Об отличимости состояний автомата при искажениях на входе

П. А. Пантелеев

В статье исследуется отличимость состояний автомата при искажениях, возникающих на его входе. Вводится соответствующая функция Шеннона для длины отличающих слов в зависимости от числа состояний автомата и числа искажений на входе. Устанавливается ряд оценок для этой функции при различных значениях параметров. Изучаются понятия k-кратной отличимости, и ω-кратной отличимости. Приводится критерий ω-кратной отличимости в терминах k-кратной отличимости. Рассматривается класс кратно-приведенных автоматов и устанавливается ряд его свойств.

1. Введение

Известная работа Э. Мура [2], приведшая к созданию теории экспериментов с автоматами, опиралась на явление отличимости состояний автомата, состоящее в том, что отличимые состояния по-разному реагируют на одно и то же входное слово. Для диагностики автоматов при возможности искажения входной последовательности необходимо несколько расширить классическое понятие отличимости состояний. Мы предполагаем, что подаваемая на автомат последовательность может исказиться не более чем в k позициях. Тогда для того, чтобы гарантированно отличить два состояния мало потребовать отличимости их самой последовательностью. Необходима их отличимость всеми последовательностями, получаемыми из исходной искажением не более чем в k позициях. Пары состояний для которых существует такое слово называются k-кратно отличимыми. В работе

изучается поведение функции Шеннона длины k-кратно отличающего слова для двух состояний в классе всех автоматов с не более чем n состояниями.

Если никак не ограничивать класс автоматов, то сложность такого слова может быть экспоненциальной. В работе получены некоторые оценки функции Шеннона для этого случая. Однако существует достаточно широкий класс так называемых *кратно-приведенных* автоматов, у которых все пары состояний ω-кратно отличимы, то есть отличимы для любого k, причем длина минимального отличающего слова ограничена полиномом второй степени относительно n. В работе получено точное значения соответствующей функции Шеннона для этого класса автоматов с не более чем n состояниями.

Также установлено предельное значение k, когда из k-кратной отличимости следует ω-кратная отличимость и показана его достижимость, что дает эффективный критерий проверки ω-кратной отличимости в терминах k-кратной отличимости.

2. Определения и результаты

Обозначим через $\mathbb{N}$, $\mathbb{N}_0$ — множество натуральных и неотрицательных целых чисел соответственно.

Пусть $f(n)$, $g(n)$ — две положительные вещественные функции от натурального аргумента. Через $f(n) \sim g(n)$ и $f(n) \lesssim g(n)$ будем обозначать соответственно утверждения:

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1 \quad \text{и} \quad \overline{\lim_{n\to\infty}} \frac{f(n)}{g(n)} \leqslant 1.$$

Рассмотрим конечное непустое множество Σ, которое мы будем называть *алфавитом*, а его элементы *символами*. *Словом* длины l над Σ назовем l-элементную последовательность $a(1)a(2)\dots a(l)$ символов из Σ. Обозначим длину слова α через $|\alpha|$. Определим *конкатенацию* $\alpha\beta$ двух слов $\alpha = a(1)\dots a(l)$ и $\beta = b(1)\dots b(m)$ как слово $a(1)\dots a(l)b(1)\dots b(m)$. Легко видеть, что множество всех слов над Σ образует полугруппу относительно операции конкатенации. Доопределим эту полугруппу до моноида, добавив *пустое слово* Λ такое, что

$\alpha\Lambda = \Lambda\alpha = \alpha$ для всех слов α. Положим $|\Lambda| = 0$. Обозначим через Σ^* множество всех слов (включая пустое) над Σ. Пусть $\alpha \in \Sigma^*$, тогда полагаем $\alpha^n = \underbrace{\alpha\alpha\ldots\alpha}_{n}$, $n \in \mathbb{N}$. Считаем, что $\alpha^0 = \Lambda$.

Под *конечным детерминированным автоматом Мили* (в дальнейшем *автоматом*) будем понимать объект $\mathfrak{A} = (A, Q, B, \varphi, \psi)$, где A, Q, B — конечные непустые множества, называемые, соответственно, *входным алфавитом*, *алфавитом состояний* и *выходным алфавитом*, а $\varphi : Q \times A \to Q$ и $\psi : Q \times A \to B$ — *функции переходов* и *выходов*.

