Об отличимости состояний решетчатых автоматов*

П.А. Пантелеев

В работе рассматривается класс автоматов специального вида, называемых решетчатыми автоматами. Множеством состояний таких автоматов служит подмножество k-мерной целочисленной решетки, а на выход подается m, $1 \leqslant m \leqslant k$, выделенных компонент текущего состояния, называемых наблюдаемыми параметрами. Два состояния называются r-отличимыми входным словом, если под его действием они перейдут в состояния, которые в одном из наблюдаемых параметров отличаются более чем на r. Для этой отличимости получен порядок соответствующей функции Шеннона.

Введение

Реальные физические системы часто описываются набором непрерывных числовых параметров, часть из которых непосредственно наблюдаемы. Возможно также воздействовать на систему для перевода ее в различные режимы работы. Для описания подобных систем и процессов, используется теория динамических систем. При дискретном моделировании таких объектов удобно использовать теорию автоматов. Мы эти параметры объектов считаем образующими своими значениями многомерную целочисленную решетку. Подмножества решетки считаем состояниями моделирующего автомата, а часть состояний считаем наблюдаемыми выходами автомата, и называем такие автоматы *решетчатыми*. Одним из базовых понятий

*Работа выполнена при частичной поддержке РФФИ, грант № 02–01–00162.

теории автоматов является отличимость состояний. Это понятие было введено и исследовано Э. Муром [1]. Здесь считаем, что параметры имеют погрешность, поэтому расширяем муровскую отличимость до r-отличимости, считая, что два состояния отличимы входным словом, если под его воздействием они переходят в состояния, которые в одном из наблюдаемых параметров отличаются более чем на r. Как и в случае с муровской отличимостью, возникает вопрос о значении функции Шеннона для r-отличимости. Как известно из результатов Мура [1] для обычной отличимости она равна $n-1$, где n — число состояний автомата. В работе [4] исследовалась ε-отличимость, которая является обобщением r-отличимости на случай произвольных автоматов с произвольно заданной метрикой ρ на множестве выходных символов. Было показано, что если отношение ε-близости, определяемое метрикой ρ и числом ε, не является отношением эквивалентности, то значение соответствующей функции Шеннона равно $\frac{n(n-1)}{2}$. Как будет показано ниже, функция Шеннона для r-отличимости занимает промежуточное значение между этими двумя случаями, принимая целый спектр значений от $n-1$ до $\frac{n(n-1)}{2}$ в зависимости от параметра m — числа наблюдаемых.

Понятия и результаты

Под *абстрактным конечным автоматом* (в дальнейшем — автоматом) понимается объект $\mathfrak{A} = (A, Q, B, \varphi, \psi)$, где A, Q, B — конечные непустые множества, называемые, соответственно, *входным алфавитом*, *алфавитом состояний* и *выходным алфавитом*; $\varphi : Q \times A \to Q$, $\psi : Q \times A \to B$ — *функции переходов* и *выходов*. Множество всех слов в алфавите A обозначим A^*. Пусть $|\alpha|$ означает длину слова $\alpha \in A^*$. При $a \in A$ и $n \in \mathbb{N}$ полагаем $a^n = \underbrace{aa\ldots a}_{n}$. Аналогично, если $\alpha \in A^*$, то $[\alpha]^n = \underbrace{\alpha\alpha\ldots\alpha}_{n}$. . Распространим функции φ и ψ на множество $Q \times A^*$ так: $\varphi(q,\Lambda) = q$, $\varphi(q,\alpha a) = \varphi(\varphi(q,\alpha),a)$ и $\psi(q,\Lambda) = \Lambda$, $\psi(q,\alpha a) = \psi(\varphi(q,\alpha),a)$, $q \in Q, a \in A, \alpha \in A^*$. Здесь Λ – пустое слово. Пусть $\overline{\psi}(q, a(1)a(2)\ldots a(l)) = \psi(q,a(1))\psi(q,a(1)a(2))\ldots\psi(q,a(1)a(2)\ldots a(l))$. Распространим функцию переходов φ на множество $2^Q \times A^*$, где $2^Q = \{Q' \mid Q' \subseteq Q\}$ так:

$\varphi(Q', \alpha) = \{\varphi(q, \alpha) \mid q \in Q'\}$.

Назовем *k-мерной целочисленной $n_1 \times \ldots \times n_k$-решеткой* с началом в точке $\tilde{x}^0 = (x_1^0, \ldots, x_k^0) \in \mathbb{Z}^k$ множество

$$\mathbb{Z}^k_{n_1,\ldots,n_k} = \{(x_1, \ldots, x_k) \in \mathbb{Z}^k \mid x_i^0 \leqslant x_i \leqslant x_i^0 + n_i, i = \overline{1, k}\}.$$

