что входное слово $\{x(1), x(2), \dots, x(k)\}$ линейного автомата $A = (X, V_n(q) \setminus 0, F_q, (B_x)_{x \in X}, (C_x)_{x \in X})$ является диагностическим тогда и только тогда, когда ранг системы $C_{x(1)}, C_{x(2)}B_{x(1)}, \dots, C_{x(k)}B_{x(k-1)} \dots B_{x(1)}$ линейных функций равен n .

Теорема 2. Пусть $A = (X, V_n(q) \setminus 0, F_q, (B_x)_{x \in X}, (C_x)_{x \in X})$ — линейный автомат без внешне автономных состояний и $L(A)_{\text{diag}} = n$. Тогда $\sigma(A) \leq 3n - 1$.

Доказательство. Пусть выполнены условия теоремы и $\sigma(A) \geq 3$. В начале доказательства леммы 2 было показано, что произвольный слабо k -автономный автомат A при $k > L(A)_{\text{hom}}$ имеет внешне $(k - L(A)_{\text{hom}})$ -автономное состояние. Так как в нашем случае $L(A)_{\text{hom}} \leq n$, автомат A имеет внешне $2n$ -автономное состояние $s \in S$, и тогда, по лемме 4, он имеет внешне автономное состояние, что противоречит условию теоремы.

Следствие 1. Пусть $A = (X, V_n(q) \setminus 0, F_q, (B_x)_{x \in X}, (C_x)_{x \in X})$ — линейный автомат без внешне автономных состояний, и линейное преобразование $B_a, a \in X$, является полноцикловым преобразованием пространства $V_n(q)$. Тогда $\sigma(A) \leq 3n - 1$.

Используя теорему 2 и следствие 3, с помощью утверждения 1 теоремы 1 легко строится класс линейных векторных автоматов, периоды выходных последовательностей которых кратны заданному простому числу ω при входных периодических последовательностях P периода ω с полнотой периодических частей, больших $3n - 1$.

Утверждение 2 теоремы 1 позволяет указать и другие классы линейных векторных автоматов с указанным выше свойством выходных последовательностей. Введем сначала необходимые понятия.

Определение 5. Система сравнимых входных слов $P_1, P_2, \dots, P_k$ (возможно $k = \infty$) линейного автомата $A = (X, V_n(q) \setminus 0, F_q, (B_x)_{x \in X}, (C_x)_{x \in X})$ называется слабо невырожденно неотличимой относительно A (или, кратко, слабо неотличимой), если найдутся состояния $s_1, s_2, \dots, s_k$ из S , при которых $A(s_1, P_1) = A(s_2, P_2) = \dots = A(s_k, P_k) \neq 0, \dots, 0$. В противном случае система слов $P_1, P_2, \dots, P_k$ называется сильно невырожденно различимой относительно A (сильно различимой).

Пусть $P_1 = x(1), x(2), \dots, x(k)$ — входное слово линейного автомата $A = (X, V_n(q) \setminus 0, F_q, (B_x)_{x \in X}, (C_x)_{x \in X})$. Обозначим через $r(P_1)$ ранг системы векторов $C_{x(1)}, C_{x(2)}B_{x(1)}, \dots, C_{x(k)}B_{x(k-1)} \dots B_{x(1)}$, а через $L(A(P_1))$ — множество (пространство) линейных соотношений между векторами этой системы.

Теорема 3. Пусть $P = ZV$ — входная периодическая последовательность автомата $A = (X, V_n(q) \setminus 0, F_q, (B_x)_{x \in X}, (C_x)_{x \in X})$ простого периода $\omega(P)$, а V содержит диагностическую последовательность автомата A и пару сравнимых слов $P_1 = x(1), \dots, x(t)$, $P_2 = x'(1), \dots, x'(t)$ таких, что

$$\text{rank}(L(A(P_1))) \cup L(A(P_2)) = t.$$

Тогда при любом s из $V_n(q) \setminus 0$ период $W(s, P)$ кратен $\omega(P)$.

Доказательству теоремы 3 предположим две леммы.

Лемма 5. Входные слова $P_1 = \{x(1), x(2), \dots, x(t)\}$, $P_2 = \{x'(1), x'(2), \dots, x'(t)\}$ линейного автомата $A = (X, V_n(q) \setminus 0, F_q, (B_x)_{x \in X}, (C_x)_{x \in X})$ сильно невырожденно различимы тогда и только тогда, когда

$$\text{rank}(L(A(P_1))) \cup L(A(P_2)) = t.$$

Доказательство. Рассмотрим системы линейных уравнений $L(P_1, y)$

$$\begin{aligned} C_{x(1)}s &= y_1, \\ C_{x(2)}B_{x(1)}s &= y_2, \\ &\dots \\ C_{x(t)}B_{x(t-1)} \dots B_{x(1)}s &= y_t \end{aligned}$$

и $L(P_2, y)$

$$\begin{aligned} C_{x'(1)}s' &= y_1, \\ C_{x'(2)}B_{x'(1)}s' &= y_2, \\ &\dots \\ C_{x'(t)}B_{x'(t-1)} \dots B_{x'(1)}s' &= y_t \end{aligned}$$

относительно неизвестных s, s' из $V_n(q) \setminus 0$. Положим

$$\Delta_y^{P_1} = \begin{cases} 1, & \text{если система } L(P_1, y) \text{ совместна,} \\ 0 & \text{в противном случае,} \end{cases}$$