Автомат можно представлять себе как абстрактное вычислительное устройство (рис. 1) работающее в дискретном времени $t = 1, 2\ldots$. В каждый момент времени t устройство находится в состоянии $q(t) \in Q$, на его вход подается $a(t) \in A$, а на выходе появляется $b(t) \in B$. Функционирование этого устройства задается следующей системой соотношений:

$$\begin{cases} q(t+1) = \varphi(q(t), a(t)), \\ b(t) = \psi(q(t), a(t)). \end{cases} \tag{1}$$

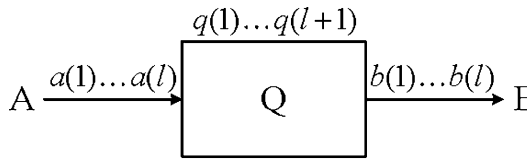

Рис. 1.

Если зафиксировать начальное состояние автомата $q(1) = q$, а на его вход подать последовательность $a(1)a(2)\ldots a(l)$, то из системы 1 однозначно определяется соответствующая выходная последовательность $b(1)b(2)\ldots b(l)$ и последовательность состояний $q(1)q(2)\ldots q(l+1)$.

Введем следующие обозначения:

$$\psi(q, a(1)\ldots a(l)) = b(l), \qquad \overline{\psi}(q, a(1)\ldots a(l)) = b(1)\ldots b(l),$$
$$\varphi(q, a(1)\ldots a(l)) = q(l+1), \quad \overline{\varphi}(q, a(1)\ldots a(l)) = q(1)\ldots q(l+1).$$

Положим также $\overline{\psi}(q, \Lambda) = \Lambda$, $\varphi(q, \Lambda) = q$. Пусть $Q' \subseteq Q$ и $\alpha \in A^*$, тогда обозначим через $\varphi(Q', \alpha)$ множество $\{\varphi(q, \alpha) \mid q \in Q'\}$.

Для задания автомата часто будет использоваться графический язык диаграмм Мура. *Диаграмма Мура* для автомата $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ это ориентированный граф вершинами которого являются состояния из Q. Для каждой вершины $q \in Q$ и входного символа $a \in A$ проводится ребро (рис. 2a) из q в $q' = \varphi(q, a)$, помеченное парой (a, b), где $b = \psi(q, a)$.

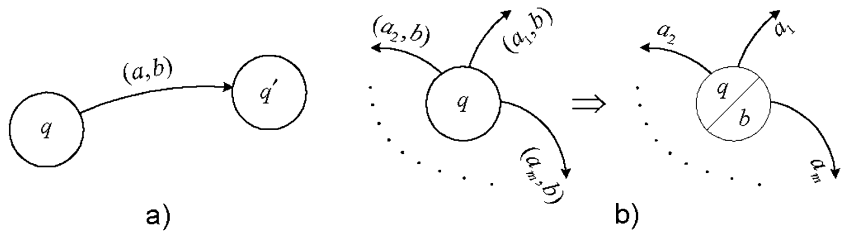

Рис. 2.

Если для некоторого состояния q функция $\psi(q, a) = b$ для всех $a \in A$, то символ b из пометок ребер выходящих из q перемещаем в q (рис. 2b).

Назовем состояния q_1, q_2 автомата $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ *отличимыми*, если существует входное слово $\alpha \in A^*$ такое, что $\overline{\psi}(q_1, \alpha) \neq \overline{\psi}(q_2, \alpha)$. Если такого слова не существует, то скажем, что состояния q_1, q_2 — *неотличимы*. Автомат *приведенный*, если все его состояния попарно отличимы. Будем говорить, что слово α *склеивает* состояния q_1, q_2, если $\varphi(q_1, \alpha) = \varphi(q_2, \alpha)$.

Везде далее при определении функции Шеннона различных видов отличимости для разных классов автоматов мы будем использовать следующую конструкцию.

Пусть S — некоторое непустое множество и на нем задана *функция сложности* $l : S \to \mathbb{N}_0$. Определим сложность класса как

$$L(S) = \max_{s \in S} l(s).$$

Например, возьмем в качестве S — множество $\mathcal{K}_n$ всех автоматов с не более чем n состояниями. Положим

$$l(\mathfrak{A}) = \max_{q_1, q_2 \in Q} l(\mathfrak{A}, q_1, q_2),$$

где $l(\mathfrak{A}, q_1, q_2)$ — минимальная длина отличающего слова для q_1, q_2 в автомате $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ и 0, если q_1, q_2 неотличимы. Тогда, согласно теореме Мура об отличимости [2, 3, 4], $L(\mathcal{K}_n) = n - 1$.

Определение 1. Рассмотрим автомат $\mathfrak{A} = (A, Q, B, \varphi, \psi)$. Назовем два его состояния q_1, q_2 *k-кратно отличимыми* словом α, если они отличимы любым словом α', $|\alpha'| = |\alpha|$, таким, что $\rho_H(\alpha, \alpha') \leqslant k$. Здесь и далее через $\rho_H(\alpha, \alpha')$ мы обозначаем количество позиций в которых отличаются слова α и α'. Два состояния q_1, q_2 *k-кратно отличимы*, если существует слово, которое их k-кратно отличает. Если такого слова нет, то q_1, q_2 называются *k-кратно неотличимыми*. Очевидно, что 0-кратная отличимость совпадает с обычной отличимостью состояний.