Будем использовать обычные алгебраические обозначения по отношению к векторам $\tilde{x}, \tilde{y}$, такие как $\tilde{x} + \tilde{y}$ и $a\tilde{x}$, для суммы векторов, и умножения вектора на число $a \in \mathbb{Z}$. Введем на $\mathbb{Z}^k_{n_1,\ldots,n_k}$ метрику

$$\rho(\tilde{x}, \tilde{y}) = \max_{1 \leqslant i \leqslant k} |x_i - y_i|,$$

$$\tilde{x} = (x_1, \ldots, x_k), \tilde{y} = (y_1, \ldots, y_k).$$

Пусть также $\mathbf{e}_1 = (1, 0, \ldots, 0), \ldots, \mathbf{e}_k = (0, 0, \ldots, 1)$. Рассмотрим класс $\mathcal{A}^{k,m}_{n_1,\ldots,n_k}$, автоматов с множеством состояний $\mathbb{Z}^k_{n_1,\ldots,n_k}$, функция выходов которых имеет вид $\psi((x_1, \ldots, x_k), a) = (x_1, \ldots, x_m)$, $2 \leqslant m \leqslant k$. Скажем, что состояния q_1, q_2 автомата $\mathfrak{A} \in \mathcal{A}^{k,m}_{n_1,\ldots,n_k}$ *r-отличимы словом* $\alpha = a(1)a(2)\ldots a(l)$, если $\rho(\psi(q_1, a(1)a(2)\ldots a(l')), \psi(q_2, a(1)a(2)\ldots a(l'))) > r$ для некоторого $l' \leqslant l$. Обозначим через $l^r_{\mathfrak{A}}(q_1, q_2)$ минимальную длину r-отличающего q_1, q_2 слова. Пусть $L^r(\mathfrak{A}) = \max\limits_{q_1, q_2} l^r_{\mathfrak{A}}(q_1, q_2)$, где максимум берется по всем парам r-отличимых состояний автомата $\mathfrak{A}$. Рассмотрим функцию Шеннона для данного вида отличимости

$$L^m_k(n_1, \ldots, n_k, r) = \max_{\mathfrak{A} \in \mathcal{A}^{k,m}_{n_1,\ldots,n_k}} L^r(\mathfrak{A}),$$

где $r \leqslant n_i$, $i = \overline{1, n}$, $m \geqslant 2$.

Теорема 1. *Имеет место соотношение*

$$L^m_k(n_1, \ldots, n_k, r) \asymp r^m \cdot n_1 \cdot \ldots \cdot n_m \cdot n^2_{m+1} \cdot \ldots \cdot n^2_k$$

при $n_1, \ldots, n_k, r \to \infty$.

Рассмотрим k-мерный булев куб $\mathbf{B}_k = \{0, 1\}^k$ и назовем две его вершины *соседними*, если они отличаются ровно в одной компоненте. *Кодом Грея* для $\mathbf{B}_k$ называется произвольная последовательность всех его вершин $\tilde{\gamma}_0, \tilde{\gamma}_1, \ldots, \tilde{\gamma}_{2^n-1}$ такая, что вершины $\tilde{\gamma}_i$ и $\tilde{\gamma}_{i+1}$,

$i = \overline{0, 2^n - 2}$, а также $\tilde{\gamma}_{2^n-1}$ и $\tilde{\gamma}_0$ — соседние. Таким образом, если рассматривать булев куб как граф, считая две его вершины смежными, если они соседние, то код Грея есть ни что иное, как гамильтонов цикл для него. И поэтому в дальнейшем будем обращаться с ним как с циклом и применять соответствующую терминологию теории графов. Легко показать, что для любого натурального $k \geqslant 2$ в $\mathbf{B}_k$ существует код Грея.

Нас будут интересовать специальные коды Грея $\mathbf{C}_k$, в которых $\tilde{\gamma}_0 = (0, \dots, 0)$ и $\tilde{\gamma}_{2^{k-1}} = (1, \dots, 1)$ при четном k, $\tilde{\gamma}_{2^{k-1}+1} = (1, \dots, 1)$ при нечетном, то есть вершины $(0, \dots, 0)$ и $(1, \dots, 1)$ находятся на максимально возможном расстоянии.

Определим коды Грея $\mathbf{C}_k$ индукцией по параметру k. В качестве $\mathbf{C}_2$ и $\mathbf{C}_3$ возьмем последовательности:

$$(0,0), (0,1), (1,1), (1,0);$$
$$(0,0,0), (0,1,0), (1,1,0), (1,0,0), (1,0,1), (1,1,1), (0,1,1), (0,0,1).$$

Если $k \geqslant 3$ и $\tilde{\alpha}_0, \tilde{\alpha}_1, \dots, \tilde{\alpha}_{2^k-1}$ — получена из последовательности $\mathbf{C}_k$ приписыванием к каждому набору справа нуля, а $\tilde{\beta}_0, \tilde{\beta}_1, \dots, \tilde{\beta}_{2^k-1}$ — единицы. Тогда $\mathbf{C}_{k+1}$ это последовательность (рис. 1):

$$\tilde{\alpha}_0, \tilde{\alpha}_1, \dots, \tilde{\alpha}_{3\cdot 2^{k-2}}, \tilde{\beta}_{3\cdot 2^{k-2}}, \tilde{\beta}_{3\cdot 2^{k-2}-1}, \dots, \tilde{\beta}_0,$$
$$\tilde{\beta}_{2^k-1}, \dots, \tilde{\beta}_{3\cdot 2^{k-2}+1}, \tilde{\alpha}_{3\cdot 2^{k-2}+1}, \tilde{\alpha}_{3\cdot 2^{k-2}}, \dots, \tilde{\alpha}_{2^k-1}.$$

Лемма 1. *В цикле $\mathbf{C}_k$ вершины $(0, \dots, 0)$ и $(1, \dots, 1)$ находятся на расстоянии 2^{k-1} при четном k и на расстоянии $2^{k-1} - 1$ при нечетном k.*