и аналогично

$$\Delta_y^{P_2} = \begin{cases} 1, & \text{если система } L(P_2, y) \text{ совместна,} \\ 0 & \text{в противном случае.} \end{cases}$$

Методами линейной алгебры легко получить равенство

$$\sum \Delta_y^{P_1} \Delta_y^{P_2} = q^{\text{rank}(L(A(P_1)) \cup L(A(P_2)))},$$

где сумма взята по всем возможным наборам $y = y_1, y_2, \dots, y_t$ из F_q^t . Левая часть этого равенства представляет собой число наборов y из F_q^t , при которых одновременно совместны системы $L(P_1, y)$ и $L(P_2, y)$. В то же время сильно невырожденная различимость системы слов P_1, P_2 означает в этой терминологии не что иное, как справедливость равенства

$$\sum_{y \neq 0} \Delta_y^{P_1} \Delta_y^{P_2} = 0.$$

Таким образом, сильная невырожденная различимость системы слов P_1, P_2 равносильна условию

$$q^{t - \text{rank}(L(A(P_1)) \cup L(A(P_2)))} = 1,$$

то есть

$$t = \text{rank}(L(A(P_1)) \cup L(A(P_2))).$$

Лемма 6. Пусть $P = ZV$ — входная периодическая последовательность линейного векторного автомата $A = (X, V_n(q) \setminus 0, F_q, (B_x)_{x \in X}, (C_x)_{x \in X})$ периода $\omega(P)$, и V содержит его диагностическую последовательность. Если

$$(W(s, P), \omega(P)) = 1$$

при некотором $s \in V_n(q) \setminus 0$, то при $k \geq n$ все k -граммы последовательности V слабо невырожденно неотличимы относительно автомата A .

Доказательство. По лемме 1 все мультиграммы одинаковой длины слабо неотличимы относительно автомата A . Пусть началом мультиграммы $V^{k(0)}$ является диагностическая последовательность $x''(1), x''(2), \dots, x''(k)$. Тогда для каждого k найдется s_k из $V_n(q) \setminus 0$, для которого справедливы равенства

$$A(s_{k(0)}, V^{k(0)}) = A(s_k, V^k).$$

Из диагностичности последовательности $x(1), x(2), \dots, x(k)$ линейного автомата $A = (X, V_n(q) \setminus 0, F_q, (B_x)_{x \in X}, (C_x)_{x \in X})$ следует, что ранг системы векторов $C_{x''(1)}, C_{x''(2)} B_{x''(1)}, \dots, C_{x''(k)} B_{x''(k-1)} \dots B_{x''(1)}$ равен n . Поэтому $A(s_{k(0)}, V^{k(0)})$ не является последовательностью, составленной из нулей. Лемма доказана.

Теперь теорема 3 непосредственно следует из лемм 1, 5, 6.

Выделим в алфавите X два различных элемента a и b . Пусть $a^k = \{a, \dots, a\}$ — слово длины k , состоящее из элементов, равных a . Аналогично, определяется b^k . Обозначим через $V_n^*(q)$ пространство линейных функций на $V_n(q)$, через B_x^* — линейное преобразование $V_n^*(q)$, сопряженное к B_x , $x \in X$. Через $\chi(x)$ обозначим минимальные многочлены вектора C_x относительно линейного преобразования B_x^* . Из теоремы 3 можно получить следующее утверждение.

Следствие 2. Пусть $P = ZV$ — входная периодическая последовательность автомата $A = (X, V_n(q) \setminus 0, GF(q), (B_x)_{x \in X}, (C_x)_{x \in X})$ простого периода $\omega(P)$, а V содержит мультиграммы a^t и b^t , причем $\deg \chi(a) = n$, $(\chi(a), \chi(b)) = 1$ и t не меньше степени наименьшего кратного $\text{LCM}(\chi(a), \chi(b))$. Тогда при любом s из $V_n(q) \setminus 0$ период $W(s, P)$ кратен $\omega(P)$.

Доказательство. Используем теорему 3 и лемму 5. Для доказательства следствия 2 нам достаточно доказать, что, во-первых, V содержит диагностическую последовательность и, во-вторых, система мультиграмм a^t и b^t сильно невырожденно различима, то есть (по лемме 5) $\text{rank}(L(A(a^t)) \cup L(A(b^t))) = t$.

Первое утверждение очевидно, так как из $\deg \chi(a) = n$ следует, что a^t — диагностическая последовательность для A . Второе утверждение сформулируем и докажем в виде отдельной леммы.

Лемма 7. Пусть t больше или равно степени наименьшего общего кратного $\text{LCM}(\chi(a), \chi(b))$. Тогда для мультиграмм a^t и b^t условие

$$\text{rank}(L(A(a^k)) \cup L(A(b^t))) = t. \quad (4)$$

равносильно условию

$$(\chi(a), \chi(b)) = 1.$$

Доказательство. Справедливо равенство

$$\begin{aligned} \text{rank}(L(A(a^t)) \cup L(A(b^t))) \\ = \dim L(A(a^k)) + \dim L(A(a^k)) - \dim(L(A(a^k)) \cap L(A(b^t))). \end{aligned}$$

Очевидно, что

$$\begin{aligned} \dim L(A(a^k)) &= t - \deg \chi(a), \\ \dim L(A(b^t)) &= t - \deg \chi(b), \\ \dim(L(A(a^k)) \cap L(A(b^t))) &= t - \deg \text{LCM}(\chi(a), \chi(b)). \end{aligned}$$

Требуемое условие (4) равносильно условию

$$t - \deg \chi(a) + t - \deg \chi(b) - t + \deg \text{LCM}(\chi(a), \chi(b)) = t$$

или

$$\deg \chi(a) + \deg \chi(b) = \deg \text{LCM}(\chi(a), \chi(b)),$$

которое, в свою очередь, эквивалентно тому, что $\text{LCM}(\chi(a), \chi(b)) = 1$.

