Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Российский экономический университет имени Г. В. Плеханова»
(ФГБОУ ВО «РЭУ им. Г. В. Плеханова»)

А. В. Бабаш

ТЕОРИЯ АВТОМАТОВ.
АНАЛИЗ ШИФРУЮЩИХ АВТОМАТОВ

Утверждено издательским советом университета
в качестве учебного пособия

Москва
ФГБОУ ВО «РЭУ им. Г. В. Плеханова»
2021

УДК 519.713(075.8)
ББК 22.18я73
Б121

Рецензенты: д-р техн. наук, проф. В. А. С к и б а (ВА РВСН им. Петра Великого); д-р техн. наук, проф. В. А. С и з о в (РЭУ им. Г. В. Плеханова)

Бабаш, А. В.

Б121 Теория автоматов. Анализ шифрующих автоматов : учебное пособие / А. В. Бабаш. – Москва : ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2021. – 296 с.
ISBN 978-5-7307-1736-7

Данное пособие содержит методический материал для инновационных курсов лекций по профилю «Криптографическая защита информации» и может быть использовано при изучении блока дисциплин этого профиля. Ряд представленных результатов полезен аспирантам и специалистам, специализирующимся в указанной области.

Для студентов, обучающихся по направлениям «Прикладная информатика» и «Информационная безопасность».

УДК 519.713(075.8)
ББК 22.18я73

ISBN 978-5-7307-1736-7
© ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Целью данного пособия является изложение новых методов анализа шифров на основе теоретико-автоматных обобщений. Ниже приведены те обозначения, сокращения и определения, с которые помогут читателю в освоении материала.

Определения, обозначения и сокращения

Для множества Z, состоящего из элементов 1, 2, …, k используется обозначение $Z = \{1, 2, \ldots, k\}$.

Далее:

$X \times Y$ – декартовым произведением множеств X и Y;

X^k – множество слов в алфавите X длины k;

$|M|$ – мощность множества M;

$h(M')$ – образ подмножества $M' \subseteq M$ для отображения $h: M \to V$. Часто мы будем опускать скобки и писать hM', а для элемента $m \in M$ будем писать $h(m)$ или hm.

Под словом *автомат* подразумевается конечный автомат $A = (X, S, Y, h, f)$, где

X – конечное непустое множество, названное множеством входных символов (входной алфавит);

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

S – конечное непустое множество, названное множеством состояний (внутренний алфавит);

Y – конечное непустое множество, названное множеством выходных символов (выходной алфавит);

$h: S \times X \to S$ – функция переходов;

$f: S \times X \to Y$ – функция выхода.

Если в момент времени $t = 1, 2, \ldots$ автомат A находится в состоянии $s(t) \in S$ и на его вход поступил символ $x(t) \in X$, то в этот же момент времени на выходе автомата A образуется символ $f(s(t), x(t))$ и автомат A переходит в новое состояние $s(t+1) = h(s(t), i(t))$.

При условии, что $f(s, x) = \lambda(s)$ для любых $x \in X$, $s \in S$, где $\lambda: S \to Y$, автомат Мили A может рассматриваться как автомат Мура и будет обозначатся через

$$A = (X, S, Y, h, \lambda).$$

Если X состоит из одного элемента $|X| = 1$, то такой автомат называется автономным, и обозначается через $A = (S, Y, h, \lambda)$.

Автомат часто задают его графом переходов: вершинами графа являются состояния автомата. Из каждого состояния s и каждого $x \in X$ проводится ориентированная дуга (стрелка) в состояние $s` = h(x, s)$. Она помечается двумя символами (x, y), где $y = f(x, s)$. Таким образом, из каждого состояния выходят $|X|$ дуг.

Говорят, что состояние s` *достижимо из* s в автомате A, если в его графе переходов существует ориентированный путь из s в s`. Для таких пар состояний (s, s`) можно ввести минимальное расстояние m(s, s`) от s до s` как минимальное число дуг, по которым можно перейти из s в s`.

Автономный автомат $A = (S, Y, h, \lambda)$ называют полноцикловым, если его граф состоит из цикла, содержащего все его состояния.

Граф переходов автомата (автомат) называют **сильно связным**, если для любой пары упорядоченных его состояний (s, s`) существует ориентированный путь из s в s`. В любом связном автомате можно выделить сильно связный подавтомат автомата.

Нам удобно зачастую использовать несколько другое обозначение автомата $A = (X, S, Y, h, f)$.

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

$h_x: S \to S$, $h_x(s) = h(x, s)$; $f_x: S \to Y$, $f_x(s) = f(x, s)$.

Новое обозначение автомата A имеет вид:

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

Итак:

$h_x: S \to S$ – частичная функция переходов автомата A, соответствующая входному символу $x \in X$, задаваемая соотношением $h_x(s) = h(s, x)$, $s \in S$ (для удобства ниже в этой записи мы опускаем скобки при h_x: $h_x s = h(s, x)$;

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

$f_x: S \to Y$ – частичная функция выхода, соответствующая входному символу $x \in X$, задаваемая соотношением $f_x(s) = f(s, x)$, $s \in S$ (для удобства ниже в этой записи мы опускаем скобки при f_x : $f_x s = f(s, x)$).

Необходимо помнить, что *слово в каком-либо алфавите мы пишем, отделяя буквы запятыми.*

Используются знаки, обозначающие:

$\Rightarrow$ – тогда;

$\Leftrightarrow$ – тогда и только тогда;

$\exists$ – если существует (существуют);

$\forall$ – для любого (любых);

: – для которого (которых) выполняется.

Используются дополнительные обозначения:

– P = x(1), x(2), …, x(k), x(j)∈X, j∈{1, 2, …, k} – входное слово длины k автомата A; в ряде случаев, например, чтобы отличить обозначение вероятности P, мы используем и другие обозначения, в частности обозначение: $\Im$ = x(1), x(2), …, x(k) или J = x(1), x(2), …, x(k);

– |P| – длина входного слова P автомата A;

– $h_P = h_{x(k-1)}\, h_{x(k-2)} \ldots h_{x(1)}$ – отображение S→S, осуществляемое автоматом A в результате приложения к нему входного слова P = x(1), x(2), …, x(k);

– каждое состояние вида $h_x(s)$ называется 1-приемником состояния s;

– состояние вида $h_{x(k)}\, h_{x(k-1)} \ldots h_{x(1)}\,(s)$ называется k-м преемником состояния s;

– $f_P = f_{x(k)}\, h_{x(k-1)}\, h_{x(k-1)} \ldots h_{x(1)}$ – отображение S→Y, осуществляемое автоматом A в результате приложения к нему входного слова P = x(1), x(2), ..., x(k);

– f_Ps или P(s) – заключительное состояние автомата, полученное с начального состояния s при вводном слове (последовательности) P;

– A(s, P) = y1, y2, ..., yk, yi∈Y, j∈[1, k] – выходное слово автомата A, полученное в результате приложения входного слова P = = x(1), x(2), …., x(k) к автомату A с начальным состоянием s∈S;

– AM(s, P) = s1, s2, …, sj, … – последовательность состояний автомата A = (X, S, Y, h, f), отвечающая его входной последовательности P и начальному состоянию s = s1 из S;

– полугруппа G = < (hx)x∈X > автомата A – это полугруппа отображений множества S в себя, порожденная частичными функциями перехода (hx)x∈X автомата A и тождественным отображением S в себя;

– автомат A называют перестановочным, если его частичные функции переходов (hx)x∈X осуществляют взаимно однозначные отображения S в S, и говорят также: биекции S в S, (подстановки на S).

Имея дело с несколькими автоматами, будем отмечать пятерки X, S, Y, h, f различными символами (верхними и нижними), например, A = (X_A, S_A, Y_A, h_A , f_A). Если же автомат обозначается символом A с каким-ни будь индексом, например A’, то иногда для простоты мы будем помечать элементы его пятерки тем же индексом, например, (X’, S’, Y’, h’, f’). Аналогичным образом мы будем поступать и для различения введенных параметров автоматов, например, полугруппу автоматов A и B удобно обозначать соответственно через G_A и G_B.

Напомним следующие основные понятия.

Определение 1. Состояние s и s’ автомата A называется k-неотличимыми, если

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

для любого входного слова P = x(1), x(2), …, x(k) длины k автомата A. В противном случае они называются k-различимыми.

Определение 2. Состояния s и s’ автомата A называются неотличимыми, если они k-неотличимы для любого k. В противном случае они называются различными (отличными).

Хорошо известна теорема 1 [6, 10]. Для неотличимости двух состояний автомата A = (X, S, Y, h, f) достаточна их (│S│– 1)-неотличимость.

Поскольку бинарное отношение k-неотличимости состояний автомата является отношением эквивалентности, все множество состояний S автомата A разбивается на непересекающиеся классы k-неотличимых состояний.

Будем обозначать это разбиение через:

$N^k = N_1^k, N_2^k, \ldots, N_{l_k}^k$,

где N_j^k, j є [1, l_k] – классы k-неотличимых состояний автомата A, l_k – число классов k-неотличимых состояний автомата A. Классы неотличимых состояний автомата A будем обозначать через N_j , j є [1; l], а само разбиение множества S эти классы через:

N = (N_1, N_2, …., N_l),

l – число классов неотличимых состояний автомата A.

Определение 3. Число R называется степенью различимости автомата A, если

$N^R = N$ и $N^k \neq N$ при $k<R$.

Определение 4. Автомат A называется приведенным (или находится в приведенной форме), если $|N_j| = 1$ для любого $j \in [1; l]$.

Очевидно, если A – приведенный автомат, то $l = |S|$.

Часть 1. ЭКСПЕРИМЕНТЫ С АВТОМАТАМИ

В данной части работы напоминаются основные понятия, связанные с экспериментами с автоматами, вводятся их обобщения и решаются задачи по определению входных слов автомата по различным известным данным (по выходной последовательности, множеству пар начальных и заключительных состояний и др.). Основной целью является построение новых методов криптоанализа на основе обобщений известных результатов по экспериментам с автоматами.

Глава 1. ОПРЕДЕЛЕНИЕ ЗАКЛЮЧИТЕЛЬНЫХ СОСТОЯНИЙ АВТОМАТА ПО ВХОДНОЙ И ВЫХОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТЯМ. АВТОМАТЫ С КОНЕЧНОЙ ПАМЯТЬЮ

Излагаются основные свойства автоматов с конечной памятью. Материалы главы 1 базируются на работах [24; 56; 58].

1.1. Основные понятия

Условимся говорить, что пара слов (P, R) является вход-выходной парой слов автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$, если найдется состояние $s \in S$, при котором

$$A(s, P) = R.$$

Определение 1. Автомат A называют автоматом с конечной памятью, если найдутся целые числа μ_1, μ_2, $0 \le \mu_1$, $1 \le \mu_2$ и функция g от $\mu_1+\mu_2+1$ переменных, при которых для любой вход-выходной пары слов $(x_1, x_2, \ldots, x_k, \ldots; y_1, y_2, \ldots, y_k, \ldots)$ автомата A выполняется равенство

$$y_j = g(x_j, x_{j-1}, \ldots, x_{j-\mu_1}; y_{j-1}, y_{j-2}, \ldots, y_{j-\mu_2}). \qquad (1)$$

Таким образом, у автомата с конечной памятью j-й выходной знак зависит от j-го входного символа, предыдущих μ_1 входных символов и от предыдущих μ_2 выходных символов. Следует отметить, что некоторые переменные из $\mu_1+\mu_2+1$ переменных могут быть несущественными переменными функции g: $X^{\mu_1+1} \times Y^{\mu_2} \to Y$. Соотношение (1) называют *характеристическим уравнением* автомата A и

считают, что хотя бы одна из переменных x_j, x_{j-1}, …, $x_{j-\mu 1}$ является существенной переменной.

Обычно для автоматов с конечной памятью решают следующую задачу. Известно характеристическое уравнение автомата A. Построить автомат A’ = (X, S’, Y, $(h'_x)_{x\in X}$, $(f'_x)_{x\in X}$), у которого множество всех вход-выходных пар слов содержит множество всех вход-выходных пар слов автомата A. Построение проводят следующим образом. Состояниями автомата A’ являются наборы значений переменных x_{j-1}, …, $x_{j-\mu 1}$, y_{j-1}, y_{j-2}, …, $y_{j-\mu_2}$, $S' = X^{\mu_1} \times Y^{\mu_2}$. Равенство (1) переписывают в виде

$$y_j = g(x_j, s_j). \qquad (2)$$

Тогда для $x \in X$ частичная функция выхода f'_x автомата A’ записывается в виде

$$f'_x s = g(x, s).$$

Из определения состояний автомата A’ следует, что если

$s_j = (x_{j-1}, \ldots, x_{j-\mu 1}, y_{j-1}, y_{j-2}, \ldots, y_{j-\mu_2})$,

то

$s_{j+1} = (x_j, x_{j-1}, \ldots, x_{j-\mu 1+1}, y_j, y_{j-1}, y_{j-2}, \ldots, y_{j-\mu_2+1}) =$

$= (x_j, x_{j-1}, \ldots, x_{j-\mu 1+1}, g(x_j, x_{j-1}, \ldots, x_{j-\mu 1}, y_{j-1}, y_{j-2}, \ldots, y_{j-\mu_2}),$ $y_{j-1}, y_{j-2}, \ldots, y_{j-\mu_2+1})$.

Анализ последнего выражения в равенстве говорит о том, что s_{j+1} является значением некоторой функции F от переменных (x_j, x_{j-1}, …, $x_{j-\mu 1}$, y_{j-1}, y_{j-2}, …, $y_{j-\mu_2}$). Таким образом, формулу для s_{j+1} можно записать в виде $s_{j+1} = F(x_j, s_j)$. Тогда для $x \in X$ частичная функция выхода f'_x автомата A’ записывается в виде:

$$h'_x s = F(x, s).$$

Числа μ_1, μ_2 называют *памятью x и памятью y* автомата A, а величину $\mu = \max(\mu_1, \mu_2)$ называют *максимальной памятью* автомата A.

Уравнение (1) для некоторой функции G может быть записано в виде:

$$y_j = G(x_j, x_{j-1}, \ldots, x_{j-\mu}, y_{j-1}, y_{j-2}, \ldots, y_{j-\mu}). \qquad (3)$$

Если при этом для автомата A не существует характеристического уравнения с меньшим значением μ

$$y_j = \Phi(x_j, x_{j-1}, \ldots, x_{j-\mu+1}, y_{j-1}, y_{j-2}, \ldots, y_{j-\mu+1}),$$

то говорят, что *автомат A имеет память μ*.

Таким образом, для автомата А с памятью выходной j-й символ y_j определен однозначно входным j-м символом и μ предыдущими μ входными и выходными символами. Следовательно, для заданной входной последовательности в отвечающей ей выходной последовательности символы все символы после μ-того символа определены однозначно.

1.2. Свойства автоматов с конечной памятью

Теорема 1. В приведенном автомате А с памятью μ для его вход-выходных последовательностей выполняется:

$s_j = g(x_{j-1}, x_2, \ldots, x_{j-\mu}, y_{j-1}, y_{j-2}, \ldots, y_{j-\mu})$.

Доказательство. Предположим обратное. Существует вход-выходное слово $(x_{j-1}, x_{j-2}, \ldots, x_{j-\mu}, y_{j-1}, y_{j-2}, \ldots, y_{j-\mu})$, которое не определяет однозначно заключительное состояние s_j. То есть существуют начальные состояния s_1, s_2, при которых

$A(s_1, x_{j-\mu}, \ldots, x_{j-2}, x_{j-1}) = y_{j-\mu}, \ldots, y_{j-2}, y_{j-1}$;

$A(s_2, x_{j-\mu}, \ldots, x_{j-2}, x_{j-1}) = y_{j-\mu}, \ldots, y_{j-2}, y_{j-1}$

и

$h_{xj-1, xj-2, \ldots, xj-\mu}\, s_1 \neq h_{xj-1, xj-2, \ldots, xj-\mu}\, s_2$.

Так как автомат А – приведенный, то для различных состояний

$$h_{xj-1, xj-2, \ldots, xj-\mu}\, s_1;\ h_{xj-1, xj-2, \ldots, xj-\mu}\, s_2\,,$$

существует входное слово $i_j, i_{j+1}, \ldots, i_{j+n}$ длины не меньше 1, при котором выходные слова

$A(h_{xj-1, xj-2, \ldots, xj-\mu}\, s_1, i_j, i_{j+1}, \ldots, i_{j+n}) = y_j, y_{j+1}, \ldots, y_{j+n-1}, y_{j+n}$

и

$A(h_{xj-1, xj-2, \ldots, xj-\mu}\, s_2, i_j, i_{j+1}, \ldots, i_{j+n}) = y_j, y_{j+1}, \ldots, y_{j+n-1}, y''_{j+n}$

отличаются лишь в последнем символе.

Автомат А является автоматом с конечной памятью μ, длины выходных последовательностей:

$A(s_1, x_{j-\mu}, \ldots, x_{j-2}, x_{j-1}, i_j, i_{j+1}, \ldots, i_{j+n}) = y_{j-\mu}, \ldots, y_{j-2}, y_{j-1}, y_j, y_{j+1}, \ldots, y_{j+n-1}, y_{j+n}$;

$A(s_2, x_{j-\mu}, \ldots, x_{j-2}, x_{j-1}, i_j, i_{j+1}, \ldots, i_{j+n}) = y_{j-\mu}, \ldots, y_{j-2}, y_{j-1}, y_j, y_{j+1}, \ldots, y_{j+n-1}, y''_{j+n}$

равны μ+n+1, поэтому последние n+1 выходных символов должны определяться однозначно. То есть пришли к противоречию с неравенством $y_{j+n} \neq y''_{j+n}$. Теорема доказана.

Теорема 2. Если для вход-выходных последовательностей автомата A при некотором μ выполняется $s_j = g(x_{j-1}, x_2, \ldots, x_{j-\mu}, y_{j-1}, y_{j-2}, \ldots, y_{j-\mu})$, то A является автоматом с памятью, не превосходящей μ.

Доказательство. При любом начальном состоянии s и входной последовательности $x_1, x_2, \ldots$ автомата A

$$y_j = h(s_j, x_j).$$

Следовательно,

$$y_j = h(s_j, x_j) = h(g(x_{j-1}, x_2, \ldots, x_{j-\mu}, y_{j-1}, y_{j-2}, \ldots, y_{j-\mu}), x_j)=$$
$$= f(x_j, x_{j-1}, x_2, \ldots, x_{j-\mu}, y_{j-1}, y_{j-2}, \ldots, y_{j-\mu})$$

для некоторой функции f. Поэтому память автомата A не превосходит μ.

В связи с предшествующими теоремами отметим следующее различие между произвольным автоматом и автоматом с конечной памятью. В любом приведенном автомате имеется, по крайней мере, одна установочная последовательность, которая, будучи приложенной к автомату, однозначно определяет его конечное состояние. В автомате с конечной памятью μ это справедливо для каждой входной последовательности длины μ или больше.

Теорема 3. Если $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ – приведенный автомат с конечной памятью μ, то

$$\mu \le \frac{|S|(|S|-1)}{2}.$$

Мы приведем основные идеи доказательства теоремы. По теореме 1 в приведенном автомате A с памятью μ для его вход-выходных последовательностей выполняется

$$s_j = g(x_{j-1}, x_2, \ldots, x_{j-\mu}, y_{j-1}, y_{j-2}, \ldots, y_{j-\mu}).$$

При этом для k меньших μ могут существовать вход-выходная последовательность $x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_k$ и разные начальные состояния s_1, s_2, при которых

$$A(x_1, x_2, \ldots, x_k, s_1) = A(x_1, x_2, \ldots, x_k, s_2) = y_1, y_2, \ldots, y_k, h_{x1, x2, \ldots, xk}\, s_1$$
$$= h_{x1, x2, \ldots, xk}\, s_2.$$

Так как μ выбрано минимальным, то должна существовать вход-выходная последовательность $x_1, x_2, \ldots, x_\mu, y_1, y_2, \ldots, y_\mu$ и разные состояния s_1, s_2 со свойствами:

$h_{x1}s_1 \ne h_{x1}s_2$, $h_{x2x1}s_1 \ne h_{x2x1}s_2$, $h_{x3x2x1}s_1 \ne h_{x3x2x1}s_2$, $\ldots$, $h_{x\mu-1, \ldots, x1}s_1 \ne$
$\ne h_{x\mu-1, \ldots, x1}s_2$,

$h_{x\mu, x\mu-1, \ldots, x1} \cdot s_1 = h_{x\mu, x\mu-1, \ldots, x1} \cdot s_1$.

Поэтому μ из указанного выше свойства не может превышать число различных пар состояний из S, которое равно величине

$|S|(|S|-1)$. Простейший дальнейший анализ показывает, что эту границу можно уменьшить до числа всех неупорядоченных пар различных состояний $\frac{|S|(|S|-1)}{2}$.

1.3. Алгоритм определения автоматов с конечной памятью

Пусть A = (X, S, Y, $(h_x)_{x\in X}$, $(f_x)_{x\in X}$) – конечный автомат. Требуется определить, является ли он автоматом с конечной памятью и если является, то определить его память.

Обозначим через $Q_k(s)$ – множество всех вход-выходных слов длины k, описываемых путями в графе переходов автомата A, заканчивающихся состоянием s. По теореме 1, если A является автоматом с конечной памятью μ, то для некоторых различных состояний s, s'

$$Q_{\mu-1}(s) \cap Q_{\mu-1}(s') \neq \varnothing$$

и для всех пар различных состояний

$$Q_{\mu}(s) \cap Q_{\mu}(s') = \varnothing.$$

По теореме 1, если A не является автоматом с конечной памятью, то $Q_t(s) \cap Q_t(s') \neq \varnothing$ при $t = \frac{|S|(|S|-1)}{2}$ для некоторых различных s, s'.

Эти выкладки позволяют предложить следующий алгоритм определения памяти заданного автомата A.

1) Полагаем k = 1.
2) Составляем все $Q_k(s)$, $s\in S$.
3) Если

а) $Q_k(s) \cap Q_k(s') \neq \varnothing$, для некоторых различных s, s', то переходим к 4);

б) $Q_k(s) \cap Q_k(s') = \varnothing$ при всех различных парах состояний s, s', то k является памятью автомата A.

4) Если

а) $k \leq \frac{|S|(|S|-1)}{2} - 1$, то увеличиваем k на 1 и возвращаемся к 2).

б) $k = \frac{|S|(|S|-1)}{2}$, то A не является автоматом с конечной памятью.

Глава 2. ОПРЕДЕЛЕНИЕ ВХОДНОГО СЛОВА АВТОМАТА ПО ЕГО НАЧАЛЬНОМУ СОСТОЯНИЮ И ВЫХОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ. АВТОМАТЫ БЕЗ ПОТЕРИ ИНФОРМАЦИИ

Решается задача распознавания неизвестной входной последовательности автомата по его начальному или заключительному состоянию и выходной последовательности. Материалы этой главы базируются на работах [24; 31; 33; 43; 46; 47].

2.1. Основные понятия

Пусть $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ – конечный автомат. Через $A(s, P)$ ($A_M(s, P)$) обозначим выходную последовательность (последовательность состояний) автомата A , отвечающую его входной последовательности P и начальному состоянию $s\in S$. Напомним ряд необходимых нам определений (например, [24; 31; 56]).

Определение 1. Состояние $s\in S$ автомата A называется состоянием с потерей информации, если существуют различные входные слова x(1), x(2), …, x(L) и x`(1), x`(2), …, x`(L) одинаковой длины $L = L_s$ $x(j), x`(j)\in X$, для которых выполнены соотношения

$$\begin{aligned}
&h_{x(L)}h_{x(L-1)}\ldots h_{x(1)}s = h_{x`(L)}h_{x`(L-1)}\ldots h_{x`(1)}s;\\
&f_{x(1)}s = f_{x`(1)}s; \qquad (1)\\
&f_{x(2)}h_{x(1)}s = f_{x`(2)}h_{x`(1)}s;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
&f_{x(L)}h_{x(L-1)}\ldots h_{x(1)}s = f_{x`(L)}h_{x`(L-1)}\ldots h_{x`(1)}s.
\end{aligned}$$

Если состояние $s\in S$ автомата A не является состоянием с потерей информации, то оно называется состоянием без потери информации. В графе переходов автомата A состояние s с потерей информации характеризуется существованием подграфа вида (рис. 1) при некотором натуральном L.

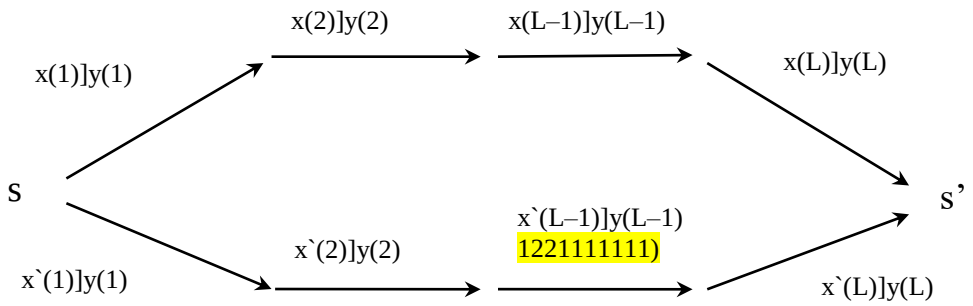

Рис. 1

Определение 2. Автомат A называется автоматом без потери информации, если любое его состояние является состоянием без потери информации. В случае *(каком? ином?)* автомат A называется автоматом с потерей информации.

Для входной последовательности $P = x_1, x_2, \ldots, x_k$ автомата A положим

$$h_P s = h_{xk} h_{xk-1} \ldots h_{x1} s.$$

Определение 3. Входная последовательность Q автомата A называется установочной, если из условий $A(s_1, Q) = A(s_2, Q)$ вытекает $h_Q s_1 = h_Q s_2$.

Далее для корректности формулировки приводимой ниже теоремы нам потребуется следующее утверждение.

Утверждение 1. Для приведенного автомата всегда существует установочная последовательность.

Доказательство. Для любой пары различных состояний (s_i, s_j) приведенного автомата A существует входное слово $P = P(s_i, s_j)$ длины, не превышающей величины $|S|-1$, при котором $A(s_i, P) \neq A(s_j, P)$. Пронумеруем все пары различных состояний автомата A. Наша задача состоит в том, чтобы построить входную последовательность T автомата A, при которой для каждой пары состояний (s_i, s_j) выполняется условие: либо $h_T s_i = h_T s_j$, либо $A(s_i, T) \neq A(s_j, T)$.

Последовательность T строим индуктивно. Для первой пары различных состояний (s_1, s'_1) найдем слово P_1, при котором $A(s_1, P_1) \neq A(s'_1, P_1)$. Это слово будет началом $T_1 = P_1$ искомой последовательности T. Для второй пары состояний (s_2, s'_2) найдем следующие приемники этих состояний $h(s_2, P_1)$, $h(s'_2, P_1)$. В случае $h(s_2, P_1) \neq h(s'_2, P_1)$ находим слово P_2, при котором $A(h(s_2, P_1), P_2) \neq A(h(s'_2, P_1), P_2)$. Конкатенацию P_1, P_2 слов P_1 и P_2 объявляем новым началом $T_2 = P_1, P_2$ искомой последовательности T и переходим к построению слова P_3. В случае когда $h(s_2, P_1) = h(s'_2, P_1)$, продолжение P_2 слова P_1 не строится и новым началом считается $T_2 = P_1$. Для построения продолжения P_3 начала T_2 слова T выбирается третья пара состояний (s_3, s'_3). Если $h(s_3, T_2) \neq h(s'_3, T_2)$, то находим слово P_3, при котором $A(h(s_3, T_2), P_3) \neq A(h(s'_3, T_2), P_3)$ и полагаем $T_3 = T_2, P_3$. Если же $h(s_3, T_2) = h(s'_3, T_2)$, то полагаем $T_3 = T_2$ и переходим к построению продолжения P_4 слова T_3. После обработки последней пары состояний получаем искомую установочную последовательность T.

2.2. Задача распознавания неизвестной входной последовательности автомата по его начальному состоянию и выходной последовательности

Неизвестная конечная входная последовательность $P = x_1, x_2, \ldots, x_k$ подается на приведенный автомат A с начальным состоянием $s \in S$. Наблюдается выходная последовательность $A(s, P) = R_1$ и автомат устанавливается в заключительное состояние $h_P s = h_{xk} h_{xk-1} \ldots h_{x1} s$. Затем на автомат A с начальным состоянием $h_P s$ подается установочная последовательность Q и наблюдается выходная последовательность $A(h_P s, Q) = R_2$. По известным данным: автомат A, начальное состояние $s \in S$, последовательности R_1, Q, R_2 – необходимо восстановить входную последовательность P.

Теорема 1. Для приведенного автомата A поставленная задача однозначно решается при любых парах (P, s) тогда и только тогда, когда автомат A – без потери информации.

Доказательство. Докажем необходимость условий теоремы. Предположим, что для начального состояния $s \in S$ приведенного автомата A без потери информации нашлись два различных слова P_1, P_2, являющихся решением задачи распознавания неизвестной входной последовательности автомата по его начальному состоянию и выходной последовательности. Тогда

$A(s, P_1) = A(s, P_2) = R_1$, $A(h_{P1} s, Q) = A(h_{P2} s, Q) = R_2$.

Следовательно,

$A(s, P_1, Q) = A(s, P_2, Q) = R_1, R_2$.

Так как Q – установочная последовательность, то $h_{P1Q} s = h_{P2Q} s$.

Таким образом, получаем, что начальное состояние $s \in S$ автомата A является состоянием с потерей информации, что противоречит условию.

Докажем достаточность условий теоремы. Предположим, что поставленная задача при заданных условиях имеет единственное решение при всех парах (P, s), а автомат A является автоматом с потерей информации. Тогда найдутся состояние $s \in S$ и пара различных входных слов V_1, V_2, для которых выполняется условие:

$A(s, V_1) = A(s, V_2) = R_1$,

$h_{V1} s = h_{V2} s$.

Для установочной последовательности Q имеем

$A(h_{V1} s, Q) = A(h_{V2} s, Q) = R_2$.

Таким образом, поставленная задача имеет по крайней мере два различных решения V_1, V_2, что противоречит начальному предположению.

Алгоритм определения входного слова автомата состоит в следующем. Строятся все возможные слова Pi, для которых $A(s, Pi) = R_1$. Устанавливается взаимно-однозначное соответствие между множеством всех слов Pi и множеством заключительных состояний $h_{Pi}s$ (так как автомат A является автоматом без потери информации). Устанавливается взаимно-однозначное соответствие между множеством выходных последовательностей $A(h_{Pi}s, Q)$ и множеством заключительных состояний $h_{PiQ}s$. Истинное состояние h_Ps среди всех возможных $h_{Pi}s$ определяется по заключительному состоянию $h_{PO}s$, найденному по наблюдаемой выходной последовательности $A(h_Ps,Q)$.

Представляют интерес решения следующих задач:

1. Описание автоматов, обладающих свойством: существуют натуральное число k и функция F_k, для которой

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

при любом входном слове P длины k и любом начальном состоянии s автомата.

2. Описание неприведенных автоматов с наличием установочной последовательности.

2.3. Автоматы без потери информации конечного порядка[1]

Понятие автомата без потери информации конечного порядка возникает в связи с вопросом, в каких случаях можно хотя бы неполностью восстановить входное слово, при подаче которого в данном начальном состоянии автомат выдал данное выходное слово. Предыдущий вопрос можно немного изменить и исследовать возможность неполного восстановления входного слова при условии, что известны выходное слово и состояние, в которое автомат A пришел при выдаче этого выходного слова. Оба вопроса впервые исследовались Д. Хаффмэном [46; 47]. Однако в его работах основное внимание уделялось полному восстановлению входного слова. Если для полного восстановления входного слова потребовалось знание начального состояния, то автомат был

[1] *Источник*: [33].

назван *автоматом без потери информации I класса*. Если требовалось знание состояния, в которое автомат пришел после выдачи выходного слова, то такой автомат был назван *автоматом без потери информации II класса.*

Хаффмэн рассматривал также такое обобщение понятия автомата без потери информации I класса, при котором входное слово можно восстановить только с некоторой задержкой (то есть для восстановления входного слова, состоящего из N букв, требуется выходное слово, содержащее более N букв). Такие автоматы названы автоматами без потери информации конечного порядка.

Вопросы распознавания того, является ли данный автомат одним из вышеперечисленных, Хаффмэном систематически не исследовались. Более систематические исследования проводил Ш. Ивен [31; 43]. Однако в его работах, по мнению А. А. Курмита, встречается ряд неточностей, а многие важные вопросы вовсе не затрагиваются [33].

Вводимые в этой главе понятия содержатся в [33] и являются обобщениями понятий, введенных Хаффмэнем.

Определение 4. Автомат A называется автоматом без потери информации I типа конечного порядка N (БПИ-I-N), если

$$A(s, x_1, x_2, \ldots, x_{N+1}) \neq A(s, x'_1, x'_2, \ldots, x'_{N+1})$$

для любых $s \in S$, любых различных x_1, x'_1 и любых $x_2, \ldots, x_{N+1}$ и $x'_2, \ldots, x'_{N+1}$ из X^N.

Автомат A называется автоматом без потери информации I типа *строго* порядка N (БПИ-1-N), если A является автоматом БПИ-I-N, но не является автоматом БПИ-I-N-1.

Определение 5. Автомат A называется *автоматом без потери информации II типа конечного порядка N* (БПИ-II-N), если

$$A(s, x_1, x_2, \ldots, x_{N+1}) \neq A(s', x'_1, x'_2, \ldots, x'_{N+1})$$

для любого состояния s” и любых состояний s, s’и слов $x_1, x_2, \ldots, x_{N+1}, x'_1, x'_2, \ldots, x'_{N+1}$ таких, что $h_{x1, x2, \ldots, xN+1}s = h_{x'1, x'2, \ldots, x'N+1}s' = s''$ при выполнении хотя бы одного из условий:

$h_{x1, x2, \ldots, xN}s \neq h_{x'1, x'2, \ldots, x'N}s'$

или

$x_{N+1} \neq x'_{N+1}$.

Автомат A называется автоматом без потери информации II типа *строго* порядка N (БПИ-II-N), если A является автоматом БПИ-II-N, но не является автоматом БПИ-II-N-1.

При исследовании автоматов БПИ-II-N ограничиваются рассмотрением таких автоматов, что для каждого состояния s существуют состояние s'и входная буква x такие, что $h_x s = s'$. На основании определения 4 нетрудно показать, что в случае автомата БПИ-I-N для любого состояния автомата A и любого выходного слова длины N+1, выданного автоматом A в этом состоянии, можно восстановить первую букву соответствующего входного слова. В случае автомата без потери информации I типа *строго* порядка N автомат имеет такое состояние и выходное слово длины N+1, выданное автоматом в этом состоянии, что на основании только этих данных невозможно однозначно восстановить больше одной начальной буквы входного слова. Аналогично из определения 5 следует, что в случае автомата БПИ-II-N на основании известного выходного слова длины N+1 и состояния, в которое автомат пришел непосредственно после выдачи этого слова, можно восстановить последнюю букву входного слова. Известные результаты по распознаванию автоматов БПИ-I-N, БПИ-II-N содержатся в [33].

Глава 3. ОБ ЭКСПЕРИМЕНТАХ ПО РАСПОЗНАВАНИЮ ИНФОРМАЦИИ О ВХОДНОМ СЛОВЕ АВТОМАТА

В главе вводится понятие закрытого однородного эксперимента с автоматом [14]. Решаются задачи частичного определения входного слова автомата по значениям некоторой функции от его входного слова и начального, или заключительного, состояния. Будем использовать следующие *обозначения*: A = (X, S, Y, h, f) – конечный автомат; X* – множество всех слов конечной длины алфавита X; $\Leftrightarrow$ – тогда и только тогда; $\Rightarrow$ – тогда; $\exists$ – существует; $\forall$ – для любого; $\vee$ – или; $\in$ – принадлежит.

3.1. Понятие закрытого однородного эксперимента с автоматами[1]

Для конечного автомата A = (X, S, Y, h, f) и натурального числа к обозначим через $R_к$, $T_к$ некоторые конечные множества. Рассмотрим сюрьективные отображения:

[1] *Источник*: [14, 31].

$$H_к: S \times X^к \to T_к,$$
$$П_к: S \times X^к \to R_к.$$

Полагаем, что на автомат A с начальными состояниями s из S подаются входные слова $P \in X^к$. При этом пары $(s, P) \in S \times X^к$, при которых функционирует автомат, неизвестны. Для каждой пары $(s, P) \in S \times X^к$ известен $t = H_к(s, P)$ – элемент наблюдения для пары (s, P). Целью эксперимента является **определение информации об элементе** $r = П_к(s, P)$, где r – значение исследуемого (искомого) параметра функционирования автомата A с начальным состоянием s при входном слове P. Под информацией о неизвестном элементе r понимается указание собственного подмножества R` множества $R_к$, в котором содержится r. Формально считаем, что задана некоторая функция $U_к$ на $R_к$ и ее значение $U_к(r) = j$ и определяет подмножество $R` = \{r`: r` \in R, U_к(r`) = j\}$ (укрупненное состояние). Считаем, что определение j (или, что то же самое, определение подмножества R`) проводится по известному элементу наблюдения $t = H_к(s, P)$. Формально полагаем, что имеется функция $Ф_к$, значение $Ф_к(t)$ которой и задает j. Таким образом, для фиксированного $(s, P) \in S \times X^к$ имеем:

$r = П_к(s, P)$ – значение исследуемого параметра для тройки (к, A, (s, P));

$t = H_к(s, P)$ – элемент наблюдения для тройки (к, A, (s, P));

$Ф_к$ – информационная функция наблюдения, $U_к$ – целевая информационная функция;

$Ф_к(t) = U_к(r) = j$,

то есть

$Ф_к(H_к(P, s)) = U_к(П_к(P, s)) = j$.

Пример 1. Диагностический эксперимент. Пусть слово $P \in X^к$ – диагностическая последовательность автомата A. В этом случае в качестве объекта наблюдения выступает t = (P, A(s, P)) – входное слово P и выходное слово A(s,P), полученное с неизвестного состояния $s \in S$ автомата A, то есть $H_к(s, P) = (P, A(s, P))$. В качестве r выступает начальное состояние s автомата A, то есть $r = П_к(s, P) = s$. Выполнение условия

$$Ф_к(H_к(s, P)) = U_к(П_к(s, P)), \text{ то есть } Ф_к(P, A(s, P)) = U_к(s) \qquad (1)$$

трактуется так: по значению функции $Ф_к$ от входной последовательности P и выходной последовательности A(s, P) однозначно находится значение функции $U_к$ от начального состояния s. Поло-

жим теперь дополнительно, что $U_к$ – тождественное отображение. Тогда (1) запишется в виде

$$\Phi_к(P, A(s, P)) = s. \qquad (2)$$

Условие «P – диагностическая последовательность для A» равносильно условию «Существует непостоянная функция $\Phi_к$, для которой справедливо равенство (2) при любом $s \in S$». Потребуем дополнительно, чтобы это равенство выполнялось и для любого $P \in X^к$. Если для автомата A выполнены указанные условия, то автомат таков, что любая последовательность $P \in X^к$ является для него диагностической. Описание таких автоматов представляет определенный криптографический интерес.

Пример 2. Для задачи построения установочного эксперимента в введенных терминах получается формулировка новой задачи, аналогичная примеру 1.

Условие неизвестности пары $(P, s) \in X^к \times S$ *для автомата A, при которой наблюдается элемент наблюдения t, мы формулируем как условие закрытости эксперимента.*

Нас будет интересовать класс автоматов, для которых *условие* $\Phi_к(H_к(s, P)) = U_к(\Pi_к(s, P))$ *выполняется при любой паре* $(s, P) \in S \times X^к$ *(как это было в примерах).* Это требование мы формулируем как условие *однородности закрытого эксперимента.*

Исследование поставленной задачи *в случае постоянных функциях* $\Phi_к$, $U_к$ не дает содержательной информации о значение исследуемого параметра r при наблюдении t. Поэтому в дальнейшем для *функций* $H_к$, $\Pi_к$ *будем искать* непостоянные *функции* $\Phi_к$, $U_к$.

Пример 3. Пусть $T_к \subseteq S \times Y^к$, $R_к = X$. Наблюдаем пары: начальное состояние s и выходное слово A(s, P) автомата A, то есть $H_к(s, P) = t = (s, A(s, P))$. Пусть $\Pi_к(P, s) = r = p(1)$ – первый элемент p(1) входного слова $P = p(1), \ldots, p(к)$. С помощью закрытого эксперимента определяется информация об элементе $r = p(1)$ по известному наблюдению $t = (s, A(s, P))$. Потребуем однородность закрытого эксперимента, поставим задачу определения информации о начальном символе произвольного входного слова $P = x(1), \ldots, x(к)$ автомата A по любым известным парам: начальному состоянию s и выходному слову A(s, P)) из $S \times X^к$. Для решения этой задачи необходимо указать непостоянные функции $\Phi_к$, $U_к$ (если они существуют для автомата A), при которых $\Phi_к((s, A(s, P)) = U_к(x(1))$ при любых $(s, P) \in S \times X^к$, $P = x(1), \ldots, x(к)$.

Итак, в данной работе при некоторых заданных функциях $H_к$, $П_к$ будет проведено описание автоматов A, для которых существуют непостоянные функции $Ф_к$, $U_к$, удовлетворяющие условию

$$Фк(Нк(s, P)) = Uк(Пк(s, P)) \qquad (3)$$

при любых $(s, P) \in S \times X^к$.

Для ряда функций $H_к$, $U_к$ будут указаны алгоритмы определения наличия у заданного автомата указанного свойства, с помощью которых будут оценены некоторые параметры сложности такого описания.

С целью формулировки и доказательства критерия существования функций $Ф_к$, $U_к$ со свойством (2) для автомата A введем дополнительные понятия и докажем вспомогательные утверждения.

Функции $H_к$, $П_к$ индуцируют разбиения множества $S \times X^к$, а последние – бинарные отношения эквивалентности $H^* = H^*_к$, $П^* = П^*_к$ на $S \times X^к$. Именно

$(s, P) H^* (s`, P`) \Leftrightarrow H_к(s, P) = H_к(s`, P`)$;

$(s, P) П^* (s`, P`) \Leftrightarrow П_к(s, P) = П_к(s`, P`)$.

Классы отношений эквивалентности $H^*_к$, $П^*_к$ будем обозначать символами t, r соответствующих множеств $T_к$, $R_к$, то есть под символом t будем понимать и $H_к^{-1}(t)$ – прообраз t. Аналогично – для символа r. Из контекста всегда будет ясно, идет ли речь об элементах t, r либо о классах t, r. В частности, $T_к$, $R_к$ будут в случае необходимости обозначать и множества классов эквивалентности отношений $H^*_к$, $П^*_к$ соответственно. Положим

t[s, P] – класс отношения $H^*_к$, содержащий (s, P);

r[s, P] – класс отношения $П^*_к$, содержащий (s, P).

Введем бинарные отношения эквивалентности $T_к/П^*_к$ на $T_к$ и $R_к/H^*_к$ на $R_к$ посредством вспомогательного бинарного отношения ~ на $T_к$ и $R_к$, рассматриваемых одновременно и как множества элементов множеств $T_к$, $R_к$ и как множества соответствующих классов.

$t \sim t` \Leftrightarrow \exists\, (s, P) \in t, (s`, P`) \in t`, r \in R_к : (s, P) \in r, (s`, P`) \in r.$

Отношение эквивалентности $T_к/П^*_к$ есть транзитивное замыкание бинарного отношения ~ , то есть

$t_1\ T_к/П^*_к\ t_L \Leftrightarrow \exists\, t_2, \ldots, t_{L-1} \in T_к : t_1 \sim t_2 \sim \ldots \sim t_{L-1} \sim t_L.$

Аналогично,

$r \sim r` \Leftrightarrow \exists\, (s, P) \in r, (s`, P`) \in r`, t \in T_r : (s, P) \in t, (s`, P`) \in t,$

а $R_к/H^*_к$ – транзитивное замыкание отношения ~ на $R_к$.

Отметим, что

$\forall\ t \in T_к,\ r \in R_к : t \sim t,\ r \sim r,\ t\ T_к/П^*_к\ t,\ rR_к/Н^*_к r.$

Определим отношение эквивалентности $Н^*_к \vee П^*_к$ на $S \times X^к$ посредством вспомогательного бинарного отношения $\approx\approx$ на $R_к/Н^*_к$

$(s, P) \approx\approx (s`,P`) \Leftrightarrow \exists\ t \in T_к,\ r \in R_к : (s, P), (s`,P`) \in t \vee r$, то есть $(s, P), (s`, P`) \in t$ либо $(s, P), (s`, P`) \in r$.

В случае необходимости уточнения события

$(s, P) \approx\approx (s`, P`),\ (s, P\ ), (s`, P`) \in t \vee r.$

Для определенности пишем:

$(s,\ P) \approx Н^*_к \approx (s`, P`) \Leftrightarrow \exists\ t \in T_к\ : (s, P), (s`, P`) \in t$

и

$(s, P) \approx П^*_к \approx (s`, P`) \Leftrightarrow \exists\ r \in R_к\ : (s, P), (s`, P`) \in r.$

Через $Н^*_к \vee П^*_к$ обозначим транзитивное замыкание бинарного отношения $\approx\approx$.

Отношения эквивалентности $T_к/П^*_к$ на $T_к$ и $R_к/Н^*_к$ на $R_к$ индуцируют отношения эквивалентности $(T_к/П_к)^*$, $(R_к/Н_к)^*$ на $S \times X^к$:

$(s, P)\ (T_к/П_к)^*(s`, P`) \Leftrightarrow t[s, P]\ T_к/П^*_к\ t[s`, P`];$

$(s, P)\ (R_к/Н_к)^*(s`, P`) \Leftrightarrow r[s, P]\ R_к/Н^*_к\ r[s`, P`].$

Через $Н^*_к \vee П^*_к[s, P]$, $(T_к/П_к)^*[s, P]$, $(R_к/Н_к)^*[s, P]$ будем обозначать класс, содержащий (s, P) отношений эквивалентности $Н^*_к \vee П^*_к$, $(T_к/П_к)^*$, $(R_к/Н_к)^*$ на $S \times X^к$.

Теорема 1. Справедливо равенство $Н^*_к \vee П^*_к = (T_к/П_к)^* = (R_к/Н_к)^*$ бинарных отношений эквивалентности $S \times X^к$.

Доказательство. Покажем, что

$$(T_к/П_к)^* = Н^*_к \vee П^*_к.$$

Равенство $(R_к/Н_к)^* = Н^*_к \vee П^*_к$ доказывается аналогично. Пусть

$(s, P)\ (T_к/П_к)^*(s`, P`) \Leftrightarrow t_1[s\ , P]\ T_к/П^*_к\ t_L[s`, P`] \Rightarrow$

$\Rightarrow \exists\ t_2, \ldots, t_{L-1} \in T_к : t_1[s, P] \sim t_2 \sim \ldots \sim t_{L-1} \sim t_L[s`, P`] \Rightarrow$

$\Rightarrow t_j \sim t_{j+1},\ j \in \{1, 2, \ldots, L-1\} \Rightarrow \exists\ (s_j, P_j) \in t_j,\ (s`_j, P`_j) \in t_{j+1},\ r_j \in R_к : (s_j, P_j), (s`_j, P`_j) \in r_j\ \Rightarrow$

$\Rightarrow (s, P) \approx Н^*к \approx (s_1, P_1) \approx П^*к \approx (s`_1, P`_1) \approx Н^*к \approx (s_2, P_2) \approx П^*к \approx (s`_2, P`_2) \approx\approx \ldots \approx\approx (s`, P`) \Rightarrow$

$\Rightarrow (s, P)\ Н^*к \vee П^*к(s`, P`).$

Обратно, пусть

$(s_1, P_1)\ Н^*к \vee П^*к(s_L, P_L) \Rightarrow \exists (s_2, P_2), \ldots, (s_{L-1}, P_{L-1}), \varepsilon(1), \varepsilon(2), \ldots, \varepsilon(L-1) \in \{Н^*к, П^*к\}$:

$: (s_1, P_1) \approx \varepsilon(1) \approx (s_2, P_2) \approx \varepsilon(2) \approx, \ldots, (s_{L-1}, P_{L-1}) \approx \varepsilon(L-1) \approx (s_L, P_L).$

Выберем цепочку минимальной длины L. В этом случае $\varepsilon(j) \neq \varepsilon(j+1)$ для любого $j \in \{1, 2, \ldots, L-2\}$. Откуда следует

$t[s_j, P_j] = t[s_{j+1}, P_{j+1}]$, если $\varepsilon(j) = H^*к$,

$t[s_j, P_j] \sim t[s_{j+1}, P_{j+1}]$, если $\varepsilon(j) = П^*к$.

Следовательно,

$\exists\ t_2, \ldots, t_{L`}$ : $t[s_1, P_1] \sim t_2, \sim \ldots \sim tL` \sim t[s_L, P_L] \Rightarrow t[s_1, P_1]$ Тк/П*к $t[s_L, P_L] \Rightarrow$

$\Rightarrow t[s_1, P_1]$ (Тк/Пк)* $t[s_L, P_L]$.

Теорема доказана.

Следствие 1. Справедливы равенства чисел классов (rang) rang $H^*к \vee П^*к$ = rang Тк/П*к = rang Rк/H*к отношений эквивалентностей $H^*_к \vee П^*_к$ на $S \times X^к$, $T_к/П^*_к$ на $T_к$ и $R_к/H^*_к$ на $R_к$.

Доказательство. В связи с теоремой 1 достаточно показать, что rang $T_к/П^*_к$= rang $(T_к/П_к)^*$.

По определению

(s, P) (Тк/Пк)*$(s`,P`) \Leftrightarrow t[s, P]$ Тк/П*к $t[s`, P`]$,

откуда вытекает, что для любого $(s, P) \in S \times X^к$

(Тк/Пк)*$[s, P] = \cup\ t_j[s_j, P_j]$,

где объединение берется по всем классам $t_j \in T_к/П^*_к[t[s,P]]$. Требуемое утверждение непосредственно вытекает из приведенного равенства.

Теорема 2. Для автомата А тогда и только тогда существуют непостоянные функции $Ф_к$, $U_к$, для которых

$$Фк(Нк(s, P)) = Uк(Пк(s, P))$$

при любых $(s, P) \in S \times X^к$, когда rang $H^*_к \vee П^*_к \geq 2$. При этом значения функций $Ф_к H_к$, $U_к П_к$ на $S \times X^к$ одинаковы и постоянны на классах $H^*_к \vee П^*_к$, а значения функций $Ф_к$, $U_к$ постоянны, соответственно, на классах $T_к/П^*_к$ и $R_к/H^*_к$.

Доказательство. Пусть для некоторых функций $Ф_к$, $U_к$ при любой паре $(s,P) \in S \times X^к$

$$Фк(Нк(s, P)) = Uк(Пк(s, P)).$$

Рассмотрим два элемента (s_1, P_1), (s_L, P_L) из одного класса отношения эквивалентности $H^*_к \vee П^*_к$. Тогда

$\exists\ \varepsilon(1), \varepsilon(2), \ldots, \varepsilon(L-1) \in \{H^*_к, П^*_к\}, (s_2, P_2), \ldots, (s_{L-1}, P_{L-1}) \in S \times X^к$:

: $(s_1, P_1) \approx \varepsilon(1) \approx (s_2, P_2) \approx \varepsilon(2) \approx \ldots \approx \varepsilon(L-1) \approx (s_L, P_L)$.

При $\varepsilon(j) = H^*_к$ получаем $Ф_к(H_к(s_j, P_j)) = Ф_к(H_к(s_{j+1}, P_{j+1}))$, следовательно,

$$U_к(П_к(s_j, P_j)) = U_к(П_к(s_{j+1}, P_{j+1})).$$

При $\varepsilon(j) = П^*_к$ получаем $U_к(П_к(s_j, P_j)) = U_к(П_к(s_{j+1}, P_{j+1}))$, следовательно,

$$Ф_к(Н_к(s_j, P_j)) = Ф_к(Н_к(s_{j+1}, P_{j+1})).$$

Таким образом, функции $Ф_кН_к$, $U_кП_к$ на $S\times X^к$ принимают одинаковые и постоянные значения на классах $Н^*_к\vee П^*_к$. По теореме 1

$Н^*_к\vee П^*_к=(Т_к/П_к)^*=(R_к/Н_к)^*$

и, следовательно, функции $Ф_кН_к$, $U_кП_к$ постоянны на классах отношений $(Т_к/П_к)^*$, $(R_к/Н_к)^*$.

Для любой пары $(s, P)\in S\times X^к$

$(Т_к/П_к)^*[s, P] = \bigcup_{t_j} t_j[s_j, P_j]$,

где объединение берется по всем $t_j\in Т_к/П^*_к[t[s,P]]$. Аналогично

$(R_к/Н_к)^*[s, P] = \bigcup_{r_j} r_j[s_j, P_j]$,

где объединение берется по всем $r_j\in R_к/Н^*_к[t[s, P]]$. Поэтому функция $Ф_к$ постоянна на классах $Т_к/П^*_к$, а $U_к$ постоянна на $R_к/Н^*_к$. Ясно, что $Ф_к$ и $U_к$ могут быть непостоянными тогда и только тогда, когда

$\operatorname{rang} Н^*_к\vee П^*_к = \operatorname{rang} Т_к/П^*_к = \operatorname{rang} R_к/Н^*_к \geq 2$.

Для заданных последовательностей

$(Т_к: к\in\{1, 2, \ldots\})$, $(R_к: к\in\{1, 2, \ldots\})$, $(Н_к: к\in\{1, 2, \ldots\})$,

$(U_к: к\in\{1, 2, \ldots\})$ (4)

обозначим через *К(А) – минимальное к* (если оно существует), при котором $\operatorname{rang} Н^*_к\vee П^*_к\geq 2$. Если такого к не существует, то полагаем $К(А) = \infty$. Функции $Ф_к$ и $U_к$, для которых имеет место равенство (3) при $к = К(А)$, будем называть *основными функциями* однородного эксперимента с функциями наблюдения $Н_к$ и поиска $П_к$.

Введенные функции $Ф_к$, $U_к$ устанавливают связи между множествами $Т_к$, $R_к$, $к\in\{1, 2, \ldots\}$. Алгоритм нахождения связей состоит в последовательном построении классов отношений эквивалентности $Н^*_к\vee П^*_к$: $к\in\{1, 2, \ldots\}$ и использовании теоремы 2 для нахождения искомых связей.

Для ряда конкретных заданий последовательностей (4) ниже будут указаны алгоритмы установления этих связей.

В плане истории возникновения решаемых ниже задач напомним (например, [33]), что известное понятие автомата без потери информации конечного порядка возникло в связи с задачей восстановления входного слова автомата по его выходному слову и начальному или же заключительному состояниям. Впервые эти вопросы начал исследовать Д. Хаффмэн [46; 47]. Эти исследования продолжил Ш. Ивен [31; 43] и А. А. Курмит [33]. В отличие от ре-

зультатов этих работ ниже указываются, во-первых, возможности приближенного определения входного слова, а во-вторых, даются методы восстановления информации о входном слове автомата по неточному заданию исходных данных – начальное (или заключительное) состояние автомата и его выходное слово.

3.2. Закрытый однородный эксперимент по распознаванию информации о первом входном символе входного слова автомата по начальному состоянию и выходной последовательности

Пусть $R_к = X$, $T_к = (S \times Y^к)$, $к \in \{1, 2, \ldots\}$;

$П_к(s, x_1, x_2, \ldots, x_к) = x(1)$, $H_к(s, x_1, x_2, \ldots, x_к) = (s, A(s, x_1, x_2, \ldots, x_к))$.

Рассмотрим бинарное отношение $R_к/H^*_к = X/H^*_к$. Оно определяется с помощью вспомогательного бинарного отношения ~:

$x \sim x` \Leftrightarrow \exists\, s \in S,\ xP,\ x`P` \in X^к : A(s, xP) = A(s, x`P`)$;

$x_1\ X/H^*_к\ x_L \Leftrightarrow \exists\, x_2, \ldots, x_{L-1} : x_1 \sim x_2 \sim \ldots \sim x_{L-1} \sim x_L$.

Ясно, что $\text{rang}\ X/H^*_{K(A)} \geq 2 \Rightarrow \forall\, j \geq 0 : \text{rang}\ X/H^*_{K(A)+j} \geq 2$.

Для получения верхних оценок параметра $К(A) = к(1)$ и нахождения основных функций нам необходимо ввести новые понятия.

Определение 1. Неупорядоченная пара состояний $(s_j, s_{j`})$, возможно и $s_j = s_{j`}$, называется 1-неотличимой парой (относительно автомата A), если выполняется одно из условий:

1) $s \in S$, $x, x` \in X$, $x \neq x`$: $f_x s = f_{x`} s$, $h_x s = s_j$, $h_{x`} s = s_{j`}$;

2) 1-неотличимая пара $s, s`$, $s \neq s`$ и $x, x` \in X$ (возможно $x = x`$) такие, что $f_x s = f_{x`} s`$, $h_x s = s_j$, $h_{x`} s` = s_{j`}$.

Алгоритм нахождения 1-неотличимых пар.

1 шаг. Находятся все пары состояний, удовлетворяющие первому условию определения 1.

n + 1 шаг. Пусть на шаге n найдены пары 1-неотличимых состояний, образованные из разных состояний, которые не были найдены на шагах, предшествующих шагу n. Для каждой такой пары, взятой в качестве пары $s, s`$ согласно условию 2 определения 1, находятся все пары $s_j, s_{j`}$.

Так как неупорядоченных пар состояний автомата конечное число, а на каждом шаге алгоритма вводится хотя бы одна новая пара, то существует n(1) такое, что на шаге n(1) не будут найдены но-

вые пары 1-неотличимых состояний и алгоритм на шаге n(1) прекращает работу.

Определение 2. Состояние s называется дефектным, если

$$\exists\ x,x`\in X,\ x \neq x`:\ f_x s = f_{x`} s.$$

Построим для автомата A ориентированный граф $\Gamma_1(X)$. Вершинами графа являются пары 1-неотличимых состояний и дефектные состояния. Для произвольных двух вершин вида (s, s`) и ($s_j$, $s_{j`}$) дуга из (s, s`) проводится в ($s_j$, $s_{j`}$) тогда и только тогда, когда 1-неотличимые пары (s, s`) и ($s_j$, $s_{j`}$) удовлетворяют второму условию определения 1 и из произвольного дефектного состояния s проводится дуга в вершину ($h_x s$, $h_{x`} s$) с пометкой (x, x`), если $f_x s = f_{x`} s$, $x \neq x`$.

Определение 3. Пометка (x, x`), $x \neq x`$ дуги, исходящей из вершины s графа $\Gamma_1(X)$, называется основной пометкой, а сама вершина – основной (x, x`)-вершиной, если из s имеется путь в вершину вида ($s_j$, $s_j$), либо в контур графа $\Gamma_1(X)$, начинающийся дугой с этой пометкой. Неосновная пометка (x, x`), $x \neq x`$ дуги, исходящая из вершины s графа $\Gamma_1(X)$, называется к-пометкой, если из s имеется путь в графе $\Gamma_1(X)$ длины к, начинающийся дугой с пометкой (x, x`) и нет таких путей длины, большей к.

Введем бинарные отношения ¬, ¬к¬ на входном алфавите автомата A:

$x \neg x` \Leftrightarrow$ x=x` либо (x, x`) является основной пометкой $\Gamma_1(X)$.

$x \neg к \neg x` \Leftrightarrow x \neg x`$ либо (x, x`) является L-пометкой $\Gamma_1(X)$ при $L \geq к$.

Для введенных отношений ¬, ¬к¬ определим их транзитивные замыкания – бинарные отношения эквивалентности σ и σ(к), соответственно, на алфавите X.

Теорема 3. Справедливо равенство $R_к/H^*_к = \sigma(к)$ бинарных отношений на X.

Для доказательства достаточно показать, что $x \sim x` \Leftrightarrow x \neg к \neg x`$. При x=x` это справедливо. Для $x \neq x`$ имеем

$$x \sim x` \Rightarrow \exists\ s \in S,\ xP,\ x`P` \in X^к : A(s, xP)=A(s, x`P`).$$

В этом случае в графе $\Gamma_1(X)$ имеется путь из s, начинающийся дугой с пометкой (x, x`), причем пометка (x, x`) является либо основной, либо L-пометкой при $L \geq к$. Следовательно, из $x \sim x`$ вытекает $x \neg к \neg x`$.

Обратное утверждение $x \neg к \neg x` \Rightarrow x \sim x`$ доказывается исходя из тех же соображений, основываясь на определении графа $Г_1(X)$. Теорема доказана.

Из определения σ(к) следует:

$\forall$ к : rang σ(к+1) ≥ rang σ(к).

Кроме того, σ(к+1) ⊆ σ(к), так как из $x \neg к+1 \neg x` \Rightarrow x \neg к \neg x`$.

В частности,

$\forall$ к : σ⊆σ(к).

Теорема 4. При к ≥ $\frac{|S|(|S|-1)}{2}+1$ справедливо равенство σ(к) = σ.

Доказательство. Так как σ⊆σ(к) для любого к, то остается доказать, что σ(к)⊆σ при указанном в теореме значении к. Для этого достаточно доказать, что для таких значений к из $x \neg к \neg x`$ следует $x \neg x`$. Это будет доказано, если мы покажем, что n-пометок при $n \geq \frac{|S|(|S|-1)}{2}+1$ не существует.

Рассмотрим произвольную вершину s с n-пометкой (x, x`) и максимальный путь, начинающийся дугой с пометкой (x, x`)

$$s \xrightarrow{(x,x)} b_1 \to b_2 \to \ldots \to b_n.$$

По определению n-пометки и графа $Г_1(X)$ среди вершин $b_1, b_2, \ldots, b_n$ нет вершин вида (s`, s`) и все вершины разные, поэтому n не превосходит числа всех неупорядоченных пар состояний вида (s`, s``), s` ≠ s``, то есть

$$n \leq \frac{|S|(|S|-1)}{2}.$$

Поэтому в $Г_1(X)$ нет n-пометок при $n \geq \frac{|S|(|S|-1)}{2}+1$. Теорема доказана.

Приведенная теорема говорит о том, что с помощью графа $Г_1(X)$ можно определить величину К(А) = к(1) и, в случае ее конечности, используя теоремы 2, 3, 1, определить основные функции $Ф_{к(1)}$, $U_{к(1)}$, для которых при любых парах $(s, x_1, x_2, \ldots, x_{к(1)}) \in S \times X^{к(1)}$

$$Ф_{к(1)}(s, A(s, x_1, x_2, \ldots, x_{к(1)}) = U_{к(1)}(x_1).$$

Если rangσ(к(1)) = |X|, то в качестве $U_{к(1)}$ можно взять функцию $U_{к(1)}(x) = x$, $x \in X$.

3.3. Закрытый однородный эксперимент по распознаванию информации о входном слове перестановочного автомата по начальному состоянию и выходной последовательности

Пусть

$R_к = X^к$, Пк : $X^к \times S \to X^к$, $П_к(x_1, x_2, \ldots, x_к, s) = x_1, x_2, \ldots, x_к$;

$T_к = S \times Y^к$, $H_к$: $X^к \times S \to S \times Y^к$, $H_к(x_1, x_2, \ldots, x_к, s) = (s, A(s, x_1, x_2, \ldots, x_к))$.

В этом пункте будем предполагать, что A = (X, S, Y, h, f) – перестановочный автомат, и его частичные функции переходов $(h_x)_{x \in X}$ являются биекциями S в S ($h_x s = h(s,x)$). Положим $R_к/H^*_к = X^к/H^*_к$. Пусть К(А) = к(2) – минимальное к, при котором rang $X^к/H^*_к \geq 2$, и к(2) = ∞ в случае ∀к: rang$X^к/H^*_к = 1$.

Теорема 5. Пусть для перестановочного автомата А к(2) – конечное число. Тогда основная функция $U_{к(2)}$ зависит лишь от первой переменной x_1, то есть имеет вид $U_{к(2)}(x_1, \ldots, x_{к(2)}) = U`(x_1)$.

Доказательство. При к(2) = 1 функция $U_{к(2)}$ определена на X, следовательно, имеет вид $U_{к(2)}(x_1) = U`(x_1)$. Пусть теперь к(2)≥2. Тогда rang$X^{к(2)-1}/H^*_{к(2)-1} = 1$ и существует цепочка $P_1 \sim P_2 \sim \ldots \sim P_L$ слов из $X^{к(2)-1}$, содержащая все элементы $P \in X^{к(2)-1}$ (возможно с повторениями). Согласно определению бинарного отношения ~

$\forall j \in \{1, \ldots, L-1\} : P_j \sim P_{j+1} \Leftrightarrow \exists\, s_j \in S : A(s_j, P_j) = A(s_j, P_{j+1})$.

В силу перестановочности автомата А из последнего равенства имеем

$\forall\, z \in X$: $A(h_z^{-1} s_j, zP_j) = A(h_z^{-1} s_j, zP_{j+1})$, $j \in \{1, \ldots, L-1\}$.

Поэтому

$\forall\, z \in X$: $zP_1 \sim zP_2 \sim \ldots \sim zP_L$, $P_j \in X^{к(2)-1}$.

Функция $U_{к(2)}$ определена на $X^{к(2)}$ и постоянна на классах отношения $X^{к(2)}/H^*_{к(2)}$ согласно теореме 2. В частности, из последнего следует, что при каждом $z \in X$ для любого $j \in \{1, \ldots, L\}$

$U_{к(2)}(zP_j) = \text{const}$.

Следовательно, $U_{к(2)}(zP) = \text{const}$ при каждом $z \in X$ для любого $P \in X^{к(2)-1}$, то есть для любого слова $x_1, \ldots, x_{к(2)}$ из $X^{к(2)}$

$U_{к(2)}(x_1, \ldots, x_{к(2)}) = U`(x_1)$.

Теорема доказана.

Напомним, что в предыдущем пункте работы мы ввели параметр к(1) автомата А.

Теорема 6. В случае конечности одной из величин к(1), к(2) для перестановочного автомата А справедливы равенства:

$к(1) = к(2) = к(0)$, $\text{rang } X/H^*_{к(0)} = \text{rang} X^{к(0)}/H^*_{к(0)}$.

Справедливость утверждения теоремы 6 непосредственно вытекает из теорем 5, 2, 1.

Таким образом, для нахождения параметра к(2) перестановочного автомата А и основной функции $U_{к(2)}$ можно использовать граф $Г_1(X)$, как это было указано в предыдущем пункте. Из приведенных результатов вытекает, что для перестановочного автомата А

$к(2) \le \frac{|S|(|S|-1)}{2}$ либо $к(2) = \infty$.

Теорема 7. Для перестановочного автомата А любая функция $U_к$, при $к \ge к(2)+1$ обладающая свойством: существует непостоянная функция $Ф_к$, для которой

$$Ф_к(s, A(s, P)) = U_к(P) \qquad (4)$$

при любых $(s, P) \in S \times X^к$, имеет вид

$U_к(x_1, \ldots, x_к) = U(x_1, \ldots, x_{к-к(2)+1})$.

Доказательство в основном будет аналогичным доказательству теоремы 5. Имеем $\text{rang } H^*_{к(2)} \vee П^*_{к(2)} \ge 2$. Легко видеть, что тогда

$\forall\ к \ge к(2) : \text{rang } H^*_к \vee П^*_к \ge 2$.

Действительно, если

$\exists\ к,\ к \ge к(2)+1 : \text{rang } H^*_к \vee П^*_к = 1 \Rightarrow$

$\Rightarrow \exists\ \varepsilon_1, \ldots, \varepsilon_{L-1}, \varepsilon_j \in \{H^*_к, П^*_к\}, (s_1, P_1), (s_2, P_2), \ldots, (s_L, P_L) \in S \times X^к : (s_1, P_1) \approx \varepsilon_1 \approx (s_2, P_2) \approx \varepsilon_2 \approx \ldots \approx \varepsilon_{L-1} \approx (s_L, P_L)$,

причем данная цепочка содержит все пары $(s,P) \in S \times X^к$.

Но $\forall\ \varepsilon \in \{H^*_к, П^*_к\} : (s, x_1, \ldots, x_к) \approx \varepsilon \approx (s`, x`_1, \ldots, x`_к) \Rightarrow$

$\Rightarrow (s, x_1, \ldots, x_{к(2)}) \approx \varepsilon` \approx (s`, x`_1, \ldots, x`_{к(2)})$, $\varepsilon` \in \{H^*_{к(2)}, П^*_{к(2)}\}$.

Для $P_j = x_1, \ldots, x_к$ положим $\hat{}P_j = x_1, \ldots, x_{к(2)}$ – начало длины к(2) слова P_j. Тогда

$(s_1, \hat{}P_1) \approx \varepsilon`_1 \approx (s_2, \hat{}P_2) \approx \varepsilon`_2 \approx \ldots \approx \varepsilon\sim_{L-1} \approx (s_L, \hat{}P_L)$, $\varepsilon`_j \in \{H^*_{к(2)}, П^*_{к(2)}\}$

и данная цепочка содержит все элементы из $S \times X^{к(2)}$, что противоречит тому, что $\text{rang } H^*_{к(2)} \vee П^*_{к(2)} \ge 2$. Следовательно, непостоянные функции $Ф_к$, $U_к$ существуют и удовлетворяют (4). Далее, если $к(2) = 1$, то $U_к$ имеет требуемый вид $U_к(x_1, \ldots, x_к) = U(x_1, \ldots, x_{к-к(2)+1})$.

Пусть $к(2) \ge 2$. Тогда $\text{rang } R_{к(2)-1}/H^*_{к(2)-1} = 1$, поэтому существует цепочка $P_1 \sim P_2 \sim \ldots \sim P_L$ слов из $X^{к(2)-1}$, содержащая все элементы из $X^{к(2)-1}$. Используя перестановочность автомата А, аналогично доказательству теоремы 5 легко доказывается, что при входном слове $P = x_1, x_2, \ldots, x_{к-к(2)+1}$ справедлива цепочка отношений $PP_1 \sim PP_2 \sim \ldots$

~ PP_L. Значения функции $U_к$ равны на этих элементах, поэтому $U_к(x_1, \ldots, x_к) = U(x_1, \ldots, x_{к-к(2)+1})$. Теорема доказана.

3.4. Закрытый однородный эксперимент по распознаванию информации о последнем символе входного слова автомата по заключительному состоянию и выходной последовательности

Пусть

$R_к = X$, $П_к$: $X^к \times S \to X$, $П_к(x_1, x_2, \ldots, x_к, s) = x_к$, $T_к = S \times Y^к$, $H_к$: $X^к \times S \to S \times Y^к$,

$H_к(x_1, x_2, \ldots, x_к, s) = (h(s, x_1, x_2, \ldots, x_к), A(s, x_1, x_2, \ldots, x_к)$.

Для нахождения $R_к/H^*_к = X/H^*_к$ и минимального $К(A) = к(3)$, при котором $\text{rang}\, H^*_{K(A)} \geq 2$, введем ряд понятий, аналогичных понятиям, введенных в пункте 1.

Определение 4. Неупорядоченная пара состояний $(s_j, s_{j`})$, возможно и $s_j = s_{j`}$, называется 2-неотличимой парой (относительно автомата А), если выполняется одно из условий:

1) $s_к \in S$, $x(L), x(n) \in X$, $x(L) \neq x(n)$: $f_{x(L)}s_j = f_{x(n)}s_{j`}$, $h_{x(L)}s_j = h_{x(n)}s_{j`} = s_к$;

2) 2-неотличимая пара $s_к$, s_L, $s_к \neq s_L$ и $x(m), x(n) \in X$ (возможно $x(m) = x(n)$ такие, что $f_{x(m)}s_j = f_{x(n)}s_{j`}$, $h_{x(m)}s_j = s_к$, $h_{x(n)}s_{j`} = s_L$.

Алгоритм нахождения 2-неотличимых пар.

1 шаг. Находятся все пары состояний, удовлетворяющие первому условию определения 1`.

n+1 шаг. Пусть на шаге n найдены пары 2-неотличимых состояний, образованные из разных состояний, которые не были найдены на шагах, предшествующих шагу n. Для каждой такой пары, взятой в качестве пары $s_к$, s_L согласно условию 2 определения 4, находятся все пары s_j, $s_{j`}$.

Алгоритм прекращает свою работу на шаге, когда не будут найдены новые пары 2-неотличимых состояний.

Определение 5. Состояние s автомата А называется дефектным, если

$\exists\, x(L), x(n) \in X$, $x(L) \neq x(n)$, $s_j, s_{j`} \in S$ : $f_{x(L)}s_j = f_{x(n)}s_{j`}$, $h_{x(L)}s_j = h_{x(n)}s_{j`} = s$.

Построим для автомата А ориентированный граф $Г_2(X)$. Вершинами графа являются пары 2-неотличимых состояний и дефектные состояния. Для произвольных двух вершин вида $(s_к, s_L)$ и $(s_j, s_{j`})$ дуга из $(s_к, s_L)$ проводится в $(s_j, s_{j`})$, если эти пары удовлетворяют

условию 2 определения 1. Из дефектного состояния s проводится дуга с пометкой (x(L), x(n)) в вершину (s_j, $s_{j`}$), если x(L) ≠ x(n) и $f_{x(L)}s_j = f_{x(n)}s_{j`}$, $h_{x(L)}s_j = h_{x(n)}s_{j`}$.

Определение 6. Пометка (x, x`), x ≠ x` дуги, исходящей из вершины s графа $\Gamma_2(X)$, называется основной пометкой, а сама вершина основной (x, x`)-вершиной, если из s имеется путь в вершину вида ($s_j$, $s_j$), либо в контур графа $\Gamma_2(X)$, начинающийся дугой с этой пометкой. Неосновная пометка (x, x`), x ≠ x` дуги, исходящая из вершины s графа $\Gamma_2(X)$, называется к-пометкой, если из s имеется путь в графе $\Gamma_2(X)$ длины к, начинающийся дугой с пометкой (x, x`) и нет таких путей длины, большей к.

Введем бинарные отношения ¬, ¬к¬ на входном алфавите X автомата A:

x¬x` ⇔ x = x` либо (x, x`) является основной пометкой $\Gamma_2(X)$;

x¬к¬x` ⇔ x¬x`, либо (x, x`) является L-пометкой $\Gamma_2(X)$ при L ≥ к.

Для введенных отношений ¬, ¬к¬ определим их транзитивные замыкания – бинарные отношения эквивалентности σ и σ(к) соответственно на алфавите X.

Теорема 8. Справедливо равенство $R_к/H^*_к$ = σ(к) бинарных отношений на X.

Для доказательства этой теоремы достаточно показать, что

x~x` ⇔ x¬к¬x`.

Для x = x` это утверждение справедливо. Пусть x ≠ x`, тогда первое отношение равносильно условию

∃ Px, P`x`∈$X^к$, P = x(1), x(2), …, x(к–1), P`= x`(1), x`(2), …,
x`(к–1), s, s`∈S : A(s, Px) = A(s`, P`x`), h(s, x(1), x(2), …,
x(к–1), x) = h(s`, x`(1), x`(2), …, x`(к–1), x`).

Рассмотрим последовательности

s, $h_{x(1)}s$, …, $h_{x(к–1)}\ldots h_{x(1)}s$, $h_x h_{x(к–1)}\ldots h_{x(1)}s$,
s`, $h_{x`(1)}s`$, …, $h_{x`(к–1)}\ldots h_{x`(1)}s`$, $h_{x`}h_{x`(к–1)}\ldots h_{x`(1)}s`$.

Возможны следующие варианты: среди неупорядоченных пар

(s, s`), ($h_{x(1)}s$, $h_{x`(1)}s`$), … ,($h_{x(к–1)}\ldots h_{x(1)}s$, $h_{x`(к–1)}\ldots h_{x`(1)}s`$)

есть пары с одинаковыми компонентами, то есть пары вида (s``, s``); или одинаковые пары, в этом случае (x, x`) есть n-пометка при n ≥ к.

Если теперь x¬к¬x`, то из определения графа $\Gamma_2(X)$ вытекает существование P, P`∈$X^{к–1}$ и s, s`, для которых выполняются равенства

A(s, Px) = A(s`, P`x`);

$h(s, x(1), x(2), \ldots, x(к–1), x) = h(s`, x`(1), x`(2), \ldots, x`(к–1), x`)$.

Теорема доказана.

Теорема 9. Для автомата А при $к \geq |S|(|S|-1)2+1$ выполняется равенство $\sigma(к) = \sigma$.

Доказательство этой теоремы вполне аналогично доказательству теоремы 4 в связи с чем мы опускаем его.

Таким образом, с помощью графа $\Gamma_2(X)$ можно определять величину к(3) и, в случае ее конечности, используя теоремы 1, 2, 3, определять основные функции $\Phi_{к(3)}$, $U_{к(3)}$. Если rang $\sigma(к(3)) = |X|$, то в качестве функции $U_{к(3)}$ можно взять функцию $U_{к(3)}(x(1), \ldots x(к(3))) = x(к(3))$.

3.5. Закрытый однородный эксперимент по распознаванию информации о входном слове автомата по заключительному состоянию и выходной последовательности

Пусть $R_к = X^к$, $П_к$: $X^к \times S \to X^к$, $П^к(x(1), \ldots, x(к), s) = (x(1), \ldots, x(к))$, $T_к = S \times Y^к$, $H_к$: $X_к \times S \to S \times Y_к$, $H_к(x(1), \ldots, x(к), s) = (h(s, x(1), \ldots, x(к)), A(s, x(1), \ldots, x(к)))$.

Положим $R_к/H^*_к = X_к/H^*_к$, $К(A) = к(4)$.

Теорема 10. Пусть для автомата А к(4) – конечное число. Тогда основная функция $U_{к(4)}$ имеет вид

$$U_{к(4)}(x(1), x(2), \ldots x(к(4)) = U(x(к(4)).$$

Доказательство. Утверждение теоремы очевидно при к(4) = 1. Пусть к(4) ≥ 2. Тогда $\mathrm{rang} X_{к(4)-1}/H^*_{к(4)-1}=1$ и можно указать цепочку $P_1 \sim P_2 \sim \ldots \sim P_L$ слов из $X^{к(4)-1}$, содержащую все элементы $X^{к(4)-1}$ (возможно с повторениями).

Из $P_j = x(1), \ldots, x(к(4)–1)$, $P_{j+1}=x`(1), \ldots, x`(к(4)–1)$, $P_j \sim P_{j+1}$, $j \in \{1, \ldots, L–1\} \Rightarrow \exists\ s_j, s_{j+1} \in S : A(s_j, P_j) = A(s_{j+1}, P_{j+1})$, $h(s_j, P_j) = h(s_{j+1}, P_{j+1}) \Rightarrow$

$\Rightarrow \forall\ z \in X : h_z h(s_j, P_j) = h_z h(s_{j+1}, P_{j+1})$, $A(s_j, P_j z) = A(s_{j+1}, P_{j+1} z) \Rightarrow$

$\Rightarrow \forall\ z \in X : P_1 z \sim P_2 z \sim \ldots \sim P_L z$.

Функция $U_{к(4)}$ постоянна на элементах последней цепочки отношений, откуда и следует утверждение теоремы.

Доказательства приводимых ниже теорем аналогичны доказательствам теорем 6 и 7.

Теорема 11. Для автомата А в случае конечности одной из величин к(4), к(3) справедливы равенства

$к(4) = к(3) = к(0)$;

$\text{rang } X/H^*_{к(0)} = \text{rang} X^{к(0)}/H^*_{к(0)}$.

Теорема 12. Пусть для автомата A при $к \geq к(4)+1$ существуют непостоянные функции $U_к$, $Ф_к$:

$U_к(x(1), x(2), \ldots, x(к)) = Ф_к((h(s, x(1), \ldots, x(к)), A(s, x(1), \ldots, x(к)))$

при любых $(s, x(1), x(2), \ldots, x(к)) \in S \times X^к$. Тогда функция $U_к$ имеет вид

$U_к(x(1), x(2), \ldots, x(к)) = U(x(к(4)), x(к(4)+1), \ldots, x(к))$.

Глава 4. О ВОССТАНОВЛЕНИИ ИНФОРМАЦИИ ВО ВХОДНОМ СЛОВЕ ПЕРЕСТАНОВОЧНОГО АВТОМАТА МЕДВЕДЕВА ПО НАЧАЛЬНЫМ И ЗАКЛЮЧИТЕЛЬНЫМ СОСТОЯНИЯМ

Приводится описание перестановочных автоматов Медведева, для которых возможно приближенное восстановление информации о входном слове по начальным и соответствующим входному слову заключительным состояниям[1].

4.1. Основные обозначения и постановка задачи восстановления информации о входном слове перестановочного автомата Медведева по начальным и заключительным состояниям

Напомним, что если для автомата $A = (X, S, Y, h, f)$ $f(s, x) = s$ для любых $x \in X$ и $s \in S$ (в этом случае $Y = S$), то автомат A называют автоматом Медведева. Иногда рассматривают так называемый автомат без выхода. В отличие от обычного автомата он не вырабатывает выходной последовательности. По существу автомат без выхода и автомат Медведева – это различные формализации одного и того же явления.

Пусть $A = (X, S, Y, h)$ – автомат Медведева $Y = S$ с функцией переходов $h: X \times S \to S$. Для функции h используем частичные функции переходов $(h_x)_{x \in X}$, $h_x: S \to S$, $h_x(s) = h(x, s)$, $x \in X$, $s \in S$. Ниже рассматриваются лишь перестановочные автоматы, то есть автоматы у

[1] *Источник*: [11].

которых $(h_x)_{x\in X}$ – биекции. Для слова P = x(k), x(k–1), …, x(1) из X^k положим $h_P = h_{x(k)}h_{x(k-1)}\ldots h_{x(1)}$. Через $h_P s$ обозначим образ s при отображении h_P, а через S^(L) обозначим множество всех подмножеств множества S мощности L, L ≥ 1.

Определим функцию $H_{k,\ L}$ на $X^k\times S^\wedge(L)$ следующим образом. Для элементов s^(L) = $\{s_{j(1)}, s_{j(2)}, \ldots, s_{j(L)}\}$ из S^(L) и P = x(k), x(k–1), …, x(1) из X^k положим

$H_{k,\ L}(P,s^\wedge(L)) = (s^\wedge(L);\ h_P s^\wedge(L)) = \{(s_{j(1)},\ h_P s_{j(1)}),(s_{j(2)},\ h_P s_{j(2)}),\ \ldots,\ (s_{j(L)},\ h_P s_{j(L)}\}$.

Через $H_{k,\ L}(X^k\times S^\wedge(L))$ обозначим образ отображения $H_{k,\ L}$.

Будем говорить, что в автомате A приближенно восстанавливаются входные слова длины k по L начальным и заключительным состояниям, если найдутся не равные константе функции $\Phi_{k,\ L}$ и $U_{k,\ L}$, определенные соответственно на $H_{k,\ L}(X^k\times S^\wedge(L))$ и X^k, для которых при любых $P\in X^k$ и $s^\wedge(L)\in S^\wedge(L)$ выполняется равенство

$U_{k,\ L}(P) = \Phi_{k,\ L}((s^\wedge(L);\ h_P s^\wedge(L))$.

Для краткости в дальнейшем этот факт будем обозначать так: автомат A обладает свойством $(X^k,\ s,\ h_P s,\ L)$-восстановления входного слова.

Задача описания автоматов со свойством $(X^k,\ s,\ h_P s,\ L)$-восстановления входного слова близка к проблемам: построения экспериментов для автоматов (см. [21; 39]) , где тестирование проводится неизвестным входным словом с наблюдением в результате эксперимента начальных и заключительных состояний; локального восстановления информации о входном слове (см. [35]) по начальным и заключительным состояниям; описания автоматов без потери информации [33].

Ряд результатов, связанных с решением поставленной задачи, опубликован автором в [7; 11; 12].

Для описания автоматов, у которых возможно приближенно восстанавливать входные слова длины k по L начальным и заключительным состояниям, введем необходимые дополнительные понятия и обозначения.

На множестве X^k определим бинарное отношение эквивалентности σ^*_k посредством вспомогательного бинарного отношения σ_k. Два элемента P, Q $\in X^k$ находятся в отношении σ_k: $P\sigma_k Q$ тогда и только тогда, когда найдется $s^\wedge(L)\in S^\wedge(L)$, при котором $(s^\wedge(L);\ h_P s^\wedge(L)) = (s^\wedge(L);\ h_Q s^\wedge(L))$, то есть $h_P s^\wedge(L) = h_Q s^\wedge(L)$. Элементы

$(P(1), P(N)) \in X^k$ находятся в отношении σ^*_k: $P(1)\sigma_k{*}P(N)$ тогда и только тогда, когда найдутся слова P(2), P(3), …, P(N–1) такие, что

$$P(1)\sigma_k P(2)\sigma_k P(3)\ldots\sigma_k P(N-1)\sigma_k P(N).$$

На множестве $H_{k,L}(X^k \times S^\wedge(L))$ определим бинарное отношение эквивалентности τ^*_k посредством вспомогательного бинарного отношения τ_k: $(s_1^\wedge(L), h_P s_1^\wedge(L))\tau_k(s_2^\wedge(L), h_Q s_2^\wedge(L))$ тогда и только тогда, когда существует $P` \in X^k$, при котором одновременно $h_P s_1^\wedge(L) = h_{P`} s_1^\wedge(L)$ и $h_Q s_2^\wedge(L) = h_{P`} s_2^\wedge(L)$. Элементы $(s_1^\wedge(L), s`_1^\wedge(L))$ и $(s_N^\wedge(L), s`_N^\wedge(L))$ из $H_{k,L}(X^k \times S^\wedge(L))$ находятся в отношении $\tau^*_k$ тогда и только тогда, если найдутся элементы $(s_j^\wedge(L), s`_j^\wedge(L))$, $j \in \{2, \ldots, N-1\}$ для которых

$(s_1^\wedge(L), s`_1^\wedge(L))\tau_k(s_2^\wedge(L), s`_2^\wedge(L))$, …, $(s_{N-1}^\wedge(L), s`_{N-1}^\wedge(L))\tau_k(s_N^\wedge(L), s`_N^\wedge(L))$.

Введенные бинарные отношения эквивалентности σ^*_k, τ^*_k являются транзитивным замыканием бинарных отношений σ_k, τ_k. Обозначим через $\mathrm{rang}\sigma^*_k$, $\mathrm{rang}\tau^*_k$ соответственно число классов отношений эквивалентностей σ^*_k, τ^*_k.

4.2. Основные утверждения

Легко доказывается следующее утверждение.

Утверждение 1.

1) $\mathrm{rang}\sigma^*_k = \mathrm{rang}\tau^*_k$;

2) автомат A обладает свойством $(X^k, s, h_P s, L)$-восстановления входного слова тогда и только тогда, когда $\mathrm{rang}\sigma^*_k > 1$;

3) функции $U_{k,L}$, $\Phi_{k,L}$ постоянны соответственно на классах эквивалентности отношений σ^*_k, τ^*_k.

Теорема 1. Если при некотором $k \geq 1$ $\mathrm{rang}\sigma^*_k = 1$, то для любого $j \geq 0$

$$\mathrm{rang}\sigma^*_{k+j} = 1.$$

Доказательство. Пусть $\mathrm{rang}\sigma^*_k = 1$. Тогда существует последовательность P(1), P(2), P(3), …, P(N) входных слов длины k автомата A, содержащая все слова из X^k и обладающая свойством

$$P(1)\sigma_k P(2)\sigma_k P(3)\ldots\sigma_k P(N).$$

Тогда из перестановочности автомата A следует, что при любом $x \in X$

$$P(1)x\sigma_{k+1}P(2)x\sigma_{k+1}P(3)x\ldots\sigma_{k+1}P(N)x.$$

Кроме того, при любом автомате A выполняется цепочка бинарных отношений

$$x`P(1)\sigma_{k+1}x`P(2)\sigma_{k+1}x`P(3)\ldots\sigma_{k+1}x`P(N)$$

при любом $x`\in X$.

Здесь $P(j)x$ – конкатенация слов $P(j)\in X^k$ и $x\in X$, аналогично $x`P(j)$ – конкатенация $x`\in X$ и $P(j)$.

Из $\{P(1)x, P(2)x, P(3)x, \ldots, P(N)x\} \cap \{x`P(1), x`P(2), x`P(3), \ldots, x`P(N)\} \neq \varnothing$

следует, что $\mathrm{rang}\sigma^*_{k+1} = 1$. Откуда и вытекает утверждение теоремы.

Через $|I|$ будем обозначать мощность множества I.

Лемма 1. Для любого $k \geq 1$

$$|H_{k,\,L}(X^k\times S^\wedge(L))| \leq |H_{k+1,\,L}(X^{k+1}\times S^\wedge(L))|.$$

Доказательство. Положим

$M_L(xX^k) = \{(s^\wedge(L), h_x h_P s^\wedge(L)): s^\wedge(L)\in S^\wedge(L), P\in X^k\}$;

$M_L(X^k x) = \{(s^\wedge(L), h_P h_x s^\wedge(L)): s^\wedge(L)\in S^\wedge(L), P\in X^k\}$.

Так как автомат A – перестановочный, то между множествами

$H_{k,\,L}(X^k\times S^\wedge(L)) = \{(s^\wedge(L), h_P s^\wedge(L)): s^\wedge(L)\in S^\wedge(L), P\in X^k\}$, $M_L(xX^k)$, $M_L(X^k x)$ можно установить биекции, в связи с чем их мощности одинаковы.

Так как

$H_{k+1,\,L}(X^{k+1}\times S^\wedge(L))= \bigcup_{x\in X} M_L(xX^k)= \bigcup_{x\in X} M_L(X^k x)$,

то $|H_{k,\,L}(X^k\times S^\wedge(L))| \leq |H_{k+1,\,L}(X^{k+1}\times S^\wedge(L))|$. Лемма 1 доказана.

Пусть $k(L)$ – минимальное k, при котором

$$|H_{k,\,L}(X^k\times S^\wedge(L))| = |H_{k+1,\,L}(X^{k+1}\times S^\wedge(L))|.$$

Лемма 2. Для любого целого $j \geq 0$

$$|H_{k(L),\,L}(X^{k(L)}\times S^\wedge(L))| = |H_{k(L)+j,\,L}(X^{k(L)+j}\times S^\wedge(L))|.$$

Доказательство. Пусть при некотором k

$$|H_{k,\,L}(X^k\times S^\wedge(L))| = |H_{k+1,\,L}(X^{k+1}\times S^\wedge(L))|.$$

Тогда, в силу перестановочности автомата A, для любого $x\in X$

$$H_{k+1,\,L}(X^{k+1}\times S^\wedge(L)) = M_L(X^k x).$$

Положим для $(x, x`)\in X$

$M_L(x`X^k x) = \{(s^\wedge(L), h_{x`} h_P h_x s^\wedge(L)) : s^\wedge(L)\in S^\wedge(L), P\in X^k\}$.

Тогда

$H_{k+2,L}(X^{k+2}\times S^\wedge(L))= \bigcup_{x`\in X} M_L(x`X^k x) = M_L(X^{k+1}x)$,

откуда следует, что $|H_{k+2,\,L}(X^{k+2}\times S^\wedge(L))| = |H_{k+1,\,L}(X^{k+1}\times S^\wedge(L))|$. Утверждение леммы доказано.

Лемма 3. Справедлива следующая оценка параметра k(L).

$k(L) \le L!C_{|S|}^{L} C_{|S|}^{L} - C_{|S|}^{L} + 1$.

Доказательство. Для любого k

$|H_{k,L}(X^k \times S\hat{}(L))| \le L!C_{|S|}^{L} C_{|S|}^{L}$.

В то же время

$|H_{1,L}(X \times S\hat{}(L))| \ge C_{|S|}^{L}$.

Учитывая лемму 1, получаем

$k(L) \le L!C_{|S|}^{L} C_{|S|}^{L} - C_{|S|}^{L} + 1$.

Теорема 2. Для любого $k \ge k(L)$

$$\mathrm{rang}\tau^*_k \ge \mathrm{rang}\tau^*_{k+1}.$$

Доказательство. Утверждение теоремы 2 вытекает из леммы 2 и следующего факта: если $k \ge k(L)$ и цепочка бинарных отношений $(s_1\hat{}(L), s`_1\hat{}(L))\tau_k(s_2\hat{}(L), s`_2\hat{}(L))\ldots(s_{N-1}\hat{}(L), s`_{N-1}\hat{}(L))\tau_k(s_N\hat{}(L), s`_N\hat{}(L))$ содержит все элементы некоторого класса бинарного отношения эквивалентности τ^*_k, то для $x \in X$

$(s_1\hat{}(L), h_x s`_1\hat{}(L))\tau_{k+1}(s_2\hat{}(L), h_x s`_2\hat{}(L))\ldots\tau_{k+1}(s_N\hat{}(L), h_x s`_N\hat{}(L))$.

Поскольку по лемме 2 для рассматриваемого k

$$|H_{k,L}(X^{k)} \times S\hat{}(L))| = |H_{k+1,L}(X^{k+1} \times S\hat{}(L))|,$$

то, с учетом перестановочности автомата A, получаем, что число классов эквивалентности отношения эквивалентности τ^*_{k+1} не может увеличиться.

Следствие 1. Если перестановочный автомат $A = (X, S, Y, (h_x)_{x \in X})$ обладает свойством $(X^k, s, h_P s, L)$-восстановления входного слова, то он обладает свойством $(X^k, s, h_P s, L)$-восстановления входного слова при некотором $k` \le k(L)$.

Доказательство. Если k в условиях следствия не превосходит k(L), то в качестве k` возьмем k. Если $k \ge k(L)+1$, то по теореме 2

$$\mathrm{rang}\tau^*_k \le \mathrm{rang}\tau^*_{k-1}$$

и, так как по условию $\mathrm{rang}\tau^* k \ge 2$, то и $\mathrm{rang}\tau^*_{k-1} \ge 2$, то есть автомат A обладает свойством $(X^{k-1}, s, h_P s, L)$-восстановления входного слова (см. утверждение 1). Откуда следует, что A обладает свойством $(X^{k(L)}, s, h_P s, L)$-восстановления входного слова.

Обозначим через j(L) минимальное $j \ge 0$, при котором $\mathrm{rang}\tau^*_{k(L)+j} = \mathrm{rang}\tau^*_{k(L)+j+1}$.

Теорема 3. Для любого целого $j \ge 0$

$$\mathrm{rang}\tau^*_{k(L)+j(L)} = \mathrm{rang}\tau^*_{k(L)+j(L)+j}.$$

Доказательство. Пусть для некоторого фиксированного $k \geq k(L)+j(L)$

$$\mathrm{rang}\tau^*_k = \mathrm{rang}\tau^*_{k+1} = r.$$

Покажем, что $\mathrm{rang}\tau^*_{k+2} = \mathrm{rang}\tau^*_{k+1} = r$.

Согласно утверждению 1 и теореме 1 при $r = 1$

$$\mathrm{rang}\tau^*_{k+2} = \mathrm{rang}\tau^*_{k+1} = 1.$$

Предположим, что $r \geq 2$, $\mathrm{rang}\tau^*_k = \mathrm{rang}\tau^*_{k+1} = r$ и $\mathrm{rang}\tau^*_{k+2} < r$.

Для $x \in X$ определим бинарное отношение $\tau_k(x)$ на множестве $M_L(X^k x) = \{(s\hat{}(L), h_P h_x s\hat{}(L)) : s\hat{}(L) \in S\hat{}(L), P \in X^k\}$следующим образом: два элемента $(s\hat{}(L), s`\hat{}(L))$ и $(s``\hat{}(L), s```\hat{}(L))$ находятся в отношении $\tau_k(x)$: $(s\hat{}(L), s`\hat{}(L))\tau_k(x)(s``\hat{}(L), s```\hat{}(L))$ тогда и только тогда, когда найдется $P \in X^k$, при котором

$$h_P h_x s\hat{}(L) = s`\hat{}(L),\ h_P h_x s``\hat{}(L) = s```\hat{}(L).$$

Через $\tau^*_k(x)$ обозначим транзитивное замыкание бинарного отношения $\tau_k(x)$.

Пусть $\{(a^j(m), b^j(m)): m \in \{1, 2, \ldots, t(j)\}\}$ – множество всех элементов j-го класса отношения эквивалентности τ^*_k, $j \in \{1, ..., r\}$. Тогда для любого $x` \in X$ элементы $\{(h_{x`}^{-1} a^j(m), b^j(m)): m \in \{1, 2, \ldots, t(j)\}\}$ образуют класс отношения эквивалентности $\tau^*_k(x`)$, в частности, эти элементы находятся в отношении τ^*_{k+1}. Так как

$\mathrm{rang}\tau^*_{k+1} = r$ и $|H_{k,L}(X^k \times S\hat{}(L))| = |H_{k+1,L}(X^{k+1} \times S\hat{}(L))|$, поскольку $k \geq k(L)$, то для любого $x` \in X$ элементы

$$\{(h_{x`}^{-1} a^j(m), b^j(m)): m \in \{1,2,\ldots,t(j)\}\}$$

образуют класс отношения эквивалентности τ^*_{k+1}, что равносильно тому, что при любом $x` \in X$ и фиксированном нами k

$$\tau^*_k(x`) = \tau^*_{k+1}.$$

Аналогично для любого $x \in X$ элементы

$\{(h_x^{-1} h_{x`}^{-1} a^j(m), b^j(m)) : m \in \{1, 2, \ldots, t(j)\}\}$

образуют класс отношения эквивалентности $\tau^*_{k+1}(x)$, и в частности, они находятся в отношении τ^*_{k+2}. Заметим, что из $k \geq k(L)$ следует

$|H_{k+2,\,L}(X^{k+2} \times S\hat{}(L))| = |H_{k+1,\,L}(X^{k+1} \times S\hat{}(L))|$

и для любого $x \in X$

$H_{k+2,L}(X^{k+2} \times S\hat{}(L)) = M_L(X^{k+1} x)$.

Так как по предположению $\mathrm{rang}\tau^*_{k+2} < r$, то найдутся такие $j(1)$, $j(2) \in \{1, 2, \ldots, r\}$, что элементы объединения множеств

$\{(h_x^{-1} h_{x`}^{-1} a^{j(1)}(m), b^{j(1)}(m)) : m \in \{1, 2, \ldots, t(j(1))\}\}$;

$\{(h_x^{-1} h_{x`}^{-1} a^{j(2)}(m), b^{j(2)}(m)) : m \in \{1, 2, \ldots, t(j(2))\}\}$

находятся в отношении τ^*_{k+2}. В этом случае, очевидно, можно считать, что j(1), j(2) выбраны так, что найдутся элементы:

$(h_x^{-1}h_{x`}^{-1}a^{j(1)}, b^{j(1)}) \in \{(h_x^{-1}h_{x`}^{-1}a^{j(1)}(m), b^{j(1)}(m)): m \in \{1, 2, \ldots, t(j(1))\}\}$,

$(h_x^{-1}h_{x`}^{-1}a^{j(2)}, b^{j(2)}) \in \{(h_x^{-1}h_{x`}^{-1}a^{j(2)}(m), b^{j(2)}(m)): m \in \{1, 2, \ldots, t(j(2))\}\}$,

для которых

$(h_x^{-1}h_{x`}^{-1}a^{j(1)}, b^{j(1)})\tau_{k+2}(h_x^{-1}h_{x`}^{-1}a^{j(2)}, b^{j(2)})$, то есть существует $P \in X^{k+2}$, P = x(k+2), x(k+1), …, x(1), для которого

$h_P h_x^{-1}h_{x`}^{-1}a^{j(1)} = b^{j(1)}$,

$h_P h_x^{-1}h_{x`}^{-1}a^{j(2)} = b^{j(2)}$.

