Math-Net.Ru

Общероссийский математический портал

А. В. Бабаш, Приближенные модели перестановочных автоматов, *Дискрет. матем.*, 1997, том 9, выпуск 1, 103–122

DOI: <https://doi.org/10.4213/dm450>

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

Параметры загрузки:

IP: 52.90.164.192

26 апреля 2023 г., 14:12:00

Приближенные модели перестановочных автоматов

© 1997 г. А. В. Бабаш

На основе метрических свойств выходных последовательностей конечных автоматов строятся приближенные модели связных перестановочных автоматов — перестановочные автоматы с меньшим числом состояний.

1. Введение

На основе расстояния Хемминга в работе указывается количественная мера близости двух инициальных автоматов — мера неотличимости, характеризующая степень несовпадения их выходных последовательностей. С использованием этой меры исследуются возможности группирования состояний связных конечных перестановочных автоматов с целью построения их приближенных моделей — автоматов с меньшим числом состояний. Таким образом, речь идет об ε -моделировании поведения конечных автоматов с использованием количественной меры близости, отличной от расстояния между о.д.-функциями, введенного в [2], однако позволяющей более точно оценить близость выходных последовательностей автоматных отображений.

Отметим, что в теории конечных автоматов наряду с задачами, относящимися к множеству всех автоматов, нередко ставятся и решаются задачи в достаточно узком классе конечных автоматов, например, в классах автономных автоматов, линейных автоматов, автоматов с конечной памятью, автоматов без потери информации, и т.п. Так, ряд теоретико-автоматных вопросов решался ранее и для класса перестановочных автоматов (см., например, [6, 7]). Необходимость изучения этого класса автоматов диктуется, в частности, тем, что функционирование некоторых узлов и блоков ряда устройств компьютерной безопасности, коммерческих систем защиты информации моделируется конечными перестановочными автоматами. Центральные результаты работы содержатся в §4, при этом предварительные результаты работы (§§2, 3) получены в классе всех конечных автоматов.

2. Основные понятия и предварительные результаты

Пусть $A = (I, S, O, (\delta_i)_{i \in I}, (\beta_i)_{i \in I})$ — конечный автомат с входным алфавитом I , множеством состояний S , выходным алфавитом O , частичными функциями

переходов $(\delta_i)_{i \in I}$, $\delta_i: S \rightarrow S$, $i \in I$, и частичными функциями выходов $(\beta_i)_{i \in I}$, $\beta_i: S \rightarrow O$, $i \in I$. Для $\kappa \subseteq S$, $\mathcal{I} = i_1, \dots, i_k$ из I^k , $s \in S$ положим

$$\delta_i \kappa = \{\delta_i s: s \in \kappa\}, \quad \delta_{\mathcal{I}} s = \delta_{i_k} \delta_{i_{k-1}} \dots \delta_{i_1} s, \quad \beta_{\mathcal{I}} s = \beta_{i_k} \delta_{i_{k-1}} \dots \delta_{i_1} s, \quad \delta_{\emptyset} s = s,$$

где $\emptyset$ — пустое множество.

Через $A_M = (I, S, (\delta_i)_{i \in I})$ обозначим автомат без выходов, соответствующий автомату A , а через $A\langle s \rangle = (I, S_s, O, (\delta_i)_{i \in I}, (\beta_i)_{i \in I})$ подавтомат автомата A , порожденный состоянием $s \in S$. Здесь для ограничений функций $(\delta_i)_{i \in I}$, $(\beta_i)_{i \in I}$, на S_s для простоты обозначений, использованы те же символы.

Автомат A будем называть перестановочным, если $(\delta_i)_{i \in I}$ — биекции S в S .

Класс инициальных автоматов с входным алфавитом I и выходным алфавитом O обозначим через $F = F(I, O)$. Инициальный автомат A'_s из F мы рассматриваем как о.д.-функцию $A'_s: I^* \rightarrow O^*$ (см. [1]), где I^* и O^* — множества всех слов конечной длины алфавита I и O , соответственно, а автомат, $A'[s] = (I, S'_s, O, (\delta'_i)_{i \in I}, (\beta'_i)_{i \in I})$ как конечный автомат с минимальным числом состояний, реализующий эту функцию. Число $|S'_s|$ (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 $\mathcal{M}$ обозначим через $E_{\mathcal{M}}$ тождественное отображение $\mathcal{M}$ в $\mathcal{M}$. Пусть $\bar{A} = (I, \bar{S}, O, (\bar{\delta}_i)_{i \in I}, (\bar{\beta}_i)_{i \in I})$ — еще один произвольный автомат. Гомоморфизм автомата A в $\bar{A}$ вида (E_I, φ, E_O) будем называть гомоморфизмом по состояниям A в $\bar{A}$. Конгруэнцию автомата A вида (P_{E_I}, P_S, P_{E_O}) , где P_{E_I} , P_{E_O} — одноэлементные разбиения множеств I , O , соответственно, будем называть конгруэнцией по состояниям автомата A . Таким образом, конгруэнция по состояниям автомата A это разбиение S (бинарное отношение эквивалентности на S) со свойством подстановки (см., например, [1]).

Пусть $P_I = (p(i))_{i \in I}$ — некоторое вероятностное распределение на I . Для инициальных автоматов A_s , $\bar{A}_{\bar{s}}$, $s \in S$, $\bar{s} \in \bar{S}$ (состояний s , $\bar{s}$ автоматов A , $\bar{A}$) определим величину

$$\mu_N^{s, \bar{s}} = \mu_N(A_s, \bar{A}_{\bar{s}}) = \frac{1}{N} \sum_{\mathcal{I} \in I^N} P(\mathcal{I}) \rho_N(A(s, \mathcal{I}), \bar{A}(\bar{s}, \mathcal{I})),$$

где для $\mathcal{I} = i_1, \dots, i_N$ положено $p(\mathcal{I}) = p(i_1) \dots p(i_N)$, $\rho_N(A(s, \mathcal{I}), \bar{A}(\bar{s}, \mathcal{I}))$ — расстояние Хемминга между начальными отрезками длины N выходных последовательностей $A(s, \mathcal{I})$, $\bar{A}(\bar{s}, \mathcal{I})$ автоматов A , $\bar{A}$, полученных при начальных состояниях $s \in S$, $\bar{s} \in \bar{S}$ и входной последовательности $\mathcal{I}$. Качественный смысл введенной величины состоит в том, что она характеризует среднее значение числа несовпадений соответствующих элементов выходных последовательностей автоматов A_s , $\bar{A}_{\bar{s}}$, в частности, при равномерном вероятностном распределении на I , данную величину можно трактовать как плотность несовпадения их выходных последовательностей.

Основная задача, решаемая в данной работе, 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 $(\mu_N^{s,\bar{s}})_{(s,\bar{s}) \in S \times \bar{S}}$ при $N \rightarrow \infty$ и равномерном вероятностном распределении P_I .

Положим

$$\bar{\mu}_N = (\mu_N^{s,\bar{s}})_{(s,\bar{s}) \in S \times \bar{S}}.$$

Изучим поведение вектора $\bar{\mu}_N$ при $N \rightarrow \infty$. Пусть $r^{(s,\bar{s},j)}$ — вероятность события $\beta_{\mathcal{I}} s \neq \beta_{\bar{\mathcal{I}}} \bar{s}$ при случайном выборе $\mathcal{I}$ из I^j . Несложно доказывается следующее утверждение.

Предложение 1. *Справедливо равенство*

$$\bar{\mu}_N^{s,\bar{s}} = \frac{1}{N} \sum_{j=1}^N r^{(s,\bar{s},j)}.$$

Для формулировки и доказательства основных результатов работы введем дополнительные обозначения.

Пусть ${}^1A, {}^2A$ — вероятностные автоматы Мили

$$c_A = (I, {}^cS, O, {}^c\delta^*, {}^c\beta^*, P_I), \quad c = 1, 2,$$

где ${}^c\delta^* = ({}^c\delta_i^*)_{i \in I}$ — семейство матриц вероятностей перехода. Элемент матрицы ${}^c\delta_i^*$ с номером $({}^c_{s_1}, {}^c_{s_2})$ есть вероятность перехода состояния ${}^c_{s_1}$ в ${}^c_{s_2}$ при входном символе $i \in I$ автомата cA , ${}^c\beta^* = ({}^c\beta_i^*)_{i \in I}$ — семейство матриц вероятностей выхода. Элемент матрицы ${}^c\beta_i^*$ с номером $({}^c_s, y)$ есть вероятность получения выходного символа $y \in O$ в состоянии c_s в автомате cA при входном символе $i \in I$, $c = 1, 2$; $P_I = (p_i)_{i \in I}$ — распределение вероятностей на входном алфавите автомата cA . Указанные распределения и вводимые ниже распределения мы рассматриваем как стохастические векторы.