Лемма 7, а вместе с ней и следствие 2, доказаны.

5. Период внешнего функционирования автономного последовательного соединения автоматов

Пусть $A_1 = (S_1, Y_1, h, \lambda)$ — приведенный полноцикловый автомат с множеством состояний S_1 , $|S_1| > 1$, выходным алфавитом Y_1 , $|Y_1| > 1$, функцией перехода h и функцией выхода λ , а $A = (X, S_2, Y_2, h, f)$, $Y_1 = X$, — перестановочный автомат с частичными функциями переходов $(h_x)_{x \in X}$ и частичными функциями выхода $(f_x)_{x \in X}$. Напомним, что последовательным соединением автоматов A_1, A_2 называют автономный автомат $A_1 \rightarrow A_2 = (S_1 \times S_2, Y_2, h^{1,2}, f^{1,2})$, у которого

$$\begin{aligned} h^{1,2}(s(1), s(2)) &= (hs(1), h_{\lambda(s(1))}s(2)), \\ f^{1,2}(s(1), s(2)) &= f_{\lambda(s(1))}s(2), \quad (s(1), s(2)) \in S_1 \times S_2. \end{aligned}$$

Наряду с последовательным соединением $A_1 \rightarrow A_2$ введенных автоматов мы будем рассматривать так называемое обобщенное последовательное соединение $A_1 \Rightarrow A_2$ автоматов A_1, A_2 , отличающееся от $A_1 \rightarrow A_2$ функцией выхода. При обобщенном соединении любое отображение $S \times S_2 \rightarrow Y$ может быть функцией выхода автомата $A_1 \Rightarrow A_2$.

Очевидно, построенный автомат $A = A_1 \Rightarrow A_2$ является перестановочным автоматом; длины циклов графа переходов автомата A кратны числу $|S_1|$. Обозначим $W(s(1), s(2))$ период выходной последовательности $A(s(1), s(2))$, соответствующей начальному состоянию $(s(1), s(2)) \in S_1 \times S_2$ автомата A . Пусть $W(A)$ — наименьшее общее кратное периодов $W(s(1), s(2))$, взятое по всем $(s(1), s(2)) \in S_1 \times S_2$. Эта величина называется периодом внешнего функционирования автомата A .

Пусть $L_1, L_2, \dots, L_t$ — связные компоненты (циклы) автомата A и $|L_j|$, $j \in \{1, \dots, t\}$, — их длины. Очевидно, периоды последовательностей автомата A от начальных состояний, содержащихся в одном цикле, совпадают, в связи с чем можно говорить о периоде выходных последовательностей состояний цикла L_j , $j = \{1, \dots, t\}$, или более кратко, о выходном периоде W_j цикла L_j . Известно, что период (длина) W_j цикла L_j совпадает с числом классов неотличимых состояний связной компоненты L_j , $j \in \{1, \dots, t\}$. Поэтому

$$W(A) = \text{LCM}(W_j, j \in \{1, \dots, t\}) = \text{LCM}(|L_j|/|N_j|),$$

где $|N_j|$ — мощность классов неотличимых состояний цикла L_j , $j = 1, \dots, t$. Для получения оценки снизу периода $W(A)$ внешнего функционирования автомата A введем необходимые обозначения и докажем вспомогательные леммы.

Пусть A_v , $v \in \{1, \dots, \Gamma\}$, — подавтомат автомата A , состоящий из v -го класса $L_{v1}, L_{v2}, \dots, L_{vt(v)}$ неотличимых связных компонент (циклов) автомата A и $N(A_v)$ — мощность его классов неотличимых состояний, $W(A_v)$, $v \in \{1, \dots, \Gamma\}$, — число его классов неотличимых состояний. Очевидно, что

$$W(A) = \text{LCM}(W(A_v), \quad v = 1, \dots, \Gamma,$$

где $W(A_v) = W(L_{vj})$, $j = 1, \dots, t(v)$.

Лемма 8. Пусть d делит $|S_1|$. Тогда $d/(d, W(A_v))$ делит $N(A_v)$, $v = 1, \dots, \Gamma$.

Доказательство. Положим $L_{vj} = dk_{vj}$. Справедливо равенство

$$\sum_{j \in \{1, \dots, t(v)\}} |L_{vj}| = W(A_v)N(A_v) = dk_{vj}.$$

Отсюда и вытекает данное утверждение.

Лемма 9. Пусть P — простое число, α — целое число, $\alpha \geq 1$, P^α делит $|S_1|$, $(P^\alpha, W(A)) = P^\beta$, $0 \leq \beta \leq \alpha$. Тогда мощность любого класса k -неотличимых состояний, $k = 1, 2, \dots$, перестановочного автомата A кратна $P^{\alpha-\beta}$.