Здесь имеется в виду равенство упорядоченных множеств (см. ранее введенное обозначение: $\{(s_{i(1)}, h_P s_{i(1)}), (s_{i(2)}, h_P s_{i(2)}), \ldots, (s_{i(L)}, h_P s_{i(L)})\} = (s\hat{}(L); h_P s\hat{}(L))$ для $s\hat{}(L) = \{s_{i(1)}, s_{i(2)}, \ldots, s_{i(L)}\}$ из $S\hat{}(L)$). Из приведенных равенств следует

$(h_x^{-1}h_{x`}^{-1}a^{j(1)}, (h_{x(k+2)})^{-1}b^{j(1)})\tau_{k+1}(h_x^{-1}h_{x`}^{-1}a^{j(2)}, (h_{x(k+2)})^{-1}b^{j(2)})$.

Ранее было отмечено, что $\tau^*_{k+1} = \tau^*_k(x)$, при любом $x \in X$. Поэтому

$(h_x^{-1}h_{x`}^{-1}a^{j(1)}, (h_{x(k+2)})^{-1}b^{j(1)})\tau^*_k(x)(h_x^{-1}h_{x`}^{-1}a^{j(2)}, (h_{x(k+2)})^{-1}b^{j(2)})$.

Отсюда легко получается

$(h_x^{-1}h_{x`}^{-1}a^{j(1)}, b^{j(1)})\tau^*_{k+1}(x)(h_x^{-1}h_{x`}^{-1}a^{j(2)}, b^{j(2)})$.

Придем к противоречию. Для этого покажем, что j(1) = j(2) противоречит их выбору. Из предыдущего отношения эквивалентности получаем

$(h_{x`}^{-1}a^{j(1)}, b^{j(1)})\tau^*_{k+1}(h_{x`}^{-1}a^{j(2)}, b^{j(2)})$.

Ранее было отмечено, что $\tau^*_k(x`) = \tau^*_{k+1}$. Поэтому

$(h_{x`}^{-1}a^{j(1)}, b^{j(1)})\tau^*_k(x`)(h_{x`}^{-1}a^{j(2)}, b^{j(2)})$.

Откуда имеем

$(a^{j(1)}, b^{j(1)})\tau^*_k(a^{j(2)}, b^{j(2)})$.

Следовательно, j(1) = j(2). Таким образом, доказано, что

$\mathrm{rang}\tau^*_{k+2} = r$.

Теорема 3 полностью доказана.

Следствие 2. Если перестановочный автомат A обладает свойством $(X^k, s, h_P s, L)$-восстановления входного слова для $k \geq k(L)+j(L)$, то он обладает свойством $(X^{k`}, s, h_P s, L)$-восстановления входного слова при любом k`.

Доказательство следует из утверждений теорем 1, 3.

4.3. Оценки параметров

Лемма 4. Справедлива следующая оценка параметра j(L):

$$j(L) \le C_{|S|}^{L} L! - 1.$$

При этом для любого $j \in \{0, 1, \ldots, j(L)\}$

$$\mathrm{rang}\tau^*_{k(L)+j} \le C_{|S|}^{L} L! - j.$$

Доказательство. Очевидно, в каждом классе отношения $\tau^*_{k(L)}$ имеется по крайней мере $C_{|S|}^{L}$ элементов, поэтому

$$\tau^*_{k(L)} \le |H_{k(L),L}(X^{k(L)} \times S\wedge(L))| \cdot \frac{1}{C_{|S|}^{L}} \le C_{|S|}^{L} L!.$$

Следовательно, согласно определению j(L) и теореме 2, для $j \in \{0, 1, \ldots, j(L)\}$

$$\mathrm{rang}\tau^*_{k(L)+j} \le C_{|S|}^{L} L! - j,$$

откуда следует

$$j(L) \le C_{|S|}^{L} L! - 1.$$

Из лемм 3, 4 непосредственно вытекает

Следствие 3. Справедлива следующая оценка:

$$k(L) + j(L) \le C_{|S|}^{L} C_{|S|}^{L} L! + C_{|S|}^{L} L! - C_{|S|}^{L}.$$

4.4. Оценки параметров полугруппы автомата

Для перестановочного автомата $A = (X, S, Y, (h_x)_{x \in X})$ рассмотрим его группу $G = \langle (h_x)_{x \in X} \rangle$, порожденную частичными функциями переходов. Напомним (см. [48; 55]), что множество Π_j элементов группы G, представимых положительными словами в образующих $(h_x)_{x \in X}$ длины j, называется j-м слоем группы G. Минимальное число R = R(G), для которого

$$\bigcup_{j=1}^{R} \Pi_j = G,$$

называют длиной группы G, а минимальное число слоев группы, объединение которых совпадает с G, называют шириной D = D(G) группы G. Параметр D(G) совпадает с периодом смешанно-периодической последовательности $\Pi_1, \Pi_2, \ldots$ слоев группы G.

Обозначим через K(0) минимальное k, при котором мощности слоев Π_k, Π_{k+1} группы G совпадают. Этот параметр называют глуби-

ной группы G в системе образующих $(h_x)_{x\in X}$ (см. [28]) или индексом системы $(h_x)_{x\in X}$ (см. [33]).

Известно (см. [55]), что $R(G) \le K(0)+D(G)-1$ и при некотором n, $0\le n\le D(G)-1$ слой $\Pi_{K(0)+n}$ является группой, порожденной подстановками $\{h_P: P\in X^D\}$, причем $\Pi_{K(0)+n}$ – нормальный делитель группы G, а слои $\Pi_{K(0)}, \Pi_{K(0)+1}, \ldots, \Pi_{K(0)+n}, \ldots, \Pi_{K(0)+D(G)-1}$ являются смежными классами группы G по $\Pi_{K(0)+n}$. Положим $K(0)+n = V(0)$. Обобщение этих результатов на случай конечной полугруппы в системе образующих $(h_x)_{x\in X}$ проведено в [9].

Из определений параметров k(L) и K(0) следует, что $k(L) \le K(0)$.

Лемма 5. При $k \ge K(0)$

$$\mathrm{rang}\sigma^*_k = \mathrm{rang}\sigma^*_{k+1}.$$

Доказательство. Ранее для $s^\wedge(L) = \{s_{j(1)}, s_{j(2)}, \ldots, s_{j(L)}\}$ из $S^\wedge(L)$ и $P = x(k), x(k-1), \ldots, x(1)\in X^k$ мы положили

$H_{k,L}(P,s^\wedge(L)) =\{(s_{j(1)}, h_P s_{j(1)}),(s_{j(2)}, h_P s_{j(2)}), \ldots, (s_{j(L)}, h_P s_{j(L)})\}$.

Это выражение можно трактовать как частичную подстановку на S (определено L переходов для подстановки h_P).

При любом k бинарное отношение σ_k и отношение эквивалентности σ^*_k на X^k определяют бинарное отношение $\Pi\sigma_k$ и бинарное отношение эквивалентности $\Pi\sigma^*_k$ на k-м слое Π_k группы G. Именно, элементы h_P, h_Q из Π_k находятся в отношении $\Pi\sigma_k$: $h_P\Pi\sigma_k h_Q$ тогда и только тогда, когда $P\sigma_k Q$. Аналогично, $h_P\Pi\sigma^*_k h_Q$ тогда и только тогда, если $P\sigma^*_k Q$. При этом очевидно, что для любого k

$$\mathrm{rang}\Pi\sigma^*_k = \mathrm{rang}\sigma^*_k.$$

Если теперь $k \ge K(0)$, то как следует из [9; 28; 55], слои Π_k являются смежными классами группы G по некоторому нормальному делителю, и в частности, при таких k для любого $x\in X$

$$\Pi_{k+1} = h_x\Pi_k = \Pi_k h_x.$$

Отсюда получаем, что для любых $g_1, g_2\in\Pi_k$

$g_1\Pi\sigma_k g_2$

тогда и только тогда, когда для $x\in X$

$$h_x g_1\Pi\sigma_{k+1} h_x g_2.$$

В связи с этим для $g, g`\in\Pi_k$

$g\Pi\sigma^*_k g`$

тогда и только тогда, когда для $x\in X$

$$h_x g\Pi\sigma^*_{k+1} h_x g`.$$

Здесь импликация сверху вниз очевидна. Импликация снизу доказывается следующим образом. Пусть $h_x g \Pi\sigma^*_{k+1} h_x g`$. Тогда существует цепочка отношений

$h_x g \Pi\sigma_{k+1} g(1) \Pi\sigma_{k+1} g(2) \ldots g(N) \Pi\sigma_{k+1} h_x g`$,

где элементы $g_j \in \Pi_{k+1}$. Так как по указанному выше равенству $\Pi_{k+1} = h_x \Pi_k = \Pi_k h_x$ элементы $g(j)$ представимы в виде $h_x g`(j)$, где $g`(j) \in \Pi_k$. Следовательно, справедлива цепочка отношений

$h_x g \Pi\sigma_{k+1} h_x g`(1) \Pi\sigma_{k+1} h_x g`(2) \ldots h_x g`(N) \Pi\sigma_{k+1} h_x g`$.

Откуда получаем

$$g \Pi\sigma_k g`(1) \Pi\sigma_k g`(2) \ldots g`(N) \Pi\sigma_k g`,$$

то есть $g \Pi\sigma^*_k g`$. Импликация доказана. Поэтому для $k \geq K(0)$

$$\mathrm{rang}\Pi\sigma^*_k = \mathrm{rang}\sigma^*_k = \mathrm{rang}\Pi\sigma^*_{k+1} = \mathrm{rang}\sigma^*_{k+1}.$$

Лемма 5 доказана. При этом мы получили дополнительное утверждение.

Утверждение 2. Для $k \geq K(0)$

$$\mathrm{rang}\Pi\sigma^*_k = \mathrm{rang}\sigma^*_k = \mathrm{rang}\Pi\sigma^*_{k+1} = \mathrm{rang}\sigma^*_{k+1}.$$

4.5. Структура отношения эквивалентности $\Pi\sigma^*_k$

Перейдем теперь к исследованию структуры отношения эквивалентности $\Pi\sigma^*_k$ при $k \geq k(L)+j(L)$. Если $\mathrm{rang}\Pi\sigma^*_k \geq 2$, то по следствию 2 такие автоматы обладают свойством $(X^{k`}, s, h_P s, L)$-восстановления входного слова при любом $k`$.

Теорема 4. Элементы одного из классов отношения эквивалентности $\Pi\sigma^*_{V(0)}$ образуют группу U, которая является нормальным делителем группы $\Pi_{V(0)}$ и группы G. Остальные классы отношения эквивалентности являются смежными классами группы $\Pi_{V(0)}$ по U.

Доказательство. Пусть цепочка элементов

$e \Pi\sigma_{V(0)} g_1 \Pi\sigma_{V(0)} g_2 \ldots \Pi\sigma_{V(0)} g_N$

содержит все элементы класса U отношения эквивалентности $\Pi\sigma^*_{V(0)}$, содержащего единицу $e \in G$ группы $G = \langle (h_x)_{x \in X} \rangle$. Тогда очевидно, что

$e\ \Pi\sigma_{V(0)} g_1^{-1} \Pi\sigma_{V(0)} g_2^{-1} \ldots \Pi\sigma_{V(0)} g_N^{-1}$,

откуда имеем $g_j^{-1} \in U$, $j \in \{1, \ldots, N\}$.

При любом $j \in \{1, \ldots, N\}$ справедливо

$g_j^{-1} \Pi\sigma_{V(0)}\ g_j^{-1} g_1 \Pi\sigma_{V(0)}\ g_j^{-1} g_2 \ldots \Pi\sigma_{V(0)}\ g_j^{-1} g_N$,

при этом в цепочке элементов, очевидно, содержится единица группы G, поэтому $g \cdot g` \in U$, для любых $(g, g`) \in U$. Таким образом, U – группа.

Для любого элемента $g \in \Pi_{V(0)}$ имеем

$g\Pi\sigma_{V(0)}gg_1\Pi\sigma_{V(0)}gg_2\ldots\Pi\sigma_{V(0)}gg_N$;

$g\Pi\sigma_{V(0)}g_1g\Pi\sigma_{V(0)}g_2g\ldots\Pi\sigma_{V(0)}g_Ng$,

то есть U – нормальный делитель группы $\Pi_{V(0)}$, и остальные классы отношения $\Pi\sigma_{V(0)}$ являются смежными классами группы $\Pi_{V(0)}$ по U.

Аналогично для любого $g \in G$

$g\Pi\sigma_{V(0)}\, gg_1\Pi\sigma_{V(0)}\, gg_2\ldots\Pi\sigma_{V(0)}\, gg_N$;

$g\Pi\sigma_{V(0)}g_1g\Pi\sigma_{V(0)}g2g\ldots\Pi\sigma_{V(0)}g_Ng$

и, следовательно, U – нормальный делитель и группы G. Теорема доказана.

Пусть $s^\wedge(L) = \{s_{j(1)}, s_{j(2)}, \ldots, s_{j(L)}\}$ – произвольное подмножество множества S мощности L. Обозначим через $U(s^\wedge(L))$ – множество всех элементов g группы $\Pi_{V(0)}$, для которых

$gs_{j(t)} = s_{j(t)}, t \in \{1, \ldots, L\}$.

Теорема 5. Элементы из объединения $O(U(s^\wedge(L))$ множеств $U(s^\wedge(L))$ по всем $s^\wedge(L) = \{s_{j(1)}, s_{j(2)}, \ldots, s_{j(L)}\}$ из $S^\wedge(L)$ порождают группу U.

Доказательство. Очевидно, что для каждого $s^\wedge(L)$

$U(s^\wedge(L)) \subseteq U$.

Пусть цепочка $e\Pi\sigma_{V(0)}g_1\Pi\sigma_{V(0)}g_2\ldots\Pi\sigma_{V(0)}g_N$ содержит все элементы группы U. Тогда $(e, g_1) \in O(U(s^\wedge(L))$. Предположим, что для некоторого $j \in \{1, \ldots, N–1\}$ g_j принадлежит группе $<O(U(s^\wedge(L))>$, порожденной элементами из $O(U(s^\wedge(L))$. Тогда $g_jg_{j+1}^{-1} \in O(U(s^\wedge(L))$. Отсюда следует, что $g_{j+1} \in <O(U(s^\wedge(L))>$. Это и требовалось доказать.

Утверждение теоремы 4 описывает строение группы U. Пользуясь этой теоремой, ранее указанным равенством

$$\mathrm{rang}\Pi\sigma^*_k = \mathrm{rang}\sigma^*_k,$$

справедливым для любого k, а также теоремой 1 и утверждением 1 пункта 1, заключаем: если $U \neq \Pi_{V(0)}$, то автомат обладает свойством (X^k, s, h_Ps, L)-восстановления входного слова при любом k.

Утверждение следующего замечания позволяет последовательно находить классы отношения τ^*_k.

Замечание. Пусть $\{(a_t, b_t): t\in\{1, \ldots, P_j\}\} = m^j$ – j-й класс отношения τ^*_k. Положим для $x\in X$

$h_x m^j = \{(a_t, h_x b_t): t\in\{1, \ldots, P_j\}\}$.

На множестве $M = \{h_x m^j: x\in X, j\in\{1, \ldots, \mathrm{rang}\tau^*_k\}\}$ определим отношение эквивалентности φ_k.

Именно элементы $h_{x(1)}m^{j(1)}$, $h_{x(N)}m^{j(N)}$ находятся в отношении φ_k тогда и только тогда, когда найдутся элементы множества $h_{x(t)}m^{j(t)}$, $t\in\{2, \ldots, N–1\}$ из M, для которых

$$h_{x(t)}m^{j(t)}\cap h_{x(t+1)}m^{j(t+1)} \neq \varnothing, \quad t\in\{1, \ldots, N–1\}.$$

4.6. Алгоритм проверки свойства автомата A приближенно восстанавливать входные слова длины k по L начальным и заключительным состояниям

Легко доказывается, что любой класс бинарного отношения τ^*_{k+1} есть объединение множеств $h_x m^j$, принадлежащих одному классу отношения эквивалентности φ_k.

На основе доказанных утверждений можно предложить следующий алгоритм проверки свойства автомата A приближенно восстанавливать входные слова длины k по L начальным и заключительным состояниям.

Алгоритм.

1. Полагаем m = 1.
2. Строятся классы бинарного отношения эквивалентности τ^*_m.
3. Если $\mathrm{rang}\tau^*_m = 1$, то автомат не обладает свойством приближенно восстанавливать входные слова длины k по L начальным и заключительным состояниям.

Если

$\mathrm{rang}\tau^*_m > 1$ и $m = k$ или $m \geq k(L)+j(L)$,

то автомат обладает свойством приближенно восстанавливать входные слова длины k по L начальным и заключительным состояниям.

Если

$\mathrm{rang}\tau^*_m > 1$ и $m < k$, $m < k(L)+j(L)$,

то заменяем m на m+1 и переходим к 2.

Глава 5. ОПРЕДЕЛЕНИЕ ВХОДНОГО СЛОВА ВЕКТОРНОГО ПЕРЕСТАНОВОЧНОГО АВТОМАТА ПО МНОЖЕСТВУ ПАР НАЧАЛЬНЫХ И ЗАКЛЮЧИТЕЛЬНЫХ СОСТОЯНИЙ С ПОМОЩЬЮ ВЕРОЯТНОСТНОЙ МОДЕЛИ ИХ СТАТИСТИЧЕСКИХ ЗАВИСИМОСТЕЙ

5.1. Постановка задачи и план ее решения

Пусть $A = (X, S, (h_x)_{x\in X})$ – векторный перестановочный автомат без выхода с входным алфавитом X, множеством состояний $S = F_2^n$, где F_2^n – векторное пространство размерности n над полем F_2 из двух элементов, h_x: $S \to S$ – биекции.

Задача состоит в решении совместной системы уравнений

$$h_{x(k)}h_{x(k-1)}\ldots h_{x(1)}s_1^j = s_k^j, \qquad (6)$$

где $j\in\{1, 2, \ldots, N)$ относительно $(x(1), x(2), \ldots, x(k))\in X^k$.

Чисто алгебраические подходы к решению данной задачи рассматривались в работе [11]. Для биекций $(h_x)_{x\in X}$, определенных законом функционирования блочного шифра DES (Data Encryption Standard), при решении системы уравнений вида (6) в работах [50–52] был применен так называемый *линейный метод*. В данной работе развивается и обобщается основная статистическая идея [50] определения ключа шифратора DES на случай определения входного слова конечного автомата указанного выше вида.

Будем далее предполагать, что система уравнений (6) имеет единственное решение (b(1), b(2), …, b(k)). Пусть Φ_1, Φ_{k+1} – произвольные двоичные функции от n переменных, $P(S) = (p(s) = \frac{1}{|S|}, s\in S)$ – равномерное вероятностное распределение на S.

Для $(a(1), a(2), \ldots, a(k))\in X^k$ положим

$P(\Phi_1, (a(1), a(2), \ldots, a(k)), \Phi_{k+1}) = P(\Phi_1(s) = \Phi_{k+1}(h_{a(k)}h_{a(k-1)}\ldots h_{a(1)}s))$.

Рассматриваемый метод определения решения системы (6) предполагает осуществление следующего плана:

1. Рассчитывается $P(\Phi_1, \Phi_{k+1}) = P\max_{(a(1), a(2), \ldots, a(k)\in X^k)} (\Phi_1, (a(1), a(2), \ldots, a(k)), \Phi_{k+1})$.

Данной максимальной вероятности соответствует множество

$X(k) = \{(a(1), a(2), \ldots, a(k)): P(\Phi_1, (a(1), a(2), \ldots, a(k)), \Phi_{k+1}) = P(\Phi_1, \Phi_{k+1})\}$.

2. Поиск решения системы (6) использует статистическую процедуру: по $s_1^1, s_1^2, \ldots, s_1^N$ и соответствующей правой части системы (6) $s_k^1, s_k^2, \ldots, s_k^N$ принимается одна из гипотез: H_0 – событие $\Phi_1(s) = \Phi_{k+1}(h_{b(k)}h_{b(k-1)}\ldots h_{b(1)}s)$ происходит с вероятностью $P(\Phi_1, \Phi_{k+1})$; событие H_1 происходит с вероятностью $\frac{1}{2}$.

3. При принятии H_0 делается вывод о том, что решение системы (1) принадлежит множеству X(k). При принятии H_1 – вывод о том, что $(b(1), b(2), \ldots, b(k)) \notin X(k)$. При принятии H_1 решение считается ненайденным. При принятии гипотезы H_0 переходят к поиску решения системы (1) при условии, что решение принадлежит множеству X(k). Данный поиск использует специфику построения вспомогательной последовательности двоичных функций $\Phi_1, \Phi_2, \ldots, \Phi_{k+1}$ от n переменных и предположения для расчета значения $P(\Phi_1, \Phi_{k+1})$ с помощью указанной последовательности функций. Поиск решения основан на последовательном опробовании компонент $a(j) \in X$, $j \in \{1, \ldots, k\}$ неизвестного решения с применением статистического критерия отсева ложных вариантов. Вспомогательная последовательность двоичных функций $\Phi_1, \Phi_2, \ldots, \Phi_{k+1}$, совместно с предположениями о вероятностных мерах на используемых множествах играет роль вероятностной модели статистических зависимостей между начальными и заключительными состояниями автомата.

Перейдем к описанию предлагаемой модернизации идеи Матсуи [50] применительно к определению входного слова автомата A – решению системы уравнений (6).

5.2. Модернизация идеи Матсуи

Построение функций Φ_1, Φ_{k+1}. Расчет $P(\Phi_1, \Phi_{k+1})$.

Ищется последовательность пар функций

$(\Phi_1, \Phi_2), (\Phi_2, \Phi_3), \ldots, (\Phi_k, \Phi_{k+1})$,

удовлетворяющая приводимым ниже условиям.

При равномерном распределении на S для слова $a(1), a(2), \ldots, a(k) \in X^k$ рассмотрим вероятности:

$P(\Phi_1(s) = \Phi_2(h_{a(1)}s)), P(\Phi_2(h_{a(1)}s) = \Phi_3(h_{a(2)}h_{a(1)}s)), \ldots,$

$P(\Phi_j(h_{a(j-1)}\ldots h_{a(1)}s) = \Phi_{j+1}(h_{a(j)}\ldots h_{a(1)}s)), \ldots,$

$P(\Phi k(ha(k-1)\ldots ha(1)s) = \Phi_{k+1}(ha(k)\ldots ha(1)s)).$ (7)

Для расчета значения $P(\Phi_1, \Phi_{k+1})$ заметим, что в силу перестановочности автомата A индуцированные равномерным распределением на S вероятностные распределения на множествах $h_{a(1)}(S)$, …, $h_{a(j)}\ldots h_{a(1)}(S)$,…, $h_{a(k)}\ldots h_{a(1)}(S)$ – равномерные. В связи с чем при случайном и равновероятном выборе s и s` из S

$$P(\Phi_j(h_{a(j-1)}\ldots h_{a(1)}s) = \Phi_{j+1}(h_{a(j)}\ldots h_{a(1)}s)) = P(\Phi_j(s`) = \Phi_{j+1}(h_{a(j)}s`)) \quad (8)$$

Утверждение 1. Если при случайном и равновероятном выборе s из S при любом $j\in\{1, \ldots, k-1\}$ события

$$\Phi_1(s) = \Phi_{j+1}(h_{a(j)}\ldots h_{a(1)}s),\ \Phi_{j+1}(h_{a(j)}\ldots h_{a(1)}s) = \Phi_{j+2}(h_{a(j+1)}\ldots h_{a(1)}s)$$

независимы, то

$$P(\Phi_1, (a(1), a(2), \ldots, a(k)), \Phi_{k+1}) = \frac{1+\delta_{a(1)}\delta_{a(2)}\ldots\delta_{a(k)}}{2},$$

где $\delta_{a(j)}$, $j\in\{1, \ldots, k\}$ определяется из равенства:

$$P(\Phi_j(s_j) = \Phi_{j+1}(h_{a(j)}s_j)) = \frac{1+\delta_{a(j)}}{2}$$

при случайном и равновероятном выборе $s_j\in S$.

Доказательство. Индукция по k. При k = 1 требуемое равенство очевидно. Пусть это равенство верно для k = j. Докажем его для j+1. Имеем:

$$P(\Phi_1, (a(1), a(2), \ldots, a(j+1)), \Phi_{j+2}) =$$

$$P(\Phi_1(s) = \Phi_{j+1}(h_{a(j)}\ldots h_{a(1)}s))\cdot P(\Phi_{j+1}(h_{a(j)}\ldots h_{a(1)}s) = \Phi_{j+2}(h_{a(j+1)}h_{a(j)}\ldots h_{a(1)}s))+$$

$$P(\Phi_1(s) \neq \Phi_{j+1}(h_{a(j)}\ldots h_{a(1)}s))\cdot P(\Phi_{j+1}(h_{a(j)}\ldots h_{a(1)}s) \neq \Phi_{j+2}(h_{a(j+1)}h_{a(j)}\ldots h_{a(1)}s))=$$

$$= \frac{1+\delta_{a(1)}\delta_{a(2)}\ldots\delta_{a(j)}}{2}\cdot P(\Phi_{j+1}(h_{a(j)}\ldots h_{a(1)}s) = \Phi_{j+2}(h_{a(j+1)}h_{a(j)}\ldots h_{a(1)}s)) +$$

$$+ \frac{1-\delta_{a(1)}\delta_{a(2)}\ldots\delta_{a(j)}}{2}\cdot P(\Phi_{j+1}(h_{a(j)}\ldots h_{a(1)}s) \neq \Phi_{j+2}(h_{a(j+1)}h_{a(j)}\ldots h_{a(1)}s)) =$$

$$= \frac{1+\delta_{a(1)}\delta_{a(2)}\ldots\delta_{a(j)}}{2}\cdot\frac{1+\delta_{a(j+1)}}{2} + \frac{1-\delta_{a(1)}\delta_{a(2)}\ldots\delta_{a(j)}}{2}\cdot\frac{1-\delta_{a(j+1)}}{2} = \frac{1+\delta_{a(1)}\delta_{a(2)}\ldots\delta_{a(j+1)}}{2}.$$

Замечание 1. При отказе от условия независимости указанных в утверждении 1 событий данное утверждение становится неверным. Так, например, взяв k>1 и слово (a(1), a(2), …, a(k)) так, чтобы $h_{a(k)}\ldots h_{a(1)} = E$, где E – тождественное отображение S в S, и $\Phi_1 = \Phi_{k+1}$, получим $P(\Phi_1(s) = \Phi_{k+1}(h_{a(k)}\ldots h_{a(1)}s)) = 1$, а для функций Φ_1 и $\Phi_{k+1} = \Phi_1+1$ вероятность $P(\Phi_1(s) = \Phi_{k+1}(h_{a(k)}\ldots h_{a(1)}s)) = 0$.

Ниже мы предполагаем независимость указанных в условии утверждения 1 событий для любого слова a(1), a(2), …, a(k) $\in X^k$.

Из утверждения 1 и (7), (8) вытекает

Следствие 1. Значение вероятности

$$P(\Phi_1, \Phi_{k+1}) = P\max_{(a(1), a(2), \ldots, a(k)\in X^k)}(\Phi_1, (a(1), a(2), \ldots, a(k)), \Phi_{k+1})$$

достигается на наборах (a`(1), a`(2), …, a`(k))$\in X^k$, компоненты a`(j), которые удовлетворяют условию

$$P(\Phi j(s) = \Phi j+1(ha`(j)s)) = P\max_{a(j)\in X}(\Phi j(s) = \Phi j+1(ha(j)s)) \qquad (9)$$

Это множество компонент обозначим через $X(\Phi_j, \Phi_{j+1})$, $j\in\{1, \dots k\}$. Положим

$$P \max_{a(j)\in X} (\Phi j(s) = \Phi j+1(ha(j)s)) = \frac{1+\delta_j^*}{2}. \qquad (10)$$

Тогда

$$P(\Phi 1, \Phi k+1) = \frac{1+\delta_1^*\delta_2^*\dots\delta_k^*}{2} \qquad (11)$$

Замечание 2. Трудоемкость (в опробованиях $a\in X$) получения значения вероятности (11) равна

$T_1 = k|X|$.

Здесь в операцию опробования входит и расчет вероятности $P(\Phi_j(s) = \Phi_{j+1}(h_a s))$, которая может быть рассчитана путем нахождения числа решений систем уравнений

$\Phi_j(s) = \Phi_{j+1}(h_a s) = 0$;

$\Phi_j(s) = \Phi_{j+1}(h_a s) = 1$.

Обозначим через $X(\Phi_1, \Phi_2, \dots, \Phi_{k+1})$ множество всех наборов a(1), …, a(k), для которых выполняется (11). Очевидно, что

$$X(\Phi 1, \Phi 2, \dots, \Phi k+1) =$$
$$= X(\Phi 1, \Phi 2) \cdot X(\Phi 2, \Phi 3) \cdot \dots \cdot X(\Phi k, \Phi k+1). \qquad (12)$$

5.3. Первый этап метода

После выбора двоичных функций $\Phi_1, \Phi_2, \dots, \Phi_{k+1}$ и расчета вероятности по формуле (11) строится, как было указано ранее, статистическая процедура разделения гипотез H_0, H_1, трактуя известные состояния $s_1^1, s_1^2, \dots, s_1^N$ как выборку из равномерного распределения на S, а наблюдения $\Phi_1(s_1^j) = \Phi_{k+1}(h_{a(k)}\dots h_{a(1)}s_1^j)$ либо $\Phi_1(s_1^j) \neq \Phi_{k+1}(h_{a(k)}\dots h_{a(1)}s_1^j)$ – как выборку из одного из распределений:

1) $P(\Phi_1(s) = \Phi_{k+1}(h_{b(k)}\dots h_{b(1)}s) = P((\Phi_1, \Phi_{k+1})$, $P(\Phi_1(s) \neq \Phi_{k+1}(h_{b(k)}\dots h_{b(1)}s) = 1 - P(\Phi_1, \Phi_{k+1})$;

2) $P(\Phi_1(s) = \Phi_{k+1}(h_{b(k)}\dots h_{b(1)}s)) = \frac{1}{2}$, $P(\Phi_1(s) \neq \Phi_{k+1}(h_{b(k)}\dots h_{b(1)}s)) = \frac{1}{2}$.

Таким образом, с помощью статистики – расстояния Хэмминга

$$\rho(\Phi_1(s_1^1), \Phi_1(s_1^2), \dots, \Phi_1(s_1^N); \quad \Phi_{k+1}(s_k^1), \Phi_{k+1}(s_k^2), \dots, \Phi_{k+1}(s_k^N))$$

принимается одна из гипотез H_0, H_1. При принятии H_0 делается вывод о том, что искомое решение (b(1), b(2), …, b(k)) системы (1) принадлежит $X(\Phi_1, \Phi_2, \ldots, \Phi_{k+1})$, затем переходят ко второму этапу метода.

Если же принимается гипотеза H_1 – $(b(1), b(2), \ldots, b(k)) \notin X(\Phi_1, \Phi_2, \ldots, \Phi_{k+1})$ то считается, что решение не найдено, метод завершает свою работу. Обозначим через $\alpha = P(H_1/H_0)$, $\beta = P(H_0/H_1)$ ошибки критерия первого и второго рода.

5.4. Второй этап метода

Итак принято решение, что $(b(1), b(2), \ldots, b(k)) \in X(\Phi_1, \Phi_2, \ldots, \Phi_{k+1})$. При этом само множество $X(\Phi_1, \Phi_2, \ldots, \Phi_{k+1})$ нам неизвестно. Рассмотрим два случая:

1) $(b(1), b(2), \ldots, b(k)) \in X(\Phi_1, \Phi_2, \ldots, \Phi_{k+1})$;
2) $(b(1), b(2), \ldots, b(k)) \notin X(\Phi_1, \Phi_2, \ldots, \Phi_{k+1})$.

Первый случай. На втором этапе последовательно ищутся варианты значений компонент b(1), b(2), …, b(k) решения. Опробуются $x(1) \in X$. Для опробуемого варианта x(1) вычисляются состояния $h_{x(1)}s_1^j$, $j \in \{1, \ldots, N\}$ автомата A. Полностью аналогично указанной выше статистической процедуре строится статистический критерий, который с помощью последовательности пар $(h_{x(1)}s_1^1, s_k^1)$, $(h_{x(1)}s_1^2, s_k^2)$, …, $(h_{x(1)}s_1^N, s_k^N)$ и статистики

$$\rho\left(\Phi_2\left(h_{x(1)}s_1^1\right), \Phi_2\left(h_{x(1)}s_1^2\right), \ldots, \Phi_2\left(h_{x(1)}s_1^N\right); \Phi_{k+1}\left(s_k^1\right), \Phi_{k+1}\left(s_k^2\right), \ldots, \Phi_{k+1}\left(s_k^N\right)\right)$$

разделяет гипотезы H_0^1, H_1^1. Гипотеза H_0^1 – состоит в том, что

$$P(\Phi_2(h_{x(1)}s) = \Phi_{k+1}(h_{b(k)\ldots}h_{b(1)}s)) = P(\Phi_2, \Phi_{k+1}),$$

где

$$P(\Phi_2, \Phi_{k+1}) = P\max_{(a(1), a(2), \ldots, a(k) \in X^k)}(\Phi_2, a(2), \ldots, a(k)), \Phi_{k+1}) = P(\Phi_2, b(2), \ldots, b(k)), \Phi_{k+1}) = \frac{1+\delta_2^* \ldots \delta_k^*}{2}.$$

Гипотеза H_1^1 состоит в том, что

$$P(\Phi_2(h_{x(1)}s) = \Phi_{k+1}(h_{b(k)\ldots}h_{b(1)}s)) = \frac{1}{2}.$$

При принятии гипотезы H_0^1 (H_1^1) делается вывод о правильном (о неправильном) определении истинной части b(1) решения.

Обозначим через $\alpha_1 = P(H_1^1/H_0^1)$, $\beta_1 = P(H_0^1/H_1^1)$ ошибки критерия первого и второго рода.

В результате за |X| опробований будет найдено в среднем $(|X|-1)\beta_1$ ложных значений x(1) и истинное значение b(1) будет найдено с вероятностью $1-\alpha_1$. Для каждого найденного значения x(1) = a(1) опробуются все значения x(2). Для опробуемого варианта x(2) по статистике

$$\rho\left(\Phi_1\left(h_{x(2)}h_{a(1)}s_1^1\right), \Phi_3\left(h_{x(2)}h_{a(1)}s_1^2\right), \dots, \Phi_3\left(h_{x(2)}h_{a(1)}s_1^N\right); \Phi_{k+1}(s_k^1), \Phi_{k+1}(s_k^2), \dots, \Phi_{k+1}(s_k^N)\right)$$

принимаются гипотезы:

$$H_0^2 - P(\Phi_3(h_{x(2)}h_{a(1)}s) = \Phi_{k+1}(h_{b(k)\dots}\, h_{b(1)}s)) = P(\Phi_3, \Phi_{k+1}) = \frac{1+\delta_2^*\dots\delta_k^*}{2};$$

$$H_1^2 - P(\Phi_3(h_{x(2)}h_{a(1)}s) = \Phi_{k+1}(h_{b(k)\dots}h_{b(1)}s)) = \frac{1}{2}.$$

При принятии гипотезы H_0^2 делается вывод о правильном определении части x(2)a(1) = b(2)b(1) входного слова автомата. При принятии гипотезы H_1^2 делается вывод о неправильном определении части x(2)a(1) входного слова автомата. Ошибки первого и второго рода критерия обозначим через α_2, β_2. За |X| опробований будет найдено в среднем $(|X|-1)\beta_1|X|\beta_2 + (1-\alpha_1)(|X|-1)\beta_2$ ложных вариантов начальных частей x(2)x(1) решения и с вероятностью $(1-\alpha_1)(1-\alpha_2)$ найдена истинная часть b(2)b(1) решения. Аналогично получаются ложные варианты начальных частей x(3)x(2)x(1) решения. Их будет $((|X|-1)\beta_1|X|\beta_2 + (1-\alpha_1)(|X|-1)\beta_2)|X|\beta_3 + (1-\alpha_1)(1-\alpha_2)(|X|-1)\beta_3$, а истинное значение b(3)b(2)b(1) будет не отсеяно с вероятностью $(1-\alpha_1)(1-\alpha_2)(1-\alpha_3)$.

Положив $\alpha_j = \alpha_1$, $\beta_j = \beta_1$, $j \in \{1, \dots, k\}$, получим, что в результате за $T_2 = k|X|$ опробований будет найдено в среднем

$$T_3 = |X-1||X|^{k-1}\beta_1^k + (1-\alpha_1)|X-1||X|^{k-2}\beta_1^{k-1} + (1-\alpha_1)^2|X-1||X|^{k-3}\beta_1^{k-2} + \dots + (1-\alpha_1)^{k-1}|X-1|\beta_1$$

ложных вариантов решения системы (1). Истинный вариант будет не отсеян с вероятностью $(1-\alpha_1)^k$.

Второй случай: $(b(1), b(2), \dots, b(k)) \notin X(\Phi_1, \Phi_2, \dots, \Phi_{k+1})$. Проводится указанная выше (случай 1) процедура определения вариантов решения системы (1). Трудоемкость процедуры равна $T_2 + T_3$ (T_2 опробований $x \in X$, T_3 опробований частей неизвестной последовательности x(1), x(2), …, x(k)).

5.5. Третий этап метода

На третьем этапе метода проводится опробование полученных вариантов решения в системе (1), то есть для каждого варианта (a(k)a(k–1)…a(1)) проверяется выполнение равенств

$h_{a(k)}h_{a(k-1)}\ldots h_{a(1)}s_1^j = s_k^j$, $j\in\{1, 2, \ldots, N)$.

Таких опробований будет проведено в среднем $T_3+(1-\alpha_1)^k$ в случае 1 и T_3 в случае 2. Таким образом, общая трудоемкость метода (без учета опробования истинного варианта на третьем этапе) выражается величиной

$$T= T_1 + T_2 + T_3 =$$
$$2k|X| + |X-1||X|^{k-1}\beta_1^k+(1-\alpha_1)|X-1||X|^{k-2}\beta_1^{k-1} +$$
$$+ (1-\alpha_1)^2|X-1||X|^{k-3}\beta_1^{k-2} + \ldots + (1-\alpha_1)^{k-1}|X-1|\beta_1.$$

Характеристиками надежности π-метода являются вероятности:

1) $P(H_0)$ – вероятность применения второго этапа метода;

2) вероятность $P((b(1), b(2), \ldots, b(k))\in X(\Phi_1, \Phi_2, \ldots, \Phi_{k+1}))$ при случайном и равновероятном выборе входного слова (b(1), b(2), …, b(k)) из X^k;

3) $(1-\alpha_1)^k$ – вероятность неотсева истинного решения на втором этапе в случае 1.

Рассмотрим события:

1) $(b(1), b(2), \ldots, b(k))\in X(\Phi_1, \Phi_2, \ldots, \Phi_{k+1})$, вероятность этого события равна $\frac{|X(k)|}{|X|^k}$;

2) на первом этапе принята гипотеза H_0, вероятность этого события (при выполнении условия 1) равна $1-\alpha$;

3) на втором этапе истинное решение не отсеялось, вероятность этого события при выполнении условий 1) и 2) есть $(1-\alpha_1)^k$.

При выполнении этих условий на этапе 3 истинное решение будет найдено. Следовательно,

$$\pi \geq \frac{|X(k)|}{|X|^k}(1-\alpha)(1-\alpha_1)^k.$$

Замечание 3. С ростом k вероятность $P(\Phi_1, \Phi_{k+1})$, подсчитанная по формуле (11) при естественных предположениях о границах значений δ^*_j, $j\in\{1, \ldots, k\}$, стремится к ½, что негативно отражается на эффективности рассматриваемого метода. В связи с этим в ряде случаев, можно ограничиться нахождением двоичных функций Φ_1, Φ_2, …, $\Phi_{k`+1}$ для k`<k и расчетом $P(\Phi_1, \Phi_{k`+1})$. В этом случае на пер-

вом этапе метода опробуются «хвосты» x(k`+1)x(k`+2)…x(k) неизвестного решения системы (1). Для опробуемого варианта a(k`+1)a(k`+2)…a(k) с помощью статистики

$$\rho\left(\Phi_1(s_1^1), \Phi_1(s_1^2), \dots, \Phi_1(s_1^N); \Phi_{k`+1}(h^{-1}_{x(k`+1)} \dots h^{-1}_{x(k-1)} h^{-1}_{x(k)} s_k^1), \dots, \Phi_{k`+1}(h^{-1}_{x(k`+1)} \dots h^{-1}_{x(k-1)} h^{-1}_{x(k)} s_k^N)\right)$$

различают гипотезы H_0, H_1:

$$H_0 - P(\Phi_1(s) = (\Phi_{k`+1}(h^{-1}_{x(k`+1)} \dots h^{-1}_{x(k-1)} h^{-1}_{x(k)} s)) = \frac{1+\delta_1^* \dots \delta_{k`}^*}{2},$$

$$H_1 - P(\Phi_1(s) = (\Phi_{k`+1}(h^{-1}_{x(k`+1)} \dots h^{-1}_{x(k-1)} h^{-1}_{x(k)} s)) = \frac{1}{2}.$$

Гипотеза H_0 соответствует опробованию истинной части b(k`+1)…b(k) решения b(1)…b(k`)b(k`+1)…b(k), H_1 – ложной. При принятии гипотезы H_0 переходят к определению оставшейся части решения системы (1). Последняя задача решается полностью аналогично представленной выше задачи. Расчет трудоемкости и надежности такого обобщенного метода с учетом приведенных формул не вызывает затруднений.

5.6. Дополнительные пояснения

Отметим, что значения величин |X(k)|, α, α_1, β_1 непосредственно не следуют из входных данных задачи. В связи с чем представляет интерес следующий комментарий, устанавливающий связь этих параметров с входными данными алгоритма.

Обращаем внимание на то, что выбор функций Φ_1, Φ_2, …, Φ_{k+1} осуществлен так, что в качестве |X(k)| может быть использована мощность множества $|X(\Phi_1, \Phi_2, \dots, \Phi_{k+1})|$. Далее по тексту следует, что

$$X(\Phi_1,\Phi_2, \dots,\Phi_{k+1}) = X(\Phi_1, \Phi_2) \cdot X(\Phi_2, \Phi_3) \cdot \dots \cdot X(\Phi_k, \Phi_{k+1}),$$

в частности, $|X(k)| = |X(\Phi_1, \Phi_2)| \cdot |X(\Phi_2, \Phi_3)| \cdot \dots \cdot |X(\Phi_k, \Phi_{k+1})|$. Множество $X(\Phi_j, \Phi_{j+1})$, $j \in \{1, \dots k\}$ состоит из тех a`(j) из X, для которых выполнено условие

$$P(\Phi_j(s) = \Phi_{j+1}(h_{a`(j)}s)) = P\max_{a(j) \in X} (\Phi_j(s) = \Phi_{j+1}(h_{a(j)}s)) \qquad (13)$$

Для нахождения множества $X(\Phi_j, \Phi_{j+1})$ необходимо предварительно рассчитывать вероятность $P(\Phi_j(s) = \Phi_{j+1}(h_{a(j)}s))$ для всех

$a(j) \in X$. Значение данной вероятности равно $\frac{m_0+m_1}{|S|}$, где m_0 – число решений относительно $s \in S$ системы из двух нулевых уравнений:

$\Phi_j(s) = 0$;

$\Phi_{j+1}(h_{a(j)}s) = 0$,

а m_1 – число решений системы уравнений:

$\Phi_j(s) = 1$;

$\Phi_{j+1}(h_{a(j)}s) = 1$.

Таким образом, вероятность $P(\Phi_j(s) = \Phi_{j+1}(h_{a(j)}s))$ полностью определена функциями $\Phi_1, \Phi_2, \ldots, \Phi_{k+1}$, а множество $X(\Phi_j, \Phi_{j+1})$ получается с помощью равенства (13).

Относительно ошибок $\alpha = P(H_1/H_0)$, $\beta = P(H_0/H_1)$ используемого критерия можно сказать следующее. Их значения зависят от выбора вида критерия различающего указанные гипотезы. Укажем связь ошибок с исходными данными для критерия Неймана-Пирсона, проверяющего гипотезы H_0: $P(\Phi_1(s) = \Phi_{k+1}(h_{b(k)}\ldots h_{b(1)}s) = P((\Phi_1, \Phi_{k+1}) = p_0$ против альтернативы $P(\Phi_1(s) = \Phi_{k+1}(h_{b(k)}\ldots h_{b(1)}s) = \frac{1}{2} = p_1$. Пусть $V = (v_1, v_2, \ldots, v_N)$ – выборка из распределения Бернулли с вероятностью «успеха» p ($P(v = 1) = p$). Критерий Неймана-Пирсона, проверяющего гипотезы H_0: $p = p_0$ против альтернативы $p = p_1$ строится следующим образом. Рассмотрим случай $0 < p_0 < p_1 < 1$. Статистика отношения правдоподобия имеет вид

$$L(V) = \frac{p_1^T(1-p_1)^{N-T}}{p_0^T(1-p_0)^{N-T}} = \frac{p_1^T(1-p_0)^T(1-p_1)^N}{p_0^T(1-p_1)^T(1-p_0)^N},$$

где T – число успехов в выборке ($T = \sum_{j=1}^{N} v_j$).

Так как $p_0 < p_1$, то $\frac{p_1^T(1-p_0)^T}{p_0^T(1-p_1)^T} > 1$. Для любого C можно выбрать t так, что неравенство $L(V) \geq C$ будет эквивалентно неравенству $T \geq t$. Параметры критерия $(v_1, v_2, \ldots, v_N)$, β, n, t таковы, что фиксируя два из них, остальные (два) определяем однозначно. Параметр N уже фиксирован. Фиксируем дополнительно вероятность ошибки первого рода α. Параметры t_α и $(1-\beta)$ – мощность критерия – находят так. Целое число t_α определяют из условия:

$$\alpha`` = \sum_{i=t_\alpha+1}^{n} C_N^i p_0^i (1-p_0)^{N-i} < \alpha \leq \sum_{i=t_\alpha}^{n} C_N^i p_0^i (1-p_0)^{N-i} = \alpha`$$

Возможны два случая: $\alpha = \alpha`$ и $\alpha < \alpha`$.

Если выбранное α совпало с α`, то критерий является нерандомизированным и задается критической областью $\{(v_1, v_2, \ldots, v_N)$:

$T \geq t_\alpha\}$ (областью принятия гипотезы H_1). Вероятность ошибки первого рода α равна вероятности события $T \geq t_\alpha$ при распределении Бернулли с вероятностью «успеха» p_0. Мощность критерия равна вероятности события $T \geq t_\alpha$ при распределении Бернулли с вероятностью «успеха» p_1. Данная вероятность подсчитывается по формуле

$$P(T \geq t_\alpha) = \sum_{i=t_\alpha}^{n} C_N^i p_1^i (1-p_1)^{N-i}.$$

Если $\alpha < \alpha`$, то критерий является рандомизированным и задается критической функцией:

$$\psi_\alpha(T) = \begin{cases} 1 \; при \; T \geq t_\alpha + 1; \\ \frac{\alpha - \alpha``}{\alpha` - \alpha``} \; при \; T = t_\alpha; \\ 0 \; при \; T \leq t_\alpha - 1. \end{cases}$$

Мощность критерия рассчитывается по формуле

$$(1-\beta) = \sum_{i=t_\alpha+1}^{N} C_N^i p_1^i (1-p_1)^{N-i} + (\alpha - \alpha``) \left(\frac{p_1}{p_0}\right)^{t_\alpha} \left(\frac{1-p_1}{1-p_0}\right)^{N-t_\alpha}.$$

При $N \to \infty$, воспользовавшись теоремой Мавра-Лапласа, критерий можно асимптотически задать критической областью

$$\{(v_1, v_2, \ldots, v_N): T \geq Np_0 - u_\alpha \sqrt{Np_0(1-p_0)}\},$$

где $\Phi(u_\alpha) = \alpha$, Φ – функция нормального распределения с параметрами (0, 1). Для $p_1 = p_0 + \frac{\gamma}{\sqrt{N}}$, $\gamma > 0$ мощность критерия при $N \to \infty$ асимптотически равна

$$\Phi\left(\gamma \sqrt{\frac{1}{p_0(1-p_0)}} + u_\alpha\right).$$

Приведем несколько пояснений относительно эффективности рассмотренного метода. Очевидно, эффективность зависит от эффективности статистических критериев. В нашем случае их эффективность растет с ростом величины $|p_0 - p_1|$. В связи с чем можно рекомендовать выбирать функции $\Phi_1, \Phi_2, \ldots, \Phi_{k+1}$ так, чтобы они не были константами и максимизировали или минимизировали вероятность p_0 (см. (11)), так как альтернативная гипотеза состоит в том, что $p = \frac{1}{2}$. Для этого надо при каждом $j \in \{1, \ldots, k\}$ произвести расчет вероятностей $P(\Phi_j(s) = \Phi_{j+1}(h_a s))$, $a \in X$ и найти максимальные значения из них (10). Такие расчеты значительно облегчаются для линейных функций $\Phi_1, \Phi_2, \ldots, \Phi_{k+1}$. В этом случае поиск наилучшей (см. замечание 1) последовательности линейных функций $U_1, \ldots, U_{k+1}$ можно вести последовательно: перебором $2^n - 2$ неконстантных функций U в качестве функции Φ_{j+1} и расчета для функции Uh_a

наилучших линейных статистических аналогов (с помощью быстрого преобразования Фурье), каждый из которых пробуется в качестве функции Φ_j. Напомним читателю основные понятия, связанные с линейными аналогами двоичных функций.

Рассмотрим двоичную функцию $f(x_1, ..., x_n)$: $F_2^n \to F_2$. Будем считать, что ее переменные являются независимыми случайными величинами с распределениями:

$$p(x_i = 1) = p(x_i = 0) = \frac{1}{2}, i \in \{1, 2, \dots n\}.$$

Тогда для любого набора $a = (a_1, \dots, a_n) \in F_2^n$ выполняется равенство $p((x_1, \dots, x_n) = (a_1, \dots, a_n)) = \frac{1}{2^n}$.

Обозначим через $p(f(x_1, \dots, x_n) = 1)$ вероятность того, что при случайном и равновероятном выборе переменных значение функции будет равно единице. Имеем

$$p(f(x_1, \dots, x_n) = 1) = \frac{\|f\|}{2^n} = \frac{\sum_{x \in F_2^n} f(x)}{2^n}, \text{ где } x = (x_1, \dots, x_n).$$

Здесь через $\|f\|$ обозначен вес функции f – число двоичных наборов, на которых она принимает значение, равное единице.

Двоичная функция $g(x)$ называется *статистическим аналогом функции* f(x), если $p(f(x) = g(x)) > \frac{1}{2}$. Здесь $p(f(x) = g(x))$ – вероятность совпадения значений функций f и g при случайном и равновероятном выборе набора $x \in F_2^n$. Очевидно свойство: если $p(f(x) = h(x)) < \frac{1}{2}$, то $p(f(x) = \overline{h(x)}) > \frac{1}{2}$. Здесь $\overline{h(x)} = h(x) \oplus 1$.

На использовании статистических аналогов двоичных функций основан целый ряд статистических методов анализа криптосхем. Основная идея этих методов заключается в замене «сложной» функции $f(x)$, используемой в исследуемой схеме, на один из ее статистических аналогов более простого вида, причем этот аналог $g(x)$ выбирают так, чтобы вероятность $p(f(x) = g(x))$ была максимальной. В этом случае функция $g(x)$ будет нести информацию о многих свойствах исследуемой функции, однако за счет отличия значений функций $f(x)$ и $g(x)$ на некоторых наборах задача из детерминированной становится вероятностной, для решения которой используются статистические методы.

Наиболее изученным классом двоичных функций, для которых имеются достаточно эффективные методы решения систем уравне-

ний, является класс линейных функций. Поэтому зачастую используют линейные статистические аналоги функций.

Пусть $(a, x) = a_1x_1 \oplus \ldots \oplus a_nx_n$ – некоторая линейная функция. Определяют параметр Δ_a^f равенством: $p(f(x) = (a, x)) = \frac{1}{2} + + \frac{\Delta_a^f}{2^n}$.

В приведенных выше обозначениях Δ_a^f называют коэффициентом статистической структуры функции f.

Получим формулу для вычисления коэффициентов статистической структуры:

$$p(f(x) = g(x)) = p(f(x) \oplus g(x) = 0) = 1 - p(f(x) \oplus g(x) = 1) =$$
$$= 1 - \frac{\|f(x) + g(x)\|}{2^n}$$

Тогда $\frac{1}{2} + \frac{\Delta_a^f}{2^n} = 1 - \frac{\|f(x) \oplus (a,x)\|}{2^n}$. Следовательно, $\Delta_a^f = 2^{n-1} - \|f(x) \oplus (a, x)\|$.

Множество $\{\Delta_a^f : a \in F_2^n\}$ называют статистической структурой функции f.

Связь между коэффициентами статистической структуры и коэффициентами Фурье двоичной функции f. Через C_a^f обозначим коэффициент Фурье двоичной функции f . Сначала рассмотрим случай $a = 0$:

$$C_0^f = \frac{1}{2^n} \cdot \sum_{x \in F_2^n} f(x) = \frac{\|f(x)\|}{2^n}, \Delta_0^f = 2^{n-1} - \|f(x)\|,$$

поэтому $\Delta_0^f = 2^{n-1} - 2^n \cdot C_0^f$. Теперь пусть $a \neq 0$:

$$C_a^f = \frac{1}{2^n} \cdot \sum_{x \in F_2^n} f(x) \cdot (-1)^{(a,x)} = \frac{1}{2^n} \cdot \left(\sum_{(a,x)=0} f(x) - \sum_{(a,x)=1} f(x)\right),$$

$$\Delta_a^f = 2^{n-1} - \|f(x) \oplus (a, x)\| = 2^{n-1} - \sum_{x \in F_2^n} (f(x) \oplus (a, x)) =$$

$$= 2^{n-1} - \sum_{(a,x)=0} f(x) - \sum_{(a,x)=1} \overline{f(x)} = \sum_{(a,x)=1} f(x) - \sum_{(a,x)=0} f(x).$$

Поэтому $\Delta_a^f = -2^n \cdot C_a^f$.

Полученные результаты можно использовать для нахождения статистической структуры функции по ее разложению в ряд Фурье, и наоборот. Кроме того, становится очевидным следующее представление двоичной функции через коэффициенты ее статистической структуры: $f(x) = \frac{1}{2} - \frac{1}{2^n} \cdot \sum_{a \in F_2^n} \Delta_a^f \cdot (-1)^{(a,\ x)}$.

5.7. Об эффективности алгоритма

Линейный криптоанализ изобрел японский криптолог Мицуру Мацуи (Mitsuru Matsui). Предложенный им в 1993 г. метод изначально был направлен на вскрытие алгоритма DES[1].

Впоследствии линейный криптоанализ был распространен и на другие алгоритмы[2; 3]. Основные идеи алгоритма ранее были реализованы различными авторами для конкретных блочных шифрсистем. В терминах блочных шифрсистем речь идет линейном методе определения раундовых ключей по множеству пар открытых и соответствующих им шифрованных текстам. В таких публикациях, как правило, речь идет о результатах применения линейного метода, состоящих в указании использованных линейных статистических аналогов и времени вычисления истинного ключа по известным данным: блочный шифр; количество используемых открытых текстов, число раундов. Так, например, линейный криптоанализ Мацуи *r*-раундового DES требует значительного числа открытых текстов. Это следует из табл. 1

Таблица 1

Количество известных открытых текстов для нахождения ключа, в зависимости от количества раундов, по Мацуи*

Количество раундов	Количество известных открытых текстов для нахождения ключа
8 12 16	2^{21} 2^{33} $2^{47} \xrightarrow{\text{Crypto '94}} 2^{43}$ } → Eurocrypt'93

**Источник*: [30].

Сложность атаки связана с количеством необходимых известных открытых текстов, так как для любой пары (открытый текст, шифртекст) требуется небольшое количество вычислений для реализации алгоритма. Например, атака на r = 8 DES занимает 40 с на

[1] Matsui M. Linear Cryptanalysis Method for DES Cipher. – URL: https://www.cs.bgu.ac.il/~beimel/Courses/crypto2001/Matsui.pdf

[2] Ritter T. Linear Cryptanalysis: A Literature Survey. – URL: http://www.ciphersbyritter.com/RES/LINANA.HTM

[3] Biham E., Shamir A. Differential Cryptanalysis of DES-like Cryptosystems // Journal of Cryptology. – 1991. – N 4. – P. 3–72.

рабочей станции, а атака на r = 12 DES занимает 50 ч, что примерно в 4 500 раз больше.

Глава 6. СЛУЧАЙНОЕ ТЕСТИРОВАНИЕ КОНЕЧНЫХ АВТОМАТОВ ПО ВХОДНОЙ И ВЫХОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТЯМ

Предложен метод подсчета надежности случайного тестирования конечного автомата с известным классом возможных неисправностей с целью проверки его исправности.

Основы теории экспериментов с автоматами впервые сформулированы в работе Мура. Систематизация основных результатов проведена в работах [21; 24]. В области изучения контрольных экспериментов с автоматами выделяются работы Хенни, Кайма, Гонсица. Отличительной особенностью, рассматриваемой в настоящей работе, в задачах тестирования, являются следующие условия: тестирование без построения диагностических последовательностей; тестирование без использования контрольных точек; заданы функции переходов и выходов неисправных автоматов; ограничены число возможных контрольных последовательностей и их длины.

Пусть A(0), A(1), …, A(T) – семейство конечных автоматов с входным алфавитом X, множеством состояний S, выходным алфавитом Y, частичными функциями перехода $(h_x^{A(j)})_{x\in X}$, $j\in[0, \ldots, T]$ и выхода $(f_x^{A(j)})_{x\in X}$, $j\in[0, \ldots, T]$, $h_x^{A(j)}: S\to S$, $f_x^{A(j)}: S\to Y$, $x\in X$, $j\in[0, \ldots, T]$. Будем называть автомат A(0) основным автоматом, а автомат A(j), $j\in[0, \ldots, T]$ – автоматом, имеющим неисправность с номером j. Решенная в работе задача состоит в установлении факта, является ли представленный автомат, о котором известно только, что он из семейства {A(0), A(1), …, A(T)}, отличным от основного или нет. Предполагается, что для любого автомата $B\in\{A(0), A(1),\ldots A(T)\}$, любого целого числа K и любой пары $(s, \mathfrak{I})\in S\times X^K$ можно получить выходную последовательность $B(s, \mathfrak{I})$, отвечающую входному слову $\mathfrak{I}$ и начальному состоянию $s\in S$.

Задача решается путем перехода к вероятностной математической модели и построения статистического критерия. Предполагаем, что при наличии всех возможных неисправностей основного автомата A(0) мы получаем соответственно автоматы A(1), …, A(T).

Считаем, что известна и вероятность p(j) любой j-й неисправности, $j \in [1, \ldots, T]$. При отсутствии неисправности получаем автомат A(0). Вероятность отсутствия неисправности p(0). Будем предполагать, что автомат представляется на тестирование с вероятностью p(j), $j \in [0, \ldots, T]$. Таким образом, предполагаем, что на тестирование представляется случайно выбранный автомат $B \in \{A(0), A(1), \ldots, A(T)\}$ и имеет место

$$P(B = A(j)) = p(j),\ j \in \{0, \ldots, T\}, \quad \sum_{i=0}^{T} p(i) = 1.$$

Задача решается на основе сравнения выходных последовательностей основного автомата A(0) и выбранного автомата B, полученных на случайно, независимо и равновероятно выбранных L парах $(s, \Im)_m \in S \times X^K$, $m \in \{1, \ldots, L\}$. В указанных условиях задача сводится к различению двух статистических гипотез: гипотезы H(0), состоящей в том, что B = A(0), и гипотезы H(1), что $B \neq A(0)$.

Для решения задачи применим следующий статистический критерий: гипотеза H(0) принимается, если для всех опробуемых L пар $(s, \Im)_m \in S \times X^K$, $m \in \{1, \ldots, L\}$ выполняются равенства:

$$A(0)((s, \Im)_m) = B((s, \Im)_m),\ m \in \{1, \ldots, L\}, \qquad (14)$$

в противном случае принимается гипотеза H(1). Из характеристик критерия нас интересует вероятность правильного принятия решения, то есть надежность π нашего метода тестирования. Для расчета надежности введем события:

b(j) – событие, состоящее в том, что выбран автомат B = A(j), $j \in \{0, \ldots, T\}$; a – событие, состоящее в выполнении равенств (14) для всех L выбранных пар $(s, \Im)_m$, $m \in \{1, \ldots, L\}$;

$\bar{a}$ – событие, противоположное событию a;

τ – решение принято правильно.

Тогда

$$\pi = P(\tau) = P(\tau/H(0))P(H(0)) + P(\tau/H(1))P(H(1)).$$

Априорные вероятности гипотез H(0) и H(1) соответственно равны

$$P(H(0)) = p(0),\ P(H(1)) = 1 - p(0).$$

Вероятность принятия правильного решения при условии гипотезы H(0) равна 1, то есть $P(\tau/H(0)) = 1$, так как при верности гипотезы H(0) всегда выполняются равенства (1). Вероятность правильного принятия решения при условии гипотезы H(1) совпадает с невыполнением хотя бы одного равенства в (14), а именно

$$P(\tau/H(1)) = P(\bar{a}/H(1)).$$

Так как $P(a) = p(0)+(1-p(0))P(a/H(1))$, откуда

$P(a/H(1)) = \frac{P(a)-p(0)}{1-p(0)}$

и

$P(\tau/H(1)) = 1- P(a/H(1)) = \frac{1-P(a)}{1-p(0)}$.

Таким образом, имеем

$$\pi = P(\tau) = 1 + p(0) - P(a).$$

По формуле полной вероятности

$$P(a) = \sum_{j=0}^{T} P(b(j))P(a/b(j)) = p(0) + \sum_{j=1}^{T} p(j)P(a/b(j))$$

окончательно для π получаем

$$\pi = 1 - \sum_{j=1}^{T} p(j)P(a/b(j)) \qquad (15)$$

Для того чтобы вычислить или оценить надежность метода π, необходимо уметь находить вероятности $P(a/b(j))$, $j\in\{1, \ldots, T\}$. Будем говорить, что пара $(x, s)\in X\times S$ j-непротиворечива (то есть непротиворечива относительно автоматов $A(0)$, $A(j)$), если

$$h_x^{A(0)}s = h_x^{A(j)}s,\ f_x^{A(0)}s = f_x^{A(j)}s.$$

Пару $(\mathfrak{I}, s)\in X^K\times S$, $\mathfrak{I} = x_1, x_2, \ldots, x_K$, назовем j-непротиворечивой, если все пары (x_1, s), $(x_2, h_{x1}^{A(0)}s)$, …, $(x_K, h_{xK-1}^{A(0)}h_{xK-2}^{A(0)}\ldots h_{x1}^{A(0)}s)$ являются j-непротиворечивыми. В противном случае будем говорить, что пара $(\mathfrak{I}, s)$ j-противоречива.

Поскольку предполагается, что структура автоматов $A(j)$, $j\in\{0, \ldots, T\}$ известна, для любого К и j можно выделить множество τ_j^K j-непротиворечивых пар $(\mathfrak{I}, s)\in X^K\times S$ и множество μ_j^K пар $(\mathfrak{I}, s)\in X^K\times S$, для которых $A(0)(\mathfrak{I}, s) = A(j)(\mathfrak{I}, s)$. Очевидно, что $\tau_j^K \subseteq \mu_j^K$.

Так как пары $(\mathfrak{I}, s)$ выбираются случайно равновероятно и независимо из $X^K\times S$, то

$$P(a/b(j)) = \left(\frac{|\mu_j^K|}{|X|^K|S|}\right)^L \geq \left(\frac{|\tau_j^K|}{|X|^K|S|}\right)^L.$$

Отсюда и из (15) имеем

$$\pi = 1 - \sum_{j=1}^{T} p(j) \left(\frac{|\mu_j^K|}{|X|^K|S|}\right)^L \leq 1- \sum_{j=1}^{T} p(j) \left(\frac{|\tau_j^K|}{|X|^K|S|}\right)^L.$$

Когда точные значения мощностей $|\mu_j^K|$, $j\in\{1, \ldots, T\}$ неизвестны для оценки π, можно применить следующую схему рассуждения. Мы уже отмечали, что все j-непротиворечивые пары $(\mathfrak{I}, s)$ принадлежат множеству μ_j^K. Если же пара $(\mathfrak{I}, s)$ j-противоречива, то не ис-

ключена возможность, что она так же принадлежит μ_j^K, поскольку ее j-противоречивость может быть основана лишь на несовпадении значений частичных функций перехода автоматов A(0) и A(j) на некоторых состояниях. В криптографической практике обычно принимается, что если состояния автоматов не совпадают, то вероятность совпадения выходных знаков равна |Y|–1. Если допустить такое предположение для нашего случая, то среднее число j-противоречивых пар, принадлежащих множеству μ_j^K, равно

$$\frac{1}{|Y|^K}\left(|X|^K|S| - |\tau_j^K|\right)$$

и приближенно (с вероятностью 1) можно считать

$$|\mu_j^K| \cong |\tau_j^K| + \frac{1}{|Y|^K}\left(|X|^K|S| - |\tau_j^K|\right).$$

Отсюда

$$\pi \cong 1 - \sum_{j=1}^{T} p(j)\left(\frac{|\tau_j^K| + \frac{1}{|Y|^K}\left(|X|^K|S| - |\tau_j^K|\right)}{|X|^K|S|}\right)^L.$$

Если K достаточно велико ($K \to \infty$), то из предыдущего следует

$$\pi \cong 1 - \sum_{j=1}^{T} p(j)\left(\frac{|\tau_j^K|}{|X|^K|S|}\right)^L \qquad (16)$$

Подсчет мощности множества τ_j^K, $j \in \{1, \ldots, T\}$ можно произвести следующим образом.

Пусть $S = \{1, 2, \ldots, |S|\}$. Обозначим через $\|\alpha_{rm}\|$ матрицу с элементами $(r, m) \in S \times S$, где α_{rm} – число элементов $x \in X$, для которых

$\delta_x^{(A(0))}r = \delta_x^{(A(j))}r = m$, $\beta_x^{(A(0))}r = \beta_x^{(A(j))}r$.

Пусть $\|\alpha_{rm}\|^K = \|\alpha_{rm}^{(K)}\|$ – K-я степень матрицы $\|\alpha_{rm}\|$.

Тогда $\|\tau_j^K| = \sum_{r,\ m=1}^{|S|} \alpha_{rm}^{(K)}$.

Как видно из изложенного выше, расчет параметров критерия в общем случае является задачей достаточно сложной, когда число состояний автомата велико. Трудоемкость практического применения рассмотренного метода тестирования в числе опробования на один такт работы автомата не превосходит $K \cdot L$. Значения параметров K и L определяются из формулы (15) при заданном π. Сформулированные результаты могут оказать помощь и в практическом решении проблемы соответствия созданных устройств их начальным схемам и законам функционирования.

Часть 2. МОДЕЛИ АВТОМАТОВ НА ОСНОВЕ СЛЕДСТВИЙ ЗАКОНОВ ИХ ФУНКЦИОНИРОВАНИЯ

В данной части будет рассмотрено построение для сложных автоматов их моделей – более простых автоматов, помогающих в решении конкретных задач для автомата – оригинала.

Пусть задан некоторый конечный автомат A = (X, S, Y, h, f). Для криптографических приложений задача моделирования в теории автоматов состоит в том, чтобы исходя из данных о внешнем функционировании автомата A построить более простой автомат A', достаточно адекватно описывающий поведение автомата A. Под словами «более простой» обычно понимают автомат с меньшим числом состояний по сравнению с исходным автоматом. При этом автомат A' может описывать внешнее поведение автомата A не полностью, а приближенно. В этом случае говорят о приближенных моделях автоматов. Мы изучаем четыре подхода к решению задачи приближенного моделирования автоматов.

Первый подход к решению проблемы моделирования состоит в построении для исходного автомата A нового автомата, являющегося некоторым следствием законов функционирования автомата A [13]. Ниже мы будем использовать более узкое понятие: под следствием автомата A будет пониматься новый автомат A', являющийся последовательным соединением A и автомата-функции, входом которого служит множество Y^L, $L \geq 1$.

Второй подход состоит в том, что на множестве всех автоматов с общими входным и выходным алфавитами вводится функция близости μ, для определения которой используется расстояние Хэмминга между выходными последовательностями.

Третий подход к построению приближенных моделей обобщает идеи приближения сложной дискретной функции более простой функцией (например, линейной). В автоматной трактовке этот подход состоит в замене исходного автомата A на его статистический аналог A'. Аналог выбирается так, чтобы решаемая задача для автомата A имела для автомата A' достаточно простое по сложности решение, и одновременно табличное задание автомата A' не намного отличалось от табличного задания автомата A. В этом случае замена A на A' позволяет снизить сложность решения за счет некоторой ненадежности ее решения.

Четвертый подход к построению приближенных моделей состоит в получении следствий из уравнений функционирования автомата А путем обобщения понятия гомоморфизма автоматов и построении обобщенных образов автомата А при таких обобщенных гомоморфизмах. Этот подход связан с тем, что гомоморфный образ автомата в ряде практических задач играет роль его модели. Суть обобщения понятия гомоморфизма состоит в рассмотрении бинарных отношений вместо отображений, входящих в определение гомоморфизма. Таким образом, расширяется класс автоматов, имеющих гомоморфный образ с меньшим числом состояний, до класса автоматов, имеющих обобщенный гомоморфный образ с меньшим числом состояний.

Глава 7. МОДЕЛИ АВТОМАТОВ – СЛЕДСТВИЯ УРАВНЕНИЙ ИХ ФУНКЦИОНИРОВАНИЯ

В этой главе изучаются возможности построения для исследуемого автомата А его моделей – следствий, то есть новых автоматов, уравнения функционирования которых являются следствиями уравнений функционирования исходного автомата. Эти модели – следствия будут далее называться *образами автомата А при его обработках.* Целью построения таких образов для А 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 А. Основные результаты работы ранее опубликованы в тезисах работ [10; 13].

7.1. Основные обозначения

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

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

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

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 читателю и основные понятия теории автоматов [24; 32].

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), A` = (X , S`, Y, h`, f`).

Автоматы A, A` считаются *неотличимыми*, если для любого состояния $s\in S$ автомата A найдется неотличимое от него состояний $s`\in S`$ 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 полугруппу 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 *перестановочным*, 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 и специальное обозначение 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.

7.2. Построение моделей-следствий автомата

Пусть A = (X, S, Y, h, f) – конечный автомат. Под обработкой степени к будем понимать произвольное отображение

Φ: $X^к \times Y^к \to Y`$, где $Y`$ – некоторый алфавит. *Образом автомата A при обработке Ф* назовем автомат $A_\Phi = (X^к, S, Y`, h_\phi, f_\phi)$ с функцией перехода

$$h_\phi(s, x(1), x(2), \ldots, x(к)) = h(s, x(1), x(2), \ldots, x(к)) = h_{x(к)}h_{x(к-1)}\ldots h_{x(1)}s$$

и выхода

$$f_\phi(s, x(1), x(2), \ldots, x(к)) = \Phi(x(1), x(2), \ldots, x(к), A(s, x(1), x(2), \ldots, x(к)),$$

где $s \in S$, $(x(1), x(2), \ldots, x(к))$ – входной символ автомата A_Φ, $(x(1), x(2), \ldots, x(к)) \in X^к$.

Указанный автомат A_Φ обладает следующим свойством. Если при входной последовательности

$$x(1), x(2), \ldots, x(Lк) = P(1), P(2), \ldots, P(L), P(j) = x((j-1)к+1), \ldots, x(jк), j \in \{1, \ldots, L\}$$

и начальном состоянии $s \in S$ выходная последовательность автомата A есть $A(s, x(1), x(2), \ldots, x(Lк)) = y_1, y_2, \ldots, y_{Lк} = У_1, У_2, \ldots, У_L$, то выходная последовательность автомата A_Φ, соответствующая входной последовательности $P(1), P(2), \ldots, P(L)$ и начальному состоянию $s \in S$, определяется равенством

$$A_\Phi(s, P(1), P(2), \ldots, P(L)) = \Phi_{P(1)}(У_1), \Phi_{P(2)}(У_2), \ldots, \Phi_{P(L)}(У_L),$$

где $\Phi_{P(j)}(У_j) = \Phi(P(j), У_j)$, $У_j = y_{(j-1)к+1}, \ldots, y_{jк}$, $j \in \{1, \ldots, L\}$. Таким образом, функционирование автомата A_Φ представимо схемой, показанной на рис. 2.

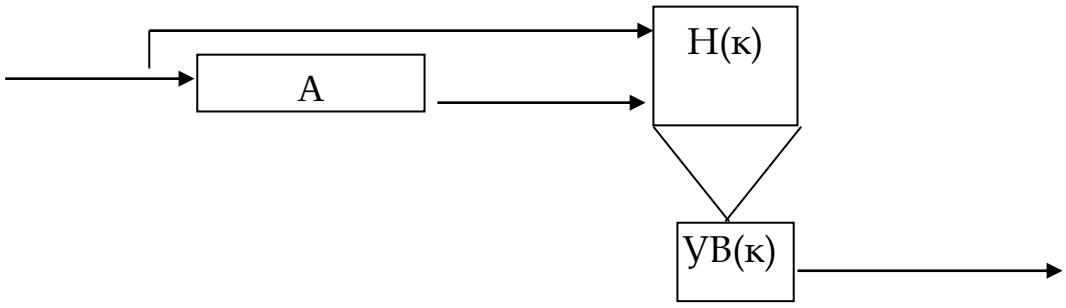

Рис. 2

Здесь Н(к) – проходной накопитель на к знаков $\begin{pmatrix} x \\ y \end{pmatrix}$, УВ(к) – узел выборки шага к.

Определение 1. Автомат A называется слабо неприведенным автоматом, если для него существует обработка Ф, при которой его образ A_Φ является неприведенным автоматом с числом классов не-

отличимых состояний больше единицы. В противном случае, автомат A называется сильно приведенным.

Очевидно следующее утверждение.

Утверждение 1. Для автомата A тогда и только тогда найдется обработка Φ: $X^к \times Y^к \to Y`$, при которой автомат $A_ф$ имеет гомоморфный приведенный образ с числом состояний $|S`|$, $2 \le |S`| \le |S| - 1$, 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:

$$P(S) = \{Z_j: j \in \{1, \ldots, t\}\}, \quad 2 \le t \le |S| - 1, \quad Z_j \cap Z_{j`} = \varnothing, j \ne j`, j, j` \in \{1, \ldots, t\}$$

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 $j \in \{1, \ldots, t\}$ существует $j` \in \{1, \ldots, t\}$, 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 только такие автоматы, у которых число состояний больше единицы и не все частичные функции выхода постоянны на всем множестве состояний.

Очевидно следующее утверждение.

Утверждение 2. Любой неприведенный автомат является слабо неприведенным автоматом.

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

$$An(M) = (X_n, S, (hP: P \in Xn)), \; hP = hx(n)hx(n-1)\ldots hx(1)$$

при $P = (x(n), x(n-1), \ldots, x(1)) \in Xn$.

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

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 к, при котором образ автомата А при обработке степени к является слабо неприведенным автоматом.

Ниже мы сужаем класс исследуемых автоматов до класса диагностируемых автоматов. Заметим, что в этот класс входят приведенные перестановочные автоматы. Полное описание слабо неприведенных диагностируемых автоматов дает теорема 1.

Теорема 1. Приведенный диагностируемый автомат А слабо неприведен тогда и только тогда, если 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 А выполнены условия теоремы. Обозначим через $Z_1, Z_2, \ldots, Z_t$ некоторую систему его блоков импримитивности. Выберем произвольное натуральное число к не меньше минимальной длины К(А) диагностической последовательности автомата А, положим $Y` = \{1, 2, \ldots, t\}$, отображение $\Phi$: $X^к \times Y^к \to Y`$ зададим с помощью функций Φ_P: $Y^к \to Y`$, $P \in X^к$ следующим образом:

1. Для произвольного $P \in X^к$ введем бинарное отношение σ_P на блоках $Z_1, Z_2, \ldots, Z_t$ системы импримитивности автомата А. Блоки Z, Z` находятся в отношении $\sigma_P$ ($Z\sigma_P Z`$) 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 $\{Z_1, Z_2, \ldots, Z_t\}$. Для каждого класса эквивалентности Z^ бинарного отношения эквивалентности σ^*_P определим минимальный номер блока из $\{Z_1, Z_2, \ldots ,Z_t\}$, принадлежащий классу Z^.

2. Пронумеруем этими номерами $\{j(1), j(2), \ldots, j(t(P))\}$, классы отношения эквивалентности σ^*_P. Пусть $\{Z^\wedge_{j(1)}, Z^\wedge_{j(2)}, \ldots, Z^\wedge_{j(t(P))}\}$ – классы эквивалентности отношения σ^*_P.

3. Для $s \in Z_j$, а $Z_j \in Z^\wedge_{j(v)}$. Положим

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

Таким образом мы пока задали значения отображение Φ на всех парах вида:

$$(P, A(s, P),\ s \in S, P \in X^к.$$

На парах $(P, У_j) \in X^к \times Y^к$, не входящих в указанное множество пар, значение Φ выбираем произвольным образом. Ясно, что частичные функции выходов автомата A_Φ, являющегося образом автомата А при обработке Φ, постоянны на блоках $\{Z_1, Z_2, \ldots, Z_t\}$ си-

стемы импримитивности автомата A. Заметим, что эти блоки в то же время являются блоками системы импримитивности автомата $A_ф$ 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 $\mathfrak{I}$ длины $K(A) \le к$. Рассмотрим фиксированную последовательность $\mathfrak{I}P$ длины к, начальное слово которой есть $\mathfrak{I}$. Тогда выходные последовательности $(A(s, \mathfrak{I}P: s \in S)$ автомата A попарно различны и по построению отношения эквивалентности $\sigma^*_{\mathfrak{I}P}$ классы этого отношения есть Z_1, Z_2, …, Z_t, то есть совпадают с блоками импримитивности автомата $A_Ф$ и $Ф(\mathfrak{I}P, A(s, \mathfrak{I}P) = j$, если $s \in Z_j$, $j \in \{1, \ldots, t\}$. Следовательно, частичная функция выходов $f_{Ф, \mathfrak{I}P}$ автомата $A_Ф$ непостоянна на S.

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

$$A^n = ((Xn, S, Yn, (hP: P \in Xn), (fP: P \in Xn))$$

с частичными функциями переходов

$$hP = hx(n)hx(n-1)\ldots hx(1)$$

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

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

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

Так как по условию автомат A^n импримитивен, то импримитивен и автомат $A^n(M)$, при этом он, очевидно, также как и A, диагностируемый автомат. По доказанному ранее частному случаю, для автомата A^n найдется обработка

$$Ф`: (Xn)к \times (Yn)к \to Y`$$

некоторой степени к, при которой образ $A^n_{Ф`}$ автомата $A^n$ больше единицы. Автомат $A^n_{Ф`}$ имеет вид $A^n_{Ф`} = (X^{кn}, S, Y`, h`_{Ф`}, f`_{Ф`})$. Очевидно, функцию Ф`, определенную на словах длины к алфавита $X^n$ можно трактовать и как функцию Ф, определенную на словах длины кn алфавита X, принимающую те же значения, что и Ф`. Непосредственно проверяется, что образ $A_Ф$ автомата A при обработке

$$Ф: Xnк \times Ynк \to Y`$$

совпадает с автоматом $A^n_{\Phi`}$ и, следовательно, автомат A слабо неприведен.

Терема доказана.

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

7.3. Изучение примитивности степеней автомата

Предварительно введем необходимые обозначения. Для полугруппы $G=<(h_x)_{x\in X}>$ 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 Г(G) – граф полугруппы G. Вершинами графа являются элементы $g\in G$. Из вершины g проводится ориентированная дуга в вершину g` с пометкой $x\in X$ тогда и только тогда, когда $gh_x = g`$. Под элементарным контуром графа Г(G) будем понимать путь из некоторой его выбранной вершины в эту же вершину, не содержащий одинаковых вершин. Обозначим через D наименьшее общее кратное длин элементарных контуров. Через $M_к$ обозначим к-й слой полугруппы $G = <(h_x)_{x\in X}>$, то есть множество всех ее элементов, представимых положительными словами $h_{x(к)}\ h_{x(к-1)}\ldots h_{x(1)}$ длины к из образующих $<(h_x)_{x\in X}>$. Если G содержит тождественное преобразование S, то она представима в виде $G = G`\cup G``$, где G` – подполугруппа группы G, не содержащая биективнных отображений S в S, а G`` – подполугруппа G, состоящая из всех биективных отображений полугруппы G. Через d(G``) будем обозначать ширину группы G``, именно 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 утверждения:

1) при любом натуральном j: $M_{|G|+j} \subseteq M_{|G|+j+D}$;

2) последовательность множеств $M_1, M_2, \ldots, M_к, \ldots$ 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) с условием $|G|+L^*D+1 \le h(G) \le |G|+L^*D+D`$, при котором слой $M_{h(G)}$ является подполугруппой полугруппы G и кроме того

$$M_{h(G)} = \mathop{\mathrm{I}}_{h=1}^{\infty} G_h ,$$

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 $M_1, M_2,\ldots, M_к,\ldots$ смешанно периодическая с длиной подхода L(G)–1 и периодом d(G``); найдется натуральное число h(G), $L(G)\le h(G)\le L(G)+d(G``)-1$, при котором $M_{h(G)}$ является полугруппой и

$$G_{d(G``)} = M_{h(G)} = \mathop{\mathrm{I}}_{h=1}^{\infty} G_h .$$

Доказательство. Рассмотрим произвольный элемент g из $M_{|G|+j}$, $j\in\{1, 2, \ldots\}$.

Он может быть представлен в виде $g = h_{x(1)}h_{x(2)}\ldots h_{x(|G|+j)}$ при некоторых $x_k\in X$, $k\in\{1, 2, \ldots, |G|+j\}$. Тогда в графе Г(G) имеется путь вида

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

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

$$h_{x(1)}h_{x(2)}\ldots h_{x(к)} \xrightarrow{x(к+1)}$$
$$h_{x(1)}h_{x(2)}\ldots h_{x(к+1)} \xrightarrow{x(к+2)} \ldots \xrightarrow{x(к+p)} h_{x(1)}h_{x(2)}\ldots h_{x(к+p)},$$

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

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

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

$$M_{|G|+1}\subseteq M_{|G|+1+D}\subseteq\ldots\subseteq M_{|G|+1+кD},\ к\in\{1, 2, \ldots\}.$$

По определению величины L* имеем $M_{|G|+L^*D+1} = M_{|G|+L^*D+1+D}$. Используя эти соотношения, непосредственно проверяем справедливость равенств

$$M_{|G|+L^*D+1} = M_{|G|+L^*D+1+кD},\quad к\in\{0, 1, \ldots\}.$$

Откуда вытекает

$$M_{|G|+L^*D+1+j} = M_{|G|+L^*D+1+j+кD},\quad j, к\in\{0, 1, \ldots\}.$$

Таким образом, доказаны утверждения 1), 2) теоремы 2.

Определим натуральное число h(G) (утверждение 3)исходя из условий:

a) $|G|+L*D+1 \le h(G) \le |G|+L*D+D`$;

b) h(G) кратно D`.

Тогда очевидно, что $M_{h(G)} \cdot M_{h(G)} = M_{h(G)+h(G)} = M_{h(G)}$ (здесь $M_{h(G)} \cdot M_{h(G)}$ – произведение множеств подстановок). Следовательно, $M_{h(G)}$ – полугруппа и

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

В частности, при $\kappa(0)h \ge h(G)$ и $\kappa(0)h$, кратном D`, $\kappa(0) \in \{1, 2, \ldots\}$ имеем $G_h \supseteq M_{\kappa(0)h}$, $M_{\kappa(0)h} = M_{h(G)}$, откуда получаем

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

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

$$|M_1| \le |M_2| \le \ldots \le |M_j| \le \ldots \quad .$$

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

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

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

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

Обозначим через d = d(G``) ширину подгруппы G`` полугруппы G. Напомним [46], что шириной группы в фиксированных образующих называют минимальное количество ее слоев, покрывающих ее как множество. Известно [46], 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 $\kappa(0)$, при котором $\kappa(0)d \ge L(G)$, $E \in M_{\kappa(0)d}$, $E \in M_{\kappa(0)d+d}$, E – единица группы G``. Тогда при любом $j \in \{0, 1, \ldots\}$

$$M_{\kappa(0)d+j} \cdot M_{\kappa(0)d} = M_{\kappa(0)d+j+\kappa(0)d} = M_{\kappa(0)d+j};$$

$$M_{\kappa(0)d+j} \cdot M_{\kappa(0)d+d} = M_{\kappa(0)d+j+\kappa(0)d+d} = M_{\kappa(0)d+j}.$$

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

Каждый слой M_j, $j\in\{1, 2, \ldots\}$ 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 $M_1``$, $M_2``$,… есть d. Учитывая, что D` должно делить d, а ранее было показано, что d делит D`, заключаем: D` = d.

Определим натуральное число h(0) = H(G) исходя из условий:

$L(G)\leq h(0)\leq L(G)+d-1$ и $E\in M_{h(0)}$. Очевидно, $M_{h(0)}$ – полугруппа и $M_j\subseteq M_{h(0)+j}$, $j\in\{1, 2, \ldots\}$. Поэтому

$$G_d = M_{h(0)} = \mathop{\mathrm{I}}_{h=1}^{\infty} G_h .$$

Доказательство теоремы завершено.

Следствие теоремы 2. 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 $G_d = M_{h(0)} = \mathop{\mathrm{I}}_{h=1}^{\infty} G_h$.

Замечание к теореме 2. 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,… группы $G = <(h_x)_{x\in X}>$ получены ранее М. М. Глуховым в [28]. 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 $G = <(h_x)_{x\in X}>$, заданной системой образующих элементов $<(h_x)_{x\in X}>$ и некоторой системой положительных определяющих слов (соотношений), и $G_n = <(h_P:P\in X^n)>$ – подгруппа группы G, порожденная всеми возможными положительными словами $h_{x(n)}h_{x(n-1)}\ldots h_{x(1)}$ длины n. Тогда найдется n(0), при котором $G_d = M_{n(0)} = \mathop{\mathrm{I}}_{n=1}^{\infty} G_n$, 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 $G_n = <(h_P: P\in X^n)>$ является нормальным делителем группы G, по которой образующие $<(h_x)_{x\in X}>$ 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 $G_n = <(h_P:P\in X^n)>$ импримитивна, то из $G_d = M_{n(0)} = \mathop{\mathrm{I}}\limits_{n=1}^{\infty} G_n$ следует, что импримитивна и группа G_d. Если не существует n, при котором группа $G_n = <(h_P:P\in X^n)>$ импримитивна, то G_d примитивна. Из примитивности G_d вытекает примитивность всех групп G_n, $n\in\{1, 2, \ldots\}$. Следовательно (см. теорему 1), справедлива теорема 3.

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 $G = <(h_x)_{x\in X}>$ 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), …, d(m)}, среди которых должен содержаться параметр d группы G, и установить примитивность групп $G_{d(1)}, G_{d(2)}, \ldots, G_{d(m)}$. Если при этом хотя бы одна из указанных групп окажется импримитивной, то импримитивна группа $M_{n(0)} = \mathop{\mathrm{I}}\limits_{n=1}^{\infty} G_n$ и автомат A слабо неприведен.

Отметим еще одну возможность. Обозначим через $<(h_x h_{x`}^{-1})_{x,x`\in X}>$ подгруппу группы G перестановочного автомата A, порожденную элементами $(h_x h_{x`}^{-1})_{x,\, x`\in X}$.

Очевидно, $(h_x h_{x`}^{-1})_{x,\ x`\in X}$ 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 $<(h_x h_{x`}^{-1})_{x,\, x`\in X}>$.

Глава 8. МОДЕЛИ АВТОМАТОВ, ПОСТРОЕННЫЕ С ПОМОЩЬЮ ОБРАБОТКИ ИХ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ИНИЦИАЛЬНЫМИ АВТОМАТАМИ

Предлагаются способы построения моделей конечного автомата – новые неприведенные автоматы, получаемые с помощью задания дополнительных функций – автоматных отображений на его выходных словах. Криптографические приложения результатов связываются с задачей определения состояния автомата по его входным и соответствующим выходным последовательностям.

В данной главе 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 при его обработках с помощью инициальных автоматов. 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. Используются известные понятия теории автоматов [10; 24]. Основные результаты работы ранее опубликованы в тезисах [14].

8.1. Построение моделей – следствий автомата. Постановка задачи

Пусть $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ – конечный автомат. $B_{q(0)}$ – инициальный автомат Мура с входным алфавитом $X\times Y$, множеством состояний S^B, начальным состоянием $q(0)$, частичными функциями переходов $({}^Bh_{x,\,y})_{(x,\,y)\in X\times Y}$ и функцией выхода E: $S^B\to S^B$, $Eq = q$ при каждом состоянии q из S^B.

Инициальным автоматом $B_{q(0)} = (X\times Y, S^B, ({}^Bh_{x,y})_{(x,y)\in X\times Y})$ задано отображение $(X\times Y)^*$ в $(S^B)^*$:

$$B_{q(0)}(q(0), x(1), x(2), \ldots, x(к), y(1), y(2), \ldots, y(к)) = q(0), q(1), \ldots, q(к).$$

Рассмотрим последовательное соединение $C = A \to B_{q(0)}$ автоматов A и $B_{q(0)}$, $C = (X, S \times S^B, ({}^C h_x)_{x \in X})$, ${}^C h_x(s, q) = (h_x s, {}^B h_{x,\, y} q)$, где $y = f_x s$, $s \in S$, $q \in S^B$ (рис. 3).

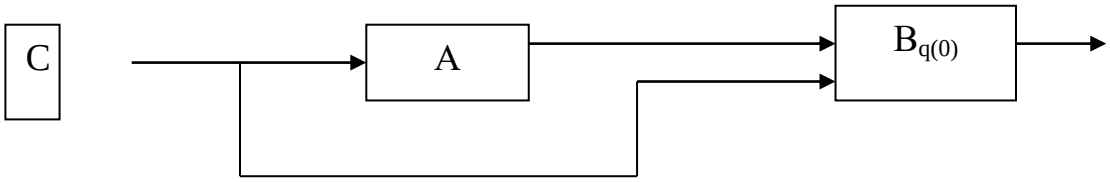

Рис. 3

Выходным словом C(s, q, P) автомата C при входном слове $P \in X^*$ и начальном состоянии $(s, q) \in S \times S^B$ будет последовательность состояний автомата $B_{q(0)}$, отвечающая входной последовательности (P, A(s, P)) и его начальному состоянию $q \in S^B$. Автомат C, построенный для A с помощью $B_{q(0)}$, будем называть *обработкой автомата A с помощью* $B_{q(0)}$. Нас будет интересовать наличие неотличимых состояний в подмножестве $S \times \{q(0)\}$ множества $S \times S^B$ обработки C автомата A с помощью $B_{q(0)}$. Наличие таких неотличимых состояний можно использовать при решении задачи определения начального состояний автомата A по его входной последовательности P и выходной последовательности A(s, P) аналогично тому как используется гомоморфный образ автомата A с меньшим числом состояний, чем у A [29].

Определение 1. Состояния s, s`$\in$S автомата A называются неотличимыми относительно $B_{q(0)}$, если состояния (s,q(0)), (s`,q(0)) неотличимы в автомате $C = A \to B_{q(0)}$, в противном случае s, s` – различимы относительно $B_{q(0)}$.

Определение 2. Автомат A называется неприведенным относительно $B_{q(0)}$, если множество состояний S автомата A содержит пару различимых состояний и пару различных неотличимых состояний относительно $B_{q(0)}$.

Через B(X, Y) обозначим множество всех инициальных автоматов вида $B_{q(0)} = (X \times Y, S^B, ({}^B h_{x,\, y})_{(x,\, y) \in X \times Y})$ с входным алфавитом $X \times Y$ и тождественной функцией выхода на состояниях.

Определение 3. Автомат A называется слабо неприведенным относительно B(X,Y), если найдется автомат $B_{q(0)}$ из B(X, Y) такой, что автомат A не приведен относительно $B_{q(0)}$, в противном случае автомат A называется сильно приведенным относительно B(X, Y).

8.2. Описание слабо неприведенных автоматов относительно B (X, Y)

Решим задачу описания слабо неприведенных автоматов относительно B(X, Y).

Для автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ при $P = x(1), x(2), \ldots, x(к)$ и $W\subseteq S$ положим

$$f_P = f_{x(к)}h_{x(к-1)}\ldots h_{x(1)},\ h_P = h_{x(к)}h_{x(к-1)}\ldots h_{x(1)},\ f_PW = \{y\in Y: f_Ps = y,\ s\in W\}.$$

Определение 4. Подмножества $W_1\subseteq S$, $W_2\subseteq S$ множества S автомата A называются неотличимыми в автомате A, если для любого $P\in X^*$

$$f_PW_1\cap f_PW_2 \neq \varnothing.$$

В противном случае W_1, W_2 различимы в A.

Отметим, что понятие неотличимости состояний автомата A получается из определения 4 в случае одноэлементных множеств W_1, W_2.

Теорема 1[1]. Автомат A с $|S|\geq 3$ слабо неприведен относительно B(X, Y) тогда и только тогда, когда найдутся подмножество $W\subset S$, $|W|=2$ и состояние $s\in S$, $s\notin W$, такие, что множества W и $\{s\}$ различимы в A.

Доказательство. Пусть A слабо неприведен относительно B(X, Y), то есть нашлись автомат $B_{q(0)}$ и состояния $(s_1, s_2, s_3)\in S$, $s_1 \neq s_2$, при которых состояния $(s_1, q(0))$, $(s_2, q(0)$ неотличимы в автомате $C = A\to B_{q(0)}$, а состояние $(s_3, q(0))$ различимо с $(s_1, q(0))$, следовательно и с $(s_2, q(0))$. Пусть $P = x(1), x(2), \ldots, x(к)$ – слово минимальной длины, при котором

$$C(s_1, q(0), P) = C(s_2, q(0), P) \neq C(s_3, q(0), P).$$

Тогда

$$f_P\{s_1, s_2\}\cap f_P\{s_3\} = \varnothing,$$

откуда следует различимость множеств $W = \{s_1, s_2\}$, $\{s_3\}$ в A.

Предположим теперь, что нашлось подмножество $W\subset S$ и $s\in S$, удовлетворяющие условиям теоремы. Для доказательства слабой неприведенности автомата A относительно B(X, Y) построим вспомогательный автомат $B_{q(0)}$. *Через* $G = \langle (h_x)_{x\in X}\cup e\rangle$ *обозначим полугруппу автомата A с добавленной единицей e.* Положим

[1] Теорема доказана автором совместно с Д. В. Шашкиным.

$$B_{q(0)} = (X\times Y,\ S^B\cup t,\ (h_{x,y})_{(x,y)\in X\times Y}),$$

где $S^B = \{gW: g\in G\}$, (gW – образ W при отображении g), $t = \varnothing$ – пустое подмножество S. Частичные функции переходов $(h_{x,\ y})_{(x,\ y)\in X\times Y}$ определим следующим образом:

$$h_{x,\ y}W` = h_xW`, \text{ если } y\in f_xW` \quad \text{и} \quad h_{x,\ y}W` = t, \text{ если } y\notin f_xW`,$$

$$W`\in S^B,\ h_{x,\ y}t = t.$$

Выходной последовательностью автомата $B_{q(0)}$ является последовательность его состояний. В качестве начального состояния $q(0)$ инициального автомата $B_{q(0)}$ взято W ($q(0) = W$). По построению $B_{q(0)}$ ясно, что состояния $(s_1, q(0))$, $(s_2, q(0))$, где $\{s_1, s_2\} = W$, неотличимы в автомате C. Покажем, что состояния $(s, q(0))$, $(s_1, q(0))$ различимы в C. По условию W и одноэлементное множество $\{s\}$ различимы в A. Пусть $P = x(1), x(2), \ldots, x(к)$ – слово минимальной длины, при котором $f_Ps\notin f_PW$. Тогда по построению $B_{q(0)}$ для слова $Px = x(1), x(2), \ldots, x(к), x$ вытекает

$$C(s_1, q(0), Px) = W, h_{x(1)}W, \ldots, h_{x(к-1)}\ldots h_{x(1)}W, h_{x(к)}\ldots h_{x(1)}W$$

$$C(s, q(0), Px) = W, h_{x(1)}W, \ldots, h_{x(к-1)}\ldots h_{x(1)}W,\ t,$$

так как $f_{x(к)}h_{x(к-1)}\ldots h_{x(1)}s\notin f_{x(к)}h_{x(к-1)}\ldots h_{x(1)}W$. Таким образом, состояния $(s_1, q(o))$, $(s, q(o))$ различимы в C, то есть автомат A слабо неприведен относительно $B(X, Y)$.

Теорема 1 доказана.

Укажем алгоритм проверки слабой неприведенности заданного автомата A относительно $B(X, Y)$. Ясно, что если $|S|\le 2$, то A сильно приведен. Пусть $|S|\ge 3$. Для каждой тройки s_1, s_2, s_3 попарно различных состояний автомата A полагаем $W= \{s_1, s_2\}$, находим множество $\{(gW): g\in G\}$. Для каждого элемента gW и $x\in X$ проверяем условие $f_xgs_3\notin f_xgW$. Если для некоторой тройки s_1, s_2, s_3 нашлись gW и $x\in X$, для которых это условие выполнено, то A – слабо неприведенный автомат, в противном случае A – сильно приведенный автомат.

С использованием теоремы 1 несложно доказывается следующее следствие.

Следствие. Автомат $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ с числом состояний $|S|\ge 3$, у которого не все частичные функции выхода постоянны на S, является слабо неприведенным автоматом относительно $B(X, Y)$.

Согласно следствию, для определения информации о начальном состоянии автомата A, удовлетворяющего условиям следствия, по его входным и выходным последовательностям всегда можно

использовать обработку автомата A с помощью некоторого инициального автомата $B_{q(0)}$. Эффективность такого приема решения задачи зависит от мощностей и числа классов неотличимых состояний (на множестве $S\times\{q(0)\}$) автомата C, построенного с помощью $B_{q(0)}$, в связи с чем представляет интерес описание условий, при которых для заданного автомата A можно найти $B_{q(0)}$ с заданными параметрами классов неотличимых состояний автомата C. Ниже решается поставленная задача.

Для произвольного разбиения $R_S = \{S_1, S_2, \ldots, S_L\}$ множества состояний S автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ и входного слова $P\in X^*$ определим бинарное отношение σ_P на множестве R_S, положив $S_j\sigma_P S_{j`}$ тогда и только тогда, когда $f_P S_j \cap f_P S_{j`} \neq \varnothing$. Через σ_P^* обозначим транзитивное замыкание σ_P на R_S.

Определение 5. Блоки S_j, $S_{j`}$ разбиения $R_S = \{S_1, S_2, \ldots, S_L\}$ $\sigma(к)^*$– неотличимы (для автомата A) тогда и только тогда, когда для любого $P\in \bigcup_{i=1}^{к} X^i$ выполняется $S_j\sigma_P^* S_{j`}$. Если блоки S_j, $S_{j`}$ $\sigma(к)^*$– неотличимы при любом $к\in\{1, 2, \ldots\}$, то они σ^*-неотличимы. В противном случае они σ^*-различимы. Очевидно, что для автомата A найдется $к\in\{1, 2, \ldots\}$, при котором $\sigma(к)^* = \sigma^*$. Минимальное к с таким свойством обозначим через $к_A$.