Доказательство. Установим индукцией по k, что код $\mathbf{C}_k = \tilde{\gamma}_0^{(k)}, \dots, \tilde{\gamma}_{2^k-1}^{(k)}$ обладает требуемыми свойствами. Для $\mathbf{C}_2$ и $\mathbf{C}_3$ это очевидно. Допустим, что утверждение справедливо для $k \geqslant 3$. Докажем его для $k+1$. В коде $\mathbf{C}_k$ по предположению индукции $\tilde{\gamma}_0^{(k)} = (0, \dots, 0)$ и $\tilde{\gamma}_{2^{k-1}}^{(k)} = (1, \dots, 1)$ при четном k, $\tilde{\gamma}_{2^{k-1}+1}^{(k)} = (1, \dots, 1)$ при нечетном. Тогда, как видно из построения кода $\mathbf{C}_{k+1}$ (рис. 1): $\tilde{\gamma}_0^{(k+1)} = (0, \dots, 0)$ и $\tilde{\gamma}_{2^k+1}^{(k+1)} = \tilde{\gamma}_{3\cdot 2^{k-2}+1+2^{k-2}}^{(k+1)} = (1, \dots, 1)$ при четном k, $\tilde{\gamma}_{2^k}^{(k+1)} = \tilde{\gamma}_{3\cdot 2^{k-2}+1+2^{k-2}-1}^{(k+1)} = (1, \dots, 1)$ при нечетном.

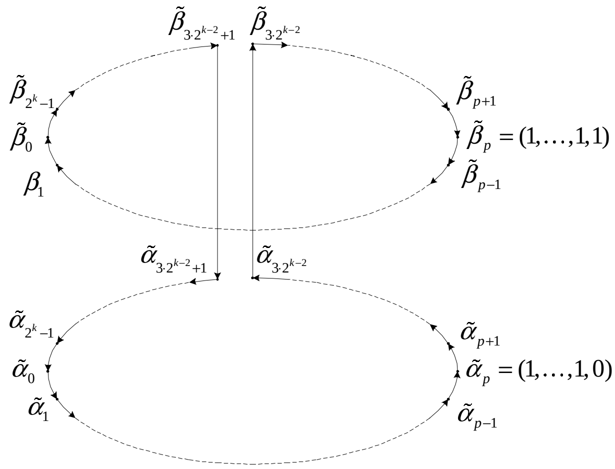

Рис. 1. Индуктивное построение кода $\mathbf{C}_{k+1}$

Таким образом, шаг индукции завершен и лемма доказана.

Далее будет определен некоторый класс графов, называемых *графами Серпинского*. Граф G из этого класса обладает следующими свойствами:

1) Он является циклом.
2) Множество его вершин — подмножество решетки $\mathbb{Z}^k_{n_1,\ldots,n_k}$ с началом в точке $\tilde{x}^0 = (x^0_1, \ldots, x^0_k)$.
3) У него выделяется 2^k *угловых* вершин, среди которых одна называется *начальной* и еще одна *конечной*.
4) Любые две смежные вершины в графе G являются смежными на решетке, то есть отличаются на единицу ровно в одной компоненте.

На множестве $\mathbb{Z}^k$ будут применяться различные геометрические преобразования (движение, гомотетия), под результатом действия которых к графу G будет пониматься изоморфный исходному граф G', получаемый применением данного преобразования к множеству вершин графа G.

Скажем, что граф Серпинского G обладает *s-свойством*, если у его начальной вершины есть смежная вершина, отличающаяся в s-й компоненте.

Определим *n^k-граф Серпинского* G с началом в $(x_1^0, \dots, x_k^0)$ индуктивно по n и назовем угловыми вершинами вершины вида $(x_1^0 + c_1 n, \dots, x_k^0 + c_k n)$, $c_i \in \{0,1\}$, $i = \overline{1,k}$, причем $(x_1^0, \dots, x_k^0)$ — назовем начальной, а $(x_1^0 + n, \dots, x_k^0 + n)$ — конечной. 1^k-граф есть любой граф, получаемый параллельным переносом из графа $\mathbf{C}_k$; 2^k-граф получается из произвольного 1^k-графа гомотетией с коэффициентом 2 и с центром в его начальной вершине, и последующим подразбиением каждого его ребра новой вершиной на две равные части. Таким образом, в 1^k-графе будет 2^k вершин, а в 2^k-графе 2^{k+1} вершины, причем оба они циклы. Допустим мы определили понятие n^k-графа Серпинского для всех $n < n'$, тогда $(n')^k$-графом Серпинского с началом в $\tilde{x}^0 = (x_1^0, \dots, x_k^0)$ будем называть граф G', получаемый так. Пусть G — n^k-граф Серпинского с началом в $\tilde{x}^0$, где $n' = 2n + 1$, если n' — нечетно, и $n' = 2n + 2$, если четно. Рассмотрим граф $G_{\tilde{\alpha}}$, $\tilde{\alpha} = (a_1, \dots, a_k) \in \mathbf{B}_k$, получаемый из графа G отражением относительно гиперплоскостей $x_i = x_i^0 + n + \frac{1}{2}$ при нечетном n' и $x_i = x_i^0 + n + 1$ при четном для всех i таких, что $a_i = 1$.