Определим вспомогательный вероятностный автомат

$$\mathfrak{A} = \mathfrak{A}({}^1A, {}^2A) = (I, {}^1S \times {}^2S, O \times O, \delta^{\mathfrak{A}}, \beta^{\mathfrak{A}}, P_I)$$

как параллельное соединение автоматов ${}^1A, {}^2A$ при едином входе. Здесь $\delta^{\mathfrak{A}} = (\delta_i^{\mathfrak{A}})_{i \in I}$, $\delta_i^{\mathfrak{A}}$ — матрица переходных вероятностей автомата $\mathfrak{A}$ при входном символе $i \in I$. Она представима в виде тензорного произведения матриц ${}^1\delta_i^*, {}^2\delta_i^*$: $\delta_i^{\mathfrak{A}} = {}^1\delta_i \times {}^2\delta_i$; аналогично, $\beta^{\mathfrak{A}} = (\beta_i^{\mathfrak{A}})_{i \in I}$, $\beta_i^{\mathfrak{A}} = {}^1\beta_i^* \times {}^2\beta_i^*$. Положим

$$S_{\mathfrak{A}} = {}^1S \times {}^2S, \quad U = U({}^1A, {}^2A) = \sum_{i \in I} p_i \delta_i^{\mathfrak{A}}.$$

Матрица U определяет вероятности перехода одних состояний автомата $\mathfrak{A}$ в другие при подаче на вход автомата $\mathfrak{A}$ случайного входного символа с распределением P_I . Пусть $r^{s,j}$ — вероятность несовпадения выходных символов автоматов 1A и 2A на j -м такте работы автомата $\mathfrak{A}$ при начальном состоянии $s \in S_{\mathfrak{A}}$, а $R(j) = (r^{s,j})_{s \in S_{\mathfrak{A}}}$ — 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 $S_{\mathfrak{A}} = {}^1S \times {}^2S$, аналогично кодируются номера компонент рассматриваемых вектор-столбцов.

Следующее утверждение непосредственно вытекает из результатов работы [3].

Предложение 2. *Существует предел*

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{j=1}^N R(j) = \tilde{R}, \quad \tilde{R} = \frac{1}{h} (E + U + \dots + U^{h-1}) (U^h)^\infty R(1),$$

где h — период однородной цепи Маркова, определяемой матрицей U , E — единичная матрица,

$$(U^h)^\infty = \lim_{k \rightarrow \infty} U^{kh}.$$

Ниже мы будем рассматривать лишь частный случай детерминированных автоматов ${}^1A = A$, ${}^2A = \bar{A}$ с вероятностным распределением $P_I = (p(i))_{i \in I}$, $p(i) > 0$, $i \in I$. При этом обозначение $\mathfrak{A}(A, \bar{A})$ будет использовано как для обозначения вероятностного автомата, когда используется распределение P_I , так и для обозначения параллельного соединения автоматов A , $\bar{A}$ при едином входе. Для этого частного случая из предложений 1 и 2 непосредственно вытекает следующее утверждение.

Следствие 1. *Последовательность $\bar{\mu}_1, \bar{\mu}_2, \dots$, имеет предел*

$$\lim_{N \rightarrow \infty} \bar{\mu}_N = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{j=1}^N R(j) = \bar{\mu} = (\mu^{s, \bar{s}})_{(s, \bar{s}) \in S \times \bar{S}},$$

$$\bar{\mu} = \tilde{U} R(1) = \frac{1}{h} (E + U + \dots + U^{h-1}) (U^h)^\infty R(1),$$

где U — матрица переходных вероятностей цепи Маркова, моделирующая внутреннее функционирование параллельного соединения $\mathfrak{A}(A, \bar{A})$ автоматов A и $\bar{A}$ при едином случайном входе, $R(1) = (r^{s, \bar{s}, 1})_{(s, \bar{s}) \in S \times \bar{S}}$.

Для автоматов A , $\bar{A}$ представляет интерес нахождение условий, при которых последовательность векторов $\bar{\mu}_N$ сходится на конечном шаге, то есть найдется натуральное число $N_0 > 0$, при котором

$$\bar{\mu}_{N_0} = \bar{\mu}_{N_0+j}$$

для любого $j = 0, 1, \dots$.

Теорема 1. *Пусть H — произвольное натуральное число. Натуральное число $N_0 > 0$, при котором*

$$\bar{\mu}_{N_0 H} = \bar{\mu}_{(N_0+j)H}, \quad j = 0, 1, \dots,$$

существует тогда и только тогда, когда минимальный аннулирующий многочлен вектора $R(1)$ относительно матрицы U делит многочлен

$$(x^{H-1} + x^{H-2} + \dots + x + 1)^2 (x - 1).$$

Доказательство. Пусть нашлось N_0 , при котором

$$\bar{\mu}_{N_0 H} = \bar{\mu}_{(N_0+j)H}, \quad j = 0, 1, \dots$$

Используя равенство

$$\mu_N = \frac{1}{N} \sum_{k=1}^N R(k),$$

получаем, что для любого $j = 0, 1, \dots$

$$\frac{j}{N_0} \sum_{k=1}^{N_0 H} R(k) = \sum_{k=N_0 H+1}^{(N_0+j)H} R(k).$$

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

$$(x^{H-1} + x^{H-2} + \dots + x + 1) \left(\frac{1}{N_0} (x^{(N_0-1)H} + x^{(N_0-2)H} + \dots + x^H + 1) - x^{N_0 H} \right),$$

$$(x^{H-1} + x^{H-2} + \dots + x + 1) x^{N_0 H} (x^H - 1).$$

Заметим, что $x \nmid f(x)$, так как ноль не является корнем первого многочлена. Следовательно,

$$f(x) \mid (x^{H-1} + x^{H-2} + \dots + x + 1)(x^H - 1).$$

Предположим теперь, что это условие выполнено. Тогда

$$\sum_{k=1}^H R(k) = \sum_{k=H+1}^{2H} R(k),$$

откуда получаем, что $\bar{\mu}_H = \bar{\mu}_{jH}$ при любом $j = 1, 2, \dots$

Следствие 2. Последовательность $(\bar{\mu}_N)_{N=1,2,\dots}$ сходится на конечном шаге тогда и только тогда, когда $UR(1) = R(1)$.

Отметим, что для введенной функции μ на $F \times F$ выполняются следующие метрические свойства:

$$\mu(A_s, \bar{A}_{\bar{s}}) = \mu(\bar{A}_{\bar{s}}, A_s), \quad \mu(A_s, \bar{A}_{\bar{s}}) + \mu(\bar{A}_{\bar{s}}, \tilde{A}_{\tilde{s}}) \geq \mu(S_s, \tilde{A}_{\tilde{s}}), \quad \mu(A_s, A_s) = 0$$

для любых инициальных автоматов $A_s, \bar{A}_{\bar{s}}, \tilde{A}_{\tilde{s}}$ из класса F .

Определение 1. Функцию μ на $F \times F$ назовем мерой неотличимости, а ее значение $\mu(A_s, \bar{A}_{\bar{s}})$ ($\mu^{s, \bar{s}}$) назовем мерой неотличимости инициальных автоматов $A_s, \bar{A}_{\bar{s}}$ из F (состояний $s, \bar{s}$ автоматов $A, \bar{A}$).

Определение 2. Инициальный автомат $\bar{A}_{\bar{s}}$ из F (состояние $\bar{s}$ автомата $\bar{A}$) назовем $\mu\varepsilon$ -неотличимым от A_s (от состояния s автомата A), если $\mu(A_s, \bar{A}_{\bar{s}}) = \varepsilon$ ($\mu^{s, \bar{s}} = \varepsilon$). В этом случае будем говорить также, что $A_s, \bar{A}_{\bar{s}}$ (состояния $s, \bar{s}$) $\mu\varepsilon$ -неотличимы.

Прямое использование приведенных свойств функции μ на $F \times F$ позволяет утверждать, что бинарное отношение $\mu 0$ -неотличимости на F является отношением эквивалентности на F , в связи с чем обозначим через $F/\mu 0$ множество классов μ -неотличимых инициальных автоматов из F . С использованием введенных понятий и известных фактов теории цепей Маркова несложно доказываются следующие утверждения.

Предложение 3. Мера неотличимости μ является метрикой на $F/\mu 0$, в частности, μ — метрика на множестве всех инициальных перестановочных автоматов из F .

Предложение 4. Значение функции μ постоянно на каждом классе существенных состояний цепи Маркова, определенной для вспомогательного вероятностного автомата $\mathfrak{A}(A, \bar{A})$.

Предложение 5. Свойство $\mu^{s, \bar{s}} = 0$ не зависит от выбора вероятностного распределения $P_I = (p(i)_{i \in I})$, $p(i) > 0$, $i \in I$.