Утверждение 1. Для автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ справедливы следующие верхние оценки параметра $к_A$:

1) $к_A \le |\{(gS_1, gS_2, \ldots, gS_L): g\in G\}| \le |G|$;

2) $к_A \le \max\limits_{1\le j(1)<j(c)\le L} |(\{gS_{j(1)}, gS_{j(c)}\},\{gS_j: j\in\{1, 2, \ldots, j(1)–1, j(1)+1, \ldots, j(c)–1, j(c)+1, \ldots, L\})|$,

где $G = \langle(h_x)_{x\in X}\rangle\cup E$, E – тождественное преобразование S.

Доказательство. Для доказательства оценки 1) очевидно достаточно доказать , что $\sigma(к(1))^* = \sigma^*$ при $к(1) = |\{(gS_1, gS_2, \ldots, gS_L): g\in G\}|$. Докажем, что $\sigma(к(1))^* = \sigma^*$. Отношения $\sigma(к(1))^*$, σ^* являются бинарными отношениями эквивалентности на

$R_S = \{S_1, S_2, \ldots, S_L\}$, причем очевидно, что $\sigma(к+1)^*\subseteq \sigma(к)^*$, именно любой класс отношения эквивалентности $\sigma(к+1)^*$ содержится в некотором классе отношения эквивалентности $\sigma(к)^*$, в связи с чем $\sigma^*\subseteq\sigma(к(1))^*$. Покажем обратное включение. Предположим, что для $j(1), j(c)\in\{1, \ldots, L\}$ $S_{j(1)}\sigma_P^*$ знак = ? $S_{j(c)}$??? для всех $P\in \bigcup_{i=1}^{к(1)} X^i$.

Пусть x(1), x(2), …, x(N–1), x(N) = Qx(N) – произвольное слово из X*. Нам достаточно показать, что

$$S_{j(1)}\sigma_{Qx(N)}{}^{*}$$ знак? $S_{j(c)}$.???

Если $Qx(N)\in \bigcup_{i=1}^{\kappa(1)} X^i$, то это отношение верно по предположению. Пусть $Qx(N)\in X^N$, $N\geq\kappa(1)+1$. Нам необходимо найти семейство $S_{j(2)}$, $S_{j(3)}$, …, $S_{j(c-1)}$, при которых

$$f_{Qx(N)}S_{j(v)}\cap f_{Qx(N)}S_{j(v+1)}\neq\varnothing,\ v\in\{1,\ldots,c-1\},$$

или

$$f_{x(N)}h_QS_{j(v)}\cap f_{x(N)}h_QS_{j(v+1)}\neq\varnothing,\ v\in\{1,\ldots,c-1\}.$$

Так как каждый набор множеств из множества нобоpов $\{(gS_1, gS_2, \ldots, gS_L): g\in G\}$ имеет вид $(h_PS_1, h_PS_2, \ldots, h_PS_L)$ для некоторого слова P длины, не превосходящей $\kappa(1)-1$, то для набора $(h_QS_1, h_QS_2, \ldots, h_QS_L)$ найдется найдется слово $T\in \bigcup_{i=1}^{\kappa(1)-1} X^i$, при котором $(h_QS_1, h_QS_2, \ldots, h_QS_L) = (h_TS_1, h_TS_2, \ldots, h_TS_L)$. Поэтому требуемые для доказательства утверждения 1 пересечения $f_{x(N)}h_QS_{j(v)} \cap f_{x(N)}h_QS_{j(v+1)} \neq \varnothing$, $v\in\{1, \ldots, c-1\}$ равносильны пересечениям

$$f_{x(N)}h_TS_{j(v)} \cap f_{x(N)}h_TS_{j(v+1)} \neq \varnothing,\ v\in\{1,\ldots,c-1\},$$

а они выполняются для слова $Tx(N)\in \bigcup_{i=1}^{\kappa(1)} X^i$, при некоторых $j(v)\in\{2, \ldots, c-1\}$, так как $S_{j(1)}\sigma_{Tx(N)}{}^{*}$ - пробел? знак? $S_{j(c)}$??? по предположению. Очевидно, $\kappa(1)\leq|G|$, G – полугруппа автомата A с добавленной единицей. Нами доказана оценка 1) утверждения 1. Оценка 2)[1] утверждения легко следует из анализа проведенного доказательства оценки 1).

Основной смысл приведенного утверждения 1 состоит в том, что бинарное отношение σ* задается конструктивно, в связи с чем конструктивны и условия приводимой ниже теоремы 2.

Предварительно введем определение.

Определение 6. Разбиение $R_S = \{S_1, S_2, \ldots, S_L\}$ множества состояний S автомата A σ*-различимо, если любая пара различных блоков S_j, $S_{j`}$ σ*-различима.

Теорема 2. Тогда и только тогда для перестановочного автомата A с множеством состояний S найдется инициальный автомат $B_{q(0)}\in B(X, Y)$, при котором классы неотличимых состояний на под-

[1] Указана Ф. М. Малышевым.

множестве $S\times\{q(0)\}$ множества состояний обработки $C = A \to B_{q(0)}$ имеют вид: $S_j\times\{q(0)\}$, $j\in\{1, 2, \ldots, L\}$, $L \geq 2$, когда множество $\{S_1, S_2, \ldots, S_L\}$ является разбиением S и разбиение $R_S = \{S_1, S_2, \ldots, S_L\}$ σ^*-различимо.

Доказательство. Пусть для автомата A нашелся автомат $B_{q(0)}$, для которого классы неотличимых состояний на подмножестве $S\times\{q(0)\}$ множества состояний обработки $C = A\to B_{q(0)}$ имеют вид: $S_j\times\{q(0)\}$, $j\in\{1, 2, \ldots, L\}$, $L \geq 2$. Заметим, что в этом случае $\{S_1, S_2, \ldots, S_L\}$ – разбиение S. Предположим, что нашлись $j(0)$, $j`(0)\in\{1, 2, \ldots, L\}$, при которых пара блоков $S_{j(0)}$, $S_{j`(0)}$ σ^*-неотличима. Состояния автомата C из одного класса неотличимых состояний дают в автомате C одинаковый выход. Поэтому для $P\in X^*$ корректна запись

$$C(S_{j(0)}, q(0), P) = q(0), q(1, P), q(2, P), \ldots,$$

где $q(j, P)\in S^B$. Аналогично,

$$C(S_{j`(0)}, q(0),P) = q(0), q`(1, P), q`(2, P), \ldots$$

Покажем, что при наших предположениях эти последовательности совпадают.

Пусть $P = x(1), x(2), \ldots$. Если имеем $S_{j(0)}\sigma_{x(1)}$* знак? $S_{j`(0)}$, то найдутся $S_{j(1)}, S_{j(2)}, \ldots, S_{j(N)}$ из $R_S$, при которых $f_{x(1)}S_{j(0)}\cap f_{x(1)}S_{j(1)} \neq \varnothing$, $f_{x(1)}S_{j(1)}\cap f_{x(1)}S_{j(2)} \neq \varnothing, \ldots, f_{x(N)}S_{j(0)}\cap f_{x(1)}S_{j`(0)} \neq \varnothing$.

В связи с этим

$$^{B}h_{x(1),f_{f(1)}S_{j(0)}}q(0) = q(1,P),$$

$$^{B}h_{x(1),f_{f(1)}S_{j(1)}}q(0) = q(1,P),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$^{B}h_{x(1),f_{f(1)}S_{j(N)}}q(0) = q(1,P),$$

$$h_{x(1),f_{f(1)}S_{j`(0)}}q(0) = q(1,P).$$

Здесь уравнение $^{B}h_{x(1),f_{f(1)}S_{j(\kappa)}}q(0) = q(1,P)$ означает $^{B}h_{x(1),y}q(0) = q(1, P)$ для всех $y\in f_{x(1)}S_{j(\kappa)}$. Поэтому $q(1, P) = q`(1, P)$. Аналогично, из $S_{j(0)}\sigma_{x(1),x(2)}$* $S_{j`(0)}$ получаем $q(2, P) = q`(2, P)$ и так далее. Таким образом, в силу произвольного выбора $P\in X^*$, заключаем, что состояния, выбранные произвольно из классов $S_{j(0)}\times\{q(0)\}$, $S_{j(0)}\times\{q(0)\}$, неотличимы в C. Полученное противоречие доказывает необходимость условий теоремы.

Пусть $R_S = \{S_1, S_2, \ldots, S_L\}$ – σ^*-различимое разбиение множества состояний S автомата A. Построим автомат $B_{q(0)}\in B(X, Y)$, для которого множество $\{S_j\times\{q(0)\}$: $j\in\{1, 2, \ldots, L\})$ есть множество

классов неотличимых состояний на $S\times\{q(0)\}$ в автомате C. Автомат $B_{q(0)} = (X\times Y, S^B, ({}^Bh_{x,\,y})_{(x,\,y)\in X\times Y})$ будем строить индуктивно. Для первого шага построения множества S^B положим $q(0) = \{S_1, S_2, \ldots, S_L\}$ – состояние автомата $B_{q(0)}$, $q(0)\in S^B$. Предположим, что на к-м шаге определено не пустое подмножество $S^к$ множества S^B, элементы которого имеют вид $q = \{{}^qS_1, {}^qS_2, \ldots, {}^qS_{L(q)}\}$, где ${}^qS_j$ – некоторые не пустые подмножества множества S. Для $x\in X$, по аналогии с отношением σ_P на $\{S_1, S_2, \ldots, S_L\}$, определим бинарное отношение ε_x на множестве $\{{}^qS_1, {}^qS_2, \ldots, {}^qS_{L(q)}\}$, положив ${}^qS_j\varepsilon_x{}^qS_{j`}$ тогда и только тогда, когда $f_x{}^qS_j\cap f_x{}^qS_{j`} \neq \varnothing$.

Пусть ε_x* – транзитивное замыкание отношения ε_x и $\{\eta(1), \eta(2), \ldots, \eta(c)\}$ – множество всех классов эквивалентности бинарного отношения ε_x*. Отметим, что бинарное отношение ε_x* на $\{S_1, S_2, \ldots, S_L\}$ совпадает с σ_x* на этом же множестве. Для $j\in\{1, \ldots, c\}$ положим

$$\overline{\eta_j} = \bigcup_{{}^qS_к\in\eta_j} {}^qS_к \qquad \text{и} \qquad {}^Bh_{x,f_x\overline{\eta_x}}\{{}^qS_1, {}^qS_2, \ldots {}^qS_{L(q)} = h_x\eta_j,$$

Здесь для $\eta_j = \{{}^qS_к: {}^qS_к\in\eta_j\}$ введено обозначение $h_x\eta_j = \{h_x{}^qS_к: {}^qS_к\in\eta_j\}$ и для

$$f_x\overline{\eta_x} = V\subseteq Y$$

$${}^Bh_{x,V}q = h_{x,y}q = h_x\eta_j$$

для всех $y\in V$.

Полученные теперь состояния $\{h_x\eta_j\}\cup S^к = S^{к+1}$ объявляем состояниями автомата $B_{q(0)}$. Заметим, что на определенных ранее состояниях $S^к\subseteq S^B$ мы определили (возможно полностью, а возможно и частично) частичные функции переходов автомата $B_{q(0)}$. Итеративное определение множества S^B заканчиваем, если все полученные состояния $h_x\eta_j$ $x\in X$, $j\in\{1, 2, \ldots, L\}$, $q\in S^к$ принадлежат $S^к$. В этом случае множество $S^к\cup\{t\}$ ($t = \varnothing$ – пустое множество) объявляем множеством состояний S^B автомата $B_{q(0)}$. Для тех $q \in S^B$ и $(x, y)\in X\times Y$ (если они существуют), для которых значение ${}^Bh_{x,y}q$ еще не определено, полагаем дополнительно

$${}^Bh_{x,y}q = t.$$

Легко проверяется, что состояния вида (s, q), $(s`, q)$, где $s, s`\in S_j$, $j\in\{1, \ldots, L\}$ автомата C неотличимы в C. В связи с чем для $P\in X^*$ корректна запись

$$C(S_j, q(0), P) = q(0), q(1, P, j), q(2, P, j), \ldots, q(к, P, j), \ldots$$

Произвольно фиксируем $j(0)$, $j`(0) \in \{1, \ldots, L\}$, $j(0) \neq j`(0)$ и предположим, что при любом $P = x(1), \ldots, x(к), P \in X^*$

$$C(S_{j(0)}, q(0), P) = C(S_{j`(0)}, q(0), P) = q(0), q(1, P), q(2, P), \ldots$$

Тогда $q(1, P) = h_{x(1)}\eta_1$, где η_1 – некоторый класс отношения эквивалентности ε_x^* на $\{S_1, S_2, \ldots, S_L\}$, причем для разных классов η_1, $\eta`_1$ этого бинарного отношения эквивалентности

$$h_{x(1)}\eta_1 \cap h_{x(1)}\eta`_1 = \varnothing,$$

так как автомат А по условию теоремы – перестановочный.

Здесь пересечение берется как пересечение множеств, состоящих из образов $S_j \in \{S_c: c \in \{1, \ldots, L\}\}$ согласно определению класса η. Поэтому состоянием $q(1, P)$ класс η определен однозначно, откуда следует, что $S_{j(0)}\varepsilon_{x(1)}^*S_{j`(0)}$. Пусть $\eta_1$ имеет вид: $\{S_{j(0)}, S_{j`(0)}, S_{j(1)}, \ldots, S_{j(L`)}\}$.

Тогда

$$q(1, P) = \{h_{x(1)}S_{j(0)}, h_{x(1)}S_{j`(0)}, h_{x(1)}S_{j(1)}, \ldots, h_{x(1)}S_{j(L`)}\} \text{ и } q(2, P) = \\ = h_{x(2)}\eta_2,$$

где η_2 – некоторый класс эквивалентности отношения $\varepsilon_{x(2)}^*$ на элементах $\{h_{x(1)}S_{j(0)}, h_{x(1)}S_{j`(0)}, h_{x(1)}S_{j(1)}, \ldots, h_{x(1)}S_{j(L`)}\}$ и η_2 определен однозначно состоянием $q(2, P)$ в силу перестановочности автомата А. Откуда получаем

$$h_{x(1)}S_{j(0)}\varepsilon_{x(1)}^* h_{x(1)}S_{j`(0)} \text{ или } S_{j(0)}\varepsilon_{x(1)x(2)}^*S_{j`(0)}.$$

Практически мы доказали справедливость индуктивных шагов для доказательства утверждения: $S_{j(0)}\sigma_P^*S_{j`(0)}$. Так как P выбиралось произвольно из $X^*$, то тем самым доказано, что $S_{j(0)}\sigma^*S_{j`(0)}$. Последнее противоречит σ^*-различимости разбиения $R_S = \{S_1, S_2, \ldots, S_L\}$. Следовательно, доказана достаточность условий теоремы.

Отметим, что из доказательства данной теоремы вытекает справедливость ее необходимых условий для произвольного автомата А.

Проведенное нами доказательство указывает конструктивный способ обработки автомата А с помощью вспомогательного автомата $B_{q(0)}$ с целью предварительного группирования состояний автомата А для решения задачи определения его начального состояния по входным и соответствующим им выходным последовательностям.

Глава 9. ФУНКЦИИ – МОДЕЛИ АВТОМАТОВ, ПОСТРОЕННЫЕ НА ОСНОВЕ СЛЕДСТВИЙ УРАВНЕНИЙ ИХ ФУНКЦИОНИРОВАНИЯ

Предлагаются способы построения функций – моделей конечного автомата – новые автоматы с одним состоянием, получаемые с помощью степеней исходного автомата и задания дополнительных функций на его выходных словах. Приложения результатов связываются с задачей определения информации о входном слове автомата по его выходному слову.

В этой главе изучаются возможности построения для исследуемого автомата A его моделей – следствий, трактующиеся как новые автоматы с одним состоянием, уравнения функционирования которых являются следствиями уравнений функционирования исходного автомата. Эти функции – модели будут называться далее образами автомата A при его обработках. Целью построения таких образов для A является разработка методов определения информации о входном слове автомата по его выходному слову. Основные результаты работы ранее опубликованы в тезисах [12].

9.1. Построение моделей-следствий автомата

Пусть $A = (X, S, Y, h, f)$ – конечный автомат. *Под обработкой степени к* автомата A будем понимать произвольное отображение $\Phi: Y^к \to Y`$, где $Y`$ – некоторый алфавит. *Образом автомата A при обработке Ф* назовем автомат $A_\Phi = (X^к, S, Y`, h_ф, f_ф)$ с функцией перехода

$$h_ф(s, x(1), x(2), \ldots, x(к)) = h(s, x(1), x(2), \ldots, x(к)) = \\ = h_{x(к)}h_{x(к-1)}\ldots h_{x(1)}s$$

и выхода

$$f_ф(s, x(1), x(2), \ldots, x(к)) = \Phi(A(s, x(1), x(2), \ldots, x(к)),$$

где $s \in S$, $(x(1), x(2), \ldots, x(к))$ – входной символ автомата A_Φ, $(x(1), x(2), \ldots, x(к)) \in X^к$.

Указанный автомат A_Φ обладает следующим свойством. Если при входной последовательности

$$x(1), x(2), \ldots, x(Rк) = P(1), P(2), \ldots, P(R), \ P(j) = x((j-1)к+1), \ldots, x(jк), \\ j \in \{1, \ldots, R\}$$

и начальном состоянии $s \in S$ выходная последовательность автомата A есть $A(s, x(1), x(2), \ldots, x(Rк)) = y_1, y_2, \ldots, y_{Rк} = Q_1, Q_2, \ldots, Q_R$,

$Q_j = y_{(j-1)к+1}, \ldots, y_{jк}$, $j \in \{1, \ldots, R\}$, то выходная последовательность автомата $A_Ф$, соответствующая входной последовательности P(1), P(2), …, P(R) и начальному состоянию $s \in S$, определяется равенством

$$A_Ф(s, P(1), P(2), \ldots, P(R)) = Ф(Q_1), Ф(Q_2), \ldots, Ф(Q_R).$$

Таким образом, функционирование автомата $A_Ф$ представимо схемой, показанной на рис. 4.

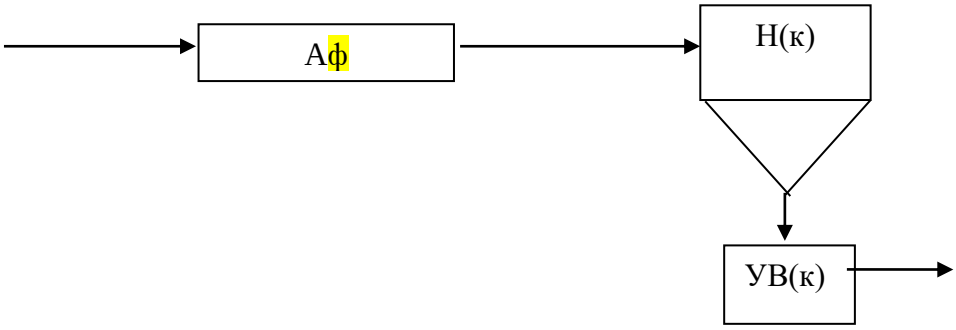

Рис. 4

Здесь Н(к) – проходной накопитель на к знаков y, УВ(к) – узел выборки шага к. Далее нас будет интересовать случай неконстантной обработки Ф – функции, неконстантной на множестве $\{A(s, P): s \in S, P \in X^к\}$.

Определение 1. Автомат A называется слабо тривиальным автоматом, если для него существует неконстантная обработка Ф, при которой его образ $A_Ф$ является неприведенным автоматом с одним классом неотличимых состояний. В противном случае автомат A называется сильно нетривиальным автоматом.

Если $A_Ф$ является неприведенным автоматом с одним классом неотличимых состояний, то его выходная последовательность

$$A_Ф(s, P(1), P(2), \ldots, P(R)) = Ф(Q_1), Ф(Q_2), \ldots, Ф(Q_R)$$

не зависит от выбора $s \in S$. И для приведенной формы ${}^{П}A_Ф$ автомата $A_Ф$ будем иметь

$${}^{П}A_Ф({}^{П}s, P(1), P(2), \ldots, P(R)) = Ф(Q_1), Ф(Q_2), \ldots, Ф(Q_R) =$$
$$= {}^{П}A_Ф({}^{П}s, P(1)), {}^{П}A_Ф({}^{П}s, P(2), \ldots, {}^{П}A_Ф({}^{П}s, P(R)),$$

где ${}^{П}s$ – единственное состояние автомата ${}^{П}A_Ф$. В частности, ${}^{П}A_Ф({}^{П}s, P(1)) = Ф(A(s, P(1))$, при любом $s \in S$ и $P(1) \in X^к$. Таким образом, для слабо тривиального автомата $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$

выполняется условие (далее – условие УС): существует новый алфавит Y`, число $к \in [1, 2, \ldots)$, отображения $F_1$: $X^к \to Y`$ и F_2: $Y^к \to Y`$, $F_1 \neq const$, для которых при любых $s \in S$, $P \in X^к$ выполнено равенство

$$F1(P) = F2(A(s, P)).$$

Обратно, если для автомата A выполнено приведенное условие, то автомат $A_Ф$ при $Ф = F_2$ будет иметь один класс неотличимых состояний и автомат A будет слабо тривиальным автоматом.

Основная задача состоит в описании сильно нетривиальных автоматов, а именно автоматов, не обладающих условием УС.

Установим сначала связь условия УС с другим известным понятием. Через $A^r = (X^r, S, Y^r, (h^r{}_P)_{P \in X^r}, (f^r{}_P)_{P \in X^r})$ обозначим r-тую степень автомата A. Здесь для $P \in X^r$, $P = x(1), x(2), \ldots, x(r)$; $h^r{}_P = h_{x(r)}h_{x(r-1)}\ldots h_{x(1)}$; $f^r{}_P s = f_{x(1)}s, f_{x(2)}\delta_{x(1)}s, \ldots, f_{x(r)}h_{x(r-1)}\ldots h_{x(1)}s$. Рассматривая функцию F_1 как автоматное отображение $F_1 = (X^r, Y`, F_1)$, можно сказать, что выполнение условия YC при указанных параметрах равносильно наличию гомоморфизма автомата $A^r$ в $F_1$ вида $(E, F_2)$, $E$: $X^r \to X^r$, $F_2$: $Y^r \to Y`$, где E – тождественное отображение. Обратно, если A^r гомоморфен при гомоморфизме (ψ, φ, η) некоторому автомату $B = (X^B, Y^B, f^B)$ с одним состоянием, реализующему неконстантный оператор, то для автомата A выполнено условие YC при $Y` = Y^B$, $F_2 = \eta$, $F_1 = f^B\psi$.

Напомним[1], что для краткости изложения используются символы:

$\Rightarrow$ – тогда;

$\Leftrightarrow$ – тогда и только тогда;

$\exists$ – если существует (существуют);

$\forall$ – для любого (любых);

: – для которого (которых) выполняется;

X^∞ – множество всех входных слов автомата бесконечной длины;

$$\bigcup_{r=1}^{\infty} X^r = X^*,$$

.

Все слова алфавита X записываются слева направо $P = x_1, x_2, \ldots, x_j \in X$. Мы будем употреблять и конкатенацию слов. Если $P \in X^r$, $P` \in X^m$, то употребляем запись $PP` \in X^{r+m}$, P – начальное под-

[1] Предлагаю этот перечень символов добавить также и во Введение, так как по книге они использовались и ранее. – ред.

слово слова PP`. Если r = 0, то любое слово из $P^r$ считаем пустым словом, то есть PP` = P`.

Для подслов слова $P = x_1, x_2, \ldots$ используем обозначения:

$P = P^1$; $P^r = x_r, x_{r+1}, \ldots$; $P]_r = x_1, x_2, \ldots, x_r$; $P^r]_m = x_r \ldots x_m$, $r \le m$.

Положим еще $(P)^к = PP\ldots P$, k раз.

Определим теперь ряд бинарных отношений на множествах X^∞, X^*, X^L, $L \in [1, 2, \ldots)$.

Отношение

$$^L\bar{\sigma}$$

на X^L:

$$P\,^L\bar{\sigma}P' \Leftrightarrow \exists s, s' \in S : A(s, P) = A(s', P').$$

Отношение

$$\bar{\sigma}$$

на X^*:

$$P\bar{\sigma}P' \Leftrightarrow \exists L : P, P' \in X^L \quad и \quad P\,^L\bar{\sigma}P'.$$

Отношение

$$\sigma$$

на X^∞:

$$P\sigma P` \Leftrightarrow \exists s, s' \in S : A(s, P) = A(s', P')$$

Отношение

$$^L\sigma$$

на X^L:

$$P_1\,^L\sigma P_2 \Leftrightarrow \exists P, P' \in X^\infty : P\sigma P', \;\; P]_L = P_1, P']_L = P_2$$

Введенные бинарные отношения обладают свойством рефлексивности и симметричности.

Определим еще отношение:

$$\tilde{\sigma}^m, \; для \; \tilde{\sigma} \in \left\{\sigma, \; ^L\sigma, \; \bar{\sigma}, \; ^L\bar{\sigma}\right\}$$

$$P\tilde{\sigma}^m P' \Leftrightarrow \exists P_1, P_2, \ldots, P_{m-1} : P\tilde{\sigma}P_1\tilde{\sigma}P_2 \ldots \tilde{\sigma}P_{m-1}\tilde{\sigma}P'.$$

Причем для m = 1 полагаем

$$\tilde{\sigma}^1 = \tilde{\sigma}.$$

Отметим, что среди $(P_j)_{j \in \{1, \ldots, m-1\}}$ возможны и одинаковые слова. В связи с чем ясно, что

$$\tilde{\sigma}^m \subseteq \tilde{\sigma}^{m+1},$$

то есть при любом m

$$P\tilde{\sigma}^m P' \Rightarrow P\tilde{\sigma}^{m+1} P'.$$

Следующее отношение есть транзитивное замыкание бинарного отношения:

$$\vartheta^{*}, \vartheta^{*} \in \left\{ \sigma^{*}, {}^{L}\sigma^{*}, \bar{\sigma}^{*}, {}^{L}\bar{\sigma}^{*} \right\};$$

$$\vartheta \in \left\{ \sigma, {}^{L}\sigma, \bar{\sigma}, {}^{L}\bar{\sigma} \right\}.$$

Отметим, что

$$\vartheta^{*}$$

есть отношение эквивалентности на соответствующем множестве. Через

$$rang\,\vartheta^{*}$$

обозначим число классов эквивалентности отношения

$$\vartheta^{*},$$

а через t(σ), (t($\bar{\sigma}$)) – минимальное К, если оно существует, при котором

$$rang\ {}^{K}\sigma^{*} > 1, \quad (rang\ {}^{K}\bar{\sigma}^{*} > 1),,$$

в противном случае полагаем t(σ) = ∞ (t($\bar{\sigma}$) = ∞).

Введенные параметры t(σ), (t($\bar{\sigma}$)) назовем *степенью транзитивности* отношений соответственно σ, $\bar{\sigma}$.

Нам потребуется следующее вспомогательное утверждение, которое несложно доказывается с использованием стандартной техники бинарных отношений.

Утверждение 1. Для автомата А выполнено условие УС тогда и только тогда, если степень транзитивности t($\bar{\sigma}$) бинарного отношения $\bar{\sigma}$ является конечным числом.

Итак, поставленная задача свелась к указанию автоматов А со степенью транзитивности t(σ) = ∞.

Определение 2. Автомат A = (X, S, Y, h, f) назовем автоматом с потерей информации первого типа (СПИ1), если для

$$L \geq \frac{|S|(|S|-1)}{2} + 1$$

при любой паре (x, x`)[1]∈X существуют s = s(x, x`)∈S и (P, P`)∈X^L , для которых

$$A(s, xP) = A(s, x`P`).$$

Определение 3. Автомат А назовем автоматом с потерей информации второго типа (СПИ2), если для

[1] если оба значения пары принадлежат X, то они могут быть взяты в скобки перед знаком ∈ - «принадлежат X», с целью показать их принадлежность - ред.

$$L \geq \frac{|S|(|S|-1)}{2}+1$$

при любой паре (x, x`)∈X найдутся (s, s`)∈S и (P, P`)∈ X^L, для которых

$$A(s`, P`x`) = A(s, Px) \quad \text{и} \quad h_{Px}s = h_{P`x`}s`.$$

Названия указанным выше свойствам автомата A мы дали исходя из аналогии с соответствующими известными понятиями книги [33].

Теорема 1. Если автомат A – СПИ2 или A – перестановочный и СПИ1, то t(σ) = ∞.

Доказательство. Предположим сначала, что A – СПИ1. Легко доказывается следующая лемма.

Лемма 1. Если автомат A – перестановочный и СПИ1, то для любой пары (x, x`)∈X, любого L∈[1, 2, …) и любого P∈$X^L$ существуют $P^\infty$, $P`^\infty \in X^\infty$, для которых $PxP^\infty \sigma Px`P`^\infty$.

Из леммы вытекает, что

$$\forall\, L, P \in X^L, \forall\, x, x`: Px\ {}^{L+1}\sigma Px`,$$

в частности, rang ${}^L\sigma^* = 1$.

Предположим, что при некотором L: rang ${}^L\sigma^* = 1$, и покажем, что rang ${}^{L+1}\sigma^* = 1$. Из данного предположения следует существование цепочки отношений вида

$$P_1\ {}^L\sigma\ P_2\ {}^L\sigma \ldots {}^L\sigma P_N,\ N \geq |X|^L,$$

содержащей все слова из X^L. По определению ${}^L\sigma$

$$\exists\, \varepsilon_j, \varepsilon_j` \in X: P_j\, \varepsilon_j\ {}^{L+1}\sigma\ P_{j+1}\, \varepsilon_j`,\ \ j \in \{1, \ldots, N-1\}.$$

С другой стороны, как было замечено ранее,

$$\forall\, x \in X: P_j\, \varepsilon_j\ {}^{L+1}\sigma\ P_j\, x\,.$$

Суммируя сказанное, заключаем, что rang ${}^{L+1}\sigma^* = 1$. Таким образом, t(σ) = ∞. Для завершения доказательства первой части теоремы остается воспользоваться включением ${}^L\sigma \subseteq {}^L\bar{\sigma}$, L∈{1, 2, …}, из которого следует

$$t(\bar{\sigma}) \geq t(\sigma).$$

Пусть теперь A является автоматом СПИ2. Обозначим через

$${}^L\bar{\bar{\sigma}}$$

новое бинарное отношение на X^L, положив

$$P'\ {}^L\bar{\bar{\sigma}}P'' \Leftrightarrow \exists N_1 = N_1(P', P'') \geq 1,\ N_2 = N_2(P', P'') \geq 0,$$

$$P_1', P_1'' \in X^{N_1};\ P_2', P_2'' \in X^{N_2}:\ \forall k \geq 1\ \ (P_1`)^k P_2` P`\ {}^{kN_1+N_2+L}\bar{\sigma}\ (P_1``)^k P_2`` P``.$$

Легко доказывается следующая лемма.

Лемма 2. Если A является автоматом СПИ2, то

$$\forall x, x` \in X,\ P \in X^L,\ L \in \{1,2,...\}:\ xP \overset{L+1}{=} \sigma x`P.$$

Лемма 3. Справедливо следующее утверждение:

$$P` \overset{L}{=} \sigma P`` \Rightarrow \exists \varepsilon_1, \varepsilon_2 \in X:\ \varepsilon_1 P` \overset{L+1}{=} \sigma\ \varepsilon_2 P``.$$

Доказательство. По определению рассматриваемого отношения имеем

$$P` \overset{L}{=} \sigma P``$$

$$\exists\ N_1, N_2;\ P_1`, P_1`` \in X^{N_1}, P_2`, P_2`` \in X^{N_2}:$$

$$\forall k \geq 1\ (P_1`)^k P_2` P` \overset{kN_1+N_2+L}{=} \sigma (P_1``)^k P_2`` P``.$$

Если $N_2>1$, $P_2` = x_1`, x_2`, \ldots, x_{N_2}`$, $P_2`` = x_1``, x_2``, \ldots, x_{N_2}``$, то очевидно

$$(P_1`)^k P_2`]_{N_2-1} x_{N_2}`\ P` \overset{kN_1+N_2+L}{=} \sigma (P_1``)^k P_2``]_{N_2-1} x_{N_2}``\ P``.$$

Следовательно,

$$x_{N_2}` P` \overset{L+1}{=} \sigma x_{N_2}`` P``,$$

и лемма доказана. Если же $N_2 = 0$, $P_1` = x_1`, x_2`, \ldots, x_{N_1}`$, $P_1`` = x_1``, x_2``, \ldots, x_{N_1}``$, то

$$(x_{N_1}, x_1`, ..., x_{N_1-1}`)^{k-1} x_{N_1}`\ P` \overset{(k-1)N_1+L+1}{=} \sigma (x_{N_1}``, x_1``, ..., x_{N_1-1}``)^{k-1} x_{N_1}``\ P``$$

Следовательно,

$$x_{N_1}`\ P` \overset{L+1}{=} \sigma x_{N_2}``\ P``.$$

Лемма 3 полностью доказана.

Пусть $\overset{L}{=} \sigma^*$ – транзитивное замыкание бинарного отношения $\overset{L}{=} \sigma$. Из леммы 2 имеем

$$\forall L, \forall P \in X^L, \forall x`, x`` \in X\ :\ x`P \overset{L+1}{=} \sigma x`` P,$$

в частности $\text{rang} \overset{1}{=} \sigma^* = 1$.

Продолжим доказательство теоремы. Предположим, что при некотором $L \geq 1$

$$\text{rang} \overset{L}{=} \sigma^* = 1,$$

и покажем, что $\text{rang} \overset{L+1}{=} \sigma^* = 1$. По предположению существует цепочка отношений

$$P_1 \overset{L}{=} \sigma P_2 \overset{L}{=} \sigma \ldots \overset{L}{=} \sigma P_C,$$

которая содержит все элементы из X^L. По лемме 3

$$P_j \overset{L}{=} \sigma P_{j+1} \Rightarrow \exists \varepsilon_j, \varepsilon_j` \in X:\ \varepsilon_j P_j \overset{L+1}{=} \sigma \varepsilon_j` P_{j+1}.$$

Ранее из леммы 2 мы заключили

$$\forall x, x` \in X,\ P \in X^L:\ xP \overset{L+1}{=} \sigma x`P.$$

Учитывая выписанные отношения, получаем

$$rang\ {}^{L+1}\bar{\bar{\sigma}}^* = 1.$$

Итак, при любом L выполняется равенство

$$rang\, {}^{L}\bar{\bar{\sigma}}^* = 1.$$

Легко теперь показывается, что

$${}^{L}\bar{\bar{\sigma}}^* \subseteq {}^{L}\bar{\sigma}^*\ ;$$

$$rang\ {}^{L}\bar{\sigma}^* = 1.$$

при любом L.

Следовательно,

$$t(\bar{\sigma}) = \infty,$$

что и требовалось доказать.

Итак, указаны классы автоматов: автоматы СПИ2 и перестановочные автоматы СПИ1, не обладающие свойством УС. Представляет интерес нахождение и других таких классов автоматов, то есть новых автоматов с параметром $t(\bar{\sigma}) = \infty$.

Ниже в данном пункте работы мы будем рассматривать в основном так называемые обратимые (биективные) автоматы. Напомним, что автомат A = (X, S, Y, h, f) называется *обратимым,* если его функция выходов f: S×X→Y при любом s∈S осуществляет биекцию f_s X в Y, |X|>1, в частности, |X| = |Y|.

Для заданного обратимого автомата A рассмотрим два вспомогательных автомата.

1. Обратный автомат

$$A^{-1} = (\bar{X}, S, \bar{Y}, (\bar{h}_y)_{y \in \bar{X}}, (\bar{f}_y)_{y \in \bar{X}}),$$

где $\bar{X} = Y, \bar{Y} = X,\ \bar{h}_y s = h_{f_s^{-1} y} s,\ \bar{f}_y s = f_s^{-1} y,\ s \in S, y \in Y.$

2. Последовательное соединение B = A → A^{-1} автоматов A, A^{-1}.

$$B = (X, S_B, Y_B, (h^B{}_x)_{x \in X}, (f^B{}_x)_{x \in X}),\ S_B = S \times S,\ Y_B = X,\ h^B{}_x(s_1, s_2) =$$

$$= (h_x s_1, \bar{h}_{f_x s_1} s_2),$$

$$f^B{}_x(s_1, s_2) = \bar{f}_{f_x s_1} s_2,\ (s_1, s_2) \in S_B.$$

Очевидно, автомат A^{-1} является обратимым автоматом и последовательное соединение обратимых автоматов также является обратимым автоматом.

Для автомата B = A→A^{-1} определим бинарные отношения ${}^{L}\bar{\alpha}$ на X^L, L∈{1, 2, …} и α на X^∞, положив, что

$$P \; {}^{L}\bar{\alpha} \; P` \Leftrightarrow \exists\, s = (s_1, s_2) \in S_B: B(s, P) = P`,$$

и аналогично для α на X^{∞}

$$P\alpha P` \Leftrightarrow \exists\, s \in SB: B(s, P) = P`.$$

Легко проверяется рефлексивность и симметричность введенных отношений, в связи с чем полностью аналогично введенным ранее бинарным отношениям $L\sigma$, σ^*, ${}^{L}\bar{\sigma}^*$, σ^* и т. д. и параметрам $rang\sigma$, $t(\sigma)$ вводим отношения ${}^{L}\alpha$, ${}^{L}\alpha^*$, ${}^{L}\bar{\alpha}^*$, $\bar{\alpha}^m$, α^m и параметр – *степень транзитивности $t(\alpha)$ отношения α.*

Легко доказывается следующее утверждение.

Лемма 4. Для обратимого автомата A справедливы следующие утверждения:

1. ${}^{L}\bar{\alpha} = {}^{L}\alpha$,
2. $P\sigma P` \Leftrightarrow P\alpha P`$,
3. $P \; {}^{L}\bar{\sigma} \; P` \Leftrightarrow P \; {}^{L}\sigma \; P`$, $L \in \{1, 2, \ldots\}$,
4. $t(\alpha) = t(\bar{\sigma})$.

Нам потребуется еще одно понятие. Бинарное отношение

$$\partial\!\!\!/ \in \{\alpha, \alpha^m, \alpha^*, \bar{\alpha}^m, \bar{\alpha}^*\}$$

на X^* назовем *отношением без памяти* и этот факт будем записывать в виде:

$$\Pi(\partial\!\!\!/) = \infty, \; \textit{если} \; \forall N \; \exists L \geq N, \; P \in X^L, P` \in X^{L-1} : \forall x \in X \quad P \; {}^{L}\partial\!\!\!/ P`x.$$

Лемма 5. Для обратимого автомата A = (X, S, Y, h, f) справедливо

$$\Pi(\bar{\alpha}^m) = \infty \Leftrightarrow \exists\, L, L < 2(|S|^{2m|X|} + 1), L > (|S|^{2m|X|} + 1), \exists\, P \in X^L,$$
$$P` \in X^{L-1}: \forall\, x \in X, P \; {}^{L}\bar{\alpha}^m \; P`x.$$

Доказательство леммы 5 не вызывает затруднений. Это доказательство может быть проведено стандартными приемами теории автоматов.

Мы не видим необходимости понижать указанную в лемме 5 оценку $|S|^{2m|X|} + 1$ или искать достижимую оценку, хотя это возможно. Смысл указанной леммы для нас состоит в том, что свойство $\Pi(\bar{\alpha}^m) = \infty$ обратимого автомата A алгоритмически проверяемо.

Теорема 2. Для обратимого автомата A

$$\Pi(\alpha^*) = \infty \Leftrightarrow t(\bar{\sigma}) = \infty.$$

Доказательство данной теоремы является несложным. Оно основано на лемме 4.

Следствие 1. Если для обратимого автомата A $\Pi(\bar{\alpha}^m) = \infty$ при некотором m, то $t(\bar{\sigma}) = \infty$.

Доказательство. Очевидно, что

$$\Pi(\bar{\alpha}^m) = \infty \Rightarrow \Pi(\bar{\alpha}^*) = \infty, \Pi(\bar{\alpha}^*) = \Pi(\alpha^*)$$

и остается воспользоваться теоремой 2.

Таким образом, для построения обратимых автоматов А, не обладающих свойством УС, можно использовать теорему 1, то есть строить автомат СПИ2, либо следствие 1.

Представляет интерес построение перестановочных, автономных по состояниям, обратимых автоматов, не обладающих свойством УС. Следующее утверждение дает отрицательный ответ на поставленный вопрос о возможности такого построения.

Теорема 3. Пусть $A = (X, S, Y, h, f)$ – перестановочный, обратимый автомат, у которого $h_x = \delta$ при всех $x \in X$ и D – наименьшее общее кратное длин его циклов. Тогда автомат А обладает свойством УС при $r \le D + 1$.

Доказательство. Предположим, что $rang\ {}^{D+1}\alpha^* = 1$. Тогда для любых $(P_1, P_N) \in X^D$ и любых $(x, x`) \in X$ существует цепочка бинарных отношений вида:

$$P_1\, x\, {}^{D+1}\alpha\, P_2\, \varepsilon_2\, {}^{D+1}\alpha \ldots {}^{D+1}\alpha\, P_{N-1}\, \varepsilon_{N-1}\, {}^{D+1}\alpha\, P_N\, x`\ .$$

Схемой это событие можно представить в виде

$$\xrightarrow{P_1 x} B \xrightarrow{P_2 \varepsilon_2} B \longrightarrow \ldots \xrightarrow{P_{N-1}\varepsilon_{N-1}} B \xrightarrow{P_N x`} ,,$$

то есть существуют состояния $s_1, s_2, \ldots, s_{N-1}$ из S_B автомата $B = A \to A^{-1}$, для которых $B(s_j, P_j\, \varepsilon_j) = P_{j+1}\varepsilon_{j+1}$, $j \in \{1, \ldots, N-1\}$.

Положим $P_j = x^j_1, x^j_2, \ldots, x^j_D$; $x = x^1_1$. Тогда из определения величины D следует $\varepsilon_2 = x^2_1$, и далее итеративно получаем

$$\varepsilon_3 = x_1^3, \varepsilon_4 = x_1^4, \ldots, \varepsilon_{N-1} = x_1^{N-1},$$

и, наконец, $x` = x_1^N$. Следовательно, при фиксированном $P_N$ однозначно определен символ x`. Полученное противоречие и завершает доказательство теоремы.

В заключение отметим, что вопрос об алгоритмической проверке наличия свойства УС у произвольно заданного автомата остается открытым. Автор выдвигает гипотезу об алгоритмической неразрешимости данной проблемы. Косвенным обоснованием выдвижения этой гипотезы служат приводимые ниже утверждения, представляющие и самостоятельный интерес.

Воспользуемся обозначениями:

$X^\infty_{с.п}$ – множество всех смешанно-периодических последовательностей;

$X^\infty_{п}$ – множество всех чисто-периодических последовательностей.

Через $X(\infty)\in\{X^{\infty}_{с.п}, X^{\infty}_{п}\}$ обозначим одно из этих множеств, а через $X^{\infty}_{P(N)}$ обозначим подмножество множества $X(\infty)$, определенное следующим образом. Последовательность $Q\in X(\infty)$ периода $\omega(Q)$ принадлежит $X_{p(N)}$ тогда и только тогда, если $\omega(Q) = 1$, либо каждый из простых делителей числа $\omega(Q)$ не больше фиксированного числа N. Аналогичные обозначения $Y^{\infty}_{с.п}$, $Y^{\infty}_{п}$, $Y(\infty)$, $Y^{\infty}_{p(N)}$ используем для алфавита Y.

Рассмотрим следующее свойство C^{∞} конечного автомата A = (X, S, Y, h, f): существует алфавит Y', функции F_1: $X(\infty) \to Y'$, F_2: $Y^{\infty}_{с.п}\to Y'$, $F_1 \neq const$, для которых при любых $(s, Q)\in S\times X(\infty)$

$$F_1(Q) = F_2(A(s,Q)).$$

Для изучения этого свойства рассмотрим ограничения $o\text{г}\sigma$, $o\text{г}\sigma^*$ на $X(\infty)$ введенных ранее отношений σ, σ^* на X^{∞}. Несложно показывается, что свойство C^{∞} выполняется для автомата A тогда и только тогда, если $rang\ o\text{г}\sigma^* \neq 1$.

Напомним, что автомат A называют *внешне наследственным,* если для любой последовательности $Q\in X^{\infty}_{с.п}$ и любого начального состояния $s\in S$, период последовательности A(s, Q) кратен периоду входной последовательности Q.

Теорема 4. Для любого внешне наследственного автомата A и для любого обратимого автомата A

$$rang\ o\text{г}\sigma^* \neq 1.$$

Доказательство. Пусть A – обратимый автомат, Q_1 – произвольная последовательность из $X^{\infty}_{p(|S^2|)}$ и Q_k – произвольная последовательность из класса эквивалентности отношения $o\text{г}\sigma^*$, содержащего Q_1, то есть справедлива цепочка отношений $Q_1\sigma Q_2\sigma\ldots\sigma Q_к$. (Здесь k может равняться и бесконечности.) Имеем $Q_1\in X^{\infty}_{p(|S^2|)}$. Предположим, что для некоторого $j\in\{1, \ldots, k\}$ $Q_j \in X^{\infty}_{p(|S^2|)}$.

Отношение $Q_j\sigma Q_{j+1}$ равносильно существованию состояния $(s^j_1, s^j_2)\in S\times S = S_B$, при котором $B((s^j_1, s^j_2),Q_j) = Q_{j+1}$. Легко показывается, что период $\omega(Q_{j+1})$ последовательности Q_{j+1} делит величину вида $k_j\omega(Q_j)$, где k_j – некоторое число из $\{1, \ldots, |S^2|\}$. Откуда в силу $Q_j\in X^{\infty}_{p(|S^2|)}$ следует $Q_{j+1}\in X^{\infty}_{p(|S^2|)}$. Следовательно, класс эквивалентности отношения $o\text{г}\sigma^*$ на $X(\infty)$, содержащий последовательность Q_1, целиком содержится в $X^{\infty}_{p(|S^2|)}\subset X(\infty)$. Заключаем, что $rang\ o\text{г}\sigma^* \neq 1$.

Перейдем к доказательству второго утверждения теоремы. Пусть A – внешне наследственный автомат, $Q_1\in X^{\infty}_{p(|S^2|)}$ и для неко-

торых $Q_2, Q_3, \ldots, Q_k \in X(\infty)$ справедливо $Q_1 \sigma Q_2 \sigma \ldots \sigma Q_k$. Покажем, что из условия $Q_j \in X^{\infty}_{p(|S|)}$, $Q_j \sigma Q_{j+1}$ следует $Q_{j+1} \in X^{\infty}_{p(|S|)}$. По определению бинарного отношения σ условие $Q_j \sigma Q_{j+1}$ равносильно существованию состояний $(s^j_1, s^j_2) \in S_B$, при которых

$$A(s^j_1, Q_j) = A(s^j_2, Q_{j+1}).$$

Учитывая внешнюю наследственность автомата A, для периодов $\omega(Q_j)$, $\omega(Q_{j+1})$, $\omega(A(s^j_1, Q_j))$, $\omega(A(s^j_2, Q_{j+1}))$ последовательностей Q_j, Q_{j+1}, $A(s^j_1, Q_j)$, $A(s^j_2, Q_{j+1})$ имеем

$$\omega(A(s^j_1, Q_j)) = \omega(A(s^j_2, Q_{j+1})) = k_j \omega(Q_j) = k_{j+1} \omega(Q_{j+1}),$$

где $k_j, k_{j+1} \in \{1, \ldots, |S|\}$. Так как $Q_j \in X^{\infty}_{p(|S|)}$, то из последних равенств получаем $Q_{j+1} \in X^{\infty}_{p(|S|)}$. Доказательство теоремы теперь завершается аналогично доказательству ее первой части.

Часть 3. МОДЕЛИ АВТОМАТОВ НА ОСНОВЕ РАССТОЯНИЙ ХЭММИНГА

В этой части книги исследуются некоторые возможности построения приближенных моделей конечных автоматов на основе расстояния Хемминга между их табличными заданиями и выходными последовательностями. (В предыдущей части рассматривались приближенные модели конечных автоматов, построенные с использованием некоторых следствий их функционирования.)

Глава 10. МОДЕЛИ АВТОМАТОВ, ПОСТРОЕННЫЕ НА ОСНОВЕ РАССТОЯНИЯ ХЭММИНГА МЕЖДУ ИХ ТАБЛИЧНЫМИ ЗАДАНИЯМИ

В данной главе речь идет о переносе идей, связанных с использованием в криптографической практике статистических аналогов К-значных функций, на конечные автоматы[1].

10.1. О задаче определения начального состояния автомата по его входной и выходной последовательностям

Обозначим через A` = (X, S, Y, h`, f) – конечный автомат. Рассмотрим задачу определения начального состояния $s` \in S$ автомата A по его входной $P = x_1, x_2, \ldots, x_L$ и выходной $A`(s`, P) = y_1, y_2, \ldots, y_L$ последовательностям. При практическом решении этой задачи из известных алгоритмов ее решения обычно выбирают алгоритм с меньшей трудоемкостью. Этот выбор, как правило, зависит от свойств автомата A`. Например, при малом числе |S| состояний автомата применяют тотальный метод: опробуют все его состояния $s \in S$ до получения состояния s*, при котором $A`(s^*, P) = y_1, y_2, \ldots, y_L$, и объявляют s* искомым состоянием. При линейном автомате, то есть в случае, когда система уравнений, описывающих выходную последовательность $y_1, y_2, \ldots, y_L$, линейна, решают эту систему каким-либо методом [23], например методом Гаусса, и одно из решений объявляют искомым. В других случаях иногда пытаются найти гомоморфный образ автомата A` с меньшим числом состояний или

[1] *Источник*: [17].

линейный гомоморфный образ (линейный автомат в упомянутом выше смысле) и решают сначала поставленную задачу для этого образа [29]. Таким образом, для известных методов решения уравнения

$$A`(s`, P) = y_1, y_2, \ldots, y_L \qquad (17)$$

относительно $s`\in S$ выделяется класс автоматов, для которых уравнение (17) решается с небольшой трудоемкостью. Для остальных автоматов A` известные методы решения (17) сравнимы по сложности с тотальным методом.

Первый этап предлагаемого нового подхода к решению уравнения (1) состоит в предварительном поиске нового вспомогательного автомата A = (X, S, Y, h, f), отличающегося от A` функцией перехода h, для которого:

1) для каждого входного символа $x\in X$ и случайно, равновероятно выбранного состояния $s\in S$ вероятность q_x события

$$hxs = h`xs \qquad (18)$$

достаточно большая;

2) уравнение вида (17) для нового автомата A решается с небольшой трудоемкостью.

На втором этапе применяют один из двух подходов: 1) решают для автомата A уравнение

$$A(s, x1, x2, \ldots, xR) = y1, y2, \ldots, yR, \qquad (19)$$

где R – максимальное из чисел {1, 2, …, L}, при котором уравнение (19) имеет решение, и найденное решение объявляется искомым решением уравнения (17); 2) выбирают C из {1, 2, …, L} и объявляют состояние $s\in S$ ложным, если $A(s, x_1, x_2, \ldots, x_C) \neq y_1, y_2, \ldots, y_C$.

В указанном способе решения уравнения (17) его трудоемкость определяется трудоемкостью построения вспомогательного автомата A – статистического аналога автомата A` – и трудоемкостью решения уравнения (19), которая по предположению 2) не велика. Естественно, возникает вопрос: как часто данный способ приводит к успеху? Этот вопрос можно более точно сформулировать следующим образом: какова вероятность правильного нахождения решения уравнения (17) при случайном и равновероятном выборе автомата – оригинала A` среди всех автоматов с заданной близостью (набор вероятностей $(q_x)_{x\in X}$) к заранее фиксированному автомату-модели A.

Далее предлагаются вероятностные модели получения выходной последовательности случайно выбранного автомата A`, при известном его вспомогательном автомате A, указываются статистические процедуры нахождения начального состояния автомата A`. В рамках этих моделей проводятся расчеты эффективности таких процедур.

Конечно же при практическом использовании приведенных в данном параграфе результатов следует проводить предварительную проверку соответствия данных вероятностных моделей конкретной практической ситуации.

Основные результаты параграфа изначально опубликованы в [16]. Более полную информацию о практических примерах возникновения задач, связанных с решением случайных систем уравнений можно найти в [20].

10.2. Использование статистического аналога конечного автомата, построенного с помощью искажений его частичных функций переходов

Пусть $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ – вспомогательный автомат (статистический аналог) автомата $A` = (X, S, Y, (h`_x)_{x\in X}, (\beta_x)_{x\in X})$, для которого вероятность события $h_x s \neq h`_x s$ при случайном и равновероятном выборе состояния $s\in S$ равна $p_x$, $x\in X$. Для автоматов A, A` построим вспомогательный вероятностный автомат

$$A^* = (X, S\cup\{t\}, Y, (h_x^*)_{x\in X}, (f_x^*)_{x\in X}, (p_x)_{x\in X}),$$

где X – входной алфавит, Y – выходной алфавит, $S\cup\{t\}$ – множество состояний (здесь t – некоторое новое состояние, $t\notin S$), ,$(h_x^*)_{x\in X}$, $(f_x^*)_{x\in X}$ – частичные функции переходов и выходов автомата A*, они заданы условными вероятностями

$$P(s`/x, s) = P(\delta_x^* s = s`) = \begin{cases} q_x = 1 - p_x, & \text{если } s' = h_x s, \\ p_x & \text{, если } s' = t, \end{cases}$$

$$P(t/x, t) = P(h_x^* t = t) = 1,\ x\in X$$

$$P(y`/x,s) = P(f_x^* s = y`) = 1, \text{ при } y` = f_x s,\ s\in S.$$

$$P(y`/x, t) = P(f_x^* t = y`) = \frac{1}{|Y|},\ y`\in Y.$$

Таким образом, вероятностный автомат A* при входном символе $x\in X$ переходит из одного состояния в другое, как автомат A с вероятностью q_x, кроме того, имеется новое состояние «сбоя» t, в ко-

торое оно переходит из любого состояния $s \in S$ с вероятностью p_x при входном символе $x \in X$. При этом переходе он затем вырабатывает, случайную, равновероятную последовательность элементов из Y.

Решаемая в этом разделе задача состоит в следующем. При фиксированной входной последовательности $P = x_1, x_2, \ldots, x_L$ и начальном состоянии $s` \in S`$, $S` \subseteq S$ получена выходная последовательность автомата A:

$$A(s`, P) = y_1^1, y_2^1 \ldots, y_L^1, y_j^1 \in Y, \ j \in \overline{1,L}.$$

Требуется построить статистическую процедуру определения s` по известным наблюдениям выходной последовательности автомата A*:

$$A^*(s`, P) = \hat{y}_1, \hat{y}_2, \ldots, \hat{y}_L, \ \hat{y}_j \in Y, \ j \in \overline{1,L}$$

и известному входному слову $P = x_1, x_2, \ldots, x_L$.

Для $s \in S`$ обозначим через ${}^A f_s^{s`}$ максимальное $j \in \overline{1,L}$, при котором

$$A(s, x_1, x_2, \ldots, x_J) = \hat{y}_1, \hat{y}_2, \ldots, \hat{y}_j.$$

Полагаем ${}^A f_s^{s`} = 0$, если $A(s, x_1) \neq \hat{y}_1$.

Первый вариант поиска состояния s` из S` таков. Пусть $S^*(s`)$-множество всех таких $s^* \in S`$, при которых

$${}^A f_{s^*}^{s`} = \max_{s` \in S`} {}^A f_s^{s`}.$$

Тогда случайно и равновероятно выбранное состояние s^* из $S^*(s`)$ объявляем искомым состоянием s`.

Несложно показывается, что данный метод является по существу методом максимального правдоподобия [22]. Поиск s` указанным методом будем кратко называть методом МП.

Второй подход определения искомого состояния s` состоит в применении порогового критерия с уровнем C, а именно фиксируется $C \in \{1, \ldots, L\}$ и состояние $s \in S`$ объявляется ложным тогда и только тогда, когда

$$A(s, x_1, x_2, \ldots, x_C) \neq \hat{y}_1, \hat{y}_2, \ldots, \hat{y}_C.$$

Представляет интерес вычисление следующих вероятностей:

1. Вероятности $P_{A, A^*}(s`) = P(s^* = s`)$ правильного принятия решения при применении метода МП для фиксированного автомата A с фиксированным начальным состоянием $s` \in S`$.

2. Вероятности $P_{A,\,A^*} = P(s^* = s`) = \frac{1}{|S`|}\sum_{s`\in S`} P(s^* = s / s = s`)$ правильного принятия решения методом МП при случайном и равновероятном выборе начального состояния s` из S` для фиксированного автомата A.

3. Вероятности $P_{\Phi}(s`) = \frac{1}{|\Phi|}\sum_{A\in\Phi} P(s^* = s`/A)$ правильного принятия решения методом МП при случайном и равновероятном выборе автомата A (с фиксированным состоянием s`) из некоторого класса автоматов Ф.

4. Вероятности правильного принятия решения методом МП при случайном и равновероятном выборе автомата A из некоторого класса автоматов Ф и случайном и равновероятном выборе его начального состояния $s`\in S`$.

При использовании второго подхода определения искомого состояния s`, состоящего в применении м методе МП порогового критерия с уровнем C, представляет интерес подсчет вероятности α отбраковки искомого состояния $s`\in S`$ и среднего числа M ложных решений при всех выше перечисленных вероятностных постановках задачи.

Теорема 1. Пусть $P = x_1, x_2, \ldots, x_L$ – фиксированная последовательность элементов алфавита X, s` – фиксированный элемент из S`, $S`\subseteq S$, Ф(1) – некоторое множество автоматов с параметрами X, S, Y такое, что при случайном и равновероятном выборе автомата $\mathcal{A} = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ из Ф(1)

$$P(\mathcal{A}(\bar{s}, x_1, \ldots, x_k) = \mathcal{A}(s`, x_1, \ldots, x_k)) \le \bar{p}_k < 1,\ k\in\overline{1,L}$$

при любом состоянии $\bar{s}\in S`$, $s`\neq\bar{s}$, причем

$$\bar{p}_k\frac{1}{|Y|} \le \bar{p}_{k+1},\ \bar{p}_{k+1} < \bar{p}_k,\ k\in\overline{1,L-1};\ \bar{p}_0 = 1.$$

1. Пусть автомат A выбирается случайно и равновероятно из Ф(1). Тогда вероятность $P_{\Phi(1)}(s^*\neq s`)$ ошибки в определении искомого состояния s` из уравнения

$$A^*(s`, x_1, x_2, \ldots, x_L) = y_1, y_2, \ldots, y_L$$

методом максимального правдоподобия оценивается следующим образом

$$P_{\Phi(1)}(s^* \neq s`) < \min(P({}^{A}f_{s`}^{s`} < c) + |S`|\ \bar{p}_{c-1}),\ c\in\overline{1,L},$$

где минимум берется по всем $c\in\{1, \ldots, L\}$ и

$$P({}^{A}f_{s`}^{s`} < 1) = 0,$$

$$P({}^{A}f_{s`}^{s`} < c) = 1 - (P\chi_1 \frac{1}{|Y|^{c-1}} + q_{x_1} p_{x_2} \frac{1}{|Y|^{c-2}} + q_{x_1} q_{x_2} p_{x_3} \frac{1}{|Y|^{c-3}} + \ldots$$

$$+ q_{x_1} q_{x_2} \ldots q_{x_{c-2}} p_{x_{c-1}} \frac{1}{|Y|} + q_{x_1} \ldots q_{x_{c-1}}).$$

Пусть дополнительно выполнены условия

$$p_x = p,\ x \in X,\ L \geq C(0),$$

где $C(0)$ – минимальное натуральное число, при котором

$$p \geq |S`|\,\bar{p}_{C(0)-1}.$$

Тогда

$$P_{\Phi(1)}(s^* \neq s`) < pC(0)$$

Пусть выполнено еще одно дополнительное условие

$$\bar{p}_k = \bar{p}_1^{\,k},\ k \in \overline{1,L},$$

и p есть функция от $|S`|$, $p = p(|S`|)$. Тогда

$$P_{\Phi(1)}(s^* \neq s`) \to 0 \text{ при } |S`| \to \infty \text{ и } P(|S`|)\ln|S`| \to 0.$$

Доказательство. Положим $\overline{S`} = S`\backslash\{s`\}$ и $\Phi_1 = \Phi$. Для $c \in \overline{1,L}$ имеем

$$P_{\Phi}(s^* \neq s`) = \frac{1}{|\Phi|} \sum_{A \in \Phi} P(s^* \neq s`/A) \leq \frac{1}{|\Phi|} \sum_{A \in \Phi} P({}^{A}f_{s`}^{s`} \leq \max_{\bar{s} \in \overline{S`}} {}^{A}f_{\bar{s}}^{s`}) =$$

$$= \frac{1}{\Phi} \sum_{A \in \Phi} [\sum_{k=1}^{c-1} P({}^{A}f_{s`}^{s`} = k,\ \max_{\bar{s} \in \overline{S`}} {}^{A}f_{\bar{s}}^{s`} \geq k) + \sum_{k=c}^{L} P({}^{A}f_{s`}^{s`} =$$

$$= k,\ \max_{\bar{s} \in \overline{S`}} {}^{A}f_{\bar{s}}^{s`} \geq k)] \leq$$

$$\leq \frac{1}{|\Phi|} \min_{c} \sum_{A \in \Phi} [\, P({}^{A}f_{s`}^{s`} < c) + \sum_{\bar{s} \in \overline{S`}} P({}^{A}f_{\bar{s}}^{s`} \geq c\,)] =$$

$$= \min_{c} [\, P({}^{A}f_{s`}^{s`} < c) + \frac{1}{|\Phi|} \sum_{A \in \Phi} \sum_{\bar{s} \in \overline{S`}} P({}^{A}f_{\bar{s}}^{s`} \geq c\,)].$$

Здесь учтено, что вероятность $P({}^{A}f_{s`}^{s`} < c)$ не зависит от $A \in \Phi$. Оценим каждое слагаемое последнего выражения. Имеем

$$P({}^{A}f_{s`}^{s`} < c) = 1 - P({}^{A}f_{s`}^{s`} \geq c) = 1 - (P x_1 \frac{1}{|Y|^{c-1}} + q_{x_1} p_{x_2} \frac{1}{|Y|^{c-2}} + \ldots +$$

$$+ q_{x_1} q_{x_2} \ldots q_{x_{c-2}} p_{x_{c-1}} \frac{1}{|Y|} + q_{x_1} \ldots q_{x_{c-1}}),$$

и в случае $q_x = q$, $p_x = p$, $x \in X$, это выражение равно

$$\frac{P}{|Y|q-1}(q^{c-1} - (\frac{1}{|Y|})^{c-1}) - q^{c-1} < 1 - q^{c-1} < P(c-1).$$

Оценим теперь второе слагаемое

$$\frac{1}{|\Phi|}\sum_{A\in\Phi}\ \sum_{\bar{s}\in\bar{S}_o} P({}^{A}f_{\bar{s}}^{s`}\geq c) = \sum_{\bar{s}\in\bar{S}`}\ \frac{1}{|\Phi|}\sum_{A\in\Phi} P({}^{A}f_{\bar{s}}^{s`}\geq c).$$

Для этого оценим вероятность

$$\frac{1}{|\Phi|}\sum_{A\in\Phi} P({}^{A}f_{\bar{s}}^{s`}\geq c) = P(\text{Ж}(\bar{s}, x_1, x_2, \ldots, x_c) = A^*(s`, x_1, x_2, \ldots, x_c)),$$

где Ж случайно и равновероятно выбирается из Ф.

Положим для краткости

$$\text{Ж}(s)_c = \text{Ж}(s, x_1, x_2, \ldots, x_c),\ \ \text{Ж}^*(s)_c = \text{Ж}^*(s, x_1, x_2, \ldots, x_c).$$

Имеем

$$P(\text{Ж}(\bar{s})_c = \text{Ж}^*(s`)_c) = P(\text{Ж}(\bar{s})_c = \text{Ж}^*(s`)_c / \text{Ж}(\bar{s})_c = \text{Ж}(s`)_c)\times$$
$$\times P((\text{Ж}(\bar{s})_c = \text{Ж}(s`)_c) + P(\text{Ж}(\bar{s})_c = \text{Ж}^*(s`)_c;\ \ \text{Ж}(\bar{s})_c \neq \text{Ж}(s`)_c).$$

По условию теоремы

$$P(\text{Ж}(\bar{s})_c = \text{Ж}(s`)_c) \leq \bar{p}_c\ .$$

Поэтому

$$P(\text{Ж}(\bar{s})_c = \text{Ж}^*(s`)_c) \leq P({}^{\text{Ж}}f_{s`}^{s`}\geq c)\ \bar{p}_c + P(\text{Ж}(\bar{s})_c = \text{Ж}^*(s`)_c;$$
$$\text{Ж}(\bar{s})_c \neq \text{Ж}(s`)_c).$$

Событие: $\text{Ж}(\bar{s})_c \neq \text{Ж}(s`)_c$ представим в виде

$$\text{Ж}(\bar{s})_c \neq \text{Ж}(s`)_c = \bigcup_{j=1}^{c}\ (\text{Ж}(\bar{s})_c \neq {}^{P}\text{Ж}(s`)_c),$$

где $\text{Ж}(\bar{s})_c \neq {}^{P}\text{Ж}(s`)_c$ – событие, состоящее в том, что первые P–1 символов последовательностей $\text{Ж}(\bar{s})_c$ и $\text{Ж}(s`)_c$ совпадают, а их P-е символы различны.

$$P(\text{Ж}(\bar{s})_c = \text{Ж}^*(s`)_c;\ \text{Ж}(\bar{s})_c \neq \text{Ж}(s`)_c) =$$
$$= \sum_{j=0}^{c-1} P(\text{Ж}(\bar{s})_c = \text{Ж}^*(s`)_c;\ \ \text{Ж}(\bar{s})_c \neq {}^{P+1}\text{Ж}(s`)_c) =$$
$$= \sum_{j=0}^{c-1} P(\text{Ж}(\bar{s})_c = \text{Ж}^*(s`)_c / \text{Ж}(\bar{s})_c \neq {}^{P+1}\text{Ж}(s`)_c) P(\text{Ж}(\bar{s})_c \neq {}^{P+1}\text{Ж}(s`)_c) \leq$$
$$\leq \sum_{j=0}^{c-1}\ \sum_{A\in\Phi} P(A(\bar{s})_c = A^*(s`)_c \,/\, A(\bar{s})_c \neq {}^{P+1}A(s`)_c)\, P(\text{Ж} = A)\ \bar{p}_j =$$
$$= \sum_{j=0}^{c-1}\ \sum_{A\in\Phi} P({}^{A}f_{s`}^{s`} = P)\ \frac{1}{|Y|^{c-j-1}}\ \frac{1}{|Y|\ -1}\ \frac{1}{|\Phi|}\ \bar{p}_j\ \leq$$

$$\leq \sum_{j=1}^{c-1} P({}^{A}f_{s`,s`} = P)\ \bar{p}_{c-1} = \bar{p}_{c-1}\ P({}^{A}f_{s`,s`} < c).$$

При получении последнего неравенства использованы неравенства

$$\bar{p}_k \frac{1}{|Y|} \leq \bar{p}_{k+1},\ k \in \overline{1, L-1}.$$

Итак,

$$P_{\Phi}(s^* \neq s`) \leq \min_{c} [\ P({}^{A}f_{s`,s`} < c) + \sum_{\bar{s} \in \bar{S}_o} (P({}^{\%}f_{s`,s`} \geq c)\bar{p}_c + \bar{p}_{c-1}$$

$$P({}^{A}f_{s`,s`} < c))] <$$

$$< \min_{c \in \overline{1,L}} [\ P({}^{A}f_{s`,s`} < c) + |S`|\ \bar{p}_{c-1}\ .$$

Пусть $p_x = p$, $x \in X$ и $L > c_0$, где c_0 – минимальное натуральное число, при котором $p \geq |S`|\ \bar{p}_{c_o-1}$. Тогда

$$P_{\Phi}(s^* \neq s`) < P({}^{A}f_{s`,s`} < c_o) + |S`|\bar{p}_{c_o-1} \leq p\ (c_0 - 1) + p = pc_0.$$

Пусть дополнительно $\bar{p}_k = p_1^k$, $k \in \overline{1, L}$. Тогда

$$P_{\Phi}(s^* \neq s`) < pc_0 \leq P(\frac{\ln p - \ln|S`|}{\ln \bar{p}_1} + 2).$$

Последняя величина стремится к нулю при $|S`| \to \infty$ и $p\ln|S`| \to 0$.

Приведем пример множества Φ автоматов A, удовлетворяющих условиям теоремы 1. Пусть Δ – некоторое непустое подмножество множества всех полноцикловых преобразований S. Λ – множество всех отображений S в Y. Множество Φ состоит из автономных автоматов $A = (S, Y, h, \lambda)$, $h \in \Delta$, $\lambda \in \Lambda$. Положим $L < \frac{1}{2}|S|$. Выберем произвольное $s \in S`$, $s \neq s`$. Тогда при случайном и равновероятном выборе автомата $\%$ из Φ

$$P(\%(s, x_1, \ldots, x_P) = \%(s`, x_1, \ldots, x_P)) = \frac{1}{|Y|^j},\ P \in \{1, 2, \ldots, L\},$$

и в качестве оценки $\bar{p}_k$ может быть взята величина $\frac{1}{|Y|^j}$.

В условиях пункта 2 данной теоремы при

$$|Y| = 2,\ |S`| = 2^n,\ p = \frac{1}{2^m},\ \bar{p}_k = \frac{1}{2^k}$$

справедлива оценка

$$P_{\Phi}(s^{*} \neq s`) \leq \frac{n+m+1}{2^{m}},$$

при $c_0 = n+m+1$, $L \geq c_0$.

Теорема 2. Пусть выполнены условия пункта 1 теоремы 1. Тогда при применении порогового критерия с уровнем c в методе максимального правдоподобия вероятность α-отбраковки истинного решения s` есть величина

$$\alpha = 1 - \left(p_{x_1} \frac{1}{|Y|^{c-1}} + q_{x_1} p_{x_2} \frac{1}{|Y|^{c-2}} + \ldots + q_{x_1} \ldots q_{x_{c-2}} p_{x_{c-1}} \frac{1}{|Y|} + q_{x_1} \ldots q_{x_{c-1}}\right) =$$

$$= P({}^{A}f_{s`}^{s`} < c),$$

а среднее число M ложных решений оценивается неравенством

$$M < |S`| \bar{p}_{c-1}.$$

Доказательство. Имеем

$$\alpha = \frac{1}{|\Phi|} \sum_{A \in \Phi} P({}^{A}f_{s`}^{s`} < c) = P({}^{A}f_{s`}^{s`} < c),\ M = \frac{1}{|\Phi|} \sum_{A \in \Phi} \sum_{\bar{s} \in \overline{S`}} P({}^{A}f_{\bar{s}}^{s`} \geq c).$$

Указанные в теореме оценки этих величин получены при доказательстве пункта 1 теоремы 1.

Пусть $A = (X, S, Y, h, f)$ – фиксированный автомат, $|Y|>1$, $|S|>1$ и $P = x_1, x_2, \ldots, x_L$ – его фиксированная входная последовательность, s` – фиксированное состояние, $s` \in S`$, $S` \subseteq S$, при котором

$$A(s`, P) = A(s`, x_1, x_2, \ldots, x_L) = y_1^{o}, y_2^{o}, \ldots, y_L^{o},$$

причем $A(s, P) \neq A(s`, P)$ при любом $s \in S`$, $s \neq s`$.

Обозначим через S^k, $k \in \overline{1, L-1}$ множество состояний $s \in \overline{S`}$, $\overline{S`} = S` \backslash \{s`\}$, для которых

$$A(s, x_1, x_2, \ldots, x_к, x_{к+1}) = y_1^{o}, y_2^{o}, \ldots, y_к^{o}, y_{к+1}, \text{ и } y_{к+1} \neq y_{к+1}^{o},$$

а *через $k_o = k_o(s`)$ – минимальное натуральное число, при котором*

$$\bigcup_{k=0}^{k_o} S^k = \overline{S`}.$$

Из указанных выше условий следует, что $k_o < L$.

Последовательность множеств S^0, S^1, …, S^{k_o} назовем *спектром автомата* A с начальным состоянием s` и входным словом P или кратко – *спектром* A(s`, P).

Пусть

$$æ_c = \{s \in S` : A(s, x_1, x_2, \ldots, x_c) = y_1^{o}, y_2^{o}, \ldots, y_c^{o}\},\ c \in \overline{1, L}.$$

Очевидно, что $\bigcup_{k=c}^{k_o} S^k = æ_c \backslash \{s`\}$ . Положим $Y^{к+1}(s`) = \bigcup_{s \in S^k} y_{к+1}(s)$,

где $y_{к+1}(s)$ определен из условия

$$A(s, x_1, x_2, \ldots, x_{к+1}) = y_1^o, y_2^o, \ldots, y_к^o, y_{к+1}(s),$$

то есть $Y^{к+1}(s`)$ – множество тех $y \in Y \backslash \{y_{к+1}^o\}$, для которых последовательность $y_1^o, y_2^o, \ldots, y_к^o, y_{к+1}(s)$ не является запретом автомата A с множеством начальных состояний S`, при входной последовательности $x_1, x_2, \ldots, x_{к+1}$ (последовательность $y_1^o, y_2^o, \ldots, y_к^o, y_{к+1}(s)$ может быть получена с автомата A с некоторого состояния из S` при входной последовательности $x_1, x_2, \ldots, x_{к+1}$).

Теорема 3. Пусть S^0 , S^1 , …, S^{k_o} – спектр $A(s_o, P)$, $s` \in S`$, $S` \subseteq S$; $P = x_1, x_2, \ldots, x_L$; s* – случайно и равновероятно выбранное состояние из множества состояний S*(s`), при которых

$$^A f_{S^*}^{S`} = \max_{s \in S`} {}^A f_s^{s`} .$$

Тогда вероятность правильного принятия решения методом МП есть величина

$$P_{A,\,A^*}(s`) = P(s^* = s`) = P({}^A f_{s`}^{s`} > k_o) + \sum_{c=1}^{k_o} \varepsilon_c P({}^A f_{s`}^{s`} = c) \frac{1}{|æ_C|},$$

где

$$\varepsilon_C = \begin{cases} 1 \quad ,\int \; если \; S^C = \varnothing, \\ 1 - \dfrac{|Y^{c+1}(s`)|}{|Y| - 1}, если \; S^C \neq \varnothing \end{cases},$$

$$P({}^A f_{s`}^{s`} > k_o) = P_{x_1} \frac{1}{|Y|^{k_0}} + q_{x_1} P_{x_2} \frac{1}{|Y|^{k_0 - 1}} + \ldots + q_{x_1} \ldots q_{x_{k_0 - 1}} P_{x_{k_0}} \frac{1}{|Y|} + q_{x_1} \ldots q_{x_{k_0}},$$

$$P({}^A f_{s`}^{s`} = c) = P_{x_1} \frac{|Y| - 1}{|Y|^c} + q_{x_1} P_{x_2} \frac{|Y| - 1}{|Y|^{c-1}} + \ldots + q_{x_1} \ldots q_{x_{c-1}} P_{x_c} \frac{|Y| - 1}{|Y|}.$$

Доказательство. Положим для краткости ${}^A f_s^{s`} = f_s$.Имеем

$$P(s^* = s`) = \sum_{c=1}^{L} P(c > \max_{\bar{s} \in \overline{S`}} f_{\bar{s}} / f_{s`} = c) P(f_{s`} = c) +$$

$$+ \sum_{c=1}^{L} P(\max_{\bar{s} \in \overline{S`}} f_{\bar{s}} = c \,/\, f_{s`} = c) \frac{1}{|æ_C|}.$$

Для подсчета отдельных слагаемых изучим предварительно понятие случайной величины $f_{\bar{s}}$, $\bar{s} \in \overline{S`}$. Пусть $y = y_1, y_2, \ldots, y_L$, $y' = y'_1, y'_2, \ldots, y'_L$ – произвольные последовательности из Y^L.

Обозначим через γ (y, y') максимальное $j \in \overline{0,L}$, при котором

$$y_1, y_2, \ldots, y_J = y'_1, y'_2, \ldots, y'_J.$$

Положим для краткости

$$A(s)_к = A(s, x_1, x_2, \ldots, x_к); \quad A^*(s)_к = A^*(s, x_1, x_2, \ldots, x_к); \; к \in \overline{1,L}, \; s \in S.$$

Пусть $A(s`)_L = y_1^o, y_2^o, \ldots, y_L^o$ и $f_{s`} = c$, $c \in \overline{1,L}$. Тогда случайная переменная величина $A^*(s`)_L$ имеет вид

$$A^*(s`)_L = y_1^o, y_2^o, \ldots, y_c^o, \tilde{y}^o_{c+1}, \tilde{y}_{c+2}, \ldots, \tilde{y}_L,$$

где $\tilde{y}^o_{c+1}$, при $c < L$, не может принять значение y^o_{c+1}.

При $s(k) \in S^k$ последовательность $A(s(k))_L$ имеет вид

$$A(s(k))_L = y_1^o, y_2^o \ldots, y_k^o, \bar{y}^o_{k+1}, y_{k+2}, \ldots, y_L,$$

где $\bar{y}^o_{k+1} \neq y^o_{k+1}$.

Случайная величина $f_{s(k)}$, по определению, есть случайная величина

$$\gamma_{s(k)} = \gamma\,(A(s(k))_L, A^*(s`)_L) =$$

$$= \gamma\,(y_1^o, y_2^o \ldots, y_к^o, \bar{y}^o_{k+1}, y_{k+2}, \ldots, y_L; y_1^o, y_2^o \ldots, y_c^o, \tilde{y}^o_{c+1}, \tilde{y}_{c+2}, \ldots, \tilde{y}_L).$$

Поэтому при $k < c$ $P(f_{s(k)} = к) = P(\gamma_{s(k)} = к) = 1$, а при $k > c$ $P(f_{s(k)} = c) = 1$.

При $k = c$, $\gamma_{s(k)}$ имеет вид

$$\gamma_{s(k)} = \gamma\,(y_1^o, y_2^o, \ldots, y_c^o, \bar{y}^o_{c+1}, y_{c+2}, \ldots, y_L; y_1^o, y_2^o, \ldots, y_c^o,$$

$$\tilde{y}^o_{c+1}, \tilde{y}_{c+2}, \ldots, \tilde{y}_L),$$

где $\tilde{y}^o_{c+1}, \tilde{y}_{c+2}, \ldots, \tilde{y}_L$ – случайные переменные величины с распределением

$$P(\tilde{y}^o_{c+1} = y) = \frac{1}{|Y|-1}, \text{ для } y \neq y_{c+1}^o,$$

$$P(\tilde{y}_{c+j} = y) = \frac{1}{|Y|}, \text{ для } y \in Y, \; J \in \overline{2, L-c}.$$

Поэтому при $k = c$

$$P(f_{s(k)} < k) = 0, \qquad P(f_{s(k)} = k) = 1 - \frac{1}{|Y|-1},$$

$$P(f_{s(k)} = k + J) = \frac{1}{(|Y|-1)|Y|^{j+1}}\left(1 - \frac{1}{|Y|}\right), \; J \in \overline{1, L-k-1},$$

$$P(f_{s(k)} = L) = \frac{1}{(|Y|-1)|Y|^{L-k-1}}.$$

Итак, можно сформулировать промежуточные выводы. Если $f_{s`} = c$, то

1.

$$\max_{s(k)\in S^k \neq \varnothing} f_{s(k)} = \begin{cases} k, & при\ \ k < c, \\ c, & при\ \ k > c, \\ \geq k, & при\ k = c. \end{cases}$$

2.

$$\max_{\bar{s}\in S`} f_{\bar{s}} = \begin{cases} k_{O'}, & при\ \ c > k_{O'}, \\ \max(c, \max_{s(c)\in S^c} f_{s(c)}), & при\ k_O \geq c. \end{cases}$$

Исходя из этих фактов, получаем:

$$P(c > \max_{\bar{s}\in S`} f_{\bar{s}} / f_{s`} = c) = \begin{cases} 0, & при\ \ k_O \geq c, \\ 1, & при\ \ k_O < c, \end{cases}$$

$$P(c = \max_{\bar{s}\in S`} f_{\bar{s}} / f_{s`} = c) = 0, \text{ при } k_o < c.$$

Следовательно,

$$P(s^* = s`) = \sum_{c=k_O+1}^{L} P(f_{s`} = c) + \sum_{c=1}^{k_O} P(\max_{\bar{s}\in S`} f_{\bar{s}} = c / f_{s`} = c))P(f_{s`} = c)\frac{1}{|æ_C|}.$$

При $c \leq k_o$ имеем

$$P(c = \max_{\bar{s}\in S`} f_{\bar{s}} / f_{s`} = c)) = P(c = \max(c, \max_{s(c)\in S^c} f_{s©}) / f_{s`} = c) =$$

$$= \begin{cases} 1, & \text{, если } S^C = \varnothing \\ P(\max_{s(c)\in S^c} f_{s(c)} = c / f_{s`} = c) = 1 - \dfrac{|Y_{s`}^{c+1}|}{|Y|-1} & \text{, если } S^C \neq \varnothing. \end{cases}$$

Таким образом,

$$P(s^* = s`) = P(f_{s`} > k_o) + \sum_{c=1}^{k_O} \varepsilon_c P(f_{s`} = c)\frac{1}{|æ_C|},$$

где ε_c определено в условиях теоремы. Получение значений $P(f_{s`} > k)$ и $P(f_{s`} = c)$ не представляет затруднений.

Теорема 4. Пусть S^0, S^1, …, S^{k_o} – спектр A(s`, P), s`∈S`, S`⊆S; P = $x_1, x_2, \ldots, x_L$. Если s* – состояние автомата A из множества состояний, при которых

$$^{A}f_{s^*}^{s`} = \max_{s \in S`} {}^{A}f_{s}^{s`},\ s^* \in S_o,$$

то

$$P(s^* = s`) \geq 1 - \sum_{k=1}^{k_O} |S^k| P({}^{A}f_{s`}^{s`} \leq k).$$

Доказательство. Положим $^{A}f_{s}^{s`} = f_s$. Имеем

$$P(s^* = s`) \geq P(f_{s`} > \max_{\bar{s} \in \overline{S`}} f_{\bar{s}}) = 1 - P(\max_{\bar{s} \in \overline{S`}} f_{\bar{s}} \geq f_{s`}) = 1 - P(\bigcup_{\bar{s} \in \overline{S`}} f_{\bar{s}} \geq f_{s`}) =$$

$$= 1 - \sum_{k=0}^{k_O} |S^k| P(f_{s(k)} \geq f_{s`}),$$

где $s(k) \in S^k$. Далее

$$P(f_{s(k)} \geq f_{s`}) = \sum_{c=1}^{L} P(f_{s(k)} \geq c / f_{s`} = c)\, P(f_{s`} = c).$$

Интервал суммирования $\overline{1,L}$ разобьем на три части:

1) $1 \leq c < k$;
2) $c = k$;
3) $L \geq c > k$.

При доказательстве теоремы 3 было показано, что

$$P(f_{s(k)} = k / f_{s`} = c) = 1, \text{ при } k < c,$$
$$P(f_{s(k)} = c / f_{s`} = c) = 1, \text{ при } c < k,$$
$$P(f_{s(k)} \geq k / f_{s`} = c) = 1, \text{ при } k = c.$$

Суммирование по трем указанным интервалам величин

$$P(f_{s(k)} \geq c / f_{s`} = c)\, P(f_{s`} = c)$$

дает соответственно значения $P(f_{s`} < k)$; $P(f_{s`} = k)$ и 0 – ноль.

Следовательно,

$$P(f_{s(k)} \geq f_{s`}) = P(f_{s`} \leq k).$$

Поэтому

$$P(s^* = s`) \geq 1 - \sum_{k=0}^{k_O} |S^k| P(f_{s`} \leq k) = 1 - \sum_{k=1}^{k_O} |S^k| P(f_{s`} \leq k),$$

так как $P(f_{s`} = 0) = 0$.

Теорема 5. Пусть S^0, S^1, …, S^{k_o} – спектр A(s`, P), s`∈S`, S`⊆S; P = x(1), x(2), …, x(L). Тогда, при применении порогового критерия

с уровнем $c \in \overline{1,L}$ в методе максимального правдоподобия вероятность α отбраковки истинного решения s` есть величина

$$\alpha = P({}^{A}f_{s`}^{s`} < c) =$$

$$= 1 - (p_{x(1)}\frac{1}{|Y|^{c-1}} + q_{x(1)}p_{x(2)}\frac{1}{|Y|^{c-2}} + \ldots + q_{x(1)}q_{x(2)}\ldots q_{x(c-2)}p_{x(c-1)}\frac{1}{|Y|} +$$

$$+ q_{x(1)}q_{x(2)}\ldots q_{x(c-1)}),$$

а среднее число ложных решений равно величине

$$M_{s`} = (|æ_c| - 1)P({}^{A}f_{s`}^{s`} \geq c) + \sum_{k=1}^{c-1} |S^k|\, P({}^{A}f_{s`}^{s`} = k)\, \frac{1}{(|Y|-1)|Y|^{c-k-1}},$$

при $c \leq к_o$, и

$$M_{s`} = \sum_{k=1}^{k_o} |S^k|\, P({}^{A}f_{s`}^{s`} = k)\, \frac{1}{(|Y|-1)|Y|^{c-k-1}} \quad \text{при } c > k_o.$$

Доказательство. Значение α найдено при доказательстве теоремы 1. Положим ${}^{A}f_{s}^{s`} = f_s$. Имеем

$$M_{s`} = \sum_{\bar{s} \in \bar{S`}} P(f_{\bar{s}} \geq c) = \sum_{k=0}^{k_o} |S^k| P(f_{s(к)} \geq c) =$$

$$= \sum_{k=0}^{k_o} |S^k| \sum_{j=1}^{L} P(f_{s(к)} \geq c / f_{s`} = j)\, P(f_{s`} = j).$$

Интервал $\overline{0,k_0}$ суммирования в случае $k_o \geq c$ разобьем на две части: $\overline{0,c-1}$ и $\overline{c,k_0}$. Используя найденное при доказательстве теоремы 1 условное распределение случайной величины $f_{s(к)}$, получаем

$$M_{s`} = \sum_{k=1}^{c-1} |S^k|\, P(f_{s(k)} \geq c / f_{s`} = k) P(f_{s`} = k) + \sum_{k=c}^{k_o} |S^k|\, P(f_{s`} \geq c) =$$

$$= \sum_{k=1}^{c-1} |S^k| \frac{1}{(|Y|-1)|Y|^{c-k-1}} P(f_{s`} = k) + P(f_{s`} \geq c) \sum_{k=c}^{k_o} |S^k|.$$

Теперь остается заметить, что $\sum_{k=c}^{k_o} |S^k| = |æ_c| - 1$.

Случай $c = k_o$ рассматривается аналогично. Теорема доказана.

Предположим, что автомат A такой, что $|S`| = |S| = |Y|^n$ и при входном слове $P = x_1, x_2, \ldots, x_L$, и случайном и равновероятном выборе его начального состояния $s \in S$ его выходная последовательность $A(s, x_1, x_2, \ldots, x_L)$ имеет равномерное распределение на $|Y|^n$. В этом

случае для любого состояния $s`\in S$ мощности спектра автомата A с начальным состоянием s` при входном слове P имеет вид:

$$|S^k| = (|Y|-1)|Y|^{n-k-1},\ k\in\overline{0,n-1}$$

и $k_o = n-1$.

Для такого автомата найденные ранее значения и оценки вероятностей, а также среднее число ложных решений принимают вид:

1) для теоремы 3

$$P(s^* = s`) = P({}^{A}f_{s`,s`} > n-1);$$

2) для теоремы 4

$$P(s^* = s`) \geq 1-\sum_{k=1}^{n-1} (|Y|-1)|Y|^{n-k-1}P({}^{A}f_{s`,s`} \leq k);$$

3) для теоремы 5 при $c > n-1$

$$M_{s`}=|Y|^{n-c}P({}^{A}f_{s`,s`} < n),$$

при $c \leq n-1$

$$M_{s`} = |Y|^{n-c}P({}^{A}f_{s`,s`} < c) + P({}^{A}f_{s`,s`} \geq c)(|Y|^{n-c}-1).$$

Предположим теперь, что поставленная задача оценки параметра метода максимального правдоподобия решается для фиксированного автомата A, фиксированной последовательности $P = x_1, x_2, \ldots, x_L$, начальное искомое состояние s выбирается случайно, независимо и равновероятно из множества $S`\subseteq S$. Для формулировки соответствующих этому случаю утверждений введем вспомогательные обозначения.

Пусть слово $P=x_1,x_2,\ldots,x_L$ такое, что уравнение $A(s, P) = y_1, \ldots, y_L$ для каждого $(y_1, \ldots, y_L)\in Y^L$ имеет не более одного решения, относительно *неизвестного* $s\in S`$. Для $c\in\overline{1,L}$ обозначим через $æ_c(s`)$, $s`\in S`$ множество решений $s\in S`$ уравнения

$$A(s, x_1, x_2, \ldots, x_c) = A(s`, x_1, x_2, \ldots, x_c).$$

Обозначим через L(c) число различных множеств вида $æ_c(s`)$, а через $K^A_{\max}$ и $K^A_{\min}$ – максимум и, соответственно, минимум величины $k_0 = k_0(s`)$ по всем $s`\in S`$.

Теорема 6. Вероятность $P_{A,\,A^*}$ правильного решения задачи для автомата A при входной последовательности $P = x_1, x_2, \ldots, x_L$ такой, что $A(s, P) \neq A(s`, P)$ при любых $s, s`\in S`$, $s \neq s`$, оценивается следующим образом:

$$P({}^{A}f_{s`}^{s`} > K_{\max}^{A}) \le P_{A,A*} = P(s^{*}=s) \le P({}^{A}f_{s`}^{s`} > K_{\min}^{A}) + \frac{1}{|S`|}\sum_{c=1}^{K_{\max}^{A}} P({}^{A}f_{s`}^{s`} = c)L(c).$$

Доказательство. Используем утверждение теоремы 3. Имеем

$$P_{A,A*} = \frac{1}{|S`|}\sum_{s`\in S`} P(s^{*} = s`) = \frac{1}{|S`|}\sum_{s`\in S`} P({}^{A}f_{s`}^{s`} > k_{o}(s`)) +$$

$$+ \frac{1}{|S`|}\sum_{s`\in S`}\sum_{c=1}^{k_{O}(s`)} P({}^{A}f_{s`}^{s`} = c)\left(1 - \frac{|Y_{s`}^{c+1}|}{|O|-1}\right)\frac{1}{|æ_{C}(s`)|}.$$

Очевидно, что

$$0 \le \left(1 - \frac{|Y_{s`}^{c+1}|}{|O|-1}\right)\frac{1}{|æ_{C}(s`)|} \le. \frac{1}{|æ_{C}(s`)|}.$$

Поэтому

$$P({}^{A}f_{s`}^{s`} > K_{\max}^{A}) \le P_{A,A*} \le P({}^{A}f_{s`}^{s`} > K_{\min}^{A}) +$$

$$+ \frac{1}{|S`|}\sum_{s`\in S`}\sum_{c=1}^{K_{\max}^{A}} P({}^{A}f_{s`}^{s`} = c)\frac{1}{|æ_{C}(s`)|} == \frac{1}{|S`|}\sum_{c=1}^{K_{\max}^{A}} P({}^{A}f_{s`}^{s`} = c)L(c) +$$

$$+ P({}^{A}f_{s`}^{s`} > K_{\min}^{A}).$$

Теорема 6 полностью доказана.

Пусть χ_{1}^{c}, χ_{2}^{c}, …, $\chi_{L(c)}^{c}$ – семейство всех различных множеств вида $æ_{c}(s`)$, $s`\in S`$.

Теорема 7. Вероятность α отбраковки истинного решения и среднее число M_A ложных решений задачи, при применении порогового критерия с уровнем «c» в методе МП при случайном и равновероятном выборе начального состояния $s\in S`$, $S`\subseteq S$ для автомата A при входной последовательности $P=x_1,x_2,\ldots,x_L$ такой, что $A(s,P)\neq A(s`,P)$ при любых $s,s`\in S`$, $s\neq s`$ оценивается следующим образом

$$\alpha = P({}^{A}f_{s`}^{s`} < c),$$

$$M_A \le \frac{1}{|S`|}\sum_{k=1}^{K_{\max}^{A}} P({}^{A}f_{s`}^{s`} = k)\frac{1}{(|Y|-1)|Y|^{c-k-1}}((|S`| - L(k))^{2} + 2|S`| - L(k))$$

для $c > K_{\max}^{A}$ и

$$M_A \le \sum_{k=1}^{c-1}\frac{1}{|S`|}[P({}^{A}f_{s`}^{s`} = k)\frac{1}{(|Y|-1)|Y|^{c-k-1}}((|S`| - L(k))^{2} + 2|S`| - L(k)) +$$

$$+\frac{1}{|S`|}\,[\,P({}^{A}f_{s`}{}^{s`}\geq c)\,((|\,S_o\,|-\,L(c)\,)^2+|\,S_o\,|-L(c)]$$

при $c \leq K^{A}_{\max}$.

Доказательство. Используя теорему 5. Имеем для $c > K^{A}_{\max}$

$$M_A = \frac{1}{|S`|}\sum_{s`\in S`} Ms` \leq \frac{1}{|S`|}\sum_{s`\in S`}\sum_{k=1}^{K^{A}_{\max}} æ_к(s`)\,P({}^{A}f_{s`}{}^{s`}=k)\frac{1}{(|Y|-1)|Y|^{c-k-1}} =$$

$$= \sum_{k=1}^{K^{A}_{\max}} P({}^{A}f_{s`}{}^{s`}=k)\,\frac{1}{(|Y|-1)|Y|^{c-k-1}}\,\frac{1}{|S`|}\sum_{j=1}^{L(k)} |æ_j^k|^2 \leq$$

$$\leq \frac{1}{|S`|}\sum_{k=1}^{K^{A}_{\max}} P({}^{A}f_{s`}{}^{s`}=k)\,\frac{1}{(|Y|-1)|Y|^{c-k-1}}\,((|\,S`\,|-L(k)\,)^2+2|\,S`\,|-L(k)\,).$$

Для $c \leq K^{A}_{\max}$ получаем

$$M_A \leq \frac{1}{|S`|}\,P({}^{A}f_{s`}{}^{s`}\geq c)\sum_{s`\in S`}(|æ_c(s`)|-1)+$$

$$+\frac{1}{|S`|}\sum_{k=1}^{c-1} P({}^{A}f_{s`}{}^{s`}=k)\,\frac{1}{(|Y|-1)|Y|^{c-k-1}}\,((|\,S`\,|-\,L(k)\,)^2+2|\,S`\,|-\,L(k))\leq$$

$$\leq \frac{1}{|S`|}\,P({}^{A}f_{s`}{}^{s`}\geq c)((|\,S`\,|-\,L(c)\,)^2+2|\,S`\,|-\,L(c)-|S`|)+$$

$$+\frac{1}{|S`|}\sum_{k=1}^{c-1} P({}^{A}f_{s`}{}^{s`}=к)\,\frac{1}{(|Y|-1)|_Y|^{c-k-1}}\,((|\,S`\,|-\,L(k)\,)^2+2|\,S`\,|-\,L(k))\,.$$

10.3. Использование статистического аналога конечного автомата, построенного с помощью искажений его частичных функций переходов и выходов

В данном разделе рассматривается прежняя задача, заключающаяся в решении уравнения $A`(s`, P) = y_1`, \ldots, y_L`$, относительно неизвестного $s`\in S`$, $S`\subseteq S$ для автомата $A` = (X, S, Y, (h_x`)_{x\in X}, (f_x`)_{x\in X})$ при входном слове $P = x_1, x_2, \ldots, x_L$. В отличие от утверждений пункта 1 будем считать, что для автомата A` с помощью искажений как функций переходов, так и выходов автомата A` найден его статический аналог – автомат $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$, для которого задача определения его начального состояния по входной и выходной последовательностям решается с малой трудоемкостью. Со-

гласно ранее приведенной общей схеме решения поставленной задачи введем вероятностную модель получения последовательности $y_1`, \ldots, y_L`$ из последовательности $A(s`, P) = y_1, \ldots, y_L$. Положим для $x \in X$

$$p_x^s = p(h_x s \neq h_x`s) = \frac{\left|\{s \in S : h_x s \neq h_x s`\}\right|}{|S|},$$

$$p_x^o = p(f_x s \neq f_x`s) = \frac{\left|\{s \in S : f_x s \neq f_x's\}\right|}{|S|},$$

$$q_x^s = 1 - p_x^s,\ q_x^o = 1 - p_x^o.$$

Аналогично определению автомата A* построим вероятностный автомат $A^{**} = (X, S \cup t, Y, (h_x^*)_{x \in X}, (f_x^*)_{x \in X})$, положив для $x \in X$

$$P(\delta_x^* s = s`) = \begin{cases} q_x^s, & \text{если } s' = h_x s, \\ p_x^s, & \text{если } s' = t, \end{cases}$$

$$P(h_x^* t = t) = 1,$$

$$P(f_x^* s = y') = \begin{cases} q_x^o, & \text{если } y = f_x s, \\ \dfrac{p_x^o}{|Y| - 1}, & \text{в противном случае,} \end{cases}$$

$$P(f_x^* t = y) = \frac{1}{|Y|},\ y \in Y.$$

Мы рассматриваем следующую математическую задачу: по известному наблюдению $y_1`, \ldots, y_L`$ выходной последовательности $A^{**}(s`, P)$ вероятностного автомата A** и его входному слову P определить состояние s`. Ниже будут использованы две статистические процедуры определения состояния s`. Первая статистическая процедура естественным образом связана с практическим алгоритмом определения ложных решений уравнения $A`(s`, P) = y_1`, \ldots, y_L`$ с помощью вспомогательного автомата A. Выбираются параметры $c \in \overline{1, L}$, $m \in \overline{0, c-1}$. Рассматривается величина

$$\rho(A(s, x_1, x_2, \ldots, x_c), y_1`, \ldots, y_c`),$$

где $\rho(A(s, x_1, x_2, \ldots, x_c); y_1`, \ldots, y_c`)$ – расстояние Хэмминга между словами $A(s, x_1, x_2, \ldots, x_c)$; $y_1`, \ldots, y_c`$. Если

$$\rho(A(s, x_1, x_2, \ldots, x_c), y_1`, \ldots, y_c`) > m,$$

то состояние $s \in S`$ отбраковывается.

Вторая статистическая процедура отражает следующую идею практического решения уравнения $A`(s`, P) = y_1`, \ldots, y_L`$ относительно $s` \in S`$ с помощью вспомогательного автомата A. Предпола-

гается, что последовательность y_1`, …, $y_L$` получена из неизвестной нам выходной последовательности A(s`, P) автомата A с того же неизвестного состояния s`. На основе вероятностей p_x^s и p_x^o, $x \in X$ в предположении, что автомат A` выбирался случайно и равновероятно среди всех автоматов с параметрами X, S, Y с фиксированной «близостью к автомату A» (параметры $p_x^s$, $p_x^o$, $x \in X$) ищется наиболее «вероятная» выходная последовательность $y_1$, …, $y_L$ автомата A полученная с s` при входной последовательности P. Затем с использованием уравнения A(s`, P) = $y_1$, …, $y_L$ ищется искомое состояние s`. В разделах 4, 5 вводятся математические модели получения последовательности y_1, …, y_L и в рамках этих моделей подсчитываются параметры эффективности предлагаемых статистических процедур. Отметим, что для второго способа определения s` мы в разделе 5 акцентируем внимание лишь на этап восстановления выходной последовательности $y_1$, …, $y_L$ автомата A по известной выходной последовательности A`(s`, P) = $y_1$`, …, y_L` автомата A`.