Пусть для состояний q_1, q_2 автомата $\mathfrak{A}$ существует k-кратно отличающее слово. Обозначим через $l^k(\mathfrak{A}, q_1, q_2)$ длину минимального такого слова и 0 если его не существует. Рассмотрим следующую функцию Шеннона:

$$L^k(\mathcal{K}_n) = \max_{\mathfrak{A} \in \mathcal{K}_n, q_1, q_2} l^k(\mathfrak{A}, q_1, q_2),$$

где максимум берется по всем автоматам $\mathfrak{A} \in \mathcal{K}_n$ и парам q_1, q_2 их состояний.

В общем случае пока удалось получить только некоторые оценки логарифма величины $L^k(\mathcal{K}_n)$.

Теорема 1. *Имеет место:*

$$n \lesssim \log_2 L^k(\mathcal{K}_n) \lesssim \frac{kn^2}{2} \text{ при } n \to \infty,\ k > 0.$$

Доказательству теоремы предпошлем несколько лемм.

Лемма 1. *Имеет место* $\log_2 L^k(\mathcal{K}_n) \lesssim \frac{kn^2}{2}$ *при* $n \to \infty$, $k > 0$.

Доказательство. Рассмотрим состояния q_1, q_2 автомата $\mathfrak{A}$ и пусть $\alpha = a(1) \dots a(l)$ — кратчайшее k-кратно отличающее слово для них. Сопоставим каждому $\alpha_i = a(1) \dots a(i)$, $1 \leqslant i \leqslant l$, объект $\mathcal{Q}_i = (\tilde{Q}_i^0, \tilde{Q}_i^1, \dots, \tilde{Q}_i^k)$, где $\tilde{Q}_i^j$ — множество всех пар состояний вида $\varphi(\{q_1, q_2\}, \alpha_i')$, где α_i' — произвольное слово такое, что $\rho_H(\alpha_i, \alpha_i') = j$ и

$\overline{\psi}(q_1, \alpha_i') = \overline{\psi}(q_2, \alpha_i')$. Заметим, что все множества $\tilde{Q}_i^j$ содержат только пары состояний, поскольку слово α_i' не может склеить q_1, q_2. Допустим в последовательности $\mathcal{Q}_0 = (\{\{q_1, q_2\}\}, \varnothing, \ldots, \varnothing), \mathcal{Q}_1, \ldots, \mathcal{Q}_l$ есть два одинаковых элемента $\mathcal{Q}_i = \mathcal{Q}_j$, $i < j$. Тогда рассмотрим слово $\gamma = \alpha_i\beta$, где $\beta = a(j+1)\ldots a(l)$ и докажем, что оно попрежнему k-кратно отличает состояния q_1, q_2. Действительно, если $\gamma' = \alpha_i'\beta'$, где $\underline{\rho}_H(\alpha_i, \alpha_i') = s$, $\rho_H(\beta, \beta') = p$, $\underline{s} + p \leqslant k$. Тогда либо $\overline{\psi}(q_1, \alpha_i') \neq \overline{\psi}(q_2, \alpha_i')$ и все доказано, либо $\overline{\psi}(q_1, \alpha_i') = \overline{\psi}(q_2, \alpha_i')$ и $\varphi(\{q_1, q_2\}\alpha_i') = \{q_1', q_2'\} \in \tilde{Q}_i^s = \tilde{Q}_j^s$. Докажем, что β' отличает q_1', q_2'. Действительно, если это не так, то существует слово α_j' такое, что $\rho_H(\alpha_j, \alpha_j') = s$, $\overline{\psi}(q_1, \alpha_j') = \overline{\psi}(q_2, \alpha_j')$ и $\varphi(\{q_1, q_2\}, \alpha_j') = \{q_1', q_2'\}$. Тогда слово $\alpha_j'\beta'$ не отличало бы q_1, q_2, несмотря на то, что оно отличается от α в $s+p \leqslant k$ позициях. Таким образом, мы пришли к противоречию и доказали, что γ k-кратно отличает состояния q_1, q_2, хотя $|\gamma| < |\alpha|$. Для доказательства леммы осталось заметить, что число элементов в последовательности $\mathcal{Q}_0, \mathcal{Q}_1, \ldots, \mathcal{Q}_l$ не превосходит $n^2 2^{kn^2/2}$, то есть $\log_2 l \lesssim \frac{kn^2}{2}$. Лемма доказана.