Доказательство. Так как каждый класс k -неотличимых состояний автомата A представляет собой объединение некоторых классов $(k+1)$ -неотличимых состояний, а $N(A_v)$, $v = 1, \dots, \Gamma$, являются мощностями его классов неотличимых состояний, для доказательства леммы достаточно показать, что $P^{\alpha-\beta}$ делит $N(A_v)$ при любом $v \in \{1, \dots, \Gamma\}$. По лемме 8

$$\frac{d}{(d, W(A_v))} \mid N(A_v), \quad v = 1, \dots, \Gamma.$$

Заметим, что из условия $(P^\alpha, W(A)) = P^\beta$, $0 \leq \beta \leq \alpha$, вытекают равенства

$$(P^\alpha, W(A_v)) = P^{\beta(v)}, \quad v = 1, \dots, \Gamma,$$

при некоторых $\beta(v) \leq \beta$, и следовательно, величина $P^\alpha / (P^\alpha, W(A_v)) = P^{\alpha-\beta(v)}$ делит $N(A_v)$, $v = 1, \dots, \Gamma$. Но тогда тем более $P^{\alpha-\beta}$ делит $N(A_v)$, $v = 1, \dots, \Gamma$, что и требовалось доказать.

Из леммы 9 непосредственно вытекают следующие два утверждения.

Следствие 3. Пусть $|S_1| = P_1^{\alpha(1)} P_2^{\alpha(2)} \dots P_n^{\alpha(n)}$, P_j — простые числа, α_j , $j = 1, \dots, n$, — целые положительные числа, и для автомата $A = A_1 \Rightarrow A_2$

$$(|S_1|, W(A)) = P_1^{\beta(1)} P_2^{\beta(2)} \dots P_n^{\beta(n)}, \quad \beta(j) \geq 0, \quad j = 1, \dots, n.$$

Тогда мощность любого класса k -неотличимых состояний автомата A кратна числу $P_1^{\alpha(1)-\beta(1)} P_2^{\alpha(2)-\beta(2)} \dots P_n^{\alpha(n)-\beta(n)}$.

Следствие 4. Пусть общий наибольший делитель мощностей некоторых классов k -неотличимых состояний автомата $A = A_1 \Rightarrow A_2$ равен единице. Тогда период внешнего функционирования автомата A кратен $|S_1|$.

6. Периоды выходных последовательностей перестановочных автоматов без потери информации при заданных периодических входных последовательностях

Ниже в данном разделе рассматриваются перестановочные автоматы и чисто периодические их входные последовательности. Напомним необходимые нам понятия [6]. Состояние s автомата A называется состоянием с потерей информации, если найдутся разные сравнимые слова $R = \{x(1), x(2), \dots, x(k)\}$, $T = \{x'(1), x'(2), \dots, x'(k)\}$ из X^* , при которых

$$A(s, R) = A(s, T), \quad h(s, R) = h(s, T),$$

в противном случае состояние s называется состоянием без потери информации. Автомат A называется автоматом с потерей информации, если у него найдется состояние с потерей информации, в противном случае он называется автоматом без потери информации.

Через $\omega(s, P)$ обозначим период последовательности состояний $A_M(s, P)$ автомата A при входной чисто периодической последовательности P и начальном состоянии s .

Обозначим через N_y , $y \in Y$, множество всех состояний $s \in S$ автомата A , для каждого из которых существует элемент $x \in X$, $x = x(s)$, удовлетворяющий равенству $f_x s = y$.

Очевидно, $|N_y| \leq |S|$ при любом $y \in Y$, а если A является автоматом Мура, то

$$\sum_{y \in Y} |N_y| = |S|,$$

что в общем случае для автоматов Мили не справедливо.

Для входной последовательности P автомата A и его состояния $s \in S$ введем параметр $N(A(s, P))$, положив $N(A(s, P)) = \min\{|N_y|\}$, где минимум берется по всем выходным символам $y \in Y$ автомата A , встречающимся в выходной последовательности $A(s, P)$.

Определение 6. Назовем грубым периодом последовательности состояний $A_M(s, P)$ перестановочного автомата A при входной чисто периодической последовательности $P = \{x(1), x(2), \dots\}$ периода $\omega = \omega(P)$ и начальном состоянии $s \in S$ число $\Omega(s, P) = C\omega$, где $C = C(s, P)$ — длина цикла подстановки $h_{x(\omega)} h_{x(\omega-1)} \dots h_{x(1)}$, содержащего состояние s .

Теорема 4. Справедливы следующие утверждения.

- (1) Если перестановочный автомат A — автомат с потерей информации, то для любого $\varepsilon > 0$ существуют входная чисто периодическая последовательность P периода $\omega(P)$ и состояние s автомата A , для которых

$$\frac{W(s, P)}{\omega(P)} < \varepsilon.$$

- (2) Если перестановочный автомат A — автомат без потери информации, то для любой входной чисто периодической последовательности $P = \{x(1), x(2), \dots\}$ периода $\omega(P)$ и любого начального состояния $s \in S$ автомата A

$$\frac{W(s, P)}{\omega(P)} \geq \frac{W(s, P)}{\Omega(s, P)} \geq \frac{1}{N(A(s, P))}.$$

Доказательство. Докажем сначала первое утверждение теоремы. Пусть автомат A — автомат с потерей информации, то есть существуют $s \in S$ и слова $R = \{x(1), \dots, x(k)\}$, $T = \{x'(1), \dots, x'(k)\}$, $R \neq T$, где $k \geq 1$, $x_j, x'_j \in X$, $j = 1, \dots, k$, для которых справедливы равенства

$$A(s, R) = A(s, T), \quad h(s, R) = h(s, T) = s', \quad s' \in S.$$

Так как A — перестановочный автомат, существует входное слово $M = x''(1), \dots, x''(n)$, $x''_j \in X$, $j \in \{1, \dots, n\}$, для которого $h_{x''(n)} h_{x''(n-1)} \dots h_{x''(1)} s' = s$.