10.4. Пороговый критерий с уровнем (m, c)

Пусть $c \in \overline{1,L}$, $m \in \overline{0,c-1}$. Данный критерий состоит в том, что состояние $s \in S$` отбраковывается, если

$$\rho(A(s, x_1, x_2, \ldots, x_c), y_1`, \ldots, y_c`) > m,$$

где $\rho(A(s, x_1, x_2, \ldots, x_c); y_1`, \ldots, y_c`)$ – расстояние Хэмминга между словами $A(s, x_1, x_2, \ldots, x_c)$; $y_1`, \ldots, y_c`$.

С использованием результатов пункта 1 несложно доказывается следующее утверждение.

Утверждение 1. Пусть $p_x^o = p$; $q = 1-p$, $x \in X$. Вероятность $1-\alpha_{c,m}$ неотбраковки истинного состояния s` оценивается следующим образом:

$$1-\alpha_{c,m} = \sum_{j=1}^{c} P(\rho(A^{**}(s`)_c, A(s`)_c) \le m / \nu_{S`} = j) P(\nu_{S`} = j).$$

Использованы обозначения:

– $\rho(A^{**}(s`)_c, A(s`)_c)$ – расстояние Хэмминга между начальными словами $A^{**}(s`)_c$, $A(s`)_c$ длины c выходных последовательностей $A^{**}(s`, P)$ и $A(s`, P)$ автоматов A**, A при входном слове P = x_1, x_2, …, x_L;

– $P(\nu_{s`} = j) = q_{x_1}^s \cdots q_{x_{j-1}}^s p_{x_j}^s$, $j \in \overline{0,c-1}$;

– $P(\nu_{s`} = c) = q^s_{x_1} \dots q^s_{x_{c-1}}$;

– $P(\rho(A^{**}(s`), A(s`)_c) \le m / \nu_{S`} = c) = q^c + C^1_c p\, q^{c-1} + \dots + C^m_c p^m q^{c-m}$;

– $P(\rho(A^{**}(s`), A(s`)_c) \le m / \nu_{s_o} = j) =$

$$= \sum_{\substack{\kappa_1+\kappa_2 \le m \\ \kappa_1 \le j \\ \kappa_2 \le c-j}} C_j^{\kappa_1} \; p^{\kappa_1} \; q^{j-\kappa_1} \; + C_{c-j}^{\kappa_2} \; \left(1-\frac{1}{|Y|}\right)^{\kappa_2} \; \left(\frac{1}{|Y|}\right)^{c-j-\kappa_2} ;$$

где $j \in \overline{0, c-1}$.

Пусть Φ_2 – класс автоматов параметрами X,S,Y, обладающие свойством: для любого фиксированного состояния $s \in S`$, $S` \subseteq S$ при случайном и равновероятном выборе автомата A` из Φ_2

$$P(A`(s, x_1, x_2, \dots, x_c) = y_1, y_2, \dots, y_c) = \frac{1}{|Y|^c}$$

для любого $(y_1, y_2, \dots, y_c) \in Y^c$.

Пусть $p_x^o = p$; $q = 1-p$, $x \in X$ и автомат A случайно и равновероятно выбирается из класса Φ_2 .Тогда среднее число $M^{c,m}$ ложных вариантов, прошедших через критерий с уровнем (c, m), оценивается следующим образом

$$M_{c,m} \le |S`| \left(\frac{1}{|Y|^c} (1 + (|Y|-1) C^1_c + (|Y|-1)^2 C^2_c + \dots + (|Y|-1)^m C^m_c\right).$$

10.5. Метод максимального правдоподобия

Ниже изучается одна из моделей получения выходной последовательности случайно и равновероятно выбранного автомата оригинала A` для заданной модели – статистического аналога A с параметрами близости $p_x^s$ , $p_x^o$ при входном слове P и начальном состоянии $s` \in S`$.

Рассмотрим теперь следующую ситуацию. Пусть $A` = (X, S, Y, (h_x`)_{x \in X}, (f_x`)_{x \in X})$ – исследуемый автомат и его статистическим аналогом является автомат $A = (X, S, Y, (\delta_x)_{x \in X}, (\beta_x)_{x \in X})$, для которого при случайном и равновероятном выборе $s \in S$ вероятность события $h_x s \ne h_x`s$ равна p_x , $x \in X$, а вероятность события $f_x s \ne f_x`s$ не зависит от $x \in X$ и равна p_o .

Введем следующую вероятностную модель. Положим

$$1 - p_x = q_x,\ x \in X,\ 1 - p_o = q_o,\ P = x_1, x_2, \ldots, x_L,$$

$$p(1) = p_{x_1}$$

$$p(2) = q_{x_1}\ p_{x_2}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$p(L-1) = q_{x_1}\ \ldots q_{x_{L-2}}\ p_{x_{L-1}}$$

$$p(L) = q_{x_1}\ q_{x_2}\ \ldots q_{x_{L-1}}\ .$$

Рассмотрим следующие матрицы переходных вероятностей a_1, a_2, a_3:

$$a_1 = \|P(y`, j/y)\|,\ y, y` \in Y^L,\ j \in \overline{1,L},$$

где $P(y, j/y) = P(j)$, $j \in \overline{1,L}$, $y \in Y^L$, а остальные элементы равны нулю;

$$a_2 = \|P(\text{ŷ}/y, j)\|,\ \text{ŷ} \in Y^L,\ y \in Y^L,\ j \in \overline{1,L},$$

где

$$P(y_1, \ldots, y_j, \text{ŷ}_{j+1}, \ldots, \text{ŷ}_L / y_1, \ldots, y_L, j) = \frac{1}{|O|^{L-j}},$$

для $j \in \overline{1,L}$, и любого слова $\text{ŷ}_{j+1}, \ldots, \text{ŷ}_L \in Y^{L-J}$, остальные элементы равны нулю;

$$a_3 = \|P^{a3}(\text{ŷ}/y)\|,\ \text{ŷ} \in Y^L,\ y \in Y^L,$$

где

$$P^{a3}(\text{ŷ}_1, \ldots, \text{ŷ}_L / y_1, \ldots, y_L) = \prod_{j=1}^{L} J(\text{ŷ}_j / y_j),\ \text{ŷ} \in Y,\ y \in Y,\ J \in \overline{1,L},$$

при этом

$$P(\text{ŷ}_i / y_j) = \begin{cases} q_O + p_O \frac{1}{|Y|}, & \text{если } \text{ŷ}_j = y_j, \\ p_O \frac{1}{|Y|}, & \text{если } \text{ŷ}_j \neq y_j. \end{cases}$$

Предположим, что для автомата-модели A его автомат-оригинал A` выбирается случайно и равновероятно из множества всех автоматов (с алфавитами X, S, Y), каждый из которых имеет введенную ранее «меру различия с автоматом A» – вероятности $p_x$, $x \in X$, $p_o$. Пусть $P = x_1, x_2, \ldots, x_L$ – входная последовательность автомата A` и $s` \in S`$, $S` \subseteq S$. В качестве модели получения последовательности $A`(s`, P) = \text{ŷ}_1, \text{ŷ}_2, \ldots, \text{ŷ}_L$ при заданной последовательности $A(s`, P) = y_1, y_2, \ldots, y_L$ будем рассматривать дискретный канал без памяти с переходными вероятностями, заданными матрицей $a = a_1 a_2 a_3 = \|P^a(\text{ŷ}/y)\|$, $\text{ŷ} \in Y^L$, $y \in Y^L$. (Использована терминология книги

[22].) Задача определения состояния s`, при котором A(s`, P) = $y_1, y_2, \ldots, y_L$, по выходной последовательности $\tilde{y}_1, \tilde{y}_2, \ldots, \tilde{y}_L$, при указанном способе выбора автомата A`, в принятой модели, адекватна задаче декодирования принятого сообщения $\tilde{y}_1, \tilde{y}_2, \ldots, \tilde{y}_L$. (Здесь подразумевается нахождение последовательности A(s`, P) = $y_1, y_2, \ldots, y_L$ и последующего определения s`. Напомним, что нами принято дополнительное предположение, состоящее в том, что трудоемкость определения s` из уравнения A(s`, P) = $y_1, y_2, \ldots, y_L$ невелика.)

В условиях теоремы 5.6.1[1], при равномерном распределении на входных последовательностях канала, средняя ошибка $p^a_{ош,s`}$ декодирования по методу максимального правдоподобия при любом ρ, 0≤ρ≤1, ограничена неравенством

$$p^a_{ош,s`} \le (|S`|-1)^{\rho} \sum_{\tilde{y} \in Y^L} \left[\sum_{y \in Y^L} \frac{1}{|Y|^L} \left(p^a(\tilde{y}/y) \right)^{\frac{1}{1+\rho}} \right]^{1+\rho}.$$

При больших значениях L, |Y| подсчет данной оценки затрудняется, так как необходимо подсчитать значение $|Y|^{2L}$ слагаемых, не считая трудоемкости получения значений $p^a(\tilde{y}/y)$, через значения элементов матриц a_1, a_2, a_3. Поэтому представляет интерес получение *более простых выражений для оценки вероятности* $p^a_{ош,s`}$. С этой целью определим следующую вспомогательною конструкцию.

Рассмотрим семейство дискретных каналов без памяти с переходными вероятностями $p_{\varepsilon_1,\ldots,\varepsilon_L}(\tilde{y}/y)$, $\tilde{y} \in Y^L$, $y \in Y^L$, заданными матрицами

$$a_{\varepsilon_1,\ldots,\varepsilon_L} = \| p_{\varepsilon_1,\ldots,\varepsilon_L}(\tilde{y}/y) \|, \ \tilde{y} \in Y^L, y \in Y^L, (\varepsilon_1, \ldots, \varepsilon_L) \in F_2^L.$$

Здесь – F_2^L – множество всех двоичных наборов длины L;

$$p_{\varepsilon_1,\ldots,\varepsilon_L}(\tilde{y}_1, \ldots, \tilde{y}_L / y_1, \ldots, y_L) = \prod_{j=1}^{L} p_{\varepsilon_j}(\tilde{y}_j / y_j), \ \tilde{y} \in Y, y \in Y, j \in \overline{1,L},$$

где при $\varepsilon_j = 0$

$$p_o(\tilde{y}_j / y_j) = \begin{cases} 1, \text{если } \tilde{y}_j = y_j, \\ 0, \text{если } \tilde{y}_j \ne y_j, \end{cases}$$

[1] См. : там же.

а при $\varepsilon_j = 1$

$$p_1(\tilde{y}_j / y_j) = \frac{1}{|Y|}, \quad \tilde{y}_j \in Y, \; y_j \in Y, \; j \in \overline{1,L}.$$

На множестве F_2^L зададим вероятностную меру

$$P(\varepsilon_1, \ldots, \varepsilon_L) = \sum_{k=1}^{L} p(k)\, P(\varepsilon_1, \ldots, \varepsilon_L/k),$$

где

$$P(\varepsilon_1, \ldots, \varepsilon_L/k) = \begin{cases} P_{\varepsilon 1} P_{\varepsilon 2} \ldots P_{\varepsilon k}, \text{при } \varepsilon_{\kappa+1} = \varepsilon_{\kappa+2} = \ldots = \varepsilon_L, \\ O, \text{ в противном случае,} \end{cases}$$

$$P_{\varepsilon j} = \begin{cases} q_O, \text{если } \varepsilon_i = 0, \\ p_O, \text{если } \varepsilon_i = 1, \end{cases} \quad j \in \overline{1,L}.$$

Необходимый нам дискретный канал без памяти определим переходными вероятностями $\rho(\tilde{y}/y)$, $\tilde{y} \in Y^L$, $y \in Y^L$, заданными с помощью матрицы переходных вероятностей

$$\sum_{((\varepsilon_1,\ldots,\varepsilon_L) \in F_2^L)} P(\varepsilon_1, \ldots, \varepsilon_L)\, a_{\varepsilon_1,\ldots,\varepsilon_L}.$$

Из качественного анализа построенной ранее матрицы $a = a_1 a_2 a_3$ вытекает, что

$$a = \sum_{(\varepsilon_1,\ldots,\varepsilon_L) \in F_2^L} P(\varepsilon_1, \ldots, \varepsilon_L)\, a_{\varepsilon_1,\ldots,\varepsilon_L}.$$

Впрочем, это можно доказать и формально, используя следующую схему рассуждений.

Предварительно введем обозначения.

Для $y = (y_1, y_2, \ldots, y_L) \in Y^L$, $\tilde{y} = (\tilde{y}_1, \tilde{y}_2, \ldots, \tilde{y}_L) \in Y^L$ через $[\tilde{y} \times y]$ обозначим множество индексов $j \in \overline{1,L}$, при которых $y_j \neq \tilde{y}_j$.

Для $(\gamma_1, \ldots, \gamma_L) \in F_2^L$ обозначим через $[\gamma_1, \ldots, \gamma_L]$ множество индексов $j \in \overline{1,L}$, для которых $\gamma_j = 1$.

Тогда для $\tilde{y} \in Y^L$, $y \in Y^L$ таких, что мощность $|[\tilde{y} \times y]|$ множества $[\tilde{y} \times y]$ равна k, имеем

$$pa_3 \quad (\text{ŷ}/y)=(p_o \frac{1}{|Y|})^{к} \ (q_o + p_o \frac{1}{|Y|})^{L-k}.$$

Введем вспомогательные матрицы a^1_3 , a^2_3 переходных вероятностей, положив

$$a^1_3 = \|P(y; \gamma_1,\ldots, \gamma_L /y)\| \quad y\in Y^L, (\gamma_1,\ldots, \gamma_L) \in F_2^L,$$

где

$$P(y; \gamma_1,\ldots, \gamma_L /y)= \prod_{j=1}^{L} (\gamma_j p_o + \bar{\gamma}_j q_o)=P(\gamma), \ \gamma =\gamma_1,\ldots, \gamma_L, \ \bar{\gamma}_j ==\gamma_J \oplus 1$$

и $P(y`; \gamma_1,\ldots, \gamma_L /y)=0$, для $y`\neq y$;

$$a^2_3 = \|P(\text{ŷ}/y; \gamma_1,\ldots, \gamma_L)\| \quad y\in Y^L, \ \text{ŷ} \in Y^L, (\gamma_1,\ldots, \gamma_L) \in F_2^L,$$

где

$$P(\text{ŷ}/y; \gamma_1,\ldots, \gamma_L) = \begin{cases} (\frac{1}{|Y|})^{\|[\gamma_1,\ldots,\gamma_L]\|}, & \text{если } [\text{ŷ} \propto y] \subseteq [\gamma_1,\ldots,\gamma_L], \\ O, & \text{в противном случае.} \end{cases}$$

Непосредственная проверка показывает, что $a_3 = a^1_3 \, a^2_3$.

Таким образом,

$$a = a_1 \, a_2 \, a^1_3 \, a^2_3 .$$

Не ограничивая общности рассуждений, для наглядности положим L = 4 и пронумеруем все двоичные наборы $(\gamma_1, \ldots, \gamma_L) \in F_2^L$, положив

$$F_2^L = \bigcup_{j\in 1,2^L} \gamma(j) .$$

Матрицы a_1, a_2, a^1_3, a^2_3 имеют вид:

$a_1 =$

p(1) O p(1)	p(2) O p(2)	p(3) O p(3)	p(4) O p(4)

a_2

$\|$

α_1
α_2
α_3
α_4

$a^1{}_3$

$\|$

$p(\gamma(1))$ O $p(\gamma(1))$	$p(\gamma(2))$ O $p(\gamma(2))$	$p(\gamma(3))$ O $p(\gamma(3))$	....	$p(\gamma(16))$ O $p(\gamma(16))$

$a^2{}_3$

$\|$

$B_{\gamma(1)}$
$B_{\gamma(2)}$
$B_{\gamma(3)}$
. . . . .
$B_{\gamma(16)}$

Перемножая указанные матрицы, в введенных обозначениях имеем для L = 4:

$$a = \sum_{j=1}^{16} p(\gamma(j)) \left(\sum_{k=1}^{4} p(k)\alpha_k \right) B_{\gamma(j)},$$

а в общем случае получаем

$$a = \sum_{\gamma \in F_2^L} \sum_{j=\overline{1,L}} p(\gamma)p(j)\, B_\gamma .$$

Рассмотрим следующее вспомогательное отображение φ: $F_2^L \times \overline{1,L} \to F_2^L$

$$\varphi(\gamma_1, \ldots, \gamma_L, к) = \gamma_1, \ldots, \gamma_к, 1, 1, \ldots, 1.$$

Непосредственно проверяется, что

$$\alpha_к\, B_{\gamma_1,\ldots,\gamma_L} = a_{\gamma_1,\ldots,\gamma_k,1,1,\ldots,1} \;;$$

$$\sum_{(\gamma,k)\in\phi^{-1}(\varepsilon_1,\ldots,\varepsilon_L)} p(\gamma)p(k) = P(\varepsilon_1, \ldots, \varepsilon_L).$$

Таким образом,

$$a = \sum_{(\varepsilon_1,\ldots,\varepsilon_L)\in F_2^L} P(\varepsilon_1, \ldots, \varepsilon_L)\; a_{\varepsilon_1,\ldots,\varepsilon_L} \;.$$

Перейдем теперь к рассмотрению возможностей *упрощения вида приведенной ранее оценки параметра* $p^{a}_{ош,s`}$. С учетом нового выражения для матрицы *a* имеем:

$$p^{a}(\theta/y))$$

$$p^{a}(|S`|-1)^{\rho} \sum_{\theta\in Y^L} \left[ \sum_{y\in Y^L} \frac{1}{|Y|^L} \left(p^{a}(\theta/y)\right)^{\frac{1}{1+\rho}} \right]^{1+\rho} = (|S`|-1)^{\rho} \left(\frac{1}{|Y|^L}\right)^{1+\rho}$$

$$\bullet\bullet \sum_{\theta\in Y^L} \left[\sum_{y\in Y^L} \left(\sum_{(\varepsilon_1,\ldots,\varepsilon_L)\in F_2^L} P(\varepsilon_1,\ldots,\varepsilon_L)\, P\varepsilon_1,\ldots,\varepsilon_L(\theta/y)^{\frac{1}{1+\rho}} \right]^{1+\rho} =$$

$$= (|S`|-1)^{\rho} \left(\frac{1}{|Y|^L}\right)^{1+\rho} \bullet$$

$$\sum_{\theta\in Y^L} \left[\sum_{y\in Y^L} \left(\sum_{\substack{(\varepsilon_1,\ldots,\varepsilon_L):\\ [\varepsilon_1,\ldots,\varepsilon_L]\supseteq[\theta\cap y]}} P(\varepsilon_1,\ldots,\varepsilon_L) \frac{1}{|Y|^{|[\varepsilon_1,\ldots,\varepsilon_L]|}} \right)^{\frac{1}{1+p}} \right]^{1+\rho}.$$

Выражение в квадратных скобках не зависит от значения $\mathcal{Y} \in Y^L$. Поэтому, фиксируя один элемент $\mathcal{Y}_0 \in Y^L$, последнюю формулу можно записать в виде

$$(|S`|-1)^{\rho}\left(\frac{1}{|Y|^{L}}\right)^{1+\rho} |Y|^{L} \left[\sum_{y \in Y^L} \left(P^a\left(\mathcal{Y}_0 / y\right)\right)^{\frac{1}{1+\rho}} \right]^{1+\rho},$$

где

$$P^a\left(\mathcal{Y}_0 / y\right) = \sum_{\substack{(\varepsilon_1,\ldots,\varepsilon_L): \\ [\varepsilon_1,\ldots,\varepsilon_L] \supseteq [\mathcal{Y}_0 \times y]}} P_{(\varepsilon_1,\ldots,\varepsilon_L)} \frac{1}{|Y|^{|[\varepsilon_1,\ldots,\varepsilon_L]|}} .$$

Данная вероятность есть функция от множества $[\mathcal{Y}_0 \times y]$ (индексов различия $\mathcal{Y}_0 \in O^L$, $y \in Y^L$). В связи с чем для $[\mathcal{Y}_0 \times y] = \{ j_1, \ldots, j_k\}$ положим

$$P^a\left(\mathcal{Y}_0 / y\right) = p\left(\{ j_1, \ldots, j_k\}\right).$$

В этих обозначениях полученное выражение оценки параметра $p^a_{ош,s`}$ принимает вид

$$(|S`|-1)^{\rho} \frac{1}{|Y|^{L\rho}} \left[\sum_{\{j_1,\ldots,j_k\}} (|Y|-1)^{k} \left(P\left(\{j_1,\ldots,j_k\}\right)\right)^{\frac{1}{1+\rho}} \right]^{1+\rho},$$

$$0 \le \rho \le 1,$$

где сумма берется по все подмножествам $\{ j_1, \ldots, j_k\}$ множества $\overline{1,L}$.

Заметим, что из полученного выше вида матрицы a и того факта, что в рассматриваемых условиях декодирование по максимуму правдоподобия минимизирует вероятность ошибки (Р. Галлагер, [22. – С. 137]) непосредственно следует, что

$$p^a_{ош,s`} \le 1 - P(0, 0, \ldots, 0) = 1 - (q_{x_1} q_{x_2} \ldots q_{x_{L-1}}) q_0^L .$$

Последнее выражение дает неплохую оценку параметра $p^a_{ош,s`}$, при достаточно больших значениях вероятностей q_x, $x \in X$; q_0. При этом значении $1 - P(0, 0, \ldots, 0)$ является оценкой сверху ошибки декодирования, осуществляемого по правилу: принятая из канала последовательность $\mathcal{Y}$ декодируется в $\mathcal{Y}$.

Заметим, что рассмотренные оценки приведенных в пункте 4 параметров в частном случае $p_x = 0$, $x \in X$ могут быть непосредственно получены из работ Г. В. Балакина, например, из [20].

Глава 11. ПРИБЛИЖЕННЫЕ МОДЕЛИ АВТОМАТОВ, ПОСТРОЕННЫЕ НА ОСНОВЕ РАССТОЯНИЯ ХЭММИНГА МЕЖДУ ИХ ВЫХОДНЫМИ ПОСЛЕДОВАТЕЛЬНОСТЯМИ

11.1. Введение

В криптографической теории и практике широкое распространение получили методы анализа шифра на основе его приближенных моделей. Так, в простейшем случае для определения ключа $\chi \in K$, из уравнения шифрования $f(x, \chi) = y$, где x – известный открытый текст, y – шифрованный текст, уравнение преобразуют к виду $\varphi(\chi) = y$ и, в случае когда φ – функция, заданная на векторном пространстве, пытаются подобрать ее линейный аналог. Линейный аналог это «...линейная функция, значения которой для достаточно большого числа наборов аргументов совпадают со значениями данной функции шифрования» [1].

В других, более сложных ситуациях уравнение шифрования, представляют некоторой системой C(A) уравнений, полученной с помощью отображений множеств некой алгебры A. Для получения решения уравнения $f(x, \chi) = y$ строят новую алгебру A`, являющуюся $\pi$-гомоморфным образом алгебры A (см. работы Ю. Н. Горчинского) и решают соответствующую систему C`(A`) уравнений в алгебре A`. Найденные решения системы C`(A`) используют как дополнительную информацию для решения начальной задачи.

В частном случае использования конечных автоматов как алгебр, для решения поставленной выше задачи, возникают свои специфические трудности, связанные с учетом закона функционирования автоматов. В связи с этим известные криптографические приложения таких моделей алгебр как π-гомоморфные образы алгебр, гомоморфные и π-гомоморфные образы стохастических алгебр в частном случае автоматов требуют своего уточнения и развития. Ниже акцентируется внимание на одном центральном вопросе анализа шифрующих автоматов – построения их приближенных моделей.

11.2. Основные понятия и предварительные результаты

Пусть A = (X, S, Y, h, f) – конечный автомат с входным алфавитом X, множеством состояний S, выходным алфавитом Y, ча-

стичными функциями переходов $(h_x)_{x\in X}$, $h_X : S\to S$, $x\in X$ и частичными функциями выходов $(f_x)_{x\in X}$, $f_x : S\to Y$, $x\in X$. Для $\chi\subseteq S$, $\mathfrak{I} = x(1), \ldots, x(k)$ из X^k, $s\in S$ положим, что

$h_x\chi = \{h_x s : s\in\chi\}$, $h_{\mathfrak{I}}s = h_{x(k)}\ldots h_{x(1)}s$, $f_{\mathfrak{I}} = f_{x(k)}h_{x(k-1)}\ldots h_{x(1)}s$, $h_\varnothing s=s$ для пустого слова $\varnothing$.

Через $A_M = (X, S, h)$ обозначим автомат без выходов, соответствующий автомату A, а через $A\langle s\rangle = (X, S_s, У, h, f)$ – подавтомат автомата A, порожденный состоянием $s\in S$. Здесь для ограничений функций $(h_x)_{x\in X}$, $(f_x)_{x\in X}$ на

$$S_S = \{h_{\mathfrak{I}}s: \mathfrak{I}\in X^*\}$$

для простоты обозначений использованы те же символы.

Класс инициальных автоматов с входным алфавитом X и выходным алфавитом Y обозначим через $F = F(X, Y)$. Инициальный автомат A'_s из F мы рассматриваем как ограниченно детерминированную функцию (О.Д. – функцию $A'_s : X^*\to Y^*$ [32].

Автомат $A'[s] = (X, S'_s, Y, (h'), (f'))$ – как конечный автомат с минимальным числом состояний, реализующий эту функцию. Число $|S'|$ (вес О.Д.-функции) будем называть числом состояний инициального автомата A'_s.

Для состояния $s\in S$ автомата A мы полагаем, что $A[s] = A\langle s\rangle$ в случае приведенности автомата $A\langle s\rangle$. Будем говорить, что инициальный автомат A_s обладает некоторым свойством, если этим свойством обладает автомат A[s]. Так, например, инициальный автомат A_s – перестановочный, если автомат A[s] – перестановочный.

Для произвольного множества элементов χ обозначим через $E(\chi)$ тождественное отображение χ в χ. Наряду с автоматом $A = (X, S, Y, h, f)$ рассмотрим еще один произвольный автомат $A' = (X, S', Y, h', f')$ с теми же входным и выходным алфавитами. Гомоморфизм автомата A в A` вида $(E(X), \varphi, E(Y))$, $\varphi: S\to S`$ будем называть гомоморфизмом по состояниям A в A'. Конгруэнцию автомата A вида $(R_{E(X)}, R_S, R_{E(Y)})$, где $R_{E(X)}$, $R_{E(Y)}$ – одноэлементные разбиения множеств X, Y соответственно будем называть конгруэнцией по состояниям автомата A. Таким образом, конгруэнция по состояниям автомата A – это разбиение $R_S = (S_1, \ldots, S_k)$ множества S (бинарное отношение эквивалентности на S) со свойством подстановки (для любых j и $x\in X$ существует k, при котором $h_x(S_j)\subset S_k$)

Пусть $P_X = (p(x))_{x\in X}$ – некоторое вероятностное распределение на X. Для инициальных автоматов A_s , A'_s, $s\in S$, $s'\in S'$ (состояний s, s′ автоматов A, A′) определим величину

$$\mu_N^{s,s'} = \mu_N(A_s, A_{s'}) = 1/N \sum_{\bar{x}\in X^N} p(\bar{x})\rho_N(A(s,\bar{x}), A'(s',\bar{x})),$$

где для $\bar{x} = x_1, \ldots, x_N$ положено: $p(\bar{x}) = p(x_1) \ldots p(x_N)$; $\rho_N(A(s,\bar{x}), A'(s',\bar{x}))$ – расстояние Хемминга между выходными последовательностями $A(s,\bar{x})$, $A'(s',\bar{x})$ автоматов A, A′, полученных при начальных состояниях $s\in S$, $s'\in S$ и входной последовательности $\bar{x}\in X^N$.

Качественный смысл введенной величины состоит в том, что она характеризует среднее значение числа несовпадений соответствующих элементов выходных последовательностей автоматов A_s, $A'_{s'}$, в частности, при равномерном вероятностном распределении на X, данную величину можно трактовать как плотность несовпадения их выходных последовательностей.

Основная задача, решаемая в данном параграфе, состоит в разработке методов группирования состояний конечного перестановочного автомата A и построении его приближенной модели (автомата с меньшим числом состояний) на основе предельного поведения величин $(\mu_N^{s,s'})_{(s,s')\in S\times S'}$ при $N\to\infty$ и равномерном вероятностном распределении P_X.

Положим

$$\bar{\mu}_N = (\mu_N^{s,s'})_{(s,s')\in S\times S'}.$$

Изучим поведение вектора $\bar{\mu}_N$ при $N\to\infty$. Пусть $r^{(s,s',j)}$ – вероятность события $f_{\mathfrak{I}}s = f'_{\mathfrak{I}}s'$ при случайном выборе $\mathfrak{I}$ из X^j. Несложно доказывается следующее

Утверждение 1. Для введенных параметров справедливо равенство

$$\mu_N^{s,s'} = 1/N \sum_{j=1}^{N} r^{(s,s',j)}.$$

Для формулировки и доказательства основных результатов работы ведем дополнительные обозначения.

Пусть ^1A, ^2A – вероятностные автоматы Мили

$$^cA = (X, {}^cS, Y, {}^ch^v, {}^cf^v, P_X),\ c\in\overline{1,2},$$

где ${}^{c}h^{v} = ({}^{c}h_{x}^{v})_{x\in X}$ – семейство матриц вероятностей перехода. Элемент матрицы ${}^{c}h_{x}^{v}$ с номером $({}^{c}s_1, {}^{c}s_2)$ есть вероятность перехода состояния ${}^{c}s_1$ в ${}^{c}s_2$ при входном символе $x\in X$ автомата ${}^{c}A$.

${}^{c}f^{v} = ({}^{c}f_{x}^{v})_{x\in X}$ – семейство матриц вероятностей выхода. Элемент матрицы ${}^{c}f_{x}^{v}$ с номером $({}^{c}s, y)$ есть вероятность получения выходного символа $y \in Y$ с состояния ${}^{c}s$ в автомате ${}^{c}A$ при входном символе $x\in X$, $c\in \overline{1,2}$. $P_X = (p_x)_{x\in X}$ – распределение вероятностей на входном алфавите автомата ${}^{c}A$. Указанные распределения и вводимые ниже распределения мы рассматриваем как стохастические вектора.

Определим вспомогательный вероятностный автомат

$$B = B\,({}^{1}A, {}^{2}A) = (X, {}^{1}S\times{}^{2}S, Y\times Y, h^{B}, f^{B}, P_X)$$

как параллельное соединение автоматов ${}^{1}A$, ${}^{2}A$ при едином входе. Здесь $h^{B} = (h_x^{B})_{x\in X}$, h_x^{B} – матрица переходных вероятностей автомата B при входном символе $x\in X$. Она представима в виде тензорного произведения матриц ${}^{1}h_x^{v}$, ${}^{2}h_x^{v}$: $h_x^{B} = {}^{1}h_x^{v}\times{}^{2}h_x^{v}$, аналогично, $f^{B} = (f_x^{B})_{x\in X}$, $f_x^{B} = {}^{1}f_x^{v}\,x\,{}^{2}f_x^{v}$.

Положим $S_B = {}^{1}S\times{}^{2}S$, при этом

$$U = U\,({}^{1}A \cdot {}^{2}A) = \sum_{x\in X} p(x)\,h_x^{B}.$$

Матрица U определяет вероятности перехода одних состояний автомата B в другие при подаче на вход автомата B случайного входного символа с распределением P_X. Пусть $r^{s,\,j}$ – вероятность несовпадения выходных символов автоматов ${}^{1}A$, ${}^{2}A$ на j-м такте работы автомата B при начальном состоянии $s\in S = S_B$, а $R(j) = (r^{s,\,j})_{s\in S}$ – вектор-столбец, элементы которого упорядочены в соответствии с порядком нумерации строк и столбцов матрицы U. Таким образом, здесь и далее мы фиксируем кодировку номеров строк и столбцов рассматриваемых матриц состояниями из $S_B = {}^{1}S \cdot {}^{2}S$, аналогично кодируются номера компонент рассматриваемых векторов-столбцов.

Следующее утверждение непосредственно вытекает из работы [23].

Утверждение 2. Существует предел

$$\lim_{N\to\infty} \frac{1}{N}\sum_{j=1}^{N} R(j) = \bar{R};\ \bar{R} = \frac{1}{h}(E + U + \ldots + U^{h-1})(U^{h})^{\infty} R(1),$$

где h – период однородной цепи Маркова, определяемой матрицей U; E – единичная матрица; $\left(U^{h}\right)^{\infty} = \lim\limits_{K\to\infty} U^{Kh}$.

Ниже мы будем рассматривать лишь частный случай детерминированных автоматов $^1A = A$, $^2A = A'$ с вероятностном распределением $P_X = (p(x))_{x\in X}$, $p(x) > 0$, $x \in X$. При этом обозначение $B(A, A')$ будет использовано как для обозначения вероятностного автомата, когда используется распределение P_X, так и для обозначения параллельного соединения автоматов A, A′ при едином входе. Для этого частного случая из утверждений 1, 2 непосредственно вытекает следующее

Следствие 1. Последовательность $\overline{\mu_1}, \overline{\mu_2}, \ldots$ имеет предел

$$\lim_{N\to\infty} \overline{\mu}_N = \lim 1/N \sum_{j=1}^{N} R(j) = \overline{\mu} = \left(\mu^{s,s`}\right)_{(s,s`)\in S\times S`}$$

$$\overline{\mu} = U^{\infty} R(1) = 1/h \left(\mathrm{E} + U + \ldots + U^{h-1}\right)\left(U^h\right)^{\infty} R(1),$$

где U – матрица переходных вероятностей цепи Маркова, моделирующая внутреннее функционирование параллельного соединения $B(A, A')$ автоматов A, A′ при едином случайном входе, $R(1) = (r^{(s,s`,1)})_{(s,s`)\in S\times S`}$.

Для автоматов A, A′ представляет интерес нахождение условий, при которых последовательность векторов $\overline{\mu}_N$ сходится на конечном шаге, то есть найдется натуральное число $N_0 > o$, при котором

$$\overline{\mu}_{N_0} = \overline{\mu}_{N_0+j}$$

для любого $j \in \{[0, 1, \ldots\}$.

Теорема 1. Пусть H – произвольное натуральное число. Существует натуральное число $N > 0$, при котором

$$\overline{\mu}_{N_0 H} = \overline{\mu}_{(N_0+j)H},\ j \in [0,1,\ldots)$$

тогда и только тогда, когда минимальный аннулирующий многочлен вектора R(1) относительно матрицы U делит многочлен

$$(x^{H-1} + x^{H-2} + x + 1)^2 (x - 1).$$

Доказательство. Пусть нашлось N_0, при котором

$$\overline{\mu}_{N_0 H} = \overline{\mu}_{(N_0+j)H},\ j \in [0,1,\ldots)$$

Используя равенство $\mu_N = 1/N \sum_{k=1}^{N} R(K)$, получаем для любого $j \in \{0, 1, \ldots\}$

$$j/N_0 \sum_{k=1}^{N_0 H} R(k) = \sum_{k=N_0 H+1}^{(N_0+j)H} R(k).$$

Следовательно,

$$\frac{1}{N_0}\sum_{k=1}^{N_0 H} R(k) = \sum_{k=N_0 H+1}^{(N_0+1)H} R(k) = \sum_{k=(N_0+1)H+1}^{(N_0+2)H} R(k).$$

Из этих равенств вытекает, что минимальный многочлен f(x) вектора R(1) делит каждый из следующих многочленов:

$$\left(x^{H-1}+x^{H-2}+...+x+1\right)\left(\frac{1}{N_0}\left(x^{(N_0-1)H}+x^{(N_0-2)H}+x^{H}+1\right)-x^{N_0 H}\right);$$

$$\left(x^{H-1}+x^{H-2}+...+x+1\right)x^{N_0 H}\left(x^{H}-1\right).$$

Заметим, что x не делит f(x), так как ноль не является корнем первого многочлена. Следовательно, $f(x) \mid (x^{H-1} + x^{H-2} + \ldots + x + 1)(x^{H} - 1)$.

Предположим теперь, что это условие выполнено. Тогда

$$\sum_{k=1}^{H} R(k) = \sum_{k=H+1}^{2H} R(k),$$

откуда получаем $\overline{\mu}_H = \overline{\mu}_{jH}$ при любом $j \in \{1, 2, ...\}$.

Следствие 2. Последовательность $\left(\overline{\mu}_N\right)_{N\in[1,2,...)}$ сходится на конечном шаге тогда и только тогда, если UR(1) = R(1).

Отметим, что для введенной функции μ на F×F выполняются следующие метрические свойства:

$$\mu(A_s, A'_{s'}) = \mu(A'_{s'}, A_s);$$

$$\mu(A_s, A'_{s'}) + \mu(A'_{s'}, A''_{s''}) \geq \mu(A'_{s'}, A''_{s''});$$

$$\mu(A_s, A_s) = 0$$

для любых инициальных автоматов A_s, $A'_{s'}$, $A''_{s''}$ из класса F.

Определение 1. Функцию μ на F×F назовем мерой неотличимости, а ее значение $\mu(A_s, A'_{s'})$ назовем мерой неотличимости инициальных автоматов A_s, $A'_{s'}$ из F (состояний s, s′ автоматов A, A′).

Определение 2. Инициальный автомат $A`_{s'}$ из F (состояние s′ автомата A′) назовем με-неотличимым от $A_s$ (от состояния s автомата A), если $\mu(A_s, A'_{s'}) = \varepsilon$ ($\mu^{s,s`} = \varepsilon$). В этом случае будем говорить также, что A_s, $A'_{s'}$ (состояния s, s′) με -неотличимы.

Прямое использование приведенных свойств функции μ на F×F позволяет утверждать, что бинарное отношение μ0-неотличимости на F является отношением эквивалентности на F, в связи с чем обозначим через F/μ0 множество классов μ0-неотличимых инициальных автоматов из F. Используя известные факты теории цепей Мар-

кова и введенные понятия несложно доказываются следующие утверждения.

Утверждение 3. Мера неотличимости μ является метрикой на F/μ0, в частности, μ – метрика на множестве всех инициальных перестановочных автоматов из F.

Утверждение 4. Значение функции μ постоянно на каждом классе существенных состояний цепи Маркова определенной для вспомогательного вероятностного автомата B(A,A′).

Утверждение 5. Условие $\mu^{s,\,s'}=0$ не зависит от выбора вероятностного распределения $P_X = (p(x)_{x\in X})$, $p(x) > 0$, $x\in X$.

Для автоматов A[s], A′[s′] рассмотрим вспомогательный вероятностный автомат B = B(A[s], A′[s′]). Пусть $V_1, \ldots, V_r$ – классы существенных состояний цепи Маркова для автомата B[s, s′] с матрицей переходных вероятностей U, а $P(V_j)$ – предельная вероятность перехода состояния (s, s′) в V_j, $j\in\{1, 2, ..., r\}$, получаемая с помощью элементов матрицы $\tilde{U}$ укрупнением состояний рассматриваемой цепи. Пусть $\mu(V_j)$ – значение функции μ на состояниях из V_j, $j\in\{1, 2, ..., r\}$.

Утверждение 6. Справедливо равенство

$$\mu^{s,s'} = \sum_{j=1}^{r} P(V_j)\mu(V_j).$$

Доказательство. Из определения функции μ легко получить равенство

$$\mu^{s,s'} = \sum_{x\in X} p(x)\mu^{h_x s, h`_x s`},$$

с помощью которого несложно доказывается требуемое утверждение.

Замечание 1. Точный подсчет компонент вектора $\bar{\mu}$ для автоматов A, A′ значительно облегчается в случае, когда матрица U, отвечающая вспомогательному автомату B(A, A′), является неразложимой и дважды стохастической, так как в этом случае матрица

$$\tilde{U} = -\frac{1}{h}\left(E + U + \ldots + U^{h-1}\right)\left(U^{h}\right)^{\infty}$$

является равновероятной матрицей.

Следующая теорема дает критерий μ0 – неотличимости состояний s, s′ автоматов A, A′.

Теорема 2. Пусть A<s> , A′<s′> – приведенные автоматы и A_1, A_2, ..., A_k; $A`_1$, $A`_2$, ..., $A`_{k`}$ соответственно, все их минимальные по-

давтоматы. Тогда и только тогда $\mu^{s,\,s'} = 0$, когда $k = k'$ и найдется подстановка $\begin{pmatrix} 1, & 2, \ldots, k \\ j_1, & j_2, \ldots, j_k \end{pmatrix}$, при которой каждый минимальный подавтомат $A_c = (X, S_c, Y, h, f)$ изоморфен по состояниям автомату $A'_{j_c} = (X, S'_{j_c}, Y, h', f')$ при некотором изоморфизме $(E(X), \varphi_c, E(Y))$, $c \in \overline{1,k}$. При этом для любого фиксированного $\mathfrak{I}` \in X^* \cup \varnothing$ найдется $\mathfrak{I} \in X^* \cup \varnothing$ при котором

$$(h_{\mathfrak{I}} h_{\mathfrak{I}`} s,\ h`_{\mathfrak{I}} h`_{\mathfrak{I}`} s`) \in \{(s_c, \varphi_c s_c),\ s_c \in S_c,\ c \in \{1, 2, \ldots k\}\}$$

Доказательство. Для автоматов $A\langle s\rangle$, $A'\langle s'\rangle$ рассмотрим вероятностный автомат $B(A\langle s\rangle, A'\langle s'\rangle)$ и соответствующую ему матрицу переходных вероятностей U однородной цепи Маркова. Матрица $\overline{U}$ в общем случае (см. [23]) может быть представлена в виде

$$\overline{U} = \begin{pmatrix} \tilde{U}_1 & & & & & \\ & \cdot & & & & \\ & & \cdot & & & \\ & & & \cdot & & \\ & & & & \tilde{U}_r & \\ \tilde{V} & & & & & o \end{pmatrix},$$

где r – число классов существенных состояний цепи Маркова.

Класс существенных состояний S^j, $j \in \overline{1,r}$ рассматриваемой цепи Маркова назовем достижимым из (s, s'), если существует $\mathfrak{I} \in X^*$, при котором $(h_{\mathfrak{I}} s,\ h'_{\mathfrak{I}} s`) \in S^j$. Пусть $S^1, S^2, \ldots, S^t$ – все достижимые из (s, s') классы существенных состояний. Отметим следующие свойства таких классов:

1. Для любого $j \in \overline{1,t}$

$$\text{Пр}_1 S^j \in \{S_c\}_{c \in \overline{1,k}},\ \text{Пр}_2 S^j \in \{S'_c\}_{c \in \overline{1,k'}}.$$

Здесь Пр_1 (Пр_2) означает выбор первой (второй) компоненты каждого состояния $(s, s`)$ из S^j.

2. При любых $c \in \overline{1,k},\ c' \in \overline{1,k'}$ найдутся $j \in \overline{1,t}$, $j` \in \overline{1,t}$, при которых

$$\text{Пр}_1 S^j = S_c,\ \text{Пр}_2 S^j = S'_{c'}.$$

По следствию 1 $\overline{\mu} = \left(\mu^{s,s`}\right)_{(s,s') \in S_s \times S'_{s'}} = \tilde{U} R(1)$. Вектор-столбец R(1) представляется в виде

$$R(1) = (R_1(l), \ldots, R_r(l), R_{r+1}(1)),$$

где нумерация вектор-столбца $R_j(1)$, $j \in \overline{1,r}$ отвечает нумерации состояний в классе S^j существенных состояний рассматриваемой цепи Маркова.

Предположим, что $\mu^{s,s'} = 0$. Тогда (по утверждению 6) для любого состояния (s, s'), принадлежащего достижимому из (s, s′) классу существенных состояний, справедливо: $\mu^{s,s'`} = 0$. Учитывая приведенное выше равенство для $\bar{\mu}$, вид матрицы $\tilde{U}$ и то, что матрицы $\tilde{U}_j$, $j \in \overline{1,r}$ положительны [23], заключаем

$$R_j(1) = 0,\ j \in \overline{1,t}\ ,$$

то есть компоненты этих векторов равны нулю. Последнее равносильно тому, что при любом $j \in \overline{1,t}$ для каждого состояния $(s_1, s'_1) \in S^j$ инициальные автоматы $A_{s(1)}$, $A'_{s`(1)}$ равны (состояния s(1), s′(1) автоматов A<s>, A`<s`> неотличимы). Справедливость необходимости условий данной теоремы вытекает теперь из указанных выше свойств (1), (2) и приведенности автоматов A<s> , A′<s′>.

Докажем теперь достаточность условий теоремы 2. При выполнении условий теоремы справедливы равенства

$$R_j\,(l) = 0,\ j \in \overline{1,t},\ t = k = \bar{k}\ ,$$

то есть $r^{s(1),\,s`(1)} = 0$ при любом состоянии (s(1), s′(1)) из класса существенных состояний цепи Маркова, отвечающей матрице U, достижимого из (s, s′). В то же время очевидно, что элемент матрицы $\tilde{U}$, стоящий на пересечении строки с номером, соответствующим состоянию (s, s′), и столбцу с номером, соответствующим состоянию (s(1), s′(1)) , не равен нулю тогда и только тогда, когда (s(1), s`(1)) принадлежит одному из классов $S^j$, $j \in \{1, 2, ..., t\}$. В связи с чем, используя приведенное в следствии 1 равенство для $\bar{\mu}$, имеем $\mu^{s,\bar{s}`} = 0$. Утверждение теоремы полностью доказано.

11.3. Вычисление значения меры неотличимости состояний по кратному эксперименту с автоматами

Пусть P_X – распределение вероятностей на X; A = (X, S, Y, h, f), A′ = (X, S′, Y, h′, f′) – конечные автоматы. Используем для автоматов A, A′, введенные ранее (см. следствие 1) обозначения: $\bar{\mu}$, U, R(1), h. Дополнительно положим

$$M = \left(m^1_{s,s'}\right) = U^h,\ M^c = \left(m^c_{s,s'}\right),\ c \in [0,1,....).$$

Минимальный аннулирующий многочлен вектора

$$\tilde{R} = \frac{1}{h}\left(\mathrm{E} + U + U^2 + ... + U^{h-1}\right) R(1)$$

матрицы M (либо минимальный или характеристический многочлен матрицы M) запишем в виде

$$f(x) = x^k + p_1 x^{k-1} + \ldots + p_{k-1} x + p_k, \; k \le |S \times S`| .$$

Имеем

$$M^k \tilde{R}_0 + p_1 M^{k-1} \tilde{R}_0 + \ldots + p_{k-1} M \tilde{R}_0 + p_k \tilde{R}_0 = 0 .$$

Положим

$$M^c \tilde{R}_0 = \left(r^c_{s,s'} \right)_{(s,s') \in S \times S'} .$$

Стандартными приемами [37; 41], получаем $\mu^{s,s'} = 0,$ если $1 + p_1 + \ldots + p_k \neq 0$, и

$$\mu^{s,s'} = \frac{r^0_{s,s'}\left(1 + p_1 + \ldots + p_{k-1}\right) + \ldots + r^{k-2}_{s,s'}\left(1 + p_1\right) + r^{k-1}_{s,s'}}{\left(1 + p_1 + \ldots + p_{k-1}\right) + \ldots + \left(1 + p_1\right) + 1}$$ в противном случае.

Используя введенные ранее обозначения, имеем

$$r^c_{s,s'} = \frac{1}{h}\left(r^{(s,s',hc+1)} + r^{(s,s',hc+2)} + \ldots + r^{(s,s',hc+h)} \right).$$

Таким образом, для вычисления значения $\mu^{s,s'}$ меры μ на состояниях s, s′ автоматов A, A′ достаточно построить их параллельное соединение B(A, A′) при едином входе и соответствующую матрицу переходных вероятностей U, найти многочлен f(x) и по кратному эксперименту длины hk с автоматом B(A,A′) при начальном состоянии (s, s′), с учетом распределения P_X на X вычислить значения вероятностей несовпадения выходных знаков $r^{s,\,s',\,j}$ при $j \in \{1, 2, \ldots, hk\}$.

11.4. Приближенные модели связных перестановочных автоматов

В разделе используется мера неотличимости $\mu(A_s, A'_{s'})$ инициальных автоматов A_s, $A'_{s'}$ из класса F(X, Y) при равномерном вероятностном распределении P_X на X.

Пусть F_Π – класс всех связных перестановочных автоматов с входным алфавитом X, выходным алфавитом Y.

Определение 3. Автомат A′ = (X, S′, Y, h′, f′) из F_Π называется με-неотличимым от автомата A = (X, S, Y, h, f) из F_Π , если для любого состояния $s \in S$ найдется состояние $s' \in S'$, при котором s, s′ με-неотличимы, и для любого состояния s_1' из S′ найдется $s_1 \in S$, при котором состояния s_1', s_1 με-неотличимы. Автомат A′, с минимальным числом состояний, με-неотличимый от автомата A, называется минимальным με-неотличимым автоматом от A.

Очевидно, что минимальный $\mu\varepsilon$-неотличимый автомат от A является приведенным автоматом, а любой приведенный связный перестановочный автомат A сам является минимальным $\mu 0$-неотличимым автоматом от A.

Для автомата A = (X, S, Y, h, f), | S |>l из $F_П$ обозначим через $F_П(A)$ множество всех автоматов из $F_П$ с числом состояний, меньшим | S | .

Определение 4. Минимальный $\mu\varepsilon$-неотличимый автомат A′ от автомата A = (X, S, Y, h, f) называется наилучшим приближенным автоматом к A (в классе $F_П$ (A)), если $A' \in F_П(A)$ и при любом $\varepsilon' < \varepsilon$ не существует автоматов из $F_П$ (A), $\mu\varepsilon$`-неотличимых от автомата A.

Аналогично вводится понятие наихудшего приближенного автомата A′ к A (в классе $F_П(A)$). Отличие состоит лишь в том, что при любом $\varepsilon' > \varepsilon$ не существует автоматов из $F_П(A)$, $\mu\varepsilon$`-неотличимых от автомата A.

Множество всех перестановочных инициальных автоматов с входным алфавитом X и выходным алфавитом Y обозначим через $F_{П,\,И} = F(X, Y)$.

Автомат из $F_{П,\ И}$ с минимальным числом состояний, $\mu\varepsilon$-неотличимый от A_s из $F_{П,}$ назовем минимальным $\mu\varepsilon$-неотличимым автоматом от A_s.

Для автомата A_s из $F_{П,\,И}$ определим множество $F_{П,\,И}(A_s)$ всех автоматов $A'_{s'}$ из $F_{П,\,И'}$, для которых $|S_s| > |S`_{s'}|$.

Определение 5. Минимальный $\mu\varepsilon$-неотличимый автомат $A'_{s'}$ от A_s называется наилучшим приближенным автоматом к A_s (в классе $F_{П,И}$ (A_s)), если $A'_{s'} \in F_{П,\,И}(A_s)$ и при любом $\varepsilon' < \varepsilon$ не существует автоматов $A''_{s''}$ из $F_{П,\,И}$ (A_s), $\mu\varepsilon$`-неотличимых от автомата A_s.

Аналогично вводится понятие наихудшего приближенного автомата $A'_{s'}$ (в классе $F_{П,И}(A_s)$). Отличие состоит лишь в том, что при любом $\varepsilon' > \varepsilon$ не существует автоматов $A''_{s''}$ из $F_{П,И}(A_s)$ $\mu\varepsilon$`-неотличимых от автомата A.

Утверждение 7. Перестановочный связный автомат A′ = (X, S′, Y, h′, f′) является наилучшим (наихудшим) приближенным автоматом к связному приведенному перестановочному автомату A = (X, S, Y, h, f) (в классе $F_П(A)$) тогда и только тогда, когда для любого состояния $s \in S$ найдется состояние $s' \in S'$, при котором инициальный автомат $A'_{s'}$ является наилучшим (наихудшим) приближенным автоматом к инициальному автомату A_s (в классе $F_{П,И}$ (A)).

Доказательство. Данное утверждение непосредственно вытекает из введенных определений и ранее установленных фактов для связных перестановочных автоматов A, A′: A<s> = A, A′<s′> = A′ при любых $s \in S$, $s' \in S'$; $\mu^{s,s'} = \mu^{h_x s, h'_x s'}$ при любом $x \in X$.

Основная задача, решаемая в данном параграфе, состоит в нахождении наилучших (наихудших) приближенных перестановочных инициальных автоматов $A'_{s'}$ к заданному перестановочному инициальному автомату A_s (в классе $F_{П,И}(A_s)$).

Отметим, что в связи с утверждением 7 данная задача адекватна описанию наилучших (наихудших) приближенных связных перестановочных автоматов к заданному приведенному связному перестановочному автомату A (в классе $F_П(A)$).

Для решения этой задачи введем необходимые понятия и докажем ряд вспомогательных утверждений.

Определение 6. Пусть (G, S) – транзитивная группа подстановок множества S и существует покрытие $æ_1 \cup \ldots \cup æ_L$ множества S, удовлетворяющее следующим условиям:

1) $1 < L < |S|$;
2) $æ_j \neq æ_{j'}$ для $j \neq j'$, $j, j' \in \overline{1,L}$;
3) для любых $g \in G$ и $j \in \overline{1,L}$ найдется $j' \in \overline{1,L}$, для которого $gæ_j = æ_{j'}$;
4) для любых $j, j' \in \overline{1,L}$ найдется $g \in G$, для которого $gæ_j = æ_{j'}$;
5) найдется $æ \in \{æ_1, \ldots, æ_L\}$, при котором группа подстановок $H_æ$ множества æ, являющаяся ограничением на æ стабилизатора $G_æ$ множества æ, является транзитивной группой.

Тогда данное покрытие называется *системой слабой импримитивности группы* G ($æ_j$ – блок системы, $j \in \overline{1,L}$), а группа G – слабо импримитивной. Если такого покрытия не существует, то группа G называется *сильно примитивной*.

Система $\{æ_1, \ldots, æ_L\}$ слабой импримитивности группы G при дополнительном условии $æ_j \cap æ_{j'} = \varnothing$ для $j \neq j'$, $j, j' \in \overline{1,L}$ является системой импримитивности группы G [38] . В связи с этим импримитивная группа подстановок является и слабо импримитивной.

Утверждение 8. Транзитивная группа подстановок (G, S) является слабо импримитивной тогда и только тогда, если существует интранзитивная подгруппа H′ группы G индекса $|G: H'| < |S|$.

Доказательство проведем с помощью следующей леммы.

Лемма 1. Орбите æ интранзитивной подгруппы H транзитивной группы (G, S) для которой $|G: G_{æ}| = L$, $L<|S|$, соответствует система слабой импримитивности группы G: $\bigcup_{j=1}^{L} g_j æ = S$, где $g_1 = e$ (e – единица G);

$G = \bigcup_{j=1}^{L} g_j G_{æ}$, – разложение G в левые смежные классы по подгруппе $G_{æ}$. Системе слабой импримитивности: $\{æ_1, \ldots, æ_L\}$ группы (G, S) соответствует некоторая орбита $æ \in \{æ_1, æ_2, \ldots, æ_L\}$ некоторой интранзитивной подгруппы H группы (G,S), для которой $|G:G_{æ}| = L$. При этом

$$\{æ_1, æ_2, \ldots, æ_L\} = \{ g_1æ, g_2æ, \ldots, g_Læ\},\ G = \bigcup_{j=1}^{L} g_j G_{æ}$$

Доказательство. Пусть æ – орбита интранзитивной подгруппы H транзитивной группы (G,S), для которой $|G: G_{æ}| = L$, $L<|S|$. Напишем разбиение группы G на левые смежные классы по подгруппе $G_{æ}$ (стабилизатор множества æ)

$$G = \bigcup_{j=1}^{L} g_j G_{æ}\ ,\ |G:G_{æ}| = L,\ g_1 = e,$$

и для $s \in æ$ положим $æ_j = g_j G_{æ} s$. Так как группа G транзитивна, то

$$\bigcup_{j=1}^{L} æ_j = S.$$

Покажем, что данное покрытие множества S является системой слабой импримитивности группы G. Очевидно, что $G_{æ} \neq G$, то есть $1<L$ и $L<|S|$; $æ_j \neq æ_{j'}$, для $j \neq j'$, $j, j' \in \overline{1,L}$; для любых $g \in G$ и $j \in \overline{1,L}$, найдется $j' \in \overline{1,L}$, для которого $gæ_j = æ_{j'}$; для любых $j, j' \in \overline{1,L}$ найдется $g \in G$, для которого $gæ_j = æ_{j'}$; группа подстановок $H_{æ}=G$ множества $æ = æ_1$, являющаяся ограничением на æ стабилизатора $G_{æ}$ множества æ, является транзитивной группой. Следовательно, $\{æ_1, \ldots, æ_L\}$ является системой слабой импримитивности группы G.

Обратно. Пусть $\{æ_1, \ldots, æ_L\}$ – система слабой импримитивности группы (G, S) и группа подстановок подстановок множества $æ_{j`} = æ$, являющаяся ограничением на æ стабилизатора $G_{æ}$ множества æ, является транзитивной группой. Тогда æ – орбита интранзитивной подгруппы $H = G_{æ}$ группы G и $|G: G_{æ}|=L$, $L<|S|$.

Очевидно, что

$$\{æ_1, æ_2, \ldots, æ_L\} = \{g_1æ, g_2æ, \ldots, g_Læ\},$$

где $G = \bigcup_{j=1}^{L} g_j G_æ$ – разложение G в правые смежные классы по подгруппе $G_æ$.

Утверждение 8 теперь непосредственно следует из леммы 1. Доказательство закончено.

Приведем примеры примитивных групп подстановок, являющихся слабо импримитивными.

Пример 1. Пусть A_n – знакопеременная группа подстановок степени n, A_α – стабилизатор элемента α в A_n, $\alpha \in \{1, ..., n\}$, $n \geq 5$; S – множество всех подмножеств мощности 2 множества {1, ..., n}; $\overline{A}_n, \overline{A}_\alpha$ – естественные представления групп A_n, A_α на S. Известно, что A_n – (n-2)-транзитивная группа и $\overline{A}_n$ — примитивная группа [57]. Группы A_n, $\overline{A}_n$ – изоморфны, подгруппа $\overline{A}_\alpha$ – интранзитивна. $\left|\overline{A}_n : \overline{A}_\alpha\right| = |A_n : A_\alpha| = n$, $n < |S|$, $S = \frac{n(n-1)}{2}$. Таким образом, группа $\overline{A}_n$ является одновременно примитивной и слабо импримитивной группой подстановок при $n \geq 5$.

Пример 2. Пусть S_n – симметрическая группа подстановок степени n, S_α – стабилизатор элемента α в S_n , $\alpha \in \{1, ..., n\}$, S – множество всех подмножеств мощности S множества {1, ..., n}; $\overline{S}_n, \overline{S}_\alpha$- представления групп S_n, S_α на S. Очевидно, что группы S_n , $\overline{S}_n$ изоморфны, группа $\overline{S}_\alpha$ интранзитивна, $|\overline{S}_n : \overline{S}_\alpha| = |S_n : S_\alpha| = n$, $n < |S|$. Таким образом, группа $\overline{S}_n$ является одновременно примитивной и слабо импримитивной группой подстановок при $n \geq 4$.

Утверждение 9. Любая система слабой импримитивности $\{æ_1, \ldots, æ_L\}$ регулярной группы (G, S) является ее системой импримитивности.

Доказательство. Пусть $\{æ_1, \ldots, æ_L\}$, – система слабой импримитивности регулярной группы (G, S). По лемме 1 данная система может быть записана в виде $\Pi = \{g_1æ, g_2æ, \ldots, gæ\}$, где $G = \bigcup_{j=1}^{L} g_j G_æ$ – разложение G в левые смежные классы по стабилизатору $G_æ$ некоторого блока $æ \in \Pi$, причем ограничение $G_æ$ на æ является транзитивной группой. Так как $G_s = e$ для $s \in æ$, то $G_s \subset G_æ \subset G$, откуда [38] и следует утверждение 9.

Обозначим через [v] целую часть числа v.

Утверждение 10. $\left[\frac{|S|}{2}\right]$ – транзитивная группа (G, S) – является сильно примитивной.

Доказательство. Пусть (G, S) – K-транзитивная группа, $K = \left[\frac{|S|}{2}\right]$ и $\Pi = \{æ_1, æ_2, \ldots, æ_L\}$ – ее система слабой импримитивности. Возможны два случая:

1) $|æ| = |æ_j| \le \left[\frac{|S|}{2}\right]$, $j \in \overline{1,L}$;

2) $|æ| > \left[\frac{|S|}{2}\right]$.

В первом случае, используя K-кратную транзитивность (G, S) и свойство (3) определения 6, заключаем, что в множестве П содержатся все подмножества множества S мощности |æ|. Следовательно, в первом случае L > |S|, что противоречит определению П. В случае (2) рассмотрим совокупность множеств $\{S\backslash æ_1, S\backslash æ_2, \ldots, S\backslash æ_L\}$ (здесь и далее знак \ – минус). Несложно проверить выполнение следующего свойства: тогда и только тогда $gæ_j = æ_{j'}$ при некоторых $g \in G$, $j,j' \in \overline{1,L}$, когда $g(S\backslash æ_j) = S\backslash æ_{j'}$. Так как в случае (2) справедливо неравенство

$$|\, S\backslash æ_j \,| \le \left[\frac{|S|}{2}\right],\ j \in \overline{1,L},$$

то используя K-кратную транзитивность G можно аналогично случаю (1) получить L>|S|, что противоречит определению П. Следовательно, группа (G, S) – сильно импримитивна.

Определение 7. Связные перестановочные автоматы вида: $A_M = (X, S, h)$; $A = (X, S, Y, h, f)$ называются слабо импримитивными автоматами (импримитивными), если их группы $G = \langle (h_x)_{x \in X} \rangle$ подстановок на S слабо импримитивны (импримитивны). В противном случае автоматы A_M, A называются сильно примитивными автоматами.

Систему слабой импримитивности (систему импримитивности) $\{æ_1, \ldots, æ_L\}$, группы G автомата A будем называть системой слабой импримитивности (системой импримитивности) автомата A.

Введенное понятие – система импримитивности связного перестановочного автомата $A_M = (X, S, h)$ – является частным случаем известного понятия – нетривиальной конгруэнции и совпадает с

введенным ранее понятием нетривиальной конгруэнцией по состояниям автомата A_M.

Замечание 2. На основании известных результатов по декомпозиции автоматов (см., например, [45]) стандартными методами алгебраической теории автоматов можно получить следующее утверждение: автомат A = (X, S, h) является слабо импримитивным автоматом тогда и только тогда, когда найдется несвязный автомат, являющийся параллельным соединением некоторых связных перестановочных автоматов $A' = (X, S', h')$, $A'' = (X, S'', h'')$, с условием $1<|S'|<|S''|$, и автомат A изоморфен по состояниям автомату A''.

Для системы слабой импримитивности $\Pi = \{æ_1, æ_2, \ldots, æ_L\}$ связного перестановочного приведенного автомата A = (X, S, Y, h, f) через $A_M(\Pi) = (X, S^\Pi, h^\Pi)$ обозначим автомат с множеством состояний $S^\Pi = \{æ_1, æ_2, \ldots, æ_L\}$, частичными функциями переходов h_x^Π, где $h_x^\Pi æ_j = æ_{j'}$, $x \in X$. Очевидно, что автомат $A_M(\Pi)$ – связный перестановочный. Для $x \in X$ и произвольного подмножества æ множества S через ${}^x æ^y$ обозначим множество тех $s \in æ$, для которых $f_x s = y$, $y \in Y$. Через Y(x, æ), ($\hat{Y}$(x, æ)) обозначим множество всех элементов $y \in O$, при которых достигается максимум (минимум) величин $|{}^x æ^y|$, по $y \in Y$. Для фиксированных $x \in X$, $j \in \overline{1,L}$ разобьем $æ_j$ на непересекающиеся подмножества ${}^x æ_j^y$: $æ_j = \bigcup_{y \in Y} {}^x æ_j^y$. Доопределим автомат $A_M(\Pi)$ частичными функциями выходов, введя множество M(A, Π) ($\hat{M}$(A, Π)) автоматов вида

$$A(\Pi) = (X, S^\Pi, Y, h^\Pi, f^\Pi)\ (\hat{A}(\Pi) = (X, S^\Pi, Y, h^\Pi, \hat{f}^\Pi)).$$

Автомат A(Π) принадлежит M (A, Π) ($\hat{M}$(A, Π)) тогда и только тогда, если $f_x^\Pi(æ_j) \in Y(x, æ_j)$ ($\hat{f}^\Pi(æ_j) \in \hat{Y}(x, æ_j)$) при любых $x \in X$, $j \in \overline{1,L}$.

Для рассматриваемого автомата A введем еще один вспомогательный класс автоматов. Для $x \in X$ обозначим через Y(x) ($\hat{Y}$(x)) множество тех $y \in Y$, при которых достигается максимум (минимум) выражения $|f_x^{-1}(y)| = |{}^x S^y|$ по всем $y \in Y$, а через M(A) ($\hat{M}$(A)) обозначим некоторый класс автоматов с одним состоянием s_0 входным и выходным алфавитами X, Y соответственно. Именно полагаем, что

автомат $A = (X, \{s_0\}, Y, \tilde{h}, \tilde{f})$ принадлежит классу $M(A)$ ($\hat{M}(A)$) только тогда, если для всех $x \in X$

$$\tilde{h}_x(s_0) = s_0, \ \tilde{f}_x(s_0) \in Y(x) \ (\tilde{f}_x(s_0) \in \hat{Y}(x)).$$

Определение 8. Любой автомат из класса $M(A, \Pi)$ ($\hat{M}(A, \Pi)$) назовем наилучшим (наихудшим) П-образом автомата $A = (X, S, Y, h, f)$, если все автоматы из $M(A, \Pi)$ ($\hat{M}(A, \Pi)$) являются приведенными автоматами. Любой автомат из класса $M(A)$ ($\hat{M}(A)$) назовем наилучшим (наихудшим) S-образом автомата A.

В связи с тем, что значение меры неотличимости $\mu(A_s, A`_{s'})$ ($\mu^{s,s'}$) двух инициальных автоматов (состояний s, s′ автоматов A, A′) рассчитывается с помощью параметров соответствующих им автоматов $A[s]$, $A'[s']$ ($A<s>$, $A'<s'>$) ниже будут использованы более удобные, адекватные предыдущим обозначения $\mu(A[s], A'[s'])$, $\mu(A<s>, A'<s'>)$.

Теорема 3. Любой наилучший (наихудший) приближенный автомат $A'_{s'_0}$ к заданному перестановочному инициальному автомату A_{s_0} (в классе $F_{П,\,И}(A_{s_0})$) таков, что ассоциированный с ним автомат $A'[s'_0]$ изоморфен по состояниям либо одному из наилучших (наихудших) П-образов $A(П)<æ_j>$ автомата $A[s_0]$ для некоторой его системы слабой импримитивности $П = \{æ_1, \ldots, æ_L\}$, при этом $s_0 \in æ_j$ либо одному из наилучших (наихудших) S_{s_0}-образов автомата $A[s_0]$.

Доказательство. Пусть $A'_{s'_0}$ – наилучший приближенный автомат к A_{s_0} и $B = B<(s_0, s'_0)>$ – подавтомат с множеством состояний S^B, порожденный начальным состоянием (s_0, s'_0) параллельного соединения $B(A[s_0], A'[s'_0])$ приведенных перестановочных автоматов

$$A[s_0] = (X, S, Y, h, f), \ A'[s'_0] = (X, S', h', f')$$

при едином входе.

Через $æ_{s'}$, $s' \in S'$ обозначим множество тех $s \in S$, для которых $(s,s') \in S^B$. Используя замечание 1, заключаем, что матрица

$$\tilde{U} = \frac{1}{h}(E + U + \ldots + U^{h-1})$$

для автомата $B<(s_0, s'_0)>$ равновероятна. По этой причине имеем

$$\mu(A[s_0], A'[s'_0]) =$$

$$= \frac{1}{|S^B|}\sum_{(s,s')\in S^B} r^{((s,s')1)} = \frac{1}{|S^B|}\sum_{s'\in S'}\sum_{s\in æ_{S`}} r^{((s,s'),1)} = \frac{1}{|X||S^B||}\sum_{x\in X}\sum_{s`\in S`}\sum_{s\in æ_{S`}} \rho(f_x s; f`_x s`),$$

где $\rho(f_x s, f`s') = 0$, если $f_x s = f`_x s`$ и $\rho(f_x s, f`s') = 1$, в противном случае.

Используя введенные выше обозначения, имеем

$$\mu(A[s_0], A'[s'_0]) = \frac{1}{|X||S^B|}\sum_{x\in X}\sum_{s'\in S'} | æ_{s`} \setminus {}^x æ_{s`}^{f`_x s`} | .$$

Так как $A'_{s'_0}$ – наилучший приближенный автомат к заданному автомату A_{s_0} (в классе $F_{ПИ}(A_{s_0})$), то

$$\mu(A[s_0], A'[s'_0]) = \frac{1}{|X||S^B|}\sum_{x\in X}\sum_{s'\in S'} | æ_{s`} \setminus {}^x æ_{s`}^{y} | \qquad (20)$$

где элементы $y = y(x, æ_{s`})$ определены возможно неоднозначно, но данное равенство выполняется при любом выборе элементов $y(x, æ_{s'})$ из $Y(x,æ_{s'})$, $x\in X$, $s'\in S'_{s'_0}$.

Рассмотрим бинарное отношение σ на S': $s'_1 \sigma s'_2$ тогда и только тогда, если $æ_{s'_1} = æ_{s'_2}$. Очевидно, что σ – отношение эквивалентности на S', (E_X, σ) – конгруэнция по состояниям автомата $A`_M[s'_0]$. Обозначим через $S'_1, \ldots, S'_k$ классы эквивалентности отношения σ. Отметим, что они равномощны. Рассмотрим следующие случаи:

1) $1<k<|S'|$;
2) $k = 1$, $S'_1 = S'_{s'_0}$, $S' = \{s'_0\}$;
3) $k = 1$, $S'_1 = S'$, $|S'|>1$;
4) $k = |S'|$, $|S'_j| = 1$.

При выполнении случая 1) можно выбрать элементы $y(x, æ_{s'})$ из $Y(x, æ_{s'})$ такими, что при любом $x\in X$ $y(x, æ_{s'}) = y(x, æ_{s''}) = y(x, j)$ для $s', s''\in S'_j$, $j\in \overline{1,k}$. При таком выборе элементов $y(x, æ_{s'})$ рассмотрим фактор-автомат

$$A'_M\langle s'_0\rangle / (E_X,\sigma),$$

у которого состояниями являются классы $S'_1, \ldots, S'_k$. Доопределим его частичными функциями выходов β_x $x\in X$, положив: $\beta_x(S'_j) = y(x, j)$. Без ограничения общности положим $s'_0\in S'_1$. Запишем полученный автомат в виде $A'\langle S'_1\rangle$.

Имеем

$$\mu(A[s_0], A'[s'_0]) =$$

$$= \frac{1}{|X||S^B|}\sum_{x\in X}\ \sum_{s'\in S'}\left|æ_{s`} \setminus {}^{x}æ_{s`}^{y(x,æ_{s`})}\right| = \frac{|S'_1|}{|X||S\ |}\sum_{x\in X}\ \sum_{j=1}^{k}\left|æ_{s`} \setminus {}^{x}æ_{s`}^{y(x,j)}\right| = \mu(A[s_0],A'[S'_1]).$$

Автомат $A'[S'_1]$ имеет меньшее число состояний, чем $A'<s'_0>$. Поэтому случай 1) невозможен.

При выполнении случая 2) формула (20) принимает вид

$$\mu(A[s_0], A'[s'_0]) = \frac{1}{|X||S^B|}\sum_{x\in X}\left|\left(S \setminus {}^{x}S^{y(x,S)}\right)\right|.$$

Следовательно, $A'[s'_0]$ изоморфен по состояниям одному из наилучших S_{s_0} – образов автомата $A[s_0]$.

Проводя полностью аналогичные случаю 1) выкладки, несложно показывается, что случай 3) невозможен. В случае 4) легко проверяется, что $\Pi = \{æ_{s'})_{s'\in S'}$ является системой слабой импримитивности автомата $A[s_0]$, и, используя формулу (1), получаем

$$\mu(A[s_0], A'[s'_0]) = \mu(A[s_0], A'(\Pi)<æ_{s'_0}>),$$

где $s_0 \in æ_{s'_0}$ при любом автомате $A(\Pi)$ из $M(A[s_0], \Pi)$. При этом $A(\Pi)<æ_{s'}>$ – наилучший П-образ автомата $A[s_0]$ для его системы слабой импримитивности $\Pi = (æ_{s'})_{s'\in S'}$, так как $A'_{s'_0}$ – наилучший приближенный автомат к заданному автомату A_{s_0} (в классе F_Π, и (A_{s_0}).

Соответствие $s' \to æ_{s'}$ устанавливает изоморфизм по состояниям автомата $A'<s'_0>$ и некоторого наилучшего П-образа $A\ (\Pi)<æ_{s'_0}>$ автомата $A<s_0>$.

Аналогично проводится доказательство утверждения теоремы для наихудшего приближенного автомата $A'_{s'_0}$ к автомату A_{s_0}.

Из теоремы 3 вытекает, что поиск всех наилучших (наихудших) приближенных автоматов $A'_{s'_0}$ к заданному перестановочному инициальному автомату A_{s_0} (в классе $F(A_s)$) можно вести путем предварительного о построения всех наилучших (наихудших) П-образов $A(\Pi)<æ_j>$ автомата $A[s_0]$ для каждой его системы слабой импримитивности П и всех наилучших (наихудших) S_{s_0} – образов автомата $A[s_0]$ с последующим опробованием этих образов на предмет выбора наилучших (наихудших) приближенных автоматов $A'_{s'_0}$ к A_{s_0}.

Следствие 3. Автомат $A'_{s'_0}$ является наилучшим (наихудшим) приближенным автоматом к заданному перестановочному сильно

примитивному инициальному автомату A_{s_0} (в классе $F_{П,И}(A_{s_0})$) тогда и только тогда, если ассоциированный с ним автомат $A[s'_0]$ изоморфен по состояниям некоторому наилучшему (наихудшему) S_{s_0}-образу автомата $A[s'_0]$.

Будем говорить, что автомат A_s из $F_{П,И}$ является *регулярным автоматом*, если группа (G, S_s) соответствующего ему автомата $A[s] = (X, S_s, Y, h, f)$ регулярна (стабилизатор любого элемента $s` \in S_s$ является единичной подгруппой).

Обозначим через $F_{П,И,р}$ множество всех регулярных перестановочных инициальных автоматов из $F_{П,И}$. Для автомата A_s из $F_{П,И,р}$ и натурального числа $N>[S_s|$ обозначим через $F_{П,И,N}(A_s)$ множество всех автоматов $A`_{s`}$ таких, что $A_M[s]$ (автомат без выхода соответствующий автомату A_s) не является гомоморфным образом по состояниям каждого из автоматов $A`_M[s`]$ и $|S`_s|\leq N$.

Определение 9. Пусть $A_s \in F_{П,И,р}$. Минимальный $\mu\varepsilon$-неотличимый автомат $A'_{s'}$ от A_s называется наилучшим приближенным автоматом к A_s (в классе $F_{П,И,N}(A_s)$), если $A'_{s'} \in F_{П,N,р}(A_s)$ и при любом $\varepsilon'<\varepsilon$ не существует автоматов $A''_{s''}$ из $F_{П,И,N}(A_s)$, $\mu\varepsilon`$-неотличимых от автомата A_s.

Аналогично вводится понятие наихудшего приближенного автомата $A'_{s'}$ к A_s (в классе $F_{П,И,N}(A_s)$). Отличие состоит лишь в том, что при любом $\varepsilon'>\varepsilon$ не существует автоматов $A''_{s''}$ из $F_{П,И,N}(A_s)$) $\mu\varepsilon'$-неотличимых от автомата A.

Теорема 4. Любой наилучший (наихудший) приближенный автомат $A'_{s'_0}$ к заданному перестановочному регулярному инициальному автомату A_{s_0} (в классе $F_{П,И,N}(A_s)$) таков, что ассоциированный с ним автомат $A'[s'_0]$ изоморфен по состояниям либо некоторому наилучшему (наихудшему) П-образу $A(П)<æ_j>$ автомата $A[s_0]$ для некоторой его *системы импримитивности* $П = \{æ_1, \ldots, æ_L\}$, либо некоторому наилучшему (наихудшему) S_{s_0}-образу автомата $A[s_0]$.

Доказательство. Положим для краткости $S = S_{s_0}$, $S' = S'_{s'_0}$. Из определения 9 и теоремы 3 вытекает, что для доказательства теоремы 4 достаточно доказать неравенство $|S|>|S'|$. Предположим, что $|S|\leq|S'|$ и $A'_{s'_0}$ – наилучший приближенный автомат к заданному перестановочному регулярному инициальному автомату A_{s_0} (в классе

$F_{П, И, N}(A_{s_0})$). Используем для автоматов $A'_{s'_0}$, A_{s_0} введенное при доказательстве теоремы 3 обозначение $B = B<s_0,s`_0)>$. Для $s \in S$ положим $æ`_s = \{s` \in S`:(s, s`) \in S^B\}$. Аналогично первой части доказательства теоремы 3 легко получить, что

$$\mu(A[s_0], A'[s'_0]) = \frac{1}{|X||S^B|}\sum_{x\in X}\sum_{s'\in S'}|æ`_s \setminus {}^x æ`_s^{f_x s}|,$$

Рассмотрим бинарное отношение $\sigma`$ на S такое, что $s(1)\sigma`s(2)$ тогда и только тогда, когда $æ`_{s(1)} = æ`_{s(2)}$. Очевидно, что $\sigma`$ – отношение эквивалентности на S. Пусть $S_1, ..., S_k$ – классы эквивалентности бинарного отношения эквивалентности σ. Очевидно, что они равномощны. Рассмотрим следующие случаи:

1) $|S_j| = |æ`_j| = 1, j \in \{1, ..., k\}$;
2) $|S_j| = 1, |æ`_j| = 1, j \in \{1, ..., k\}$;
3) $k = 1, S_1 = S$;
4) $|S_j|>1, 1<|æ`_s|<|S|$.

Первый случай невозможен, так как в этом случае автомат $A_M[s_0]$ является изоморфным образом по состояниям автомата $A`_M[s`_0]$. Второй случай также невозможен, так как в этом случае множество $\{æ`_s: s \in S\}$ является системой импримитивности автомата $A`[s`_0]$ и несложно проверяется, что $A_M[s_0]$ является гомоморфным образом по состояниям автомата $A`[s`_0]$.

В случаях 3), 4) представим величину $\mu(A[s_0], A'[s'_0])$

$$\mu(A[s_0], A'[s'_0]) = \frac{1}{|X||S^B|}\sum_{x\in X}\sum_{j=1}^{k}\sum_{s\in S_j}|æ`_j \setminus {}^x æ_s^{f_x s}|.$$

Для завершения доказательства теоремы 4 о наилучшем инициальном автомате $A`_s$ достаточно для случаев 3), 4) получить противоречие начального предположения $|S| \le |S`|$ с условиями теоремы. С этой целью мы построим новый инициальный автомат $A^\wedge_{s^\wedge}$, для которого множество $S^\wedge_{s^\wedge}$ его состояний удовлетворяет условию $|S^\wedge_{s^\wedge}|<|S|$ и $\mu(A[s_0], A'[s'_0]) \ge \mu(A[s_0], A^\wedge[s^\wedge])$. Данное построение будет проведено с помощью выбора новых частичных функций выхода автомата $A`[s`_0]$, при которых мы получим автомат $A``<s``>$, приведенная форма которого будет являться искомым автоматом $A^\wedge[s^\wedge]$. Для выполнения этого плана рассмотрим возможности минимизации величины $\mu(A[s_0], A'[s'_0])$ путем выбора новых частичных функций выхода автомата $A'[s'_0]$.

Положим $æ`_j = æ`_s$ для $s \in S_j$, $j \in \{1, ..., k\}$. Так как разные блоки из $\{æ`_1, ..., æ`_k\}$ попарно не пересекаются, наша задача сводится к минимизации величин

$$\sum_{s \in S_j} |æ`_j \setminus {}^x æ_j^{f_x s}|, \; j \in \{1, ... k\}, \; x \in X.$$

Для фиксированных $j \in \{1, ... k\}$, $x \in X$, $y \in Y$ обозначим через $v(y)$ число состояний $s \in S_j$, для которых $f_x s = y$, и положим $æ`_j = æ$, ${}^x æ`_j^y = æ^y$. В этих обозначениях последняя сумма записывается в виде

$$\sum_{y \in Y} v(y)(|æ| - |æ^y|).$$

Для минимизации данного выражения с помощью выбора значений на æ новой частичной функции выхода β_x достаточно найти максимум суммы

$$\sum_{y \in Y} v(y)|æ^y|$$

относительно неизвестных $|æ^y|$, $y \in Y$, $\sum_{y \in Y} |æ^y| = |æ|$,

то есть найти

$$\max \sum_{y \in Y} v(y)p(y)$$

относительно неизвестных $p(y)$, $y \in Y$, где

$$p(y) = \frac{|æ^y|}{|æ|}, \quad \sum_{y \in Y} p(y) = 1.$$

Несложно проверить, что данный максимум равен $v(y`)$, где $y`$ – произвольный элемент из Y, для которого

$$v(y`) = \max_{y \in Y} v(y),$$

и он достигается, в частности, при $p(y`) = 1$. Следовательно, выбрав новые частичные функции выходов $(\beta_x)_{x \in X}$ для автомата $A`[s`_0]$ таким образом, чтобы на каждом блоке $æ_j$, $j \in \{1, ..., k\}$ они были постоянными и принимали указанные выше значения, мы получим автомат $A``<s``>$, для которого

$$\mu(A<s_0>, A'<s'_0>) \geq \mu(A<s_0>, A``<s``>),$$

причем его приведенная форма $A\wedge<s\wedge> = A\wedge[s\wedge]$ такова, что $|S\wedge_{s\wedge}|$ строго меньше числа состояний $A<s_0>$ и

$$\mu(A<s_0>, A'<s'_0>) \geq \mu(A<s_0>, A\wedge<s\wedge>).$$

Аналогично доказывается утверждение теоремы 4 о наихудшем приближенном автомате $A'_{s'_0}$ к A_{s_0}. Основное отличие состоит в

выборе автомата $A'_{s'_0}$, который находится с помощью поиска минимума величины

$$\sum_{y \in Y} v(y) | æ^{y} |$$

Доказательство теоремы 4 завершено.

Глава 12. НЕОТЛИЧИМОСТЬ СОСТОЯНИЙ КОНЕЧНЫХ АВТОМАТОВ ПО МЕРЕ μ0

В предыдущей главе было введено понятие με-неотличимости состояний конечного автомата, обобщающее классическое, известное понятие неотличимости состояний автомата. Данная глава посвящена изучению возможностей группирования состояний конечного автомата с использованием μ0-неотличимых состояний и построения на этой основе его приближенных моделей.

Без ограничения общности в данной главе мы рассматриваем случай равномерного вероятностного распределения P_X на X. Пусть $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$ – конечный автомат. Несложно показывается, что бинарное отношение μ0-неотличимости состояний инициальных автоматов является отношением эквивалентности, в связи с чем все множество состояний автомата A разбивается на классы $S_1, S_2, \ldots, S_c$ μo-неотличимых состояний, c – число классов. При этом преемники μ0-неотличимых состояний μo-неотличимы.

Определение 1. Автомат A называется μ0-приведенным (приведенным по мере μo), если c = |S|, то есть $|S_j| = 1$, $j \in \{1, \ldots, c\}$, в противном случае A называется μ0-неприведенным автоматом.

Через u(A, A) обозначим вероятностный автомат, представляющий собой параллельное соединение автомата A с автоматом A, при едином случайном входе; через Г обозначим матрицу переходных вероятностей, отвечающую однородной цепи Маркова, моделирующей поведение состояний вероятностного автомата u(A, A). Эту цепь далее будем кратко называть цепью Маркова вероятностного автомата u(A, A).

Утверждение 1. Состояния $s, \bar{s} \in S$ приведенного автомата являются μo-неотличимыми тогда и только тогда, если все достижимые из состояния $(s, \bar{s})$ классы существенных состояний цепи Маркова

автомата u(A, A) состоят лишь из состояний вида (s'',s''), $s''\in S$. В скобке одинаковые величины, не нужна ли сверху s'' черта? – ред.

Наряду с автоматом A рассмотрим автомат $\overline{A}=\left(X,S,Y,(h_x)_{x\in X},(f_x)_{x\in X}\right)$.

Определение 2. Автоматы $A,\overline{A}$ μ0-неотличимы (неотличимы по мере μ0), если для любого $s\in S$ найдется $\bar{s}\in S$ и для любого $\overline{s''}\in S$ найдется $s''\in S$, при которых инициальные автоматы $A_s,\overline{A_s}$ и $A_{\bar{s}},\overline{A_{\bar{s}}}$ μo-неотличимы. В противном случае автоматы $A,\overline{A}$ μ0-различимы (различимы по мере μ0).

Обозначим через $A_M=(X,S,Y,(h_x)_{x\in X})$ ассоциированный с автоматом A автомат без выходов.

Определение 3. Для автоматов A, $\overline{A}$ двойку сюрьективных отображений (E_I,ϕ), $E_I{:}i\to i$, $i\in I$, $\phi{:}S\to\overline{S}$ назовем гомоморфизмом по состояниям с мерой μ = 0 автомата A на $\overline{A}$ или μ0-гомоморфизмом A на $\overline{A}$, если (E_I,ϕ)-гомоморфизм по состояниям автомата A_M на $\overline{A_M}$ и при любом $s\in S$ состояния $s,\phi s$ автоматов A, $\overline{A}$ μo-неотличимы.

Для произвольного μ0-гомоморфизма (E_I,ϕ) A на $\overline{A}$ рассмотрим вспомогательный автомат $A/\mu C\phi=\left(X,\left\{\phi^{-1}(\bar{s})\right\}_{\bar{s}\in\bar{S}},Y,(\phi_{h_x})_{x\in x},(\phi_{f_x})_{x\in x}\right)$, где $\phi^{-1}(\bar{s})$-прообраз $\bar{s}\in\bar{S}$ при отображении ϕ, а для $\bar{s}\in\bar{S}$ $\phi_{h_x}\phi^{-1}(\bar{s})=\phi^{-1}(\overline{s''})$, $\overline{s''}\in\bar{S}$, $\phi_{f_x}\phi^{-1}(\bar{s})=y,y\in Y$ тогда и только тогда, если $h_x\phi^{-1}(\bar{s})\subseteq\phi^{-1}(\overline{s''}),y=\overline{f_x}\bar{s}$.

Стандартными приемами теории автоматов несложно доказываются следующие утверждения.

Утверждение 2. Если A приведенный автомат, $\overline{A}$- μ0-приведенный автомат, и A, $\overline{A}$- μ0-неотличимы, то существует μ0-гомоморфизм автомата A на $\overline{A}$.

Утверждение 3. Тройка отображений:

$(E_I,\phi_{ИЗ},E_O)$ $E_X{:}x$ a x, $x\in X$, $\phi_{ИЗ}{:}\phi^{-1}(\bar{s})$ a $\bar{s}$, $\bar{s}\in\bar{S}$, $E_Y{:}y$ a y, $y\in Y$ осуществляет изоморфизм по состояниям автомата $A/\mu 0\phi$ на $\overline{A}$, а двойка отображений $\left(E_X,\hat{\phi}\right)$: $\hat{\phi}:s\to\phi^{-1}(\phi s)$, $s\in S$ где ϕs – образ s при отображении ϕ, есть $\mu 0$-гомоморфизм A на $A/\mu 0\phi$.

Для автомата $A=(X,S,Y,(h_x)_{x\in X},(f_x)_{x\in X})$ рассмотрим ассоциированный автомат Медведева $A^M=(X,S,S,(h_x)_{x\in X},(f_x^M)_{x\in X})$, где для $x\in X,\ s\in S$ $f_x^M s=s$.

Следствие. Состояния $s, \bar{s}$ приведенного автомата A μ0-неотличимы тогда и только тогда, когда они μ0-неотличимы в автомате A^M.

Неотличимость состояний конечного автомата по мере μ0 можно трактовать как некоторую приближенную неотличимость состояний, в связи с чем естественно для данного понятия решить задачи, аналогичные классическим задачам по неотличимости состояний для конечного автомата. Решения указанных задач будет дано в следующей главе.

Глава 13. ПРИБЛИЖЕННЫЕ МОДЕЛИ АВТОМАТОВ, ПОСТРОЕННЫЕ НА ОСНОВЕ ПРЕДНЕОТЛИЧИМОСТИ СОСТОЯНИЙ И ЧАСТИЧНЫХ ГОМОМОРФИЗМОВ

В этой главе вводятся понятия преднеотличимости состояний и частичного гомоморфизма автомата, обобщающие известные понятия неотличимости состояний и гомоморфизма автомата. На этой основе предлагаются новые модели автомата, имеющие меньшее число состояний, аналогичные известным моделям: приведенной формы автомата и его образа при гомоморфизме.

13.1. Преднеотличимость состояний конечных автоматов

Пусть A = (X, S, Y, h, f) – конечный автомат. Положим X^* – множество слов конечной длины в алфавите X, $X^{**} = X^*\cup\{e\}$, где e – пустое слово. Для слова $\mathfrak{I}$ = x(1), x(2), …, x(k) полагаем $h_{\mathfrak{I}}$ = $= h_{x(к)}\ldots h_{x(1)}$ и $h_e s = s$ при любом $s\in S$.

Пусть A = (X, S, Y, h, f), A` = (X, S`, Y, h`, f`) – конечные автоматы.

Определение 1. Состояния s, s` автоматов A, A` называются преднеотличимыми состояниями (ПН-состояниями), если для любого фиксированного слова $\mathfrak{I}\wedge\in X^{**}$ существует $\mathfrak{I}\in X^{**}$, при котором

$$A(h_{\mathfrak{I}}h_{\mathfrak{I}\wedge}s, P) = A`(h`_{\mathfrak{I}}h`_{\mathfrak{I}\wedge}s`, P)$$

для любого слова $P \in X^{**}$.

Обозначим через $A_M = (X, S, (h_x)_{x \in X})$, $A`_M = (X, S`, (h`_x)_{x \in X})$ ассоциированные с A, A` автоматы без выхода. Аналогично вводится понятие преднеотличимости состояний s, s` автоматов $A_M$, $A`_M$, при этом последнее равенство заменяется на равенство

$$h_{\mathfrak{z}} h_{\mathfrak{z}^\wedge} s = h`_{\mathfrak{z}} h`_{\mathfrak{z}^\wedge} s`.$$

На интуитивном уровне прослеживается определенная близость введенного понятия с понятием μ0-неотличимости состояний конечных автоматов (см. предыдущую главу и работу [15]). Это соображение является определенным обоснованием для обсуждения вопросов группирования состояний конечных автоматов на основе понятия преднеотличимости состояний автоматов. Центральная идея такого группирования – возможность «склейки» состояний неперестановочного автомата при некоторой входной последовательности с целью группирования его состояний очевидна.

В первой части работы изучается указанное понятие для автоматов без выхода, во второй части указываются возможности переноса полученных результатов на случай произвольных автоматов.

13.2. Преднеотличимость состояний автоматов без выхода

Определение преднеотличимости состояний s, s` автоматов без выхода $A_M$, $A`_M$ конструктивно, то есть существует алгоритм проверки преднеотличимости любой пары состояний автоматов A_M, $A`_M$. Дело в том, что преднеотличимость состояний s, s` сводится к преднеотличимости состояний некоторого одного автомата A, состоящего из подавтоматов A_M, $A`_M$. И для доказательства существования алгоритма проверки преднеотличимости состояний s, s` остается заметить, что для нахождения всех достижимых пар из пары состояний $(s, s`) \in S \times S$ (приемников) можно использовать лишь слова из $X^D$, где D – диаметр графа переходов параллельного соединения $A \times A$ автомата A с собой при едином входе. Собственно, проверка «склейки», с помощью некоторого входного слова, каждого приемника пары (s, s`) может быть проведена перебором слов из X^D.

Обозначим через $\sigma_M = \sigma(A_M)$ бинарное отношение преднеотличимости (ПН) состояний S автомата $A_M = (X, S, (h_x)_{x \in X})$. Факт ПН-состояний $s, s' \in S$ будем обозначать через $s \sigma_M s'$. Если $S' \subseteq S$ и $X' \subseteq X$, то через $h_{X'} S'$ обозначим множество $\{h_{x'} s' : s' \in S', x' \in X'\}$.

Утверждение 1. Бинарное отношение преднеотличимости $\sigma = \sigma_{A_M}$ на множестве состояний S автомата A_M является отношением эквивалентности.

При чтении приводимого ниже доказательства удобно использовать рис. 5.

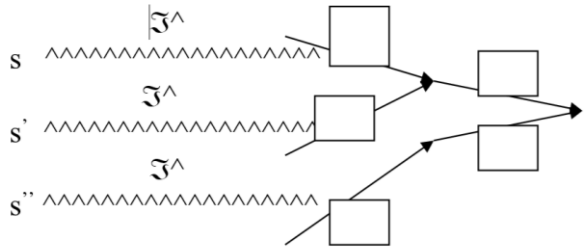

Рис. 5

По определению преднеотличимости состояний автомата A_M имеем: $s\sigma_M s$ при любом $s \in S$ и $s\sigma_M s'$ равносильно $s'\sigma s$. Пусть $s\sigma_M s'$ и $s'\sigma_M s''$. Покажем, что $s\sigma_M s''$. Выберем произвольное слово $\mathfrak{I}\wedge$ из X^{**}. Для s, s', $\mathfrak{I}\wedge$ существует $\mathfrak{I}(1)$ из X^{**}, при котором

$$h_{\mathfrak{I}(1)} h_{\mathfrak{I}\wedge} s = h_{\mathfrak{I}(1)} h_{\mathfrak{I}\wedge} s'.$$

Для s', s'', $\mathfrak{I}\wedge\mathfrak{I}(1)$ существует $\mathfrak{I}(2)$ из X^{**}, при котором

$$h_{\mathfrak{I}(2)} h_{\mathfrak{I}(1)} h_{\mathfrak{I}\wedge} s' = h_{\mathfrak{I}(2)} h_{\mathfrak{I}(1)} h_{\mathfrak{I}\wedge} s'',$$

следовательно,

$$h_{\mathfrak{I}(2)} h_{\mathfrak{I}(1)} h_{\mathfrak{I}\wedge} s = h_{\mathfrak{I}(2)} h_{\mathfrak{I}(1)} h_{\mathfrak{I}\wedge} s''.$$

Учитывая теперь, что $\mathfrak{I}\wedge$ – произвольное фиксированное слово из X^{**}, заключаем, что $s\sigma_M s''$. Доказательство завершено.

Обозначим через $\chi = \{\chi(1), \chi(2), \ldots, \chi(L)\}$ множество классов σ_M-эквивалентных состояний автомата A_M, через $\chi[s]$ обозначим класс эквивалентности, содержащий состояние из S. Из определения преднеотличимости состояний автомата A_M непосредственно вытекает, что для любых $x \in X$, $j \in \{1, \ldots, L\}$ существует $j' \in \{1, \ldots, L\}$, при котором

$$h_x \chi(j) \subseteq \chi(j').$$

Таким образом, двойка разбиений множеств X, S

$$P_{E_X} = \{x : x \in X\}, P_{\sigma_M} = \{\chi(j) : \chi(j) \in \chi\}$$

является конгруэнцией автомата A_M, в связи с чем определяется фактор-автомат $A_M/(P_{E_X}, P_{\sigma_M}) = (X, \chi, (h_x)_{x \in X})$ автомата A_M по этой конгруэнции.

При этом двойка отображений

$$E_X : x \to x,\ x \in X,\ \varphi_\sigma : s \to x[s],\ s \in S,\ \sigma = \sigma_M$$

является естественным гомоморфизмом A_M на $A_M/(P_{E_X}, P_{\sigma_M})$.

Определение 2. Автомат A_M называется послеприведенным автоматом (ПП-автоматом), если он не имеет различных преднеотличимых состояний.

Утверждение 2. Фактор-автомат $A_M/(P_{E_X}, P_{\sigma_M})$ является послеприведенным автоматом.

Доказательство. Предположим, что автомат $A_M/(P_{E_X}, P_{\sigma_M})$ не является ПП-автоматом. Тогда найдутся два его состояния $\chi[s_1]$, $\chi[s_2]$ такие, что при каждом фиксированном $\mathfrak{I}^\wedge$ из X^{**} найдется $\mathfrak{I}$ из X^{**}, при котором

$$h_{\mathfrak{I}} h_{\mathfrak{I}^\wedge} \chi[s_1] \subseteq \chi(j),\ h_{\mathfrak{I}} h_{\mathfrak{I}^\wedge} \chi[s_2] \subseteq \chi(j)$$

при некотором $j \in \{1, \ldots, L\}$. В частности, найдутся s', s'' из $\chi(j)$, при которых

$$h_{\mathfrak{I}} h_{\mathfrak{I}^\wedge} s_1 = s',\ h_{\mathfrak{I}} h_{\mathfrak{I}^\wedge} s_2 = s''.$$

Так как состояния s', s'' из $\chi(j)$ являются ПН-состояниями, то существует $\mathfrak{I}'$ из X^{**}, при котором

$$h_{\mathfrak{I}'} s' = h_{\mathfrak{I}'} s'' = s,\ s \in S.$$

Следовательно, для любого $\mathfrak{I}^\wedge \in X^{**}$ нашлось $\mathfrak{I}\mathfrak{I}' \in X^{**}$, при котором

$$h_{\mathfrak{I}'} h_{\mathfrak{I}} h_{\mathfrak{I}^\wedge} s_1 = h_{\mathfrak{I}'} h_{\mathfrak{I}} h_{\mathfrak{I}^\wedge} s_2,$$

то есть $\chi[s_1] = \chi[s_2]$. Доказательство завершено.

13.3. Преднеотличимость состояний произвольных автоматов

Пусть $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$ – произвольный конечный автомат. Через $A_M = (X, S, (h_X)_{x \in X})$ обозначим автомат без выхода, ассоциированный с автоматом A.

Определение 3. Автомат A называется послеприведенным, если он не имеет различных преднеотличимых состояний.

Обозначим через τ бинарное отношение преднеотличимости состояний автомата A. С использованием стандартных приемов несложно показать, что τ – отношение эквивалентности на S.

Пусть $Z = \{z_1, \ldots, z_L\}$ – классы эквивалентности отношения τ на S – множестве состояний автомата A. Легко видеть, что двойка разбиений множеств X, S

$$P_{E_X} = \{x : x \in X\},\ P_\tau = \{z(j) : z(j) \in Z\}$$

есть конгруэнция на автомате $A_M = (X, S, (\delta_x)_{x \in X})$, причем конгруэнция

$$(P_{E_X}, P_{\sigma_M}) = (\{x : x \in X\}, \{\chi(j) : x(j) \in \chi\})$$

содержится в конгруэнции (P_{E_X}, P_τ): $(P_{E_X}, P_{\sigma_M}) \subseteq (P_{E_X}, P_\tau)$.