Пусть $\tilde{x}^1$ — конечная вершина графа G, тогда обозначим через $\tilde{x}_{\tilde{\alpha}}$ и $\tilde{x}'_{\tilde{\alpha}}$ вершины графа $G_{\tilde{\alpha}}$ в которые перейдут вершины $\tilde{x}^1$ и $\tilde{x}^1 - \mathbf{e}_1$ соответственно. Пусть $\mathbf{C}_k = \tilde{\alpha}_0, \tilde{\alpha}_1, \dots, \tilde{\alpha}_{2^k-1}$ — описанный выше код Грея. Назовем вершину $\tilde{x}_{\tilde{\alpha}_i}$ графа $G_{\tilde{\alpha}_i}$ — выходной для четного i и входной для нечетного, а вершину $\tilde{x}'_{\tilde{\alpha}_i}$ того же графа входной при четном i и выходной для нечетного. Граф G' получается объединением графов $G_{\tilde{\alpha}_0}, G_{\tilde{\alpha}_1}, \dots, G_{\tilde{\alpha}_{2^k-1}}$, удалением 2^k ребер $(\tilde{x}_{\tilde{\alpha}_i}, \tilde{x}'_{\tilde{\alpha}_i})$ и добавлением 2^k ребер, соединяющих выходную вершину $G_{\tilde{\alpha}_i}$ с входной вершиной следующего за ним графа $G_{\tilde{\alpha}_{i+1}}$ (за $G_{\tilde{\alpha}_{2^k-1}}$ следует $G_{\tilde{\alpha}_0}$). В случае, если n' — четно, подразбиваем каждое добавленное ребро новой вершиной на две равные части. Легко проверить, что G' удовлетворяет перечислинным выше условиям 1-3. Любой граф, получаемый из G' движением, также называется графом Серпинского. Обозначим через $\rho_G(\tilde{x}, \tilde{y})$ расстояние на графе G между двумя его вершинами $\tilde{x}$ и $\tilde{y}$.

Лемма 2. *Число вершин в n^k-графе не меньше $\frac{(n+2)^k}{2^k}$.*

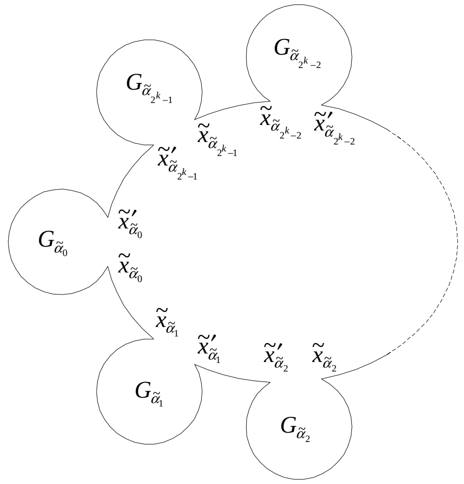

Рис. 2.

Доказательство. Установим утверждение индукцией по n. При $n = 1, 2$ оно очевидно. Пусть оно доказано для всех значений меньших n', где $n' = 2n+1$, если n' — нечетно и $n' = 2n+2$ иначе. Докажем его для n'. Из построения $(n')^k$-графа и предположения индукции видно, что число его вершин не меньше чем $2^k\frac{(n+2)^k}{2^k} = \frac{(2n+2+2)^k}{2^k} \geqslant \frac{(2n+1+2)^k}{2^k}$, что и требовалось. Лемма доказана.

Лемма 3. *Если $\tilde{x}^0$ и $\tilde{x}^1$ — начальная и конечная вершины n^k-графа G соответственно, то*

$$\rho_G(\tilde{x}^0, \tilde{x}^1) \geqslant \frac{N_k}{4^k}(n+2)^k, \text{ где } N_k = \begin{cases} 2^{k-1} - 1 & k \text{ — четное,} \\ 2^{k-1} - 2 & k \text{ — нечетное.} \end{cases}$$

Доказательство. Установим утверждение индукцией по n. При $n = 1, 2$, используя лемму 1, получаем $\rho_G(\tilde{x}^0, \tilde{x}^1) \geqslant N_k \geqslant \frac{N_k}{4^k}(n+2)^k$. Пусть утверждение доказано для значений меньших n', где $n' = 2n+1$, если n' — нечетно, и $n' = 2n+2$ иначе. Докажем его для n'. Действительно, из построения $(n')^k$-графа G и леммы 1 видно, что

$$\rho_G(\tilde{x}^0, \tilde{x}^1) \geqslant N_k \frac{(n+2)^k}{2^k} = \frac{N_k}{4^k}(2n+2+2)^k \geqslant \frac{N_k}{4^k}(2n+1+2)^k,$$

что и требовалось доказать.

Лемма 4. *Если $\tilde{x}$ — произвольная, а $\tilde{x}^1$ — конечная вершины n^k-графа G, то*

$$\rho_G(\tilde{x}, \tilde{x}^1) \geqslant \frac{N_k}{8^k}(\rho(\tilde{x}, \tilde{x}^1) + 2)^k.$$

Доказательство. Установим утверждение индукцией по n. При $n = 1, 2$ оно следует из неравенства $\rho(\tilde{x}, \tilde{x}^1) \leqslant 2$. Пусть оно справедливо для значений меньших n', где $n' = 2n+1$, если n' — нечетно, и $n' = 2n+2$ иначе. Тогда возможны два случая.

1) $\rho(\tilde{x}, \tilde{x}^1) \leqslant n$, то есть вершина $\tilde{x}^1$ находится в графе $G_{\tilde{\alpha}_p}$, $\tilde{\alpha}_p = (1, \ldots, 1)$, тогда утверждение справедливо по предположению индукции.
2) $\rho(\tilde{x}, \tilde{x}^1) > n$. В этом случае $\rho_G(\tilde{x}, \tilde{x}^1) \geqslant \rho_G(\tilde{x}_p^0, \tilde{x}^1)$, где $\tilde{x}_p^0$ — начальная вершина графа $G_{\tilde{\alpha}_p}$. По лемме 3 получаем $\rho_G(\tilde{x}_p^0, \tilde{x}^1) \geqslant \frac{N_k}{4^k}(n+2)^k = \frac{N_k}{8^k}(2n+2+2)$. Поскольку $\rho(\tilde{x}, \tilde{x}^1) \leqslant 2n+2$, то получаем $\rho_G(\tilde{x}, \tilde{x}^1) \geqslant \frac{N_k}{8^k}(\rho(\tilde{x}, \tilde{x}^1) + 2)^k$.