Для автоматов $A[s], \bar{A}[\bar{s}]$ рассмотрим вспомогательный вероятностный автомат $\mathfrak{A} = \mathfrak{A}(A[s], \bar{A}[\bar{s}])$. Пусть $V_1, \dots, V_r$ — классы существенных состояний цепи Маркова для автомата $\mathfrak{A}[s, \bar{s}]$ с матрицей переходных вероятностей U , а $P(V_j)$ — предельная вероятность перехода состояния $(s, \bar{s})$ в V_j , $j = 1, \dots, r$, получаемая с помощью элементов матрицы $\tilde{U}$ укрупнением состояний рассматриваемой цепи. Пусть $\mu(V_j)$ — значение функции μ на состояниях из V_j , $j = 1, \dots, r$.

Предложение 6. Справедливо равенство

$$\mu^{s, \bar{s}} = \sum_{j=1}^r P(V_j) \mu(V_j).$$

Доказательство. Из определения функции μ легко получить равенство

$$\mu^{s, \bar{s}} = \sum_{i \in I} p(i) \mu^{\delta_i s, \delta_i \bar{s}},$$

с помощью которого несложно доказывается требуемое утверждение.

Замечание 1. Точный подсчет компонент вектора $\bar{\mu}$ для автоматов $A, \bar{A}$ значительно облегчается в случае, когда матрица U , отвечающая вспомогательному автомату $\mathfrak{A}(A, \bar{A})$, является неразложимой и дважды стохастической, так как в этом случае матрица

$$\tilde{U} = \frac{1}{h}(E + U + \dots + U^{h-1})(U^h)^\infty$$

является равновероятной матрицей.

Следующая теорема дает критерий μ_0 -неотличимости состояний $s, \bar{s}$ автоматов $A, \bar{A}$.

Теорема 2. Пусть $A\langle s \rangle, \bar{A}\langle \bar{s} \rangle$ — приведенные автоматы и $A_1, \dots, A_k, \bar{A}_1, \dots, \bar{A}_{\bar{k}}$, соответственно, — все их минимальные подавтоматы. Равенство $\mu^{s, \bar{s}} = 0$ выполняется тогда и только тогда, когда $k = \bar{k}$ и найдется подстановка

$$\begin{pmatrix} 1, & 2, & \dots & k \\ j_1, & j_2, & \dots & j_k \end{pmatrix}$$

при которой каждый минимальный подавтомат

$$A_c = (I, S_c, O, (\delta_i)_{i \in I}, (\beta_i)_{i \in I})$$

изоморфен по состояниям автомату

$$\bar{A}_{j_c} = (I, \bar{S}_{j_c}, O, (\bar{\delta}_i)_{i \in I}, (\bar{\beta}_i)_{i \in I})$$

при некотором изоморфизме (E_I, φ_c, E_0) , $c = 1, \dots, k$. При этом для любого фиксированного $\tilde{\mathcal{I}} \in I^* \cup \emptyset$ найдется $\mathcal{I} \in I^* \cup \emptyset$, при котором

$$(\delta_{\mathcal{I}} \delta_{\tilde{\mathcal{I}}} s, \bar{\delta}_{\mathcal{I}} \bar{\delta}_{\tilde{\mathcal{I}}} \bar{s}) \in \{(s_c, \varphi_c s_c) : s_c \in S_c, c = 1, \dots, k\}.$$

Доказательство. Для автоматов $A\langle s \rangle, \bar{A}\langle \bar{s} \rangle$ рассмотрим вероятностный автомат $\mathfrak{A}(A\langle s \rangle, \bar{A}\langle \bar{s} \rangle)$ и соответствующую ему матрицу переходных вероятностей U однородной цепи Маркова. Матрица $\tilde{U}$ в общем случае (см. [3]) может быть представлена в виде

$$\tilde{U} = \begin{pmatrix} \tilde{U}_1 & \dots & & \\ & \ddots & & \\ & & \tilde{U}_r & \\ \tilde{W} & \dots & & 0 \end{pmatrix},$$

где r — число классов существенных состояний цепи Маркова.

Назовем класс существенных состояний S^j , $j = 1, \dots, r$, рассматриваемой цепи Маркова достижимым из $(s, \bar{s})$, если существует $\mathcal{I} \in I^*$, при котором $(\delta_{\mathcal{I}} s, \bar{\delta}_{\mathcal{I}} \bar{s}) \in S^j$. Пусть $S^1, S^2, \dots, S^t$ — все достижимые из $(s, \bar{s})$ классы существенных состояний. Отметим следующие свойства таких классов.

(1) Для любого $j = 1, \dots, t$

$$\text{Pr}_1 S^j \in \{S_c\}_{c=1, \dots, k}, \quad \text{Pr}_2 S^j \in \{\bar{S}_{\bar{c}}\}_{\bar{c}=1, \dots, \bar{k}}.$$

(2) При любых $c = 1, \dots, k$, $\bar{c} = 1, \dots, \bar{k}$ найдутся $j \in \{1, \dots, t\}$, $\bar{j} \in \{1, \dots, \bar{t}\}$, при которых

$$\text{Pr}_1 S^j = S_c, \quad \text{Pr}_2 S^{\bar{j}} = \bar{S}_{\bar{c}}.$$

По следствию 1

$$\bar{\mu} = (\mu^{s', \bar{s}'}_{(s', \bar{s}') \in S_s \times \bar{S}_{\bar{s}}}) = \tilde{U} R(1).$$

Вектор-столбец $R(1)$ представляется в виде

$$R(1) = (R_1(1), \dots, R_r(1), R_{r+1}(1)),$$

где нумерация вектор-столбца $R_j(1)$, $j = 1, \dots, r$, отвечает нумерации состояний в классе S^j существенных состояний рассматриваемой цепи Маркова.

Предположим, что $\mu^{s, \bar{s}} = 0$. Тогда, по предложению 6, для любого состояния $(s', \bar{s}')$, принадлежащего достижимому из $(s, \bar{s})$ классу существенных состояний, справедливо равенство $\mu^{s', \bar{s}'} = 0$. Учитывая приведенное выше равенство для μ , вид матрицы $\tilde{U}$ и то, что матрицы $\tilde{U}_j$, $j = 1, \dots, r$, положительны (см. [3]), заключаем, что

$$R_j(1) = 0, \quad j = 1, \dots, t,$$

то есть компоненты этих векторов равны нулю. Последнее равносильно тому, что при любом $j = 1, \dots, t$ для каждого состояния $(s', \bar{s}') \in S^j$ инициальные автоматы $A_{s'}$, $\bar{A}_{\bar{s}'}$ равны (состояния s' , $\bar{s}'$ автоматов $A\langle s \rangle$, $\bar{A}\langle \bar{s} \rangle$ неотличимы). Справедливость необходимости условий данной теоремы вытекает теперь из указанных выше свойств 1, 2 и приведенности автоматов $A\langle s \rangle$, $\bar{A}\langle \bar{s} \rangle$.

Докажем теперь достаточность условий теоремы 2. При выполнении условий теоремы справедливы равенства

$$R_j(1) = 0, \quad j = 1, \dots, t, \quad t = k = \bar{k},$$

то есть $r^{s', \bar{s}', 1} = 0$ при любом состоянии $(s', \bar{s}')$ из класса существенных состояний цепи Маркова, отвечающей матрице U , достижимого из $(s, \bar{s})$. В то же время очевидно, что элемент матрицы $\tilde{U}$, стоящий на пересечении строки с номером, соответствующим состоянию $(s, \bar{s})$, и столбца с номером, соответствующим состоянию $(s', \bar{s}')$, не равен нулю тогда и только тогда, когда $(s', \bar{s}')$ принадлежит одному из классов S^j , $j = 1, \dots, t$. В связи с чем, используя приведенное в следствии 1 равенство для μ , видим, что $\mu^{s, \bar{s}} = 0$. Утверждение теоремы полностью доказано.

3. Вычисление меры неотличимости состояний по кратному эксперименту с автоматами

Пусть P_I — распределение вероятностей на I ;

$$A = (I, S, O, (\delta_i)_{i \in I}, (\beta_i)_{i \in I}), \quad \bar{A} = (I, \bar{S}, O, (\bar{\delta}_i)_{i \in I}, (\bar{\beta}_i)_{i \in I})$$

— конечные автоматы. Используем для автоматов A , $\bar{A}$ введенные ранее (см. следствие 1) обозначения $\bar{\mu}$, U , $R(1)$, h . Дополнительно положим

$$M = (m_{s, \bar{s}}^1) = U^h, \quad M^c = (m_{s, \bar{s}}^c), \quad c = 0, 1, \dots$$

Минимальный аннулирующий многочлен вектора

$$\tilde{R} = \frac{1}{h}(E + U + U^2 + \dots + U^{h-1})R(1)$$

матрицы M (либо минимальный или характеристический многочлен матрицы M) запишем в виде

$$f(x) = x^k + p_1 x^{k-1} + \dots + p_{k-1} x + p_k, \quad k \leq |S \times \bar{S}|.$$

Ясно, что

$$M^k \tilde{R} + p_1 M^{k-1} \tilde{R} + \dots + p_{k-1} M \tilde{R} + p_k \tilde{R} = 0.$$

Положим

$$M^c \tilde{R} = (r_{s,\bar{s}}^c)_{(s,\bar{s}) \in S \times \bar{S}}.$$

Стандартными приемами (см., например, [2, 8]) получаем, что $\mu^{s,\bar{s}} = 0$, если $1 + p_1 + \dots + p_k \neq 0$ и

$$\mu^{s,\bar{s}} = \frac{r_{s,\bar{s}}^0(1 + p_1 + \dots + p_{k-1}) + \dots + r_{s,\bar{s}}^{k-2}(1 + p_1) + r_{s,\bar{s}}^{k-1}}{(1 + p_1 + \dots + p_{k-1}) + \dots + (1 + p_1) + 1}$$

в противном случае.