Рассмотрим последовательность $P = RMRM \dots RMTMRMRM \dots RMTM \dots$, где $RMRM \dots RM$ — подпоследовательности длины L . Период $\omega(P)$ этой последовательности, очевидно, является делителем числа

$$L(k+n) + k + n = (L+1)(k+n).$$

Возьмем в качестве $L+1$ простое число $p < (k+n)/\varepsilon$. Из условия $R \neq T$ следует, что $\omega(P)$ не является делителем числа $k+n$ и, следовательно, $\omega(P)$ кратно p , так как

$\omega(P)$ делит $p(k+n)$. Кроме того, из построения последовательности P и выбора $s \in S$ вытекает, что $W(s, P)$ делит $k+n$. Таким образом, можно заключить, что

$$\frac{W(s, P)}{\omega(P)} \leq \frac{k+n}{\omega(P)} \leq \frac{k+n}{p} < \varepsilon.$$

Первое утверждение теоремы доказано.

Докажем второе утверждение теоремы. Очевидно, что $W = W(s, P)$ и $\omega(P)$ являются делителями грубого периода $\Omega(s, P)$ последовательности состояний $A_M(s, P)$ автомата A , поэтому, в частности,

$$\frac{W(s, P)}{\omega(P)} \geq \frac{W(s, P)}{\Omega(s, P)}.$$

Пусть

$$\frac{\Omega(s, P)}{W(s, P)} = L(s, P) = L.$$

Положим $A_M(s, P) = \{s_1, s_2, \dots, s_n, \dots\}$, где $s_{n+1} = h_{x(n)} \dots h_{x(1)}s$ и $s_1 = s$. Для доказательства требуемого утверждения теперь достаточно показать, что для любого $j = 0, 1, \dots, W-1$ все состояния вида s_{j+1+kW} , $k = 0, 1, \dots, L-1$ различны. Действительно, если это не так, то $L \leq |N_y|$ для любого y , содержащегося в последовательности $A(s, P)$, и следовательно, $L \leq N(A(s, P))$. Поэтому

$$\frac{W(s, P)}{\omega(P)} \geq \frac{W(s, P)}{\Omega(s, P)} = \frac{1}{L}.$$

Покажем теперь, что при любом $j \in \{0, 1, \dots, \omega-1\}$ указанные выше L состояний различны. Предположим противное, то есть предположим, например, что для $j = 0$ существуют целые числа $k(1), k(2)$, $0 \leq k(1) < L-1$, $k(1) < k(2) \leq L-1$, для которых $s_{1+k(1)W} = s_{1+k(2)W}$.

Для последовательности $P = \{x(1), x(2), \dots\}$ введем вспомогательные последовательности $P' = \{x(t), x(t+1), \dots\}$, $P' = P$. Справедливо равенство

$$A(s_{1+k(1)W}, P^{k(1)W+1}) = A(s_{1+k(2)W}, P^{k(2)W+1}),$$

так как $W = W(s, P)$ — период последовательности $A(s, P)$.

Пусть $s^* = s_{1+k(1)W} = s_{1+k(2)W}$, $\Omega^{\text{ext}}(s^*, P^{k(1)W+1}) = C_1\omega$, $\Omega^{\text{ext}}(s^*, P^{k(2)W+1}) = C_1\omega$ — грубые периоды последовательностей $A_M(s^*, P^{k(1)W+1})$, $A_M(s^*, P^{k(2)W+1})$, и пусть $H = \text{LCM}(C_1\omega, C_1\omega)$, где $\omega = \omega(P) = \omega(P^{k(1)W+1}) = \omega(P^{k(2)W+1})$. Тогда

$$h_{x(k(1)W+H)} \dots h_{x(k(1)W+2)} h_{x(k(1)W+1)} s^* = h_{x(k(2)W+H)} \dots h_{x(k(2)W+2)} h_{x(k(2)W+1)} s^*.$$

Так как автомат A — автомат без потери информации, из этого равенства следует, что $P^{(k(1)W+1)} = P^{(k(2)W+1)}$, и следовательно, $(k(2) - k(1))W = 0 \pmod{\omega(P)}$. Учитывая это сравнение, равенство состояний $s_{1+k(1)W}$, $s_{1+k(2)W}$ и перестановочность автомата A , получаем, что

$$s = h_{x(k(2)-k(1))W} \dots h_{x(2)} h_{x(1)} s.$$

Из определения величины $\Omega(s, P)$ и того факта, что $\omega(P)$ делит $(k(2) - k(1))W$, следует, что $\Omega(s, P)$ делит $(k(1) - k(2))W$. Последнее условие противоречит тому, что $k(2) - k(1) < L$. Утверждение 2 теоремы полностью доказано.