Лемма доказана.

Лемма 5. *Если $\tilde{x}$, $\tilde{y}$ — произвольные вершины n^k-графа G, то*

$$\rho_G(\tilde{x}, \tilde{y}) \geqslant \frac{N_k}{16^k}(\rho(\tilde{x}, \tilde{y}) + 2)^k.$$

Доказательство. Установим утверждение индукцией по n. При $n = 1, 2$ оно следует из неравенства $\rho(\tilde{x}, \tilde{y}) \leqslant 2$. Допустим, что утверждение справедливо для значений меньших n', где $n' = 2n+1$, если n' — нечетно, и $n' = 2n+2$ иначе.

Тогда возможны три случая.

1) Вершины $\tilde{x}$ и $\tilde{y}$ находятся в одном графе $G_{\tilde{\alpha}_i}$. Тогда утверждение справедливо по предположению индукции.

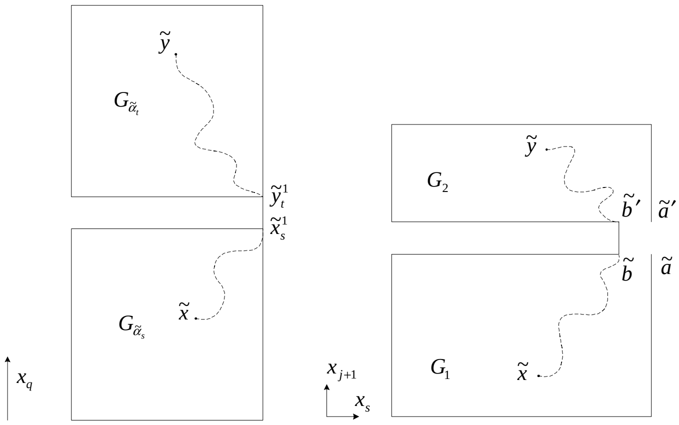

Рис. 3.

2) Вершины $\tilde{x}$ и $\tilde{y}$ находятся в графах $G_{\tilde{\alpha}_s}$ и $G_{\tilde{\alpha}_t}$ соответственно, где $\tilde{\alpha}_s$ и $\tilde{\alpha}_t$ не являются соседними наборами в цикле $\mathbf{C}_k$. Тогда кратчайший путь, соединяющий $\tilde{x}$ и $\tilde{y}$, проходит через все вершины некоторого графа $G_{\tilde{\alpha}_q}$ и по лемме 1 получаем $\rho_G(\tilde{x},\tilde{y}) \geqslant \frac{(n+2)^k}{2^k} \geqslant \frac{N_k}{16^k}(2n+2+2)^k$. Поскольку $\rho(\tilde{x},\tilde{y}) \leqslant 2n+2$, получаем требуемое неравенство.
3) Вершины $\tilde{x}$ и $\tilde{y}$ находятся в графах $G_{\tilde{\alpha}_s}$ и $G_{\tilde{\alpha}_t}$ соответственно и наборы $\tilde{\alpha}_s$ и $\tilde{\alpha}_t$ соседние в цикле $\mathbf{C}_k$. Пусть наборы $\tilde{\alpha}_s$ и $\tilde{\alpha}_t$ отличаются в q-й компоненте. Если $\max\limits_{1\leqslant i\leqslant k}|x_i-y_i|$ достигается на $i \neq q$, то либо $\rho(\tilde{x},\tilde{y}) \leqslant \rho(\tilde{x},\tilde{x}_s^1)$, либо $\rho(\tilde{x},\tilde{y}) \leqslant \rho(\tilde{y}_t^1,\tilde{x})$, где $\tilde{x}_s^1$, $\tilde{y}_t^1$ — конечные вершины графов $G_{\tilde{\alpha}_s}$ и $G_{\tilde{\alpha}_t}$ соответственно. Тогда $\rho_G(\tilde{x},\tilde{y}) \geqslant \rho_{G_{\tilde{\alpha}_s}}(\tilde{x},\tilde{x}_s^1) + \rho_{G_{\tilde{\alpha}_t}}(\tilde{y}_t^1,\tilde{y})$. По предположению индукции $\rho_{G_{\tilde{\alpha}_s}}(\tilde{x},\tilde{x}_s^1) \geqslant \frac{N_k}{16^k}(\rho(\tilde{x},\tilde{x}_s^1)+2)^k$ и $\rho_{G_{\tilde{\alpha}_t}}(\tilde{y}_t^1,\tilde{y}) \geqslant \frac{N_k}{16^k}(\rho(\tilde{y}_t^1,\tilde{y})+2)^k$. Отсюда получаем неравенство $\rho_G(\tilde{x},\tilde{y}) \geqslant \frac{N_k}{16^k}(\rho(\tilde{x},\tilde{y})+2)^k$. Пусть теперь $i = q$ и $\Delta x = \rho(\tilde{x},\tilde{x}_s^1)$, $\Delta y = \rho(\tilde{y}_t^1,\tilde{y})$, $\Delta = \max\{\Delta x, \Delta y\}$, тогда

$$\rho_G(\tilde{x},\tilde{y}) \geqslant \rho_{G_{\tilde{\alpha}_s}}(\tilde{x},\tilde{x}_s^1) + \rho_{G_{\tilde{\alpha}_t}}(\tilde{y}_t^1,\tilde{y}) \geqslant \frac{N_k}{8^k}((\Delta x+2)^k + (\Delta y+2)^k),$$

$$\rho_G(\tilde{x},\tilde{y}) \geqslant \frac{N_k}{8^k}(\Delta+2)^k \geqslant \frac{N_k}{16^k}(\Delta x+\Delta y+2+2)^k.$$

Лемма доказана.