Очевидно, для приведенного автомата A справедливо равенство конгруэнций

$$(P_{E_X}, P_{\sigma_M}) = (P_{E_X}, P_\tau).$$

Обозначим через ε – бинарное отношение неотличимости состояний автомата A, а через

$$(P_{E_X}, P_\varepsilon, P_{E_Y}),\ P_{E_Y} = \{y : y \in Y\} –$$

соответствующую ему конгруэнцию автомата A. Очевидно,

$$(P_{E_X}, P_\varepsilon) \subseteq (P_{E_X}, P_\tau).$$

Определим фактор-автомат $A/(P_{E_X}, P_\varepsilon, P_{E_Y}) = A_П$ автомата A и ассоциированный с ним автомат без выхода $(A/(P_{E_X}, P_\varepsilon, P_{E_Y}))_M = (A_П)_M$.

По известной теореме о соответствии между конгруэнциями автомат $A_M/(P_{E_X}, P_\tau)$ изоморфен, во-первых, автомату

$$(A_П)_M/(P_{E_X}, P_\tau)/(P_{E_X}, P_\varepsilon)$$

(фактор-автомату автомата $(A_П)_M/(P_{E_X}, P_\tau)$ по конгруэнции (P_{E_X}, P_ε)) и, во-вторых, автомату

$$A_M/(P_{E_X}, P_{\sigma_M})/(P_{E_X}, P_\tau)/(P_{E_X}, P_{\sigma_M}).$$

Последний автомат представляет собой фактор-автомат автомата $A_M/(P_{E_X}, P_{\sigma_M})$ по конгруэнции $(P_{E_X}, P_\tau)/(P_{E_X}, P_{\sigma_M}) = (P_{E_X}, K)$, где K – разбиение S, соответствующее произведению (пересечению) P_τ и P_{σ_M}. Несложно показывается, что конгруэнция $(P_{E_X}, P_\tau)/(P_{E_X}, P_\varepsilon)$ автомата $(A_П)_M$ совпадает с его конгруэнцией $(P_{E_X}, P_{\sigma((A_п)_M)})$.

Подведем итог проведенных исследований.

1. Вышеизложенные результаты сводят задачу оценки или расчета числа классов отношения эквивалентности τ состояний автомата A к двум задачам:

а) описания приведенной формы $A_П = A/(P_{E_X}, P_\varepsilon, P_{E_Y})$ автомата A;

б) расчета или оценки числа классов отношения эквивалентности $\sigma((A_n)_M)$ автомата без выхода $(A_П)_M$.

2. Автомат A является послеприведенным автоматом тогда и только тогда, если A – приведенный автомат и ассоциированный с ним автомат без выхода AM является послеприведенным автоматом.

3. Любой перестановочный, приведенный автомат является послеприведенным автоматом.

Замечание 1. В работе [15] было введено понятие $\mu\varepsilon$-неотличимости состояний конечного автомата, обобщающее классическое, известное понятие неотличимости состояний автомата.

Ниже используются понятия [15]. Пусть $A = (X,S,Y,(h_x)_{x\in X},(f_x)_{x\in X})$ – конечный автомат. Без ограничения общности мы рассматриваем случай равномерного вероятностного распределения на X. Исходя из определения $\mu 0$-неотличимости состояний автомата A несложно показывается, что бинарное отношение $\mu 0$-неотличимости состояний является отношением эквивалентности, в связи с чем все множество состояний автомата A разбивается на классы $\chi_1,\chi_2,...,\chi_c$ $\mu 0$-неотличимых состояний, c – число классов. В [15] доказано, что преемники μo-неотличимых состояний $\mu 0$-неотличимы.

Назовем автомат A $\mu 0$-приведенным, если $c = |S|$, то есть $|\chi_j| = 1$, $j\in\{1, \ldots, c\}$, в противном случае автомат A называется $\mu 0$-неприведенным автоматом.

Через U(A, A) обозначим вероятностный автомат, представляющий собой параллельное соединение автомата A с собой, то есть с автоматом A, при едином случайном входе; через Г обозначим матрицу переходных вероятностей, отвечающую однородной цепи Маркова, моделирующей поведение состояний вероятностного автомата U(A, A). Эту цепь далее будем кратко называть цепью Маркова вероятностного автомата U(A, A). Из работы [15] непосредственно вытекает следствие.

Следствие 1. Состояния $s,\bar{s}\in S$ приведенного автомата являются $\mu 0$-неотличимыми тогда и только тогда, если все достижимые из состояния $(s,\bar{s})$ классы существенных состояний цепи Маркова автомата u(A, A) состоят лишь из состояний вида (s'',s''), $s''\in S$.

Наряду с автоматом A рассмотрим автомат $\overline{A}=\left(X,\overline{S},Y,\left(\overline{h}_x\right)_{x\in X},\left(\overline{f}_x\right)_{x\in X}\right)$.

Назовем автоматы A, $\overline{A}$ *μ0-неотличимыми*, если для любого $s\in S$ найдется $\bar{s}\in S$ и для любого $\overline{s''}\in S$ найдется $s''\in S$, при которых инициальные автоматы $A_s,\overline{A_s}$ и $A_{\bar{s}},\overline{A_{\bar{s}}}$ μ0-неотличимы (см. определение 2 работы [15]). В противном случае они μ0-различимы.

Данное замечание указывает новые возможности группирования состояний конечного автомата с использованием μ0-неотличимых состояний и построения на этой основе его приближенных моделей. Кроме того, из замечания следует очевидное утверждение, заключающееся в том, что понятия преднеотличимости и μ0-неотличимости состояний автомата эквивалентны.

13.4. Частичные гомоморфизмы автоматов без выхода

В данном разделе вводятся и изучаются приближенные модели автоматов без выхода, а в следующем разделе указываются возможности переноса и обобщения полученных результатов на случай произвольного конечного автомата.

Пусть $A_м$ = (X, S,(h_x)$_{x\in X}$), $\overline{A_м}$= ($\overline{X}$, $\overline{S}$, $(\overline{h}_{\bar{x}})_{\bar{x}\in\overline{X}}$) – произвольные конечные автоматы без выхода, а ψ: X→$\overline{X}$ – некоторое сюрьективное отображение. Продолжим ψ до отображения на X^{**} на $\overline{X}^{**}$, положив для $\mathfrak{I}$ = x_1, …, x_k

$$\psi(\mathfrak{I}) = \psi(x_1),...,\psi(x_k),\ \psi(e)=e.$$

Определение 4. Двойку сюръективных отображений (ψ,ϕ), ψ: X→$\overline{X}$, φ: S →$\overline{S}$ назовем частичным гомоморфизмом автомата без выходов $A_м$ на $\overline{A_м}$ (ЧГ $A_м$ на $\overline{A_м}$), если для любой фиксированной пары $(s,\overline{\mathfrak{I}})\in S\times X^{**}$ выполняется условие: существует $\mathfrak{I}\in X^{**}$, $\mathfrak{I}$ =$\mathfrak{I}$(s, $\overline{\mathfrak{I}}$), при котором для любого $\mathfrak{I}\wedge\in X^{**}$справедливо равенство

$$\varphi h_{\mathfrak{I}\wedge} h_{\mathfrak{I}}\, h_{\overline{\mathfrak{I}}}\, s=\overline{h}_{\psi(\mathfrak{I}\wedge)}\overline{h}_{\psi(\mathfrak{I})}\overline{h}_{\psi(\overline{\mathfrak{I}})}\varphi s.$$

Введенное понятие определяет некоторый частичный гомоморфизм алгебры, производной от автомата $A_м$, на некоторую алгебру, производную от автомата $\overline{A_м}$. Лишь в целях краткости этот частичный гомоморфизм алгебр мы назвали частичным гомоморфизмом автомата без выхода $A_м$ на $\overline{A_м}$.

Свойство: (ψ,ϕ) является частичным гомоморфизмом $A_м$ на $\overline{A_м}$ - алгоритмически проверяемо. Действительно, рассмотрим параллельное соединение (рис. 6) $\alpha_{M,\psi} = A_м \times \overline{A_м}$ автоматов $A_м, \overline{A_м}$ вида с входным алфавитом $\{(x,\psi(x)) : x \in X\}$.

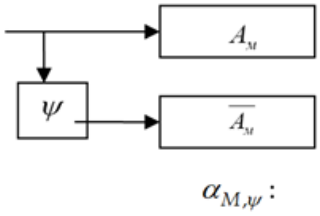

Рис. 6

Тогда все приемники произвольного состояния автомата $\alpha = \alpha_{M,\psi}$ вида $(s,\phi s)$ достижимы из него за число шагов, не превышающих диаметр D_α графа переходов автомата α и для каждого фиксированного приемника требуемое в определении 4 слово $\Im \in X^{**}$, если оно существует, можно выбрать длины, не превосходящей D_α.

С использованием техники доказательств утверждений 1, 2 несложно доказывается с утверждение.

Утверждение 3. Если (ψ_1,ϕ_1) ЧГ $A_м$ на $\overline{A_м}$ и (ψ_2,ϕ_2) ЧГ $\overline{A_м}$ на $\overline{\overline{A_м}}$, то пара суперпозиций $(\psi_2 o\psi_1,\ \phi_2 o\phi_1)$ является ЧГ $A_м$ на $\overline{\overline{A_м}}$.

Пусть $P_T = \{T_j, j\in\{1, \ldots, L\}\}$ – разбиение некоторого конечного множества T. Произвольные слова $\Im = t_1,t_2,...,t_k$, $\Im' = t_1',t_2',...,t_k'$ из M^{**} назовем сравнимыми по P_T, если $\Im = \Im' = e$, $e \in T^{**}$ (e – пустое слово), либо для любого $j\in\{1, \ldots, k\}$ существует $j'\in\{1, \ldots, L\}$, при котором $t_j \in T_{j'}$, $t`_j \in T_{j'}$.

Определение 5. Пару разбиений множеств X, S

$$P_X = \{X_j, j\in\{1, \ldots, n\}\},\ P_S = \{S_c, c\in\{1, \ldots, L\}\},$$

назовем частичной конгруэнцией (ЧК) автомата $A_м$, если для любых фиксированных $c\in\{1, \ldots, L\}$, $\overline{\Im} \in X^{**}$ найдется $\Im \in X^{**}$, $\Im = \Im(S_c, \overline{\Im})$, при котором для любой фиксированной пары сравнимых по P_X слов $\overline{\Im_1}, \overline{\Im_2} \in X^{**}$ существует $j'\in\{1, \ldots, L\}$, при котором

$$h_{\overline{\Im_1}} h_{\Im} h_{\overline{\Im}} S_c \subseteq S_{j'},\ h_{\overline{\Im_2}} h_{\Im} h_{\overline{\Im}} S_c \subseteq S_{j'}.$$

В силу конечного числа различных подмножеств множества состояний конечного автомата, несложно показывается алгоритмическая разрешимость проблемы проверки выполнимости для пары разбиений P_X, P_S произвольного автомата A_M условий сформулированных в данном определении.

Утверждение 4. Если (ψ,ϕ) частичный гомоморфизм автомата A_M на $\overline{A_M}$, то пара семейств множеств

$$P_\psi = (\psi^{-1}(\bar{x}),\ \bar{x} \in \bar{X},),\ P_\varphi = (\phi^{-1}(\bar{s}),\ \bar{s} \in \bar{S})$$

является частичной конгруэнцией автомата A_M.

Доказательство. Пусть выполнены условия данного утверждения и $\bar{s}$ – произвольное фиксированное состояние из $\bar{S}$, а $\bar{\mathfrak{I}}$ – произвольное фиксированное слово из X^{**}. Положим $\phi^{-1}(\bar{s})=\{s_1,s_2,...,s_k\}$. По определению ЧГ (ψ,ϕ) существует $\mathfrak{I}_1 \in X^{**}$, при котором для любого $\bar{\bar{\mathfrak{I}}} \in X^{**}$ справедливо равенство

$$\varphi h_{\bar{\bar{\mathfrak{I}}}}\, h_{\mathfrak{I}_1}\, h_{\bar{\mathfrak{I}}}\, s_1 = \bar{h}_{\psi(\bar{\bar{\mathfrak{I}}})}\bar{h}_{\psi(\mathfrak{I}_1)}\bar{h}_{\psi(\bar{\mathfrak{I}})}\bar{s}.$$

Аналогично для $\bar{\mathfrak{I}}\mathfrak{I}_1$, s_2 найдется $\mathfrak{I}_2$, при котором

$$\varphi h_{\bar{\bar{\mathfrak{I}}}}\, h_{\mathfrak{I}_2}\, h_{\bar{\mathfrak{I}}\mathfrak{I}_1}\, s_2 = \bar{h}_{\psi(\bar{\bar{\mathfrak{I}}})}\bar{h}_{\psi(\mathfrak{I}_2)}\bar{h}_{\psi(\bar{\mathfrak{I}}\mathfrak{I}_1)}\bar{s}.$$

при любом $\bar{\bar{\mathfrak{I}}} \in X^{**}$. Продолжая так же далее, получим, что для слова $\bar{\mathfrak{I}}\mathfrak{I}_1\mathfrak{I}_2...\mathfrak{I}_{j-1}$ и состояния s_j, $j\in\{2, \ldots, k\}$ найдется $\mathfrak{I}_j \in X^{**}$, при котором

$$\varphi h_{\bar{\bar{\mathfrak{I}}}}\, h_{\mathfrak{I}_j}\, h_{\bar{\mathfrak{I}}\mathfrak{I}_1...\mathfrak{I}_{j-1}}\, s_j = \bar{h}_{\psi(\bar{\bar{\mathfrak{I}}})}\bar{h}_{\psi(\mathfrak{I}_j)}\bar{h}_{\psi(\bar{\mathfrak{I}}\mathfrak{I}_1...\mathfrak{I}_{j-1})}\bar{s}.$$

Таким образом, для $\phi^{-1}(\bar{s}) = \{s_1,s_2,...,s_k\}$ и произвольного фиксированного слова $\bar{\mathfrak{I}} \in X^{**}$ нашлось слово $\mathfrak{I}_1\mathfrak{I}_2...\mathfrak{I}_k$, при котором при любом $\bar{\bar{\mathfrak{I}}} \in X^{**}$ справедливо равенство

$$\varphi h_{\bar{\bar{\mathfrak{I}}}}\, h_{\mathfrak{I}_1\mathfrak{I}_2...\mathfrak{I}_k}\, h_{\bar{\mathfrak{I}}}\, \phi^{-1}(\bar{s}) = \bar{h}_{\psi(\bar{\bar{\mathfrak{I}}})}\bar{h}_{\psi(\mathfrak{I}_1...\mathfrak{I}_k)}\bar{h}_{\psi(\bar{\mathfrak{I}})}\bar{s},$$

или

$$h_{\bar{\bar{\mathfrak{I}}}}\, h_{\mathfrak{I}_1\mathfrak{I}_2...\mathfrak{I}_k}\, h_{\bar{\mathfrak{I}}}\, \phi^{-1}(\bar{s}) \subseteq \phi^{-1}\, \bar{h}_{\psi(\bar{\bar{\mathfrak{I}}})}\bar{h}_{\psi(\mathfrak{I}_1...\mathfrak{I}_k)}\bar{h}_{\psi(\bar{\mathfrak{I}})}\bar{s}.$$

Откуда следует, что (P_ψ, P_φ)-ЧК на A_M. Доказательство завершено.

Пусть $s\in S$, $\bar{s} \in \bar{S}$ состояния автоматов A_M, $\overline{A_M}$ соответственно. Инициальные автоматы $A_M(s)$, $\overline{A_M}(\bar{s})$ задают отображения. Через $A_M\langle s\rangle = (X, S_s, (h_x)_{x\in X})$, $\overline{A_M}\langle\bar{s}\rangle = (\bar{X}, \bar{S}_{\bar{s}}, (\bar{h}_{\bar{x}})_{\bar{x}\in\bar{X}})$, соответственно, обозначим подавтоматы автоматов A_M, $\overline{A_M}$, реализующие эти отображения (подавтоматы, порожденные состояниями s, $\bar{s}$).

Здесь $S_s=\{h_{\mathfrak{I}}s:\mathfrak{I}\in X^{**}\}$, $\overline{S}_{\bar{s}}=\{\bar{h}_{\bar{x}}\bar{s}:\bar{\mathfrak{I}}\in X^{**}\}$.

В данном случае и далее в ряде случаев для краткости отображения и их ограничения на соответствующих подмножествах обозначены одним и тем же символом.

Будем говорить, что двойка отображений $\psi':X\to\overline{X}$, $\phi':S_s\to\overline{S}_{\bar{s}}$ - является *гомоморфизмом инициального автомата* $A_м(s)$ на $\overline{A_м}(\bar{s})$, если (ψ',ϕ') – гомоморфизм автомата $A_м<s>$ на $\overline{A_м}<\bar{s}>$ и $\bar{s}=\phi's$.

Лемма 1. Если (ψ,ϕ) – частичный гомоморфизм автомата $A_м$ на $\overline{A_м}$, то найдутся $s'\in S$, $\bar{s}'\in\bar{S}$ такие, что $(\psi,\phi_{S_{s'}})$ есть гомоморфизм $A_м(s)$ на $\overline{A_м}(\bar{s})$ ($\phi_{S_{s'}}$ – ограничение ϕ на $S_{s'}$).

Доказательство. Достаточно показать наличие $s'\in S$, при котором

$$\varphi h_x h_{\bar{\bar{\mathfrak{I}}}} s'=\bar{h}_{\psi(x)}\varphi\bar{h}_{\bar{\bar{\mathfrak{I}}}} s',\ x\in X$$

при любом $\bar{\bar{\mathfrak{I}}}\in X^{**}$. Для указанной в определении 4 пары $(s,\bar{\mathfrak{I}})$ по определению 4 имеем

$$\varphi h_{\bar{\bar{\mathfrak{I}}}}\, h_{\mathfrak{I}}\, h_{\bar{\mathfrak{I}}}\, s = \bar{h}_{\psi(\bar{\bar{\mathfrak{I}}})}\bar{h}_{\psi(\mathfrak{I})}\bar{h}_{\psi(\bar{\mathfrak{I}})}\varphi s,$$

$$\varphi h_x h_{\bar{\bar{\mathfrak{I}}}}\, h_{\mathfrak{I}}\, h_{\bar{\mathfrak{I}}}\, s = \bar{h}_{\psi(i)}\bar{h}_{\psi(\bar{\bar{\mathfrak{I}}})}\bar{h}_{\psi(\mathfrak{I})}\bar{h}_{\psi(\bar{\mathfrak{I}})}\varphi s.$$

Положив теперь $s'=h_{\mathfrak{I}}\, h_{\bar{\mathfrak{I}}}\, s$, получаем требуемое равенство.

Пусть (ψ,ϕ) – частичный гомоморфизм автомата $A_м$ на $\overline{A_м}$. В автомате $A_м$ однозначно определен его подавтомат $A_{м,1}$ с максимальным по мощности множеством состояний $\hat{S}_1$ и подавтомат $\overline{A_{M,1}}$ с множеством состояний $\hat{\overline{S}}_1=\phi\hat{S}_1$, такие, что пара $(\psi,\phi_{\hat{S}_1})$ – гомоморфизм $A_{м,1}$ на $\overline{A_{M,1}}$. Очевидно следующее утверждение.

Лемма 2. Подавтомат $A_{м,1}$ ($\overline{A_{M,1}}$) содержит все тупиковые сильно связные (см. [58]) подавтоматы автомата $A_м$ ($\overline{A_м}$).

Обозначим через $A_{м,0}$ ($\overline{A_{M,0}}$) подавтомат автомата $A_{м,1}$ ($\overline{A_{M,1}}$), состоящий из всех сильно связных тупиковых подавтоматов автомата $A_м$ ($\overline{A_м}$).

Положим

$$A_{м,1}=(X,\ \hat{S}_1,(h_x)_{x\in X}),\ \overline{A_{M,1}}=(\overline{X},\hat{\overline{S}}_1,(\bar{h}_{\bar{x}})_{\bar{x}\in\bar{X}}),$$

$$A_{м,0}=(X,\ \hat{S}_0,(h_x)_{x\in X}),\ \overline{A_{M,0}}=(\overline{X},\hat{\overline{S}}_0,(\bar{h}_{\bar{x}})_{\bar{x}\in\bar{X}}).$$

Очевидно,

$$\phi \hat{S}_0 = \hat{\overline{S}}_0 .$$

Определение 6. Частичный гомоморфизм (ψ,ϕ) автомата $A_м$ на $\overline{A_м}$ будем называть частичным изоморфизмом (ЧИ) автомата $A_м$ на $\overline{A_м}$, если ограничение $\phi_{\hat{S}_0}$ отображения $\phi : S \to \bar{S}$ на $\hat{S}_0$ взаимнооднозначно.

Пусть (ψ,ϕ) – частичный гомоморфизм автомата $A_м$ на $\overline{A_м}$. В введенных обозначениях, из сказанного выше следует, что двойка отображений $(\psi,\varphi_{\hat{S}_\nu})$ – гомоморфизм $A_{м,\nu}$ на $\overline{A_{M,\nu}}$, $\nu \in \{0,1\}$ и фактор-автомат $A_{м,\nu}/(P_\psi, P_{\phi_{\hat{S}_\nu}})$ автомата $A_м$ по конгруэнции

$$P_\psi = \{\, \psi^{-1}(\bar{x}) : x \in \overline{X} \,\},\ P_{\phi_{\hat{S}_\nu}} = \{\, \phi^{-1}(\bar{s}) :\ \bar{s} \in \overline{S_\nu} \,\}$$

изоморфен автомату $\overline{A_{M,\nu}}$, $\nu \in \{0,1\}$. Обозначим этот изоморфизм через $(U_{1,\nu}, U_{2,\nu})$, $\nu \in \{0,1\}$

$$U_{1,\nu} : \psi^{-1}(\bar{x}) \to \bar{x},\quad \bar{x} \in \overline{X} ,$$

$$U_{2,\nu} : \phi^{-1}(\bar{s}) \to \bar{s},\ \bar{s} \in \hat{\overline{S_\nu}} .$$

Следовательно, в частности, пара разбиений

$$P_{E_X} = \{\mathrm{x}:\ \mathrm{x} \in \mathrm{X}\},\ P_{\hat{S}_\nu} = \{\, \varphi^{-1}_{\hat{S}_j}(\bar{s}) : \bar{s} \in \hat{\overline{S_\nu}} \,\}$$

множеств I, $\hat{S}_j$ есть конгруэнция на $A_{м,\nu}, \nu \in \{0,1\}$.

Для автомата $A_м$ определим вспомогательные автоматы $A_{м,P_\nu}$, $\nu \in \{0,1\}$, положив

$$A_{м,P_0} = (\mathrm{X},\ \{\phi^{-1}_{\hat{S}_\nu}(\bar{s})\}_{\bar{s} \in \hat{\overline{S_\nu}}} \cup (S \setminus \bigcup_{\bar{s} \in \hat{\overline{S_\nu}}} \phi^{-1}(\bar{s})),\ (h_x^{P_\nu})_{x \in X}).$$

Здесь состояниями автомата $A_{м,P_\nu}$ являются, во первых, блоки $\{\phi^{-1}_{\hat{S}_\nu}(\bar{s})\}_{\bar{s} \in \hat{\overline{S_\nu}}}$ разбиения $P_{\hat{S}_\nu}$ и состояния s автомата $A_м$, не вошедшие ни в один из этих блоков. Функции переходов автомата $A_{м,P_\nu}$ заданы следующим образом. Для $\mathrm{s} \in S \setminus \bigcup_{\bar{s} \in \hat{\overline{S_\nu}}} \phi^{-1}(\bar{s})$

$$h_x^{P_\nu} s = \phi^{-1}_{\hat{S}_\nu}(\bar{s}),$$

если $h_x s \in \phi^{-1}_{\hat{S}_\nu}(\bar{s})$, для некоторого $\bar{s} \in \hat{\overline{S_j}}$ и

$$h_x^{P_\nu} s = h_x s$$

в противном случае. Далее

$$h_x^{P_\nu}\ \phi^{-1}_{\hat{S}_\nu}(\bar{s}) = \phi^{-1}_{\hat{S}_\nu}(\bar{s}'),$$

если

$$h_x\ \phi^{-1}_{\hat{S}_\nu}(\bar{s}) \subseteq \phi^{-1}_{\hat{S}_\nu}(\bar{s}').$$

Очевидно, пара разбиений

$$P_{E_X},\ P_S = \{\{\phi^{-1}_{\hat{S}_\nu}(\bar{s})\}_{\bar{s}\in\hat{\bar{S}}_\nu}, \{s\colon s\in S,\ s\notin \bigcup_{\bar{s}\in\hat{\bar{S}}_\nu}\varphi^{-1}_{\hat{S}_\nu}(\bar{s})\}\}$$

является конгруэнцией автомата A_M и фактор-автомат $A_M/(P_{E_X}, P_S)$ автомата A_M по данной конгруэнции совпадает с A_{M,P_ν}. Обозначим через $(E_X, \Gamma_{\psi,\nu})$ естественный гомоморфизм A_M на $A_M/(P_{E_X}, P_S) = A_{M,P_\nu}$.

Определим отображение ϕ_{Γ,P_ν} множества состояний автомата A_{M,P_ν} на $\bar{S}$, положив

$$\varphi^{-1}_{\hat{S}_\nu}(\bar{s}) : \to \bar{s},\ \bar{s}\in\hat{\bar{S}}_\nu,$$

$$\phi_{\Gamma,P_\nu}:$$

$$s \to \varphi s,\ s\in S,\ s\notin \bigcup_{\bar{s}\in\hat{\bar{S}}_\nu}\varphi^{-1}_{\hat{S}_\nu}(\bar{s}).$$

Из доказательства утверждения 4 следует, что $(\psi,\ \phi_{\Gamma,P_\nu})$ – частичный изоморфизм автомата $A_{M,\nu}$ на $\overline{A_M}$, $\nu\in\{0,1\}$.

Таким образом, в введенных обозначениях, из указанных выше фактов непосредственно вытекает утверждение.

Утверждение 5. Для частичного гомоморфизма (ψ,ϕ) автомата A_M на $\overline{A_M}$ коммутативна следующая диаграмма рис. 7 частичных гомоморфизмов:

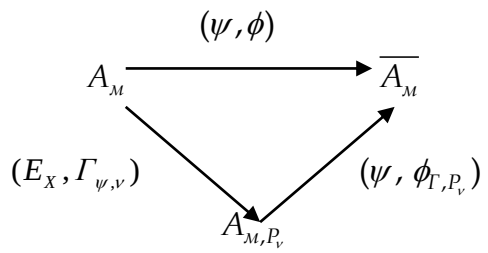

Рис. 7

Здесь $(E_X, \Gamma_{\psi,\nu})$ – гомоморфизм A_M на A_{M,P_ν}, а $(\psi, \phi_{\Gamma,P_\nu})$ – частичный изоморфизм A_{M,P_ν} на $\overline{A_M}$. Из утверждения 5 вытекает, что для описания образов частичных гомоморфизмов автомата A_M достаточно решить две задачи:

1) описать гомоморфные образы автомата A_M;

2) дать описание образов частичных изоморфизмов произвольного автомата без выхода.

Первая задача является классической задачей теории автоматов, решение которой приведено в ряде известных статей и книг.

Перейдем к решению второй задачи.

Утверждение 6. Пусть (ψ,ϕ) частичный изоморфизм автомата A_M на $\overline{A_M}$. Тогда при любом $\bar{s} \in \bar{S}$, состояния из множества $\phi^{-1}(\bar{s})$ автомата A_M преднеотличимы.

Доказательство. Пусть $\bar{s} \in \bar{S}$ и выполнены условия данного утверждения. Для его доказательства достаточно показать, что произвольно выбранные состояния $s_1, s_2 \in \phi^{-1}(\bar{s})$ являются ПН-состояниями. По определению 4 при любом $\bar{\mathfrak{I}} \in X^{**}$ найдется $\mathfrak{I}_1$, при котором

$$\varphi h_{\bar{\bar{\mathfrak{I}}}}\, h_{\mathfrak{I}_1}\, h_{\bar{\mathfrak{I}}}\, s_1 = \bar{h}_{\psi(\bar{\bar{\mathfrak{I}}})} \bar{h}_{\psi(\mathfrak{I}_1)} \bar{h}_{\psi(\bar{\mathfrak{I}})} \bar{s}$$

при любом $\bar{\bar{\mathfrak{I}}} \in X^{**}$. Аналогично, для $\bar{\mathfrak{I}}\mathfrak{I} \in X^{**}$ найдется $\mathfrak{I}_2$, при котором

$$\varphi h_{\bar{\bar{\mathfrak{I}}}}\, h_{\mathfrak{I}_2} h_{\mathfrak{I}_1}\, h_{\bar{\mathfrak{I}}}\, s_2 = \bar{h}_{\psi(\bar{\bar{\mathfrak{I}}})} \bar{h}_{\psi(\mathfrak{I}_2)} \bar{h}_{\psi(\mathfrak{I}_1)} \bar{h}_{\psi(\bar{\mathfrak{I}})} \bar{s},$$

при любом $\bar{\bar{\mathfrak{I}}} \in I^{**}$. Следовательно, при любом фиксированном $\bar{\mathfrak{I}} \in X^{**}$ нашлось слово $\mathfrak{I}_1, \mathfrak{I}_2 = \mathfrak{I},\ \mathfrak{I} \in I^{**}$, при котором

$$\varphi h_{\bar{\bar{\mathfrak{I}}}}\, h_{\mathfrak{I}}\, h_{\bar{\mathfrak{I}}}\, s = \bar{h}_{\psi(\bar{\bar{\mathfrak{I}}})} \bar{h}_{\psi(\mathfrak{I})} \bar{h}_{\psi(\bar{\mathfrak{I}})} \bar{s},$$

при любом $\bar{\bar{\mathfrak{I}}} \in X^{**}$ и любом $s \in \{s_1, s_2\}$. Так как (ψ,ϕ) – частичный изоморфизм, то состояния s_1, s_2 – ПН- состояния.

Утверждение 7. Если (ψ,ϕ) – частичный изоморфизм автомата A_M на $\overline{A_M}$ и A_M – послеприведенный автомат, то (ψ,ϕ) – гомоморфизм A_M на $\overline{A_M}$, причем ϕ – взаимнооднозначное отображение.

Доказательство. Пусть (ψ,ϕ) – частичный изоморфизм A_M на $\overline{A_M}$ и A_M – послеприведенный автомат, s_1 – произвольное состояние из S. Тогда для любого фиксированного слова вида $\bar{x}\bar{\mathfrak{I}} \in X^{**}$ найдется $\mathfrak{I}_1 \in X^{**}$, при котором

$$\varphi h_{\bar{\bar{\Im}}}\, h_{\Im_1}\, h_{\bar{\Im}} h_{\bar{x}}\, s_1 \;=\; \bar{h}_{\psi(\bar{\bar{\Im}})} \bar{h}_{\psi(\Im_1)} \bar{h}_{\psi(\bar{\Im})} \bar{h}_{\psi(\bar{i})} \varphi s_1,$$

при любом $\bar{\bar{\Im}} \in X^{**}$. Кроме того, для состояний $\overline{s_2} = \bar{h}_{\psi(\bar{x})} \varphi s_1$ и $s_2 = \varphi^{-1}(\bar{\delta}_{\psi(\bar{x})} \varphi s_1)$ при любом фиксированном $\bar{\Im} \in X^{**}$ для слова $\bar{\Im}\Im_1$ найдется $\Im_2 \in X^{**}$, при котором

$$\varphi h_{\bar{\bar{\Im}}}\, h_{\Im_2} h_{\Im_1}\, \delta_{\bar{\Im}}\, s_2 \;=\; \bar{h}_{\psi(\bar{\bar{\Im}})} \bar{h}_{\psi(\Im_2)} \bar{h}_{\psi(\Im_1)} \bar{h}_{\psi(\bar{\Im})} \overline{s_2},$$

при любом $\bar{\bar{\Im}} \in X^{**}$.

Таким образом, при указанных словах справедливо равенство

$$h_{\bar{\bar{\Im}}}\, h_{\Im_2} h_{\Im_1}\, h_{\bar{\Im}}\, s \;=\; \bar{h}_{\psi(\bar{\bar{\Im}})} \bar{h}_{\psi(\Im_2)} \bar{h}_{\psi(\Im_1)} \bar{h}_{\psi(\bar{\Im})} \overline{s_2},$$

при любом $s \in \{\delta_{\bar{x}} s_1, s_2\}$ и любом $\bar{\bar{\Im}} \in X^{**}$. Так как $\bar{\Im} \in X^{**}$ выбиралось произвольным образом и по условию (ψ, ϕ) есть ЧИ $A_м$ на $\overline{A_м}$, то состояния $\delta_{\bar{x}} s_1$ и s_2 автомата $A_м$ преднеотличимы. Так как $A_м$ – ПП-автомат, то $s_2 = \delta_{\bar{x}} s_1$, то есть

$$\varphi h_{\bar{x}} s_1 = \bar{h}_{\psi(\bar{x})} \varphi s_1 .$$

Утверждение полностью доказано в силу произвольного выбора $s_1 \in S$, $\bar{x} \in X$ и утверждения 7.

Утверждение 8. Пусть (ψ, ϕ) – частичный гомоморфизм автомата $A_м$ на $\overline{A_м}$ и $\overline{A_м}$ – послеприведенный автомат, то (ψ, ϕ) – гомоморфизм $A_м$ на $\overline{A_м}$.ДОКАЗАТЕЛЬСТВО. Пусть (ψ, ϕ)– ЧГ $A_м$ на $\overline{A_м}$ и s_1 - произвольное состояние из S. Тогда для любого фиксированного слова $\bar{x}\bar{\Im} \in X^{**}$ найдется $\Im_1 \in X^{**}$, при котором

$$\varphi h_{\bar{\bar{\Im}}}\, h_{\Im_1}\, h_{\bar{\Im}} h_{\bar{x}}\, s_1 \;=\; \bar{h}_{\psi(\bar{\bar{\Im}})} \bar{h}_{\psi(\Im_1)} \bar{h}_{\psi(\bar{\Im})} \bar{h}_{\psi(\bar{x})} \varphi s_1,$$

Аналогично, для состояний $h_{\bar{x}} s_1$, $\overline{s_2} = \varphi h_{\bar{x}} s_1$, при любом фиксированном $\bar{\Im} \in X^{**}$ для слова $\bar{\Im}\Im_1$ найдется $\Im_2 \in X^{***}$, при котором

$$\varphi h_{\bar{\bar{\Im}}}\, h_{\Im_2} h_{\Im_1}\, h_{\bar{\Im}} h_{\bar{x}}\, s_1 \;=\; \bar{h}_{\psi(\bar{\bar{\Im}})} \bar{h}_{\psi(\Im_2)} \bar{h}_{\psi(\Im_1)} \bar{h}_{\psi(\bar{\Im})} s_2 .$$

Следовательно, при заданных словах справедливо равенство

$$\bar{h}_{\psi(\bar{\bar{\Im}})} \bar{h}_{\psi(\Im_2)} \bar{h}_{\psi(\Im_1)} \bar{h}_{\psi(\bar{\Im})} \bar{h}_{\psi(\bar{x})} \varphi s_1 = \bar{h}_{\psi(\bar{\bar{\Im}})} \bar{h}_{\psi(\Im_2)} \bar{h}_{\psi(\Im_1)} \bar{h}_{\psi(\bar{\Im})} \overline{s_2} .$$

То есть состояния $\bar{h}_{\psi(\bar{x})} \varphi s_1$, $\overline{s_2} = \varphi h_{\bar{x}} s_1$ преднеотличимы в автомате $\overline{A_м}$, и, в силу его послеприведенности, эти состояния совпадают. Следовательно, (ψ, ϕ) – гомоморфизм A_M на $\overline{A}_M$. Утверждение доказано.

Ниже, в ряде случаев, чтобы избежать громоздких обозначений мы фактор-автомат A/K по конгруэнции K, соответствующей гомоморфизму H будем обозначать и через A/H.

Пусть $(E_{\overline{X}}, \varphi_{\sigma_{\overline{A}_M}})$ – естественный гомоморфизм A_M на $\overline{A}_M/(E_{\overline{X}}, \varphi_{\sigma_{\overline{A}_M}})$, где $\sigma_{\overline{A}M}$ – бинарное отношение преднеотличимости состояний автомата $\overline{A}_M$; $(E_X, \varphi_{\sigma_{A_M}})$ – естественный гомоморфизм A_M на $A_M/(E_X, \varphi_{\sigma_{A_M}})$. Несложно показывается, что пара суперпозиций отображений

$$(E_{\overline{X}}\psi, \sigma_{\overline{A}_M}\varphi) = (\psi, \Gamma)$$

является гомоморфизмом A_M на $\overline{A}_M/(E_{\overline{X}}, \varphi_{\sigma_{\overline{A}_M}})$. Пусть (P_ψ, P_Γ) – конгруэнция на A_M, отвечающая гомоморфизму (ψ, Γ), и $A_M/(P_\psi, P_\Gamma)$ – фактор-автомат по этой конгруэнции, изоморфный автомату $\overline{A}_M/(E_{\overline{X}}, \varphi_{\sigma_{\overline{A}_M}})$. Обозначим этот изоморфизм через $(И_1, И_2)$.

Введем дополнительные обозначения. Если K_1 и K_2 – конгруэнции автомата A_M такие, что $K_1 \subseteq K_2$, то в автомате A_M/K_1 естественным образом вводится конгруэнция K_2/K_1. В связи с чем, определен фактор-автомат

$$A_M/K_1 / K_2/K_1$$

автомата A_M/K_1 по конгруэнции K_2/K_1.

Стандартными приемами несложно доказывается следующее

Утверждение 9. Справедливо включение конгруэнций автомата A_M.

$$(P_{E_X}, P_\sigma) \subseteq (P_\psi, P_\Gamma), \quad P_\sigma = \{\chi_1, ..., \chi_L\},$$

где $\chi = \{\chi_1, ..., \chi_L\}$ – классы отношения эквивалентности $\sigma = \sigma_{A_M}$. В частности, автоматы

$$A_M/(P_{E_X}, P_\sigma) / (P_\psi, P_\Gamma) / (P_{E_X}, P_\sigma),$$
$$A_M/(P_\phi, P_\Gamma)$$

изоморфны.

Таким образом, нами доказана коммутативность следующей диаграммы
(рис. 8) частичных гомоморфизмов и гомоморфизмов введенных автоматов

Таким образом, в частности, для нахождения послеприведенных образов при частичных изоморфизмах автомата A_M достаточно найти послеприведенные гомоморфные образы автомата A_M.

Теперь у нас есть все необходимое для изучения частичных гомоморфизмов произвольных автоматов.

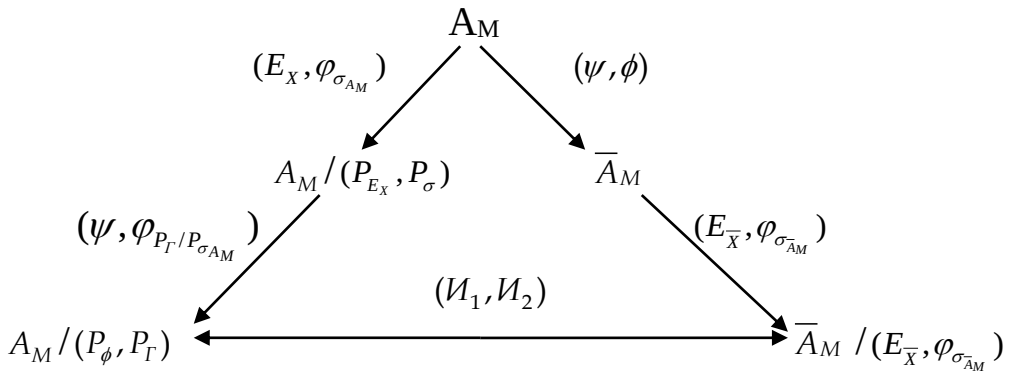

Рис. 8

13.5. Частичные гомоморфизмы произвольных автоматов

Определение 7. Тройку сюрьективных отображений (ψ, φ, η)

$$\psi: X \to \overline{X}, \quad \varphi: S \to \overline{S}, \quad \eta: Y \to \overline{Y}$$

назовем частичным гомоморфизмом (ЧГ) автомата A = (X, S, Y, $(h_x)_{x\in X}$,$(f_x)_{x\in X}$) на автомат $\overline{A} = (\overline{X}, \overline{S}, (\overline{h}_{\overline{x}})_{\overline{x}\in\overline{X}}, (f_{\overline{x}})_{\overline{x}\in\overline{X}})$, если для любой фиксированной пары $(s, \overline{\mathfrak{I}}) \in S\times X^{**}$ существует $\mathfrak{I}\in X^{**}$, при котором для любого $\mathfrak{I}^\wedge \in X^{**}$ справедливы равенства

$$\varphi h_{\mathfrak{I}^\wedge} h_{\mathfrak{I}} \overline{h}_{\overline{\mathfrak{I}}} s = h_{\psi\mathfrak{I}^\wedge} h_{\psi\mathfrak{I}} \overline{h}_{\psi\overline{\mathfrak{I}}} \varphi s.$$

Несложно доказывается

Утверждение 10. Если $(\psi_1,\varphi_1,\eta_1)$ – ЧГ A_1 на A_2 и $(\psi_2,\varphi_2,\eta_2)$ – ЧГ A_2 на A_3, то тройка отображений

$$(\psi_2\psi_1, \varphi_2\varphi_1, \eta_2\eta_1)$$

является ЧГ A_1 на A_3.

Перейдем теперь к построению критерия того, что тройка (ψ,φ,η) сюрьективных отображений задает частичный гомоморфизм автомата A на $\overline{A}$. Для этого введем дополнительные обозначения.

Обозначим через A_T, ($\overline{A_T}$) подавтомат автомата A ($\overline{A}$), состоящий из всех сильно связных тупиковых подавтоматов автомата A

($\overline{A}$). *Пусть* ψ: X→$\overline{X}$ – сюрьективное отображение, а $A\underset{\times}{\overset{\psi}{}}\overline{A}$ параллельное соединение рис. 9 автоматов A $\overline{A}$ вида ?

Автомат $A\underset{\times}{\overset{\psi}{}}\overline{A}$ как параллельное соединение автоматов A, $\overline{A}$ с множеством состояний $S\times\overline{S}$ имеет входной алфавит {(x,ψx): x∈X}, частичные функции переходов $\Delta_{(x,\psi x)}(s,\overline{s})=(h_x s,\overline{h}_{\psi x}\overline{s})$ и выходов $f_{(x,\psi x)}(s,\overline{s})=(f_x s,\overline{f}_{\psi x}\overline{s})$, $(s,\overline{s})\in S\times\overline{S}$.

Пусть S_T ($\overline{S}_T$) – множество состояний автомата A_T ($\overline{A_T}$), φ: S→$\overline{S}$, а φ_T – ограничение φ на S_T. Несложно проверяется справедливость следующих утверждений.

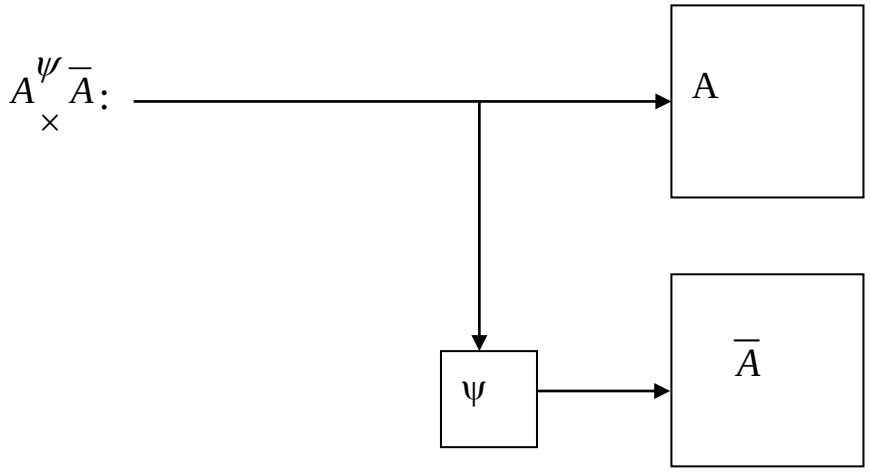

Рис. 9

Утверждение 11. Тройка сюрьективных отображений (ψ, φ, η)

ψ: X→$\overline{X}$, φ: S→$\overline{S}$, η: Y→$\overline{Y}$

является частичным гомоморфизмом (ЧГ) автомата A = (X, S, Y, $(h_x)_{x\in X}$,$(f_x)_{x\in X}$) на автомат $\overline{A}$ = ($\overline{X}$, $\overline{S}$, $(\overline{h}_{\overline{x}})_{\overline{x}\in\overline{X}}$, $(\overline{f}_{\overline{x}})_{\overline{x}\in\overline{X}}$) тогда и только тогда, когда выполнены два условия:

1) тройка (ψ, φ, η) – гомоморфизм A_T на $\overline{A_T}$;

2) для любого состояния автомата $A\underset{\times}{\overset{\psi}{}}\overline{A}$ вида $\Delta_{\mathfrak{I}^\wedge}(s,\varphi s)$, где s∈S, $\mathfrak{I}^\wedge$ – произвольное фиксированное слово в алфавите {(x,ψx): x∈X}, найдется слово $\mathfrak{I}$ в том же алфавите, при котором $\Delta_{\mathfrak{I}}\Delta_{\mathfrak{I}^\wedge}(s,\varphi s)\in\{(s`,\varphi s`): s`\in S_T\}$.

Для автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ и сюрьективного отображения $\eta: Y\to\overline{Y}$ рассмотрим вспомогательный автомат

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

где $\eta f_x s=\eta(f_x s)$, $s\in S$.

Утверждение 12. Тройка сюрьективных отображений (ψ, φ, η)

$$\psi: X\to\overline{X},\ \ \varphi: S\to\overline{S},\ \ \eta: Y\to\overline{Y}$$

является ЧГ автомата A на автомат $\overline{A}$ тогда и только тогда, когда тройка отображений $(\psi, \varphi, E_{\overline{Y}})$, где $E_{\overline{Y}}$ тождественное отображение $\overline{Y}$ на $\overline{Y}$, есть ЧГ ηA на $\overline{A}$.

Это утверждение сводит задачу описания образов ЧГ-автомата A к описанию ЧГ вида (ψ, φ, E_Y) произвольного конечного автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$.

Утверждение 13. Если (ψ, φ, E_Y) ЧГ A на $\overline{A}$ $(\overline{Y}=Y)$, то для любого состояния $\overline{s}\in\overline{S}$ автомата $\overline{A}$ состояния из множества $\varphi^{-1}(\overline{s})$ преднеотличимы.

Следствие 2. Если (ψ, φ, E_Y) ЧГ A на $\overline{A}$ и автомат A является послеприведенным автоматом, то (ψ, φ) – гомоморфизм автомата A_M на $\overline{A}_M$, причем отображение φ биективно.

Утверждение 14. Если (ψ, φ, η) ЧГ A на послеприведенный автомат $\overline{A}$, то (ψ, φ) – гомоморфизм A_M на $\overline{A}_M$.

Для автомата A и бинарного отношения преднеотличимости τ на его множестве состояний построим вспомогательный автомат $A_\tau = (X, S_\tau, Y, ({}^\tau h_x)_{x\in X}, ({}^\tau f_x)_{x\in X})$. Ниже мы определяем его параметры. Пусть $Z = \{Z_1, \ldots, Z_L\}$ – классы эквивалентности отношения τ, а $\chi = \{\chi_1, \ldots, \chi_{L`}\}$ – классы эквивалентности отношения $\varepsilon_T$ – неотличимости состояний подавтомата $A_T$ автомата A. Из вышеизложенных свойств бинарных отношений $\tau$, $\varepsilon_T$ следует, что для любого $j`$ существует единственное $j\in\{1, \ldots, L\}$, при котором $\chi_{j`}\subseteq Z_j$; в связи с чем, в частности, $L`\le L$. Без ограничения общности будем считать, что $\chi_j\subseteq Z_j$, $j\in\{1, \ldots, L`\}$. Положим $S_\tau = Z$, а частичные функции переходов $({}^\tau h_x)_{x\in X}$ определим так:

$${}^\tau h_x Z_j = Z_k,\ (j, k)\in\{1, \ldots, L\}$$

тогда и только тогда, когда

$$h_x Z_j\subseteq Z_k.$$

Определение частичных функций переходов $({}^{\tau}h_x)_{x\in X}$ вполне корректно, так как ранее было отмечено, что (P_{E_X}, P_τ) – конгруэнция автомата A_M.

Для Z_j, $j\in\{1, \ldots, L`\}$ и $x\in X$ положим

$$ {}^{\tau}f_x Z_j = f_x(\chi_j), $$

а для $j>L`$, если такие найдутся, положим

$$ {}^{\tau}f_x Z_j = y(j), $$

где $y(j)$ – произвольный фиксированный элемент из Y.

Через $Z[s](\chi[s])$ обозначим класс эквивалентности бинарного отношения τ, (ε_T), содержащий состояние $s\in S$.

Стандартными методами легко доказываются следующие утверждения.

Утверждение 15. Тройка отображений (E_X,φ_τ,E_Y)

$$ E_X(x) = x,\ x\in X,\ \varphi_\tau(s) = Z[s],\ s\in S,\quad E_Y(y) = y,\ y\in Y $$

является частичным гомоморфизмом автомата A на A_τ.

Утверждение 16. Автомат A_τ является послеприведенным автоматом.

Следствие 3. Пусть (ψ, φ, η) – частичный гомоморфизм автомата A на $\overline{A}$; $\overline{Z}=\{\overline{Z}_1,\ldots,\overline{Z}_{\overline{L}}\}$ – классы отношения преднеотличимости автомата $\overline{A}$; $\varphi_{\overline{\tau}}$ – отображение $\overline{s}$ а $Z[\overline{s}]$; $\overline{A_{\overline{\tau}}}$ – вспомогательный автомат для $\overline{A}$. Тогда тройка суперпозиций $(E_X\psi,\ \varphi_{\overline{\tau}}\varphi,\ E_Y\eta)$ введенных ранее отображений является частичным гомоморфизмом автомата A на $\overline{A_{\overline{\tau}}}$, причем $(\psi,\varphi_{\overline{\tau}}\varphi)$ – гомоморфизм автомата A_M на $(\overline{A_{\overline{\tau}}})_M$.

Итак, приведенные результаты позволяют для заданного автомата A (A_M) строить его приближенные модели – его образы при частичных гомоморфизмах.

Замечание 2. Обозначим через $A_M=(X,S,Y,(h_x)_{x\in X})$ ассоциированный с автоматом $A = (X, S, (h_x)_{x\in X}, (f_x)_{x\in X})$ автомат без выходов.

Определение 8. Для автоматов $A = (X, S, (h_x)_{x\in X}, (f_x)_{x\in X})$, $\overline{A} = (\overline{X}, \overline{S}, (\overline{h}_{\overline{x}})_{\overline{x}\in\overline{X}}, (\overline{f}_{\overline{x}})_{\overline{x}\in\overline{X}})$ двойку сюрьективных отображений

$$ (E_X,\varphi),\ E_X\colon x\to x,\ x\in X,\ \varphi\colon S\to\overline{S} $$

назовем гомоморфизмом по состояниям с мерой $\mu = 0$ автомата A на $\overline{A}$ или $\mu 0$-гомоморфизмом A на $\overline{A}$, если (E_X,φ)-гомоморфизм по

состояниям автомата A_M на $\overline{A_M}$, и при любом $s \in S$ состояния s, φs автоматов A, $\overline{A}$ μ0-неотличимы.

Для произвольного μ0-гомоморфизма (E_X, φ) A на $\overline{A}$ рассмотрим вспомогательный автомат

$$A/\mu 0\text{-}\varphi = \left(X, \left\{\varphi^{-1}\left(\bar{s}\right) : \bar{s} \in \bar{S}\right\}, Y, \left({}^{\varphi}h_x\right)_{x \in X}, \left({}^{\varphi}f_x\right)_{x \in X}\right),$$

где $\phi^{-1}\left(\bar{s}\right)$ – прообраз $\bar{s} \in \bar{S}$ при отображении ϕ, а для $\bar{s} \in \bar{S}$

$$^{\varphi}h_x \varphi^{-1}\left(\bar{s}\right) = \varphi^{-1}\left(\overline{s''}\right), \ \overline{s''} \in \bar{S},$$
$$^{\varphi}f_x \varphi^{-1}\left(\bar{s}\right) = y, \ \ y \in Y$$

тогда и только тогда, если

$$h_x \varphi^{-1}\left(\bar{s}\right) \subseteq \varphi^{-1}\left(\overline{s''}\right), \ y = \overline{f_x}\bar{s}.$$

Стандартными приемами теории автоматов несложно доказываются следующие утверждения.

Утверждение 17. Если A – приведенный автомат, $\overline{A}$ – μ0-приведенный автомат и A, $\overline{A}$ – μ0-неотличимы, то существует μ0-гомоморфизм автомата A на $\overline{A}$.

Утверждение 18. Тройка отображений $(E_X, \varphi_{ИЗ}, E_Y)$:

$$E_x : x \to x, \ x \in X,$$
$$\varphi_{ИЗ} : \varphi^{-1}\left(\bar{s}\right) \to \bar{s}, \ \bar{s} \in \bar{S},$$
$$E_Y : y \to y, \ y \in O$$

осуществляет изоморфизм по состояниям автомата $A/\mu 0 - \varphi$ на $\overline{A}$, а двойка отображений $\left(E_X, \hat{\varphi}\right)$, где $\hat{\varphi} : s \to \varphi^{-1}(\varphi s), s \in S$ (φs – образ s при отображении φ), есть $\mu 0$-гомоморфизм A на $A/\mu 0 - \varphi$.

Для автомата A = (X, S, Y, $(h_x)_{x \in X}$, $(f_x)_{x \in X}$) рассмотрим ассоциированный автомат Медведева $A^M = (X, S, S, (h_x)_{i \in X}, (f_x^M)_{x \in X})$, где для $x \in X$, $s \in S$

$$f_x^M s = s.$$

Следствие 4. Состояния s, $\bar{s}$ приведенного автомата A μ0-неотличимыми тогда и только тогда, когда они μ0-неотличимы в автомате A^M.

Глава 14. МЕТОД ПРИБЛИЖЕННЫХ МОДЕЛЕЙ В РЕШЕНИИ ЗАДАЧ ОПРЕДЕЛЕНИЯ НАЧАЛЬНЫХ СОСТОЯНИЙ И ВХОДНЫХ СЛОВ АВТОМАТА[1]

Получены формулы для параметров сложности методов определения состояния и входного слова автомата, основанных на предварительном построении его приближенных моделей.

Указываются методы определения:

– начального состояния и входного слова автомата по его выходному слову;

– входного слова автомата по его начальному состоянию и выходному слову;

– входного слова автомата по его начальному и заключительному состояниям; в частности, входного слова регистра сдвига по его начальному и заключительному состояниям;

– начального состояния автомата по входной и выходной последовательностям.

14.1. Постановка задачи

Пусть Ω, Z – конечные непустые множества. Рассмотрим следующую задачу. Известно отображение □: Ω□Z и z□Z. Требуется найти хотя бы одно решение относительно неизвестного ω□Ω, совместного уравнения

$$\square(\omega) = z. \qquad (21)$$

Известные методы решения данной задачи [30] условно делятся на классы: универсальные, например, метод полного перебора [20], аналитические [42. – С. 397]; статистические [16; 20; 36]; методы типа «разделяй и побеждай» [44]; методы на основе наличия декомпозиции функции φ или наличия ее гомоморфных образов [29], например, метод «встреча посредине» [53. – С. 235] и др.

Предлагаемый в данной работе общий метод решения задачи состоит в следующем. Строится вспомогательное отображение □`: Ω□Z, для которого сравнительно несложно определяется неко-

[1] Благодарю Вячеслава Дмитриевича Аносова за полезные замечания к работе, содержащей результаты данной главы, позволившие мне улучшить ее качество, устранить неточности и по новому оценить для себя ряд результатов.

торое множество R(□`)□Ω, содержащее все решения R(□`, z) уравнения

□`(ω) = z.

По очереди для каждого случайно и равновероятно выбранного ω□R(□`) проверяется равенство (21) и первое ω, для которого оно выполняется (если такое ω существует), объявляется решением задачи. Мы будем сравнивать эффективность предлагаемого метода решения задачи с тотальным методом опробования ω□Ω до получения одного из решений уравнения (21). Эффективность метода опробования задается параметрами:

$\frac{|R(\varphi,z)|}{|\Omega|}$ – вероятностью выбора решения при случайном и равновероятном выборе ω□Ω;

$\frac{|\Omega|+1}{|R(\varphi,z)|+1}$ – средним числом опробований без возвращения до получения первого решения заданного уравнения (21).

При расчете параметров сложности предлагаемого метода мы будем считать, что мощность |R(□,z)| множества R(□,z) решений данного уравнения нам известна.

Пусть задано равномерное вероятностное распределение на Ω, и P – условная вероятность события ω□R(□, z)

$$P = P(\omega\square R(\square,z)/\omega\square R(\square`)) = \frac{|R(\phi`)\mathrm{I}\ R(\phi,z)|}{|R(\phi`)|}$$

(вероятностью выбора решения при случайном и равновероятном выборе ω□R(□`)).

Если P>0, то среднее число E(T) опробований элементов ω в выборке без возвращения из R(□`) равно

$$E(T) = \frac{|R(\phi`)|+1}{P|R(\phi`)|+1}$$

(параметры сложности нахождения множества R(□`) пока не обсуждаются). Если P таково, что

$$\frac{|R(\phi,z)|}{|\Omega|}<P<1,$$

то E(T) строго меньше среднего числа опробований

$$\frac{|\Omega|+1}{|R(\varphi,z)|+1},$$

совершаемых при решении уравнения (1) методом перебора ω□Ω до получения первого решения этого уравнения.

Для вычисления вероятности P и ее оценок введем обозначения. Положим R(□, z) = ^{непр}R(□, z)□^{пр}R(□, z), где ^{непр}R(□, z) – произвольное фиксированное подмножество множества

R(□, z)□R(□`, z),

мощность |^{непр}R(□, z)| которого предполагается известной.

Очевидно,

$$P = \frac{|R(\phi`) \mathrm{I}\ R(\phi,z)|}{|R(\phi`)|} = \frac{|R(\phi`) \mathrm{I}\ {}^{пр}R(\phi,z)|}{|R(\phi`)|} + \frac{|{}^{непр}R(\phi,z)|}{|R(\phi`)|} \square \frac{|{}^{непр}R(\phi,z)|}{|R(\phi`)|}$$

и

$$E(T) \square \frac{|R(\phi`)|+1}{|{}^{непр}R(\phi,z)|+1}.$$

При известной мощности множества ^{непр}R(□, z) данная оценка может быть использована на практике. Для уточнения оценки E(T) необходимо подсчитать или оценить величину $|R(\phi`) \mathrm{I}\ {}^{пр}R(\phi,z)|$.

В ряде конкретных задач, о которых речь пойдет ниже, подсчет этой величины, а вместе с ней и точного значения вероятности P, вызывает значительные трудности. Поэтому представляет интерес расчет среднего значения величины P при случайном выборе □. Сформулируем последнюю задачу более точно. Обозначим через M(Ω□Z) множество всех отображений Ω в Z, таких что □``□M(Ω□Z) тогда и только тогда, когда

^{непр}R(□, z) □ R(□``, z),

где R(□``, z) – множество решений уравнения □``(ω) = z, и одновременно |R(□, z)| = |R(□``, z)|.

Предположим, что ω и □``выбираются случайно и равновероятно соответственно из R(□`) и M(Ω□Z). Тогда вероятность P(ω□R(□``, z) / ω□R(□`)) события ω□R(□``, z) является случайной величиной и ее среднее значение P^ (по всем □``□M(Ω□Z)) вычисляется по формуле

$$P\wedge = \frac{{}^{непр}R(\phi,z)}{R(\phi`)} + \frac{|{}^{пр}R(\phi,z)|}{|\Omega| - |{}^{непр}R(\phi,z)|} \cdot \frac{|R(\phi`)| - |{}^{непр}R(\phi,z)|}{|R(\phi`)|}.$$

Поясним данную формулу. Наличие первого слагаемого очевидно. Далее, в указанных условиях каждый элемент ω из Ω\$^{непр}$R(□, z) с равной вероятностью $\frac{|{}^{пр}R(\varphi,z)|}{|\Omega| - |{}^{непр}R(\varphi,z)|}$ может быть решением случайного уравнения □``(ω) = z. Тогда среднее значение числа решений ω из Ω\$^{непр}$R(□, z) принадлежащих R(□`), равно

$$\frac{|{}^{пр}R(\varphi,z)|}{|\Omega| - |{}^{непр}R(\varphi,z)|}|R(\varphi`)| - |{}^{непр}R(\varphi,z)|$$

Представляет интерес подсчет величины

$$T\wedge = \frac{|R(\phi`)|+1}{P\wedge \cdot |R(\phi`)|+1},$$

которая являющейся определенным ориентиром для величины E(T). Несложно показывается, что если

$$P\wedge > \frac{R(\phi,z)}{|\Omega|}, \qquad (22)$$

то

$$T\wedge < \frac{|\Omega|+1}{R(\phi,z)+1}.$$

Основная цель работы состоит в расчете параметров, входящих в формулу для вероятности P^. Этот расчет будет проведен для ряда автоматных уравнений вида (21).

14.2. Определение начального состояния и входного слова автомата по его выходному слову

Вспомогательное отображение □`: Ω□Z, указанное в 14.1 для отображения □: Ω□Z, с криптографической точки зрения трактуется как статистический аналог отображения □□□□. При конкретизации объекта исследования – отображения □□и цели исследования – получения решения поставленной задачи вспомогательное отображение □`: Ω□Z также конкретизируется, в связи с чем проявляется многоликость этого понятия, зависящая от задачи и объекта исследования.

Пусть A = (X, S, Y, $(h_x)_{x\square X}$, $(f_x)_{x\square X}$) – конечный автомат с входным алфавитом X, множеством состояний S, выходным алфавитом Y, частичными функциями перехода $(h_x)_{x\square X}$, h_x:S□S и выхода $(f_x)_{x\square X}$, f_x:S□Y. Через A(s, Q) = y(1), y(2), …, y(k) обозначим выходную последовательность автомата A, отвечающую его входному слову Q = x(1), x(2), …, x(k) и начальному состоянию s□S, а через $A_M(s_1, Q)$ его последовательность состояний

$$A_M(s_1, Q) = s_1, s_2, \ldots, s_k.$$

Положим Ω = S×X^k, Z = Y^k, □□□□-автоматное отображение, определенное автоматом A. Требуется найти одно из решений (s, Q) совместного уравнения

$$A(s, Q) = y(1), y(2), \ldots, y(k).$$

Для решения поставленной задачи выберем вспомогательный автомат $A^* = (X, S, Y, (h^*_x)_{x\square X}, (f^*_x)_{x\square X})$ (вспомогательное отображение □`). При его выборе будем стараться максимально удовлетворить каждому из следующих качественно сформулированных условий:

1. Трудоемкость решения уравнения

$$A^*(s, Q) = y(1), y(2), \ldots, y(k)$$

относительно $(s, Q)\in S\times X^k$ сравнительно мала, либо мала трудоемкость нахождения некоторого множества $R(A^*)$, содержащего множество $R(A^*, y(1), y(2), \ldots, y(k))$ решений указанного уравнения. Указанные трудоемкости в дальнейшем не учитываются.

2. На значительном числе состояний $s\in S$ функции переходов и выходов автоматов A и A* совпадают. Вспомогательный для A автомат A* назовем статистическим аналогом заданного автомата A.

Заметим, что указанные условия для рассматриваемого автомата A могут быть противоречивыми. Такая ситуация является обычной для методов криптографического анализа: стараясь минимизировать трудоемкость решения задачи, мы зачастую уменьшаем надежность метода.

Будем говорить, что пара $(s, x)\in S\times X$ является A,A*-противоречивой, если выполняется хотя бы одно из неравенств

$$h_x s \neq h^*_x s,$$

$$f_x s \neq f^*_x s.$$

В противном случае пара (s, x) является A,A*-непротиворечивой. При $Q = x(1), x(2), \ldots, x(k)$ пара (s, Q), называется A,A*-противоречивой, если хотя бы одна из пар

$$(s, x(1)), (h_{x(1)}s, x(2)), \ldots, (h_{x(k-1)}\ldots h_{x(1)}s, x(k))$$

A,A*-противоречива. В противном случае пара (s, Q) называется A,A*-непротиворечивой.

Для $z = y(1), y(2), \ldots, y(k)\in Y^k$ через R(A, z), R(A*, z) обозначим, соответственно, множества решений (s,Q) уравнений

$$A(s, Q) = z, A^*(s, Q) = z.$$

Положим $R(A, z) = R^{пр}(A, z)\cup R^{непр}(A, z)$, где $R^{пр}(A, z)$, $R^{непр}(A, z)$ соответственно множества A,A*-противоречивых и A,A*-непротиворечивых пар из R(A, z). Дальнейшие построения будут сделаны в предположении, что множество $R^{непр}(A, z)$ – непустое.

Очевидно,

$$R^{непр}(A, z)\subseteq R(A, z)\cup R(A^*, z).$$

При равномерной вероятностной мере на $\Omega = S\times X^k$

$$P_k = P((s, Q)\square R(A, z) / (s,Q)\square R(A^*)) =$$

$$= \frac{|R^{непр}(A,z)|}{|R(A^*)|} + \frac{|(R(A^*)\setminus R^{непр}(A,z))\cap R^{пр}(A,z)|}{|R(A^*)|}.$$

Через $M(S\times X^k\square Y^k)$ обозначим множество всех отображений $\Omega = S\times X^k$ в $Z = Y^k$ таких, что отображение $\square``\square M(S\times X^k\square Y^k)$ тогда и только тогда, если

$$^{непр}R(A, z) \square R(\square``, z),$$

где $R(\square``, z)$ – множество решений уравнения $\square``(\omega) = z$, и одновременно $|R(A, z)| = |R(\square``, z)|$. Предположим, что на $M(S\times X^k\square Y^k)$ и $S\times X^k$ заданы равномерные вероятностные распределения. Тогда

$$P_k^{\wedge} = P(\square``(\omega)=z / \omega\square R(A^*))=$$

$$= \frac{|R^{непр}(A,z)|}{|R(A^*)|} + \frac{|(R(A^*)| - |R^{непр}(A,z)|}{|R(A^*)|}\cdot\frac{|R^{пр}(A,z)|}{|S\times X^k| - |R^{непр}(A,z)|}.$$

Перейдем теперь к методике вычисления параметров

$$|R^{непр}(A,z)|,\ |R^{пр}(A, z)| = |R(A, z)| - |R^{непр}(A, z)|.$$

Обозначим через α_{ab}^{y} число дуг с выходной отметкой y, ведущих из состояния «a» в состояние «b» в графе переходов автомата A, а через $^*\alpha_{ab}^{y}$ число A,A*-непротиворечивых пар из $\{(a,x): x\in X\}$, для которых

$$f_x a = y,\ h_x a = b.$$

Образуем матрицы размером $|S|\times|S|$

$$\alpha^{y} = ||\alpha_{ab}^{y}||,\ ^*\alpha^{y} = ||^*\alpha_{ab}^{y}||$$

и их произведения

$$\alpha^{y(1),y(2),\ldots,y(k)} = ||\alpha_{ab}^{y(1),y(2),\ldots,y(k)}|| = \alpha^{y(1)}\cdot\alpha^{y(2)}\cdot\ldots\cdot\alpha^{y(k)},$$

$$^*\alpha^{y(1),y(2),\ldots,y(k)} = ||^*\alpha_{ab}^{y(1),y(2),\ldots,y(k)}|| = {}^*\alpha^{y(1)}\cdot{}^*\alpha^{y(2)}\cdot\ldots\cdot{}^*\alpha^{y(k)}.$$

Тогда при z = y(1), y(2), …, y(k)

$$|R(A,z)| = \sum_{(a,b)\in S\times S}\alpha_{a,b}^{y(1),\ldots y(k)},\ |R^{непр}(A, z)| = \sum_{(a,b)\in S\times S}{}^*\alpha_{a,b}^{y(1),\ldots y(k)}.$$

Замечание 1. Предложенный метод нельзя считать общим, так как данные вычисления невозможно провести с матрицами больших размеров. В то же время если автомат $A = (X, S, Y, (h_x)_{x\square X}, (f_x)_{x\square X})$ – векторный, то есть X, S, Y наделены алгебраической структурой, например, $X = Y = F_q$ – конечное поле из q элементов, а S – векторное пространство над F_q, то элементы R(A*, z), совпадая с решениями уравнения

$$A^*(s, Q) = z,$$

могут быть представлены в виде решений некоторой системы уравнений вида

$$\varphi_1(s,Q) = 0$$
$$\varphi_2(s,Q) = 0$$
$$\ldots\ldots\ldots\ldots$$
$$\varphi_n(s,Q) = 0$$

В этом случае, не решая эту систему, в качестве множества R(A*) удобно взять множество решений системы каких-нибудь простых уравнений, например, линейных, являющихся следствием указанной системы.

Замечание 2. Напомним, что для нахождения хотя бы одного решения $\omega_0 = (s_0, Q_0)$ уравнения

$$A(s, Q) = z$$

ранее в п. 1 было предложено по очереди для каждой пары (s, Q)□R(A*) проверять равенство (1) и первое ω, для которого оно выполняется (если такое ω существует), объявить решением данного уравнения.

Для нахождения всех решений или части решений уравнения

$$A(s, Q) = z$$

можно поступить следующим образом. Фиксируем, если это возможно, некоторое число N не меньше числа решений данного уравнения. Производим N опробований сначала элементов из множества R(A*), а затем, если $N > |R(A^*)|$, и элементов $S\times X^k$. При этом за N опробований мы определяем множество R(A, z) с некоторой надежностью π(N).

14.3. Определение входного слова автомата по его начальному состоянию и выходному слову

Изложенный в разделе 14.2 метод при некоторой модификации может быть применен для нахождения входного слова Q по заданным начальному состоянию и выходному слову z = y(1), y(2), ..., y(k) автомата $A = (X, S, Y, (h_x)_{x\square X}, (f_x)_{x\square X})$. Требуется найти хотя бы одно решение уравнения A(s, Q) = z относительно неизвестного $Q\in X^k$. При этом предполагается известной мощность |R(A, z)| множества R(A, z) решений данного уравнения. В обозначениях раздела 5.1 мы здесь положили

$$\Omega = X^k,\ Z = Y^k,\ \square(\omega) = A(s, Q),\ Q\in X^k.$$

Для решения этой задачи строим вспомогательный автомат A* – статистический аналог автомата A:

$$A^* = (X, S, Y, (h^*_x)_{x\square X}, (f^*_x)_{x\square X}).$$

Назовем входное слово Q = x(1), x(2), …, x(k) A,A*,s-непротиворечивым, если пара (s,Q) A,A*-непротиворечива и A,A*,s-противоречивым, если пара (s, Q) A,A*,s-противоречива.

Через R(A, s, z), и R(A*, s, z) обозначим, соответственно, множества решений Q уравнений

$$A(s, Q) = z, A^*(s, Q) = z.$$

Полагаем, что

$$R(A, s, z) = R^{пр}(A, s, z) \cup R^{непр}(A, s, z),$$

где $R^{пр}(A, s, z)$, $R^{непр}(A, s, z)$ соответственно множества A,A*,s-противоречивых и A,A*,s-непротиворечивых входных слов из R(A, s, z). Считаем известным множество R(A*), для которого

$$R(A^*, s, z) \subseteq R(A^*),$$

и предполагаем, что множество $R^{непр}(A, s, z)$ – непустое. При равновероятном распределении на X^k, очевидно

$$P_k = P((s, Q) \square R(A, s, z) / Q \square R(A^*)) =$$

$$= \frac{|R^{непр}(A,s,z)|}{|R(A^*)|} + \frac{|(R(A^*) \setminus R^{непр}(A,s,z)) \cap R^{пр}(A,s,z)|}{|R(A^*)|}.$$

Через $M(X^k \square Y^k)$ обозначим множество всех отображений $\Omega = X^k$ в $Z = Y^k$ таких, что отображение $\square``$ $\square$ $M(X^k \square Y^k)$ тогда и только тогда, если

$$^{непр}R(A, s, z) \square R(\square``, z),$$

где $R(\square``, z)$ – множество решений уравнения $\square``(\omega) = z$, и одновременно $|R(A, z)| = |R(\square``, z)|$. Предположим, что на $M(X^k \square Y^k)$ и X^k заданы равномерные вероятностные меры. Получаем

$$P^{\wedge}_{s,k} = P(\square``(\omega) = z / \omega \square R(A^*)) =$$

$$= \frac{|R^{непр}(A,s,z)|}{|R(A^*)|} + \frac{|R(A^*)| - |R^{непр}(A,s,z)|}{|R(A^*)|} \cdot \frac{|R^{пр}(A,s,z)|}{|X|^k - |R^{непр}(A,s,z)|}.$$

Нахождение входного слова Q (или всех слов Q), для которого A(s, Q) = z, проводится с помощью алгоритмов, полностью аналогичных приведенным ранее, в разделах 14.1, 14.2. Так же используется и вероятность $P^{\wedge}_{s,k}$ для расчета средней трудоемкости алгоритмов.

Несколько замечаний следует сделать относительно расчета |R(A, s, z)| и $|R^{непр}(A, s, z)|$ и рекомендаций по выбору A*. Именно при z = y(1), y(2), ..., y(k)

$$|R(A, s, z)| = \sum_{b \in S} a_{sb}^{y(1),\ldots,y(k)},$$

$$|R^{непр}(A, s, z)| = \sum_{b \in S} {}^{*}a_{sb}^{y(1),\ldots,y(k)}.$$

Здесь использованы обозначения α_{ab}^{y}, ${}^{*}\alpha_{ab}^{y}$ из раздела 14.2.

Выбор наилучшего статистического аналога для автомата A является сложной самостоятельной задачей. В то же время очевидно, что выбирать статистический аналог A* автомата A следует исходя из следующих соображений:

1. Трудоемкость нахождения множества $R(A^*) \supseteq R^*(A,s,z)$ достаточно мала.
2. На значительном числе состояний функции переходов и выходов автоматов A* и A совпадают.

14.4. Определение входного слова автомата по его начальному и заключительному состояниям

Рассмотрим задачу: для заданной пары состояний $a, b \in S$ автомата $A = (X, S, Y, (h_x)_{x \square X}, (f_x)_{x \square X})$ определить все слова $Q = x(1), \ldots, x(k)$ (хотя бы одно слово Q), для которых

$$h_{x(k)} h_{x(k-1)} \ldots h_{x(1)} a = b$$

Таким образом, мы рассматриваем общую задачу при ее параметрах

$$\Omega = X^k,\ Z = S \times S,\ \square(\omega) = (a, h_{x(k)} h_{x(k-1)} \ldots h_{x(1)} a).$$

В ряде случаев трудоемкость решения этой задачи тотальным методом, как и предыдущих задач (см. п. 14.2, 14.3), можно уменьшить за счет предварительного указания множества R, так сказать, «наиболее вероятных» слов, переводящих a в b.

В данном пункте в отличие от предыдущих разделов для заданных автоматов без выхода $A = (X, S, Y, (h_x)_{x \square X})$ $A^* = (X, S, Y, (h^*_x)_{x \square X})$ пару $(s, x) \in S \times X$ назовем *непротиворечивой*, если

$$h_x s = h^*_x s,$$

и противоречивой, в противном случае. Слово $Q = x(1), \ldots, x(k)$ назовем s-непротиворечивым, если все пары

$$(s, x(1)), (h_{x(1)} s, x(2)), \ldots, (h_{x(k-1)} \ldots h_{x(1)} s, x(k))$$

непротиворечивы. В противном случае слово Q назовем s-противоречивым.

Обозначим через R(A, a, b), R(A*, a, b) множества входных слов $Q \in X^k$, переводящих a в b в автомате A и A* соответственно. Множество R(A, a, b) представимо в виде

$$R(A, a, b) = R^{непр}(A, s, z) \cup R^{а\text{-}пр}(A, a, b),$$

где $R^{а\text{-}непр}(A, a, b)$ множество а-непротиворечивых слов из R(A, a, b), а $R^{а\text{-}пр}(A, a,b)$ – множество а-противоречивых слов из R(A, a, b). Пусть R – некоторое подмножество X^k, для которого $R(A, a, b) \subseteq R$ и множество $R^{непр}(A, s, z)$ – непустое.

Предположим, что на вход автомата A подаются случайно и равновероятно слова из X^k. Тогда

$$P_k^{ab} = P(Q \square R(A,a,b) / Q \square R) =$$

$$= \frac{|R^{непр}(A,a,b)|}{|R|} + \frac{|(R \setminus R^{непр}(A,a,b)) \cap R^{пр}(A,a,b)|}{|R|}.$$

Через $M_a(X^k \square S)$ обозначим множество всех отображений $\Omega = X^k$ в Z = S таких, что отображение $\square_a$`` $\square$ $M_a(X^k \square S)$ тогда и только тогда, если

$$\square_a``(Q) = b$$

для всех $Q \in R^{а\text{-}пр}(A,a,b)$ и одновременно $|R(A,a,b)|=|R(\square``,b)|$. Предположим, что на $M(X^k \square S)$ и X^k заданы равномерные вероятностные меры. Тогда

$$\hat{P}_k^{ab} = P(\square``(Q) = b / Q \square R) =$$

$$\frac{|R^{a-непр}(A,a,b)|}{|R|} + \frac{|R| - |R^{a-непр}(A,a,b)|}{|R|} \cdot \frac{|R^{a-пр}(A,a,b)|}{|X|^k - |R^{a-непр}(A,a,b)|}. \qquad (23)$$

Для нахождения хотя бы одного слова Q = x(1), ..., x(k), для которого

$$h_{x(k)} h_{x(k-1)} \ldots h_{x(1)} a = b,$$

производим опробование с возвращением элементов множества R. Трудоемкость этого алгоритма (в среднем числе опробований) не превосходит $(\hat{P}_k^{ab})^{-1}$ (без учета трудоемкости нахождения R).

Укажем рекуррентные соотношения для расчета величин

$$|R(A,a,b)|, |R^{а\text{-}непр}(A, a, b)|.$$

Обозначим через a_{ab}^k число слов длины k ведущих из состояния a в состояние b в графе переходов автомата A, через $*a_{ab}^k$ число а-непротиворечивых слов длины k ведущих из состояния a в состояние b. Таким образом, в частности, a_{ab}^1 есть число элементов $x \in X$, для которых $h_x a = b$, а $*a_{ab}^1$ есть число элементов $x \in X$, для которых

$h_x a = b$, $h^*_x a = b$. Образуем матрицы $\|a_{ab}^k\|$ и $\|{}^*a_{ab}^k\|$ размеров $|S|\times|S|$. Непосредственно проверяется, что

$$\|a_{ab}^{k-1}\|\cdot\|a_{ab}^1\| = \|a_{ab}^k\|,$$

$$\|{}^*a_{ab}^{k-1}\|\cdot\|{}^*a_{ab}^1\| = \|{}^*a_{ab}^k\|.$$

Таким образом,

$$\|a_{ab}^k\| = \|a_{ab}^1\|^k,\ \|{}^*a_{ab}^k\| = \|{}^*a_{ab}^1\|^k$$

и

$$|R(A,a,b)| = a_{ab}^k,\ |R^{\text{а-непр}}(A,a,b)| = {}^*a_{ab}^k.$$

Данный метод нельзя признать универсальным, так как он не позволяет работать с матрицами больших размеров. Приведем для данной задачи один из возможных способов выбора множества R. Отметим, что он может быть использован и в задачах, изложенных ранее. Рассмотрим аффинный автомат $A``= (X, S``, (h``_x)_{x\in X})$, где $X = F_q$-конечное поле из q элементов, $S`` = V_n$ – векторное пространство размерности n над полем F_q ,

$$h_x s = Qs + d\cdot x,$$

где Q-линейное преобразование V_n, а d – некоторый вектор из V.

В качестве статистического аналога $A^* = (X, S, Y, (h^*_x)_{x\square X})$ автомата A рассмотрим автомат $A`` = (X, S``, (h``_x)_{x\in X})$ такой, что $\psi b = Q^k\psi a + \sum_{m=2}^{k} Q^{k-m+1} d\cdot x_{m-1} + d\cdot x_k$. нашлось ψ – сюръективное отображение S в S», осуществляющее гомоморфизм по состояниям автомата A в A``. В качестве множества R возьмем множество решений уравнения

$$h``_{x(k)}h``_{x(k-1)}\ldots h``_{x(1)}\ \psi a=\psi b,$$

которое, в нашем случае, является линейным и имеет вид ???

Очевидно, $R\supseteq R(A^*, a, b)$, так как ψ осуществляет гомоморфизм автоматов A в A».

Следующие теоремы легко доказываются стандартными средствами теории автоматов.

Теорема 1. Для автоматов A, A* тогда и только тогда для любого k найдутся a, b из S, для которых

$$R^{\text{а-непр}}(A, a, b) \neq \varnothing,$$

если для некоторого $s\in S$ найдется s-непротиворечивое слово Q = x(1), x(2), …, x(k) переводящее в графе переходов автомата A s в s, то есть

$$h_{x(k)}h_{x(k-1)}\ldots h_{x(1)}s = s.$$

Теорема 2. Пусть R = R(A*, a, b), A ≠ A* и A автомат, для которого существует некоторое число D со свойством: при любой паре (s,s')∈S×S существует входное слово длины D, ведущее из s в s'. Тогда для любой пары состояний (a,b)∈S×S при любом k > 2D

$$P_k^{ab} < 1.$$

14.5. Определение входного слова автомата по его начальному и заключительному состояниям

Будем использовать обозначения раздела 14.4. В качестве примера приложения приведенных там результатов рассмотрим регистр сдвига.

Пусть V_n – векторное пространство размерности n над полем F_2 из двух элементов, $f(x_1, \ldots, x_n)$ – некоторая двоичная функция, $X = F_2$, $S = V_n$

$$h_0: V_n \to V_n,\ h_0(x_1, \ldots, x_n)) = (x_2,\ldots,x_n,f(x_1, \ldots, x_n))$$

$$h_1: Vn \to Vn,\ h_1(x_1, \ldots, x_n)) = (x_2, \ldots, x_n,f(x_1, \ldots, x_n)\oplus 1).$$

Каждой функции f поставим в соответствие автомат A(f) = = (X = F_2, S = V_n,(h_0, h_1)). В качестве статистического аналога A* автомата A(f) рассмотрим автомат A(f*) для некоторой двоичной функции f*. Напомним, что автомат A = (X, S, $(h_x)_{x\square X}$) называется перестановочным, если $(h_x)_{x\square X}$ – биекции S в S. Справедлив следующий аналог теоремы 2.

Теорема 3. Пусть A = A(f), A* = A(f*) регистры сдвига и A(f) ≠ A(f*), R = R(A*, a, b). Тогда

1) для любой пары состояний a, b при любом k > 2n–1

$$\hat{}P_k^{ab} < 1;$$

2) если дополнительно A(f), A* = A(f`) перестановочные автоматы, то для любой пары состояний a, b при любом k>2n–2

$$\hat{}P_k^{ab} < 1.$$

Доказательство. Докажем утверждение 2. Утверждение 1 доказывается аналогично. Пусть (x(1), …, x(n)) – некоторый произвольный элемент из S и пусть для определенности k = 2n–l, тогда случай k >2n–1 доказывается аналогично. Предположим, что $\hat{}P_k^{ab}$ = = 1. Тогда $R^{а\text{-}непр}$(A, a, b) = R(A, a, b). Положим a = a(1), …, a(n); b = b(1), …, b(n). Известно, что регистр сдвига A(f) является перестановочным автоматом в том и только в том случае, если его функция $f(x_1, x_2, \ldots, x_n)$ представима в виде $f(x_1, x_2, \ldots, x_n) = x_1+g(x_2, \ldots, x_n)$.

Связи с чем положим $f(x_1, x_2, \ldots, x_n) = x_1+g(x_2, \ldots, x_n)$, $f^*(x_1, x_2, \ldots, x_n) = x_1+g^*(x_2, \ldots, x_n)$. Выберем входные слова $\mathfrak{I} = i(1), i(2), \ldots, i(n-1)$, $\mathfrak{I}` = i`(1), i`(2), \ldots, i`(n-1), i`(n)$ автоматов A(f), A(f*) исходя из равенств

$$i(1) = a(1)+g(a(2), \ldots, a(n))+x(2)$$
$$i(2) = a(2)+g(a(3), \ldots, a(n), x(2))+x(3)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$i(n-1) = a(n-1)+g(a(n),x(2), \ldots, x(n-1))+x(n);$$
$$i`(1) = a(n)+g(x(2), \ldots, x(n))+b(1)$$
$$i`(2) = x(2)+g(x(3), \ldots, x(n), b(1))+b(2)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$i`(n) = x(n)+g(b(1), \ldots, b(n-1))+b(n)$$

Тогда

$$h_{i(n-1)}\ldots h_{i(1)}(a(1), \ldots, a(n)) = (a(n), x(2), \ldots, x(n))$$
$$h_{i`(n)}\ldots h_{i`(1)}\,(a(n), x(2), \ldots, x(n)) = (b(1), \ldots, b(n))$$

и слово $\mathfrak{I}\mathfrak{I}` = i(1), i(2), \ldots, i(n-1), i`(1), i`(2), \ldots, i`(n-1), i`(n)$ принадлежит множеству $(A, a, b) = R^{\text{а-непр}}(A, a, b)$. Следовательно, пара: состояние $(a(n), x(2), \ldots, x(n))$ и входной символ $i`(1)$ непротиворечива, то есть

$$h_{i`(1)}\,(a(n), x(2), \ldots, x(n)) = h^*_{i`(1)}\,(a(n), x(2), \ldots, x(n)),$$

или

$$a(n) + i`(1) + g(x(2), \ldots x(n)) = a(n) + i`(1) + g^*(x(2), \ldots x(n)),$$

или

$$g(x(2), \ldots x(n)) = g^*(x(2), \ldots x(n)).$$

Так как $(x(2), \ldots x(n))$ выбрано произвольно, то A(f) = A(f*). Полученное противоречие доказывает справедливость теоремы.

Замечание 3. Полезно отметить, что для регистра сдвига при $k \geq n$

$$|R(A, a, b)| = a_{ab}^k = 2^{k-n},\ R^{\text{а-пр}}(A, a, b) = 2^{k-n} - {}^*a_{ab}^k$$

при любых a, b.

Рассмотрим один из возможных способов выбора множества R при k>n.

Пусть V_n, $V_{n``}$ – векторные пространства размерностей n, n`` над полем F_2, $A``(f``) = (X = F_2, S = V_{n``}, (h``_0, h``_1))$-линейный регистр сдвига, (f`` – линейная функция),

ψ: $V_n \to V_{n``}$ – сюръективное отображение, осуществляющее гомоморфизм по состояниям регистра A(f*) на A`` = A``(f``).

В качестве множества R возьмем множество R(A``, ψa, ψb) решений (i(1), i(2), …, i(k)) уравнения

$$h``_{i(k)}h``_{i(k-1)}\ldots h``_{i(1)}\psi a = \psi b.$$

При этом очевидно, что R⊇R(A*, a, b). Положим

$$\psi a = a`` = (a``_1, \ldots, a``_n),\ \psi b = c = (c_{2n+m}, \ldots, c_{3n+m-1}),\ k = n+m+1.$$

Рассмотрим вспомогательную систему уравнений

$$i(1)+f``(a``_1, \ldots, a``_n)+x_{n+1} = 0$$
$$i(2)+f``(a``_2, \ldots, a``_n,x_{n+1})+x_{n+2} = 0$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$i(n)+f``(a``_n,x_{n+1}, \ldots, x_{2n-1})+x_{2n} = 0$$
$$i(n+1)+f``(x_{n+1}, \ldots, x_{2n})+x_{2n+1} = 0$$
$$i(n+2)+f``(x_{n+2}, \ldots, x_{2n+1})+x_{2n+2} = 0$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$i(n+m)+f``(x_{n+m}, \ldots, x_{2n+m-1})+x_{2n+m} = 0$$
$$i(n+m+1)+f``(x_{n+m+1},\ldots,x_{2n+m-1},c_{2n+m})+c_{2n+m+1} = 0$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$i(2n+m)+f``(x_{2n+m-1}, c_{2n+m}, \ldots, c_{3n+m-2})+c_{3n+m-1} = 0$$

Заметим, что R(A``, a, b) есть объединение решений этой системы при всех фиксациях промежуточных переменных $x_{n+1}$, …, $x_{2n+m-1}$. Исключим промежуточные переменные из этой системы следующим способом. Из первого уравнения находим $x_{n+1}$ = $i(1)+f``(a``_1, \ldots, a``_n)$ и подставляем в остальные уравнения, содержащие x_{n+1}, из второго уравнения находим значение x_{n+2} и подставляем это выражение в уравнения, содержащие x_{n+2}, и так далее. В результате мы получим линейную систему уравнений относительно неизвестных i(1), i(2), …, i(k). Решая ее, мы найдем множество R. Оценим теперь сверху величину $|R^{a-непр}(A,a,b)|$, входящую в формулу

$$\hat{}P_k^{ab} = \frac{|R^{a-непр}(A,a,b)|}{|R|} + \frac{|R|-|R^{a-непр}(A,a,b)|}{|R|}\cdot\frac{2^{k-n}-|R^{a-непр}(A,a,b)|}{2^k-|R^{a-непр}(A,a,b)|}.$$

для вероятности $\hat{}P_k^{ab}$ при k>n в случае, если значения функций f, f* регистров сдвига A(f), A*(f*) отличаются ровно на t наборах переменных. Оценим сначала величину

$$\frac{|R^{a-непр}(A,a,b)|}{2^{k-n}} = P,$$

которую можно трактовать как вероятность выбора а-непротиворечивого слова при случайном и равновероятном выборе слов из множества R(A, a, b). Рассмотрим вспомогательную

последовательность $x = x_1, x_2, \ldots, x_{k+n}$ переменных, которым придадим следующие значения

$$(x_1, \ldots, x_n) = a = (a_1, \ldots, a_n),$$
$$(x_{k+1}, \ldots, x_{k+n}) = (b_1, \ldots, b_n)$$
$$x_{n+j} = i(j)+f(x_j, \ldots, x_{n+j-1}),\ j\in\{1, \ldots, k\}.$$

Вектора $(x_L, \ldots, x_{L+n-1})$, $L\in\{1, \ldots, k+1\}$ являются состояниями регистра сдвига A(f) при входной последовательности i(1), i(2), …, i(k). Заданное распределение вероятности на R(A, a, b) индуцирует распределение вероятности и на значениях переменных x_j, $j\in\{n+1, \ldots, k\}$. Из законов функционирования регистра сдвига A(f) следует, что x_{n+j}, $j\in\{1, \ldots, k-n\}$ случайны, независимы и равновероятны. Обозначим через U – множество состояний s регистра A(f), для которых $f(s) \neq f^*(s)$. Обозначим через r целую часть величины $\frac{k-2n}{n}$. Тогда P не превосходит вероятности того, что ни один из векторов $(x_{jn+1}, \ldots, x_{(j+1)n})$, $j\in\{1, \ldots, r\}$ не принадлежит U. Последняя вероятность равна $\left(1-\frac{t}{2^n}\right)^r$. Поэтому $|R^{\text{а-непр}}(A, a, b)|\le\left(1-\frac{t}{2^n}\right)^r\cdot 2^{k-n}$. Представляет интерес получение оценки вероятности ${}^{\wedge}P_k^{ab}$. Мы высказываем гипотезу о том, что ${}^{\wedge}P_k^{ab}$ приблизительно равна величине

$$\frac{\left(1-\frac{t}{2^n}\right)^{k-2n}\cdot 2^{k-n}}{|R|}+\frac{|R|-\left(1-\frac{t}{2^n}\right)^{k-2n}\cdot 2^{k-n}}{|R|}\cdot\frac{2^{k-n}-\left(1-\frac{t}{2^n}\right)^{k-2n}\cdot 2^{k-n}}{2^k-\left(1-\frac{t}{2^n}\right)^{k-2n}\cdot 2^{k-n}},$$

полученной при расчете ${}^{\wedge}P_k^{ab}$ в предположении независимости состояний $(x_{j+1}, \ldots, x_{k+n})$ регистра A(f), $j\in\{n+1, \ldots, k\}$, так как в этом случае можно считать, что

$$|R^{\text{а-непр}}(A,a,b)|=\left(1-\frac{t}{2^n}\right)^{k-2n}\cdot 2^{k-n}.$$

14.6. Метод сведения изложенных задач к задачам решения системы уравнений с искаженными правыми частями

Приведем метод сведения изложенных задач к задачам решения системы уравнений с искаженными правыми частями.

Рассмотрим первую задачу – задачу нахождения решения (или всех решений) уравнения A(s, Z) = y(1), y(2), …, y(k) относительно пар (s, Z). Возьмем в качестве статистического аналога автомата A =

$(X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ векторный автомат $A` = (X, S, Y, (h`_x)_{x\in X}, (f`_x)_{x\in X})$, для которого система уравнений

$$f`_{x(1)}s = y(1)$$
$$f`_{x(2)}h`_{x(1)}s = y(2)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$f`_{x(k)}h`_{x(k-1)}\ldots h`_{x(1)}s = y(k)$$

является линейной относительно i(1), i(2), …, i(k), s. Тогда вероятность

$$P_L = P(f_{x(L)}h_{x(L-1)}\ldots h_{x(1)}s = f`_{x(L)}h`_{x(L-1)}\ldots h`_{x(1)}s)$$

того, что при случайном выборе пары (s; x(1), x(2), …, x(L)) значения функций

$$f_{(L)}h_{x(L-1)}\ldots h_{x(1)},\ f`_{x(L)}h`_{x(L-1)}\ldots h`_{x(1)}$$

на них совпадут, может быть рассчитана по формуле

$$P_L = P\begin{pmatrix} f_{x(L)}h_{x(L-1)}\ldots h_{x(1)}s = \\ f`_{x(L)}h`_{x(L-1)}\ldots h`_{x(1)}s \end{pmatrix}\Big|(s,x(1),\ldots,x(L)\in R^{непр}(A,y))\Big)\times P\Big((s,x(1),\ldots,x(L)\in R^{непр}(A,y)\Big)+$$

$$+P\Big(f_{x(L)}h_{x(L-1)}\ldots h_{x(1)}s = f`_{x(L)}h`_{x(L-1)}\ldots h`_{x(1)}s\Big|(s,x(1),\ldots,x(L)\in R^{пр}(A,y)\Big)\times$$
$$P\Big((s,x(1),\ldots,x(L)\in R^{пр}(A,y)\Big)=$$
$$=P\Big((s,x(1),\ldots,x(L)\in R^{непр}(A,y)\Big)+\frac{1}{|Y|}P\Big((s,x(1),\ldots,x(L)\in R^{пр}(A,y)\Big)=$$
$$\frac{|R^{непр}(A,y)|}{|X|^L|S|}+\frac{1}{|Y|}\left(1-\frac{|R^{непр}(A,y)|}{|X|^L|S|}\right)$$

Здесь мы использовали предположение о том, что при любом

$$y\in Y$$

$$P\Big(f`_{x(L)}h`_{x(L-1)}\ldots h`_{x(1)}s = y,/(s,x(1),\ldots,x(L)\in R^{пр}(A,y)\Big)=\frac{1}{|Y|}.$$

Теперь для решения данной системы уравнений

$$f_{x(1)`}s = y_1$$
$$f_{x(2)}h_{x(1)}s = y_2$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$f_{x(k)}h_{x(k-1)}\ldots h_{x(1)}s = y_k$$

можно использовать теорию решения системы линейных уравнений с искаженными правыми частями [20]:

$$f`_{x(1)`}s = y`_1$$
$$f`_{x(2)}h`_{x(1)}s = y`_2 \qquad .$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$f`_{x(k)}h`_{x(k-1)}\ldots h`_{x(1)}s = y`_k$$

Вероятность искажения правой части L-го уравнения определяется из соотношений

$$P\left(y'_L = y_L\right) = P_L,$$

$$P\left(y'_l = y\right) - \frac{1-P_L}{|Y|-1},\ для\ y \neq y_L.$$

Аналогично могут решаться и другие рассмотренные выше задачи. Некоторую специфику имеет решение уравнения

$$h_{x(k)} \ldots h_{x(1)} a = b.$$

В этом случае в качестве автомата $A` = (X, S, Y, (h`_x)_{x \in X},)$ следует взять автомат, для которого уравнение

$$h`_{x(k)} \ldots h`_{x(1)} a = b$$

является линейным относительно x(1), …, x(k) при любом $b \in S$. Через H обозначим событие $h_{x(k)} \ldots h_{x(1)} a = h`_{x(k)} \ldots h`_{x(1)} a$ при случайном и равномерном выборе $x(1), \ldots, x(k) \in X^k$. Имеем

$$P(H) = P\left(H \middle| x(1),\ldots,x(k)_k \in \bigcup_{c \in S} R^{a-непр}(A,a,c)\right) \times P\left(x(1),\ldots,x(k)_k \in \bigcup_{c \in S} R^{a-непр}(A,a,c)\right) +$$

$$+P\left(H \middle| x(1),\ldots,x(k) \notin \bigcup_{c \in S} R^{a-непр}(A,a,c)\right) \times P\left(x(1),\ldots,x(k) \notin \bigcup_{c \in S} R^{a-непр}(A,a,c)\right) =$$

$$P\left(x(1),\ldots,x(k)_k \in \bigcup_{c \in S} R^{a-непр}(A,a,c)\right) + \frac{1}{|S|} P\left(x(1),\ldots,x(k) \notin \bigcup_{c \in S} R^{a-непр}(A,a,c)\right) =$$

$$= \frac{1}{|X|^k} \sum_{c \in S} \left|R^{a-непр}(A,a,c)\right| + \frac{1}{|S|}\left(1 - \frac{1}{|X|^k} \sum_{c \in S} \left|R^{a-непр}(A,a,c)\right|\right)$$

Здесь мы использовали дополнительное предположение о том, что при любом $s \in S$

$$P\left(h`_{x(k)} \ldots h`_{x(1)} a = s \middle| x(1),\ldots,x(k) \in R^{a-непр}(A,a,c)\right) = \frac{1}{|S|}$$

Поиск решений уравнения $h_{x(k)} \ldots h_{x(1)} a = b$ сводится к применению известных методов поиска решений линейного уравнения с искаженной правой частью

$$h`_{x(k)} \ldots h`_{x(1)} a = b`;$$

$$P(b = b`) = P(H);$$

$$P(b' = c) = \frac{1-P(H)}{|S|-1} \text{ при } c \neq b.$$

Часть 4. МОДЕЛИ АВТОМАТОВ НА ОСНОВЕ ОБОБЩЕНИЯ ПОНЯТИЯ ГОМОМОРФИЗМА АВТОМАТОВ

Ранее отмечалось, что для анализа шифрсистем особое значение имеет возможность использования их приближенных моделей. Одно из направлений построения таких моделей основано на использовании понятия гомоморфизма алгебр и конечных автоматов [29]. В данной части работы изложены результаты по построению обобщенных гомоморфных образов автоматов, получаемых при бинарных отношениях на автоматных множествах, согласованных с законами функционирования автоматов. Основные результаты работы опубликованы в [5]. С возможными практическими приложениями результатов можно ознакомиться в [19].

Глава 15. МНОГОЗНАЧНЫЕ ГОМОМОРФИЗМЫ КОНЕЧНЫХ АВТОМАТОВ

Дается обобщение понятия гомоморфизма автоматов, основанное на замене отображений в определении гомоморфизма автоматов на бинарные отношения. Указаны возможные образы автомата при таком обобщенном гомоморфизме.