Используя введенные ранее обозначения, находим, что

$$r_{s,\bar{s}}^c = \frac{1}{h} (r^{(s,\bar{s},hc+1)} + r^{(s,\bar{s},hc+2)} + \dots + r^{(s,\bar{s},hc+h)}).$$

Таким образом, для вычисления значения $\mu^{s,\bar{s}}$ меры μ на состояниях $s, \bar{s}$ автоматов $A, \bar{A}$ достаточно построить их параллельное соединение $\mathfrak{A}(A, \bar{A})$ при едином входе и соответствующую матрицу переходных вероятностей U , найти многочлен $f(x)$ и по кратному эксперименту длины hk с автоматом $\mathfrak{A}(A, \bar{A})$ при начальном состоянии $(s, \bar{s})$, с учетом распределения P_I на I , вычислить значения вероятностей несовпадения выходных знаков $r^{s,\bar{s},j}$ при $j = 1, \dots, hk$.

4. Приближенные модели связных перестановочных автоматов

В данном параграфе используется мера неотличимости $\mu(A_s, \bar{A}_{\bar{s}})$ инициальных автоматов $A_s, \bar{A}_{\bar{s}}$ из класса $F(I, O)$ при равномерном вероятностном распределении P_I на I .

Пусть F_p — класс всех связных перестановочных автоматов с входным алфавитом I , выходным алфавитом O .

Определение 3. Автомат $\bar{A} = (I, \bar{S}, O, (\bar{\delta}_i)_{i \in I}, (\bar{\beta}_i)_{i \in I})$ из F_p называется $\mu\varepsilon$ -неотличимым от автомата $A = (I, S, O, (\delta_i)_{i \in I}, (\beta_i)_{i \in I})$ из F_p , если для любого состояния $s \in S$ найдется состояние $\bar{s} \in \bar{S}$, при котором $s, \bar{s}$ $\mu\varepsilon$ -неотличимы, и для любого состояния $\bar{s}'$ из $\bar{S}$ найдется $s' \in S$, при котором состояния $\bar{s}' s'$ $\mu\varepsilon$ -неотличимы. Автомат $\bar{A}$ с минимальным числом состояний, $\mu\varepsilon$ -неотличимый от автомата A , называется минимальным $\mu\varepsilon$ -неотличимым от A автоматом.

Очевидно, что минимальный $\mu\varepsilon$ -неотличимый от A автомат является приведенным автоматом, а любой приведенный связный перестановочный автомат A сам является минимальным $\mu 0$ -неотличимым автоматом от A .

Для автомата $A = (I, S, O, (\delta_i)_{i \in I}, (\beta_i)_{i \in I})$, $|S| > 1$, из F_p обозначим через $F_p(A)$ множество всех автоматов из F_p с числом состояний меньшим $|S|$.

Определение 4. Минимальный $\mu\varepsilon$ -неотличимый автомат $\bar{A}$ от автомата $A = (I, S, O, (\delta_i)_{i \in I}, (\beta_i)_{i \in I})$ называется наилучшим приближенным автоматом к A (в классе $F_p(A)$), если $\bar{A} \in F_p(A)$ и при любом $\varepsilon' < \varepsilon$ не существует автоматов A' из $F_p(A)$, $\mu\varepsilon'$ -неотличимых от автомата A .

Аналогично вводится понятие наихудшего приближенного автомата $\bar{A}$ к A (в классе $F_p(A)$). Отличие состоит лишь в том, что при любом $\varepsilon' > \varepsilon$ не существует автоматов A' из $F_p(A)$ $\mu\varepsilon'$ -неотличимых от автомата A .

Множество всех перестановочных инициальных автоматов с входным алфавитом I и выходным алфавитом O обозначим через $F_{p,i} = F_{p,i}(I, O)$.

Автомат $\bar{A}_{\bar{s}}$ из $F_{p,i}$ с минимальным числом состояний, $\mu\varepsilon$ -неотличимый от A_s из $F_{p,i}$, назовем минимальным $\mu\varepsilon$ -неотличимым автоматом от A_s .

Для автомата A_s из $F_{p,i}$ определим множество $F_{p,i}(A_s)$ всех автоматов $\bar{A}_{\bar{s}}$ из $F_{p,i}$, для которых $|S_s| > |\bar{S}_{\bar{s}}|$.

Определение 5. Минимальный $\mu\varepsilon$ -неотличимый автомат $\bar{A}_{\bar{s}}$ от A_s называется наилучшим приближенным автоматом к A_s (в классе $F_{p,i}(A_s)$), если $\bar{A}_{\bar{s}} \in F_{p,i}(A_s)$ и при любом $\varepsilon' < \varepsilon$ не существует автоматов A'_s из $F_{p,i}(A_s)$ $\mu\varepsilon'$ -неотличимых от автомата A_s .

Аналогично вводится понятие наихудшего приближенного автомата $\bar{A}_s$ к A_s (в классе $F_{p,i}(A_s)$). Отличие состоит лишь в том, что при любом $\varepsilon' > \varepsilon$ не существует автоматов A'_s из $F_{p,i}(A_s)$, $\mu\varepsilon'$ -неотличимых от автомата A .

Предложение 7. Перестановочный связный автомат $\bar{A} = (I, \bar{S}, O, (\bar{\delta}_i)_{i \in I}, (\bar{\beta}_i)_{i \in I})$ является наилучшим (наихудшим) приближенным автоматом к связному приведенному перестановочному автомату $A = (I, S, O, (\delta_i)_{i \in I}, (\beta_i)_{i \in I})$ (в классе $F_p(A)$) тогда и только тогда, когда для любого состояния $s \in S$ найдется состояние $\bar{s} \in \bar{S}$, при котором инициальный автомат $\bar{A}_{\bar{s}}$ является наилучшим (наихудшим) приближенным автоматом к инициальному автомату A_s (в классе $F_{p,i}(A_s)$).

Доказательство. Данное утверждение непосредственно вытекает из введенных определений и ранее установленных фактов для связных перестановочных автоматов $A, \bar{A}$: $A\langle s \rangle = A$, $\bar{A}\langle \bar{s} \rangle = \bar{A}$ при любых $s \in S$, $\bar{s} \in \bar{S}$; $\mu^{s, \bar{s}} = \mu^{\delta_i s, \bar{\delta}_i \bar{s}}$ при любом $i \in I$.

Основная задача, решаемая в данном параграфе, состоит в нахождении наилучших (наихудших) приближенных перестановочных инициальных автоматов $\bar{A}_{\bar{s}}$ к заданному перестановочному инициальному автомату A_s (в классе $F_{p,i}(A_s)$).

Отметим, что, в связи с предложением 7, данная задача адекватна описанию наилучших (наихудших) приближенных связных перестановочных автоматов к заданному приведенному связному перестановочному автомату A (в классе $F_p(A)$).

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

$$\bigcup_{j=1}^L \kappa_j = S,$$

множества S , удовлетворяющее следующим условиям:

- (1) $1 < L < |S|$;
- (2) $\kappa_j \neq \kappa_{j'}$ для $j \neq j'$, $j, j' = 1, \dots, L$;
- (3) для любых $g \in G$ и $j \in \{1, \dots, L\}$ найдется $j' \in \{1, \dots, L\}$, для которого $g\kappa_j = \kappa_{j'}$;
- (4) для любых $j, j' \in \{1, \dots, L\}$ найдется $g \in G$, для которого $g\kappa_j = \kappa_{j'}$;
- (5) найдется $j \in \{1, \dots, L\}$, при котором группа подстановок H_{κ_j} множества κ_j , являющаяся ограничением на κ_j стабилизатора G_{κ_j} множества κ_j , является транзитивной группой.

Тогда данное покрытие называется системой слабой импримитивности группы G (κ_j — блок системы, $j = 1, \dots, L$), а группа G слабо импримитивной. Если такого покрытия не существует, то группа G называется сильно примитивной.