Определим теперь понятие $n_1 \times \ldots \times n_k$-графа Серпинского, где $n_1 \leqslant n_2 \leqslant \ldots \leqslant n_k$, индукцией по совокупности параметров $(n_1, \ldots, n_k)$ и докажем, что для данных $n_1, \ldots, n_k$ и для любого s, $1 \leqslant s \leqslant k$ найдется соответствующий $n_1 \times \ldots \times n_k$-граф обладающий s-свойством.

Если $n_1 = n_2 = \ldots = n_k$, то $n_1 \times \ldots \times n_k$-графом назовем n_1^k-граф, определенный выше, его угловыми, начальной и конечной вершинами будем считать соответствующие вершины n_1^k-графа. Причем для любого s, $1 \leqslant s \leqslant k$, существует n_1^k-граф, обладающий s-свойством (его можно получить из любого n_1^k-графа применением соответствующего ортогонального преобразования, изменяющего порядок координат). Пусть теперь $n_1 = \ldots = n_j$, $n_{j+1} = n_j + \Delta n$, $\Delta n > 0$, и для всех наборов $(n_1{}', \ldots, n_k{}')$, где $n_1{}' \leqslant n_1, \ldots, n_k{}' \leqslant n_k$ уже определено понятие $n_1{}' \times \ldots \times n_k{}'$-графа и доказаны все его необходимые свойства. Тогда возможны два случая.

1) $\Delta n < n_1 + 1$, тогда $n_1 \times \ldots \times n_{j+1} \times \ldots \times n_k$-граф G полагаем равным $n_1 \times \ldots \times (n_{j+1} - \Delta n) \times \ldots \times n_k$-графу G'. Если G обладал s-свойством, то G' тоже им обладает. Угловые, начальную и конечную вершины графа G пологаем равными соответствующим вершинам графа G'.

2) $\Delta n \geqslant n_1 + 1$, тогда $n_1 \times \ldots \times n_{j+1} \times \ldots \times n_k$-графом G, обладающим s-свойством, $1 \leqslant s \leqslant k$, полагаем граф получающийся так:

   а) Объединением $n_1 \times \ldots \times (n_{j+1} - \Delta n) \times \ldots \times n_k$-графа G_1 с началом в $\tilde{x}^0 = (x_1^0, \ldots, x_k^0)$, обладающего s-свойством и $n_1 \times \ldots \times (\Delta n - 1) \times \ldots \times n_k$-графа G_2 с началом в $\tilde{a}' = (x_1^0, \ldots, x_{j+1}^0 + n_{j+1} + 1, \ldots, x_k^0)$, обладающего s'-свойством, где $s' \neq j + 1$ — номер компоненты в которой $\tilde{a}'$ отличается от некоторой смежной с ней вершины $\tilde{b}' = \tilde{a}' + \mathbf{e}_{s'}$ в G_2. Поскольку, по предположению индукции, G_2 — цикл, то смежных вершин две и хотя бы одна из них подойдет.

   б) Выбрасыванием ребер $(\tilde{a}, \tilde{b})$ и $(\tilde{a}', \tilde{b}')$.

   в) Добавлением новых ребер $(\tilde{a}, \tilde{a}')$, $(\tilde{b}, \tilde{b}')$.

Здесь $\tilde{a} = \tilde{a}' - \mathbf{e}_{j+1}$, $\tilde{b} = \tilde{b} - \mathbf{e}_{j+1}$. Угловыми вершинами графа G назывем 2^{k-1} угловые вершины графа G_1, у которых $(j+1)$-я компонента равна x^0_{j+1}, а так же 2^{k-1} угловые вершины графа G_2 с $(j+1)$-й компонентой большей $x^0_{j+1} + n_{j+1} + 1$. Начальной вершиной графа G назовем начальную вершину графа G_1, а конечной - конечную вершину графа G_2.

Замечание. Из определения $n_1 \times \ldots \times n_k$-графа G легко видеть, что если $n_{\min} = \min\limits_{1 \leqslant i \leqslant k} n_i$, $\tilde{x}$ — его угловая, а $\tilde{y}$ — произвольная вершина такая, что $\rho(\tilde{x}, \tilde{y}) \leqslant n_{\min}$, то $\rho_G(\tilde{x}, \tilde{y}) = \rho_{G'}(\tilde{x}, \tilde{y})$, где G' — некоторый $(n_{\min})^k$-граф, являющийся подграфом G.

Лемма 6. *Если $\tilde{x}$ и $\tilde{y}$ произвольные вершины $n_1 \times \ldots \times n_k$-графа G, то*

$$\rho_G(\tilde{x}, \tilde{y}) \geqslant \frac{N_k}{32^k} (\rho(\tilde{x}, \tilde{y}) + 2)^k.$$

Доказательство. Установим утверждение индукцией по построению графа G. Если $n_1 = \ldots = n_k$ или $n_1 = \ldots = n_j$, $n_{j+1} = n_j + \Delta n$, $\Delta n < n_1 + 1$, то утверждение следует из леммы 5.