Следствие 5. Пусть A — перестановочный автомат без потери информации. Тогда для любой входной чисто периодической последовательности P периода $\omega(P)$ и любого состояния s автомата A выполнены неравенства

$$\Omega(s, P) \geq W(s, P) \geq \frac{\Omega(s, P)}{N(A(s, P))} \geq \frac{\omega(P)}{N(A(s, P))},$$

в частности,

$$|S|\omega(P \geq W(s, P)) \geq \frac{\omega(P)}{|S|}.$$

Доказательство. Верхняя оценка периода $W(s, P)$ очевидна, а нижняя оценка периода справедлива согласно лемме 2.

Говорят, что граф автомата $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$ не имеет параллельных дуг, если $h_x s \neq h_{x'} s$ при любом $s \in S$ для каждой пары различных элементов x, x' из X .

Следствие 6. Пусть $A = (X, S, Y, h, f)$ — перестановочный автомат и его граф не имеет параллельных дуг, P — его входная периодическая последовательность периода $\omega(P)$, $s \in S$ — его начальное состояние. Тогда период $\omega(s, P)$ последовательности состояний $A_M(s, P)$ автомата A кратен периоду $\omega(P)$. Если автомат A не является автоматом без параллельных дуг, то найдется его начальное состояние $s \in S$ и входная периодическая последовательность P некоторого периода $\omega(P)$, при которых период последовательности состояний $A_Y(s, P)$ не кратен $\omega(P)$.

Доказательство. Используем теорему 4. В качестве вспомогательного возьмем автомат Медведева A_M , соответствующий автомату $A = (X, S, Y, h, f)$. Автомат A_M имеет вид $A_M = (X, S, S, h, E)$, где S одновременно есть его множество состояний и выходной алфавит. Функция выхода E такова, что $E(s, x) = s$ при каждом s из S и x из X . Для автомата A_M ранее введенные множества N_y , $y \in Y$, одноэлементны, поэтому параметр $N(A(s, P))$ равен единице. Используя утверждение 2 теоремы 4, получаем, что

$$\Omega(s, P) \geq W(s, P) \geq \Omega(s, P),$$

то есть

$$\Omega(s, P) = W(s, P).$$

Обратно, если граф автомата A имеет параллельные дуги, то автомат $A_M = (X, S, S, h, E)$ является автоматом с потерей информации. Тогда искомые параметры, состояние s и периодическая входная последовательность P , найдутся согласно утверждению 1 теоремы 4. Доказательство завершено. Заметим, что это утверждение было получено ранее В. А. Башевым.

Пусть P — фиксированная чисто периодическая последовательность символов некоторого алфавита X , $|X| > 1$, периода $\omega(P)$ и s_1 — фиксированный элемент некоторого множества S . Следующая теорема отвечает на вопрос о достижимости приведенных в следствии 6 верхней и нижней оценок периода $W(s, P)$ выходной последовательности $A(s, P)$ автомата A .

Теорема 5. В классе перестановочных автоматов Мура $A = (X, S, Y, h, \lambda)$ без потери информации с входным алфавитом X и множеством состояний S оценки

$$\Omega(s_1, P) \geq W(s_1, P) \geq \frac{\Omega(s_1, P)}{N(A(s_1, P))}$$

периодов $W(s, P)$ выходных последовательностей $A(s, P)$ автоматов не могут быть улучшены.

Доказательство. Проведем сначала доказательство утверждения теоремы 5 относительно нижней оценки. Пусть A — некоторый перестановочный автомат Мура без потери информации. Рассмотрим отношение

$$\frac{\Omega(s_1, P)}{W(s_1, P)} = L(s_1, P) = L.$$

Исследуем сначала случай, когда $W(s_1, P) = 1$. Если $L = 1$, то утверждение доказано. В случае $L \geq 2$, как следует из доказательства леммы 2, первые L членов последовательности состояний $A_M(s_1, P)$ автомата A различны, поэтому $N(A(s_1, P)) > 1$, и мы можем построить новый автомат $A' = (X, S, Y', h, \lambda')$, отличающийся от A выходным алфавитом Y' , который мы определяем соотношением $Y' = Y \cup \{z\}$, где $z \notin Y$ — некоторый новый символ. Функцию выхода λ' определяем равенствами $\lambda'(s) = \lambda(s)$ в двух случаях: если s находится среди состояний последовательности $A_M(s_1, P)$ и если $s \notin N_y$ для каждого y из выходной последовательности $A(s_1, P)$ автомата A . Далее полагаем $\lambda'(s) = z$, если в последовательности состояний $A_M(s_1, P)$ не содержится s и $s \in N_y$ для некоторого y из последовательности $A(s_1, P)$. Ясно, что A' является перестановочным автоматом без потери информации, для которого достигается доказываемая нижняя оценка.

Рассмотрим теперь случай $W(s_1, P) > 1$. При $L = N(A(s_1, P))$ утверждение доказано. Допустим, что $L < N(A(s_1, P))$. Пусть $P = x(1), x(2), \dots, x(k), \dots$ и

$$A_M(s_1, P) = \{s_1, s_2, \dots, s_k, \dots\}, \quad s_{k+1} = h_{x(k)} h_{x(k-1)} \dots h_{x(1)} s_1, \quad k = 0, 1, \dots$$

Выберем $k \in \{0, 1, \dots, W(s_1, P) - 1\}$ так, чтобы $s_k \in N_y$, $|N_y| = N(A(s_1, P))$. Определим новый автомат A' следующими условиями: A' отличается от A только выходным алфавитом $Y' = Y \cup z$, где z — некоторый символ, $z \in Z$, и выходной функцией λ' , определенной условиями $\lambda'(s) = \lambda(s)$, если s находится в наборе состояний $(s_{1+k+jW} : j \in \{0, 1, \dots, L - 1\})$, $W = W(s_1, P)$ или $s \notin N$ для каждого y из выходной последовательности $A(s_1, P)$ автомата A . В противном случае, полагаем $\lambda'(s) = z$.