Система слабой импримитивности группы G

$$\bigcup_{j=1}^L \kappa_j = S,$$

при дополнительном условии $\kappa_j \cap \kappa_{j'} = \emptyset$ для $j \neq j'$, $j, j' = 1, \dots, L$, является системой импримитивности группы G (см., например, [4]). В связи с этим, импримитивная группа подстановок является и слабо импримитивной.

Предложение 8. Транзитивная группа подстановок (G, S) является слабо импримитивной тогда и только тогда, когда существует интранзитивная подгруппа H' группы G индекса $|G : H'| < |S|$.

Доказательство проведем с помощью следующей леммы.

Лемма 1. Орбите κ интранзитивной подгруппы H транзитивной группы (G, S) , для которой $|G : G_\kappa| = L$, $L < |S|$, соответствует система слабой импримитивности группы G

$$\bigcup_{j=1}^L g_j \kappa = S,$$

где $g_1 = e$ (e — единица G),

$$G = \bigcup_{j=1}^L g_j G_\kappa,$$

есть разложение G в левые смежные классы по подгруппе G_κ .

Системе слабой импримитивности

$$\bigcup_{j=1}^L \kappa_j = S$$

группы (G, S) соответствует некоторая орбита $\kappa \in \{\kappa_1, \kappa_2, \dots, \kappa_L\}$ некоторой интранзитивной подгруппы H группы (G, S) , для которой $|G : G_\kappa| = L$. При этом

$$\{\kappa_1, \kappa_2, \dots, \kappa_L\} = \{g_1 \kappa, g_2 \kappa, \dots, g_L \kappa\}, \quad G = \bigcup_{j=1}^L g_j G_\kappa.$$

Доказательство. Пусть κ — орбита интранзитивной подгруппы H транзитивной группы (G, S) , для которой $|G : G_\kappa| = L$, $L < |S|$. Рассмотрим разбиение группы G на левые смежные классы по подгруппе G_κ

$$G = \bigcup_{j=1}^L g_j G_\kappa, \quad |G : G_\kappa| = L, \quad g_1 = e,$$

и для $s \in \kappa$ положим $\kappa_j = g_j G_\kappa s$. Так как группа G транзитивна,

$$\bigcup_{j=1}^L \kappa_j = S.$$

Покажем, что данное покрытие множества S является системой слабой импримитивности группы G . Очевидно, что $G_\kappa \neq G$, то есть $1 < L$, и $L < |S|$; $\kappa_j \neq \kappa_{j'}$ для $j \neq j'$, $j, j' = 1, \dots, L$; для любых $g \in G$ и $j \in \{1, \dots, L\}$ найдется $j' \in \{1, \dots, L\}$, для которого $g\kappa_j = \kappa_{j'}$; для любых $j, j' \in \{1, \dots, L\}$ найдется $g \in G$, для которого $g\kappa_j = \kappa_{j'}$; группа подстановок H_{κ_1} множества $\kappa_1 = \kappa$, являющаяся ограничением на κ стабилизатора G_κ множества κ , является транзитивной группой. Следовательно,

$$\bigcup_{j=1}^L \kappa_j = S,$$

является системой слабой импримитивности группы G .

Докажем обратное утверждение. Пусть

$$\bigcup_{j=1}^L \kappa_j = S,$$

есть система слабой импримитивности группы (G, S) и группа подстановок множества $\kappa_{j'} = \kappa$, являющаяся ограничением на κ стабилизатора G_κ множества κ , является транзитивной группой. Тогда κ — орбита интранзитивной подгруппы $H = G_\kappa$ группы G , и $|G : G_\kappa| = L$, $L < |S|$. Очевидно, что

$$\{\kappa_1, \kappa_2, \dots, \kappa_L\} = \{g_1 \kappa, g_2 \kappa, \dots, g_L \kappa\},$$

где

$$G = \bigcup_{j=1}^L g_j G_\kappa,$$

есть разложение G в левые смежные классы по подгруппе G_κ .

Предложение 8 теперь непосредственно следует из леммы 1.

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 , $\alpha = 1, \dots, n$, $n \geq 5$; S — множество всех подмножеств мощности 2 множества $\{1, \dots, n\}$; $\bar{A}_n, \bar{A}_\alpha$ — представления групп A_n, A_α на S . Известно (см., например, [5]), что A_n — $(n-2)$ -транзитивная группа и $\bar{A}_n$ — примитивная группа. Группы $A_n, \bar{A}_n$ изоморфны, подгруппа $\bar{A}_\alpha$ интранзитивна, $|\bar{A}_n : \bar{A}_\alpha| = |A_n : A_\alpha| = n$, $n < |S|$, $|S| = n(n-1)/2$. Таким образом, группа $\bar{A}_n$ 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 , $\alpha = 1, \dots, n$, $n \geq 4$; S — множество всех подмножеств мощности 2 множества $\{1, \dots, n\}$; $\bar{S}_n, \bar{S}_\alpha$ — представления групп S_n, S_α на S . Очевидно, что группы $S_n, \bar{S}_n$ изоморфны, группа $\bar{S}_\alpha$ интранзитивна, $|\bar{S}_n : \bar{S}_\alpha| = |S_n : S_\alpha| = n$, $n < |S|$. Таким образом, группа $\bar{S}_n$ является одновременно примитивной и слабо импримитивной группой подстановок при $n \geq 4$.

Предложение 9. Любая система слабой импримитивности

$$\bigcup_{j=1}^L \kappa_j = S$$

регулярной группы (G, S) является ее системой импримитивности.

Доказательство. Пусть

$$\bigcup_{j=1}^L \kappa_j = S$$

есть система слабой импримитивности регулярной группы (G, S) . По лемме 1 данная система может быть записана в виде $\Pi = \{g_1\kappa, g_2\kappa, \dots, g_L\kappa\}$, где

$$G = \bigcup_{j=1}^L g_j G_\kappa$$

есть разложение G в левые смежные классы по стабилизатору G_κ некоторого блока $\kappa \in \Pi$, причем ограничение G_κ на κ является транзитивной группой. Так как $G_s = e$ для $s \in \kappa$, то $G_s \subset G_\kappa \subset G$, откуда (см., например, [4]) и следует предложение 9.

Будем обозначать через $[v]$ целую часть числа v .

Предложение 10. $[|S|/2]$ -транзитивная группа (G, S) является сильно примитивной.

Доказательство. Пусть (G, S) — K -транзитивная группа, $K = \lfloor |S|/2 \rfloor$ и $\Pi = \{\kappa_1, \kappa_2, \dots, \kappa_L\}$ — ее система слабой импримитивности. Возможны два случая: $|\kappa| = |\kappa_j| \leq \lfloor |S|/2 \rfloor$, $j = 1, \dots, L$ и $|\kappa| > \lfloor |S|/2 \rfloor$. В первом случае, используя K -кратную транзитивность (G, S) и свойство 3 определения 6, заключаем, что в множестве Π содержатся все подмножества множества S мощности $|\kappa|$. Следовательно, в первом случае $L > |S|$, что противоречит определению Π . Во втором случае рассмотрим совокупность множеств

$$\bar{\Pi} = \{S \setminus \kappa_1, S \setminus \kappa_2, \dots, S \setminus \kappa_L\}.$$

Несложно проверить выполнение следующего свойства: $g\kappa_j = \kappa_{j'}$ при некоторых $g \in G$, $j' \in \{1, \dots, L\}$ тогда и только тогда, когда $g(S \setminus \kappa_j) = S \setminus \kappa_{j'}$. Так как во втором случае справедливо неравенство

$$|S \setminus \kappa_j| \leq \lfloor |S|/2 \rfloor, \quad j = 1, \dots, L,$$

используя K -кратную транзитивность G , можно аналогично первому случаю получить неравенство $L > |S|$, что противоречит определению Π . Следовательно, группа (G, S) сильно импримитивна.

Определение 7. Связный перестановочный автомат $A_M = (I, S, (\delta_i)_{i \in I})$ ($A = (I, S, O, (\delta_i)_{i \in I}, (\beta_i)_{i \in I})$) называется слабо импримитивным автоматом (импримитивным), если его группа $G = \langle (\delta_i)_{i \in I} \rangle$ подстановок на S слабо импримитивна (импримитивна). В противном случае, автомат A_M (A) называется сильно примитивным (примитивным) автоматом.

Систему слабой импримитивности (систему импримитивности)

$$\bigcup_{j=1}^L \kappa_j = S$$

группы G автомата A будем называть системой слабой импримитивности (системой импримитивности) автомата A .

Введенное понятие, система импримитивности связного перестановочного автомата $A_M = (I, S, (\delta_i)_{i \in I})$, является частным случаем известного понятия нетривиальной конгруэнции и совпадает с введенным ранее понятием нетривиальной конгруэнции по состояниям автомата A_M .