В случае, если $\Delta n \geqslant n_1 + 1$ и граф G получается объединением $n_1 \times \ldots \times (n_{j+1} - \Delta n) \times \ldots \times n_k$-графа G_1 и $n_1 \times \ldots \times (\Delta n - 1) \times \ldots \times n_k$-графа G_2, тогда, если $\tilde{x}$ и $\tilde{y}$ находятся внутри одного из этих графов, то утверждение будет справедливо по предположению индукции. Пусть теперь $\tilde{x}$ находится в G_1, а $\tilde{y}$ в G_2 (рис. 3) и $\Delta x = \rho(\tilde{x}, \tilde{a})$, $\Delta y = \rho(\tilde{y}, \tilde{a}')$, $\Delta = \max\{\Delta x, \Delta y\}$. Поскольку $\rho_G(\tilde{x}, \tilde{y}) \geqslant \rho_{G_1}(\tilde{x}, \tilde{a}) + \rho_{G_2}(\tilde{y}, \tilde{a}')$, используя замечание и лемму 5, получим, что

$$\rho_G(\tilde{x}, \tilde{y}) \geqslant \frac{N_k}{16^k} (\Delta x + 2)^k + \frac{N_k}{16^k} (\Delta y + 2)^k \geqslant$$
$$\geqslant \frac{N_k}{16^k} (\Delta + 2)^k \geqslant \frac{N_k}{32^k} (\Delta x + \Delta y + 2 + 2)^k.$$

Лемма доказана.

Рассмотрим автомат $\mathfrak{A}$ без выхода диаграмма Мура которого изображена на рис. 1.

Из рисунка видно, что диаграмма имеет форму цикла. Назовем *расстоянием* между двумя состояниями автомата наименьшее расстояние между ними на этом цикле.

Лемма 7. *Для любого* $1 < l \leqslant [\frac{n}{2}]$ *существует слово* α*, переводящее* $\{q^0, q^{n-1}\}$ *в пару на расстоянии* l*, причем, кратчайшее такое слово имеет длину* ln*.*

Доказательство. Установим утверждение индукцией по l, что если $1 < l \leqslant [\frac{n}{2}]$, то существует входное слово α, переводящее пару $\{q^0, q^{n-1}\}$ в пару состояний, находящихся на расстоянии l, причем кратчайшее такое слово переведет $\{q^0, q^{n-1}\}$ в $\{q^0, q^{n-l}\}$, пройдя через все пары на расстоянии, меньшем l.

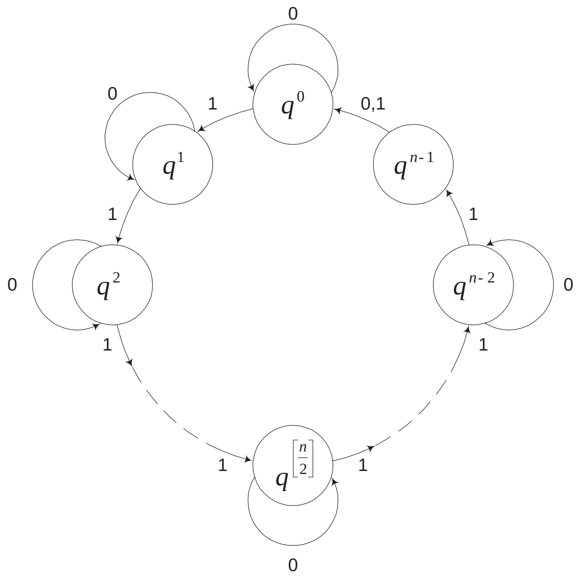

Рис. 4.

Действительно, при $l = 2$ для того, чтобы из $\{q^0, q^{n-1}\}$ попасть в $\{q^0, q^{n-2}\}$, необходимо пройти последовательно пары $\{q^0, q^1\}, \{q^1, q^2\}, \ldots, \{q^{n-2}, q^{n-1}\}$. Находясь в паре $\{q^{n-2}, q^{n-1}\}$, можно подать либо 1 и опять попасть в $\{q^0, q^{n-1}\}$, либо 0 и оказаться в $\{q^0, q^{n-2}\}$. Таким образом, кратчайшее входное слово переводящее в пару на расстоянии 2 имеет вид $0^{n-1}1$. Допустим, что утверждение верно, для l. Докажем его для $l+1$. По предположению индукции существует слово α, переводящее $\{q^0, q^{n-1}\}$ в $\{q^0, q^{n-l}\}$. Но тогда слово

$\alpha 0^{n-1}1$ переводит эту пару в $\{q^0, q^{n-l-1}\}$. С другой стороны, если β — кратчайшее слово, переводящее $\{q^0, q^{n-1}\}$ в пару на расстоянии $l+1$, то, как видно из рис. 4, для этого сначала надо попасть в некоторую пару на расстоянии l. По предположению индукции это означает, что у β существует начальный отрезок β', переводящий $\{q^0, q^{n-1}\}$ в $\{q^0, q^{n-l}\}$, пройдя через все пары состояний на расстоянии, меньшем l. Из диаграммы видно, что кратчайшее слово, переводящее $\{q^0, q^{n-1}\}$ в некоторую пару на расстоянии $l+1$, есть $0^{n-1}1$. Таким образом, $\beta = \beta' 0^{n-1}1$ и шаг индукции завершен. Лемма доказана.