15.1. Обозначения

Для $P = x(1), x(2), ..., x(k)$ из X^* положим $h_P s = h(P, s) = h_{x(k)}...h_{x(1)}s$. Через $A(s, P) = y(1), y(2), ..., y(k)$, как и ранее, будем обозначать выходное слово автомата A, соответствующее входному слову $P = x(1), x(2), ..., x(k)$ и начальному состоянию $s \in S$.

Для $M \subseteq S$, $N \subseteq X$ полагаем: $h_N(M) = h(N, M) = \{s' : h_x s = s', s \in M, x \in N\}$, $f_N(M) = f(N,M) = \{y : f_x s = y, s \in M, x \in N\}$.

Пусть $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$, $A` = (X`, S`, Y`, (h`_{x`})_{x` \in X`}, (f`_{x`})_{x` \in X`})$ – конечные автоматы и ψ, φ, χ – бинарные отношения, $\psi \subseteq X \times X`$, $\varphi \subseteq S \times S`$, $\chi \subseteq Y \times Y`$. Ниже будет использован ряд понятий и обозначений теории отношений [54]. Факт $(x, x`) \in \psi$ будем также записывать в виде $x\psi x`$. Вводим обозначения

$$Пр_1\psi = \{x: x\psi x` \text{для некоторого } x` \text{ из } X`\};$$

$$Пр_2\psi = \{x`: x\psi x` \text{ для некоторого } x \text{ из } X\}.$$

Аналогично определяются $Пр_1\varphi$, $Пр_1\chi$ и $Пр_2\varphi$, $Пр_2\chi$.

Положим также

$$\psi^{-1}(x`) = \psi^{-1}x`=\{x: x\psi x`, x\in X\};$$

$$\psi(x) = \psi x = \{x`: x\psi x`, x`\in X`\}.$$

Аналогичные обозначения используем для бинарных отношений φ и χ.

15.2. Многозначные гомоморфизмы автоматов

Определение 1. Тройка (ψ, φ, χ) называется многозначным гомоморфизмом (МГ) автомата A на автомат A`, если

1) $Пр_1\psi = X$, $Пр_1\varphi = S$, $Пр_2\psi = X`$, $Пр_2\varphi = S`$;
2) для любых $x`\in X`$, $s`\in S`$

а) $h_{\psi^{-1}(x`)}\phi^{-1}s`\subseteq \phi^{-1}h`_{x`}s`$,

б) $f_{\psi^{-1}(x`)}\phi^{-1}s`\subseteq \chi^{-1}f`_{x`}s`$.

Автомат A` называется образом многозначного гомоморфизма (ψ, φ, χ) автомата A.

Условие 2 данного определения требует, что бы образы элементов, находящихся в бинарном отношении, также состояли в этом бинарном отношении.

Множество всех МГ A на A` обозначим через МГ(A, A`).

Замечание 1. Условие 1 в определении 1 не играет принципиальной роли. Полученные ниже результаты легко обобщаются на случай отказа от условия 1 в определении 1. В этом случае образы МГ могут быть частичными автоматами. Отметим, что понятие многозначного гомоморфизма в частном случае, когда ψ, χ – отображения совпадают с понятием слабого гомоморфизма, введенного в работе [51].

Для автоматов A, A` через

$$A_M = (X, S, Y, (h_x)_{x\in X}),\ A`_M = (X`, S`, Y`, (h`_{x`})_{x`\in X`})$$

обозначим соответствующие им автоматы без выходов.

Двойку отношений $\psi^\wedge$, $\varphi^\wedge$ на $X\times X`$, $S\times S`$ естественно называть многозначным гомоморфизмом A_M на $A`_M$ и писать $(\psi^\wedge, \varphi^\wedge)\in МГ(A_M, A`_M)$, если для нее выполняется условие 1 и условие 2а определения 1. Очевидно, если $(\psi, \varphi, \chi)\in МГ(A, A`)$, то $(\psi, \varphi)\in МГ(A_M, A`_M)$.

Лемма 1. Пусть $(\psi^\wedge, \varphi^\wedge) \in МГ(A_M, A`_M)$ и $\chi^\wedge$ – бинарное отношение на $Y \times Y`$, определенное условием $y\chi^\wedge y`$, $y \in Y$, $y` \in Y`$ тогда и только тогда, если существуют $x \in X$, $s \in S$, $x` \in X`$, $s` \in S`$, для которых

$$x\psi x`,\ s\varphi s`,\ f_x s = y,\ f`_{x`} s` = y`.$$

Тогда

$$(\psi^\wedge, \varphi^\wedge, \chi^\wedge) \in МГ(A, A`).$$

Если $(\psi^\wedge, \varphi^\wedge, \chi) \in МГ(A, A`)$, то $\chi^\wedge \subseteq \chi$. Утверждение леммы непосредственно вытекает из из определения 1.

При фиксированном автомате A указанное в лемме отношение $\chi^\wedge$ зависит от $A`_M$ и частичных функций выхода $(f`_{x`})_{x` \in X`}$, в связи с чем удобно в ряде случаев пользоваться его новым обозначением $\chi^\wedge = \chi(A`)$.

Пусть МГ(A) ($МГ(A_M)$) – множество всех образов многозначных гомоморфизмов автомата A (A_M).

Следствие леммы 1. Автомат $A` \in МГ(A)$ тогда и только тогда, если $A`_M \in МГ(A_M)$.

Замечание 2. Данное утверждение в частности сводит задачу поиска образов многозначных гомоморфизмов автомата A к конструктивному описанию образов автомата A_M. Основную роль при таком описании ниже будут играть следующие обобщения известных понятий конгруэнции автомата и фактор-автомата.

Определение 2. Многозначным покрытием (МП) автомата $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$ или кратко МП(A) называется система из трех семейств множеств:

$$(X_j, j \in \{1, ..., m\}), (S_j, j \in \{1, ..., n\}), (Y_j: j \in \{1, ..., L\}),$$

удовлетворяющих двум условиям:

1) $X_j \subseteq X$, $\bigcup_{j=1}^{m} X_j = X$, $X_j \neq \varnothing$, $j \in \{1, ..., m\}\}$,

$S_j \subseteq S$, $\bigcup_{j=1}^{n} S_j = S$, $S_j \neq \varnothing$, $j \in \{1, ..., n\}\}$,

$Y_j \subseteq Y$, $j \in \{1, ..., L\}$;

2) для любых $j \in \{1, ..., m\}$, $k \in \{1, ..., n\}$ существуют $k` \in \{1, ..., n\}$ и $c \in \{1, ..., L\}$, при которых

а) $h_{X_j} S_k \subseteq S_{k`}$; б) $f_{X_j} S_k \subseteq Y_c$.

Если в условиях 2а, 2б индексы k`, c определены однозначно для каждой пары (j, k), то МП(A) назовем согласованным многозначным покрытием автомата A или кратко СМП(A).

Аналогично вводится понятие МП(A_M) и СМП(A_M) для автомата без выхода A_M. Здесь должны быть выполнены условия 1, 2а определения 2.

Замечание 3. Акцентируем внимание на то, что в определении 2 любое семейство множеств может содержать одинаковые множества, например, возможно, что $X_j = X_{j`}$ при некоторых $j, j` \in \{1, ..., m\}\}$, аналогично для S_j и Y_j.

Определение 3. Для МП(А):

$$(X_j, j\in\{1, ..., m\}), (S_j, j\in\{1, ..., n\}), (Y_j, j\in\{1, ..., L\})$$

обозначим через А/МП(А) и назовем многозначным фактором МФ(А) автомата А по МП(А) семейство автоматов с входным алфавитом $X^\wedge=\{X_j, j\in\{1, ..., m\}\}$, множеством состояний $S^\wedge = \{S_j, j\in\{1, ..., n\}\}$, выходным алфавитом $Y^\wedge = \{Y_j, j\in\{1, ..., L\}\}$. Здесь элементы алфавитов пронумерованы и определены нижними индексами, в частности, $|X^\wedge| = m$, $|S^\wedge| = n$, $|Y^\wedge| = L$. Автомат $A^\wedge = (X^\wedge, S^\wedge, Y^\wedge, h^\wedge, f^\wedge)$ принадлежит А/МП(А), если из условия

$$h^\wedge(X_j,S_k) = S_{k`}, f^\wedge(X_j,S_k) = Y_c$$

следует

$$h(X_j,S_k)\subseteq S_{k`}, f(X_j,S_k)\subseteq Y_c.$$

Аналогично вводится многозначный фактор A_M/МП(A_M) автомата A_M по многозначному покрытию автомата А.

Лемма 2. Каждому МГ $(\psi, \varphi, \chi)\in$МГ(А, А`) соответствует МП(А) вида

$$(\psi^{-1}(x`), x`\in X`), (\varphi^{-1}(s`), s`\in S`), (\chi^{-1}(y`), y`\in Y`).$$

Доказательство. Действительно, имеем

$$\bigcup_{x`\in X`} \psi^{-1}(x`) = \text{Пр}_1\psi = X, \quad \bigcup_{s`\in S`} \phi^{-1}(s`) = \text{Пр}_1\varphi = S,$$

$$h(\psi^{-1}(x`),\varphi^{-1}(s`))\subseteq\varphi^{-1}(h`_{x`}s`);$$

$$f(\psi^{-1}(x`),\varphi^{-1}(s`))\subseteq\chi^{-1}(f`_{x`}s`).$$

Обозначим через МП(А, ψ, φ, χ) указанное в лемме 2 многозначное покрытие автомата А, аналогично МП(A_M, ψ, φ) для автоматов без выходов.

Теорема 1.

1. Если $(\psi, \varphi, \chi)\in$МГ(А, А`), то автомат А` изоморфен одному из автоматов многозначного фактора А/МП(А, ψ, φ, χ).
2. Каждый автомат $A^\wedge\in$А/МП(А) при МП(А) вида

$$(X_j, j\in\{1, ..., m\}), (S_j, j\in\{1, ..., n\}), (Y_j, j\in\{1, ..., L\})$$

является образом многозначного гомоморфизма (ψ, φ, χ) A на A^, где отношения ψ, φ, χ определены так:

$x\psi X_j$ тогда и только тогда, когда $x \in X_j$, $j \in \{1, ..., m\}$;

$s\varphi S_j$ тогда и только тогда, когда $s \in S_j$, $j \in \{1, ..., n\}$;

$y\chi Y_j$ тогда и только тогда, когда $y \in Y_j$, $j \in \{1, ..., L\}$.

Доказательство. Если (ψ, φ, χ)$\in$МГ(A, A`), то по лемме 2

$$(\psi^{-1}(x`), x` \in X`), (\varphi^{-1}(s`), s` \in S`), (\chi^{-1}(y`), y` \in Y`)$$

есть МП(A). Автомат

$$A` = (X`, S`, Y`, h`, f`)$$

изоморфен автомату A^$\in$A/МП(A, ψ, φ, χ), A^ = (X^, S^, Y^, h^, f^), у которого входной алфавит состоит из элементов – множеств $\psi^{-1}(x`)$, $x` \in X`$ занумерованных (отмеченных) элементами $x` \in X`$. Таким образом, элементы $\psi^{-1}(x`)$ из X^ мы рассматриваем как пары ($\psi^{-1}(x`)$, x`) оставляя для них прежнее обозначение. Аналогично поступаем при определении множеств S^, Y^. Итак

$$X^\wedge = \{\psi^{-1}(x`), x` \in X`\}, S^\wedge = \{\varphi^{-1}(s`), s` \in S`\}, \{\chi^{-1}(y`), y` \in Y`\}.$$

Функции перехода h^ и выхода f^ определяем по правилу:

$$h^\wedge(\psi^{-1}(x`),\varphi^{-1}(s`_1)) = \varphi^{-1}(s`_2);$$

$$f^\wedge(\psi^{-1}(x`),\varphi^{-1}(s`_1)) = \chi^{-1}(y`)$$

тогда и только тогда, если

$$h`(x`,s`_1) = s`_2,\ f`(x`,s`_1) = y`.$$

Утверждение 2 теоремы вытекает из определений 1, 3.

Определение 4. (ψ, φ, χ)$\in$МГ(A, A`) называется согласованным многозначным гомоморфизмом или кратко СМГ(A, A`), если многозначное покрытие МП(A, ψ, φ, χ) является согласованным.

Для согласованного многозначного покрытия многозначный фактор A/СМП(A) автомата A состоит из одного автомата, который мы назовем фактор автоматам A/СМП(A).

Следствие теоремы 1. (ψ, φ, χ)$\in$СМГ(A, A`) тогда и только тогда, когда A` изоморфен фактор автомату A/СМП(A, ψ, φ, χ).

При формулировке достаточности условий следствия использованы обозначения пункта 2 теоремы 1.

Произвольный (ψ, φ, χ)$\in$МГ(A, A`) индуцирует естественным образом многозначные гомоморфизмы ($\psi$, $\varphi$*, $\chi$*) каждой связной компоненты автомата A на некоторые подавтоматы автомата A`. Здесь φ*, χ* – соответствующие ограничения бинарных отношений φ, χ. В свою очередь, многозначный гомоморфизм связной компо-

ненты (с. к.) $A_{с.к.}$ автомата A на подавтомат $A`_п$ автомата A` индуцирует многозначный гомоморфизм каждой сильно связной компоненты автомата $A_{с.к.}$ на некоторую связную компоненту автомата $A`_п$. В связи с чем представляет интерес конструктивное описание многозначных гомоморфизмов для сильно связных автоматов.

Сказанное здесь и замечание 2 позволяет нам при изучении множества МГ(A) ограничиться рассмотрением МГ сильно связных автоматов A_M без выхода в сильно связные автоматы $A`_M$.

Конкретизируем высказанное утверждение. Заметим, прежде всего, что приведенные выше понятия и утверждения, начиная с определения 2, легко переносятся на случай автоматов без выходов.

Итак, пусть $(\psi, \varphi) \in МГ(A_M, A`_M)$. Рассмотрим вспомогательный автомат – параллельное соединение автоматов $A_M$, $A`_M$

$$B = B(A_M, A`_M) = (I, S \times S`, \delta),$$

где $I = \psi$, ψ – данное бинарное отношение, $\psi \subseteq X \times X`$, функция перехода задана частичными функциями переходов $\delta_{(x, x`)}$, $(x, x`) \in \psi$

$$\delta_{(x, x`)}(s, s`) = (h_x s, h`_{x`} s`).$$

Для каждого состояния (s, s`) автомата B определим бинарное отношение $\varepsilon_{(s,s`)}$ на $S \times S`$, положив, что $(s,s`) \in \varepsilon_{(s,s`)}$ и $(s^*,s`^*) \in \varepsilon_{(s,s`)}$ тогда и только тогда, когда найдется входное слово $P \in I^*$ $(I = \psi)$ , при котором $\delta_P(s, s`) = (s^*, s`^*)$. Таким образом, $\varepsilon_{(s, s`)}$ – множество состояний автомата B<s, s`>, порожденного состоянием (s, s`) автомата B. Ясно, что $(\psi, \varepsilon_{(s, s`)})$ – многозначный гомоморфизм автомата $A_M$<s> на автомат $A`_M$<s`>. Здесь: $A_M$<s> – автомат, порожденный состоянием s в автомате $A_M$; $A`_M$<s`> – автомат, порожденный состоянием s` в автомате $A`_M$. При подробном доказательстве этого утверждения следует использовать условия

$$Пр_1\psi = X, Пр_2\psi = X`$$

из пункта 1 определения 1. Для любого $P \in I^*$ при $\nabla(P) = \delta_P(s, s`)$ очевидно включение

$$\varepsilon_{\nabla(P)} \subseteq \varepsilon_{(s,s`)}$$

и очевидно равенство

$$\bigcup_{(s,s`) \in \phi} \varepsilon_{(s,s`)} = \phi .$$

Поэтому можно выбрать минимальное по мощности подмножество $M(\varphi) \subseteq \varphi$, для которого

$$\bigcup_{(s,s`) \in M(\phi)} \varepsilon_{(s,s`)} = \phi .$$

Такое подмножество определено возможно неоднозначно.

Полученный вид φ сводит задачу описания множества МГ(A_M, $A`_M$) при фиксированном ψ на X×X` к задаче описания многозначных гомоморфизмов вида (ψ, $\varepsilon_{(s,s`)}$) автомата $A_M$<s> на $A`_M$<s`> для каждой пары состояний (s,s`)∈S×S`.

Ниже сначала решается указанная задача для связного перестановочного автомата A_M.

15.3. Описание многозначных гомоморфизмов для связных перестановочных автоматов

Определение 5. Тройка бинарных отношений (ψ, φ, χ) на соответствующих алфавитах X×X`, S×S`, Y×Y` автоматов A, A` называется инверсным гомоморфизмом A на A`, если отношения ψ, φ, χ таковы, что тройка обратных к ним бинарных отношений

$$(\psi^{-1}, \varphi^{-1}, \chi^{-1})$$

на X`×X, S`×S, Y`×Y является гомоморфизмом A` на A.

Отметим, что в данном определении мы отображения ψ^{-1}, φ^{-1}, χ^{-1} трактуем как частный случай бинарных отношений.

Лемма 3. Инверсный гомоморфизм (ψ, φ, χ) A на A` принадлежит МГ(A, A`).

Доказательство. Отображения ψ^{-1}, φ^{-1}, χ^{-1} определены соответственно на X`, S`, Y`, причем

$$\psi^{-1}(X`) = X,\ \varphi^{-1}(S`) = S,\ \chi^{-1}(Y`) = Y.$$

По этой причине

$$Пр_1\psi = X,\quad Пр_1\varphi = S,\quad Пр_2\psi = X`,\quad Пр_2\varphi = S`.$$

Далее

$$h_{\psi^{-1}(x`)}\phi^{-1}s` = \phi^{-1}h`_{x`}s`,$$

$$f_{\psi^{-1}(x`)}\phi^{-1}s` = \chi^{-1}f`_{x`}s`,$$

так как (ψ^{-1}, φ^{-1}, χ^{-1}) – гомоморфизм A` на A и, следовательно,

$$\{h_{\psi^{-1}(x`)}\phi^{-1}s`\} \subseteq \{\phi^{-1}h`_{x`}s`\},$$

$$\{f_{\psi^{-1}(x`)}\phi^{-1}s`\} \subseteq \{\chi^{-1}f`_{x`}s`\}.$$

В этих включениях участвуют одноэлементные множества. Таким образом, (ψ, φ, χ) – многозначный гомоморфизм A на A` (см. определение 1).

Символ • используется ниже для композиции (суперпозиции) бинарных отношений и многозначных гомоморфизмов.

Теорема 2. Пусть A_M – перестановочный автомат, а $A`_M$ – сильно связный автомат и $(\psi, \varphi)\in МГ(A_M, A`_M)$.

1. Найдется гомоморфизм $(\psi_г, \varphi_г)$ автомата $A`_M$ на некоторый автомат $A``_M$, при котором

$$(\psi\bullet\psi_г,\varphi\bullet\varphi_г)\in СМГ(A_M, A``_M).$$

2. Многозначный гомоморфизм (ψ, φ) A_M на $A`_M$ представим суперпозицией $(\psi_c, \varphi_c)\bullet(\psi_г^{-1}, \varphi_г^{-1})$ некоторого согласованного многозначного гомоморфизма (ψ_c, φ_c) A_M на $A``_M$ с некоторым инверсным гомоморфизмом $(\psi_г^{-1}, \varphi_г^{-1})$ автомата $A``_M$ на $A`_M$.

Доказательство. Приведем предварительно вспомогательные леммы.

Лемма 4. Если $(\psi, \varphi, \chi)\in МГ(A, A`)$, то для любого слова $P` = x`(1), x`(2), ..., x`(k)$ в алфавите $X`$ и произвольного $s`\in S`$

$$h(\psi^{-1}(P`), \varphi^{-1}(s`))\subseteq\varphi^{-1}h`(P`, s`),$$
$$f(\psi^{-1}(P`), \varphi^{-1}(s`))\subseteq\chi^{-1}f`(P`, s`).$$

Здесь использованы обозначения из пункта 1 (введения) и дополнительно для $P`= x`(1), x`(2), ..., x`(k)$ положено

$$\psi^{-1}(P`) =\{(x(1), ..., x(k)): x(j)\in\psi^{-1}(x`(j)), j\in\{1, ..., k\}\}$$

Данное утверждение следует из определения 1.

Лемма 5. В условиях теоремы 2 множества $\varphi^{-1}(s`)$, $s`\in S`$ равномощны и

$$h(P, \varphi^{-1}(s`)) =\varphi^{-1}h`(P`, s`)$$

при любом слове $P`= x`(1), x`(2), ..., x`(k)$ в алфавите $X`$ и любом слове $P\in\psi^{-1}(P`)$.

Доказательство. Пусть $s`(1), s`(2)\in S`$. Достаточно показать, что $|\varphi^{-1}(s(2))|\geq|\varphi^{-1}(s(1))|$. Выберем входное слово $P`$ автомата $A`_M$ так, чтобы

$$h`(P`, s`(1))= s`(2).$$

По лемме 4

$$h(\psi^{-1}(P`), \varphi^{-1}(s`(1)))\subseteq\varphi^{-1}h`(P`, s`(1)) = \varphi^{-1}(s`(2)).$$

То есть для любого $P\in\psi^{-1}(P`)$

$$h(P, \varphi^{-1}(s`(1)))\subseteq\varphi^{-1}(s`(2)).$$

Так как A_M по условию перестановочный автомат, получаем

$$|h_P\varphi^{-1}(s`(1))| = |\varphi^{-1}(s`(1))|\leq|\varphi^{-1}(s`(2))|.$$

Лемма 6. В условиях теоремы 2 пара бинарных отношений $(\psi\wedge, \varphi\wedge)$ определенных на $X`$, $S`$ условиями:

$x`\psi\wedge x``$ тогда и только тогда, когда $\psi^{-1}(x`) = \psi^{-1}(x``)$;

$s`\varphi\hat{}s``$ тогда и только тогда, когда $\varphi^{-1}(s`) = \varphi^{-1}(s``)$ является конгруэнцией на $A`_M$.

Доказательство. Пусть

$$\psi^{-1}(x`) = \psi^{-1}(x``),\ \varphi^{-1}(s`) = \varphi^{-1}(s``).$$

Надо показать, что

$$\varphi^{-1}(h`_{x`}s`) = \varphi^{-1}(h`_{x``}s``).$$

Из леммы 2 имеем

$$h(\psi^{-1}(x`),\varphi^{-1}(s`))\subseteq\varphi^{-1}(h`_{x`}s`);$$
$$h(\psi^{-1}(x``),\varphi^{-1}(s``))\subseteq\varphi^{-1}(h_{x``}s``).$$

Учитывая перестановочность автомата A и утверждение леммы 5 можно предыдущие включения заменить на равенства:

$$h(\psi^{-1}(x`), \varphi^{-1}(s`)) = \varphi^{-1}(h`_{x`}s`);$$
$$h(\psi^{-1}(x``), \varphi^{-1}(s``)) = \varphi^{-1}(h_{x``}s``).$$

Из определения $(\psi\hat{}, \varphi\hat{})$ следует совпадение левых частей этих равенств, поэтому равны и их правые части. Лемма 6 доказана.

Для доказательства теоремы 2 рассмотрим фактор автомат $A_M/(\psi\hat{}, \varphi\hat{})$ и через $(\psi_г, \varphi_г)$ обозначим естественный гомоморфизм $A`_M$ на $A``_M = A_M/(\psi\hat{},\varphi\hat{})$, соответствующий конгруэнции $(\psi\hat{}, \varphi\hat{})$. Непосредственно проверяется, что суперпозиция $(\psi, \varphi)\bullet(\psi_г, \varphi_г) = (\psi\bullet\psi_г, \varphi\bullet\varphi_г)$ отношений (ψ, φ), $(\psi_г, \varphi_г)$ принадлежит СМГ$(A_M, A``_M)$ и $(\psi, \varphi)=(\psi, \varphi)\bullet(\psi_г, \varphi_г)\bullet(\psi_г^{-1}, \varphi_г^{-1})$. Доказательство теоремы 2 закончено.

Таким образом, согласно теореме 2 многозначные гомоморфизмы перестановочного автомата A_M на сильно связные автоматы с точностью до инверсных гомоморфизмов являются согласованными многозначными гомоморфизмами.

15.4. Образы СМГ связных перестановочных автоматов

Перейдем к описанию алгоритма получения всех связных автоматов, являющихся образами, с точностью до изоморфизма, заданного связного перестановочного автомата A_M при согласованных многозначных гомоморфизмах.

Пусть S(1) – непустое подмножество множества состояний S автомата $A = (X, S, Y, h, f)$, $G = g_1G_{S(1)}\cup g_2G_{S(1)}\cup\ldots\cup g_nG_{S(1)}$ – разложение группы $G = \langle h_x, x\in X\rangle$ (порожденной $\{h_x, x\in X\}$) автомата A в левые смежные классы по стабилизатору $G_{S(1)}$ множества S(1) в группе G. Положим $S(j) = g_jS(1)$, $j\in\{1, \ldots, n\}$. Определим бинарное

отношение σ на X: $x(1)\sigma x(2)$ тогда и только тогда, когда $h(x(1)), S(j)) = h(x(2)), S(j))$ для всех $j\in\{1, ..., n\}$. Очевидно σ – бинарное отношение эквивалентности на X. Рассмотрим произвольное покрытие множества X вида $(X(j), j\in\{1, ..., m\})$, где каждое X(j) является некоторым подмножеством одного из класса эквивалентности отношения σ. Непосредственно проверяется, что пара покрытий $(X(j), j\in\{1, ..., m\})$, $(S(j), j\in\{1, ..., n\})$ есть СМП автомата A_M.

Указанным способом можно получить с точностью до изоморфизма все связные автоматы, являющиеся образами автомата A_M при согласованных многозначных гомоморфизмах. Действительно, пусть пара покрытий $(X(j), j\in\{1, ..., m\})$, $(S(j), j\in\{1, ..., n\})$ есть СМП автомата A_M, при котором автомат А/СМП(A_M) является связным автоматом. Из связности последнего автомата и перестановочности автомата A_M следует $|S(j)| = |S(j`)|$ при любых $j, j`\in\{1, ..., n\}$. Кроме того, для любых $j\in\{1, ..., m\}$ и $c\in\{1, ..., n\}$ существует единственный номер $k = k(j,c)$, при котором $h(X(j), S(c)) = S(k)$. Из согласованности МП(A_M) вытекает, что элементы $(S(j), j\in\{1, ..., n\})$ попарно различны. Таким образом, можно сделать вывод о том, что при каждом $x\in X$ частичная функция переходов h_x автомата A_M осуществляет перестановку элементов множества $\{S(j), j\in\{1, ..., n\}\}$. Следовательно, если $G = g_1G_{S(1)}\cup...\cup g_nG_{S(n)}$ разложение группы автомата A_M в левые смежные классы по стабилизатору $G_{S(1)}$ множества S(1) в группе G, то $S(j) = g_jS(1)$.

Замечание 4. Несложно доказывается следующее

Утверждение 1. Если для СМП $(X(j), j\in\{1, ..., m\})$, $(S(j), j\in\{1, ..., n\})$ связного перестановочного автомата A_M выполнены условия:

1) А/СМП(A_M) – связный автомат;
2) $(X(j), j\in\{1, ..., m\})$ – разбиение X;
3) $G_s\subseteq G_{S(1)}$, где s – некоторый фиксированный элемент из S(1), группа $G_{S(1)}$ транзитивна на S(1),

то покрытие $(S(j), j\in\{1, ..., n\})$ множества S является разбиением, в связи с чем автомат А/СМП(A_M) является гомоморфным образом автомата А.

15.5. Образы МГ-произвольного автомата без выходов

Перейдем к конструктивному описанию образов многозначных гомоморфизмов произвольного автомата $A_M = (X, S, Y, (h_x)_{x\in X})$.

Определение 6. Многозначное покрытие

$$(X(j), j\in\{1, ..., m\}), (S(j), j\in\{1, ..., n\})$$

автомата A_M называется системным покрытием относительно состояний автомата A_M, или кратко МСП(A_M), если каждое множество S(j) не является подмножеством любого другого множество из набора множеств (S(j), $j\in\{1, ..., n\}$), то есть из $S(j)\subseteq S(j`)$ следует S(j) = S(j`).

Непосредственно из определений МП(A_M) и МСП(A_M) вытекают следующие утверждения.

1. Если

$$(X(j), j\in\{1, ..., m\}), (S(j), j\in\{1, ..., n\})$$

есть МП автомата A_M, то найдется подмножество $V\subseteq\{1, ..., n\}$, при котором

$$(X(j), j\in\{1, ..., m\}), (S(j), j\in V)$$

есть МСП автомата A_M.

2. Если

$$(X(j), j\in\{1, ..., m\}), (S(j), j\in\{1, ..., n\})$$

есть МП автомата A_M, то система множеств

$$(X(j), j\in\{1, ..., m\}),\ (S(j), S`(j`), j\in\{1, ..., n\}, j`\in\{1, ..., n`\}),$$

где $S`(j`)\subseteq S$, $j`\in\{1, ..., n`\}$ и для каждого $j`\in\{1, ..., n`\}$ найдется $j\in\{1, ..., n\}$, при котором $S`(j`)\subseteq S(j)$ также является МП автомата A_M.

Определение 7. Многозначное покрытие

$$(X(j),j\in\{1,...,m\}), (S`(j`), j\in\{1,...,n`\})$$

автомата A_M называется подпокрытием по состояниям многозначного покрытия

$$(X(j),j\in\{1,...,m\}), (S(j), j\in\{1,...,n\})$$

автомата A_M, если для любого $j`\in\{1, ..., n`\}$ найдется $j\in\{1,...,n\}$ при котором $S`(j`)\subseteq S(j)$.

Очевидно, любое МП автомата A_M является подпокрытием по состояниям некоторого МСП автомата A_M.

Через ($\{x\}$, $x\in X$) обозначим тривиальное покрытие множества X, состоящее из неповторяющихся всех его элементов ($\{x\}$ – множество, состоящее из одного элемента x).

Определение 8. МП (МСП) автомата A_M вида

$$(\{x\}, x\in X), (S(j), j\in\{1, ..., n\})$$

называется многозначным покрытием состояний автомата A_M (многозначным системным покрытием состояний автомата A_M).

Очевидно, если

$$(X(j), j\in\{1, ..., m\}), (S(j), j\in\{1, ..., n\})$$

есть МП автомата A_M, то

$$(\{x\}, x\in X), (S(j), j\in\{1, ..., n\})$$

есть МП состояний автомата A_M.

Определение 9. Любое непустое подмножество $X(0)\subseteq X$ называется неотличимым множеством относительно МП состояний

$$(\{x\}, x\in X), (S(j), j\in\{1, ..., n\})$$

автомата A_M, если для любого $j\in\{1, ..., n\}$ найдется $j`\in\{1, ..., n\}$, при котором

$$h_{X(0)}S(j)\subseteq S(j`).$$

Несложно доказывается следующее утверждение.

Утверждение 2.

Две системы множеств

$$(X(j), j\in\{1, ..., m\}), (S(j), j\in\{1, ..., n\}),$$

где $X(j)\subseteq X$, $S(j)\subseteq S$, являются МП (МСП) автомата A_M тогда и только тогда, когда выполнены два условия:

1) $(\{x\}, x\in X), (S(j), j\in\{1,...,n\})$ есть МП состояний (МСП состояний) автомата A_M;

2) $(X(j), j\in\{1,...,m\})$ является покрытием X и любое множество X(j) является неотличимым множеством относительно МП (МСП) автомата A_M указанного в условии 1).

Таким образом, задача описания образов МГ произвольного автомата А свелась к задаче описания образов МГ соответствующего ему автомата без выходов A_M (замечание 2). Последняя задача сводится к описанию МП состояний автомата без выходов A_M (утверждение 2).

Для связного перестановочного автомата А задача описания его связных образов при МГ свелась к описанию СМП по состояниям автомата A_M (замечание 2, теорема 2, утверждение 2). МП состояний

$$(\{x\}, x\in X), (S(j), j\in\{1, ..., n\})$$

автомата A_M в терминах работы [31. – С. 293] эквивалентно понятию «системного множества со свойством подстановки». Конструктивное описание таких системных множеств, то есть описание МП состояний автомата A_M дается процедурой 5.2 [40. – С. 309].

15.6. Пример использования МГ-автомата

Для произвольного автомата $A = (X, S, Y, h, f)$ и его состояния $s \in S$ рассмотрим подавтомат $A\langle s\rangle = (X, S_s, Y, h, f)$ порожденный состоянием $s \in S$. Будем рассматривать $A\langle s\rangle$ как инициальный автомат. Пусть F – множество инициальных автоматов, полученных из произвольных автоматов с фиксированными алфавитами X, Y, а μ – произвольная действительная функция на $F \times F$ с условием: если для инициальных автоматов $A\langle s\rangle$, $A`\langle s`\rangle$

$$\mu\,(A\langle s\rangle, A`\langle s`\rangle) = 0,$$

то при любом слове $P \in X^*$

$$\mu\,(A\langle h_P s\rangle, A`\langle h`_P s`\rangle) = 0.$$

Определение 10. Автоматы $A = (X, S, Y, h, f)$, $A` = (X, S`, Y, h`, f`)$ называются $(\mu,0)$-неотличимыми, если существует бинарное отношение

$$\sigma \subseteq S \times S`, \quad Пр_1\sigma = S, \; Пр_2\sigma = S`,$$

при котором для любого $s \in S$

$$\mu((A\langle s\rangle, A`\langle \sigma(s)\rangle) = 0.$$

Примером функции μ может служить мера неотличимости состояний автоматов, введенная в [15]. Другим частным случаем $(\mu, 0)$-неотличимости автоматов является известное понятие неотличимости автоматов (см., например, [24]).

Следующее утверждение очевидно.

Утверждение 3. Если автоматы A и A` из F $(\mu, 0)$-неотличимы, то автомат $A`_M$ является образом автомата A_M при некотором многозначном гомоморфизме вида (E, σ), где E – тождественное отображение X в X.

Таким образом, поиск $(\mu, 0)$-неотличимых от A автоматов A` следует вести с учетом того, что $A`_M$ находится среди образов МГ автомата A_M.

15.7. Некоторые обобщения многозначных гомоморфизмов автомата

Определение 11. Слабым многозначным гомоморфизмом (слабым МГ) автомата $A = (X, S, Y, h, f)$ на автомат $A` = (X`, S`, Y`, h`, f`)$ называется тройка бинарных отношений (ψ, φ, χ), соответственно, на $X \times X`$, $S \times S`$, $Y \times Y`$, для которых выполняются условия:

1) $Пр_1\psi = X$, $ПР_1\varphi = S$, $Пр_2\psi = X`$, $Пр_2\varphi = S`$;

2) если для $P \in X^*$, $P = x_1, x_2, ..., x_k$, и $s \in S$

$$A(s, x_1, x_2, ..., x_k) = y_1, y_2, ..., y_k$$

и

$$s\varphi s`, x_j\psi x`_j, j \in \{1, ..., k\},$$

то

$$A`(s`, x`_1, x`_2, ..., x`_k) = y`_1, y`_2, ..., y`_k,$$

где $y_j\chi y`_j$, $j \in \{1, ..., k\}$.

Из леммы 4 вытекает, что МГ (ψ, φ, χ) автомата A на A` является одновременно и слабым МГ A на A`.

Лемма 7. Если (ψ, φ, χ) является слабым МГ автомата A на A`, то существует бинарное отношение $\varphi^\wedge$ такое, что $\varphi \subseteq \varphi^\wedge$, при котором $(\psi, \varphi^\wedge, \chi)$ – МГ A на A`.

Доказательство. Пусть (ψ, φ, χ) – слабый многозначный гомоморфизм автомата A на автомат A`. Тогда для произвольного слова $x_1, x_2, ..., x_k$ из $X^*$ и элементов $x \in X$, $x` \in X`$, $s \in S$, $s` \in S`$, для которых $x\psi x`$, $s\varphi s`$, из условия

$$A(s, x, x_1, x_2, ..., x_k) = y_1, y_2, ..., y_{k+1}, x_j\psi x`_j, j \in \{1, ..., k\}$$

следует

$$A`(s`, x`, x`_1, x`_2, ..., x`_k) = y`_1, y`_2, ..., y`_{k+1},$$

где $y_j\chi y`_j$, $j \in \{1, ..., k+1\}$. В частности,

$$A(h_x s, x_1, x_2, ..., x_k) = y_2, ..., y_{k+1};$$

$$A`(h`_{x`}s`, x`_1, x`_2, ..., x`_k) = y`_2, ..., y`_{k+1}.$$

Доопределим φ до $\varphi^\wedge$ элементами $(h_x s, h`_{x`}s`)$ для любых x и x`, s, s` таких, что $x\psi x`$, $s\varphi s`$ (в случае, если $(h_x s, h`_{x`}s`)$ не принадлежит φ). По определению 1 $(\psi, \varphi^\wedge, \chi)$ – многозначный гомоморфизм A на A`.

Лемма 7 отчасти сводит поиск образов слабых МГ к поиску образов МГ заданного автомата A. Здесь имеется в виду то, что при известных МГ вида (ψ, φ, χ), поиск слабых МГ можно проводить среди троек бинарных отношений вида $(\psi, \varphi^\wedge, \chi)$, где $\varphi \subseteq \varphi^\wedge$.

Замечание 5. Очевидно любой гомоморфизм автомата A на A` является одновременно и слабым многозначным гомоморфизмом. Одна из связей слабого МГ с гомоморфизмом проявляется в следующем утверждении.

Утверждение 4. Если (ψ, φ, χ) – слабый МГ A на A`, где $\chi$ – отображение Y в Y` и A` – приведенный автомат, то $(\psi, \varphi, \chi)$ – МГ A на A`, причем множества $\varphi(s)$, $s \in S$ одноэлементные, то есть

φ – отображение S в S`. Если дополнительно $\psi$ – отображение X в X`, то (ψ, φ, χ) – гомоморфизм A на A`.

Доказательство данного утверждения проводится несложно с использованием доказательства леммы 7.

Определение 12. K-слабым многозначным гомоморфизмом автомата A на A` называется тройка бинарных отношений $(\psi, \varphi, \chi)$ на $X\times X`$, $S\times S`$, $Y\times Y`$, для которых выполнены условия:

1) $Пр_1\psi = X$, $ПР_1\varphi = S$,

$$Пр_2\psi = X`, Пр_2\varphi = S`;$$

2) если для $P\in X^k$, $P = x_1, x_2, ..., x_k$, и $s\in S$

$$A(s, x_1, x_2, ..., x_k) = y_1, y_2, ..., y_k$$

и

$$s\varphi s`, x_j\psi x`_j, j\in\{1, ..., k\},$$

то

$$A`(s`, x`_1, x`_2, ..., x`_k) = y`_1, y`_2, ..., y`_k,$$

где $y_j\chi y`_j$, $j\in\{1, ..., k\}$.

Очевидно, слабый многозначный гомоморфизм автомата A на A` является и k-слабым многозначным гомоморфизмом A на A`. Для установления вида обратной связи этих понятий рассмотрим для произвольного бинарного отношения $\psi\subseteq X\times X`$ и автоматов A = = (X, S, Y, h, f), A` = (X`, S`, Y`, h`, f`) параллельное соединение B = = B(A, A`) автоматов без выходов $A_M = (X, S, Y, h)$, $A`_M = (X`, S`, Y`, h`)$ вида

$$B = (X_B, S\times S`, h^B),$$

где $X_B = \psi$, а для $(x, x`)\in\psi$ частичная функция переходов $h^B_{(x, x`)}$ автомата B определена так

$$h^B_{(x, x`)} (s, s`) = (h_x s, h`_{x`}s`), (s, s`)\in S\times S`.$$

Напомним, что h_x, $h`_{x`}$ – частичные функции переходов автоматов A, A`.

Обозначим через D_B диаметр графа переходов автомата B. То есть D_B – минимальное число D такое, что если

$$h^B_P (s_1, s`_1) = (s_2, s`_2), (s_1, s`_1) \neq (s_2, s`_2)$$

для $P\in(X_B)^*$, то существует $k\leq D$ и $P^\wedge\in (X_B)^k$, при котором

$$h^B_{P^\wedge} (s_1, s`_1) = (s_2, s`_2).$$

Стандартными методами теории автоматов легко доказывается следующее утверждение.

Утверждение 5. Если (ψ, φ, χ) – k-слабый многозначный гомоморфизм автомата A на A` и $k \geq D_B+1$, то $(\psi,\varphi,\chi)$ – слабый многозначный гомоморфизм автомата A на A`.

Глава 16. МОДЕЛИ КОНЕЧНЫХ АВТОМАТОВ, ПОСТРОЕННЫЕ НА ОСНОВЕ ГОМОМОРФИЗМОВ ПОВЕДЕНИЯ

16.1. Обозначения

Через $A = (X, S, Y, h, f)$ или $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$, как и ранее, будет обозначаться конечный автомат, $h: X\times S\to S$, $f: X\times S\to Y$, $h_x: S\to S$, $f_x: S\to Y$, $h_x s = h(x, s)$, $h_x s = f(x, s)$ для $x\in X$, $s\in S$. Для $M\subseteq X\times S$ используем обозначение $h(M) = \{s': h_x s = s', (x, s)\in M\}$.

Частичным автоматам называют автомат $A = (X, S, Y, h, f)$, у которого значения функций переходов h и выходов f определены возможно не на всех парах $(x, s)\in X\times S$.

Ниже будут использоваться частичные автоматы, у которых функции переходов h и выходов f определены на некотором непустом подмножестве $@\in X\times S$ (возможен случай и $@ = X\times S$). Ограничения функций h, f на @ будем обозначать теми же буквами. Четверку (@, Y^, h, f) (Y^ – выходной алфавит) с естественным законом функционирования, индуцированным законом функционирования автомата A, будем также называть *частичным автоматом с заданным множеством @ пар* (входной символ, состояние).

16.2. Обобщенный гомоморфизм поведения автоматов

Пусть $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$, $A` = (X`, S`, Y`, (h`_{x`})_{x`\in X`}, (f`_{x`})_{x`\in X`})$ – конечные автоматы.

Определение 1. Отображение $\Phi: X\times S\times Y\to X\times S\times Y\to X`\times S`\times Y`$ назовем обобщенным гомоморфизмом поведения (ОГП) автомата A в A`, если для любых $x(1), x(2)\in X$, $s_1\in S$ из условия $\Phi(x(1), s_1, f_{x(1)}s_1) = (x`(1), s`_1, y`)$ следует:

а) $y` = f`_{x`(1)}s`_1$;

б) $\Phi(x_2, h_{x(1)}s_1, f_{x(2)}h_{x(1)}s_1) = (x`(2), s`_2, y`_2)$, где $s`_2 = h`_{x`(1)}s`_1$.

Заметим, что из условия а) следует $y`_2 = f`_{x`(2)}s`_2$, и образ Ф(А) при ОГП А в $\overline{A}$ является в общем случае частичным подавтоматом автомата А`. Кроме того, суперпозиция (последовательное выполнение) ОГП есть ОГП.

Разложим отображение Ф: $X\times S\times Y\to X`\times S`\times Y`$ по координатным функциям:

$$\Phi_1 : X\times S\times Y\to X`,\ \Phi_2 : X\times S\times Y\to S`,\ \Phi_3: X\times S\times Y\to Y`.$$

Через ОГП (А, А`) обозначим множество всех ОГП А в А`.

Очевидно, что $\Phi = (\Phi_1, \Phi_2, \Phi_3)\in$ОГП (А, А`) тогда и только тогда, когда для любых $x(1), x(2)\in X$, $s_1 \in S$ выполняются равенства

$$\Phi_2(x_2, h_{x(1)}s1, f_{x(2)}h_{x(1)}s_1) = h`_{\Phi_1(x(1),\ s_1, f_{x(1)}\ s_1)}\Phi_2(x(1), s_1, f_{x(1)}s_1),$$

$$\Phi_3(x(1), s_1, f_{x(1)}s_1) = f`_{\Phi_1(x(1),\ s_1, f_{x(1)}\ s_1)}\Phi_2(x(1), s_1, f_{x(1)}s_1).$$

Для $\Phi = (\Phi_1, \Phi_2, \Phi_3)\in$ОГП(А, А`) введем вспомогательные функции $(\Phi_{11}, \Phi_{22}, \Phi_{33})$ на $X\times S$, положив

$$\Phi_{11}(x, s) = \Phi_1(x, s, f_x s),\ \Phi_{22}(x, s) = \Phi_2(x, s, f_x s),\ \Phi_{33}(x, s) =$$
$$= \Phi_3(x, s, f_x s),\ x\in X,\ s \in S.$$

Легко видеть, что для описания всех $\Phi = (\Phi_1, \Phi_2, \Phi_3)\in$ОГП(А, А`) достаточно для каждого из них конструктивно указать соответствующие ОГП $\Phi = (\Phi_1, \Phi_2, \Phi_3)$ отображения

$$\Phi_{11}: X\times S\to X`,\ \Phi_{22}:X\times S\to S`,\ \Phi_{33}: X\times S\to Y`.$$

В связи с чем *за исходное изучаемое понятие может быть взято следующее.*

Определение 2. Тройку отображений (Φ_1, Φ_2, Φ_3)

$$\Phi_1: X\times S\to X`,\ \Phi_2: X\times S\to S`,\ \Phi_3: X\times S\to Y`$$

назовем обобщенным гомоморфизмом поведения в узком смысле автомата А в А`(УОГП (А, А`)), если для любых $x(1), x(2)\in X$, $s_1\in S$ выполняются равенства

$$\Phi_2(x(2), h_{x(1)}s_1) = h`_{\Phi_1(x(1),\ s_1)}\Phi_2(x(1), s_1),$$

$$\Phi_3(x(1), s_1) = f`_{\Phi_1(x(1),\ s_1)}\Phi_2(x(1), s_1).$$

Ниже будет показано, что и обобщенный гомоморфизм поведения в узком смысле автомата А в А` во многом определен более сильными условиями, которые приводят к новому понятию «гомоморфизма поведения (ГП) автомата А в автомат А`», которое будет приведено далее.

Определение 3. Состояние $s\in S$ автомата А назовем внутренним состоянием, если существуют такие $x\in X$, $s'\in S$, что $s = h_x s'$. В противном случае состояние s назовем внешним.

Обозначим через J(S, A) – множество внутренних состояний автомата A, а через J(A) – подавтомат автомата A, порожденный множеством J(S, A). Автомат J(A**)** назовем *внутренним подавтоматом автомата A.* Он получается удалением в графе переходов автомата A внешних состояний вместе с выходящими из них дугами.

Определение 4. Тройку отображений $(\varphi_1, \varphi_2, \varphi_3)$

$$\varphi_1: X\times S\to X`,\ \ \varphi_2: S\to S`,\ \ \varphi_3: X\times S\to Y`$$

назовем гомоморфизмом поведения (ГП) автомата A в A`, если для каждого $x\in X$ и каждого $s\in S$ из равенств

$$\varphi_1(x, s) = x`,\ \varphi_2(s) = s`$$

следует

$$\varphi_2(h_x s) = h`_{x`}s`,\ \varphi_3(x, s) = f`_{x`}s`.$$

Для автоматов без выходов $A = (X, S, (h_x)_{x\in X})$, $A` = (X`, S`, (h`_{x`})_{x`\in X`})$ двойку отображений $(\varphi_1, \varphi_2)$, удовлетворяющую соответствующим условиям определения 4 (из $\varphi_1(x, s) = x`$, $\varphi_2(s)= s`$ следует $\varphi_2(h_x s) = h`_{x`}s`$), также будем называть *гомоморфизмом поведения (ГП)* автомата A в A`.

Ниже мы используем сокращенные названия – обозначения: ОГП(A, A`), УОГП(A, A`) или ОГП(A, A`) в узком смысле и ГП(A, A`) для обобщенного гомоморфизма поведения, обобщенного гомоморфизма поведения в узком смысле и гомоморфизма поведения A в A` соответственно, а для $\Phi = (\Phi_1, \Phi_2, \Phi_3)\in$УОГП(A, A`) и $\varphi = (\varphi_1, \varphi_2, \varphi_3)\in$ГП(A, A`) мы используем обозначения Φ(A), φ(A) для образов автомата A.

Пусть $\Phi = (\Phi_1, \Phi_2, \Phi_3)\in$УОГП (A,A`). Тогда из первого равенства

$$\Phi_2(x(2), h_{x(1)}s_1) = h`_{\Phi_1(x(1),\ s_1)}\Phi_2(x(1), s_1)$$

определения 2 для внутреннего состояния $s\in S$ автомата A получаем

$$\Phi_2(x, s) = \Phi_2(x', s)$$

при любых $(x, x')\in X$.

Из данных равенств вытекает *следующее утверждение.* Если $\Phi = (\Phi_1, \Phi_2, \Phi_3)\in$УОГП(A,A`) и $\varphi_1, \varphi_2, \varphi_3$ – соответствующие ограничения отображений $\Phi_1, \Phi_2, \Phi_3$ на $X\times J(S, A)$, то $\varphi = (\varphi_1, \varphi_2, \varphi_3)\in$ГП(J(A), A`). Здесь отождествлено обозначение ограничения отображения Φ_2: $X\times S\to S`$ на $X\times J(S, A)$ с соответствующим отображением $\varphi_2$: $J(S,A)\to S`$ (у ограничения Φ_2 первая переменная является несущественной).

Полученную тройку отображений $\varphi = (\varphi_1, \varphi_2, \varphi_3) \in ГП(J(A), A`)$ будем называть *ограничением* ОГП $\Phi = (\Phi_1, \Phi_2, \Phi_3)$ в узком смысле A в A`, а $\Phi = (\Phi_1, \Phi_2, \Phi_3) \in УОГП(A, A`)$ – *продолжением* $\varphi = (\varphi_1, \varphi_2, \varphi_3) \in ГП\ (J\ (A), A)$.

Замечание 1. Несложно проверить, что ГП $\varphi = (\varphi_1, \varphi_2, \varphi_3)$ автомата J(A) в A` допускает продолжение до ОГП $\Phi = (\Phi_1, \Phi_2, \Phi_3)$ в узком смысле A в A` тогда и только тогда, если для образа $\varphi(A)$ автомата имеет место включение $\varphi(A) \subseteq J(A`)$. Каждый ОГП $\Phi = (\Phi_1, \Phi_2, \Phi_3)$ в узком смысле A в A` получается из своего ограничения – ГП $\varphi = (\varphi_1, \varphi_2, \varphi_3)\ J_n\ (A)$ в A` соответствующим доопределением отображений $\varphi_1, \varphi_2, \varphi_3$ на множестве $X \times (S \backslash J(S, A))$ (знак \ обозначает минус).

Для этого предварительного находятся решения уравнения

$$s`_0 = h`_{x`} s`,$$

относительно $(x`, s`) \in X \times S`$, при каждом $s`_0$, которое получается из каждой пары (s, x), где $s \in S \backslash J(S,A)$ и $x \in X$, по правилу: $s`_0 = \varphi_2\,(h_x s)$.

С практической точки зрения данное замечание для автоматов A с небольшой мощностью входного алфавита и с небольшим числом внешних состояний сводит поставленную задачу описания множества УОГП $(A, \overline{A})$ и множества всех образов УОГП(A) автомата A при ОГП в узком смысле к описанию гомоморфизмов поведения автомата J(A) в A` и множества всех образов $\varphi(A)$ при ГП A.

Замечание 2. Заметим, что отображение φ_2, фигурирующее в определении 4, и отображение Φ_3 из определения 2 полностью пределяются *соответственно* отображениями $(f`_{x`})_{x` \in X`}$, φ_1, φ_2 и $(f`_{x`})_{x` \in X`}$, Φ_1, Φ_2, в связи с чем *поставленные задачи сводятся к описанию гомоморфизмов поведения ассоциированных с A и A` автоматов без выходов* $A_M = (X, S, (h_x)_{x \in X})$, $A`_M = (X`, S`, (h`_{x`})_{x` \in X`})$.

16.3. Гомоморфизм поведения автоматов

Для автомата A = (X, S, Y, h, f) введем следующее обозначения. Для $S_j \subseteq S$ положим $\mathcal{S}_j = X \times S_j$, а для $M \subseteq X \times S$ – $h(M) = \{s': h_x s = s', (x, s) \in M\}$.

Приведенное выше *замечание 2 позволяет для описания гомоморфизмов поведения (ГП) автомата A в дальнейшем ограничиться рассмотрением лишь автомата A без выходов*, тем не менее сле-

дующие вспомогательные понятия и утверждения представляют интерес и для производных автоматов.

Определение 5. Конгруэнцией поведения автомата A = (X, S, Y, h, f) назовем тройку разбиений: разбиения $P_{X\times S} = \{K_j\}_{j\in\overline{1,m}}$, $P'_{X\times S} = \{K'_j\}_{j\in\overline{1,m'}}$ множества X×S и разбиения $P_S = \{S_j\}_{j\in\overline{1,n}}$ множества S, для которых выполнено условие: если для $j\in\overline{1,m}$, $j`\in\overline{1,n}$ $K_j \cap \mathcal{S}_{j'} \neq \varnothing$, то существуют $j''\in\overline{1,n}$ j'''и $\in\overline{1,m'}$, при которых $h(K_j \cap \mathcal{S}_{j'})\subseteq S_{j''}$, $K_j \cap \mathcal{S}_{j'} \subseteq K'_{j'''}$, где, напомним, для $S_j\subseteq S$ положено $\mathcal{S}_j = X\times S_j$.

Определение 6. Фактор-автоматом по конгруэнции поведения $P_{X\times S} = \{K_j\}_{j\in\overline{1,m}}$, $P'_{X\times S} = \{K'_j\}_{j\in\overline{1,m'}}$, $P_S = \{S_j\}_{j\in\overline{1,n}}$ автомата A = = (X, S, Y, h, f) назовем, вообще говоря, частичный автомат $A/P_{X\times S}, P'_{X\times S}, P_S = (P_{X\times S}, P_S, P'_{X\times S}, \Delta, F)$, где Δ: $P_{X\times S}\times P_S \to P_S$, F: $P_{X\times S}\times P_S \to P'_{X\times S}$ такие, что если

$$K_j \cap S_{j'} \neq \varnothing,\ h(K_j \cap \mathcal{S}_{j'})\subseteq S_{j''},\ K_j \cap \mathcal{S}_{j'} \subseteq K'_{j'''},$$

то

$$\Delta(K_j, S_{j'}) = S_{j''},\ F(K_j, S_{j'}) = K'_{j'''},$$

где, напомним, для $S_j\subseteq S$ положено $\mathcal{S}_j = X\times S_j$, а для $M\subseteq X\times S$ положено $h(M) = \{s': h_x s = s', (x, s)\in M\}$.

Обозначим через S[s], K[x,s], K'[x,s] блоки разбиений P_S, $P_{X\times S}$, $P'_{X\times S}$, содержащие $s\in S$ и $(x, s)\in X\times S$ соответственно.

Для гомоморфизма поведения (φ_1, φ_2, φ_3) автомата A в A` через $\varphi_1(X\times S)$ обозначим образ множества X×S при отображении $\varphi_1$, аналогичные обозначения используем и для $\varphi_2$, $\varphi_3$. Прообразы элементов x`, s`, y` отображений φ_1, φ_2, φ_3 будем обозначать соответственно $\varphi_1^{-1}(x`)$, $\varphi_2^{-1}(s`)$, $\varphi_3^{-1}(y`)$.

С использованием приведенных выше определений стандартными приемами теории автоматов несложно доказывается следующая теорема.

Теорема 1. Если $P_{X\times S}$, $P'_{X\times S}$, P_S – конгруэнции поведения автомата A = (X, S, Y, $(h_x)_{x\in X}$, $(f_x)_{x\in X}$), то тройка отображений φ_1: $X\times S\to P_{X\times S}$, φ_2: $S\to P_S$, φ_3: $X\times S\to P'_{X\times S}$, где $\varphi_1(x, s) = K[x, s]$, $\varphi_2(s) = S[s]$, $\varphi_3(x, s) = K'[x, s]$ – является гомоморфизмом поведения автомата A на автомат $A/P_{X\times S}, P'_{X\times S}, P_S$.

Если (φ_1, φ_2, φ_3)-гомоморфизм поведения автомата A = (X, S, Y, (h, f) в автомат A = (X`, S`, Y`, h`, f`), то тройка разбиений

$P\varphi_1 = \{\varphi_1^{-1}(x`), x`\in\varphi_1(X\times S)\}$, $P\varphi_3 = \{\varphi_3^{-1}(y`), y`\in\varphi_3(X\times S)\}$, $P\varphi_2 = \{\varphi_2^{-1}(s`), s`\in\varphi_2(S)$ – является конгруэнцией поведения автомата A и кроме того образ автомата A при ГП (φ_1, φ_2, φ_3) изоморфен автомату $A/P\varphi_1, P\varphi_3, P\varphi_1$.

Замечание 3. Отметим, что во второй части сформулированной теоремы имеется в виду изоморфизм, вообще говоря, частичных автоматов. Нетрудно заметить, что автомат $A/P_{X\times S}, P'_{X\times S}, P_S$, указанный в первой части теоремы, является полностью определенным тогда и только тогда, когда $K_j \cap \mathcal{S}_{j'} \neq \varnothing$ для любых $j\in\overline{1,m}$, $j'\in\overline{1,n}$.

Таким образом, *для описания с точностью до изоморфизма всех образов автомата A = (X, S, Y, h, f) при гомоморфизме поведения достаточно указать способ построения всех его конгруэнций поведения.*

Переформулировка данных определений и утверждения теоремы 1 для автоматов без выходов не представляет затруднений. Учитывая сделанное ранее замечание 2 о том, что для описания гомоморфизмов поведения (ГП) автомата A в дальнейшем можно ограничиться рассмотрением лишь автомата A без выходов, *перейдем к построению всех конгруэнций поведения автомата без выходов.*

16.4. Построение всех конгруэнций поведения автомата без выходов

Пусть $P_S = \{S_j\}_{j\in\overline{1,n}}$ – произвольное фиксированное разбиение множества состояний S автомата без выходов A = (X, S, h). Оно индуцирует разбиение $P_{X\times S} = \{\mathcal{S}_{j'}\}_{j\in\overline{1,n}}$ множества X×S. Для каждого $j\in\overline{1,n}$ строим произвольное фиксированное разбиение $P_{\mathcal{S}_j} = \{K_c^j, c\in\overline{1,N_j}\}$ множества $\mathcal{S}_j$ с условием: для любого $K_c^j \in P_{\mathcal{S}_j}$ найдется $j'\in\overline{1,n}$, при котором $h(K_c^j)\subseteq S_{j'}$. Положим $P^{э}_{X\times S} = \{K_c^j, j\in\overline{1,n}, c\in\overline{1,N_j}\}$. Назовем данное разбиение элементарным разбиением X×S, соответствующим разбиению P_S. Построенная таким образом пара разбиений $P^{э}_{I\times S}$, P_S множеств X×S, S соответственно является, очевидно, конгруэнцией поведения автомата A = (X, S, h). Назовем эту пару: $P^{э}_{I\times S}$, P_S – элементарной конгруэнцией поведения автомата A.

Определение 7. Пусть пара $P^{э}_{X\times S} = \{ K^{j}_{c}, j\in\overline{1,n}, c\in\overline{1,N_j} \}$, $P_S = \{S_j\}_{j\in\overline{1,n}}$ – произвольная элементарная конгруэнция поведения автомата без выходов А. Будем говорить, что блоки K^{j}_{c}, $K^{j'}_{c'}$ из $P^{э}_{I\times S}$ *неотличимы (относительно P_S)*, если j = j' и найдется $j''\in\overline{1,n}$, при котором

$$h(K^{j}_{c})\subseteq S_{j''},\ h(K^{j'}_{c'})\subseteq S_{j''};$$

в противном случае будем говорить, что они *различимы (относительно P_S)*.

Произвольное разбиение $P^{П}_{X\times S} = \{ K_j, j\in\overline{1,N} \}$ множества X×S назовем продолжением элементарного разбиения $P^{э}_{X\times S} = \{ K^{j}_{c}, j\in\overline{1,n}, c\in\overline{1,N_j} \}$, а $P^{П}_{X\times S}$, P_S – продолжением элементарной конгруэнции поведения $P^{э}_{X\times S}$, P_S, если выполнены два условия:

1) каждый блок K_j, $j\in\overline{1,N}$ является объединением некоторых блоков из $P^{э}_{X\times S}$;

2) для любых $j\in\overline{1,N}$, $j'\in\overline{1,n}$ множество $S_{j'} \cap K_j$ является либо пустым множеством, либо состоит из объединения некоторых неотличимых блоков разбиения $P^{э}_{X\times S}$. Другими словами, различимые блоки разбиения $P^{э}_{X\times S}$ лежат заведомо в разных блоках разбиения $P^{П}_{X\times S} = \{ K_j, j\in\overline{1,N} \}$.

Несложно проверить, что *любая конгруэнция поведения автомата А является продолжением некоторой его элементарной конгруэнции поведения.*

Таким образом, нами фактически указан алгоритм поиска всех образов автомата без выходов при гомоморфизмах поведения.

С учетом сделанных выше замечаний, тем самым дано конструктивное описание гомоморфизмов поведения произвольного конечного автомата и множества его образов.

16.5. Полностью определенные образы автомата при гомоморфизмах поведения

Представляет интерес описание полностью определенных образов автомата при гомоморфизмах поведения. Для этого, очевидно, достаточно (см. замечание 2) дать описание полностью определен-

ных образов автомата без выходов. Для этого введем дополнительные обозначения.

Пусть $P_S = \{S_j\}_{j\in\overline{1,n}}$ – произвольное фиксированное разбиение множества состояний S автомата A = (X, S, h). Для произвольного фиксированного элементарного разбиения $P^{э}_{X\times S} = \{K^j_c,\ j\in\overline{1,n},\ c\in\overline{1,N_j}\}$ обозначим через $\mathrm{rang}(P^{э}_{X\times S}, \mathcal{S}_j)$ число *различимых блоков* из $P^{э}_{X\times S}$ (см. определение 7), содержащиеся в $\mathcal{S}_j$, $j\in\overline{1,n}$. Введем обозначения

$$r_{P_S} = \max_{j\in\overline{1,n}} \mathrm{rang}(P^{э}_{X\times S}, \mathcal{S}_j),$$

$$m_{P_S} = \min_{j\in\overline{1,n}} |\mathcal{S}_j|.$$

Заметим, что при заданном разбиении P_S параметр r_{P_S} не зависит от выбора элементарного разбиения (соответствующего разбиению P_S).

Выясним условия, при которых из заданной элементарной конгруэнции поведения $P^{э}_{X\times S}$, P_S автомата A = (X, S, h) можно построить конгруэнцию поведения $P^{П}_{X\times S} = \{K_j,\ j\in\overline{1,N}\}$, P_S, являющуюся ее продолжением, при которой фактор-автомат $A/P^{П}_{X\times S}$, P_S является полностью определенным автоматом.

Очевидно, из построения продолжения $P^{П}_{X\times S}$, P_S, $P^{П}_{X\times S} = \{K_j\}_{j\in\overline{1,N}}$ элементарной конгруэнции $P^{э}_{X\times S}$, P_S следует: если $K_j \cap \mathcal{S}_{j'} \neq \varnothing$ для $j\in\overline{1,N}$, $j'\in\overline{1,n}$, то $N\le m_{P_S}$, $N\ge r_{P_S}$ и, в частности, $r_{P_S} \le m_{P_S}$. Обратно, если для заданного разбиения $P_S = \{S_j,\ j\in\overline{1,n}\}$ множества S $r_{P_S} \le m_{P_S}$, то нетрудно указать элементарное разбиение $P^{э}_{X\times S}$ и его продолжение $P^{П}_{X\times S} = \{K_j,\ j\in\overline{1,N}\}$, при $N = r_{P_S}$, для которых $K_j \cap \mathcal{S}_{j'} \neq \varnothing$ при любых $j\in\overline{1,N}$, $j'\in\overline{1,n}$, то есть указать продолжение, при котором фактор-автомат $A/P^{П}_{X\times S}$, P_S является полностью определенным. Таким образом, доказано следующее утверждение.

Утверждение 1. Для автомата A = (X, S, h) и разбиения $P_S = \{S_j,\ j\in\overline{1,n}\}$ множества S существует конгруэнция поведения автомата A вида $P_{X\times S}$, P_S, при которой фактор-автомат $A/P_{X\times S}$, P_S полностью определен тогда и только тогда, когда $r_{P_S} \le m_{P_S}$.

Из определения 7 неотличимых (различных) блоков (относительно заданного разбиения $P_S = \{S_j, j \in \overline{1,n}\}$ вытекает, что $r_{P_S} \le n$. Следовательно, для любого разбиения $P_S = \{S_j, j \in \overline{1,n}\}$ множества состояний S автомата без выходов A, для которого $n \le |S_j|$ для всех $j \in \overline{1,n}$, найдется конгруэнция поведения автомата A вида $P_{X \times S}$, P_S, $P_{X \times S} = \{K_j, j \in \overline{1,N}\}$, N<n, для которых фактор-автомат $A/P_{X \times S}$, P_S полностью определен, причем $Nn \le n^2$.

Таким образом, доказана следующая теорема.

Теорема 2. Для автомата A = (X, S, h), $|S| \ge 4$ при любом n с условием $2 \le n \le \sqrt{|S|}$ найдется при гомоморфизме поведения его полностью определенный образ – автомат A = (X`, S`, h`), у которого $|X` \times S`| \le n^2 < |S|$.

Для практических приложений в ряде случаев представляет интерес рассмотрение образов заданного автомата при некоторых частных случаях его гомоморфизмов поведения.

16.6. Частные случаи гомоморфизма поведения автоматов

Пусть $(\varphi_1, \varphi_2, \varphi_3)$ – гомоморфизм поведения автомата A = (X, S, Y, h, f) в автомат A = (X`, S`, Y`, h`, f`). Возможны следующие случаи:

1. Отображение φ_3 представимо в виде $\varphi_3(x, s) = \psi(x, f_x s)$, где $\psi: X \times Y \to Y`$.

1a. $\varphi_3(x, s) = \psi(f_x s)$, где $\psi: Y \to Y`$.

2. Отображение φ_1 представимо в виде $\varphi_1(x, s) = \varphi(x, f_x s)$, где $\varphi: X \times Y \to X`$.

2a. $\varphi_1(x, s) = \varphi(\beta_x s)$, где $\varphi: Y \to Y`$.

При выполнении для отображений $\varphi_1, \varphi_2, \varphi_3$ некоторых из рассматриваемых условий будем говорить для краткости что $(\varphi_1, \varphi_2, \varphi_3)$ является гомоморфизмом поведения автомата A в $\overline{A}$ соответствующего типа. Например, при выполнении условий 1, 2a тройка $(\varphi_1, \varphi_2, \varphi_3)$ является гомоморфизмом поведения A в A` типа 1, 2a.

Для гомоморфизма поведения соответствующего типа автомата A в A` аналогично определениям 5, 6 вводятся понятия конгруэнции поведения соответствующего типа, фактор-автомата по конгруэн-

ции соответствующего типа и легко доказываются аналогии теоремы 6. Рассмотрим несколько таких примеров.

Для автомата $A = (X, S, Y, h, f)$ и $M \subseteq X \times S$ положим

$$F(M) = \{(x, f_x s) : (x, s) \in M\}.$$

Определение 8. Конгруэнцией поведения типа 1 автомата A назовем тройку разбиений множеств $X \times S$, S, $X \times Y$

$$P_{X\times S} = \{K_j\}_{j\in\overline{1,m}}, \; P_S = \{S_j\}_{j\in\overline{1,n}}, \; P_{X\times Y} = \{\chi_j\}_{j\in\overline{1,L}},$$

для которых пара $P_{X\times S}$, P_S является конгруэнцией поведения автомата без выходов $A_M = (X, S, Y, h)$, ассоциированного с A, причем для любых $j' \in \overline{1,m}$, $j \in \overline{1,n}$ найдется $j'' \in \overline{1,L}$, при котором $F(K_{j'} \cap \mathcal{S}_j) \subseteq \chi_{j''}$.

Конгруэнция поведения типа 1а автомата A отличается от типа 1 лишь заменой разбиения $P_{X\times Y}$ на разбиение $P_Y = \{Y_j\}_{j\in\overline{1,L}}$ множества Y и требованием $F(K_{j'} \cap \mathcal{S}_j) \subseteq Y_{j''}$.

Определение 9. Фактор-автоматом по конгруэнции поведения типа 1 автомата A назовем, вообще говоря, частичный автомат $A/P_{X\times S}, P_S, P_{X\times Y} = (P_{X\times S}, P_S, P_{X\times Y}, \Delta, \beta)$, где $\Delta : P_{X\times S} \times P_S \to P_S$, и $\beta: P_{X\times S} \times P_S \to P_{X\times Y}$ такие, что если $K_j \cap \mathcal{S}_{j'} \neq \varnothing$ и $h(K_j \cap \mathcal{S}_{j'}) \subseteq S_{j''}$, $F(K_j \cap \mathcal{S}_{j'}) \subseteq \chi_{j'''}$, то $\Delta(K_j, S_{j'}) = S_{j''}$ и $\beta(K_j, S_{j'}) = \chi_{j'''}$.

Перейдем к рассмотрению гомоморфизма поведения типа 2 автомата A.

Для $\chi \subseteq X \times Y$ *положим* $\mathcal{X}_\chi = \{(x, s) : (x, f_x s) \in \chi\}$.

Определение 10. Конгруэнцией поведения типа 2 автомата A назовем тройку разбиений множеств $X \times Y$, S, $X \times S$

$$P_{X\times Y} = \{\chi_j\}_{j\in\overline{1,m}}, \; P_S = \{S_j\}_{j\in\overline{1,n}}, \; P_{X\times S} = \{K'_j\}_{j\in\overline{1,L}},$$

для которых выполнено условие: если $\mathcal{X}_{\chi_j} \cap \mathcal{S}_{j'} \neq \varnothing$ $j \in \overline{1,m}$, $j' \in \overline{1,n}$, то существуют $j'' \in \overline{1,n}$, $j''' \in \overline{1,L}$, при которых

$$h(\mathcal{X}_{\chi_j} \cap \mathcal{S}_{j'}) \subseteq S_{j''}, \; \mathcal{X}_{\chi_j} \cap \mathcal{S}_{j'} \subseteq K'_{j'''}.$$

Положим для $Y_j \subseteq Y$ $\mathcal{Y}_{Y_j} = \{(x, s) : f_x s \in Y_j\}$. Конгруэнция поведения типа 2а автомата A отличается от типа 2 тем, что вместо разбиения $P_{X\times Y} = \{\chi_j\}_{j\in\overline{1,m}}$ рассматривается разбиение $P_Y = \{Y_j\}_{j\in\overline{1,m}}$ с требованием

$$h(\mathcal{Y}_{Y_j} \cap \mathcal{S}_{j'}) \subseteq S_{j''}, \; \mathcal{Y}_{Y_j} \cap \mathcal{S}_{j'} \subseteq K'_{j'''}.$$

Определение 11. Фактор-автоматом по конгруэнции поведения типа 2 автомата A назовем, вообще говоря, частичный автомат $A/P_{X\times O}$, P_S, $P_{X\times S}$ = ($P_{X\times Y}$, P_S, $P_{X\times S}$, Δ , f), где Δ : $P_{X\times Y}\times P_S \to P_S$, f: $P_{X\times Y}\times P_S \to P_{X\times S}$ такие, что если ($\mathcal{X}_j$ I $\mathcal{S}_j$') $\neq \varnothing$ и h($\mathcal{X}_j$ I $\mathcal{S}_j$')$\subseteq S_{j''}$, $\mathcal{X}_j$ I $\mathcal{S}_j$' $\subseteq K'_{j'''}$, то Δ (χ_j, S_j) = $S_{j''}$, f(X_j, S_j) = $K'_{j'''}$.

Аналогично уточняются понятия конгруэнции поведения автомата и фактор-автомата по конгруэнции поведения и для остальных случаев.

Наиболее интересными, с точки зрения методов криптографического анализа, являются гомоморфизмы поведения типа 1, 2, типа 1а, 2а, типа 2а конечного автомата A в A`. Так при гомоморфизме поведения типа 1, 2 автомата A в A` для определения его начального состояния s по входной последовательности P = x_1, x_2, ..., x_k и выходной последовательности A(s, P) = y_1, y_2, ..., y_k достаточно по входной последовательности P` = (P`, s`), $x`_j = \varphi_1(x_j, y_j)$ и выходной последовательности Q` = $y`_1$, $y`_2$, ..., $y`_k$, $y`_j = \varphi_3(x_j, y_j)$ автомата A` определить все его начальные состояния s`$\in$S`, для которых A`(s`, P`) = Q`, и опробовать для них состояния из прообразов $\varphi_2^{-1}(s`)$ в автомате A. Параметры эффективности такого метода легко рассчитываются аналогично методу гомоморфизма [5; 29].

В случае гомоморфизма поведения типа 1а, 2а атомата A в A` для определения входной последовательности P и начального состояния s автомата A по его выходной последовательности Q = $y_1$, $y_2$, …, $y_K$ достаточно определить по входной последовательности P` = $x`_1$, $x`_2$, ..., $x`_k$, $x`_j = \varphi_1(y_j)$ и выходной последовательности Q` = $y`_1$, $y`_2$, ..., $y`_k$, $y`_j = \varphi_3(y_j)$ множество состояний {$s`_1$, ..., $s`_m$}, для которых A`(s`, P`) = Q`для s`$\in${$s`_1$, ...,$s`_m$}, и затем опробовать пары из $X^K\times${$s`_1$, ..., $s`_m$} в автомате A.

При гомоморфизме поведения типа 1а автомата A в A` для решения поставленной выше задачи достаточно найти все решения (пары (P`, s`)) уравнения A`(s`, P`) = $y`_1$, $y`_2$, ..., $y`_k$, где $y`_j = \varphi_3(y_j)$. Далее для каждого решения – пары (x`(1), x`(2), ..., x`(k), s`) найти вторые компоненты $s`_j$, j$\in${1, ..., k} последовательности

$$\begin{pmatrix} x`(1) \\ s`_1 \end{pmatrix}, \begin{pmatrix} x`(2) \\ s`_2 \end{pmatrix}, \dots, \begin{pmatrix} x`(k) \\ s`_k \end{pmatrix}$$

по формулам

$$s`_1 = s`,\ s`_j = h`_{x`(j-1)}\dots h`_{x`(1)}s` .$$

Далее надо найти прообразы каждой пары $\begin{pmatrix} x`(j) \\ s`_j \end{pmatrix}$ при отображениях φ_1 , φ_2. Затем отбраковать ложные прообразы с использованием закона функционирования автомата А. Трудоемкости предложенных последних методов рассчитываются вполне аналогично соответствующим трудоемкостям частных случаев метода обобщенных гомоморфизмов [5; 29].

Вопрос об использовании в методах дешифрования образов заданного автомата при его гомоморфизме поведения (ГП) в общем случае остается открытым. Из возможных приложений ГП состоит в его использовании в следующей ситуации. С целью повышения надежности работы вычислительных комплексов используют принцип дублирования некоторых его узлов и блоков, то есть проводят физическую реализацию двух одинаковых автоматов А. В этом случае замена одного автомата на его образ А` при гомоморфизме поведения ($\varphi_1$, $\varphi_2$, $\varphi_3$), с элементами контроля (моделируемыми функциям $\varphi_1$, $\varphi_2$, $\varphi_3$), при удачном выборе А` (например, при малой величине $|X`\times S`|$) может дать экономию элементной базы (при соответствующей потере надежности функционирования). Использование образа А` при ГП автомата А возможно и для решения проблемы соответствия заданной схемы автомата с ее физической реализацией. В этом случае замена схемы на ее образ – автомат А` – может облегчить решение задачи с соответствующей потерей надежности ее решения. Рассмотренные приложения и высказанные соображения дают основание для развития введенных понятий на пути замены отображений в определении обобщенного гомоморфизма поведения автомата А в А` на бинарные отношения.

16.7. Обобщенный многозначный гомоморфизм автоматов

Для произвольных конечных автоматов $A = (X, S, Y, h, f)$ и $A = (X`, S`, Y`, h`, f`)$ положим $Z_A = \{(x, s, f(x,s)): (x, s)\in X\times S\}$, $Z_{A`} = \{(x`,s`,f`(x`,s`): (x`,s`)\in X`\times S`\}$. Мы будем рассматривать бинарные отношения Ф на $Z_A\times Z_{A`}$ и использовать обозначения:

– $(x, s, f(x, s))\Phi(x`, s`, f`(x`, s`)$ – элемент $(x, s, f(x, s))$ находится в отношении Ф с элементом $(x`, s`, f`(x`, s`))$;

– $\Phi(x, s, f(x, s)) = \{(x`, s`, f`(x`, s`)\in Z_{A`}: (x, s, f(x, s))\Phi(x`, s`, f`(x`, s`))$ – образ элемента $(x, s, f(x, s))$ при бинарном отношении Ф;

– $\Phi^{-1}(x`, s`, f`(x`, s`)) =)) = \{(x, s, f(x, s)\in Z_A: (x, s, f(x, s))\Phi(x`, s`, f`(x`, s`))$ – прообраз элемента $(x`, s`, f(x`, s`))$ при бинарном отношении Φ;

– $h(V) = \{h(x, s), (x, s)\in V\}$ для $V\subseteq X\times S$.

Определение 12. Бинарное отношение Φ на $Z_A\times Z_{A`}$ назовем обобщенным многозначным гомоморфизмом автомата A в A` или кратко ОМГ A в A`, если для отношения $\Phi$ и автоматов A, A` выполняются два условия:

1) для любых $(x, s)\in X\times S$

$$\Phi(x, s, f(x, s)) \neq \varnothing,$$

2) если для некоторых $(x, s, f(x, s))\in Z_A$ выполнено

$$(x_1, s_1, f(x_1, s_1))\Phi(x`_1, s`_1, f`(x`_1, s`_1)),$$

то для любого $x_2\in X$ найдется $x`_2\in X`$, при котором

$$(x_2, h(x_1, s_1), f(x_2, h(x_1, s_1)))\Phi(x`_2, h`(x`_1, s`_1), f`(x`_2, h`(x`_1, s`_1))).$$

Пусть φ – некоторое бинарное отношение на $(X\times S)\times(X`\times S`)$, а Φ – бинарное отношение на $Z_A\times Z_{A`}$. Правило: $(x, s)\varphi(x`, s`)$ тогда и только тогда, когда $(x, s, f(x, s))\Phi(x`, s`, f`(x`, s`))$ устанавливает *биекцию* $\eta=\eta(A,A`)$: $\Phi\to\varphi$ ($\varphi = \eta\Phi$) между множеством всех бинарных отношений на $Z_A\times Z_{A`}$ и множеством всех бинарных отношений на $(X\times S)\times(X`\times S`)$. Следовательно, условия 1, 2 определения 12 для бинарного отношения Φ адекватны следующим условиям налагаемым на $\varphi = \eta(\Phi)$:

1) для любых $(x, s)\in X\times S$

$$\varphi(x, s)\neq\varnothing,$$

2) для любых $x`(1), x`(2)\in X`$, $s`_1\in S`$

$$X\times h(\varphi^{-1}(x`(1), s`_1))\subseteq \bigcup_{x`(2)\in X`} \phi^{-1}(x`(2), h`(x`(1), s`_1)).$$

Таким образом, получено равносильное определение (условия (1), (2) для φ) обобщенного многозначного гомоморфизма автомата A в A` в терминах бинарного отношения $\varphi$, определенного на множестве $(X\times S)\times(X`\times S`)$.

Определение 13. Пару: покрытие $\Pi_{X\times S} = (K_1, K_2, ..., K_m)$ множества $X\times S$ и разбиение $P_{\{1,...,m\}} = \{R_1,...,R_m\}$ множества $\{1, ..., m\}$ назовем обобщенной многозначной конгруэнцией автомата $A = (X, S, Y, h, f)$, или кратко, ОМК автомата A, если для любого $j\in\{1,...,m\}$ найдется j`, при котором

$$X\times h(K_j)\subseteq\cup K_v,$$

где объединение берется по всем $v\in R_{j`}$.

Для заданной ОМК

$$\Pi_{X\times S} = (K_1, K_2, ..., K_m),\ P_{\{1,...,m\}} = \{R_1, ..., R_n\}$$

автомата А можно провести двойную нумерацию блоков из $\Pi_{X\times S}$. С этой целью сначала упорядочиваем элементы каждого блока R_j, $j\in\{1, ...n\}$: $R_j = \{j_1, j_2, ..., j_{N(j)}\}$.

Для $r\in\{1, ..., m\}$ положим $K_{v,j} = K_r$, если $r\in R_j = \{j_1, j_2, ..., j_{N(j)}\}$ и $K_r = K_{j`}$ при $j` = j_v$.

Для рассматриваемого покрытия $\Pi_{X\times S}$, блоки которого индексированы теперь двойными номерами из множества @ = $\{(v, j): v\in N(j),\ j\in\overline{1,n}\}$ выполняется свойство: для любой пары $(v, j)\in$@ найдется $j`\in\overline{1,n}$, при котором

$$X\times h(K_{v,j})\subseteq\cup K_{v,j`},$$

где объединение берется по всем $v\in\{1, ... ,N(j`)\}$.

Таким образом, как нетрудно видеть, получено следующее равносильное 13 определение обобщенной многозначной конгруэнции автомата А.

Определение 13`. Обобщенной многозначной конгруэнции (ОМК) автомата А называется покрытие

$$\Pi_{X\times S} = (K_{v,j}: (v,j)\in @,),\ @ = \{(v,j): v\in N(j),\ j\in\overline{1,n}\}$$

множества X×S, для которого для любой пары $(v, j)\in$@ найдется $j`\in\overline{1,n}$, при котором

$$X\times h(K_{v,j})\subseteq\cup K_{v,j`},$$

где объединение берется по всем $v\in\{1, ..., N(j`)\}$.

Заметим, что *индекс j` в определениях 13, 13` определен, вообще говоря, неоднозначно.*

Определение 14. Фактор-автоматом $A/\Pi_{X\times S}$ автомата A = (X, S, Y, h, f) по его ОМГ

$$\Pi_{X\times S} = (K_{v,j}: (v,j)\in @,),\ @ = \{(v,j): v\in N(j),\ j\in\overline{1,n}\}$$

назовем множество всех частично определенных автоматов A^ = = (@, Y^, h^, f^), построенных по правилу: $A^\wedge\in A/\Pi_{X\times S}$ тогда и только тогда, если его пары (входной символ, состояние) имеют вид $(v,j)\in$@, а его функция переходов h^, определенная на @, обладает свойством: h^(v, j) = j` *лишь в случае, если*

$$X\times h(K_{v,j})\subseteq\cup K_{v,j`},$$

где объединение берется по всем $v\in\{1, ..., N(j`)\}$.

Стандартными приемами алгебраической теории автоматов, использованными ранее не один раз, доказываются следующие утверждения.

Теорема 3. Если покрытие

$$\Pi_{X\times S} = (K_{v,j}: (v,j)\in @,),\ @ = \{(v,j): v\in N(j),\ j\in \overline{1,n}\}$$

множества X×S является ОМК автомата A=(X,S,Y,h,f), то бинарное отношение Ф вида:

$(x,s,f_x s)\Phi(v,j,f\hat{}(v,j))$ тогда и только тогда, когда $(x,s)\in K_{v,j}$,

является обобщенным многозначным гомоморфизмом автомата A в каждый автомат A^=(@,Y^,h^,f^) из факторавтомата $A/\Pi_{X\times S}$ автомата A по ОМК $\Pi_{X\times S}$.

ТЕОРЕМА 4. Если Ф – обобщенный многозначный гомоморфизм автомата A=(X,S,Y,h,f) в A`=(X`,S`,Y`,h`,f`), то для φ=ηФ (обозначение η=η(A,A`) введено ранее) покрытие множества X×S вида

$$\Pi_\varphi=(\varphi^{-1}(x`,s`),\ (x`,s`)\in\varphi(X`\times S`))$$

является обобщенной многозначной конгруэнцией автомата A, причем образ Ф(A) автомата A при ОМГ Ф изоморфен одному из автоматов факторавтомата A/Π_φ.

В заключение приведем один частный случай обобщенного многозначного гомоморфизма автоматов названный нами *многозначным гомоморфизмом* (МГ) автомата A=(X,S,Y,h,f) в A`=(X`,S`,Y`,h`,f`). Он определяется тройкой бинарных отношений $(\varphi_1,\varphi_2,\varphi_3)$, соответственно на множествах X×X`, S×S`, Y×Y` со свойствами:

1) образы $\varphi_1(X)$, $\varphi_2(S)$ отношений φ_1, φ_2 равны, соответственно, X`, S`; прообразы $\varphi_1^{-1}(X`)$,$\varphi_2^{-1}(S`)$ отношений φ_1,φ_2 равны, соответственно, X, S;

2) для любых x`∈X`, s`∈S`

$$h(\varphi_1^{-1}(x`),\varphi_2^{-1}(s`))\subseteq\varphi_2^{-1}(h`(x`, s`)),$$
$$f(\varphi_1^{-1}(x`)\varphi_2^{-1}(s`)\subseteq\varphi_3^{-1}(f`(x`, s`)).$$

Задача описания образов A` с заданными множествами X`, S`, Y` при многозначных гомоморфизмах автомата A = (X, S, Y, h, f) для заданных бинарных отношений φ_1, φ_2, φ_3 сводится к нахождению функций h`, f` из приведенных выше включений. Описание таких образов можно получить как следствие теорем 3, 4.

Глава 17. МЕТОДЫ ОПРЕДЕЛЕНИЯ НАЧАЛЬНОГО СОСТОЯНИЯ АВТОМАТА ПО ВХОДНОЙ И ВЫХОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТЯМ С ИСПОЛЬЗОВАНИЕМ ОБОБЩЕНИЙ ПОНЯТИЯ ГОМОМОРФИЗМА АВТОМАТОВ

Получены формулы для сложности методов определения начального состояния автомата по входной и выходной последовательностям с использованием его приближенных моделей, построенных на основе обобщений понятия гомоморфизма автоматов.

17.1. Постановка задачи

Пусть A = (X, S, Y, h, f) – конечный автомат. Через A(s, Q) = = y(1), y(2), …, y(k) обозначим выходную последовательность автомата A, отвечающую его выходному слову Q = x(1), x(2), …, x(k) и начальному состоянию s□S, а через $A_M(s_1, Q)$ – его последовательность состояний

$$A_M(s_1, Q) = s_1, s_2, \ldots, s_k.$$

Требуется найти одно из решений s-совместного уравнения

$$A(s,Q) = y(1), y(2), \ldots, y(k). \qquad (24)$$

При практическом решении этой задачи из известных алгоритмов ее решения обычно выбирают алгоритм с меньшей трудоемкостью. Этот выбор, как правило, зависит от свойств автомата A. Например, при малом числе |S| состояний автомата применяют тотальный метод: опробуют все его состояния s∈S до получения состояния s(0), при котором A(s(0), Q) = y(1), y(2), …, y(L) и объявляют s(0) искомым состоянием. При линейном автомате, то есть в случае, когда система уравнений, описывающих выходную последовательность y(1), y(2), …, y(L), является линейной, решают эту систему методом Гаусса и одно из решений объявляют искомым. В других случаях иногда пытаются найти гомоморфный образ автомата A` с меньшим числом состояний или линейный гомоморфный образ (линейный автомат в упомянутом выше смысле) и решают сначала поставленную задачу для этого образа [29].

В данной работе для решения поставленной задачи выбирается вспомогательный автомат A* = (X, S*, Y, h*, f*) – приближенная модель A. При его выборе стараются максимально удовлетворить каждому из следующих качественно сформулированных условий.

1) Трудоемкость решения уравнения

$$A^*(s^*, Q) = y(1), y(2), \ldots, y(k) \qquad (25)$$

относительно s* сравнительно мала.

2) При известном решении уравнения (25) имеется метод решения уравнения (24) с достаточно небольшой трудоемкостью.

17.2. Определение начального состояния автомата по входной и выходной последовательностям с использованием гомоморфного образа ассоциированного с ним автомата Медведева

Предлагаемый ниже подход к определению начального состояния $s \in S$ автомата $A = (X, S, Y, h, f)$ по входной $Q = x(1), x(2), \ldots, x(L)$ и выходной $A(s, \Im) = Z = y_1, y_2, \ldots, y_L$ последовательностям основан на нахождении приближенной модели автомата A пары: вспомогательного автомата $A^* = (X, S^*, Y^*, h, f^*)$ и выполнения условия У(1): наличия сюрьективного отображения φ: $S \to S^*$, осуществляющего гомоморфизм по состояниям автомата Медведева $A_M = (X, S, Y, h)$, соответствующего автомату A, в автомат Медведева $A_M^* = (X, S^*, Y^*, h^*)$, соответствующего автомату A^*.

Для опробуемого состояния s* автомата A* находится последовательность $A^*(s^*, \Im) = y^*_1, y^*_2, \ldots, y^*_L$, которая сравнивается с заданной последовательностью $A(s, \Im) = Z = y_1, y_2, \ldots, y_L$. Целью сравнения является выяснение наличия события $s^* = \varphi s$ или его отрицания $s^* \neq \varphi s$. Если установлено, что $s^* = \varphi s$, то искомое состояние принадлежит образу $\varphi^{-1}s^*$. В этом случае, опробуя состояния s` из множества $\varphi^{-1}s^*$ в автомате A на предмет проверки равенства $A(s`, \Im) = Z$, можно определить искомое состояние $s \in S$. Для подсчета параметров эффективности такого метода примем следующие соглашения и предположения.

Определим случайные значения $\xi_x = (h_x s, h^*_x s^*)$, $x \in X$, где пара $(s, s^*) \in S \times S^*$ равномерно распределена на множестве $S \times S^*$.

Рассмотрим события

$$B_0 = \{(s, s^*) \in S \times S: \varphi s = s^*\}, \; B_1 = \{(s, s^*) \in S \times S^*: \varphi s \neq s^*\}$$

и вероятность $P(\xi_x = (y, y^*)/B)$, $B \in \{B_0, B_1\}$.

Через У(2) обозначим предположение, состоящее в том, что при входной последовательности $\Im = x(1), x(2), \ldots, x(L)$, выходной последовательности $A(s_0, \Im)$ автомата A и построенной последова-

тельности $A^*(s^*, \Im)$ для опробуемого в автомате A^* состояния $s^* \in S^*$ последовательность

$$(f_{x(1)}s_0, f^*_{x(1)}s^*), (f_{x(2)}h_{x(1)}s_0, f^*_{x(2)}h^*_{x(1)}s^*), \ldots$$
$$\ldots, (f_{x(L)}h_{x(L-1)}\ldots h_{x(1)}s_0, f^*_{x(L)}h^*_{x(L-1)}\ldots h^*_{x(1)}s^*)$$

является случайной выборкой из распределения L-мерной случайной величины $(\xi_{x(1)}, \xi_{x(2)}, \ldots, \xi_{x(L)})$, где $\xi_{x(j)}$, $j \in \{1, \ldots, L\}$ – независимые случайные значения с распределением

$$P(\xi_{x(j)} = (y, y^*)/B_0), \text{ если } (s, s^*) \in B_0,$$
$$P(\xi_{x(j)} = (y, y^*)/B_1), \text{ если } (s, s^*) \in B_1.$$

Через У(3) обозначим условие, состоящее в том, что существует $x \in X$, при котором распределения $P(\xi_x = (y, y^*)/B_0)$ и $P(\xi_x = (y, y^*)/B_1)$ не совпадают.

Определение 1. Статистическим аналогом автомата A для рассматриваемой задачи назовем автомат $A^* = (X, S^*, Y, h^*, f^*)$, удовлетворяющий введенным условиям У1, У3.

Таким образом, если входная последовательность $\Im$ автомата A содержит все элементы алфавита X, A^* – статистический аналог автомата A – и выполняется предположение У2, то можно указать статистический критерий, с помощью которого принимается с ошибками первого и второго рода α, β одно из решений: опробуемое состояние s^* в автомате A^* таково, что $(s_0, s^*) \in B_0)$, то есть s^* – «истинный» вариант либо $(s_0, s^*) \in B_1$, то есть s^* – «ложный» вариант. Алгоритм определения начального состояния автомата A по входной и выходной последовательностям состоит в опробовании всех состояний $s^* \in S^*$, затем тотального перебора всех состояний из классов $\varphi^{-1}(s^*)$ (для всех состояний s^*, признанных по статистическому критерию за «истинный» вариант). Для опробуемого состояния $s`$ из классов $\varphi^{-1}(s^*)$ проверяется равенство $A(s`, \Im) = Z$.

В предположении, что уравнение $A(s, \Im) = Z$ имеет единственное решение и классы $\varphi^{-1}(s^*)$, $s^* \in S^*$ равномощны, трудоемкость T в среднем числе опробований и надежность H такого метода определяются выражениями:

$$T = |S^*| + ((|S^*|-1)\beta + (1-\alpha))\frac{|S|}{|S^*|}; \quad H = 1-\alpha.$$

Отметим, что в предложенном подходе определения начального состояния автомата A при необходимости полагая $Y^* = Y$ можно вместо случайных значений ξ_x, $x \in X$ использовать случайные величины:

$$\eta_x = 1, \text{ если } f_x s = f^*_x s^*,$$
$$\eta_x = 0, \text{ если } f_x s \neq f^*_x s^*, \ x \in X.$$

Внесение соответствующих корректив в сформулированные предположения, условия и выводы не представляет затруднений. Так, например, условие У3 заменяется на условие У'3: существует $x \in X$, для которого распределения $P(\eta_x = \varepsilon/B_0)$ и $P(\eta_x = \varepsilon/B_1)$, $\varepsilon \in \{0, 1\}$, не совпадают.

Приведем формулы расчета некоторых основных параметров статистических критериев, используемых при таком подходе к решения задачи.

Обозначим через $\Delta(x, y, s^*)$ множество состояний $s \in S$, для которых $s \in \varphi^{-1}(s^*)$, $f_x s = y$, а через $^*\Delta(x, y^*)$ – множество состояний $s^* \in S^*$, для которых $f^*_x s^* = y^*$. Тогда

$$P(\xi_x = y, y^*/B_0) = \frac{1}{|S|} \sum_{s^* \in {}^*\Delta(x, y^*)} |\Delta(x, y, s^*)|$$

$$P(\xi_x = y, y^*/B_1) =$$

$$= \frac{1}{((|S^*|-1)|S|} \left(\sum_{s^* \in S^*} |\Delta(x, y, s^*)| \cdot |{}^*\Delta(x, y^*) - \sum_{s^* \in {}^*\Delta(x, y^*)} |\Delta(x, y, s^*)| \right).$$

$$P(\eta_x = 1/B_0) = \frac{1}{|S|} \sum_{s^* \in S^*} |\Delta(x, f_x^* s^*)|$$

$$P(\eta_x = 1/B_1) = \frac{1}{|S|(|S^*|-1)} \sum_{y \in Y, s^* \in S^*} |\Delta(x, y, s^*)| \cdot |{}^*\Delta(x, y) - \sum_{s^* \in S^*} |\Delta(x, f_x^* s^*)|.$$

Укажем некоторые из возможных способов построения вспомогательного автомата A^* для автомата $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$.

Пусть φ – гомоморфизм по состояниям автомата Медведева $A_M = (X, S, Y, h_x)$, соответствующего автомату A, в автомат $A_M = (X, S^*, h^*)$, $|S^*|<|S|$. Для каждого элемента $x \in X$ и множества $\varphi^{-1}(s^*)$, $s^* \in S^*$ определим два элемента $^*y = {}^*y(\varphi^{-1}(s^*),x)$ и $_*y = {}_*y(\varphi^{-1}(s^*), x)$ из Y, удовлетворяющие, соответственно, следующим равенствам:

$$\max_{y \in Y} |\Delta(x, y, s^*) = |\Delta(x, {}^*y, s^*)|,$$

$$\min_{y \in Y} |\Delta(x, y, s^*) = |\Delta(x, {}_*y, s^*)|.$$

Если элемент $^*y$ или $_*y$ предыдущими равенствами определен неоднозначно, то выбираем произвольным образом один из таких элементов. В качестве вспомогательного автомата мы будем рассматривать один из следующих автоматов:

$$A = (X, S^*, Y, h^*, {}^*f),$$

у которого $^*f_x s^* = {}^*y(\varphi^{-1}(s^*),x)$ и автомат

$$_*A = (X, S^*, Y, h^*, {}^*f),$$

у которого $_*f_x s^* = {}_*y(\varphi^{-1}(s^*), x)$.

Следующая лемма дает пример выполнения условий $У_3$, $У'_3$ для автоматов A, $^*A$, (A, $_*A$).

Лемма 1. Пусть частичная функция $\beta_{x(0)}$, $x(0) \in X$, автомата A = = (X, S, Y, h_x, f_x) равновероятна на S и φ – гомоморфизм автомата A_M = (X, S, h) в автомат A_M^* = (X, S*, h*), $|S^*| < |S|$, причем существует $s_0^* \in S^*$, при котором функция $f_{x(0)}$ не равновероятна на множестве $\varphi^{-1}(s_0^*)$. Тогда для автоматов A, *A, (A, $_*A$) выполнены условия $У_3$, $У'_3$.

Доказательство. Отметим прежде всего, что выполнение условия $У'_3$ влечет выполнение условия $У_3$. При выполнении условий леммы имеем:

$$P(\eta_{x(0)} = 1/B_0) = \frac{1}{|S|}\sum_{s^* \in S^*} |\Delta(x, f^*_{x(0)} s^*)| > \frac{1}{|S||Y|}\sum_{s^* \in S^*} |\phi^{-1}(s^*)| = \frac{1}{|Y|},$$

если рассматривается автомат A;

$$P(\eta_{x(0)} = 1/B_0) < \frac{1}{|S||Y|}\sum_{s^* \in S^*} |\phi^{-1}(s^*)| = \frac{1}{|Y|}$$

для автомата *A. В то же время, если $P(\eta_{x(0)} = 1/B_0) = P(\eta_{x(0)} = 1/B_1)$, то

$$P(\eta_{x(0)} = 1/B_0) = P(\eta_{x(0)} = 1/B_1) = P(\eta_{x(0)} = 1) =$$
$$= \frac{1}{|S||S^*|}\sum_{y \in Y} |f^{-1}_{x(0)}(y)| \cdot |f^{*-1}_{x(0)}(y)| = \frac{1}{|Y|}$$

как при f* = *f, так и при f* = $_*f_x$, и лемма полностью доказана.

Предложенный подход к определению начального состояния автомата A по входной и выходной последовательностям, при наличии дополнительной информации об автомате A, допускает некоторые уточнения, возможно, повышающие его эффективность. Приведем примеры такой модификации.

Пример 1. Предположим, что среди вспомогательных автоматов для автомата A можно выбрать векторный автомат A*, линейный по выходу, то есть A* = (X, S*, Y*, h_x^*, f_x^*) таков, что при любом входном слове x(1), x(2), …, x(j), j∈{1, 2, …} функция $f_{x(j)}^* h_{x(j-1)}^* \ldots h_{x(1)}^*$ линейна на S^*.

Пусть $\mathfrak{I}$ = x(1), x(2), …, x(L) – известная входная последовательность и $A(s_0, \mathfrak{I}) = y_1, y_2, \ldots, y_L$ – известная выходная последовательность автомата A. Тогда нахождение «истинного» варианта s_0^*

то есть $s_0^* = \varphi(s_0)$, может быть осуществлено с помощью решения системы линейных уравнений

$$f_{x(1)}^* s^* = y_1^*$$
$$f_{x(2)}^* h_{x(1)}^* s^* = y_2^*$$
$$\dots\dots\dots\dots\dots\dots$$
$$f_{x(L)}^* h_{x(L-1)}^* \dots h_{x(1)}^* s^* = y_L^*$$

с искаженной правой частью, где вероятность искажения знака y_j^* естественным образом задается с помощью распределения

$$P(\xi_{x(j)} = y, y^*/B_0),\ (y, y^*) \in Y \times Y^*.$$

Пример 2. Пусть автомат $A = (X, S, Y, h, f)$ является последовательным соединением двух автоматов $A(1) = (X(1), S(1), Y(1), h(1), f(1))$ и $A(2) = (X(2), S(2), Y(2), h(2), f(2))$ (рис. 10). При этом $X=X(1)$, $Y=Y(2)$, $Y(1)=X(2)$, $S=S(1)\times S(2)$, $|S_1|>1$, $|S_2)>1$.