Замечание 2. На основании известных результатов по декомпозиции автоматов (см., например, [9]) стандартными методами алгебраической теории автоматов можно получить следующее утверждение: автомат $A = (I, S, (\delta_i)_{i \in I})$ является слабо импримитивным автоматом тогда и только тогда, когда найдется несвязный автомат, являющийся параллельным соединением некоторых связных перестановочных автоматов $A'' = (I, S'', (\delta''_i)_{i \in I})$, $\hat{A} = (I, \hat{S}, (\hat{\delta}_i)_{i \in I})$ с условием $1 < |S''| < |\hat{S}|$ и автомат A изоморфен по состояниям автомату $\hat{A}$.

Для системы слабой импримитивности $\Pi = \{\kappa_1, \kappa_2, \dots, \kappa_L\}$ связного перестановочного приведенного автомата $A = (I, S, (\delta_i)_{i \in I}, (\beta_i)_{i \in I})$ через $A_M(\Pi) = (I, S^\Pi, (\delta^\Pi_i)_{i \in I})$ обозначим автомат с множеством состояний $S^\Pi = \{\kappa_1, \kappa_2, \dots, \kappa_L\}$,

частичными функциями переходов $(\delta_i^\Pi)_{i \in I}$, где $\delta_i^\Pi \kappa_j = \kappa_j$, тогда и только тогда, когда $\delta_i \kappa_j = \kappa_j$, $i \in I$. Очевидно, что $A_M(\Pi)$ — связный перестановочный автомат.

Для $i \in I$ и произвольного подмножества κ множества S через ${}^i \kappa^y$ обозначим множество тех $s \in \kappa$, для которых $\beta_i s = y$, $y \in O$. Через $O(i, \kappa)$ ($\hat{O}(i, \kappa)$) обозначим множество всех элементов $y \in O$, при которых достигается максимум (минимум) величин $|{}^i \kappa^y|$ по $y \in O$. Для фиксированных $i \in I$, $j = 1, \dots, L$, разобьем κ_j на непересекающиеся подмножества ${}^i \kappa_j^y$ так, что

$$\kappa_j = \bigcup_{y \in O} {}^i \kappa_j^y.$$

Доопределим автомат $A_M(\Pi)$ частичными функциями выходов, введя множество $M(A, \Pi)$ ($\hat{M}(A, \Pi)$) автоматов вида

$$A(\Pi) = (I, S^\Pi, O, (\delta_i^\Pi)_{i \in I}, (\beta_i^\Pi)_{i \in I}) \quad (\hat{A}(\Pi) = (I, S^\Pi, O, (\delta_i^\Pi)_{i \in I}, (\hat{\beta}_i^\Pi)_{i \in I})).$$

Автомат $A(\Pi)$ ($\hat{A}(\Pi)$) принадлежит $M(A, \Pi)$ ($\hat{M}(A, \Pi)$) тогда и только тогда, когда $\beta_i^\Pi \kappa_j \in O(i, \kappa_j)$ ($\hat{\beta}_i^\Pi \kappa_j \in \hat{O}(i, \kappa_j)$) при любых $i \in I$, $j = 1, \dots, L$.

Для рассматриваемого автомата A введем еще один вспомогательный класс автоматов. Для $i \in I$ обозначим через $O(i)$ ($\hat{O}(i)$) множество тех $y \in O$, при которых достигается максимум (минимум) выражения $|\beta_i^{-1}(y)| = |{}^i S^y|$ по всем $y \in O$, а через $M(A)$ ($\hat{M}(A)$) обозначим некоторый класс автоматов с одним состоянием s_0 , входным и выходным алфавитами I, O , соответственно. А именно, полагаем, что автомат $A = (I, \{s_0\}, O, (\delta_i)_{i \in I}, (\beta_i)_{i \in I})$ принадлежит классу $M(A)$ ($\hat{M}(A)$) тогда и только тогда, когда для всех $i \in I$

$$\tilde{\delta}_i s_0 = s_0, \quad \tilde{\beta}_i s_0 \in O(i) \quad (\tilde{\beta}_i s_0 \in \hat{O}(i)).$$

Определение 8. Любой автомат из класса $M(A, \Pi)$ ($\hat{M}(A, \Pi)$) назовем наилучшим (наихудшим) Π -образом автомата $A = (I, S, (\delta_i)_{i \in I}, (\beta_i)_{i \in I})$, если все автоматы из $M(A, \Pi)$ ($\hat{M}(A, \Pi)$) являются приведенными автоматами. Любой автомат из $M(A)$ ($\hat{M}(A)$) назовем наилучшим (наихудшим) S -образом автомата A .

В связи с тем, что значение меры неотличимости $\mu(A_s, \bar{A}_{\bar{s}})$ ($\mu^{s, \bar{s}}$) двух инициальных автоматов (состояний $s, \bar{s}$ автоматов $A, \bar{A}$) рассчитывается с помощью параметров соответствующих им автоматов $A[s], \bar{A}[\bar{s}]$ ($A(s), \bar{A}(\bar{s})$), ниже будут использованы более удобные, адекватные предыдущим, обозначения $\mu(A[s], \bar{A}[\bar{s}])$, $\mu(A(s), \bar{A}(\bar{s}))$.

Теорема 3. Любой наилучший (наихудший) приближенный автомат $\bar{A}_{s_0}$ к заданному перестановочному инициальному автомату A_{s_0} (в классе $F_{p,i}(A_{s_0})$) таков, что ассоциированный с ним автомат $\bar{A}[\bar{s}_0]$ изоморфен по состояниям либо одному из наилучших (наихудших) Π -образов $A(\Pi)(\kappa_j)$ автомата $A[s_0]$ для некоторой его системы слабой импримитивности $\Pi = (\kappa_1, \dots, \kappa_L)$, при этом $s_0 \in \kappa_j$, либо одному из наилучших (наихудших) S_{s_0} -образов автомата $A[s_0]$.

Доказательство. Пусть $\bar{A}[\bar{s}_0]$ — наилучший приближенный автомат к A_{s_0} и $\mathfrak{A} = \mathfrak{A}((s_0, \bar{s}_0))$ — подавтомат с множеством состояний $S^{\mathfrak{A}}$, порожденный начальным состоянием $(s_0, \bar{s}_0)$ параллельного соединения $\mathfrak{A}(A[s_0], \bar{A}[\bar{s}_0])$ приведенных перестановочных автоматов

$$A[s_0] = (I, S, O, (\delta_i)_{i \in I}, (\beta_i)_{i \in I}), \quad \bar{A}[\bar{s}_0] = (I, \bar{S}, O, (\bar{\delta}_i)_{i \in I}, (\bar{\beta}_i)_{i \in I})$$

при едином входе.

Через $\kappa_{\bar{s}}$, $\bar{s} \in \bar{S}$, обозначим множество тех $s \in S$, для которых $(s, \bar{s}) \in S^{\mathfrak{A}}$. Используя замечание 1, заключаем, что матрица

$$\tilde{U} = \frac{1}{h}(E + U + \dots + U^{h-1})$$

для автомата $\mathfrak{A}((s_0, \bar{s}_0))$ равновероятна. По этой причине

$$\begin{aligned} \mu(A[s_0], \bar{A}[\bar{s}_0]) &= \frac{1}{|S^{\mathfrak{A}}|} \sum_{(s, \bar{s}) \in S^{\mathfrak{A}}} r^{((s, \bar{s}), 1)} = \frac{1}{|S^{\mathfrak{A}}|} \sum_{\bar{s} \in \bar{S}} \sum_{s \in \kappa_{\bar{s}}} r^{((s, \bar{s}), 1)} \\ &= \frac{1}{|I||S^{\mathfrak{A}}|} \sum_{i \in I} \sum_{\bar{s} \in \bar{S}} \sum_{s \in \kappa_{\bar{s}}} \hat{\beta}_i(s, \bar{s}), \end{aligned}$$

где $\hat{\beta}_i(s, \bar{s}) = 0$, если $\beta_i s = \bar{\beta}_i \bar{s}$ и $\hat{\beta}_i(s, \bar{s}) = 1$ в противном случае.

Используя введенные выше обозначения, находим, что

$$\mu(A[s_0], \bar{A}[\bar{s}_0]) = \frac{1}{|I||S^{\mathfrak{A}}|} \sum_{i \in I} \sum_{\bar{s} \in \bar{S}} |\kappa_{\bar{s}} \setminus {}^i \kappa_{\bar{s}}^{\bar{\beta}_i \bar{s}}|.$$

Так как $\bar{A}_{\bar{s}_0}$ — наилучший приближенный автомат к заданному автомату A_{s_0} (в классе $F_{p,i}(A_{s_0})$),

$$\mu(A[s_0], \bar{A}[\bar{s}_0]) = \frac{1}{|I||S^{\mathfrak{A}}|} \sum_{i \in I} \sum_{\bar{s} \in \bar{S}} |\kappa_{\bar{s}} \setminus {}^i \kappa_{\bar{s}}^y(i, \kappa_{\bar{s}})|. \quad (1)$$

Напомним, что элементы $y(i, \kappa_{\bar{s}})$ определены возможно неоднозначно, но данное равенство выполняется при любом выборе элементов $y(i, \kappa_{\bar{s}})$ из $O(i, \kappa_{\bar{s}})$, $i \in I$, $\bar{s} \in \bar{S}_{\bar{s}_0}$.