Доказательство теоремы. Пусть $Q_0 = \{q_1, q_2\}$ — неупорядоченная пара r-отличимых состояний и $\alpha = a(1)a(2)\dots a(l)$ — кратчайшее слово, отличающее их. Рассмотрим последовательность пар состояний $Q_0, Q_1, \dots Q_l$, где $Q_i = \varphi(Q_0, a(1)a(2)\dots a(i)), i = \overline{1,l}$. Очевидно, что в этой последовательности $Q_i \neq Q_j$ при $i < j$, поскольку иначе слово $\alpha' = a(1)a(2)\dots a(i)a(j+1)\dots a(l)$ r-отличало бы q_1, q_2 и $|\alpha'| < |\alpha|$. Следовательно, l не превосходит числа N_r различных пар $\{(x_1, \dots, x_k), (y_1, \dots, y_k)\}$ таких, что $\rho((x_1, \dots, x_m), (y_1, \dots, y_m)) \leqslant r$. Пусть

$$B_r(q) = \{(y_1, \dots, y_k) \in \mathbb{Z}^k_{n_1,\dots,n_k} \mid 1 \leqslant \rho((x_1, \dots, x_m), (y_1, \dots, y_m)) \leqslant r\},$$

где $q = (x_1, \dots, x_k)$, тогда

$$N_r = \frac{1}{2} \sum_{q \in \mathbb{Z}^k_{n_1,\dots,n_k}} |B_r(q)| \leqslant$$
$$\leqslant \frac{(2r+1)^m}{2}(n_1+1)\cdot\ldots\cdot(n_m+1)\cdot(n_{m+1}+1)^2\cdot\ldots\cdot(n_k+1)^2,$$

поскольку $|B_r(q)| \leqslant (2r+1)^m(n_{m+1}+1)\cdot\ldots\cdot(n_k+1)$, для любого $q \in \mathbb{Z}^k_{n_1,\dots,n_k}$. Таким образом, $l \leqslant N_r \leqslant \frac{(2r+1)^m}{2}(n_1+1)\cdot\ldots\cdot(n_m+1)\cdot(n_{m+1}+1)^2\cdot\ldots\cdot(n_k+1)^2$ и следовательно $L(n_1, \dots, n_k, r) = O(r^m \cdot n_1\cdot\ldots\cdot n_m \cdot n^2_{m+1}\cdot\ldots\cdot n^2_k)$ при $n_1, \dots, n_k, r \to \infty$.

Для доказательства теоремы осталось привести пример автомата $\mathfrak{A} \in \mathcal{A}^{k,m}_{n_1,\dots,n_k}$, у которого есть два состояния с минимальной длиной r-отличающего слова по порядку равной $r^m \cdot n_1\cdot\ldots\cdot n_m \cdot n^2_{m+1}\cdot\ldots\cdot n^2_k$.

Для этого рассмотрим произвольный $n_1 \times \ldots \times n_k$-граф G и пусть V — множество его вершин. Тогда множеством состояний автомата $\mathfrak{A}$ будет $V \times \mathbb{Z}^{k-m}_{n_{m+1},\ldots,n_k}$, а входной алфавит $A = \{0,1\}$. Пусть $z_1, z_2, \ldots, z_p$, где $p = n_{m+1} \cdot n_{m+2} \cdot \ldots \cdot n_k$, — некоторым образом упорядоченная последовательность всех элементов из $\mathbb{Z}^{k-m}_{n_{m+1},\ldots,n_k}$, а $v_1, \ldots, v_q$ — цикл, проходящий через все вершины графа G, где v_1 — начальная вершина G. Рассмотрим следующую последовательность

$$(v_1, z_1), \ldots, (v_1, z_p), (v_2, z_1), \ldots, (v_2, z_p), \ldots, (v_q, z_q)$$

Обозначим ее элементы $q^0, q^1, \ldots, q^{n-1}$, где $n = pq$. Определим функцию переходов автомата $\mathfrak{A}$ так, как показано на рис. 4

Из построения автомата $\mathfrak{A}$ видно, что, если α r-отличает состояния q^0 и q^{n-1}, то $\varphi(\{q^0, q^{n-1}\}, \alpha) = \{(v, z), (v', z')\}$ и из леммы 6 следует, что $\rho_G(v, v') \geqslant \frac{N_k}{32^k}(r+2)^k$. Тогда в цикле на рис. 4 они будут находиться на расстоянии не меньшем, чем $\frac{N_k}{32^k}(r+2)^k p$, и из леммы 7 получаем

$$|\alpha| \geqslant \frac{N_k}{32^k}(r+2)^k pn = \frac{N_k}{32^k}(r+2)^k n_1 \cdot \ldots \cdot n_m \cdot n_{m+1}^2 \cdot \ldots \cdot n_k^2.$$

Таким образом, теорема полностью доказана.

Пользуясь случаем, автор хотел бы выразить признательность за помощь во время работы над статьей своему научному руководителю профессору кафедры МаТИС А.С. Подколзину и зав. кафедрой МаТИС академику В.Б. Кудрявцеву.

Список литературы

[1] Мур Э.Ф. Умозрительные эксперименты с последовательными машинами // Автоматы. М.: ИЛ, 1956. С. 179–210.

[2] Кудрявцев В.Б., Подколзин А.С., Ушчумлич Ш.М. Введение в теорию абстрактных автоматов. М.: Изд-во МГУ, 1985.

[3] Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Элементы теории автоматов. М.: Изд-во МГУ, 1978.

[4] Пантелеев П.А. Об отличимости состояний автоматов // Дискретная математика. Т. 15. Вып. 3. 2003