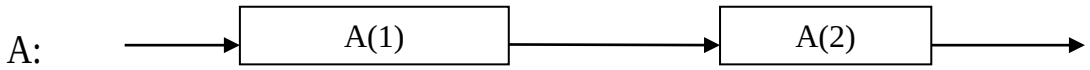

Рис. 10

Таким образом, при $x \in X$, $(s(1), s(2)) \in S(1)\times S(2)$

$$h_x(s(1), s(2)) = (h(1)_x s(1),\ h(2)_{f(1)_x s(1)} s(2)),$$
$$f_x(s(1), s(2)) = f(2)_{f(1)_x s(1)} s(2).$$

Очевидно, множества $\{(s(1), S(2))\}$ представляют собой блоки системы импримитивности автомата A. В качестве вспомогательного автомата A^* возьмем автомат $A(1)$. Определим, как и ранее, случайные переменные $\xi_x = (f_x s, f_{x^*} s^*)$, $x \in X$, где пары $(s, s^*) \in S\times S(1)$ равномерно распределены на множестве $S\times S(1)$ и события:

$$B_0: \{(s, s^*) \in SxS(1),\ s = (s(1), s(2)): s(1) = s^*\};$$
$$B_1: \{(s, s^*) \in SxS(1),\ s = (s(1), s(2)): s(1) \neq s^*\}.$$

Вероятности $P(\xi_x = (y, y^*)/B)$, $B \in \{B_0, B_1\}$ в нашем случае имеют вид

$$P(\xi_x = (y, y^*)/B_0) = P(f(2)_{f(1)_x s(1)} s(2) = y,\ f(1)_x s(1) = y^*);$$
$$P(\xi_x = (y, y^*)/B_1) = P(f(2)_{f(1)_x s(1)} s(2) = y,\ f(1)_x s^* = y^* / s^* \neq s(1)).$$

Положим

$$\triangle^1(x,\varepsilon) = \{s(1) \in S(1): f(1)_x s(1) = \varepsilon\},\ \varepsilon \in Y(1),$$
$$\triangle^2_{\varepsilon\to y} = \{s(2) \in S(2): f(2)_\varepsilon s(2) = y\},\ y \in Y(2),\ \varepsilon \in Y(1).$$

Тогда

$$P(\xi_x = (y, y^*)/B_0) = \frac{|\rho^1(x, y^*)||\rho^2_{y^*\to y}|}{|S(1)||S(2)|} = P(A(1), x\to y^*)\, P(A(2), y^*\to y),$$

где

$$P(A(1), x\to y^*) = \frac{|\rho^1(x, y^*)|}{|S(1)|},\ P(A(2), y^*\to y) = \frac{|\rho^2_{y^*\to y}|}{|S(2)|}$$

и

$$P(\xi_x = (y,y^*)/B_1) = \frac{|\rho^1(x, y^*)|\left(\sum_{\varepsilon\in Y(1)} |\rho^1(x,\varepsilon)||\rho^2_{\varepsilon\to y}|\right) - |\rho^1(x, y^*)||\rho^2_{y^*\to y}|}{|S(1)|^2|S(2)| - |S(1)||S(2)|} =$$

$$= \frac{1}{|S(1)|-1}\rho^1(x, y^*)P(A, x\to y) - \frac{1}{|S(1)|-1}\ P(\xi_x = (y, y^*)/B_0),$$

где $P(A, x\to y)$ – вероятность получения выходного знака y» автомата A при случайном и равновероятном выборе его начального состояния из множества S при условии, что x – его входной символ. Очевидно, справедливо приближенное равенство

$$P(\xi_x = (y, y^*)/B_1) \approx P(A(1), x\to y^*)\, P(A, x\to y).$$

Определение начального состояния $s_0 = (s_0(1), s_0(2))$ автомата A по его входной последовательности $\Im = x(1), x(2), \ldots, x(L)$ и выходной последовательности $A(s_0,\Im) = (y^0_1, y^0_2, \ldots, y^0_L)$ с помощью построенного вспомогательного автомата $A^* = A(1)$ может быть решена последовательным выполнением двух этапов. Первый этап состоит в определении истинной части $s_0(1)$ состояния $s_0 = (s_0(1), s_0(2))$ по известным $\Im$ и $A(s_0, \Im)$. Второй этап состоит в определении второй части $s_0(2)$ состояния s_0 по известным последовательностям $\Im$, $A(s_0, \Im)$ и известному начальному состоянию $s_0(1)$ автомата $A^* = A(1)$. На первом этапе проводится опробование состояний $s(1)\in S(1)$. Для каждого состояния s(1) строится последовательность $A^*(s(1), \Im) = \varepsilon(1), \ldots, \varepsilon(L)$. Предполагая, что последовательность

$$Z = (y^0_1, \varepsilon(1)), (y^0_2, \varepsilon(2)),\ldots, (y^0_L, \varepsilon(L))$$

является случайной выборкой из распределения L-мерной случайной переменной $(\xi_{x(1)}, \xi_{x(2)},\ldots, \xi_{x(L)})$, где $\xi_{x(j)}$, $j\in\{1,\ldots,L\}$ – независимые случайные переменные с распределением $P(\xi_{x(j)} = (y, y^*)/B_0)$, если $s(1) = s_0(1)$, и $P(\xi_{x(j)} =(y,y^*)/B_1)$ если $s(1) \neq s_0(1)$. Для опробуемой части s(1) состояния s относительно рассматриваемой выборки Z выдвигаются, соответственно, две простые гипотезы: H_0 – все случайные переменные $\xi_{x(j)}$ имеют распределения $P(\xi_{x(j)} = (y, y^*)/B_0)$, со-

ответственно, и H_1 – эти же случайные переменные распределены по законам $P(\xi_{x(j)} = (y, y^*)/B_1)$, $j \in \{1, \ldots, L\}$. Таким образом, гипотеза H_0 соответствует опробованию истинной части состояния, а H_1 – ложной.

Для заданной выборки вида Z статистика наиболее мощного критерия в смысле Неймана-Пирсона для проверки гипотез H_0 и H_1 имеет вид

$$V(Z) = \frac{P((\xi_{x(1),}\xi_{x(2)},...,\xi_{x(L),}) = Z / H_0)}{P((\xi_{x(1),}\xi_{x(2)},...,\xi_{x(L),}) = Z / H_1)}.$$

Без ограничения общности полагаем

$$P(\xi_{x(j)} = (y,y^*)/B) > 0,\ B \in \{B_0, B_1\}.$$

При этом

$$P((\xi_{x(1),}\xi_{x(2)},...,\xi_{x(L),}) = Z / H_0) = \prod_{\substack{x \in X \\ (y,\varepsilon) \in Y \times Y(1)}} \left(P(\xi_{x(j)} = (y,\varepsilon) / B_0)\right)^{V(x,y,\varepsilon)},$$

где $V(x, y, \varepsilon)$ – число значений $j \in \{1, \ldots, L\}$, для которых

$$x(j) = x,\ (y^0_j, \varepsilon_j) = (y,\varepsilon).$$

Аналогично

$$P((\xi_{x(1),}\xi_{x(2)},...,\xi_{x(L),}) = Z / H_1) = \prod_{\substack{x \in X \\ (y,\varepsilon) \in Y \times Y(1)}} \left(P(\xi_{x(j)} = (y,\varepsilon) / B_1)\right)^{V(x,y,\varepsilon)},$$

Следовательно,

$$V(Z) = \prod_{\substack{x \in X \\ (y,\varepsilon) \in Y \times Y(1)}} \left(\frac{P(\xi_x = (y,\varepsilon) / B_0)}{P(\xi_x = (y,\varepsilon) / B_1)}\right)^{V(x,y,\varepsilon)}$$

Отсюда следует, что в качестве статистики наиболее мощного критерия можно принять также статистику

$$\ln V(Z) = \sum_{\substack{x \in X \\ (y,\varepsilon) \in Y \times Y(1)}} V(x,y,\varepsilon)\left(\ln P(\xi_x = (y,\varepsilon) / B_0) - \ln P(\xi_x = (y,\varepsilon) / B_1\right)$$

Критическая область гипотезы H_0, определяется неравенством

$$\mathrm{Ln}V(Z) \le C.$$

Введем ошибки этого критерия $\alpha = P(H_1/H_0)$, $\beta = P(H_0/H_1)$. Статистика $\mathrm{Ln}V(Z)$ при $L \to \infty$ имеет асимптотически нормальное распределение при каждой из гипотез Но, H_1. Поэтому при больших значениях L (для не слишком малых значений α, β) можно пользоваться приближенными формулами:

$$\alpha \approx \Phi\left(\frac{c - E(\ln V(Z) / H_0)}{\sqrt{D(\ln V(Z) / H_0)}}\right),\quad \beta \approx 1 - \Phi\left(\frac{c - E(\ln V(Z) / H_1)}{\sqrt{D(\ln V(Z) / H_1)}}\right),$$

где $\Phi(x)$ – функция распределения нормального закона с параметрами (0, 1).

Таким образом, указана вероятностная процедура нахождения истиной части $s_0(1)$ начального состояния $(s_0(1), s_0(2))$ автомата A, характеризующаяся двумя вероятностями α, β.

Если второй этап алгоритма определения начального состояния $(s_0(1), s_0(2))$ автомата A состоит в опробовании состояний $s(2)\in S(2)$ автомата A, то указанная задача определения начального состояния автомата A может быть решена с трудоемкостью (среднем числе опробований)

$$T = |S(1)|+((|S(1)|-1)\beta+(1-\alpha))|S(2)|$$

и надежностью метода $H = 1 - \alpha$.

При получении формулы для T предполагалось единственность решения уравнения $A((s(1), s(2)), \Im) = (y^0_1, y^0_2, \ldots, y^0_L)$.

Замечание 1. Рассматриваемый в данном пункте метод определения начального состояния $s\in S$ автомата $A = (X, S, Y, h, f)$ по входной $Q = x(1), x(2), \ldots, x(L)$ и выходной $A(s, \Im) = Z = y_1, y_2, \ldots, y_L$ последовательностям основан на нахождении приближенной модели автомата A. В случае неэффективности рассматриваемого метода для автомата A, например, в случае отсутствия нетривиальных гомоморфных образов автомата $A_M = (X, S,h)$, что равносильно примитивности полугруппы автомата A, метод может быть редуцирован для так называемой *n*-й степени автомата A. Именно для автомата A рассмотрим следующий автомат, который удобно называть *n*-й степенью автомата A.

$$A^n = (X^n, S, Y^n, h\wedge, f\wedge),$$

где при $X\wedge = X^n$, $x\wedge = (x(1), x(2), \ldots, x(n))\in X^n$,

$$h\wedge_{x\wedge}s = h_{x(n)}h_{x(n-1)}\ldots h_{x(1)}s,\ f_{x\wedge s} = (f_{x(1)}s, f_{x(2)}h_{x(1)}s, \ldots, f_{x(n)}h_{x(n-1)}\ldots h_{x(1)}s).$$

Если $L = nL'$, то сформулированная задача для автомата A адекватна аналогичной задаче для автомата A^n. В ряде случаев выбором n можно добиться наличия необходимых условий для ее решения предложенными методами.

Замечание 2. В работе [17] решалась задача определения начального состояния $s\in S$ автомата A по его входной $Q = x(1), x(2), \ldots, x(L)$ и выходной $A(s, Q) = Z = y(1), y(2), \ldots, y(L)$ последовательностям. Для известных методов решения данного уравнения относительно $s\in S$ выделяется класс автоматов, для которых это уравнение решается с небольшой трудоемкостью. Для остальных автома-

тов A известные методы решения сравнимы по сложности с тотальным методом. Рассматриваемый в [17] подход к решению задачи состоял в выборе для автомата A его приближенной модели – нового вспомогательного автомата $A^* = (X, S, Y, h^*, f)$, отличающегося от A функцией перехода h^*, для которого:

1) для каждого входного символа $x \in X$ и случайно, равновероятно выбранного состояния $s \in S$ вероятность q_x события

$$h_x s = h`_x s \qquad (27)$$

перед этой формулой пропущена нумерация одной формулы

достаточно большая;

2) уравнение вида $A^*(s, Q) = Z$ для нового автомата A^* решается с небольшой трудоемкостью.

Далее применялся один из двух подходов:

1) решали для автомата A^* уравнение

$$A^*(s, x(1), x(2), \ldots, x_k) = y(1), y(2), \ldots, y(k),$$

где k – максимальное из чисел $\{1, 2, \ldots, L\}$, при котором последнее уравнение имеет решение. Данное найденное решение объявлялось искомым решением уравнения $A(s, Q) = Z$;

2) выбирали C из $\{1,2, \ldots, L\}$ и объявляли состояние $s \in S$ ложным, если

$$A(s, x_1, x_2, \ldots, x_C) \neq y_1, y_2, \ldots, y_C.$$

Параметры сложности данного метода рассчитаны в [17].

17.3. Определение начального состояния перестановочного автомата по входным и соответствующим выходным последовательностям с использованием меры неотличимости состояний μ

Для формулировки и обоснования этого метода напомним необходимые нам понятия главы 11 «Приближенные модели автоматов, построенные на основе расстояния Хэмминга между их выходными последовательностями».

Основные понятия. Пусть $A = (X, S, Y, h, f)$, $A` = (X, S`, Y, h`, f`)$ – конечные автоматы и $P_X = (p(x) = \frac{1}{|X|}, x \in X)$ – равномерное вероятностное распределение на X. Для инициальных автоматов A_s, A'_s, $s \in S$, $s' \in S'$ (состояний s, s′ автоматов A, A′) определим величину

$$\mu_N^{s,s'} = \mu_N(A_s, A_{s'}) = \frac{1}{N|X|^N} \sum_{\bar{x} \in X^N} \rho_N(A(s, \bar{x}), A'(s', \bar{x})),$$

где $\rho_N(A(s, \bar{x}), A'(s', \bar{x}))$ – расстояние Хемминга между выходными последовательностями $A(s, \bar{x})$, $A'(s', \bar{x})$ автоматов A, A′, полученных при начальных состояниях $\in S$, $s' \in S$ и входной последовательности $\bar{x} \in X^N$. Качественный смысл введенной величины состоит в том, что она характеризует «плотность несовпадения» их выходных последовательностей.

Положим

$$\bar{\mu}_N = (\mu_N^{s,s'})_{(s,s') \in SxS'}.$$

В параграфе 8.5 доказано, что последовательность $\bar{\mu}_1, \bar{\mu}_2, \ldots$ имеет предел $\bar{\mu} = \left(\mu^{s,s`}\right)_{(s,s`) \in S \times S`}$,

$$\bar{\mu} = UR(1) = \frac{1}{h}\left(E + U + \ldots + U^{h-1}\right)\left(U^h\right)^{\infty} R(1),$$

где U – матрица переходных вероятностей цепи Маркова, моделирующая внутреннее функционирование параллельного соединения B(A, A′) автоматов A, A′ при едином случайном входе, R(1) – вектор столбец $R(1) = (r^{(s,s`,1)})_{(s,s`) \in S \times S`}$, $r^{(s,s`,1)}$ – вероятность события $f_x s \neq f`_x s`$ при случайном и равновероятном выборе $x \in X$, h – период цепи Маркова, а

$$\left(U^h\right)^{\infty} = \lim_{k \to \infty}\left(U^h\right)^k.$$

Величина $\mu^{s,s`} = \varepsilon$ характеризует вероятность несовпадения элементов случайно выбранных пар (y(j), y`(j)) выходных последовательностей $A(s, \bar{x})$, $A'(s', \bar{x})$ с состояний s, s` автоматов A, A` при случайной входной последовательности $\bar{x}$. При этом сами состояния s, s` называются $\mu\varepsilon$-неотличимыми. Напомним, что автомат A = (X, S, Y, h, f) называется перестановочным, если его частичные функции переходов $(h_x)_{x \in X}$ осуществляют биекции S в S.

Пусть A = (X, S, Y, h, f) – перестановочный, связный приведенный [46; 47] автомат с импримитивной группой $G = \langle (h_x)_{x \in X} \rangle$, порожденной частичными функциями переходов $(h_x)_{x \in X}$. Через S(1), S(2), …, S(k), $2 \leq k \leq |S|-1$ обозначим блоки импримитивности группы G. Положим $G_{S(j)}$ – стабилизатор блока S(j) в G; G_s – стабилизатор состояния $s \in S(j)$ в G; G^ – образ G при гомоморфизме φ: $g \to g^\wedge$, где $g^\wedge$ подстановка на множестве блоков S^, индуцированная элементом $g \in G$; $G_{S(j)}|S(j)$ – группа подстановок на S(j), $j \in \{1, 2, \ldots, k\}$, индуцированная ограничением действия группы $G_{S(j)}$ на множестве S(j).

Будем предполагать, что A таков, что автомат A×A, являющийся параллельным соединением автомата A с собой при едином входе, имеет три компоненты связности. Стандартными приемами легко доказывается, что данное условие выполняется тогда и только тогда, когда G^ – дважды транзитивная группа, $G_{S(1)}|S(1)$ – дважды транзитивная группа и $G_s \cap \ker\varphi|S(j)$ – дважды транзитивная группа на каждом блоке S(j), $j \in \{2, \ldots, k\}$, $s \in S(1)$, где $\ker\varphi$ – ядро гомоморфизма $\varphi: G \to G^\wedge$.

Одним из примеров такой группы является группа сплетения $F^1 Wr F^2$ на множестве $S(1) \times S^\wedge$, где F^1 – дважды транзитивная группа на S(1), F^2 – дважды транзитивная группа подстановок множества S^.

В веденных обозначениях имеем $\bar{\mu} = \tilde{U}\tilde{R}(1)$, где матрица $\tilde{U}$ имеет вид

$$\tilde{U} = \begin{Vmatrix} \tilde{U}_1 & & \\ & \tilde{U}_2 & \\ & & \tilde{U}_3 \end{Vmatrix},$$

где $\tilde{U}_1, \tilde{U}_2, \tilde{U}_3$ – равновероятные матрицы, отвечающие компонентам связности вероятностного автомата B(A, A), соответствующего автомату A×A при случайном входе. Первая компонента состоит из состояний вида (s, s``), $s \neq s``$ где s, s``лежат в одном произвольном блоке системы блоков импримитивности S(1), S(2), …, S(k) группы G, вторая – из состояний (s, s``), где s, s`` принадлежат разным блокам, и третья компонента состоит из состояний вида (s, s), $s \in S$. Значение функции μ постоянно на каждой компоненте связности автомата (A×A) и равно вероятности события $f_x s \neq f_x s``$ при случайном и равновероятном выборе $x \in X$ для состояния (s, s``) автомата A×A из первой, второй и третьей компоненты соответственно.

Первые две вероятности μ_1 и μ_2 [15] легко подсчитываются при известном числе решений относительно $s \in S(j)$, $j \in \{1, 2, \ldots, k\}$ уравнений

$$f_x s = y, \quad y \in Y, x \in X.$$

Очевидно, значение μ_3 равно нулю. Предположим дополнительно, что $\mu_1 \neq \mu_2$ и рассмотрим следующую задачу.

17.4. Определение начального состояния s(0) автомата A по его входной Q = x(1), x(2), …, x(L) и выходной A(s(0), Q) = Z последовательностям

Предположим для простоты, что задача имеет единственное решение. Предлагаемый способ ее решения состоит в последовательном опробовании представителей s(j) блоков S(j), $j \in \{1, ..., k\}$. Для каждого опробуемого представителя s(j) вырабатывается последовательность

$$A(s(j), Q) = y^j(1), y^j(2), \ldots, y^j(L).$$

Для нахождения блока S(v), которому принадлежит искомое состояние s(0), используем следующую вероятностную модель. Относительно последовательностей

$$A(s(0), Q) = y(1), y(2), \ldots, y(L);$$
$$A(s(j), Q) = y^j(1), y^j(2), \ldots, y^j(L)$$

предполагаем, что:

а) при s(0), $s(j) \in S(v)$, $S(v) \in \{S(1), \ldots, S(k)\}$, $s(0) \neq s(j)$ каждая пара символов $(y(c), y^j(c))$, $c \in \{1, \ldots, k\}$ получена переработкой автоматом $A \times A$ случайно и равновероятно выбранного символа $x \in X$ при случайно и равновероятно выбранной паре различных начальных состояний из множества $\bigcup_{j=1}^{k} (S(j) \times S(j))$;

б) при s(0), s(j) из разных блоков, указанная пара символов выходного алфавита получена переработкой автоматом $A \times A$ случайно и равновероятно выбранного символа $x \in X$ при случайно и равновероятно выбранных двух начальных состояний автомата A из разных блоков;

в) при s(0)=s(j) указанная пара получена при случайном и равновероятном выборе $x \in X$ и $s \in S$ по правилу: $y_c = f_x s$, $y^j(c) = f_x s$.

Поставим в соответствие предположениям а), б), в) соответствующие гипотезы:

– опробуемое состояние s(j) лежит в одном блоке с искомым состоянием и не равно ему, то есть $\mu^{s(0),\, s(j)} = \mu_1$;

– опробуемое состояние не лежит в одном блоке с искомым состоянием (ложный вариант), то есть $\mu^{s(0),s(j)} = \mu_2$;

– опробуемое состояние совпадает с искомым состоянием, то есть $\mu^{s(0),s(j)} = 0$.

С помощью статистики

$$\sum_{c=1}^{L} f\wedge(y(c), y_c^j),$$

где

$$f\wedge(y(c), y_c^j) = \begin{matrix} 1, & при\ \ y(c) \neq y_c^j, \\ 0, & при\ \ y(c) = y_c^j \end{matrix},$$

Стандартными приемами разделяем сформулированные гипотезы, затем состояния неотсеянных статистическим критерием блоков опробуются в автомате.

17.5. Определение начального состояния автомата по входной и выходной последовательностям с использованием με-неотличимых состояний

Через A = (X, S, Y,h , f) обозначим автомат с параметрами: X = = Y = G, где G – абелева группа, при любом $x \in X$ $h_x = h$, h: $S \to S$, $f_x(s) = f(s)+x$, $x \in X$, $s \in S$, где f: $S \to G$. Пусть P(X) = (p(x), $x \in X$) – вероятностное распределение на X, а Q = x(1), x(2), …, x(L) – выборка длины L из этого распределения. Задача состоит в определении начального состояния s(0) автомата A по входной последовательности Q и выходной последовательности A(s(0), Q) = y_1, …, y_L, а именно решении системы уравнений:

$$x(1)+fs(0) = y_1;$$
$$x(2)+fhs(0) = y_2;$$
$$\dots\dots\dots\dots\dots\dots$$
$$x(j)+fh^{j-1}s(0) = y_j;$$
$$\dots\dots\dots\dots\dots\dots$$
$$x(L)+fh^{L-1}s(0) = y_L$$

относительно s(0).

Предлагаемый метод основан на наличии у вспомогательного автономного автомата B = (S, h, f, Y), h: $S \to S$ με-неотличимых состояний при малом ε. Метод состоит из двух этапов. Сначала последовательно опробуются состояния $s \in S$. Для опробуемого состояния s вычисляется последовательность

$$Q` = (x`(1), x`(2), \dots, x`(j), \dots, x`(L)) = (y_1–fs, y_2–fhs, \dots, y_j–fh^{j-1}s,\dots,y_L–fh^{L-1}s).$$

Статистическим критерием с ошибками первого и второго рода α, β различаем две простые гипотезы: H(0) – последовательность;

Q – выборка из распределения P(X); H(1) – Q – выборка из равномерного вероятностного распределения на X. Те состояния s*, которым соответствует решение о том, что Q получено при гипотезе H(0), принимаются за «близкие» состояния к неизвестному состоянию s(0), то есть $\mu^{s(0),s^*} = \varepsilon$. Для определения s(0) выбираем одно из «близких» состояний s* и и переходим ко второму этапу: решаем систему уравнений

$$fs(0) = fs^* = y`_1$$
$$fhs(0) = fhs^* = y`_2$$
$$\ldots\ldots\ldots\ldots$$
$$fh^{j-1}s(0) = fh^{j-1}s^* = y`_j$$
$$\ldots\ldots\ldots\ldots$$
$$fh^{L-1}s(0) = fh^{L-1}s^* = y`_L$$

с искаженной правой частью, считая, что ее позначные искажения определены вероятностью ε. Параметры сложности решения системы уравнений с искаженной правой частью рассчитаны в [20].

17.6. Определение начального состояния перестановочного автомата по входной и выходной последовательностям с использованием με-гомоморфизмов автоматов

Пусть A = (X, S, Y, h, f) – конечный автомат. Через $A_M = (X, S, (h_x)_{x\square X})$ обозначим ассоциированный с A автомат без выхода. Пусть A* = (X, S*, Y, h*, f*) – еще один автомат с теми же входным и выходным алфавитами.

Определение 2. Сюрьективное отображение φ: S→S называется με-гомоморфизмом автомата A = (X, S, Y, h,f) на A* = (X, S*, Y, h*, f*), если для всех s∈S

$$\mu^{s,\phi s} = \varepsilon.$$

Если дополнительно

$$\mu^{s,s^*} \neq \varepsilon$$

для всех s* ≠ φs, то φ называется точным με-гомоморфизмом. Автомат A* называется образом автомата A при με-гомоморфизме (при точном με-гомоморфизме).

Для автоматов A, A* обозначим через σ = σ(ε) следующее бинарное отношение на S×S*: sσs* тогда и только тогда, если $\mu^{s,s^*} = \varepsilon$. Через $\sigma^{-1}(s^*)$ будем обозначать прообраз элемента s* для σ, а через E_X – тождественное отображение X в X.

Следующее утверждение непосредственно вытекает из определений и свойств меры μ приближенной неотличимости состояний перестановочных автоматов.

Утверждение 1. Если φ: $S \to S^*$ является точным $\mu\varepsilon$-гомоморфизмом связного перестановочного автомата A на перестановочный автомат A*, то (E_X, φ) – гомоморфизм $A_M = (X, S, h)$ на $A^*_M = (X, S^*, h^*)$ и

$$\sigma^{-1}(s^*) = \varphi^{-1}(s^*)$$

для любого $s^* \in S^*$ (E_X – тождественное отображение X в X).

Определение 3. Множество сюрьективных отображений φ_1, φ_2, …, φ_L S в S* называется точным -μ-гомоморфизмом автомата A на A*, если для любого $j \in \{1, \ldots, L\}$ φ_j является точным $\mu\varepsilon$-гомоморфизмом A на A* при некотором $\varepsilon = \varepsilon_j$ и для любых $s \in S$ и $s^* \in S^*$

$$\mu^{s,s^*} \in \{\varepsilon_1, \ldots, \varepsilon_L\}.$$

Автомат A* называется образом автомата A при точном μ-гомоморфизме.

Заметим, что из данных определений следует, что $|\{\varepsilon_1, \ldots, \varepsilon_L\}| = L$. Через $G = \langle (h_x)_{x \square X} \rangle$ обозначим группу перестановочного автомата A, порожденную биекциями $(h_x)_{x \square X}$, через G_s – стабилизатор элемента $s \in S$, G: H – индекс H в G [38].

Теорема 1. Множество $\{\varphi_1, \varphi_2, \ldots, \varphi_L\}$ сюрьективных отображений S в S*, $1<|S^*|<|S|$ является точным μ-гомоморфизмом связного перестановочного автомата A на перестановочный автомат A* тогда и только тогда, если выполнены условия:

1) найдется подгруппа H группы G автомата A, для которой: G: H = L; при некотором $s^* \in S^*$ множество $\{\varphi_1^{-1}(s^*), \ldots, \varphi_L^{-1}(s^*)\}$ является множеством всех ее орбит; $G_s \subset H$ при любом $s \in S$;

2) для каждой пары $\{j(1), j(2)\}$, $j(1) \neq j(2)$, $j(1), j(2) \in \{1, \ldots, L\}$ выполняется неравенство

$$\sum_{x \in X} \sum_{s^* \in S^*} \sum_{s(1) \in \phi_{j(1)}^{-1}(s^*)} f_x^{\wedge}(s(1), s^*) \neq \sum_{x \in X} \sum_{s^* \in S^*} \sum_{s(2) \in \phi_{j(2)}^{-1}(s^*)} f_x^{\wedge}(s(2), s^*),$$

где $f_x^{\wedge}(s, s^*) = 1$ при $f_x s \neq f^*_x s^*$ и $f_x^{\wedge}(s, s^*) = 0$ при $f_x s = f^*_x s^*$.

Доказательство. Пусть $\{\varphi_1, \varphi_2, \ldots, \varphi_L\}$ – точный μ-гомоморфизм A на A*, s* – фиксированное состояние автомата A*, H(j) – стабилизатор множества $\phi_j^{-1}(s^*)$ в G, $j \in \{1, \ldots, L\}$. Так как φ_j – точный $\mu\varepsilon$-гомоморфизм A на A*, то по утверждению 1 для

$j \in \{1, \ldots, L\}$ (E_X, φ_j) – гомоморфизм $A_M = (X, S, (h_x)_{x \square X})$ на $A^*_M = (X, S^*, (h^*_x)_{x \square X})$. Отсюда следует, что $H(j) = H(j`) = H$, для любых $j$, $j` \in \{1, \ldots, L\}$, G: $H = |S^*|$, $G_s \subset H$ при любом $s \in S$. Поэтому

$\{\varphi_1^{-1}(s^*), \ldots, \varphi_L^{-1}(s^*)\}$ – орбиты группы H одинаковой мощности и $L=|S^*|$.

Условие 2 получается из формулы

$$\mu^{s,s^*} = \frac{1}{|X||S \times S^*|} \sum_{x \in X} \sum_{s^* \in S^*} \sum_{s \in \phi^{-1}_{j(1)}(s^*)} f_x^{\wedge}(s, s^*),$$

полученной при доказательстве теоремы 3 главы 11 «Приближенные модели автоматов, построенные на основе расстояния Хэмминга между их выходными последовательностями» ([15] и условия $|\{\varepsilon_1, \ldots, \varepsilon_L\}| = L$).

Достаточность условий теоремы 1 проверяется аналогичным образом.

Замечание 3. Отметим, что подгруппа H нерегулярной группы G подстановок на множестве S, для которой $G_s \subset H$ при любом $s \in S$, содержит нормальный делитель $N = \langle\{G_s, s \in S\}\rangle$ группы G. Для связного перестановочного автомата $A = (X, S, h, f)$ с группой $G = \langle(h_x)_{x \in X}\rangle$, содержащей нетривиальный интранзитивный нормальный делитель N, можно предложить следующий способ построения его образа при точном μ-гомоморфизме.

Пусть $G = \bigcup_{j=1}^{L} g_j N$ – разложение G на левые смежные классы по подгруппе N, а $\chi_1, \ldots, \chi_L$ – орбиты нормального делителя N. Они являются областями импримитивности группы G [47]. Следовательно, определен фактор-автомат

$$A^*_M = (X, S^*, h^*), \; S^* = \{\chi_1, \ldots, \chi_L\}$$

автомата $A_M = (X, S, (h_x)_{x \in X})$ на множестве блоков импримитивности группы G. Для $j \in \{1, \ldots, L\}$ определим частичное отображение ψ_j: $S \to S^*$, положив $\psi_j(s) = \chi_1$ для всех s из χ_j. Очевидно, ψ_j можно продолжить до гомоморфизма φ_j A_M на A^*_M. Для получения образа A^* автомата A при точном μ-гомоморфизме $\{\varphi_1, \varphi_2, \ldots, \varphi_L\}$ определим частичные функции выхода для автомата A^*_M, выбирая их значения на состояниях из $S^* = \{\chi_1, \ldots, \chi_L\}$ так, чтобы выполнялось условие 2

теоремы 1. Это можно сделать не всегда, например, это нельзя сделать для автомата A, у которого число решений уравнения

$$f_x s = y,$$

относительно $s \in \chi_j$, не зависит от $y \in Y$ при каждом $x \in X$ и каждом $j \in \{1, \ldots, L\}$. В последнем случае

$$\mu^{s,\chi_j} = \frac{|Y|-1}{|Y|},\ s \in S,\ j \in \{1, \ldots, L\}.$$

Для связного перестановочного приведенного автомата A = (X, S, Y, h, f) рассмотрим следующую задачу.

17.7. Определение начального состояния s0 автомата по известным входным словам $\mathfrak{I} \in XN$ и соответствующим им выходным словам $A(s0, \mathfrak{I}) = Q(\mathfrak{I})$

Предположим, что задача имеет единственное решение.

Первый метод. Используем понятия работы [15]. Пусть $\Pi = \{\chi_1, \ldots, \chi_L\}$ – некоторая система слабой импримитивности автомата A и A* = (X, S*, Y, h*, f*) – некоторый наилучший П-образ автомата A, $S^* = \{\chi_1, \ldots, \chi_L\}$. Пусть $\mu^{s,s^*} = \varepsilon$ для всех $s \in s^*$, $s^* \in S^*$.

Для решения задачи опробуются все состояния $s^* \in S^*_{s^*(1)}$ для некоторого $s^*(1) \in S^*$. Множество $S^*_{s^*(1)}$ есть множество состояний автомата A*<s*(1)>, порожденного состоянием s*(1) в автомате A*. Для каждого $s^* \in S^*_{s^*(1)}$ подсчитывают величину $\mu_N^{s_0,s^*}$ исходя из определения этой величины. Находят все такие s*, для которых

$$|\mu_N^{s_0,s^*} - \varepsilon| \le \max_{\substack{s \in S \\ s^* \in S^*_{s^*(1)}}} \xi_N^{s,s^*},$$

где ξ_N^{s,s^*} – скорость сходимости величины μ_N^{s,s^*} к μ^{s,s^*}. Для всех найденных s* опробуются все состояния s из множеств s* в автомате A. Если длина N слов достаточно велика, то по кратному эксперименту с каждым состоянием s* автомата A в можно однозначно определить величины μ^{s_0,s^*} и, следовательно, множество всех состояний s*, для которых $\mu^{s_0,s^*} = \varepsilon$. Поставленная задача теперь ре-

шается опробованием в автомате A состояний множеств s* для найденных s*.

Аналогичным образом может быть использован и наихудший П-образ автомата A.

Второй метод. Пусть (φ_1, …, φ_L) – точный μ-гомоморфизм автомата A на связный, перестановочный автомат A*, где φ_j – точный $\mu\varepsilon_j$-гомоморфизм A на A*, $j\in\{1, 2, \ldots, L\}$.

Выберем некоторый параметр C, 0<C<1 и произвольное состояние $s^*\in S^*$ автомата A. Подсчитаем величину $\mu_N^{s_0,s^*}$. Для всех $j\in\{1, \ldots, L\}$, для которых

$$|\mu_N^{s_0,s^*}-\varepsilon_j|<C,$$

опробуем состояния автомата A из множеств $\phi_j^{-1}s^*$ для нахождения искомого s_0. Если N достаточно велико, то по кратному эксперименту с состояний s_0, s* можно однозначно определить величину μ^{s_0,s^*} и, следовательно, j, при котором $\mu^{s_0,s^*}=\varepsilon_j$. Опробуя теперь состояния $s\in\phi_j^{-1}s^*$ в автомате A, находим s_0.

Третий метод. Пусть выполнено условие 1) $\Pi=\{\chi_1, \chi_2, \ldots, \chi_L\}$ – некоторая система слабой импримитивности автомата A [24] и Ae* = (X, S*, Y, h*, f*) – наихудший приближенный автомат к A в классе $F_п(A)$ – всех связных перестановочных автоматов с входным алфавитом X, выходным Y с числом состояний, меньшим |S|, причем мера приближения автомата A к A* равна единице.

Опробованием в автомате A* находят все состояния $s^*\in S^*$, для которых

$$f_{x(k)}h_{x(k-1)}\ldots h_{x(1)}s^*\neq f_{x(k)}h_{x(k-1)}\ldots h_{x(1)}s$$

при всех $(x(1), x(2), \ldots, x(k))\in X\cup X_2\cup\ldots\cup X(N)$.

Опробуя все состояния автомата A, принадлежащие всем найденным множествам s*, находят s_0.

Отметим, что при выполнении указанного выше условия 1) аналогично может решаться задача определения начального состояния автомата A по его входной и выходной последовательностям.

Таким образом, для решения этой задачи при наличии у автомата A наихудшего приближенного автомата в классе $F_п(A)$ с наихудшей мерой приближения равной единице, можно использовать методы, аналогичные известному методу гомоморфизма [29].

17.8. Определение начального состояния (s_0^1, s_0^2) по выходной последовательности A (s_0^1, s_0^2) = g(1), g(2), … , g(N) последовательного соединения автоматов

Рассмотрим автомат A, являющийся последовательным соединением автономного полноциклового автомата $A_1 = ({}^1S, {}^1h, {}^1Y)$ с неавтономным связным перестановочным автоматом $A_2 = ({}^2X, {}^2S, {}^2Y, {}^2h, {}^2f)$, где ${}^1У = {}^2X \times G$, ${}^2Y = G$, где G – группа с операцией o, |G|>1. Для пар (x, g)$\in {}^2X \times G$ частичные функции переходов не зависят от $g \in G$, то есть ${}^2h_{x,g}s^2 = {}^2h_x s^2$, $s^2 \in {}^2S$ частичные функции выходов ${}^2f_{x,g}$ определены так: ${}^2f_{x,g}s^2 = fs^2 \circ g$, где f – некоторая функция f: ${}^2S \to G$. Предположим, что для автомата A_2 наилучшим приближенным автоматом является автомат A_2* с одним состоянием с наилучшей мерой приближения ε, где $\varepsilon < \frac{|G|-1}{|G|}$. Рассмотрим модель A* автомата A – аналогичное последовательное соединение, полученное заменой A_2 на A_2*. Для решения поставленной задачи опробуем состояния s^1 автомата A_1. Для каждого $s^1 \in {}^1S$ получаем последовательность

$$A_1(s^1) = {}^1g(1), {}^1g(2), \ldots, {}^1g(N).$$

Образуем последовательность

$$A\left(s_0^1, s_0^2\right) \circ (A_1(s^1))^{-1} = g(1) \circ ({}^1g(1))^{-1}, g(2) \circ ({}^1g(2))^{-1}, \ldots, g(N) \circ ({}^1g(N))^{-1}.$$

Поставим ей в соответствие двоичную последовательность $y(s^1) = y(1), \ldots, y(N)$, где y(j) = 0, если элемент $g(j) \circ ({}^1g(j))^{-1}$ является единицей группы G и y(j) = 1, в противном случае. Предполагая, что при $s^1 = s_0^1$ последовательность $y(s^1)$ является случайной и независимой выборкой из вероятностного распределения (P(1) = ε, P(0) = 1–ε), а при $s^1 \neq s_0^1$ – такой же выборкой из распределения (P(1) = $\frac{|G|-1}{|G|}$, P(0) = $\frac{1}{|G|}$), статистическим критерием отбраковываем варианты состояний автомата A_1. Для состояний $s^1 \in {}^1S$ прошедших критерий, опробуем в исходном автомате A все состояния автомата A_2 с целью определения истинного начального состояния автомата A.

Перейдем к построению приближенных моделей конечного автомата на основе обобщения понятия неотличимости состояний по мере μ.

17.9. Гомоморфизмы автоматов по мере μ

Ранее нами в главе 17 «Определение начального состояния перестановочного автомата по входным и соответствующим выходным последовательностям с использованием меры неотличимости состояний μ» рассматривались автоматы A = (X, S, Y, h, f), A` = (X, S`, Y, h`, f`) и равномерное вероятностное распределение $P_X = (p(x) = \frac{1}{|X|}, x \in X)$ на X. Для инициальных автоматов A_s ,A'_s, $s \in S$, $s' \in S'$ (состояний s, s′ автоматов A, A′) была определена величина

$$\mu_N^{s,s'} = \mu_N(A_s, A_{s'}) = \frac{1}{N|X|^N} \sum_{\bar{x} \in X^N} \rho_N(A(s, \bar{x}), A'(s', \bar{x})),$$

Укажем обобщения введенных в пункте 2 понятий на случай автоматов с разными входными и выходными алфавитами.

Пусть

$$A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X}),$$
$$\overline{A} = (\overline{X}, \overline{S}, \overline{Y}, (\overline{h_{\bar{x}}})_{\bar{x} \in \overline{X}}, (\overline{f_{\bar{x}}})_{\bar{x} \in \overline{X}}) \quad -$$

конечные автоматы и ψ, χ – сюрьективные отображения $\psi : X \to X, \eta : Y \to \overline{Y}$.

Для $\Im = x_1, ..., x_N$ из X^N, $y = y_1, ..., y_N$ из Y^N положим

$$\psi\Im = \psi x_1, ..., \psi x_N \ , \eta\, y = \eta y_1, ..., \eta y_N \quad \text{и}$$

$$^{\psi,\eta}\mu_N^{s,\bar{s}} = {}^{\psi,\eta}\mu_N\left(A_s, \overline{A_{\bar{s}}}\right) = 1/N \sum_{\Im \in X^N} P(\Im)\rho\left(\eta A(s, \Im), \overline{A}\left(\bar{s}, \psi\Im\right)\right),$$

где $\rho\left(\eta A(s, \Im), \overline{A}\left(\bar{s}, \psi\Im\right)\right)$ – расстояние Хэмминга между словами $\eta A(s, \Im)$, $\overline{A}\left(\bar{s}, \psi\Im\right)$, а $(P(\Im), \Im \in X^N)$ – вероятностное распределение на X^N, индуцированное заданным равномерным вероятностным распределением на X.

Как и ранее (см. также [15]) нас интересует поведение величины $^{\psi,\eta}\mu_N^{s,\bar{s}}$ при $N \to \infty$. Для указанных автоматов и отображений рассмотрим вспомогательные автоматы

$$\eta A = (X, S, Y, (h_x)_{x \in X}, (\eta f_x)_{x \in X}),$$
$$\overline{A}\psi^{-1} = (X, \overline{S}, \overline{Y}, (\overline{h}_x)_{x \in X}, (\overline{f}_x)_{x \in X}),$$

где ηf_x, $x \in X$ – суперпозиция отображений, а для $\bar{x} \in \overline{X}$

$$\overline{h}_x = \overline{h_{\bar{x}}}, \ \overline{f}_x = \overline{f_{\bar{x}}}$$

для всех таких $x \in X$, для которых $\psi(x) = \bar{x}$.

Тогда в введенных обозначениях получаем

$$ {}^{\psi,\eta}\mu_N^{s,\bar{s}} = \mu_N\left((\eta A)_s, \left(\bar{A}\psi^{-1}\right)_{\bar{s}}\right), $$

где (ηA_s), $\left(\bar{A}\psi^{-1}\right)_{\bar{s}}$ – инициальные автоматы автоматов ηA, $\bar{A}\psi^{-1}$. Из результатов пункта 17.2 (см. также п. 17.3) имеем

$$ \lim_{N\to\infty} {}^{\psi,\eta}\mu_N^{s,\bar{s}} = \mu\left((\eta A)_s, \left(\bar{A}\psi^{-1}\right)_{\bar{s}}\right). $$

Таким образом, во-первых, появляется возможность естественных обобщений введенных ранее понятий, во-вторых – возможность сведения описания свойств таких обобщенных понятий к рассмотренному ранее случаю сравнения автоматов с общими входным и выходным алфавитами.

Пусть

$$ \mathrm{A} = (\mathrm{X},\mathrm{S},\mathrm{Y},(\mathrm{h}_x)_{x\in X},(\mathrm{f}_x)_{x\in X}), $$
$$ \bar{\mathrm{A}} = (\bar{\mathrm{X}},\bar{\mathrm{S}},\bar{\mathrm{Y}},(\bar{h}_{\bar{x}})_{\bar{x}\in\bar{X}},(\bar{f}_{\bar{x}})_{\bar{x}\in\bar{X}}) \quad - $$

произвольные конечные автоматы.

Определение 4. Для автоматов A и $\bar{A}$ тройку сюрьективных отображений:

$$ (\psi,\varphi,\eta) \quad \psi : X \to \bar{X},\ \varphi : S \to \bar{S},\ \eta : Y \to \bar{Y} $$

назовем гомоморфизмом по мере ${}^{\psi,\eta}\mu$ автомата A на $\bar{A}$, или кратко ${}^{\psi,\eta}\mu$-гомоморфизмом A на $\bar{A}$, если двойка отображений (ψ,φ) осуществляет гомоморфизм автомата без выходов $\mathrm{A}_\mathrm{M} = (\mathrm{X},\mathrm{S},(\mathrm{h}_x)_{x\in X})$ на автомат без выходов $\bar{\mathrm{A}}_M = (\bar{\mathrm{X}},\bar{\mathrm{S}},(\bar{h}_{\bar{x}})_{\bar{x}\in\bar{X}})$ и для любого $s \in \mathrm{S}$

$$ {}^{\psi,\eta}\mu^{s,\varphi s} = 0. $$

Для автоматов A, $\bar{A}$ и ${}^{\psi,\eta}\mu$-гомоморфизма Г = (ψ,φ,η) A на $\bar{A}$ рассмотрим вспомогательный автомат

$$ A/(\psi,\varphi,\eta) = \left(\left\{\psi^{-1}(\bar{x})\right\}_{\bar{x}\in\bar{X}}, \left\{\varphi^{-1}(\bar{s})\right\}_{\bar{s}\in\bar{S}}, Y, \left({}^{\Gamma}h_{\psi^{-1}(\bar{x})}\right)_{\psi^{-1}(\bar{x})\in\left\{\psi^{-1}(\bar{x})\right\}_{\bar{x}\in\bar{X}}}, \left({}^{\Gamma}f_{\psi^{-1}(\bar{x})}\right)_{\psi^{-1}(\bar{x})\in\left\{\psi^{-1}(\bar{x})\right\}_{\bar{x}\in\bar{X}}}\right). $$

Здесь ассоциированный с ним автомат без выходов $\left(A/(\psi,\varphi,\eta)\right)_M$ есть фактор-автомат автомата A_M по конгруэнции, порожденной гомоморфизмом (ψ,φ) A_M на $\bar{\mathrm{A}}_M$, а функции выходов $\left({}^{\Gamma}h_{\psi^{-1}(\bar{x})}\right)_{\psi^{-1}(\bar{x})\in\left\{\psi^{-1}(\bar{x})\right\}_{\bar{x}\in\bar{X}}}$, определены так:

$$ {}^{\Gamma}h_{\psi^{-1}(\bar{x})}\varphi^{-1}(s) = \bar{h}_{\bar{x}}\bar{s}. $$

Очевидно следующее утверждение.

Утверждение 2. Тройка отображений:

$\left(\psi_{из}, \varphi_{из}, E_{\overline{Y}}\right)$,

$\psi_{из} : \psi^{-1}\left(\overline{x}\right)$ а $\overline{x}$, $\varphi_{из} : \varphi^{-1}\left(\overline{s}\right)$ а $\overline{s}$, $E_{\overline{Y}} : \overline{y}$ а $\overline{y}$, $\overline{X} \in \overline{X}, \overline{s} \in \overline{S}$, $\overline{y} \in \overline{Y}$

осуществляет изоморфизм автомата $\left(A/(\psi, \varphi, \eta)\right)$ на $\overline{A}$, а тройка отображений:

$\left(\hat{\psi}, \hat{\varphi}, \eta\right)$, $\hat{\psi} : x$ а $\psi^{-1}(\psi x)$, $\hat{\varphi} : s$ а $\varphi^{-1}(\varphi s)$ осуществляет ${}^{\hat{\psi},\eta}\mu$-гомоморфизм А на $A/(\psi, \varphi, \eta)$.

Теорема 2. Пусть $(\psi_1, \varphi_1, \eta_1)$ ${}^{\psi_1,\eta_1}\mu$-гомоморфизм автомата $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$ на автомат $\overline{A} = (\overline{X}, \overline{S}, \overline{Y}, (\overline{h}_{\overline{x}})_{\overline{x} \in \overline{X}}, (\overline{f}_{\overline{x}})_{\overline{x} \in \overline{X}})$, а $(\psi_2, \varphi_2, \eta_2)$ ${}^{\psi_2,\eta_2}\mu$-гомоморфизм $\overline{A}$ на $\overline{\overline{A}} = (\overline{\overline{X}}, \overline{\overline{S}}, \overline{\overline{Y}}, (\overline{\overline{h}}_{\overline{\overline{x}}})_{\overline{\overline{x}} \in \overline{\overline{X}}}, (\overline{\overline{f}}_{\overline{\overline{x}}})_{\overline{\overline{x}} \in \overline{\overline{X}}})$. Тогда суперпозиция отображений

$$(\psi_2\psi_1, \varphi_2\varphi_1, \eta_2\eta_1) = (\mathring{\psi}, \mathring{\varphi}, \mathring{\eta})$$

является ${}^{\mathring{\psi},\mathring{\eta}}\mu$-гомоморфизмом А на $\overline{\overline{A}}$.

Доказательство. Очевидно, что двойка отображений $(\psi_2\psi_1, \varphi_2\varphi_1)$ является гомоморфизмом A_M на $\overline{\overline{A}}_M$. Для доказательства теоремы остается доказать, что при любом $s \in S$

$${}^{\mathring{\psi},\mathring{\eta}}\mu_{s,\mathring{\varphi}s} = \mu(\mathring{\eta}A_s, \overline{A}\mathring{\varphi}^{-1}_{\mathring{\varphi}s}) = 0.$$

В введенных ранее обозначениях из условий теоремы получаем

$$\mu((\eta_1 A)_s, (\overline{A}\psi_1^{-1})_{\varphi_1 s}) = 0, \ s \in S.$$

Очевидно, что

$$\mu((\eta_1 A)_s, (\overline{A}\psi^{-1})_{\varphi_1 s}) \geq \mu((\eta_2\eta_1 A)_s, (\eta_2 \overline{A}\psi^{-1})_{\varphi_1 s})$$

при любом отображении η_2 $\overline{Y}$ в $\overline{\overline{Y}}$. Следовательно,

$$\mu((\eta_2\eta_1 A)_s, (\eta_2 \overline{A}\psi^{-1})_{\varphi_1 s}) = 0.$$

Обозначим через $\vartheta = (p(\overline{x}), \ \overline{x} \in \overline{X})$ вероятностное распределение на $\overline{X}$.

$$p(\overline{x}) = \frac{|\psi^{-1}(\overline{x})|}{|X|}, \ \overline{x} \in \overline{X}.$$

Очевидно, $p(\overline{x}) \neq 0$ для каждого $\overline{x} \in \overline{X}$. Из условий теоремы следует

$$\mu((\eta_2 \overline{A})_{\varphi_1 s}, (\overline{A}\varphi_2^{-1})_{\varphi_2\varphi_1 s}) = 0, \ s \in S.$$

Теперь можно получить

$${}^{\vartheta}\mu((\eta_2 \overline{A})_{\varphi_1 s}, (\overline{\overline{A}}\psi_2^{-1})_{\varphi_2\varphi_1 s}) = 0, \ s \in S.$$

Здесь верхний индекс ϑ показывает, что в формуле для $\mu((\eta_2 \overline{A})_{\varphi_1 s}, (\overline{\overline{A}}\psi_2^{-1})_{\varphi_2\varphi_1 s})$ *необходимо использовать распределение на* X^N, *индуцированное вероятностным распределением* $\vartheta = (p(\overline{x}),\ \overline{x} \in \overline{X})$ *на* $\overline{X}$.

Несложно доказывается, что последнее равенство равносильно равенству

$$\mu((\eta_2 \overline{A}\psi_1^{-1})_{\varphi_1 s}, (\overline{\overline{A}}\psi_2^{-1} \cdot \psi_1^{-1})_{\varphi_2\varphi_1 s}) = 0,\ \ s \in S.$$

Заметим, что инициальные автоматы

$$(\eta_2 \cdot \eta_1 A)_s,\ \ (\eta_2 \overline{A}\psi_1^{-1})_{\varphi_1 s},\ (\overline{\overline{A}}\psi_2^{-1} \cdot \psi_1^{-1})_{\varphi_2\varphi_1 s},\ \ s \in S$$

имеют входной алфавит X и выходной алфавит $\overline{\overline{Y}}$, причем первый автомат μ-неотличим от второго, а второй от третьего. По свойству треугольника меры μ (см. [15]) заключаем

$$\mu((\eta_2\eta_1 A)_s, (\overline{\overline{A}}\psi_2^{-1}\psi_1^{-1})_{\varphi_2\varphi_1 s}) = 0$$

то есть

$$\mu((\eta A)_s, (\overline{\overline{A}}\psi^{-1})_{\varphi s}) = 0.$$

Теорема доказана.

Таким образом, указаны приближенные модели конечных автоматов – образов при ${}^{\psi,\eta}\mu$-гомоморфизмах. Вопросы использования ${}^{\psi,\eta}\mu$-гомоморфизмов в решении задач определения входного слова автомата А либо его начального состояния по входной и выходной последовательностям остается открытым.

Глава 18. СИСТЕМНЫЕ МНОЖЕСТВА СО СВОЙСТВОМ ПОДСТАНОВКИ

Глава[1] включает системные множества со свойством подстановки, описывает неточности, обнаруженные в работе, а также алгоритм поиска всех системных множеств со свойством подстановки работы и новый алгоритм поиска всех системных множеств со свойством подстановки. Производится поиск систем слабой импримитивности группы подстановок.

---

[1] Данная глава написана автором на основе результатов, полученных А. В. Быковым в курсовой работе.

В этой главе представлен алгоритм поиска всех системных множеств, обладающих свойством подстановки (см. [40]). Подобные объекты играют важную роль при декомпозиции конечных автоматов. Этот алгоритм может использоваться при поиске всех систем слабой импримитивности, что важно при построении наилучших (наихудших) моделей автоматов, описанных в главе 11 [15; 40].

18.1. Основные определения и обозначения работы[1]

Пусть $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ – конечный автомат, $|S| = n$.

Определение 1. Системным множеством π на множестве S называется совокупность $B_1, \ldots, B_к$ – подмножеств из S таких, что $\cup^k_{i=1} \cdot B_i = S$ и ($B_i \not\subset B_j$ и $B_i \neq B_j$ при $i \neq j$). Множества $B_1, \ldots, B_к$ будем называть *блоками системного множества* π.

Отметим, что блоки могут иметь непустое пересечение.

Определение 2. Системное множество π обладает свойством подстановки (обозначим это событие через $S(\pi)$ тогда и только тогда, когда для любого блока B_j из π и для любого $x\in X$ найдется j, при котором $h_x(B_i) \subseteq B_j$.

Определение 3. Для двух системных множеств π_1 и π_2, определенных на множестве S, вводится бинарное отношение $\leq$: $\pi_1 \leq \pi_2$ тогда и только тогда, когда каждый блок из π_1 содержится в некотором блоке из π_2.

Определение 4. Произведением двух системных множеств π_1 и π_2, определенных на множестве S, называется такое системное множество (обозначается $\pi_1\cdot\pi_2$), что:

а) $\pi_1\cdot\pi_2 \leq \pi_1$; б) $\pi_1\cdot\pi_2 \leq \pi_2$;

б) если для любого другого системного множества π: $\pi \leq \pi_1$ и $\pi \leq \pi_2$, то $\pi \leq \pi_1\cdot\pi_2$.

Определение 5. Суммой двух системных множеств π_1 и π_2, определенных на множестве S, называется такое системное множество (обозначается $\pi_1+\pi_2$), что

а) $\pi_1 \leq \pi_1+\pi_2$; б) $\pi_2 \leq \pi_1+\pi_2$;

б) если для любого другого системного множества π: $\pi_1 \leq \pi$ и $\pi_2 \leq \pi$, то $\pi_1+\pi_2 \leq \pi$.

---

[1] Источник: [40].

Определение 6. Пара системных множеств π_1 и π_2, определенных на множестве S, называется упорядоченной парой (этот факт обозначается (π_1, π_2)) тогда и только тогда, когда для любой частичной функции переходов h_x автомата A для блока B_i из π_1 существует блок B_j из π_2 такой, что $h_x(B_i) \subseteq B_j$.

Определение 7. Для системного множества π определено системное множество $m(\pi)$ такое, что $(\pi, m(\pi))$ – упорядоченная пара и если (π, w) – другая упорядоченная пара, то $m(\pi) \leq w$.

Определение 8. Для системного множества π определено системное множество $M(\pi)$ такое, что $(M(\pi), \pi)$ – упорядоченная пара и если (w, π) – другая упорядоченная пара, то $w \leq M(\pi)$.

Лемма 1. Для любого системного множества π, определенного на множестве S, системные множества $m(\pi)$ и $M(\pi)$ – единственны [56].

Определение 9. Упорядоченная пара (π, w) системных множеств π и w, определенных на множестве S, называется Mm-парой тогда и только тогда, когда $\pi = M(w)$ и $w = m(\pi)$.

Обозначим через $\pi_{i,\ j}$ такое системное множество, которое содержит только один блок, состоящий только из элементов q_i, $q_j \in S$, а остальные блоки состоят из одного элемента каждый.

18.2. Системные множества со свойством подстановки

Необходимость поиска подобных объектов подтверждает следующая теорема.

Теорема. 1. Существует нетривиальная параллельная декомпозиция автомата A тогда и только тогда, если существуют два нетривиальных системных множества π_1 и π_2, определенные на S, такие, что $\pi_1 \cdot \pi_2 = 0$ и $S(\pi_1)$, $S(\pi_2)$, то есть π_1 и π_2 обладают свойством подстановки. 2. Существует нетривиальная последовательная декомпозиция автомата A тогда и только тогда, когда существует нетривиальное системное множество π такое, что $S(\pi)$, то есть π обладает свойством подстановки [40].

Отметим, что параллельная декомпозиция зависит непосредственно от вида системных множеств π_1 и π_2 или π.

В работе [40] предлагается использовать системные множества со свойством подстановки при кодировании состояний конечного автомата.

18.3. Неточности, обнаруженные в работе[1]

В работе ([40]) для конечного автомата A предлагаются два подхода к поиску системных множеств со свойством подстановки. Один из подходов основан на построении всех Mm-пар (приводится алгоритм построения Mm-пар), второй подход не использует построение Mm-пар.

Ниже будет показана некорректность работы обоих алгоритмов. Будет показано, что в обоих случаях строятся, во-первых, не все системные множества со свойством подстановки, во-вторых, часть строящихся системных множеств не обладает свойством подстановки.

Определение 10. Для каждого системного множества π определяется системное множество $C(\pi)$ так, что элементы $q_1, \ldots, q_k$ из множества S находятся в одном блоке в $C(\pi)$ тогда и только тогда, когда каждая из C_k^2 пар этих элементов находится в одном и том же блоке в π [40].

Утверждение 1. В рамках определения 10 для любого системного множества π может существовать более одного системного множества $C(\pi)$.

Доказательство. Приведем следующий пример: пусть π = (12, 13, 23, 24, 34). Докажем, что системные множества π_1 = (123, 24, 34) и π_2 = (123, 234) удовлетворяет определению $C(\pi)$.

1. Проверим, удовлетворяет ли π_1 определению $C(\pi)$.

Необходимость. Элементы $q_1q_2q_3$ = 123 находятся в одном блоке в π_1, следовательно, каждая из C_3^2 пар этих элементов должна находиться в одном блоке в π. Это действительно так.

Достаточность. Каждая из C_3^2 пар элементов $q_1q_2q_3$ = 123 находится в одном блоке в π, следовательно элементы $q_1q_2q_3$ должны находиться в одном блоке в $C(\pi)$. Эти элементы находятся в одном блоке в π_1.

2. Аналогичные рассуждения можно провести и для элементов q_2q_4 = 24 и q_3q_4 = 34. Учитывая, что π_1 – системное множество, делаем вывод, $C(\pi) = \pi_1$.

Проверка того, что π_2 удовлетворяет определению $C(\pi)$, осуществляется полностью аналогично пункту 1.

---

[1] Неточности обнаружены в работе [40].

Нетрудно видеть, что и само системное множество π удовлетворяет определению $C(\pi)$. Утверждение 1 говорит о неоднозначности определения системного множества $C(\pi)$. Такая неоднозначность делает неверными некоторые утверждения работы [56], часть из которых используется для поиска системных множеств со свойством подстановки в [56]. Далее приводятся эти утверждения и доказательства их некорректности.

Определение 11. По аналогии с $C(\pi)$ в [56] определяется $C^{-1}(\pi)$-системное множество, блоки которого содержат не более двух элементов. Элементы q_1 и q_2 находятся в одном блоке в $C^{-1}(\pi)$ тогда и только тогда, когда они находятся в одном блоке в π [40].

Лемма 2. Для двух системных множеств π_1 и π_2, определенных на множестве состояний S автомата A, упорядоченная пара (π_1, π_2) является Mm-парой тогда и только тогда, когда упорядоченные пары $(C(\pi_1), C(\pi_2))$ и $(C^{-1}(\pi_1), C^{-1}(\pi_2))$ являются Mm-парами [40].

Утверждение 2. $(C(\pi_1), C(\pi_2))$ не всегда является упорядоченной парой (лемма 2 не корректна).

Доказательство. Для обоснования утверждения достаточно привести противоречащий пример. Пусть X = (0, 1), S = (1, 2, 3, 4, 5) и автомат A задан табл. 2.

Таблица 2

S\X	0	1
1	1	4
2	5	5
3	2	1
4	5	3
5	1	3

Пусть π = (145, 23, 13), тогда $m(\pi)$ = (15, 34, 25, 12, 14), $M(m(\pi))$ = (145, 23, 13) – это Mm-пара. Это доказано в [21]. Пара $C(m(\pi))$ = (125, 14, 34), $C(M(m(\pi)))$ = (145, 23, 13) должна быть Mm-парой согласно лемме 2. Но это не так. По лемме 1 для любого системного множества π существуют единственные $M(\pi)$ и $m(\pi)$. Следовательно, получили противоречие с этим фактом. Значит, лемма 2 не верна, то есть $(C(w), C(\pi))$ – не обязана быть Mm-парой при условии, что (w, π).

Отметим, что в работе [40] лемма 2 используется при обосновании корректности алгоритма поиска всех Mm-пар.

18.4. Алгоритм поиска всех системных множеств со свойством подстановки работы

Алгоритм (первый) поиска всех Mm-пар [40]. Шаги:

1. Для каждой пары отличных друг от друга элементов q_i и q_j из S найти $m(\pi_{i,j})$ и Mm-пару $(M(m(\pi_{i,j})), m(\pi_{i,j}))$.

2. Определить все возможные суммы системных множеств $m(\pi_{i,j})$, полученных на шаге 1. Для каждого полученного таким образом системного множества π_k определить $M(\pi_k)$ для получения Mm-пары $(M(\pi_k), \pi_k)$.

3. Для каждой Mm-пары (π_i, π_j), полученной на шаге 2, вычислить Mm-пару $(C(\pi_i), C(\pi_j))$.

Отметим, что в силу утверждения 2 пара $(C(\pi_i), C(\pi_j))$, строящаяся на шаге 3 алгоритма, не обязана быть Mm-парой, а это означает, что вышеизложенный алгоритм нельзя применять для построения всех Mm-пар и только их. Необходимость же поиска всех Mm-пар обуславливает следующая лемма.

Лемма 3. Пусть π – системное множество, определенное на множестве S; π обладает свойством подстановки тогда и только тогда, когда $M(\pi) \le \pi \le m(\pi)$ [40].

В связи с этой леммой в [40] утверждается, что все системные множества со свойством подстановки могут быть получены из Mm-пар. Однако представленный в [40] алгоритм поиска всех таких пар работает некорректно, следовательно, вопрос о поиске всех Mm-пар остается открытым.

В работе [40] предлагается также и другой способ нахождения всех системных множеств со свойством подстановки без построения всех Mm-пар.

Второй алгоритм – построение всех системных множеств со свойством подстановки [40].

1. Рассмотрим системное множество π_{ij} для каждой пары $(q_i, q_j) \in S$.

2. Вычисляем $\tau^1_{ij} = \pi_{ij} + m(\pi_{ij})$.

3. Вычисляем $\tau^k_{ij} = \tau^{k-1}_{ij} + m(\tau^{k-1}_{ij})$ при k = 1, 2, 3, … до тех пор, пока $\tau^k_{ij} = \tau^{k-1}_{ij} = \tau_{ij}$.

4. Образуем все возможные суммы системных множеств τ_{ij}, полученных на шаге 3.

5. Для каждого из системных множеств π, полученных на шаге 4, образуем $C(\pi)$. Таким образом строятся все системные множества со свойством подстановки.

Утверждение 3. Указанный алгоритм построения всех системных множеств со свойством подстановки некорректен. В результате работы данного алгоритма могут быть построены системные множества, не обладающие свойством подстановки.

Доказательство. Вновь рассмотрим автомат А, заданный табл. 2. Нетрудно видеть, что взяв системное множество π_{12} на шаге 1, мы на шаге 3 получим системное множество π = (12, 13, 14, 15, 25, 34, 35, 45), обладающее свойством подстановки.

Рассмотрим системные множества w_1 = (125, 1345) и w_2 = (125, 134, 35, 45). Согласно определению $C(\pi)$, замечаем, что $w_1 = C(\pi)$ и $w_2 = C(\pi)$, но w_2 не обладает свойством подстановки ($h_1(125) = (345) \notin w_2$).

Таким образом, предложенные в [40] способы нахождения всех системных множеств со свойством подстановки некорректны, а следовательно, необходимо найти новый способ построения таких объектов. Ниже будет представлен алгоритм построения всех системных множеств со свойством подстановки, и только их.

18.5. Новый алгоритм поиска всех системных множеств со свойством подстановки

Ранее отмечалось, что для каждого системного множества π могут существовать несколько системных множеств $C(\pi)$.

В связи с этим дадим следующее определение.

Определение 12. Среди всех системных множеств $C(\pi)$ для заданного системного множества π выберем такое системное множество (обозначим его $C_m(\pi)$ и будем называть максимальным), что $C(\pi) \le C_m(\pi)$ для любого $C(\pi)$.

Утверждение 4. Системное множество $C_m(\pi)$ определено корректно, то есть существует единственное $C_m(\pi)$ для каждого системного множества π.

Замечание 1. Отметим, что если в алгоритмах и леммах работы [40], признанных некорректными, заменить $C(\pi)$ на $C_m(\pi)$, то они по прежнему останутся некорректными. Уточним это замечание.

Некорректность леммы 1 обосновывает очевидный аналог утверждения 2 (в нем в качестве $C(m(\pi))$ и $C(M(m(\pi)))$ надо выбрать $C_m(m(\pi))$ $C_m(M(m(\pi)))$), а следовательно, алгоритм поиска всех Mm-пар по-прежнему неверен.

Что касается поиска *всех* системных множеств со свойством подстановки, то при таком переопределении на шаге 5 алгоритма из [40] будут построены не все системные множества со свойством подстановки. Это нетрудно видеть, рассмотрев автомат A, заданный табл. 2. Легко показать, что в этом случае никогда не будет построено следующее системное множество со свойством подстановки $\pi = (125, 345, 13, 14)$.

Новый основной алгоритм поиска всех системных множеств со свойством подстановки будет состоять из трех этапов (A, B, C). Этап A представляет собой второй алгоритм из [40], кроме шага 5. На этом этапе строятся все системные множества со свойством подстановки, блоки которых содержат не более двух элементов.

Новый основной алгоритм.

Этап A.

1. Рассмотрим системное множество $\pi_{i,\,j}$ для каждой пары элементов q_i, q_j из S.

2. Вычисляем $w_{i,\,j}^{1} = \pi_{i,\,j} + m(\pi_{i,\,j})$.

3. Вычисляем $w_{i,\,j}^{k} = w_{i,\,j}^{k-1} + m(w_{i,\,j}^{k-1})$ при $k = 2, 3, \ldots$ до тех пор, пока $w_{i,\,j}^{k} = w_{i,\,j}^{k-1} = w_{i,\,j}$.

4. Образуем все возможные суммы системных множеств $w_{i,\,j}$, полученных на шаге 3.

Далее находим $C_m(\pi)$ для каждого π, образованного на шаге 3 и на шаге 4.

Приведем один из возможных алгоритмов построения $C_m(\pi)$. Обозначим ab – блок, состоящий из элементов $(a, b) \in S$, и только из них.

Алгоритм построения $C_m(\pi)$.

1. Строим множество T_0, состоящее из всех блоков из множества π, содержащих не менее двух элементов.

2. Вычеркиваем из T_0 любой блок ab и выписываем для него два множества T_0^1 и T_0^2, в T_0^1 переписываем блоки из T_0 вида ac, в T_0^2 – вида bd.

3. Сравниваем T_0^1 и T_0^2, если существует c = d, то выписываем блоки вида abc в T_1, для всех c = d, если таких c и d и не существует, то ab помещаем в R. Очищаем T_0^1, T_0^2 и переходим к следующему блоку из T_0.

4. Продолжаем шаги 2 и 3 до тех пор, пока T_0 не станет пустым. Далее работаем с T_1. Как и с T_0, строим T_2. В итоге на некотором шаге построим пустое множество T_j. Тогда переходим к шагу 5.

5. Рассмотрим множество R. Если в нем есть блоки, которые являются подблоками в других блоках, то удаляем их до тех пор, пока таких подблоков не останется.

6. Если существуют элементы в S, которые не участвуют ни в одном блоке из R, то допишем их в R в виде блоков, состоящих из одного элемента. Если в π были блоки, состоящие из одного элемента, то допишем их в R.

В результате в R будет содержаться системное множество $C_m(\pi)$.

Для дальнейших целей представим $C_m(\pi)$ в виде графа, где вершинам соответствуют блоки, а ребро заходит из одной вершины в другую тогда и только тогда, когда существует частичная функция переходов, отображающая один блок на другой. Тогда этот граф будет иметь вид циклов с подходами. Построим множество $P(\pi)$, состоящее из всех блоков, которым соответствуют вершины на подходах.

Утверждение 5. Если системное множество π обладает свойством подстановки, то системное множество $C_m(\pi)$ также обладает свойством подстановки.

Доказательство. Доказательство осуществим от противного. Пусть $C_m(\pi)$ не обладает свойством подстановки. Это означает, что в $C_m(\pi)$ существует блок $B = (b_1, \ldots, b_t)$ и частичная функция переходов h_x, что для любого блока B_1 из $C_m(\pi)$: $h_x(B) \not\subset B_1$. Очевидно, что должно быть $|B| > 2$. Выпишем из B все подмножества состоящие из двух элементов и для каждого подмножества выпишем его образ под действием частичной функции переходов h_x: $h_x(ab) = cd$ и т. д.

Легко видеть, что используя алгоритм построения $C_m(\pi)$ применительно к множеству всех выписанных образов получим в R блок, такой, что любой из h_x-образов является в нем подблоком, а значит этот блок является h_x-образом блока B и он обязан лежать в C_m (π), так как все эти двухэлементные образы лежат в множестве π (поскольку оно обладает свойством подстановки). Таким образом, получили противоречие с максимальностью $C_m(\pi)$. А это означает, что наше предположение не верно, следовательно, C_m (π) обладает свойством подстановки.

Дальнейшая часть доказательства будет проведена в предположении, что граф системного множества $C_m(\pi)$ состоит из не более чем одного цикла с не более чем одним подходом. Позже мы откажемся от этого ограничения.

Теперь зная $C_m(\pi)$) построим все остальные множества со свойством подстановки, порожденные множеством π. Для этого обратимся к $P(\pi)$. В нем содержатся блоки из π, в которые не переходят другие блоки из π. Если $P(\pi) \neq \varnothing$, то будут работать блоки Б и С алгоритма, если $P(\pi) = \varnothing$, то будет работать только блок С алгоритма. Независимо от $P(\pi)$ необходимо выполнить следующие действия:

1. Определить максимальный размер блока в C_m (π): n, к: = n .
2. Выписать все блоки и подблоки из C_m (π) размера к в множество О.
3. Переместить любой элемент из множества О в множество T_0. Если $P(\pi) = \varnothing$, то далее выполнять только блок С. В противном случае необходимо проверять, содержится ли какой-либо элемент из $P(\pi)$ в элементе из T_0. Если да, то выполнять блок Б, в противном случае выполняем С.

Вернемся к *основному алгоритму*:

Этап Б.

1. Строим множество T_1. В него помещаем все h_x-образы элемента из T_0, для всех x. Если некоторый элемент из T_1 включается как подмножество в элемент из T_0, то его удаляем из T_1.
2. (Для i-го шага.) Если $T_i \neq \varnothing$, то T_{i+1} строим следующим образом: в него помещаем все h_x-образы элементов из T_i; если какой-либо элемент из T_{i+1} является подмножеством некоторого элемента из T_{i+1} или из T_k, k ={0, …, i}, то его исключаем из T_{i+1}.
3. Шаг 2 повторяем до тех пор, пока не появится $T_j = \varnothing$. В таком случае в объединении T_k по к от 0 до j–1 содержится системное

множество со свойством подстановки. Назовем его системным множеством, порожденным соответствующим элементом из T_0. Обозначим его M_0.

4. Дальнейшая цель состоит в построении всех системных множеств, порожденных этим элементом. Очевидно, что $M_0 \leq F \leq C_m(\pi)$, где F – означает любое порожденное элементом из T_0 множество. Будем дополнять определенным образом каждый блок из M_0 до соответствующего блока из $C_m(\pi)$, получая новые системные множества со свойством подстановки.

5. Рассмотрим блоки, которые лежат в T_{j-1}. Если в T_{j-1} существует блок, при добавлении к которому элементов из соответствующего блока из C_m (π) этот блок не включает в себя ни один из блоков из T_k, $k = \{0, \ldots, j-2\}$, то строим M_1^{j-1}. Дополняя все блоки из T_{j-1} до соответствующих блоков в $C_m(\pi)$ всеми возможными способами, получим некоторые множества $\{M_i^{j-1}\}$. Если в соответствии с вышесказанным ни один блок в T_{j-1} невозможно дополнить, то переходим к T_{j-2} и так далее до T_1. Нельзя дополнять так, чтобы блок из T_0 содержался в дополняемом.

6. Для каждого M_i^{j-1} находим все h_x-образы дополненного блока. Если они содержатся в каких-либо блоках из некоторого T_k, то построение данного M_i завершено. В противном случае существует хотя бы одно T_k, содержащее блок, являющийся подмножеством некоторого h_x-образа. Заменим в каждом T_k такие блоки на соответствующие образы, повторы в T_k – уберем. Затем в T_{k+1} поместим образы блоков из T_k, удаляя повторы и подблоки, и так далее до тех пор пока нечего будет больше менять. Таким образом, завершаем построение M_i^{j-1} .

7. При помощи шага 5 завершаем построение всех $M^{j-1}{}_i$.

8. Перейдем к T_{j-2} и построим все M_i^{j-2} и так далее до T_1.

9. Рассмотрим все M_i^k и уберем повторы, если они есть. Все оставшиеся в итоге множества – системные множества, обладающие свойством подстановки, порожденные одним множеством из T_0.

10. Переместим из O следующее множество в T_0, предварительно обнулив все T_k и применим к нему соответствующий блок алгоритма.

11. Повторим все вышеописанные действия, до тех пор пока O не станет пустым. Как только это случится, положим к: = к – 1.

12. Повторим вышеописанные действия до тех пор, пока к не станет равным 1.

В итоге выписываются все системные множества, обладающие свойством подстановки.

Этап С.

Все шаги, кроме шага 5, повторяют этап Б.

5. Дополнительно к шагу 5 из этапа Б потребуем проверку следующего условия: если элемент из T_0 окажется подмножеством какого-либо образа дополняемого множества, то такое дополнение считаем недействительным и вычеркиваем.

Замечание 2. Если у некоторого цикла более одного подхода, то выделим цикл вместе с каждым из подходов в отдельное $C_m^1(\pi)$ и применим к нему алгоритм. В случае нескольких циклов поступим аналогично. Получив все множество $\{C_m^i(\pi)\}$, построим при помощи алгоритма все системные множества со свойством подстановки для каждого $C_m^i(\pi)$.

Для того чтобы для данного $C_m(\pi)$ построить все такие объекты, рассматриваются все возможные комбинации из полученных системных множеств для каждого $C_m^i(\pi)$. Если в какой-либо комбинации есть повторяющиеся блоки или блоки, являющиеся подблоками в других блоках, то их исключим.

Утверждение 6. Новый алгоритм строит все системные множества со свойством подстановки.

Доказательство. Пусть есть $C_m(\pi)$ и системное множество M со свойством подстановки, для которого выполнено условие $M \leq C_m(\pi)$. Необходимо показать, что M всегда может быть построено при помощи вышеуказанного алгоритма. Если в M есть блок, не являющийся h_x-образом любого другого блока, то надо показать (1), что M может быть построено на этапе Б алгоритма, в противном случае – на этапе С.

1. Выпишем M в виде объединения T_j^1. Выберем максимальное j, при котором $T_j^1 \neq T_j$, и дополним блок из T_j до соответствующего блока из T_j^1 в соответствии с алгоритмом. Если полученное множество совпало с M, то (1) доказано, в противном случае опять найдем максимальное j, что $T_j^1 \neq T_j$ и повторим все вышеуказанные действия до тех пор, пока наше множество не совпадет с M.

2. Доказывается аналогично пункту 1. В качестве T_0 возьмем максимальный по включению блок из M.

18.6. Поиск систем слабой импримитивности для заданного автомата

Пусть (G, S) – транзитивная группа подстановок множества S и B_1, …, B_L – покрытие множества S. Напомним некоторые необходимые нам понятия [15].

H_{Bj} – группа подстановок множества B_j, являющаяся ограничением стабилизатора G_{Bj} на B_j.

Определение 13. Система множеств B_1, …, B_L называется системой слабой импримитивности группы (G, S), если выполнены следующие условия:

1) $1<L<S$;
2) $B_i \neq B_j$ при $i \neq j$;
3) для любого $g \in G$, для любого $j \in \{1, \ldots, L\}$ существует j_1: $g(B_j) = B_{j1}$;
4) для любых $(j, j') \in \{1, \ldots, L\}$ существует $g \in G$: $g(B_j) = B_{j1}$;
5) найдется $j \in \{1, \ldots, L\}$, при котором группа H_{Bj} является транзитивной.

Напомним, что с помощью систем слабой импримитивности ранее нами строились наилучшие и наихудшие приближенные модели заданного перестановочного автомата [15].

Замечание 3. Отметим, что из пункта 4 вытекает равномощность множеств B_1, …, B_L. Поэтому очевидно, что любая система слабой импримитивности является системным множеством со свойством подстановки. Обратное, вообще говоря, не верно.

Вывод. Для поиска систем слабой импримитивности надо отбирать системные множества со свойством подстановки, удовлетворяющие пунктам 1), 4), 5) определения системы слабой импримитивности.

Применительно к новому алгоритму, изложенному в предыдущей части работы, это означает, что достаточно оставить этапы A) и C) и для построенных в результате системных множеств проверить пункты 1) и 5) определения системы слабой импримитивности.

Для ускорения поиска вначале следует проверять пункт 1) определения 13.

Часть 5. ПОМЕХОУСТОЙЧИВЫЕ АВТОМАТЫ

Начало исследований отображений множеств слов заданного алфавита начато А. А. Марковым. В 1956 г. А. А. Марков получил результат о биективных преобразованиях ϕ множества слов Ω^* в конечном алфавите Ω, сохраняющих длины слов и не увеличивающих расстояния Хемминга между словами одной длины, то есть не размножающих искажений типа замены букв в словах.

Рассмотренная А. А. Марковым задача имеет много различных вариаций. В частности, представляют интерес не только биективные, но и инъективные отображения. Кроме того, наряду с искажениями (например, замены букв) могут происходить искажения других типов, например пропуски букв, по-разному может определяться понятие близости слов и т. д. Некоторые из таких вариаций и рассматривались в работах [3; 5; 6; 19].

Глава 19. АВТОМАТНЫЕ ОТОБРАЖЕНИЯ ПЕРИОДИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, НЕ РАЗМНОЖАЮЩИЕ ИСКАЖЕНИЙ

Описываются приведенные перестановочные автоматы, реализующие отображения множества периодических входных последовательностей в множество периодических выходных последовательностей, не увеличивающие или сохраняющие введенное в параграфе расстояние между периодическими последовательностями.

В данной главе продолжаются исследования[1], где приведено описание преобразований множества X* всех слов конечной длины в алфавите X, не размножающих искажений типа замены букв и пропуска букв в словах. Представляет интерес описание отображений множества $X_П$ всех бесконечных периодических последовательностей в алфавите X в множество $Y_П$ всех бесконечных периодических последовательностей алфавита Y, не размножающих искажений типа замены букв в последовательностях. Описанные в данной работе преобразования, не размножающие искажений типа замены букв в словах, можно рассматривать как отображения, не

[1] См. : Глухов М. М. Инъективные отображения слов, не размножающие искажений // Труды по дискретной математике. – 2001. – Т. 4 – С. 17–32.

увеличивающие значения расстояния Хемминга между словами. Отображение, не размножающее искажения типа замены букв в последовательностях, трактуется как отображение, не увеличивающее значение вводимой ниже метрики на множестве бесконечных последовательностей элементов конечного алфавита. Метрика вводится с помощью расстояния Хемминга между словами конечной одинаковой длины, и в этом смысле ее можно понимать как расстояние Хемминга между бесконечными периодическими последовательностями элементов алфавита. Основной результат состоит в описании класса автоматных отображений $X_П$ в $Y_П$ не увеличивающих или не изменяющих указанного расстояния Хемминга между периодическими последовательностями. При этом под автоматным отображением понимается отображение, осуществляемое подходящим конечным автоматом при некотором фиксированном начальном состоянии. Приводимые результаты опубликованы в [2; 3].

19.1. Основные обозначения и понятия

Мы будем придерживаться следующих обозначений:

$[\omega, \omega']$ – наименьшее общее кратное чисел ω, ω';

$W|R$ – W делит R;

X, Y, S – конечные алфавиты;

X^* – множество всех слов конечной длины алфавита X без пустого слова;

PP' – произведение (конкатенация) слов P, P′;

$X_П$, $Y_П$ – множества всех периодических последовательностей (чисто периодических) элементов алфавитов X, Y соответственно;

$\rho(P, Q)$ – расстояние Хемминга между словами P, Q;

$\rho_k(P, P')$ – расстояние Хемминга между начальными словами длины k последовательностей P, P′;

$|P|$ – длина слова $P \in X^*$;

$|Z|$ – мощность множества Z;

$A(X, S, Y, h, f)$ или $A(X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ – конечный автомат с входным алфавитом X, $|X|\geq 2$, множеством состояний S, выходным алфавитом Y, $h: S\times X\to S$ – функция переходов автомата A;

$f: S\times X\to Y$ – функция выходов автомата A;

$h_x: S\to S$ –частичная функция переходов автомата A;

$f_x: S\to Y$ – частичная функция выходов автомата A;

Мы будем использовать и функции f_s: $X \to Y$, $f_s x = f_x s$, $x \in X$, $s \in S$;

$A(s, P)$ – выходное слово автомата A с начальным состоянием $s \in S$ при входном слове $P \in X^*$ или выходная последовательность при $P \in X_П$;

при $P = x(1)x(2) \ldots x(k)$

$$h_P = h_{x(k)}h_{x(k-1)} \ldots h_{x(1)}, \quad h_P s = h_{x(k)}h_{x(k-1)} \ldots h_{x(1)}s;$$

$A_M(s, P)$ – последовательность состояний автомата A, отвечающая входу P и начальному состоянию s;

$A(s) = (X, S(s), Y, (h_x)_{x \in X}, (f_x)_{x \in X})$ – подавтомат, порожденный состоянием $s \in S$ в автомате A, при этом $s \in S(s)$ и $s' \in S(s)$ при $s' \neq s$ тогда и только тогда, когда найдется $P \in X^*$ такое, что $\delta_P s = s`$; для простоты обозначений ограничения функций $(h_x)_{x \in X}$, $(f_x)_{xX}$ автомата A на S(s) обозначены теми же символами.

Из результатов работы [2; 15] следует, что для любых последовательностей P, P′ из $X_П$ периодов ω, ω′ соответственно существует предел

$$\lim_{k \longrightarrow \infty} \frac{\rho_k(P, P`)}{k},$$

равный величине

$$\mu(P,P') = \frac{1}{[\omega, \omega`]} \rho_{[\omega,\omega']}(P,P').$$

Заметим, что данный предел существует и для любых смешанно-периодических последовательностей элементов алфавита X и он равен величине μ(P, P′), где P, P′ – периодические части данных последовательностей [58].

С использованием метрических свойств расстояния Хемминга непосредственно проверяется, что μ является метрикой на $X_П$, но не является метрикой на множестве смешанно-периодических последовательностей.

Определение 1. Отображение φ: $X_П \to Y_П$ называется сохраняющим метрику μ, если

$$\mu(P, P') = \mu(\varphi P, \varphi P')$$

при любых P, P` из $X_П$. Отображение φ называется не увеличивающим значение метрики μ, если

$$\mu(P, P') \geq \mu(\varphi P, \varphi P')$$

при любых P, P` из $X_П$.

Напомним, что автомат $A = (X, S, Y, (\delta_x)_{x\in X}, (\beta_x)_{x\in X})$ называется перестановочным, если $(\delta_x)_{x\in X}$ − биекции S в S, и внутренне автономным, если

$$\delta_x s = \delta_{x'} s$$

при любых $s\in S$ и x, x′ из X.

Легко проверяется, что любой перестановочный автомат A с любым начальным состоянием s перерабатывает периодические входные последовательности в периодические. В связи с этим определено отображение

$$\varphi_{A(s)}: X_\Pi \to Y_\Pi, \quad \varphi_{A(s)}(P) = A(s, P), \ P\in X_\Pi.$$

Множество всех перестановочных приведенных автоматов

$$A(s) = (X, S(s), Y, (\delta_x)_{x\in X}, (\beta_x)_{x\in X}),$$

для которых отображение $\varphi_{A(s)}$ X_Π в Y_Π не увеличивает значение метрики μ, обозначим через $GA(X_\Pi, Y_\Pi, \geq, \mu)$, а множество всех перестановочных приведенных автоматов A(s), для которых отображение $\varphi_{A(s)}$ сохраняет значение метрики μ, обозначим через $GA(X_\Pi, Y_\Pi, =, \mu)$. Отметим важное обстоятельство, состоящее в том, что отображения $\varphi_{A(s)}$, $s\in S$, возможно, и не инъективны.

19.2. Описание множества GA (X_Π, Y_Π, =, μ)

Нас интересуют автоматы A(s), реализующие при начальном состоянии s отображение X_Π в Y_Π. Ранее отмечалось, что перестановочные автоматы обладают этим свойством. Ниже будет дано описание перестановочных автоматов A(s), для которых отображение $\varphi_{A(s)}$ X_Π в Y_Π, реализуемое автоматом A при начальном состоянии s, сохраняет метрику μ.

Определение 2. Автомат $A = (X, S, Y, (\delta_x)_{x\in X}, (\beta_x)_{x\in X})$ называется автоматом с потерей информации о метрике ρ, если найдутся входные слова P, P` из X* и состояния s, s′ из S, при которых

$$\delta_P s = s', \ \delta_{P`} s = s', \ |P| = |P'|; \qquad (26)$$

$$\rho(P, P') \neq \rho(A(s, P), A(s, P')), \qquad (27)$$

в противном случае автомат A называется автоматом без потери информации о метрике ρ. Состояние s, для которого выполнены условия (26), (27), называется состоянием с потерей информации о метрике ρ.

Отметим, что автомат A без потери информации о метрике ρ является и автоматом без потери информации [24].

Теорема 1. Отображение $\phi_{A(s_0)}$ множества ХП в УП, реализуемое перестановочным автоматом A(s0) при начальном состоянии s0, сохраняет метрику μ, тогда и только тогда, когда A(s0) – автомат без потери информации о метрике ρ.

Доказательство. Пусть $A(s_0)$ – перестановочный автомат с потерей информации о метрике ρ. Тогда $A(s_0)$ – сильно связный автомат с потерей информации о метрике ρ. Следовательно, найдутся его входные слова $P = P_2$, $P' = P_3$ и состояния $s = s_1$, $s' = s_2$, при которых выполняются условия (26), (27), а также входные слова P_1, P_4, для которых справедливы равенства

$$\delta_{P_1} s_0 = s_1,\ \delta_{P_4} s_2 = s_0.$$

Рассмотрим периодические последовательности

$$P = P_1P_2P_4\ldots\ ,\ \overline{P} = P_1P_3P_4, \ldots$$

элементов алфавита X периодов ω, $\overline{\omega}$ соответственно таких, что $\omega \mid L$ и $\overline{\omega} \mid L$, где $L = |P_1P_2P_4| = |P_1P_3P_4|$, и выходные последовательности $A(s_0, P)$, $A(s_0, \overline{P})$ периодов W, $\overline{W}$ соответственно. Очевидно, что $W \mid L$, $\overline{W} \mid L$, в связи с чем непосредственно проверяется, что

$$\mu(P, \overline{P}) \neq \mu(A(s_0, P), A(s_0, \overline{P})).$$

Предположим теперь, что $A(s_0)$ – перестановочный автомат без потери информации о метрике ρ. Рассмотрим произвольные периодические последовательности P, $\overline{\omega}$ периодов ω, $\overline{\omega}$ соответственно. Очевидно, найдутся m_1, m_2, при которых периоды последовательностей состояний $A_M(s_0, P)$, $A_M(s_0, \overline{P})$ делят соответственно величины $m_1\omega$, $m_2\overline{\omega}$. Положим

$$N = [m_1\omega, m_2\overline{\omega}].$$

Легко видеть, что периоды последовательностей $A(s_0, P)$, $A(s_0,)$ делят N, поэтому

$$\mu(A(s_0, P), A(s_0, \overline{P})) = \frac{1}{N}\rho(A(s_0, P)]_N, A(s_0, \overline{P})]_N) = \frac{1}{N}\rho(P]_N, \overline{P}]_N) = \mu(P, \overline{P}).$$

Теорема доказана.

В связи с приведенным утверждением представляет интерес описание конечных автоматов без потери информации о метрике ρ.

Пусть $A = (X, S, Y, (\delta_x)_{x\in X}, (\beta_x)_{x\in X})$ – конечный автомат с потерей информации о метрике ρ. Для состояния $s\in S$ с потерей информации о метрике ρ через L(s) обозначим минимальную длину входных слов P, P′, для которых выполняются приведенные выше условия (26), (27). Положим

$$L(A) = \min L(s),$$

где минимум берется по всем состояниям s автомата A с потерей информации о метрике ρ.

Предложение 1. Для автомата $A(X, S, Y, (\delta x)x\in X, (\beta x)x\in X)$, $|S|>1$, с потерей информации о метрике ρ выполняется неравенство

$$L(A) \le \frac{3}{2}\,|S|(|S| - 1) + 2.$$

Доказательство. Пусть s – состояние с потерей информации о метрике ρ и $L(A) = L(s) = L$. Тогда найдутся $s'\in S$ и

$$P = x_1, x_2, \ldots, x_L,\ P' = x_1', x_2', \ldots, x_L',$$

при которых выполняются условия (26), (27), то есть

$$h_P s = s',\ h_{P'} s = s',$$

$$\rho(P, P') \ne \rho(A(s, P), A(s, P')).$$

Положим:

$A(s, P) = y_1, y_2, \ldots, y_L$, $A(s, P') = y_1', y_2', \ldots, y_L'$,

$A_M(s, P) = s_1, s_2, \ldots, s_{L+1}$, $A_M(s, P') = s_1', s_2', \ldots, s'_{L+1}$,

$s_1 = s'_1 = s$, $s_{L+1} = s'_{L+1} = s'$.

Покажем, что $s_j \ne s'_j$, $j\in\{2, \ldots, L\}$ при $L>1$. Действительно, если $s_{j'} = s'_{j'}$ для некоторого j', то из определения величины L следует, что

$$\rho(P, P') = \rho(x_1, x_2,\ldots, x_{j'-1}; x'_1, x'_2, \ldots, x'_{j'-1}) + \rho(x_j, \ldots, x_L; x'_j, \ldots, x'_L) =$$
$$= \rho(y_1, y_2, \ldots, y_{j'-1}; y'_1, y'_2, \ldots, y'_{j'-1}) + \rho(y_j, \ldots, y_L; y'_{j'}, \ldots, y'_L) =$$
$$= \rho(A(s, P), A(s, P')),$$

что противоречит начальному выбору s.

Предположим, что $L-1 \ge |S|(|S|-1)+1$. Тогда в последовательности пар состояний (s_j, s'_j), $j \in\{2, \ldots, L\}$ имеются одинаковые пары $\{s_{k+1}\, s'_{k+1}\}$, $\{s_{k+n}, s'_{k+n}\}$, где

$$1\le n - 1\le(1/2)\,|S|(|S| - 1).$$

Предположим для определенности, что

$$s_{k+1} = s'_{k+n},\ s'_{k+1} = s_{k+n}.$$

Случай $s_{k+1} = s_{k+n}$, $s'_{k+1} = s'_{k+n}$ рассматривается аналогично.

Для слов

$$\overline{P} = x_1, \ldots, x_k, x'_{k+n}, \ldots, x'_L,\ \overline{P}` = x'_1, \ldots, x'_k, x_{k+n}, \ldots, x_L$$

в силу выбора L справедливы равенства:

$$h_{\overline{P}} s = s`,\ h_{\overline{P}`} s = s`,\ \rho(\overline{P}, \overline{P}`) = \rho(A(s, \overline{P}), A(s, \overline{P}`)).$$

При этом

$$A_M(s, x_1, \ldots, x_k, x'_{k+n}, \ldots, x'_L) = s_1, s_2, \ldots, s_{k+1}, s'_{k+n+1}, \ldots, s'_{L+1},$$
$$A_M(s, x'_1, \ldots, x'_k, x_{k+n}, \ldots, x_L) = s_1, s'_2, \ldots, s'_{k+1}, s_{k+n+1}, \ldots, s_{L+1},$$
$$\rho(P, P') = \rho(\overline{P}, \overline{P}`) + \rho(x_{k+1}, \ldots, x_{k+n-1}; x'_{k+1}, \ldots, x'_{k+n-1}).$$

Следовательно,

$$\rho(A(s_{k+1}, x_{k+1}, \ldots, x_{k+n-1}), A(s'_{k+1}, x'_{k+1}, \ldots, x'_{k+n-1})) \neq \rho(x_{k+1}, \ldots, x_{k+n-1}; x'_{k+1}, \ldots, x'_{k+n-1})).$$

Если среди последовательности пар состояний $\{s_j, s'_j\}$, $j \in \{2, \ldots, k\}$, имеются одинаковые пары, например, $s_c = s'_{c+d}$, $s'_c = s_{c+d}$, то в силу выбора L для слов

$$^{\wedge}P = x_1, \ldots, x_{c-1}, x'_{c+d}, \ldots, x'_k, x_{k+n}, \ldots, x_L,$$

$$^{\wedge}P` = x'_1, \ldots, x'_{c-1}, x_{c+d}, \ldots, x_k, x'_{k+n}, \ldots, x'_L$$

выполняются соотношения

$$h_{^{\wedge}P}s = s`,\ h_{^{\wedge}P}s = s`,\ \rho(^{\wedge}P, {}^{\wedge}P`) = \rho(A(s, {}^{\wedge}P), A(s, {}^{\wedge}P`)).$$

Поэтому для слов

$$P(1) = x_1, \ldots, x_{c-1}, x'_{c+d}, \ldots, x'_k, x'_{k+1}, \ldots, x'_L;$$

$$P(2) = x'_1, \ldots, x'_{c-1}, x_{c+d}, \ldots, x_k, x_{k+n}, \ldots, x_L$$

длины, меньшей L, выполняются соотношения:

$$h_{P(1)}s = s`,\ h_{P(2)}s = s`,\ \rho(P(1), P(2)) \neq \rho(A(s, P(1)), A(s, P(2))),$$

что противоречит выбору L. Значит, среди пар состояний $\{s_j, s'_j\}$, $j \in \{2, \ldots k\}$ нет одинаковых неупорядоченных пар вида $s_c = s'_{c+d}$, $s'_c = s_{c+d}$.

Аналогично доказывается, что среди пар состояний $\{sj, s'j\}$, $j \in \{2, \ldots, k\}$, нет одинаковых пар вида $sc = s'c$, $s'c+d = sc+d$. Таким образом, в последовательности пар состояний $\{sj, s'j\}$, $j \in \{2, \ldots, k\}$ нет одинаковых неупорядоченных пар.

С помощью аналогичных приемов доказывается, что среди пар состояний $\{sj, s'j\}$, $j \in \{k+n+1, \ldots, L\}$ также нет одинаковых неупорядоченных пар.

Следовательно, если $L-1 \geq |S|(|S|-1)+1$, то $L-1 \leq (3/2)|S|(|S|-1)+1$, откуда и вытекает справедливость предложения 1.

Данное утверждение характеризует трудоемкость проверки автомата

$$A = (X, S, Y, (\delta_x)_{x \in X}, (\beta_x)_{x \in X}),\ |S| > 1,$$

на предмет потери информации о метрике ρ. Такая проверка может быть проведена с помощью опробования всех его состояний и нахождения для каждого состояния s-выходных последовательностей A(s, P) и последовательностей состояний $A_M(s, P)$ для всех входных слов P длины $(3/2)|S|(|S|-1) + 2$.

Представляет интерес получение явного описания перестановочных автоматов A(s), реализующих при начальном состоянии s отображения $X_П$ в $Y_П$, сохраняющих метрику μ.

Теорема 2. Отображение $X_П$ в $Y_П$, реализуемое перестановочным приведенным автоматом A(s) = (X, S, Y, h, f) при начальном состоянии s, сохраняет метрику μ тогда и только тогда, когда автомат A(s) внутренне автономен и при каждом фиксированном состоянии $s' \in S$ отображение $f_{s'}$: $X \to Y$, ($f_{s`}(x) = f(x, s`)$) является инъективным.

Доказательство. Если перестановочный приведенный автомат A(s) внутренне автономен и при каждом состоянии s′ из S(s) отображение $h_{s'}$ является инъективным, то, очевидно, отображение $\varphi_{A(s)}$, реализуемое перестановочным приведенным автоматом A, сохраняет метрику μ.