Рассмотрим бинарное отношение σ на $\bar{S}$ такое, что $\bar{s}_1 \sigma \bar{s}_2$ тогда и только тогда, когда $\kappa_{\bar{s}_1} = \kappa_{\bar{s}_2}$. Очевидно, что σ — отношение эквивалентности на $\bar{S}$, (E_I, σ) — конгруэнция по состояниям автомата $\bar{A}_M[\bar{s}_0]$. Обозначим через $(\bar{S}_j)_{j=1, \dots, k}$ классы эквивалентности отношения σ . Отметим, что они равномощны. Рассмотрим следующие случаи:

- (1) $1 < k < |\bar{S}|$;
- (2) $k = 1$, $\bar{S}_1 = \bar{S}_{\bar{s}_0}$, $\bar{S} = \{\bar{s}_0\}$;
- (3) $k = 1$, $\bar{S}_1 = \bar{S}$, $|\bar{S}| > 1$;
- (4) $k = |\bar{S}|$, $|\bar{S}_j| = 1$.

При выполнении случая 1 можно выбрать элементы $y(i, \kappa_{\bar{s}})$ из $O(i, \kappa_{\bar{s}})$ такими, что при любом $i \in I$

$$y(i, \kappa_{\bar{s}}) = y(i, \kappa_{\bar{s}'}) = y(i, j), \quad \bar{s}, \bar{s}' \in \bar{S}_j, \quad j = 1, \dots, k.$$

При таком выборе элементов $y(i, \kappa_{\bar{s}})$ рассмотрим фактор-автомат $\bar{A}_M\langle\bar{s}_0\rangle/(E_I, \sigma)$, состояниями которого являются классы $(\bar{S}_j)_{j=1, \dots, k}$. Доопределим его функциями выходов $\tilde{\beta}_i$, $i \in I$, положив $\tilde{\beta}_i \bar{S}_j = y(i, j)$. Без ограничения общности положим $\bar{s}_0 \in \bar{S}_1$. Запишем полученный автомат в виде $\bar{A}\langle\bar{S}_I\rangle$. Справедливы равенства

$$\begin{aligned} \mu(A[s_0], \bar{A}[\bar{s}_0]) &= \frac{1}{|I||S^{\mathfrak{A}}|} \sum_{i \in I} \sum_{\bar{s} \in \bar{S}} |\kappa_{\bar{s}} \setminus {}^i \kappa_{\bar{s}}^y(i, \kappa_{\bar{s}})| \\ &= \frac{|S_1|}{|I||S^{\mathfrak{A}}|} \sum_{i \in I} \sum_{j=1}^k |\kappa_{\bar{s}} \setminus {}^i \kappa_{\bar{s}}^y(i, j)| = \mu(A[s_0], \bar{A}\langle\bar{S}_I\rangle). \end{aligned}$$

Автомат $\bar{A}\langle\bar{S}_I\rangle$ имеет меньшее число состояний чем $\bar{A}\langle\bar{s}_0\rangle$. Поэтому случай 1 невозможен.

При выполнении случая 2 формула (1) принимает вид

$$\mu(A[s_0], \bar{A}[\bar{s}_0]) = \frac{1}{|I||S^{\mathfrak{A}}|} \sum_{i \in I} |S \setminus {}^i S^{y(i, S)}|.$$

Следовательно, $\bar{A}[\bar{s}_0]$ изоморфен по состояниям одному из наилучших S_{s_0} -образов автомата $A[s_0]$.

Проводя полностью аналогичные случаю 1 выкладки, несложно показывает, что случай 3 невозможен. В случае 4 легко проверяется, что $\Pi = \{\kappa_{\bar{s}}\}_{\bar{s} \in \bar{S}}$ является системой слабой импримитивности автомата $A[s_0]$, и используя формулу (1), получаем, что

$$\mu(A[s_0], \bar{A}[\bar{s}_0]) = \mu(A[s_0], A(\Pi)\langle\kappa_{\bar{s}_0}\rangle),$$

где $s_0 \in \kappa_{\bar{s}_0}$ при любом автомате $A(\Pi)$ из $M(A[s_0], \Pi)$. При этом $A(\Pi)\langle\kappa_{\bar{s}}\rangle$ — наилучший Π -образ автомата $A[s_0]$ для его системы слабой импримитивности $\Pi = (\kappa_{\bar{s}})_{\bar{s} \in \bar{S}}$, так как $\bar{A}_{s_0}$ — наилучший приближенный автомат к заданному автомату A_{s_0} (в классе $F_{p,i}(A_{s_0})$). Соответствие $\bar{s} \rightarrow \kappa_{\bar{s}}$ устанавливает изоморфизм по состояниям автомата $\bar{A}\langle\bar{s}_0\rangle$ и некоторого наилучшего Π -образа $A(\Pi)\langle\kappa_{\bar{s}_0}\rangle$ автомата $A\langle s_0 \rangle$.

Аналогично проводится доказательство утверждения теоремы для наихудшего приближенного автомата $\bar{A}_{\bar{s}_0}$ к автомату A_{s_0} .

Из теоремы 3 вытекает, что поиск всех наилучших (наихудших) приближенных автоматов $\bar{A}_{\bar{s}_0}$ к заданному перестановочному инициальному автомату A_{s_0} (в классе $F(A_s)$) можно вести путем предварительного построения всех наилучших (наихудших) Π -образов $A(\Pi)\langle\kappa_j\rangle$ автомата $A[s_0]$ для каждой его системы слабой импримитивности Π и всех наилучших (наихудших) S_{s_0} -образов автомата $A[s_0]$ с последующим опробованием этих образов на предмет выбора наилучших (наихудших) приближенных автоматов $\bar{A}_{\bar{s}_0}$ к A_{s_0} .

Следствие 3. Автомат $\bar{A}_{\bar{s}_0}$ является наилучшим (наихудшим) приближенным автоматом к заданному перестановочному сильно примитивному инициальному автомату A_{s_0} (в классе $F_{p,i}(A_{s_0})$) тогда и только тогда, когда ассоциированный с ним автомат $\bar{A}[\bar{s}_0]$ изоморфен по состояниям некоторому наилучшему (наихудшему) S_{s_0} -образу автомата $A[s_0]$.

Будем говорить, что автомат A_s из $F_{p,i}$ является регулярным, если группа (G, S_s) соответствующего ему автомата $A[s] = (I, S_s, O, (\delta_i)_{i \in I}, (\beta_i)_{i \in I})$ регулярна.

Обозначим через $F_{p,i,r}$ множество всех регулярных перестановочных инициальных автоматов из $F_{p,i}$. Для автомата A_s из $F_{p,i,r}$ и натурального числа $N > |S_s|$ обозначим через $F_{p,N,r}(A_s)$ множество всех автоматов $\bar{A}_{\bar{s}}$ из $F_{p,i,r}$ таких, что $A_M[s]$ не является гомоморфным образом по состояниям каждого из автоматов $\bar{A}_M[\bar{s}]$ и $|\bar{S}_{\bar{s}}| \leq N$.

Определение 9. Минимальный $\mu\epsilon$ -неотличимый автомат $\bar{A}_{\bar{s}}$ от A_s , $A_s \in F_{p,i,r}$, называется наилучшим приближенным автоматом к A_s (в классе $F_{p,N,r}(A_s)$), если $\bar{A}_{\bar{s}} \in F_{p,N,r}(A_s)$ и при любом $\epsilon' < \epsilon$ не существует автоматов A'_s из $F_{p,N,r}(A_s)$ $\mu\epsilon'$ -неотличимых от автомата A_s .

Аналогично вводится понятие наихудшего приближенного автомата $\bar{A}_{\bar{s}}$ к A_s (в классе $F_{p,N,r}(A_s)$). Отличие состоит лишь в том, что при любом $\epsilon' > \epsilon$ не существует автоматов A'_s из $F_{p,N,r}(A_s)$ $\mu\epsilon'$ -неотличимых от автомата A_s .

Теорема 4. Любой наилучший (наихудший) приближенный автомат $\bar{A}_{\bar{s}_0}$ к заданному перестановочному регулярному инициальному автомату A_{s_0} (в классе $F_{p,N,r}(A_{s_0})$) таков, что ассоциированный с ним автомат $\bar{A}[\bar{s}_0]$ изоморфен по состояниям либо некоторому наилучшему (наихудшему) Π -образу $A(\Pi)\langle \chi_j \rangle$ автомата $A[s_0]$ для некоторой его системы импримитивности $\Pi = (\chi_1, \dots, \chi_L)$, либо некоторому наилучшему (наихудшему) S_{s_0} -образу автомата $A[s_0]$.