Непосредственно проверяется, что A' — перестановочный автомат без потери информации, для которого

$$W(s_1, P) = \frac{\Omega(s_1, P)}{N(A(s_1, P))}.$$

Перейдем теперь к доказательству достижимости верхней оценки периода $W(s_1, P)$. Рассмотрим произвольный перестановочный автомат Мура A без потери информации, для которого отображение $\lambda: S \rightarrow Y$, осуществляемое функцией выхода λ , сюръективно. Предположим, что $|Y| = |S|$. Тогда отображение λ взаимно однозначно. Из доказательства утверждения 2 теоремы 4 следует, что

$$\frac{\Omega(s_1, P)}{W(s_1, P)} = L = 1,$$

и следовательно, в этом случае утверждение теоремы 5 относительно верхней оценки доказано.

Пусть теперь $|Y| < |S|$. Если $W(s_1, P) = \Omega(s_1, P)$, то теорема 5 верна, в противном случае определим новый автомат A' , отличающийся от A выходным алфавитом $Y' \in Y \cup z$, $z \notin Y$ и выходной функцией λ' , удовлетворяющей условиям $\lambda'(s_1) = z$, $\lambda'(s) = \lambda(s)$, $s \in S$, $s \neq s_1$.

Очевидно, что A' — перестановочный автомат без потери информации, для которого $W(s_1, P) = \Omega(s_1, P)$. Теорема 5 полностью доказана.

7. Периоды выходных последовательностей последовательного соединения автономного автомата с перестановочным автоматом без потери информации

Рассмотрим приложения полученных в разделе 5 результатов к задаче оценки периодов выходных последовательностей и мощностей классов неотличимых состояний перестановочных автоматов, представимых последовательным соединением приведенного автономного автомата с неавтономным перестановочным автоматом без потери информации. Для последовательного соединения автоматов используем обозначения раздела 4. Пусть $A_1 = (S_1, Y_1, h, \lambda)$ — приведенный полноцикловой автомат с множеством состояний S_1 , $|S_1| > 1$, выходным алфавитом Y_1 , $|Y_1| > 1$, а $A_2 = (X, S_2, Y_2, h, f)$, $Y_1 = X$, — перестановочный автомат без потери информации. Напомним, что функция выхода автономного последовательного соединения $C = A_1 \rightarrow A_2 = (S_1 \times S_2, Y_2, h^{1,2}, f^{1,2})$ автоматов A_1, A_2 определена функцией выхода автомата A_2 .

Для $s(1) \in S_1$, $s(2) \in S_2$ обозначим через $W(s(1), s(2))$ период выходной последовательности автомата $C = A_1 \rightarrow A_2$, соответствующей его начальному состоянию $(s(1), s(2))$, а через $A_1(s(1))$ — выходную последовательность автомата A_1 , отвечающую начальному состоянию $s(1) \in S_1$. Из приведенных в разделе 5 результатов непосредственно вытекает теорема 6.

Теорема 6. *В указанных выше условиях*

$$W(s(1), s(2)) \geq \frac{|S_1|}{N(C(t, s))},$$

где $N(C(t, s))$ — множество минимальной мощности в совокупности множеств N_y по всем y из выходной последовательности автомата $C(s(1), s(2))$, отвечающей его начальному состоянию $s(1), s(2)$.

Напомним и введем некоторые новые обозначения:

$L(s(1), s(2))$ — связная компонента графа перехода автомата C , содержащая состояние $(s(1), s(2))$;

$C(s(1), s(2))$ — выходная последовательность автомата C , отвечающая его начальному состоянию $(s(1), s(2))$;

$W(s(1), s(2))$ — период выходной последовательности $C(s(1), s(2))$;

$A_1(s(1))$ — выходная последовательность автомата A_1 при начальном состоянии $s(1) \in S_1$;

$\omega(A_1(s(1)))$ — период выходной последовательности $A_1(s(1))$ автомата A_1 при начальном состоянии $s(1) \in S_1$;

$W(s(2), A_1(s(1)))$ — период выходной последовательности автомата A_2 , отвечающей входной периодической последовательности $A_1(s(1))$ и начальному состоянию $s(2)$;

$\Omega(s(2), A_1(s(1)))$ — грубый период последовательности состояний перестановочного автомата A_2 для входной периодической последовательности $A_1(s(1))$ и начального состояния $s(2) \in S_2$.

Теорема 7. Мощности классов неотличимых состояний автомата $C = A_1 \rightarrow A_2$ ограничены сверху величиной $|S_1| \max\{|N_y|\}_{y \in Y}$.