Пусть отображение $\varphi_{A(s)}$ сохраняет метрику μ. Выберем произвольное состояние $s^{\sim} \in S(s)$ и предположим, что при некоторых x_1, x'_1 из X

$$h_{x_1} s^{\sim} \neq h_{x`_1} s^{\sim}.$$

Так как A(s) – перестановочный автомат, можно найти его входные слова вида

$$P = x_1, x_2, \ldots, x_N, P' = x'_1, x'_2, \ldots, x'_N$$

и состояние $s_{N+1} \in S(s)$, при которых

$$h_P s^{\sim} = h_{P`} s^{\sim} = s_{N+1}.$$

По теореме 1 автомат A(s) является автоматом без потери информации о метрике ρ. Следовательно,

$$\rho(P, P') = \rho(A(s^{\sim}, P), A(s^{\sim}, P')).$$

Для произвольного входного слова $P^{\sim} = x^{\sim}_1, x^{\sim}_2, \ldots, x^{\sim}_k$ автомата A(s), используя перестановочность автомата A(s), можно найти его входное слово вида $P^{\wedge} = P^{\sim}, P^{\sim}, \ldots, P^{\sim}$,
при котором

$$h_{P^{\wedge}} h_{x_1} s^{\sim} = h_{x_1} s^{\sim}, \quad h_{P^{\wedge}} h_{x`_1} s^{\sim} = h_{x`_1} s^{\sim}.$$

Тогда

$$h_{x_N} \ldots h_{x_2} h_{P^{\wedge}} h_{x_1} s^{\sim} = h_{x`_N} \ldots h_{x`_2} h_{P^{\wedge}} h_{x`_1} s^{\sim}$$

Ранее отмечалось, что A(s) – автомат без потери информации о метрике ρ. Поэтому наряду с равенством

$$\rho(P, P') = \rho(A(s^{\sim}, P), A(s^{\sim}, P')),$$

справедливо равенство

$$\rho(x_1, P^\wedge, x_2, \ldots, x_N; x'_1, P^\wedge, x'_2, \ldots, x'_N) =$$
$$= \rho(A(s^\sim, x_1, P^\wedge, x_2, \ldots, x_N), A(s^\sim, x'_1, P^\wedge, x'_2, \ldots, x'_N)),$$
откуда следует, что
$$A(h_{x_1} s^\sim, P^\wedge) = A(h_{x'_1} s^\sim, P^\wedge).$$

Начальное слово $P^\sim$ слова $P^\wedge$ было выбрано произвольным. Следовательно, состояния $h_{x_1} s^\sim$ и $h_{x'_1} s^\sim$ автомата A(s) неотличимы, что противоречит его приведенности. Таким образом, автомат A(s) является внутренне автономным автоматом. Если для некоторого $s' \in S(s)$ найдутся x, x′, при которых $f_x s' = f_{x'} s'$, то, очевидно, внутренне автономный автомат A(s) будет автоматом с потерей информации о метрике ρ, и следовательно, по теореме 1, отображение $\varphi_{A(s)}$ не является отображением, сохраняющим метрику μ.

Теорема доказана.

Представляет интерес описание автоматных отображений $X_П$ в $Y_П$, сохраняющих наряду со значениями функции μ и периоды последовательностей.

Следствие 1. Для того чтобы, отображение $X_П$ в $Y_П$, реализуемое перестановочным приведенным автоматом
$$A(s) = (X, S(s), Y, h, f)$$
при начальном состоянии s, сохраняло метрику μ и периоды входных последовательностей, необходимо и достаточно, чтобы S(s) = {s} ({s} – одноэлементное множество) и отображение f_s ($f_s(x) = f(x, s)$) было инъективным.

Доказательство. Достаточность условий следствия очевидна. Докажем их необходимость. По теореме 2 автомат A(s) внутренне автономен и при каждом $s \in S(s)$ функция f_s инъективна. Так как при начальном состоянии s автоматное отображение $X_П$ в $Y_П$ сохраняет периоды, для каждого $x \in X$ период выходной последовательности A(s, x, x, ...) равен единице. Отсюда следует, что все отображения $f_{s'}$, $s' \in S(s)$ совпадают. Условие |S(s)| = 1 теперь следует из приведенности автомата A(s).

19.3. Описание множества GA(XП, YП, ≥, μ)

Перейдем к описанию автоматных отображений множества $X_П$ в $Y_П$, не увеличивающих значение метрики μ. Ниже будет дано описание перестановочных автоматов A, для которых отображение $X_П$ в

$Y_П$, реализуемое автоматом A при любом начальном состоянии s, не увеличивает значение метрики μ.

Определение 3. Автомат $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ называется автоматом с возрастающей потерей информации о метрике ρ, если найдутся входные слова P, P′ из X*, состояния s, s′ из S, при которых

$$h_P s = s', h_{P'} s = s', \ |P|=|P'|; \qquad (28)3$$

$$\rho(P, P') < \rho(A(s, P), A(s, P')). \qquad (29)4$$

В противном случае автомат A называется автоматом с невозрастающей потерей информации о метрике ρ. Состояние s, для которого выполнены условия (28), (29), называется состоянием с возрастающей потерей информации о метрике ρ.

Теорема 3. Отображение $X_П$ в $Y_П$, реализуемое перестановочным автоматом A при начальном состоянии s_0, не увеличивает значение метрики μ тогда и только тогда, когда $A(s_0)$ – автомат с невозрастающей потерей информации о метрике ρ.

Доказательство. Предположим, что $A(s_0)$ – сильно связный автомат с возрастающей потерей информации о метрике ρ. Тогда найдутся входные слова $P = P_2$, $P' = P_3$ и состояния $s = s_1$, $s' = s_2$, о которых говорится в определении 3, и входные слова P_1, P_4, при которых

$$h_{P_1} s_0 = s_1, \ h_{P_4} s_2 = s_0.$$

Рассмотрим периодические последовательности

$$P = P_1P_2P_4\ldots, \ P^\wedge = P_1P_3P_4\ldots$$

элементов алфавита X периодов, ω, ω^, соответственно, таких, что ω| R, где

$$R = |P_1P_2P_4| = |P_1P_3P_4|,$$

и выходные последовательности $A(s_0, P)$, $A(s_0, P^\wedge)$ периодов W, W^ соответственно. Очевидно, что W| R, W^| R, в связи с чем непосредственно проверяется, что

$$\mu(P, P^\wedge) = \frac{\rho_{[\omega,\omega^\wedge]}(P, P^\wedge)}{[\omega,\omega^\wedge]} = \frac{\rho_R(P, P^\wedge)}{R} = \frac{\rho(P_2, P_3)}{R};$$

$$\mu(A(s_0, P), A(s_0, P^\wedge) = \frac{\rho_{[W,W^\wedge]}(A(s_0, P), A(s_0, P^\wedge)}{[W,W^\wedge]};$$

$$= \frac{\rho_R(A(s_0, P), A(s_0, P^\wedge)}{R} = \frac{\rho(A(s_1, P_2), A(s_1, P_3)}{R},$$

в связи с чем

$$\mu(P, P^\wedge) < \mu(A(s_0, P), A(s_0, P^\wedge)),$$

то есть получено противоречие.

Предположим теперь, что $A(s_0)$ – перестановочный автомат с невозрастающей потерей информации о метрике ρ. Рассмотрим произвольные периодические последовательности P, $P^\wedge$ периодов ω, $\omega^\wedge$ соответственно. Очевидно, найдутся m_1, m_2, при которых периоды последовательностей состояний $A_M(s_0, P)$, $A_M(s_0, P^\wedge)$ делят соответственно величины $m_1\omega$, $m_2\omega^\wedge$. Положим $N = [m_1\omega, m_2\omega^\wedge]$. Легко видеть, что периоды последовательностей $A(s_0, P)$ и $A(s_0,P^\wedge)$ делят N, поэтому

$$\mu(A(s_0, P), A(s_0, P^\wedge)) = \frac{\rho_N(A(s_0,P), A(s_0,P^\wedge))}{N} \le \frac{\rho_N(P,P^\wedge)}{N} = \mu(P, P^\wedge).$$

Теорема доказана.

В связи с утверждением теоремы 3 представляет интерес описание конечных автоматов с возрастающей потерей информации о метрике ρ.

Пусть $A(X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ – конечный автомат с возрастающей потерей информации о метрике ρ. Для состояния $s\in S$ с возрастающей потерей информации о метрике ρ обозначим через $L'(s)$ минимальную длину входных слов P, P', для которых выполняются условия (28), (29). Положим

$$L'(A) = \min L'(s),$$

где минимум берется по всем состояниям s автомата A с возрастающей потерей информации о метрике ρ.

Предложение 2. Если $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ – автомат с возрастающей потерей информации о метрике ρ и $|S| > 1$, то выполняется неравенство

$$L'(A) \le 2c^2 + 5c + 2,$$

где $c = \frac{1}{2}|S|(|S| - 1)$.

Доказательство. Пусть s – состояние автомата A с возрастающей потерей информации о метрике ρ и $L'(A)=L'(s)=L$. Тогда найдутся $s' \in S$ и входные слова

$$P = x_1, x_2, \ldots, x_L, P' = x'_1, x'_2, \ldots, x'_L$$

автомата A, при которых

$$h_P s = s', h_{P'} s = s', \rho(P, P') < \rho(A(s, P), A(s, P'));$$
$$A(s, P) = y_1, y_2, \ldots, y_L, A(s, P') = y'_1, y'_2, \ldots, y'_L;$$
$$A_M(s, P) = s_1, s_2, \ldots, s_{L+1}, A_M(s, P') = s'_1, s'_2, \ldots, s'_{L+1};$$
$$s_1 = s'_1 = s, s_{L+1} = s'_{L+1} = s'.$$

Покажем, что $s_j \neq s'_j$, $j \in \{2, \ldots, L\}$ при $L > 1$. Действительно, если $s_{j'} = s'_{j'}$ для некоторого j', то из определения величины L вытекает, что

$$\rho(P, P') = \rho(x_1, x_2, \ldots, x_{j'-1}; x'_1, x'_2, \ldots, x'_{j'-1}) + \rho(x_j, \ldots, x_L; x'_j, \ldots, x'_L)$$
$$\geq \rho(y_1, y_2, \ldots, y_{j'-1}; y'_1, y'_2, \ldots, y'_{j'-1}) + \rho(y_j, \ldots, y_L; y'_j, \ldots, y'_L) =$$
$$= \rho(A(s, P), A(s, P')),$$

что противоречит начальному выбору s.

Предположим, что $L - 1 \geq (1/2)|S|(|S|-1)+1$.

Тогда в последовательности пар состояний (s_j, s'_j), $j \in \{2, \ldots, L\}$, имеются одинаковые пары $\{s_{k+1}, s'_{k+1}\}$, $\{s_{k+n}, s'_{k+n}\}$, где $1 \leq n-1 \leq (1/2)|S|(|S|-1)$.

Предположим для определенности, что имеет место случай

$$s_{k+1} = s'_{k+n},\ s'_{k+1} = s_{k+n}.$$

Случай $s_{k+1} = s_{k+n}$, $s'_{k+1} = s'_{k+n}$ рассматривается аналогично. Для слов

$$\wedge P = x_1, \ldots, x_k, x'_{k+n}, \ldots, x'_L,\ \wedge P` = x'_1, \ldots, x'_k, x_{k+n}, \ldots, x_L$$

в силу выбора L справедливы соотношения:

$$h_{\wedge P} s = s`,\ h_{\wedge P`} s = s`,\ \rho(\wedge P, \wedge P`) \geq \rho(A(s, \wedge P), A(s, \wedge P`)), \qquad (30)5$$

при этом

$$A_M(s, x_1, \ldots, x_k, x'_{k+n}, \ldots, x'_L) = s_1, s_2, \ldots, s_{k+1}, s'_{k+n+1}, \ldots, s'_{L+1};$$
$$A_M(s, x'_1, \ldots, x'_k, x_{k+n}, \ldots, x_L) = s_1, s'_2, \ldots, s'_{k+1}, s_{k+n+1}, \ldots, s_{L+1},$$

Далее,

$$\rho(P, P') = \rho(\wedge P, \wedge P`) + \rho(x_{k+1}, \ldots, x_{k+n-1}; x'_{k+1}, \ldots, x'_{k+n-1}) <$$
$$< \rho(A(s, P), A(s, P')) = \rho(A(s, \wedge P), A(s, \wedge P`)) +$$
$$+ \rho(A(s_{k+1}, x_{k+1}, \ldots, x_{k+n-1}), A(s'_{k+1}, x'_{k+1}, \ldots, x'_{k+n-1})).$$

Учитывая (27), получаем (для первого случая) важный промежуточный результат

$$\rho(x_{k+1}, \ldots, x_{k+n-1}; x'_{k+1}, \ldots, x'_{k+n-1}) <$$
$$< \rho(A(s_{k+1}, x_{k+1}, \ldots, x_{k+n-1}), A(s'_{k+1}, x'_{k+1}, \ldots, x'_{k+n-1})) \qquad (31)6$$

и

$$h_{\wedge P} s = s`,\ h_{\wedge P`} s = s`,\ \rho(\wedge P, \wedge P`) \geq \rho(A(s, \wedge P), A(s, \wedge P`)).$$

Аналогичные соотношения выписываются для случая $s_{k+1} = s_{k+n}$, $s'_{k+1} = s'_{k+n}$.

Именно,

$$\rho(x_{k+1}, \ldots, x_{k+n-1}; x'_{k+1}, \ldots, x'_{k+n-1}) <$$
$$< \rho(A(s_{k+1}, x_{k+1}, \ldots, x_{k+n-1}), A(s'_{k+1}, x'_{k+1}, \ldots, x'_{k+n-1}))$$

и

$$h_{\wedge P}s = s`, h_{\wedge P`}s = s`, \ \rho(\wedge P, \wedge P`) \geq \rho(A(s, \wedge P), A(s, \wedge P`)).$$

при $\wedge P = x_1, \ldots, x_k, x_{k+n}, \ldots, x_L$; $\wedge P` = x'_1, \ldots, x'_k, x'_{k+n}, \ldots, x'_L$. Докажем теперь, что для состояний s, s′ существуют входные слова ^P, ^P′ вида

$$\wedge P = \wedge P_1, \wedge P_2, \wedge P_3, \wedge P` = \wedge P`_1, \wedge P`_2, \wedge P`_3$$

длины L^, для которых выполняются следующие четыре условия:

(1) Справедливы соотношения:

$$h_{\wedge P}s = s`, \ h_{\wedge P`}s = s`, \ \rho(\wedge P, \wedge P`) \geq \rho(A(s, \wedge P), A(s, \wedge P`)),$$

$$A(s,\wedge P) = \wedge y_1, \wedge y_2, \ldots, \wedge y_{L\wedge}, \ A(s, \wedge P') = \wedge y`_1, \wedge y`_2, \ldots, \wedge y`_{L\wedge}$$

$$A_M(s,\wedge P) = \wedge s_1, \wedge s_2, \ldots, \wedge s_{L\wedge+1}, \ A_M(s, \wedge P') = \wedge s`_1, \wedge s`_2, \ldots, \wedge s`_{L\wedge+1},$$

$$\wedge s_1 = \wedge s`_1 = s, \ \wedge s_{L\wedge+1} = \wedge s`_{L\wedge+1} = s'.$$

(2) Существует k^, при котором

$$\wedge s_{k\wedge+1}, \ldots, \wedge s_{k\wedge+n} = s_{k+1}, \ldots, s_{k+n}, \wedge s`_{k\wedge+1}, \ldots, \wedge s`_{k\wedge+n} = s`_{k+1}, \ldots, s`_{k+n}$$

$$h_{\wedge P_2} \wedge s_{k\wedge+1} = \wedge s_{k\wedge+n}, \ h_{\wedge P`_2} \wedge s`_{k\wedge+1} = \wedge s`_{k\wedge+n}$$

$$\wedge P_2 = x_{k+1}, \ldots, x_{k+n-1}, \wedge P`_2 = x'_{k+1}, \ldots, x'_{k+n-1},$$

$$h_{\wedge P_1} \wedge s_1 = \wedge s_{k\wedge+1}, h_{\wedge P`_1} \wedge s_1 = \wedge s`_{k\wedge+1}.$$

(3) Среди пар состояний

$$(\wedge s_j, \wedge s'_j), j \in \{2, \ldots, k\}, \qquad (32)7$$

нет одинаковых неупорядоченных пар.

(4) Среди пар состояний

$$(\wedge s_j, \wedge s'_j), j \in \{k + n + 1, \ldots, L\}, \qquad (33)8$$

нет одинаковых неупорядоченных пар (параметр n определен ранее).

Для доказательства этого утверждения достаточно привести способ построения указанных последовательностей из последовательностей P, P′. Заметим, что для пары слов P, P′ могут не выполняться лишь условия (3) или (4).

Предположим, что для P, P′ среди пар состояний (s_j, s_j'), $j \in \{2, \ldots, k\}$, имеются одинаковые неупорядоченные пары, например, $s_c = s'_{c+d}$, $s'_c = s_{c+d}$ (случай $s_c = s_{c+d}$, $s'_c = s'_{c+d}$ рассматриваются аналогично). Тогда для слов

$$\tilde{P} = x_1, \ldots, x_{c-1}, x'_{c+d}, \ldots, x'_k, x'_{k+1}, \ldots, x'_L;$$

$$\tilde{P}` = x'_1, \ldots, x'_{c-1}, x_{c+d}, \ldots, x_k, x_{k+1}, \ldots, x_L$$

выполняются условия (1), (2), причем число неупорядоченных одинаковых пар в системе пар (32) для слов ~P, ~P` строго меньше, чем для слов P, P′. Если в системе пар (32) для слов ~P, ~P` еще остались одинаковые неупорядоченные пары, то аналогичным образом строится новая пара слов, для которой выполняются условия (1), (2),

причем для этих слов число неупорядоченных пар в системе (32) строго меньше, чем для ˜P, ˜P`. В силу конечности значения числа L в результате будет получена пара слов X(1), X(2), удовлетворяющая условиям (1), (2), (3). Аналогичные индукционные шаги для построения пары искомых слов $\wedge P = \wedge P_1, \wedge P_2, \wedge P_3$, $\wedge P` = \wedge P`_1, \wedge P`_2, \wedge P`_3$ исходя из слов X(1), X(2), очевидно, могут быть проведены для удовлетворения условия (4).

Теперь мы имеем все необходимое для получения верхней оценки величины L. Итак, пусть слова $\wedge P = \wedge P_1, \wedge P_2, \wedge P_3$, $\wedge P` = \wedge P`_1, \wedge P`_2, \wedge P`_3$ длины L удовлетворяют условиям 1–4. Тогда

$$|\wedge P_1| = |\wedge P`_1| \le c + 1,\ |\wedge P_3| = |\wedge P`_3| \le c + 1,\ |\wedge P_2| = |\wedge P`_2| = n - 1 \le c,\ L\wedge \le 3c + 2,$$

$$\wedge P_2 = x_{k+1}, \ldots, x_{k+n-1},\ \wedge P`_2 = x'_{k+1}, \ldots, x'_{k+n-1},\ h_{\wedge P_1} s = s_{k+1},\ h_{\wedge P`_1} s = s`_{k+1},$$

$$\rho(\wedge P, \wedge P`) \ge \rho(A(s, \wedge P), A(s, \wedge P`)),$$

$$\rho(\wedge P, \wedge P`) = \rho(\wedge P_1, \wedge P`_1) + \rho(\wedge P_2, \wedge P`_2) + \rho(\wedge P_3, \wedge P`_3),$$

$$\rho(A(s, \wedge P), A(s, \wedge P`)) = \rho(A(s, \wedge P_1), A(s\wedge, P`_1)) +$$

$$\rho(A(h_{\wedge P_1} s, \wedge P_2), A(h_{\wedge P`_1} s, \wedge P`_2)) +$$

$$+ \rho(A(h_{\wedge P_1 \wedge P_2} s, \wedge P_3), A(h_{\wedge P`_1 \wedge P`_2} s, \wedge P`_3)). \qquad (34)9$$

Исходя из этих соотношений, получаем неравенство

$$\rho(\wedge P_1, \wedge P`_1) + \rho(\wedge P_2, \wedge P`_2) + \rho(\wedge P_3, \wedge P`_3) \ge$$

$$\rho(A(s, \wedge P_1), A(s\wedge P`_1,)) + \rho(A(h_{\wedge P_1} s, \wedge P_2), A(h_{\wedge P`_1} s, \wedge P`_2)) +$$

$$+\rho(A(h_{\wedge P_1 \wedge P_2} s, \wedge P_3), A(h_{\wedge P`_1 \wedge P`_2} s, \wedge P`_3)) \qquad (35)10$$

Из (34) получаем, что

$$\rho(\wedge P_1, \wedge P`_1) + \rho(\wedge P_3, \wedge P`_3) \le 2(c+1).$$

Из (31) следует, что

$$\rho(\wedge P2, \wedge P`2) < \rho(A(h_{\wedge P_1} s, \wedge P_2), A(h_{\wedge P`_1} s, \wedge P`_2)). \qquad (36)11$$

В случае $s_{k+1} = s_{k+n}$, $s'_{k+1} = s'_{k+n}$ рассмотрим пару слов вида

$$\wedge P_1(\wedge P_2)^K \wedge P_3, \quad \wedge P`_1(\wedge P`_2)^K \wedge P`_3$$

где K – некоторое натуральное число. Справедливы равенства

$$h_{\wedge P_1(\wedge P_2)^K \wedge P_3} s = s`,\ h_{\wedge P`_1(\wedge P`_2)^K \wedge P`_3} s = s`.$$

Из (34) получаем, что

$$\rho(\wedge P_1(\wedge P_2)^K \wedge P_3, \wedge P`_1(\wedge P`_2)^K \wedge P`_3) = \rho(\wedge P_1, \wedge P`_1) + \rho(P_3, \wedge P`_3) + K\rho(\wedge P_2, \wedge P`_2).$$

В то же время из (35) и (36) следуют соотношения

$$\rho(A(s, \wedge P_1(\wedge P_2)^K \wedge P_3), A(s, \wedge P`_1(\wedge P`_2)^K \wedge P`_3)) =$$

$$= \rho(A(s, \wedge P_1), A(s\wedge P`_1,)) + \rho(A(h_{\wedge P_1 \wedge P_2} s, \wedge P_3),$$

$$A(h_{\wedge P`_1 \wedge P`_2} s, \wedge P`_3)) + K\rho(A(h_{\wedge P_1} s, \wedge P_2),$$

$$A(h_{\wedge P`_1} s, \wedge P`_2)) \ge \rho(A(s, \wedge P_1), A(s\wedge P`_1,)) + \rho(A(h_{\wedge P_1 \wedge P_2} s, \wedge P_3),$$

$$A(h_{\wedge P`_1 \wedge P`_2} s, \wedge P`_3)) + K + K\rho(\wedge P_2, \wedge P`_2) \geq K + K\rho(\wedge P_2, \wedge P`_2).$$

Итак, получены неравенства

$$\rho(\wedge P_1(\wedge P_2)^K \wedge P_3, \wedge P`_1(\wedge P`_2)^K \wedge P`_3) \leq 2(c + 1) + K\rho(\wedge P_2, \wedge P`_2),$$

$$\rho(A(s, \wedge P_1(\wedge P_2)^K \wedge P_3), A(s, \wedge P`_1(\wedge P`_2)^K \wedge P`_3)) \geq K + K\rho(\wedge P_2, \wedge P`_2).$$

Положив $K = 2c + 3$, получаем неравенство

$$\rho(\wedge P_1(\wedge P_2)^K \wedge P_3, \wedge P`_1(\wedge P`_2)^K \wedge P`_3) < \rho(A(s, \wedge P_1(\wedge P_2)^K \wedge P_3), A(s, \wedge P`_1(\wedge P`_2)^K \wedge P`_3))$$

при длине входных слов, используемых в неравенстве, не большей $2c+2+(2c+3)c$. Следовательно, и в рассматриваемом случае значение оцениваемой величины L не превосходит $2c^2 + 5c + 2$. В случае $s_{k+1} = s'_{k+n}$, $s'_{k+1} = s_{k+n}$ рассмотрим пару слов вида

$$\wedge P_1(\wedge P_2 \wedge P`_2)^K \wedge P_2 \wedge P_3, \wedge P`_1(\wedge P`_2 \wedge P_2)^K \wedge P`_2 \wedge P`_3,$$

где K – некоторое натуральное число. Справедливы равенства

$$h_{\wedge P_1(\wedge P_2 \wedge P`_2)^K \wedge P_2 \wedge P_3} s = s`;$$

$$h_{\wedge P`_1(\wedge P`_2 \wedge P_2)^K \wedge P`_2 \wedge P`_3} s = s`.$$

Из (34) вытекает равенство

$$\rho(\wedge P_1(\wedge P_2 \wedge P`_2)^K \wedge P_2 \wedge P_3, \wedge P`_1(\wedge P`_2 \wedge P_2)^K \wedge P`_2 \wedge P`_3) =$$
$$= \rho(\wedge P_1, \wedge P`_1) + \rho(\wedge P_3, \wedge P`_3) + (2K + 1)\rho(\wedge P_2, \wedge P`_2) \leq$$
$$\leq 2(c + 1) + (2K + 1)\rho(\wedge P_2, \wedge P`_2).$$

В то же время из (35) и (36) получаем, что

$$\rho(A(s, \wedge P_1(\wedge P_2 \wedge P`_2)^K \wedge P_2 \wedge P_3), A(s, \wedge P`_1(\wedge P`_2 \wedge P_2)^K \wedge P`_2 \wedge P`_3)) =$$
$$= \rho(A(s, \wedge P_1), A(s, \wedge P`_1)) + \rho(A(h_{\wedge P_1 \wedge P_2} s, \wedge P_3), A(h_{\wedge P`_1 \wedge P`_2} s, \wedge P`_3))$$
$$+ (2K + 1)\rho(A(h_{\wedge P_1} s, \wedge P_2), A(h_{\wedge P`_1} s, \wedge P`_2)) \geq$$
$$\geq \rho(A(s, \wedge P_1), A(s, \wedge P`_1) + \rho(A(h_{\wedge P_1 \wedge P_2} s, \wedge P_3), A(h_{\wedge P`_1 \wedge P`_2} s, \wedge P`_3)) +$$
$$+ (2K + 1) + (2K + 1)\rho(\wedge P_2, \wedge P`_2) \geq (2K + 1) + (2K + 1)\rho(\wedge P_2, \wedge P`_2).$$

Итак,

$$\rho(\wedge P_1(\wedge P_2 \wedge P`_2)^K \wedge P_2 \wedge P_3, \wedge P`_1(\wedge P`_2 \wedge P_2)^K \wedge P`_2 \wedge P`_3) \geq 2(c + 1) + (2K + 1)\rho(\wedge P_2, \wedge P`_2),$$

$$\rho(A(s, \wedge P_1(\wedge P_2 \wedge P`_2)^K \wedge P_2 \wedge P_3), A(s, \wedge P`_1(\wedge P`_2 \wedge P_2)^K \wedge P`_2 \wedge P`_3)) \geq$$
$$(2K + 1) + (2K + 1)\rho(\wedge P_2, \wedge P`_2).$$

Положив $K = c + 1$, находим, что

$$\rho(\wedge P_1(\wedge P_2 \wedge P`_2)^K \wedge P_2 \wedge P_3, \wedge P`_1(\wedge P`_2 \wedge P_2)^K \wedge P`_2 \wedge P`_3)$$
$$< \rho(A(s, \wedge P_1(\wedge P_2 \wedge P`_2)^K \wedge P_2 \wedge P_3), A(s, \wedge P`_1(\wedge P`_2 \wedge P_2)^K \wedge P`_2 \wedge P`_3))$$

при длине входных слов, используемых в неравенстве, не большей

$$3c+2+(c+1)2c = 2c^2+5c+2.$$

Следовательно, и во втором случае значение оцениваемой величины L не превосходит $2c^2+5c+2$. Предложение 2 доказано.

Данное утверждение характеризует трудоемкость проверки автомата

$$A = (X, S, Y, (h_x)_{xX}, (f_x)_{xX}), |S| > 1,$$

на предмет возрастания потери информации о метрике ρ. Такая проверка может быть проведена с помощью опробования всех его состояний и нахождения для каждого состояния s выходных последовательностей $A_M(s, P)$ для всех входных слов P длины $2c^2+5c+2$.

Теорема 4. Для того чтобы отображение $X_П$ в $Y_П$, реализуемое перестановочным приведенным автоматом

$$A = (X, S, Y, h, f)$$

при начальном состоянии в, не увеличивало значение метрики μ, необходимо и достаточно, чтобы автомат A(s) был внутренне автономен.

Доказательство. Достаточность условий теоремы очевидна. Докажем необходимость этих условий. Пусть отображение $X_П$ в $Y_П$, реализуемое перестановочным приведенным автоматом

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

при начальном состоянии $s\in S$ не увеличивает значение метрики μ. Выберем произвольное состояние $s` \in S(s)$ и предположим, что при некоторых $(x_1, x'_1)\in X$

$$h_{x_1} s` \neq h_{x`_1} s`.$$

Так как автомат A(s) – перестановочный, можно найти входные слова вида

$$P = x_1, x_2, \ldots, x_N, P' = x'_1, x'_2, \ldots, x'_N$$

и состояние $s_{N+1}S(s)$, при которых

$$h_P s` = h_{P'} s` = s_{N+1}.$$

По теореме 3 автомат A(s) является автоматом с невозрастающей потерей информации о метрике ρ. Следовательно,

$$\rho(P, P') \geq \rho(A(s`, P), A(s`, P')).$$

Для произвольного входного слова $P^{\sim} = x^{\sim}_1, x^{\sim}_2, \ldots, x^{\sim}_k$ автомата A(s) можно найти входное слово вида $P^{\wedge} = P^{\sim} P^{\sim} \ldots P^{\sim} = (P^{\sim})^r$, при котором

$$h_{\wedge P} h_{x_1} s` = h_{x_1} s`, \; h_{\wedge P} h_{x`_1} s` = h_{x`_1} s`,$$

Здесь r зависит от состояний $h_{x_1} s`$, $h_{x`_1} s`$ и от слова $P^{\sim}$. Тогда

$$h_{x_N} \ldots h_{x_2} h_{\wedge P} h_{x_1} s` = h_{x`_N} \ldots h_{x`_2} h_{\wedge P} h_{x`_1} s`$$

Ранее отмечалось, что A(s) – автомат с невозрастающей потерей информации о метрике ρ. Поэтому наряду с неравенством

$$\rho(P, P') \geq \rho(A(s`, P), A(s`, P'))$$

справедливо неравенство

$$\rho(x_1,\hat{}P,x_2,\ldots,x_N;\ x'_1,\hat{}P,x'_2,\ldots,x'_N) \geq$$
$$\geq\rho(A(s`,x_1,\hat{}P,x_2,\ldots,x_N),\ A(s`,x'_1,\hat{}P,x'_2,\ldots,x'_N)).$$

Справедливы соотношения

$$\rho(x_1,\ \hat{}P,\ x_2,\ \ldots,\ x_N;\ x`_1,\ \hat{}P,\ x'_2,\ \ldots,\ x'_N) =$$
$$= \rho(x_1,\ x_2,\ \ldots,\ x_N;\ x'_1,\ x'_2,\ \ldots,\ x'_N) \geq$$
$$\geq \rho(A(s`,\ x_1,\ \hat{}P,\ x_2,\ \ldots,\ x_N),\ A(s`,\ x'_1,\ \hat{}P,\ x'_2,\ \ldots,\ x'_N)) =$$
$$= \rho(A(s`,\ x_1,\ x_2,\ \ldots,\ x_N),\ A(s`,\ x'_1,\ x'_2,\ \ldots,\ x'_N)) + \rho(A(h_{x_1}s`,\hat{}P),$$
$$A(h_{x`_1}s`,\hat{}P).$$

Предыдущее неравенство теперь можно записать в виде

$$\rho(x_1,\ x_2,\ \ldots,\ x_N;\ x'_1,\ x'_2,\ \ldots,\ x'_N) \geq \rho(A(s`,\ x_1,\ x_2,\ \ldots,\ x_N);$$
$$A(s`,\ x'_1,\ x'_2,\ \ldots,\ x'_N)) + \rho(A(h_{x_1}s`,\hat{}P),\ A(h_{x`_1}s`,\hat{}P). \qquad (37)12$$

Напомним, что слово $P^{\sim}$ для построения слова $\hat{}P = (P^{\sim})^r$ было выбрано произвольным образом. Следовательно, данное неравенство выполняется при каждом слове $\hat{}P$, построенном для произвольного слова $P^{\sim}$. При различных состояниях $h_{x_1}s`$, $h_{x`_1}s`$ автомата A(s) в силу его приведенности для любого натурального числа C, очевидно, можно подобрать слово $P^{\sim}$ так, чтобы

$$\rho(A(h_{x_1}s`,\ P^{\sim}),\ A(h_{x`_1}s`,\ P^{\sim})) > C$$

и, следовательно,

$$\rho(A(h_{x_1}s`,\hat{}P,),\ A(h_{x`_1}s`,\hat{}P)) > C,$$

что противоречит некоторым из неравенств (37). Следовательно, при любых $s'\in S(s)$, $(x_1,\ x'_1)\in X$ справедливо равенство $h_{x_1}s`=h_{x`_1}s`$, то есть автомат A(s) внутренне автономен.

Теорема доказана.

Из теоремы 4 непосредственно вытекает следующее следствие.

Следствие 2. Отображение $X_П$ в $Y_П$, реализуемое перестановочным приведенным автоматом

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

при начальном состоянии s, является инъективным и не увеличивающим значение метрики μ, тогда и только тогда, когда автомат A(s) внутренне автономен и при каждом фиксированном состоянии s′ S(s) отображение $f_{s'}$ ($f_{s'}(x) = f_x(s`)$) является инъективным.

Глава 20. АВТОМАТНЫЕ ОТОБРАЖЕНИЯ СЛОВ, РАЗМНОЖАЮЩИЕ ИСКАЖЕНИЯ В МЕТРИКАХ ХЭММИНГА И ЛЕВЕНШТЕЙНА НЕ БОЛЕЕ ЧЕМ В К РАЗ

Пусть Ω* – множество всех слов конечных длин в конечном алфавите Ω. Дается полное описание всех автоматных отображений множества X* в Y*, которые размножают ошибки типа замены букв в словах не более чем в К раз. Дается полное описание инъективных автоматных отображений множества X* в Y*, которые размножают ошибки типа пропуска букв не более чем в К раз. Аналогичный результат получен для метрики выпадений и вставок букв. Предполагается, что алфавиты автоматов конечны.

20.1. Историческая справка

В главе продолжаются исследования, связанные с проблемой описания отображений множества X* в Y*, которые размножают ошибки типа замены букв не более чем в К раз. Данная проблема была поставлена А. А. Марковым в 1956 г. Им были описаны все биективные преобразования множества слов Ω*, сохраняющие длины слов и не увеличивающие расстояния Хэмминга между словами одной длины, то есть не размножающими искажения типа замены букв в словах. Дальнейшие исследования по указанной проблеме, связанные с исследованием инъективных отображений, а также с рассмотрением и других искажений слов, например, искажений типа выпадений или вставки букв в слова, были проведены в работе М. М. Глухова[1]. Описание же всех инъективных отображений множества X* в Y*, не размножающих ошибки типа пропуска букв, было дано в [26]. Таким образом, говоря о конечных результатах исследований по указанной проблеме А. А. Маркова, можно заметить, что она решена пока в частном случае К = 1, при этом описаны лишь биективные отображения с требуемым свойством. В данном параграфе дается полное описание произвольных (то есть, возможно, не инъективных) конечно-автоматных отображений множества X* в Y*, которые размножают ошибки типа замены букв не более чем в К раз. Дается и полное описание инъективных ко-

[1] См. : Глухов М. М. Инъективные отображения слов, не размножающие искажений // Труды по дискретной математике. – 2001. – Т. 4 – С. 17–32.

нечно-автоматных отображений множества X* в Y*, которые размножают ошибки типа пропуска букв не более чем в К раз. Аналогичный результат получен для метрики выпадений и вставок букв, введенной в [34].

20.2. Обозначения и основные понятия

Используем следующие обозначения:

$|\Omega|$ – мощность множества Ω;

X, Y – конечные алфавиты $|X|>1$, $|Y|>1$, $x\in X$, $y\in Y$;

X* (Y*) – множество всех слов конечной длины алфавита X (Y), считаем, что пустое слово $\varnothing$ принадлежит X* (Y*);

для $\mathfrak{I},\mathfrak{I}`\in X^k$ , $\mathfrak{I}=x1,x2,\ldots,xk$, $\mathfrak{I}`=x`1,x`2,\ldots,x`k$ $\rho(\mathfrak{I},\mathfrak{I}`)$ – расстояние Хэмминга между словами $\mathfrak{I},\mathfrak{I}`\in X^k$ $\mathfrak{I}=x1,x2,\ldots,xk$, $\mathfrak{I}`=x`1,x`2,\ldots,x`k$.

Определение 1. Отображение φ: $X^*\to Y^*$ называется отображением увеличивающим метрику ρ не более чем в К раз, если для любых слов $\mathfrak{I},\mathfrak{I}`\in X^*$ выполняются условия

$$|\mathfrak{I}| = |\mathfrak{I}`| \Rightarrow |\varphi(\mathfrak{I})| = |\varphi(\mathfrak{I}`)| \qquad (38)$$

$$K\rho(\mathfrak{I}, \mathfrak{I}`) \geq \rho(\varphi(\mathfrak{I}), \varphi(\mathfrak{I}`) \qquad (39)$$

При К = 1 такое отображение называют *не увеличивающим метрику ρ (не размножающим искажения типа замены букв* [56]).

Множество всех отображений φ: $X^*\to Y^*$, увеличивающих метрику ρ не более чем в К раз, обозначим через $G(X^*,Y^*\rho, K)$. Множество всех инъективных отображений из $G(X^*,X^*\rho, 1)$ полностью описано в [18].

Через $A = (X, S, Y, (\delta_x)_{x\in X}, (\beta_x)_{x\in X})$ обозначим конечный автомат с входным алфавитом X, множеством состояний S, выходным алфавитом Y, частичными функциями переходов $(\delta_x)_{x\in X}$, δ_x: $S\to S$ и частичными функциями выхода $(\beta_x)_{x\in X}$, β_x: $S\to S$. Выходное слово автомата A, соответствующее входному слову $\mathfrak{I}\in X^*$ и начальному состоянию $s\in S$, обозначим через $A(s, \mathfrak{I})$; при $\mathfrak{I} = x1, x1, \ldots, xk$ слово $A(s, \mathfrak{I}) = y1, y2, \ldots, yk = \beta_{x1}s, \beta_{x2}\delta_{x1}s, \ldots, \beta_{xk}\delta_{xk-1}\ldots\delta_{x1}s$, $xj\in X$, $yj\in Y$, $j\in\{1, \ldots, k\}$.

Автоматным отображением назовем отображение A_s: $X^* \to Y^*$, задаваемое равенством $A_s(\mathfrak{I}) = A(s, \mathfrak{I})$. Для описания автоматного отображения A_s будем использовать подавтомат $A[s]$ автомата A, порожденный состоянием $s \in S$. Множеством состояний автомата A_s является подмножество S_s множества S, состоящее из состояния s и всех состояний, достижимых из s в графе переходов автомата A. Подграф Γ_s графа автомата A, соответствующий множеству S_s, определяет подавтомат $A[s] = (X, S_s, Y, (\delta_x)_{x \in X}, (\beta_x)_{x \in X})$ автомата A. Здесь для простоты обозначений ограничения отображений $(\delta_x)_{x \in X}, (\beta_x)_{x \in X}$ на множестве S_s обозначены теми же символами.

Через $A((X^*, Y^* \rho, K)$ обозначим множество всех автоматных отображений A_s: $X^* \to Y^*$, увеличивающих метрику ρ не более чем в K раз, то есть отображений A_s, для которых

$$K\rho(\mathfrak{I}, \mathfrak{I}`) \geq \rho(A_s(\mathfrak{I}), A_s(\mathfrak{I}`))$$

при любых словах $\mathfrak{I}, \mathfrak{I}` \in X^*$ одинаковой длины ($A_s(\varnothing) = \varnothing$).

Полное описание множества $A((X^*, Y^* \rho, K)$ дано в разделе 20.3 данной главы.

Обозначим через ε – бинарное отношение на множестве X^*, $\mathfrak{I}\varepsilon\mathfrak{I}`$ означает, что слово $\mathfrak{I}`$ получено из $\mathfrak{I}$ удалением одного вхождения некоторой его буквы (ε – бинарное отношение выпадения буквы); ε^t – t-я степень бинарного отношения ε. Через ε^{-1} обозначим обратное к ε бинарное отношение, именно, $\mathfrak{I}`\varepsilon^{-1}\mathfrak{I} \Leftrightarrow \mathfrak{I}\varepsilon\mathfrak{I}`$; ε^{-1} – бинарное отношение вставки буквы.

Бинарное отношение ε будет иметь тот же смысл и на множестве слов Y^*.

Определение 2. Отображение φ: $X^* \to Y^*$ называется отображением увеличивающим бинарное отношение ε не более чем в K раз, если для любых слов $\mathfrak{I}, \mathfrak{I}` \in X^*$ и любого $n \in \{1, 2, \ldots, |\mathfrak{I}|\}$ найдется число $m \in \{1, \ldots, Kn\}$ такое, что выполняется импликация

$$\mathfrak{I}\varepsilon^n\mathfrak{I}` \Rightarrow \varphi(\mathfrak{I})\varepsilon^m\varphi(\mathfrak{I}`).$$

При K = 1 такое отображение φ будем называть *не размножающим искажений типа пропуска букв* [18]. Через $AG((X^*, Y^* \varepsilon, K)$ обозначим множество всех автоматных инъективных отображений A_s: $X^* \to Y^*$, увеличивающих бинарное отношение ε не более чем в K раз. Описание множества $AG((X^*, Y^* \varepsilon, K)$ дается в пункте 4 данного параграфа.

Обозначим через D метрику Левенштейна на множестве X* (Y*) [34]; $D(\mathfrak{I},\mathfrak{I}`)$ означает минимальное число выпадений и вставок букв для получения из слова $\mathfrak{I}$ слова $\mathfrak{I}`$.

Определение 3. Отображение φ: $X^*\to Y^*$ называется отображением, увеличивающим метрику D не более чем в К раз, если для любых слов $(\mathfrak{I}, \mathfrak{I}`)\in X^*$ выполняется условие

$$KD(\mathfrak{I}, \mathfrak{I}`) \geq D(\varphi(\mathfrak{I}), \varphi(\mathfrak{I}`)).$$

Через AG((X*, Y*D, К) обозначим множество всех автоматных инъективных отображений A_s: $X^*\to Y^*$, увеличивающих метрику D не более чем в К раз. Описание множества AG((X*, Y*, D, К) дается в разделе 20.5.

20.3. Описание множества A((X*, Y*, ρ, К)

Определение 4. Б-шестеркой атомата $A = (X, S, Y, (\delta_x)_{x\in X}, (\beta_x)_{x\in X})$ называется набор $(s, x, x`, y, s_1, s`_1)\in S\times X\times X\times Y\times S\times S$, для компонент которого выполняются условия: $x \neq x`$, $\delta_x s = s_1$, $\delta_{x`} s = s`_1$, $s_1 \neq s`_1$, $\beta_x s = \beta_{x`} s = y$.

Б-шестерке $(s, x, x`, y, s_1, s`_1)$ в графе переходов автомата A соответствует фрагмент (рис. 20.3.1.)

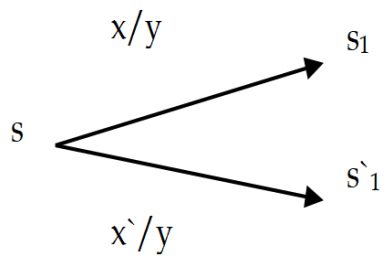

Рис. 20.3.1.

Для $\mathfrak{I}\in X^k$, $\mathfrak{I}$ = x1, x2, …, xk положим $\delta_{\mathfrak{I}} = \delta_{xk}\ldots\delta_{x2}\delta_{x1}$, $\delta_{\varnothing} s = s$ при любом $s\in S$.

Определение 5. Приемником Б-шестерки $(s, x, x`, y, s_1, s`_1)$ автомата A называется тройка $(x``, s_L, s`_L)\in X\times S\times S$, для элементов которой выполняются условия:

$s_L = s_1$, $s`_L = s`_1$, и $\beta_{x``} s_L \neq \beta_{x``} s`_L$ либо

$s_L = \delta_{\mathfrak{I}} s_1$, $s`_L = \delta_{\mathfrak{I}} s`_1$ для некоторого $\mathfrak{I}\in X^*\backslash\varnothing$ и $\beta_{x``} s_L \neq \beta_{x``} s`_L$.

При этом приемник $(x``, s_L, s`_L)$ называется особым, если $\delta_{x``}s_L = \delta_{x``}s`_L$; в противном случае приемник $(x``, s_L, s`_L)$ называется неособым.

Б-шестерке и ее приемнику в графе переходов автомата А соответствует фрагмент (рис. 20.3.2.)

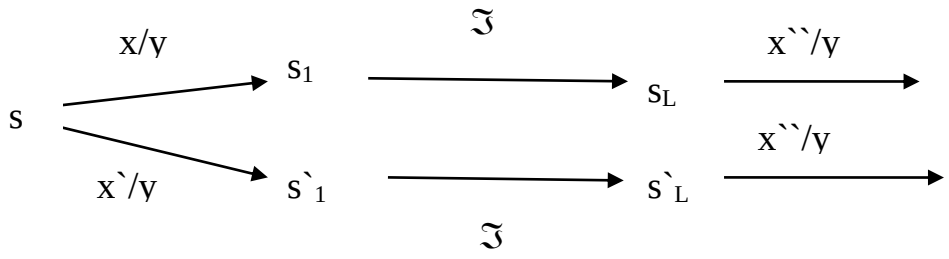

Рис. 20.3.2. – справа после стрелок нужны символы?

Определение 6. Б-семеркой автомата А называется набор $(s, x, x`, y, y`, s_1, s`_1) \in S \times X \times X \times Y \times Y \times S \times S$, для компонент которого выполняются условия:

$$x \neq x`,\ y \neq y`,\ \delta_x s = s_1,\ \delta_{x`} s = s`_1,\ s_1 \neq s`_1;\ \beta_x s = y,\ \beta_{x`} s = y`.$$

Б-семерке автомата А в его графе переходов соответствует фрагмент (рис. 20.3.3).

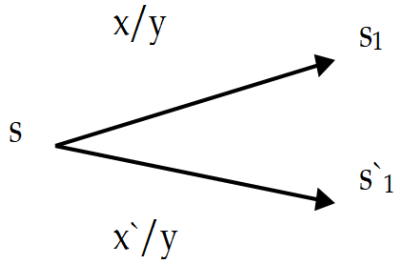

Рис. 20.3.3 – одинаковый с рисунком 20,3,1. Правильно? может быть, дать ссылку на рис. 20.3.1?

Для описания множества $A((X^*, Y^*\rho, K)$ выделим два случая $K=1$ и $K \geq 2$, которым соответствуют множество $A((X^*, Y^*\rho, K=1)$ всех автоматных отображений X^* в Y^*, не увеличивающих метрику ρ, и множество $A((X^*, Y^*\rho, K \geq 2)$ автоматных отображений X^* в Y^*, увеличивающих метрику ρ не более чем в K раз, $K \geq 2$.

Определение 7. Автомат А называется внутренне автономным автоматом, если для любого состояния $s \in S$ и любых $(x, x`) \in X$ справедливо равенство

$$\delta_x s = \delta_{x`} s.$$

Согласно определению, переходы состояний внутренне автономного автомата не зависят от входного слова: $\delta_{\mathfrak{I}} s = \delta_{\mathfrak{I}`} s$, $s \in S$.

Напомним, что автомат $A = (X, S, Y, (\delta_x)_{x \in X}, (\beta_x)_{x \in X})$ называется *приведенным,* если для любых различных состояний $(s, s`) \in S$ найдется входное слово $\mathfrak{I} \in X^*$, при котором $A(s, \mathfrak{I}) \neq A(s`, \mathfrak{I})$.

Описание первого множества $A((X^*, Y^*\rho, K = 1)$ дается следующей теоремой.

Теорема 1. Автоматное отображение A_{s0} не увеличивает метрику ρ тогда и только тогда, когда в приведенном автомате $A[s0] = (X, S_{s0}, Y, (\delta_x)_{x \in X}, (\beta_x)_{x \in X})$, реализующим отображение A_{s0}, во-первых, отсутствуют Б-семерки и, во-вторых, либо автомат A[s0] является внутренне автономным автоматом, либо каждый из приемников любой Б-шестерки автомата является особым.

Для формулировки описания множества $A((X^*, Y^*\rho, K \geq 2)$ введем дополнительные определения.

Определение 8. К-м приемником ($K \geq 1$) Б-шестерки $(s, x_1, x`_1, y, s_1, s`_1)$ автомата А (Б-семерки $(s, x_1, x`_1, y, y`, s_1, s`_1)$) называется тройка $(x, s_L, s`_L)$, компоненты которой удовлетворяют условиям: $s_L = \delta_{\mathfrak{I}} s_1$, $s`_L = \delta_{\mathfrak{I}} s`_1$, для некоторого $\mathfrak{I} \in X^*$ и $\beta_x s_L \neq \beta_x s`_L$ и

$$\rho(A(s1, \mathfrak{I}x), A(s`1, \mathfrak{I}x) = K.$$

Б-шестерке $(s, x_1, x`_1, y, s_1, s`_1)$ и ее К-му приемнику в графе переходов автомата А соответствует фрагмент (рис. 20.3.4.)

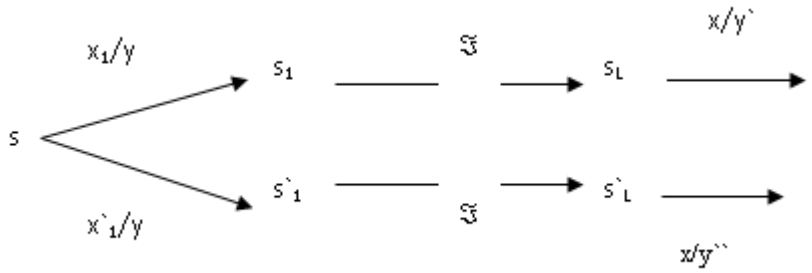

Рис. 20.3.4 - справа после стрелок, возможно, нужны символы?

Определение 9. К-й приемник $(x, s_L, s`_L)$ Б-шестерки $(s, x_1, x`_1, y, s_1, s`_1)$ автомата А (Б-семерки $(s, x_1, x`_1, y, y`, s_1, s`_1)$) называется особым, если

$$\delta_x s_L = \delta_x s`_L.$$

В противном случае К-й приемник $(x, s_L, s`_L)$ называется неособым.

Теорема 2. Автоматное отображение A_{s0} увеличивает метрику ρ не более чем в К раз (К≥2) тогда и только тогда, когда для приведенного автомата $A[s0] = (X, S_{s0}, Y, (\delta_x)_{x\in X}, (\beta_x)_{x\in X})$, реализующего отображение A_{s0}, выполнены условия:

1) либо автомат A[s0] является внутренне автономным;
2) либо

а) все К-приемники любой Б-шестерки особые,

б) все (К-1)-приемники любой Б-семерки особые.

Конструктивность условий теорем 1, 2 будет показана позднее. Перейдем к доказательствам.

Доказательство. Докажем сначала две вспомогательные леммы.

Лемма 1. Отображение $\varphi: X^* \to Y^*$ увеличивает метрику ρ не более чем в К раз тогда и только тогда, когда для любых слов $(\mathfrak{I}, \mathfrak{I}`) \in X^*$ одинаковой длины из условия $\rho(\mathfrak{I}, \mathfrak{I}`) = 1$ следует $\rho(\varphi(\mathfrak{I}), \varphi(\mathfrak{I}`)) \le K$.

Доказательство. Если отображение φ увеличивает метрику ρ не более чем в К раз то, по определению 1, для слов одинаковой длины справедлива импликация $\rho(\mathfrak{I}, \mathfrak{I}`) = 1 \Rightarrow \rho(\varphi(\mathfrak{I}), \varphi(\mathfrak{I}`)) \le K$. Предположим теперь, что эта импликация верна. Рассмотрим слова $\mathfrak{I}_0, \mathfrak{I}_m \in X^*$ одинаковой длины, для которых $\rho(\mathfrak{I}_0, \mathfrak{I}_m) = (m, m) \ge 2$. Для слов $\mathfrak{I}_0, \mathfrak{I}_m$ найдутся слова $\mathfrak{I}_1, \mathfrak{I}_2, \ldots, \mathfrak{I}_{m-1} \in X^*$, при которых

$$\rho(\mathfrak{I}_0, \mathfrak{I}_1) = \rho(\mathfrak{I}_1, \mathfrak{I}_2) = \ldots = \rho(\mathfrak{I}_{m-1}, \mathfrak{I}_m) = 1.$$

Согласно импликации получаем

$$\rho(\varphi(\mathfrak{I}_0), \varphi(\mathfrak{I}_1)) \le K, \rho(\varphi(\mathfrak{I}_1), \varphi(\mathfrak{I}_2)) \le K \ldots \rho(\varphi(\mathfrak{I}_{m-1}), \varphi(\mathfrak{I}_m)) \le K,$$

откуда следует, что $\rho(\varphi(\mathfrak{I}_0), \varphi(\mathfrak{I}_m)) \le mK$, согласно метрическим свойствам расстояния Хэмминга.

Лемма доказана.

Для слов $(\mathfrak{I}, \mathfrak{I}`) \in X^*$ будем через $\mathfrak{I}\mathfrak{I}`$ обозначать конкатенацию слов $\mathfrak{I}, \mathfrak{I}`$ (слово $\mathfrak{I}$ является началом слова $\mathfrak{I}\mathfrak{I}`$).

Лемма 2. Если автоматное отображения A_{s0} увеличивает метрику ρ не более чем в К раз, то при любом состоянии $s \in S_{s0}$ автомата

$A[s0] = (X, S_{s0}, Y, (\delta_x)_{x\in X}, (\beta_x)_{x\in X})$ автоматное отображение $A[s0]_s = A_s$ увеличивает метрику ρ не более чем в К раз.

Доказательство. Предположим противное. При выполнении условий леммы нашлось состояние $s\in S_{s0}$, при котором отображение $A[s0]_s$ не является увеличивающим метрику ρ не более чем в К раз. Тогда найдутся $(\mathfrak{I}`, \mathfrak{I}``)\in X^*$, при которых $\rho(A(s,\mathfrak{I}`), A(s, \mathfrak{I}``))>K\rho(\mathfrak{I}`, \mathfrak{I}``)$. Из определения автомата A[s0] следует, что найдется слово $\mathfrak{I}\in X^*$, при котором $\delta_{\mathfrak{I}}s0 = s$. Для конкатенаций $\mathfrak{I}\mathfrak{I}`$, $\mathfrak{I}\mathfrak{I}``$ слов $\mathfrak{I}, \mathfrak{I}`, \mathfrak{I}``$ получаем

$$\rho(A(s0, \mathfrak{I}\mathfrak{I}`), A(s0, \mathfrak{I}\mathfrak{I}``)) > K\rho(\mathfrak{I}\mathfrak{I}`, \mathfrak{I}\mathfrak{I}``),$$

что противоречит условиям леммы.

1. *Доказательство* теоремы 2. Пусть автоматное отображения A_{s0} увеличивает метрику ρ не более чем в К раз и автомат $A[s0] = (X, S_{s0}, Y, (\delta_x)_{x\in X}, (\beta_x)_{x\in X})$ не является внутренне автономным автоматом. Предположим, что в множестве всех К-приемников некоторой Б-шестерки $(s, x_1, x`_1, y_1, s_1, s`_1)$ имеется неособенный К-приемник $(x_L, s_L, s`_L)$, то есть в графе переходов автомата A[s0] существует диаграмма вида (рис. 20.3.5).

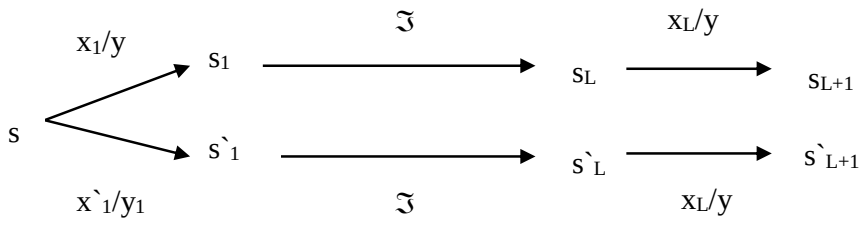

Рис. 20.3.5

$$x_1\neq x`_1,\ s_1\neq s`_1,\ s_L\neq s`_L,\ s_{L+1}\neq s`_{L+1},\ y_L\neq y`_L,\ \rho(A(s_1, \mathfrak{I}x_L), A(s`_1, \mathfrak{I}x_L) = K.$$

Так как A[so] – приведенный автомат, то для не равных состояний s_{L+1}, $s`_{L+1}$ найдется слово $\mathfrak{I}^\wedge\in X^*$, при котором $A(s_{L+1}, \mathfrak{I}^\wedge) \neq$ $\neq A(s`_{L+1}, \mathfrak{I}^\wedge)$. По этой причине

$$\rho(A(s, x_1\mathfrak{I}x_L\mathfrak{I}^\wedge), A(s, x`_1\mathfrak{I}x_L\mathfrak{I}^\wedge) \geq K+1.$$

Одновременно имеем

$$\rho(x_1\mathfrak{I}x_L\mathfrak{I}^\wedge, x`_1\mathfrak{I}x_L\mathfrak{I}^\wedge) = 1.$$

Следовательно, автоматное отображение A_s не является отображением, увеличивающим метрику ρ не более чем в К раз. Из леммы 2 вытекает, что и автоматное отображение A_{s0} не является отображением, увеличивающим метрику ρ не более чем в К раз. Таким

образом, получено противоречие с предположением о том, что в множестве всех К-приемников некоторой Б-шестерки (s, x_1, $x`_1$, $y_1$, $s_1$, $s`_1$) имеется неособенный К-приемник (x_L, s_L, $s`_L$). Аналогично получается противоречие, если предположить, что в множестве всех (К-1)-приемников некоторой Б-семерки ($s$, $x_1$, $x`_1$, y, $y`$, $s_1$, $s`_1$) имеется неособенный (К-1)-приемник (x_L, s_L, $s`_L$), то есть в графе переходов автомата A[s0] существует диаграмма вида (рис. 20.3.6)

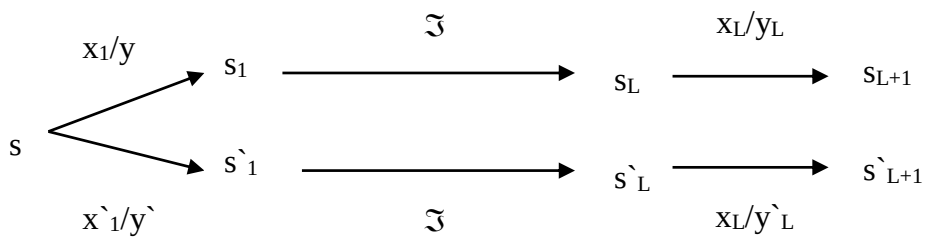

Рис. 20.3.6

Имеем $x_1 \neq x`_1$, $y \neq y`$, $s_1 \neq s`_1$, $s_L \neq s`_L$, $s_{L+1} \neq s`_{L+1}$, $y_L \neq y`_L$, $\rho(A(s_1, \Im x_L), A(s`_1, \Im x_L)) = К–1$.

В этом случае

$$\rho(A(s, x_1 \Im x_L \Im^{\wedge}), A(s, x`_1 \Im x_L \Im^{\wedge})) \geq К+1.$$

Одновременно имеем

$$\rho(x_1 \Im x_L \Im^{\wedge}, x`_1 \Im x_L \Im^{\wedge}) = 1.$$

Откуда получается противоречие.

Докажем теперь обратное утверждение теоремы 2.

Если автомат A[s0] внутренне автономен, то его отображение A_{s0} представимо в виде: $A_{s0}(x1, x2, \ldots, xk) = \beta_{x1}s0, \beta_{x2}s1, \ldots, \beta_{xk}sk–1$ для некоторых состояний s1, s2, …, sk–1 из S, не зависящих от x1, x2, …, xk. Поэтому отображение A_{s0} увеличивает ρ не более чем в один раз, и, следовательно, не более чем в К раз при любом К. Предположим, что выполнены условия: 1) автомат A[s0] не является внутренне автономным; 2) любой К-й приемник (если он существует) каждой Б-шестерки является особым; 3) любой К–1 приемник (если он существует) каждой Б-семерки является особым.

Из леммы 1 вытекает, что для доказательства достаточности условий теоремы 2 нам достаточно доказать, что из условия

$\rho(\mathfrak{I}, \mathfrak{I}`) = 1$, $(\mathfrak{I}, \mathfrak{I}`) \in X^*$ вытекает $\rho(A(s_0, \mathfrak{I}), A(s_0, \mathfrak{I}`)) \le K$. Докажем эту импликацию. Пусть $\rho(\mathfrak{I}, \mathfrak{I}`) = 1$, $(\mathfrak{I}, \mathfrak{I}`) \in X^*$. Представим слова $\mathfrak{I}$, $\mathfrak{I}`$ в виде $\mathfrak{I} = \mathfrak{I}_1 x_j \mathfrak{I}_2$, $\mathfrak{I}` = \mathfrak{I}_1 x`_j \mathfrak{I}_2$, где $x_j \ne x`_j$. Возможны случаи (рис. 20.3.7, 20.3.8).

Априори возможны лишь следующие случаи:

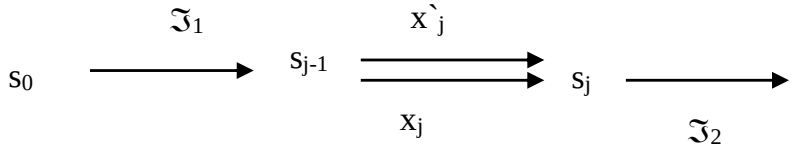

Рис. 20.3.7 справа после стрелок, возможно, нужны символы?

В первом случае (рис. 20.3.7): $\delta_{x_j} s_{j-1} = \delta_{x`_j} s_{j-1} = s_j$.
Во втором случае (рис. 20.3.8): $\delta_{x_j} s_{j-1} \ne \delta_{x`_j} s_{j-1}$, $\beta_{x_j} s_{j-1} = \beta_{x`_j} s_{j-1} = y$.

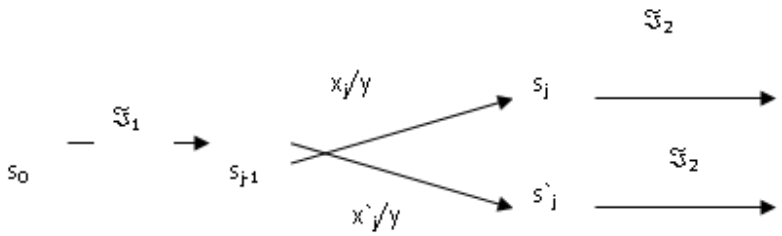

Рис. 20.3.8 справа после стрелок, возможно, нужны символы? левая стрелка не видна, посередине стрелки перекрепщиваются. Это правильно?

В третьем случае (рис. 20.3.9): $\delta_{x_j} s_{j-1} \ne \delta_{x`_j} s_{j-1}$, $\beta_{x_j} s_{j-1} = y \ne \beta_{x`_j} s_{j-1} = y`$.

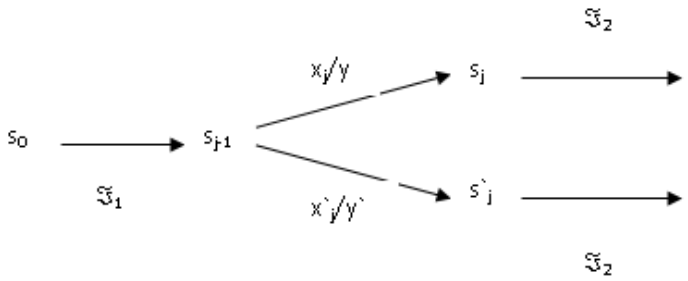

Рис. 20.3.9 справа после стрелок, возможно, посередине стрелки закрыты символами

В первом случае, очевидно, $\rho(A(s_0, \mathfrak{I}_1 x_j \mathfrak{I}_2), A(s_0, \mathfrak{I}_1 x`_j \mathfrak{I}_2)) \le 1 \le K$.

Рассмотрим оставшиеся два случая. Пусть имеет место случай 2, и предположим, что $\rho(A(s_0, \mathfrak{I}_1 x_j \mathfrak{I}_2), A(s_0, \mathfrak{I}_1 x`_j \mathfrak{I}_2)) \geq K+1$. Тогда $\rho(A(s_j, \mathfrak{I}_2), A(s`_j, \mathfrak{I}_2)) \geq K+1$. Рассмотрим номера позиций, на которых элементы последовательностей $A(s_j, \mathfrak{I}_2)$, $A(s`_j, \mathfrak{I}_2)$ различны. Пусть $y_c = \beta_x s_c$, $y`_c = \beta_x s`_c$ – К-е несовпадающие элементы в последовательностях $A(s_j, \mathfrak{I}_2)$, $A(s`_j, \mathfrak{I}_2)$. Тогда состояния s_{c+1}, $s`_{c+1}$, отвечающие (c+1)-моменту времени функционирования автомата А с состояний $s_j$, $s`_j$ при входной последовательности $\mathfrak{I}_2$, не совпадают, так как в последовательностях $A(s_j, \mathfrak{I}_2)$, $A(s`_j, \mathfrak{I}_2)$ имеется (К+1)-я позиция несовпадения их элементов.

Таким образом, доказано существование неособенного К-приемника Б-шестерки $(s_{j-1}, x_j, x`_j, y, s_j, s`_j)$, что противоречит условию 2. Итак, для случая 2 доказано неравенство $\rho(A(s_0, \mathfrak{I}_1 x_j \mathfrak{I}_2), A(s_0, \mathfrak{I}_1 x`_j \mathfrak{I}_2)) \leq K$. Это неравенство для случая 3 доказывается аналогично.

Доказательство теоремы 1. Для автомата A[s0] априори возможны два случая: 1) автомат A[s0] внутренне автономен, что равносильно тому, что множество всех Б-шестерок, и множество всех Б-семерок яляются пустыми множествами; 2) хотя бы одно из указанных множеств не является пустым, то есть автомат A[s0] не является автономным.

Предположим, что автоматное отображение A_{s0} не увеличивает метрику ρ. Если в автомате A[s0] имеется Б-семерка $(s, x, x`, y, y`, s_1, s`_1)$, то в его графе переходов имеется диаграмма следующего вида (рис. 20.3.10).

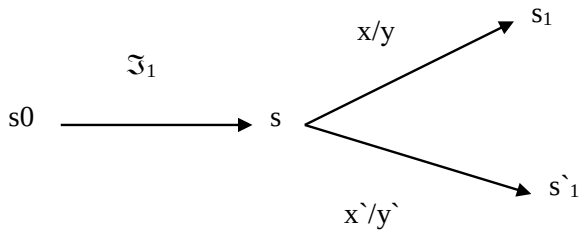

Рис. 20.3.10

Здесь $x \neq x`$, $y \neq y`$, $s_1 \neq s`_1$. Так как A[s0] – приведенный автомат, то найдется слово $\mathfrak{I}_2 \in X^*$, при котором $A(s_1, \mathfrak{I}_2) \neq A(s_2, \mathfrak{I}_2)$. Тогда

$$\rho(\mathfrak{I}_1 x \mathfrak{I}_2, \mathfrak{I}_1 x` \mathfrak{I}_2) = 1, \ \rho(A(s0, \mathfrak{I}_1 x \mathfrak{I}_2, A(s0, \mathfrak{I}_1 x` \mathfrak{I}_2)) \geq 2,$$

что противоречит предположению о том, что автоматное отображение A_{s0} не увеличивает метрику ρ. Таким образом, если автоматное отображение A_{s0} не увеличивает метрику ρ, то в автомате A[s0] отсутствуют Б-семерки.

Пусть отображение A_{s0} не увеличивает метрику ρ и автомат A[s0] не является внутренне автономным.

Предположим, что в множестве всех приемников некоторой Б-шестерки (s, x, x`, y, s_1, s_2) имеется неособый приемник, то есть в графе переходов автомата A[s0] имеется диаграмма вида (рис. 20.3.11).

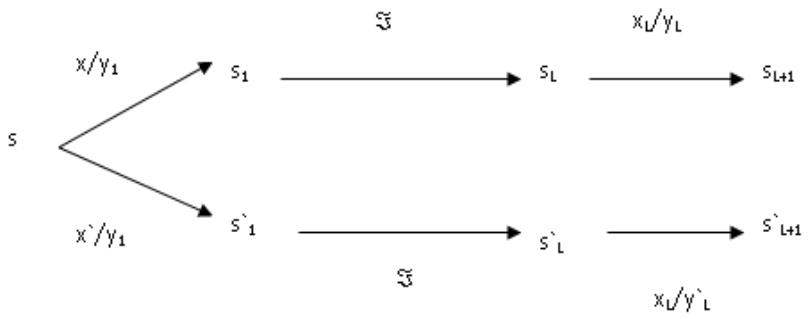

Рис. 20.3.11

Тогда $s_1 \neq s`_1$, $x \neq x`$, $\Im \in X^*$, $y_L \neq y`_L$, $s_{L+1} \neq s`_{L+1}$. Из приведенности автомата A[s0] следует существование $\Im^\wedge \in X^*$, при котором $A(s_{L+1}, \Im^\wedge) \neq A(s`_{L+1}, \Im^\wedge)$. И далее

$$\rho(x\Im x_L\Im^\wedge, x`\Im x_L\Im^\wedge) = 1, \rho(A(s, x\Im x_L\Im^\wedge), A(s, x`\Im x_L\Im^\wedge))\geq 2.$$

Следовательно, отображение A_s не является отображением, не увеличивающим ρ. Тогда, по лемме 2, и отображение A_{s0} не является отображением, не увеличивающим ρ, что противоречит начальному предположению. Таким образом, доказано, что если автомат A[s0] не является внутренне автономном, и у него отсутствуют Б-семерки, и отображение A_{s0} не увеличивает ρ, то каждый приемник любой Б-шестерки является особым.

Перейдем теперь к доказательству достаточности условий теоремы 1. Очевидно, что при внутренне автономном автомате A[s0] автоматное отображение A_{s0} не увеличивает метрику ρ.

Предположим, что A[s0] не является внутренне автономным автоматом, в нем отсутствуют Б-семерки, и каждый приемник любой

Б-шестерки – особый. Согласно лемме 1 для доказательства того, что отображение A_{s0} не увеличивает ρ, нам достаточно доказать, что выполняется импликация: из $\rho(\mathfrak{I}, \mathfrak{I}`) = 1$, $(\mathfrak{I}, \mathfrak{I}`) \in X^*$ следует $\rho(A(s0, \mathfrak{I}), A(s0, \mathfrak{I}`) \leq 1$.

Пусть $\rho(\mathfrak{I}, \mathfrak{I}`) = 1$ для некоторых $(\mathfrak{I}, \mathfrak{I}`) \in X^*$. Представим $\mathfrak{I}$, $\mathfrak{I}`$ в виде: $\mathfrak{I} = \mathfrak{I}_1 x_j \mathfrak{I}_2$, $\mathfrak{I}` = \mathfrak{I}_1 x`_j \mathfrak{I}_2$, где $x_j \neq x`_j$, $(\mathfrak{I}_1, \mathfrak{I}_2) \in \mathfrak{I}^*$. Рассмотрим пути в графе переходов автомата A[s0], отвечающие состоянию s0 и входным словам $\mathfrak{I}$, $\mathfrak{I}`$. Априори возможны лишь следующие случаи.

Случай 1 (рис. 20.3.12):

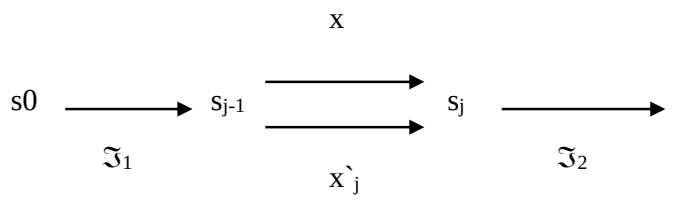

Рис. 20.3.12 справа итоговый символ?

Случай 2 (рис. 20.3.13): $s_j \neq s`_j$.

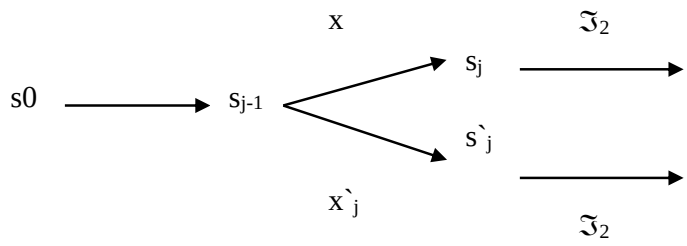

Рис. 20.3.13 - справа итоговые символы?

Случай 2 распадается на два подслучая:

а) $\beta_{x_j} s_{j-1} = \beta_{x`_j} s_{j-1}$;

б) $\beta_{x_j} s_{j-1} \neq \beta_{x`_j} s_{j-1}$.

В случае 2а, используя условие, что каждый приемник любой Б-шестерки является особым, заключаем, что

$$\rho(A(s0, \mathfrak{I}_1 x_j \mathfrak{I}_2), A(s0, \mathfrak{I}_1 x`_j \mathfrak{I}_2)) \leq 1.$$

Случай 2б невозможен, так как по условию у автомата A[s0] отсутствуют Б-семерки. Таким образом, доказана достаточность условий теоремы 1.

Напомним, что авомат $A = (X, S, Y, (\delta_x)_{x\in X}, (\beta_x)_{x\in X})$ называется перестановочным, если его частичные функции перехода $(\delta_x)_{x\in X}$ осуществляют биекции S в S.

В классе автоматных отображений выделим два подкласса: множество всех инъективных автоматных отображений X* в Y* и множество всех автоматных отображений A_s, для которых автомат A[s] является перестановочным.

Для этих подклассов автоматных отображений приведем некоторые следствия доказанных теорем 1, 2. Для автомата $A[s0] = (X, S_{s0}, Y, (\delta_x)_{x\in X}, (\beta_x)_{x\in X})$ через β_s, $s\in S$ обозначим следующее отображение X в Y: $\beta_s(x) = \beta_x(s)$, $x\in X$. Очевидно следующее утверждение.

Утверждение 1. Автоматное отображение A_{s0} инъективно тогда и только тогда, когда все отображения β_s, $s\in S_{s0}$ инъективны.

Отметим, что наличие Б-шестерки у автомата A[s0] является достаточным условием неинъективности отображения A_{s0}. Из факта утверждения 1 теоремы 1 непосредственно вытекает следствие 1.

Следствие 1. Пусть A_{s0} – инъективное отображение и A[s0] – приведенный автомат. Отображение A_{s0} не увеличивает метрику ρ тогда и только тогда, когда автомат A[s0] является внутренне автономным.

Из теоремы 1 и определения перестановочности автомата A непосредственно вытекает следствие 2.

Следствие 2. Пусть A[s0] – приведенный перестановочный автомат. Отображение A_{s0} не увеличивает метрику ρ тогда и только тогда, когда автомат A[s0] является внутренне автономным.

Из теоремы 2 несложно получить следующие следствия 3 и 4.

Следствие 3. Пусть A_{s0} – инъективное отображение и A[s0] – приведенный автомат. Отображение A_{s0} увеличивает метрику ρ не более чем в К раз (К≥2) тогда и только тогда:

либо автомат A[s0] является внутренне автономным,

либо все его К–1 приемники любой Б-семерки являются особыми.

Следствие 4. Пусть A[s0] – приведенный перестановочный автомат. Отображение A_{s0} увеличивает метрику ρ не более чем в К раз (К≥2) тогда и только тогда, когда автомат A[s0] является внутренне автономным.

Выделим тот факт, что расширение класса автоматных отображений (осуществляемых инициальными приведенными пе-

рестановочными автоматами), увеличивающих метрику ρ не более чем в один раз, *при переходе к автоматным отображениям*, увеличивающим метрику ρ строго более чем в один раз, *не происходит.*

Замечание 1. Для проверки условий теорем 1, 2 требуется проверить наличие или отсутствие в графе переходов автомата A[s0] некоторых диаграмм (фрагментов). Сложность такой проверки выражается через максимальную длину входных слов, характеризующих диаграмму. Несложно доказать, что для проверки приемника Б-шестерки на его особенность достаточно рассматривать входные слова $\Im$ (см. определение 5) длины, не превосходящей

$$M = \frac{|S|(|S|-1)}{2} - 1$$

Для проверки К-приемника Б-шестерки на его особенность достаточно рассматривать входные слова $\Im$ (см. определение 9) длины, не превосходящей КМ. Аналогично, для (К–1)-приемника Б-семерки – слова длины не более, чем (К–1)М. Получение минимальных оценок указанных слов $\Im$ представляет собой отдельную задачу. Приведенные оценки доказывают лишь конструктивность условий теорем 1, 2.

20.4. Описание множества AG((X*, Y*ε, К)

Предположим, что некоторое автоматное отображение A_{s0}: $X^* \to Y^*$ увеличивает бинарное отношение ε не более чем в К раз, то есть для любых $\Im, \Im` \in X^*$ и любого $n \in \{1, 2, \ldots, |\Im|\}$ имеется число $m \in \{1, 2, \ldots, Kn\}$ такое, что выполняется импликация

$$\Im \varepsilon^n \Im` \Rightarrow A(s0, \Im) \varepsilon^m A(s0, \Im`).$$

Так как автоматное отображение сохраняет длины слов, то из этого соотношения следует m = n. В частности, A_{s0} не размножает искажения типа пропуска букв. Обратно, если A_{s0} не размножает искажения типа пропуска букв, то, очевидно, A_{s0} увеличивает бинарное отношение ε не более чем в К раз при любом К. Таким образом, множество AG((X*, Y*ε, К) всех автоматных инъективных отображений A_s: $X^* \to Y^*$, увеличивающих бинарное отношение ε не более чем в К раз, совпадает с множеством AG((X*, Y*ε, 1). Описание последнего множества дается в следующей теореме.

Теорема 3. Инъективное автоматное отображение A_{s0} не размножает искажения типа пропуска букв тогда и только тогда, когда для автомата $A[s0] = (X, S_{s0}, Y, (\delta_x)_{x\in X}, (\beta_x)_{x\in X})$ при любом $s\in S_{s0}$ отображение β_s не зависит от выбора $s\in S_{s0}$.

Отметим, что данное утверждение видимо возможно доказать используя работы М. М. Глухова[1] по описанию инъективных отображений, не распространяющих искажения [27]. Нам представляется, что приводимое ниже теоретико-автоматное доказательство теоремы 3 также имеет право на существование и опубликование.

Приведем вспомогательные утверждения, представляющие и самостоятельный интерес. Очевидно следующее утверждение.

Утверждение 2. Инъективное отображение φ: $X^*\to Y^*$ не размножает искажения типа пропуска букв тогда и только тогда, если из $(\mathfrak{I}\varepsilon\mathfrak{I}`, \mathfrak{I}, \mathfrak{I}`)\in X^*$ следует $\varphi(\mathfrak{I})\varepsilon\varphi(\mathfrak{I}`)$.

Пусть $A[s0] = (X, S_{s0}, Y, (\delta_x)_{x\in X}, (\beta_x)_{x\in X})$ автомат, реализующий автоматное отображение A_{s0}. Ниже мы допускаем, что автомат $A[s0]$ может быть и неприведенным автоматом.

Утверждение 3. Если автоматное отображение A_{s0} не размножает искажения типа пропуска букв, то при любом $s\in S_{s0}$ автоматное отображение A_s не размножает искажения типа пропуска букв.

Пусть для $s\in S_{s0}$ автоматное отображение A_s не размножает искажения типа пропуска букв. Тогда при любых $x\in X$, $\mathfrak{I}\in X^*$, $\mathfrak{I}\neq\varnothing$ и $\mathfrak{I}`$, для которого $\mathfrak{I}\varepsilon\mathfrak{I}`$, справедливы отношения $x\mathfrak{I}\varepsilon x\mathfrak{I}`$, $A(s, x\mathfrak{I})\varepsilon A(s, x\mathfrak{I}`)$. Учитывая, что первые символы в словах $A(s, x\mathfrak{I})$, $A(s, x\mathfrak{I}`)$ равны, получаем $A(\delta_x s, \mathfrak{I})\varepsilon A(\delta_x s, \mathfrak{I}`)$, то есть (см. утверждение 2) отображение $A_{s`}$, $s` = \delta_x s$ не размножает искажения типа пропуска букв. Следовательно, при любом $s\in S_{s0}$ автоматное отображение A_s не размножает искажения типа пропуска букв.

Доказательство теоремы 3. Пусть инъективное отображение A_{s0}, не размножает искажения типа пропуска букв. Тогда (см. утверждение 3) при любом $s\in S_{s0}$ автоматное отображение A_s не размножает искажения типа пропуска букв. При этом отображение A_s инъективно (см. утверждение 1).

Покажем, что при любых *различных* $(x_1, x_2)\in X$ выходное слово $A(s, x_1x_2) = y_1y_2$ таково, что $y_1 \neq y_2$. Предположим, что $A(s, x_1x_2) = yy$.

---

[1] См. : Глухов М. М. Инъективные отображения слов, не размножающие искажений // Труды по дискретной математике. – 2001. – Т. 4 – С. 17–32.

Имеем $x_1x_2 \varepsilon x_2$, $yy \varepsilon A(s,x_2)$. Откуда получаем $A(s, x_2) = y$, что противоречит инъективности отображения A_s, так как $A(s, x_1) = y$.

Итак при любом $x \in X$, $x \neq x`$ имеем: $xx` \varepsilon x`$, $A(s, xx`) = yy`$, где $y \neq y`$. Откуда получаем $yy` \varepsilon A(s, x`)$, $A(s, x) = y$. Следовательно, $\beta_s(x`) = y`$, а из $A(s, xx`) = yy`$ имеем: $\beta_{s1}(x`) = y`$, $s1 = \delta_x s$. Поэтому $\beta_{s1}(x`) = y` = \beta_s(x`)$ для всех $x`$из X, не равных x. Так как любое отображение $A_{s`}$, $s` \in S_{s0}$ не размножает искажения типа пропуска букв, то для любых $x \in X$, $s` \in S_{s0}$ получаем

$$\beta_{s`1}(x`) = \beta_{s`}(x`), \quad s`1 = \delta_x s` \qquad (40)$$

для всех $x` \neq x$.

Покажем теперь, что эти равенства выполняются и при $x` = x$. Очевидно, для этого достаточно доказать, что

$$\beta_{s1}(x) = \beta_s(x), \; s1 = \delta_x s$$

при любом $x \in X$. Для доказательства последних равенств, в свою очередь, достаточно доказать, что при любом $x \in X$

$$A(s, xx) = yy$$

при некотором $y \in Y$, зависящим от x.

Предположим, что нашлось $x \in X$, при котором $A(s, xx) = y_1y_2$, $y_1 \neq y_2$. Тогда при некотором $x` \in X$, $\mathbf{x \neq x`}$ получаем

$$A(s, xxx`) = y_1y_2y`,$$

при некотором $y` \in Y$. Используя равенства (40) имеем

$$\beta_s(x`) = \beta_{s1}(x`) = \beta_{s2}(x`) = y`, \quad s1 = \delta_x s, \; s2 = \delta_x\delta_x s.$$

Следовательно, учитывая инъективность отображения, получаем

$$y` \neq y_1, \; y` \neq y_2.$$

Если $|Y|=2$, то получено противоречие и, следовательно, доказано, что $y_1=y_2$, то есть доказана необходимость условий теоремы 2.

Пусть $|Y| \geq 3$. Нами доказано, что элементы y_1, y_2, $y_3=y`$ различны.

Имеем

$A(s, xxx`) = y_1y_2y_3$, $\beta_s(x`) = \beta_{s1}(x`) = \beta_{s2}(x`) = y`$, $s1 = \delta_x s$, $s2 = \delta_x\delta_x s$.

Из этих равенств получаем

$$A(s, xx`) = y_1y_3,$$

$$A(s,xx`x) = y_1y_3(\beta_x\delta_{x`}\delta_x s) = y_1y_3\beta_{\delta x`\delta x s}(x) = y_1y_3\beta_{s1}(x) = y_1y_3y_2, \quad s1 = \delta_x s$$

$$A(s,x`x) = y_3(\beta_x\delta_{x`}s) = y_3\beta_{s`1}(x) = y_3\beta_s(x) = y_3y_1, \; s`1 = \delta_{x`}s.$$

Имеем $xx`x \varepsilon x`x$ и, следовательно, должно быть справедливо отношение:

$$A(s,xx`x) \varepsilon A(s,x`x),$$

но слово $A(s,xx`x)=y_1y_3y_2$ не находится в бинарном отношении ε со словом $A(s,x`x)=y_3y_1$. Полученное противоречие завершает доказательство промежуточного утверждения о том, что $y_1=y_2$, которое, как было ранее показано, достаточно для завершения доказательства необходимости условий теоремы 3. Достаточность ее условий очевидна.

Следствие 5. Если инъективное отображение A_{s0} не размножает искажения типа пропуска букв, и $A[s0]=(X,S_{so},Y,(\delta_x)_{x\in X},(\beta_x)_{x\in X})$ – приведенный автомат, то $|S_{s0}|=1$.

20.5. Описание множества AG((X*, Y*, D, К)

Обозначим через D метрику Левенштейна [34] на множестве X* (Y*); $D(\mathfrak{I},\mathfrak{I}`)$ означает минимальное число выпадений и вставок букв для получения из слова $\mathfrak{I}$ слова $\mathfrak{I}`$.

Определение 3. Отображение φ: $X^*\to Y^*$ называется отображением увеличивающим метрику D не более чем в К раз, если для любых слов $\mathfrak{I},\mathfrak{I}`\in X^*$ выполняется условие

$$KD(\mathfrak{I}, \mathfrak{I}`) \geq D(\varphi(\mathfrak{I}), \varphi(\mathfrak{I}`)).$$

Через AG((X*, Y*D, К) обозначим множество всех автоматных инъективных отображений A_s: $X^*\to Y^*$ увеличивающих метрику D не более чем в К раз.

Предположим, что некоторое автоматное отображение A_{s0}: $X^*\to Y^*$ увеличивает метрику D не более чем в К раз, то есть, для любых слов $\mathfrak{I}$, $\mathfrak{I}`\in X^*$ выполняется условие

$$KD(\mathfrak{I},\mathfrak{I}`) \geq D(A_{s0}(\mathfrak{I}), A_{s0}(\mathfrak{I}`)) \quad (**)$$

Аналогично доказательству леммы 1 доказывается

Лемма 3. Отображение φ: $X^*\to Y^*$ увеличивает метрику D не более чем в К раз тогда и только тогда, когда для любых слов $\mathfrak{I},\mathfrak{I}`\in X^*$ из условия $D(\mathfrak{I},\mathfrak{I}`) = 1$ следует $D(\varphi(\mathfrak{I}),\varphi(\mathfrak{I}`))\leq K$.

Ниже дается описание множества AG((X*,Y*D,К) для: К=1 и К=2. Случай К≥3 остается открытым.

Утверждение 4. Автоматное отображение A_{s0}: $X^*\to Y^*$ увеличивает метрику D не более чем в 1 раз тогда и только тогда, когда оно увеличивает бинарное отношение ε не более чем в 1 раз.

Доказательство. Предположим, что автоматное отображение A_{s0}: $X^*\to Y^*$ увеличивает метрику D не более чем в 1 раз. Пусть для слов $\mathfrak{I},\mathfrak{I}`$, выполняется равенство: $D(\mathfrak{I},\mathfrak{I}`)=1$, то есть: либо а) $\mathfrak{I}\varepsilon\mathfrak{I}`$,

либо б) $\mathfrak{I}`\varepsilon\mathfrak{I}$. Так как автоматное отображение сохраняет длины слов, то в случае а) $\mathfrak{I}\varepsilon\mathfrak{I}`$из неравенства $D(A_{s0}(\mathfrak{I}), A_{s0}(\mathfrak{I}`))\leq 1$ получаем $A_{s0}(\mathfrak{I})\varepsilon A_{s0}(\mathfrak{I}`)$. В случае б) получаем $A_{s0}(\mathfrak{I}`)\varepsilon A_{s0}(\mathfrak{I})\mathfrak{I}`\varepsilon\mathfrak{I}$. Следовательно (см. лемму 3), если отображение A_{s0}: $X^*\rightarrow Y^*$ увеличивает метрику D не более чем в 1 раз, то оно увеличивает бинарное отношение ε не более чем в 1 раз. Обратное утверждение очевидно.

Утверждение 5. Автоматное отображение A_{s0}: $X^*\rightarrow Y^*$ увеличивает метрику D не более чем в 2 раза тогда и только тогда, когда оно увеличивает бинарное отношение ε не более чем в 1 раз.

Доказательство. Предположим, что автоматное отображение A_{s0}: $X^*\rightarrow Y^*$ увеличивает метрику D не более чем в 2 раза. Пусть для слов $\mathfrak{I},\mathfrak{I}`$, выполняется равенство: $D(\mathfrak{I},\mathfrak{I}`)=1$, то есть либо а) $\mathfrak{I}\varepsilon\mathfrak{I}`$, либо б) $\mathfrak{I}`\varepsilon\mathfrak{I}$. Так как автоматное отображение сохраняет длины слов, то в случае а) $\mathfrak{I}\varepsilon\mathfrak{I}`$, из неравенства $D(A_{s0}(\mathfrak{I}), A_{s0}(\mathfrak{I}`))\leq 2$, получаем $A_{s0}(\mathfrak{I})\varepsilon A_{s0}(\mathfrak{I}`)$. В случае б) получаем $A_{s0}(\mathfrak{I}`)\varepsilon A_{s0}(\mathfrak{I})\mathfrak{I}`\varepsilon\mathfrak{I}$. Следовательно (см. лемму 3), если отображение A_{s0}: $X^*\rightarrow Y^*$ увеличивает метрику D не более чем в 2 раза, то оно увеличивает бинарное отношение ε не более чем в 1 раз. Обратное утверждение очевидно.

Таким образом, множества AG((X*, Y*, D, 1), AG((X*, Y*, D, 2) *совпадают с множеством автоматных инъективных отображений сохраняющих бинарное отношение ε* (см. теорему 3).

Список литературы

1. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. – 2002.

2. *Бабаш А. В.* Автоматные отображения периодических последовательностей, не размножающие искажений // Дискретная математика. – Т. 13. – Вып. 3. – 2001. – С. 42–56.

3. *Бабаш А. В.* Автоматные отображения периодических последовательностей, не размножающие искажений // Труды по дискретной математике. – Т. 5. – М. : Физматлит, 2002. – С. 7–20.

4. *Бабаш А. В.* Верхняя оценка степени различимости связных перестановочных автоматов с заданным диаметром // Комбинаторно-алгебраические методы в прикладной математике. — Горький, 1983. – С. 3–43.

5. *Бабаш А. В.* Криптографические и теоретико-автоматные аспекты современной защиты информации. – Т. 1. – М. : Евразийский открытый институт, 2008. – 414 с.

6. *Бабаш А. В.* Криптографические и теоретико-автоматные аспекты современной защиты информации. – Т. 2. – М. : Евразийский открытый институт, 2008. – 257 с.

7. *Бабаш А. В.* Локальное восстановление входных слов автоматов по начальным и заключительным состояниям // Второй Всероссийский симпозиум по прикладной и промышленной математике. – Самара, 2001. – С. 93–94.

8. *Бабаш А. В.* Многозначные гомоморфизмы конечных автоматов // Обозрение прикладной и промышленной математики. Четвертая Всероссийская школа-коллоквиум по стохастическим методам : тезисы докладов. – М. : ТВП, 1997. – С. 321–322.

9. *Бабаш А. В.* Неотличимость состояний конечного автомата относительно функции, заданной на его входных и выходных словах // Обозрение прикладной и промышленной математики : тезисы докладов Второго Всероссийского симпозиума по прикладной и промышленной математике. – Т. 8. – Вып. 1. – М. : ТВП, 2001. – С. 94–95.

10. *Бабаш А. В.* Неотличимость состояний конечного автомата относительно функции, заданной на его входных и выходных словах //Обозрение прикладной и промышленной математики : тезисы докладов Второго Всероссийского симпозиума по прикладной и промышленной математике. – Т. 15. – Вып. 3. – М., 2003. – С. 66–75.

11. *Бабаш А. В.* О восстановлении информации о входном слове перестановочного автомата Медведева по начальным и заключительным состояниям // Проблемы передачи информации. – Т. 43. – Вып. 2. – М., 2007. – С. 74–84.

12. *Бабаш А. В.* О некоторых инвариантах конечного автомата // Обозрение прикладной и промышленной математики : тезисы докладов V Международной Петрозаводской конференции. – Т. 7. – Вып. 1. – М. : ТВП, 2000. – С. 88–89.

13. *Бабаш А. В.* О свойствах специальной композиции автоматов // Труды по дискретной математике. – Т. 1. – М. : ТВП, 1997. – С. 43–66.

14. *Бабаш А. В.* Об экспериментах по распознаванию информации о входном слове автомата // Труды по дискретной математике. – Т. 8. – М. : Физматлит, 2004. – С. 7–24.

15. *Бабаш А. В.* Приближенные модели перестановочных автоматов // Дискретная математика. – Т. 9. – Вып. 1. – 1997. – С. 103–122.

16. *Бабаш А. В.* Решение автоматных уравнений с искажениями в функции переходов автомата // Обозрение прикладной и промышленной математики : тезисы докладов Пятой Всероссийской школы-коллоквиума по стохастическим методам. – Т. 5. – Вып. 2. – М. : ТВП, 1998. – С. 198–199.

17. *Бабаш А. В.* Решение автоматных уравнений с искажениями в функции переходов автомата // Проблемы передачи информации. – Т. 38. – Вып. 3. – 2002.

18. *Бабаш А. В., Глухов М. М., Шанкин Г. П.* О преобразованиях множества слов в конечном алфавите, не размножающих искажений. – Дискретная математика. – Т. 9. – Вып. 3. – 1997. – С. 3–19.

19. *Бабаш А. В., Шанкин Г. П.* Криптография. ─ М. : Солон-Р, 2002.

20. *Балакин Г. В.* Введение в теорию случайных систем уравнений // Труды по дискретной математике. – Т. 1. – М. : ТВП, 1997. – С. 1–18.

21. *Богомолов А. М., Барашко А. С., Грунский И. С.* Эксперименты с автоматами. – Киев : Наукова думка, 1973.

22. *Галлагер Р.* Теория информации и надежная связь. – М. : Советское радио, 1974.

23. *Гантмахер Ф. Р.* Теория матриц. Государственное издательство технико-теоретической литературы. – 1954.

24. *Гилл А.* Введение в теорию конечных автоматов. – М. : Наука, 1966.

25. *Гинсбург С. В.* О длине кратчайшего однородного эксперимента, устанавливающего конечные состояния машины // Кибернетический сборник. – № 3. – М. : ИЛ, 1961. – С. 167–186.

26. *Глухов М.* Инъективные отображения слов, не размножающие искажений типа пропуска букв // Дискретная математика. – Т. 11. – Вып. 2. – 1999. – С. 20–39.

27. *Глухов М. М.* Инъективные отображения слов, не размножающие искажений // Математические вопросы кибернетики. – Т. 7. – М., 1998.

28. *Глухов М. М.* О числовых параметрах, связанных с заданием конечных групп системами образующих элементов // Труды по дискретной математике. – Т. 1. – М. : ТВП, 1997. – С. 43–66.

29. *Горчинский Ю. Н.* О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями // Труды по дискретной математике. – Т. 1. – М. : ТВП, 1997. – С. 67–84.

30. *Грушо А. А., Тимонина Е. Е., Применко Э. А.* Анализ и синтез алгоритмов. – Йошкар-Ола, 2000.

31. *Ивен Ш.* Об автоматах конечного порядка без потери информации. Теория конечных и вероятностных автоматов // Труды международного симпозиума по теории релейных устройств и конечных автоматов. – М. : Наука, 1965. – С. 269–279.

32. *Кудрявцев В. Б., Алешин С. В., Подколзин А. С.* Введение в теорию автоматов. – М. : Наука, 1985.

33. *Курмит А. А.* Автоматы без потери информации конечного порядка. – Рига : Зинатне, 1972.

34. *Левенштейн В. И.* О совершенных кодах в метрике выпадений и вставок // Дискретная математика. – Т. 3. Вып. 1. – 1991. – С. 3–20.

35. *Логачев О. А., Проскурин Г. В., Ященко В. В.* Локальное обращение конечного автомата с помощью автоматов // Дискретная математика. – Т. 7. – Вып. 2. – С. 19–33.

36. *Сидельников В. М.* Быстрые алгоритмы построения набора маркировок дискретных массивов информации // Труды по дискретной математике. – Т. 1. – М. : ТВП, 1977. – С. 251–264.

37. *Строганов А. С.* Об £-моделировании поведения конечных автоматов // Материалы 1-го Всесоюзного семинара по дискретной математике и ее приложениям. – М. : Изд-во МГУ, 1986. – С. 48–56.

38. *Супруненко Д. А.* Группы матриц. – М. : Наука, 1972.

39. *Твердохлебов В. А.* Логические эксперименты с автоматами. – Саратов : Изд-во Саратовского университета, 1988.

40. *Фридман А., Менон П.* Теория и проектирование переключательных схем. – М. : Мир, 1978.

41. *Хомский М., Миллер Д.* Языки с конечным числом состояний // Кибернетический сборник. – № 4. – М. : ИЛ, 1962. – С. 233–255.

42. *Шеннон К.* Работы по теории информации и кибернетике. – М. : Иностранная литература, 1963.

43. *Even Sh.* On information-lossless automata of finite order. – IEE Trans. Electronic Comput., 14. – 1965. – P. 4, 561–569.

44. *Golic J.* Intrinsic Statistical Weakness of Key stream generators // Advances in Cryptology. – Asiacrypt 94, Lecture Notes in Computer Science, Springer. – Vol. 917. – Verlag, 1995. – P. 91–103.

45. *Hartmanis I., Stearns R. E.* Algebraic structure theory of sequential machines. – Toronto, 1966.

46. *Huffman D. A.* Canonical Forms for Information – Lossless Finite – State Logical Machines // IRE Transactions on Information Theory. – Vol. 5. – Issue 5. – 1959. – P. 4–59.

47. *Huffman D. A.* Notes on information-lossless finite-state automata. –1959. – P. 397–405.

48. *Krapez A.* On a generalization of Fermat‘s theorem in theory of groups // Inst. Math., Nouvelle Ser. – Vol. 17 (31). – 1974. – P. 77–81.

49. *Majewski W., Albicki A.* Algebraiczna theory automata. – Warszawa, 1980.

50. *Matsui M.* Linear Cryptanalysis Method for DES. – Eurocrypt, 1993. – P. 24–27.

51. *Matsui M.* On correlation between the order of S-boxes and the strength of DES. – Eurocrypt, 1994. – P. 375–387.

52. *Matsui M.* The First Experimental Cryptanalysis of the data Encryption Standard. – FSIA CRYPT`94. – P. 1–11.

53. *Menzes A., van Oorschot P., Vanstone S.* Hadbook of Applied Cryptography. – CRC Press, 1997.

54. *Riquet G.* Relations binaries, fermetures, correspondences de Galois // Bull. Sos. math. – France, 76, 1948. – (Кибернетический сборник. – № 7. – 1963).

55. *Rothaus O. S.* Asymptotic properties of group generation // Pacific J. Math. –Vol. 17. – № 2. – 1966. – P. 312–322.

56. *Simon J. M.* A note on the Memory Aspects of sequence Transducers // IRE Trans. – Vol. CT-6. – 1959. – P. 26–29.

57. *Wieland P.* H. Finite permutation grups. – New York and London : Academic Press, 1964.

58. *Zadeh L. A.* Unpublshed notes on discrete – state systems and automata. – Berkeley : University of California. – 1960.

Учебное издание

БАБАШ Александр Владимирович

ТЕОРИЯ АВТОМАТОВ.
АНАЛИЗ ШИФРУЮЩИХ АВТОМАТОВ

Учебное пособие

Редактор *Н. В. Пятосина*
Оформление обложки *Ю. С. Жигалова*

Подписано в печать __.__.2021. Формат 60x84 1/16.
Усл. печ. л. 18,5. Уч.-изд. л. 18,3. Тираж 100 экз. Заказ .

ФГБОУ ВО «РЭУ им. Г. В. Плеханова».
117997, Москва, Стремянный пер., 36.
Напечатано в ФГБОУ ВО «РЭУ им. Г. В. Плеханова».
117997, Москва, Стремянный пер., 36.

Для заметок