Доказательство. Положим для краткости $S = S_{s_0}$, $\bar{S} = \bar{S}_{\bar{s}_0}$. Из предложения 9 и теоремы 3 вытекает, что для доказательства теоремы 4 достаточно доказать неравенство $|S| > |\bar{S}|$. Предположим, что $|S| \leq |\bar{S}|$ и $\bar{A}_{\bar{s}_0}$ — наилучший приближенный автомат к заданному перестановочному регулярному инициальному автомату A_{s_0} (в классе $F_{p,N,r}(A_{s_0})$). Используем для автоматов $\bar{A}_{\bar{s}_0}$, A_{s_0} введенное при доказательстве теоремы 3 обозначение $\mathfrak{A} = \mathfrak{A}\langle (s_0, \bar{s}_0) \rangle$. Для $s \in S$ положим $\bar{\chi}_s = \{\bar{s} \in \bar{S} : (s, \bar{s}) \in S^{\mathfrak{A}}\}$. Аналогично первой части доказательства теоремы 3 легко получить, что

$$\mu(A[s_0], \bar{A}[\bar{s}_0]) = \frac{1}{|I||S^{\mathfrak{A}}|} \sum_{i \in I} \sum_{s \in S} |\bar{\chi}_s \setminus {}^i \bar{\chi}_s^{\beta_i} s|.$$

Рассмотрим бинарное отношение $\bar{\sigma}$ на S такое, что $s_1 \bar{\sigma} s_2$ тогда и только тогда, когда $\bar{\chi}_{s_1} = \bar{\chi}_{s_2}$. Очевидно, что $\bar{\sigma}$ — отношение эквивалентности на S . Пусть $(S_j)_{j=1, \dots, k}$ суть классы эквивалентности отношения $\bar{\sigma}$. Очевидно, что они равномошны.

Рассмотрим следующие случаи:

$$(1) |S_j| = |\bar{\chi}_j| = 1, j = 1, \dots, k;$$

$$(2) |S_j| = 1, |\bar{\kappa}_j| > 1, j = 1, \dots, k;$$

$$(3) k = 1, S_1 = S;$$

$$(4) |S_j| > 1, 1 < |\bar{\kappa}_s| < |S|.$$

Первый случай невозможен, так как в этом случае автомат $A_M[s_0]$ является изоморфным образом по состояниям автомата $\bar{A}_M[\bar{s}_0]$. Второй случай также невозможен, так как в этом случае множество $\{\bar{\kappa}_s : s \in S\}$ является системой импримитивности автомата $\bar{A}[\bar{s}_0]$ и несложно проверяется, что $A_M[\bar{s}_0]$ является гомоморфным образом по состояниям автомата $\bar{A}_M[\bar{s}_0]$.

В случаях 3 и 4 представим величину $\mu(A[s_0], \bar{A}[\bar{s}_0])$ в виде

$$\mu(A[s_0], \bar{A}[\bar{s}_0]) = \frac{1}{|I||S^{\mathfrak{A}}|} \sum_{i \in I} \sum_{j=1}^k \sum_{s \in S_j} |\bar{\kappa}_j \setminus {}^i \bar{\kappa}_s^{\beta_i s}|.$$

Для завершения доказательства утверждение теоремы 4 о наилучшем инициальном автомате $\bar{A}_s$ достаточно для случаев 3 и 4 получить противоречие начального предположения $|S| \leq |\bar{S}|$ с условиями теоремы. С этой целью мы построим новый инициальный автомат $\hat{A}_{\hat{s}_0}$, для которого $|\hat{S}_{\hat{s}_0}| < |S|$ и $\mu(A[s_0], \bar{A}[\bar{s}_0]) \geq \mu(A[s_0], \hat{A}[\hat{s}_0])$. Данное построение будет проведено с помощью выбора новых частичных функций выхода автомата $\bar{A}[\bar{s}_0]$, при которых мы получим автомат $\hat{A}[\hat{s}_0]$, приведенная форма которого будет являться искомым автоматом $\hat{A}[\hat{s}_0]$. Для выполнения этого плана рассмотрим возможности минимизации величины $\mu(A[s_0], \bar{A}[\bar{s}_0])$ путем выбора новых частичных функций выхода автомата $\bar{A}[\bar{s}_0]$. Положим $\bar{\kappa}_j = \bar{\kappa}_s$ для $s \in S_j, j = 1, \dots, k$. Так как разные блоки из $\{\bar{\kappa}_1, \dots, \bar{\kappa}_l\}$ попарно не пересекаются, наша задача сводится к минимизации величин

$$\sum_{s \in S_j} |\bar{\kappa}_j \setminus {}^i \bar{\kappa}_s^{\beta_i s}|, \quad j = 1, \dots, k, \quad i \in I.$$

Для фиксированных $j = 1, \dots, k, i \in I, y \in O$ обозначим через $\nu(y)$ число состояний $s \in S_j$, для которых $\beta_i s = y$, и положим $\bar{\kappa}_j = \kappa, |{}^i \bar{\kappa}_s^y| = |\kappa^y|$. Последнюю сумму запишем в виде

$$\sum_{y \in O} \nu(y)(|\kappa| - |\kappa^y|).$$

Для минимизации данного выражение с помощью выбора значений на κ новой функции $\bar{\beta}_i$ достаточно найти максимум суммы

$$\sum_{y \in O} \nu(y) |\kappa^y|$$

относительно неизвестных

$$|\kappa^y|, \quad y \in O, \quad \sum_{y \in O} |\kappa^y| = |\kappa|,$$

то есть найти

$$\max \sum_{y \in O} \nu(y) p(y)$$

относительно неизвестных $p(y)$, $y \in O$, где

$$p(y) = \frac{|\mathcal{K}^y|}{|\mathcal{K}|}, \quad \sum_{y \in O} p(y) = 1.$$

Несложно проверить, что данный максимум равен $\nu(\tilde{y})$, где $\tilde{y}$ — произвольный элемент из O , для которого

$$\nu(\tilde{y}) = \max_{y \in O} \nu(y),$$

и он достигается, в частности, при $p(\tilde{y}) = 1$.

Следовательно, выбрав новые частичные функции выходов $(\tilde{\beta}_i)$ для автомата $\bar{A}[\bar{s}_0]$ таким образом, чтобы на каждом блоке $\bar{\mathcal{K}}_j$, $j = 1, \dots, k$, они были постоянными и принимали указанные выше значения, мы получим автомат $\tilde{A}(\bar{s}_0)$, для которого

$$\mu(A\langle s_0 \rangle, \bar{A}(\bar{s}_0)) \geq \mu(A\langle s_0 \rangle, \tilde{A}(\bar{s}_0)),$$

причем его приведенная форма $\hat{A}(\hat{s}_0) = \hat{A}[\hat{s}_0]$ такова, что $|\hat{S}_{\hat{s}_0}| < |S_{s_0}|$ и

$$\mu(A\langle s_0 \rangle, \bar{A}(\bar{s}_0)) \geq \mu(A\langle s_0 \rangle, \hat{A}(\hat{s}_0)).$$

Аналогично доказывается утверждение теоремы 4 о наихудшем приближенном автомате $\bar{A}_{s_0}$ к A_{s_0} . Основное отличие состоит в выборе автомата $\hat{A}(\hat{s}_0)$, который находится с помощью поиска минимума величины $\sum_{y \in O} \nu(y)|\mathcal{K}^y|$. Доказательство теоремы 4 завершено.

В заключение автор пользуется случаем выразить признательность В. Б. Кудрявцеву и А. С. Строгалову за внимание к работе и полезные замечания, способствовавшие улучшению работы.

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. *Введение в теорию автоматов*. Наука, Москва, 1985.
2. Строгалов А. С. Об ε -моделировании поведения конечных автоматов. *Материалы Первого Всесоюзного семинара по дискретной математике и ее приложениям*. Издательство МГУ, Москва, 1986, 42–56.
3. Гантмахер Ф. Р. *Теория матриц*. Наука, Москва, 1966.
4. Супруненко Д. А. *Группы матриц*. Наука, Москва, 1972.
5. Wieland H. *Finite permutation groups*. Academic Press, New York, 1964.
6. Гинсбург С. В. О длине кратчайшего однородного эксперимента, устанавливающего конечные состояния машины. *Киберн. сб.* (1961) **3**, 167–186.
7. Бабаш А. В. Верхняя оценка степени различимости связанных перестановочных автоматов с заданным диаметром. В сб.: *Комбинаторно-алгебраические методы в прикладной математике*. Издательство Горьковского университета, Горький, 1983, 3–43.
8. Хомский М., Миллер Д. Языки с конечным числом состояний. *Киберн. сборник* (1962) **4**, 233–255.
9. Hartmanis J., Stearns R. E. *Algebraic Structure Theory of Sequential Machines*. Prentice-Hall, Englewood Cliffs, NJ, 1966.

Статья поступила 17.08.95.