Доказательство. Очевидны равенства

$$\omega(A_1(s(1))) = |S_1|, \quad W(s(1), s(2)) = W(s(2), A_1(s(1))), \\ |L(t, s)| = \Omega(s(2), A_1(s(1))).$$

Так как A — автомат без потери информации, из этих равенств следует, что

$$W(s(1), s(2)) \geq \frac{L(s(1), s(2))}{\max\{|N_y|\}_{y \in Y}}.$$

С другой стороны, $W(s(1), s(2))$ есть число классов неотличимых состояний связной компоненты автомата C , содержащей состояние $(s(1), s(2))$. Поэтому, если $d(s(1), s(2))$ — мощность классов неотличимых состояний этой компоненты, то

$$d(s(1), s(2)) = \frac{|L(s(1), s(2))|}{W(s(1), s(2))} \leq \frac{|L(s(1), s(2))| \max\{|N_y|\}_{y \in Y}}{|L(s(1), s(2))|},$$

то есть

$$d(s(1), s(2)) \leq \max\{|N_y|\}_{y \in Y}.$$

Теперь утверждение теоремы 7 следует из того, что каждый класс неотличимых состояний автомата C представляет собой объединение некоторых классов неотличимых состояний его связных компонент, причем число связных компонент автомата C не превосходит $|S_1|$.

Теорема 8. Пусть

$$|S_1| > \max\{|N_y|\}_{y \in Y}.$$

Тогда $(W(s(1), s(2)), |S_1|) \neq 1$ для любого состояния $(s(1), s(2))$ автомата C .

Доказательство. Пусть $(W(s(1), s(2)), |S_1|) = 1$. Равенство $|L(s(1), s(2))| = C|S_1|$ справедливо для некоторого целого $C = C(s(1), s(2))$, поэтому из соотношения

$$d(s(1), s(2)) = \frac{|L(s(1), s(2))|}{W(s(1), s(2))} \leq \max_{y \in Y}\{|N_y|\}$$

следует, что $|S_1| \leq \max\{|N_y|\}_{y \in Y}$, получаем противоречие условию теоремы 8.

Следствие 7. Пусть $|S_1|$ — простое число и $|S_1| > \max\{|N_y|\}_{y \in Y}$. Тогда

- (1) для любого состояния $(s(1), s(1)) \in S_1 \times S_2$ периоды $W(s(1), s(2))$ выходных последовательностей $C(s(1), s(2))$ автомата $C = A_1 \rightarrow A_2$ кратны $|S_1|$,
- (2) мощности классов неотличимых состояний автомата $C = B \Rightarrow A$ ограничены сверху величиной $|S_2|$.

Доказательство. Утверждение 1 непосредственно вытекает из теоремы 8.

Докажем утверждение 2. Пусть $L_j = D_j|S_1|$, $j \in \{1, 2, \dots, m\}$ — мощности связанных компонент графа перехода автомата C . Тогда мощности классов неотличимых состояний этих связанных компонент имеют вид k_j , где k_j делит $|D_j|$, $j \in \{1, 2, \dots, m\}$. Следовательно, так как

$$\sum_{j=1}^m k_j \leq \sum_{j=1}^m D_j = |S_2|,$$

мощности классов неотличимых состояний ограничены сверху величиной $|S_2|$.

Замечание 1. При получении выше приведенных результатов перестановочность автомата A использовалась для доказательства наличия входного слова $M = \{x''(1), \dots, x''(n)\}$, переводящего приемник $h_{x(k)}h_{x(k-1)} \dots h_{x(1)}s$ состояния $s \in S$ в состояние s . В связи с этим, аналогичные результаты, видимо, можно получить и для сильно связанных автоматов A . При этом необходимо учесть специфику возможной небиjectивности преобразований вида $h_{x(k)}h_{x(k-1)} \dots h_{x(1)}$ автомата A , в частности, необходима корректировка понятия грубого периода последовательности состояний автомата A при его начальном состоянии и входной периодической последовательности.

Автор благодарен М. М. Глухову за внимание к работе и полезные замечания.

Список литературы

1. Трахтенброт Б. А., Барздин Я. М., *Конечные автоматы (поведение и синтез)*. Наука, Москва, 1970.
2. Burks A. W., Wright J. B., Theory of logical nets. *Proc. IRE* (1953) **41**, 1357–1365.
3. Кобринский Н. Е., Трахтенброт Б. А., *Введение в теорию конечных автоматов*. Физматгиз, Москва, 1962.
4. Бабаш А. В., О периодичности последовательности состояний автомата, отвечающей его начальному состоянию и входной периодической последовательности. *Дискретная математика* (2002) **14**, №2, 54–64.
5. Hibbard T. H., Least upper bounds on minimal terminal state experiments for two classes of sequential machines. *J. Assoc. Comput. Mach.* (1961) **8**, 601–612.
6. Гилл А., *Введение в теорию конечных автоматов*. Наука, Москва, 1966.
7. Коршунов А. Д., О верхней оценке длин кратчайших однородных экспериментов по распознаванию заключительного состояния для почти всех автоматов. *Докл. АН СССР* (1969) **184**, 28–29.
8. Коршунов А. Д., Об асимптотических оценках числа приведенных конечных автоматов. *Дискретный анализ* (1966) **6**, 35–50.
9. Babash A. V., Isoperiods of output sequences of automata. In: *Probabilistic Methods in Discrete Mathematics* (Kolchin V. F. et al., eds.). VSP, Utrecht, 2002, pp. 147–158.

Статья поступила 11.06.2006.

Переработанный вариант поступил 15.10.2008.