Лемма 2. *Если у автомата $\mathfrak{A} = (A, Q, B, \varphi, \psi)$, $|A| \geqslant 2$, $|Q| = n$, состояния q_1, q_2, k-кратно отличимы и α — кратчайшее k-кратно отличающее их слово, то $\mathfrak{A}$ можно доопределить до автомата $\mathfrak{A}' = (A, Q \cup \{q_1', q_2'\}, B, \varphi', \psi')$, добавив два новых состояния q_1', q_2', которые:*

1) *$(k+1)$-кратно отличимы;*
2) *кратчайшее $(k+1)$-отличающее их слово имеет длину большую, чем $|\alpha|$.*

Доказательство. Поскольку у автомата $\mathfrak{A}$ есть отличимые состояния, то в его выходном алфавите содержатся, по крайней мере, два различных символа b_1 и b_2. Выделим в множестве входных символов A произвольный элемент a_1. Определим функции переходов и выходов для $\mathfrak{A}'$ (рис. 3): $\varphi'(q', a) = \varphi(q, a)$, $\psi'(q, a) = \psi(q, a)$, если $q \in Q$; $\varphi'(q_1', a) = q_1$, $\varphi'(q_2', a) = q_2$, $\psi'(q_2, a_1) = b_2$ и $\psi'(q, a) = b_1$ во всех остальных случаях.

Пусть слово $\beta = a(1)a(2)\ldots a(l)$ $(k+1)$-кратно отличает состояния q_1', q_2'. Тогда слово $\gamma = a(2)\ldots a(l)$ должно k-кратно отличать q_1,

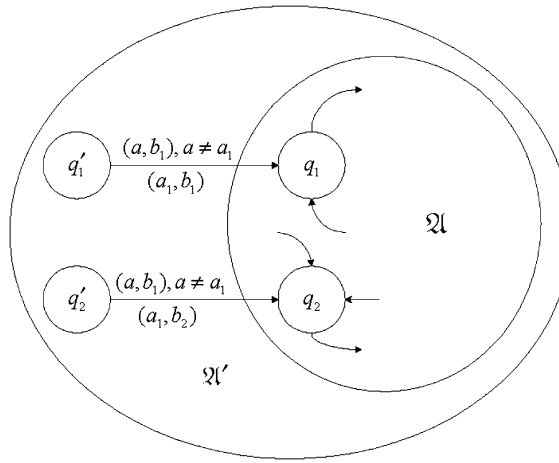

Рис. 3.

q_2. Действительно, если бы γ не k-кратно отличало q_1, q_2, то существовало бы слово γ' такое, что $\rho_H(\gamma, \gamma') \leqslant k$ и $\overline{\psi}'(q_1, \gamma) = \overline{\psi}'(q_2, \gamma')$. Тогда слово $\beta' = a_2\gamma$, где $a_2 \in A$, $a_2 \neq a_1$, не отличало бы q'_1, q'_2, но $\rho_H(\beta, \beta') \leqslant k + 1$.

Таким образом, мы доказали, что γ — k-кратно отличает q_1, q_2 и $|\beta| = 1 + |\gamma| \geqslant 1 + |\alpha|$. В тоже время, легко видеть, что слово $a_1\alpha$ является $(k+1)$-кратно отличающим для q'_1, q'_2. Действительно, пусть для некоторого слова $a\alpha'$ выполняется $\rho_H(a_1\alpha, a\alpha') \leqslant k + 1$. Тогда либо $a \neq a_1$, $\rho_H(\alpha, \alpha') \leqslant k$, либо $a = a_1$, $\rho_H(\alpha, \alpha') \leqslant k + 1$. Очевидно, что в обоих случаях слово $a\alpha'$ отличает состояния q'_1, q'_2. Лемма доказана.

Введем несколько определений

Определение 2. Назовем входной символ $a \in A$ *корректным* для подмножества Q' состояний автомата $\mathfrak{A} = (A, Q, B, \varphi, \psi)$, если для любых двух состояний $q_1, q_2 \in Q'$ из $\varphi(q_1, a) = \varphi(q_2, a)$ следует $\psi(q_1, a) \neq \psi(q_2, a)$. Таким образом, корректный символ не может склеить различные состояния из Q' не отличив их (рис. 4). В случае, если $Q' = Q$ назовем a корректным для $\mathfrak{A}$. Аналогично, входное слово $\alpha \in A^*$ назовем *корректным для* Q', если для любых двух $q_1, q_2 \in Q'$ из $\varphi(q_1, \alpha) = \varphi(q_2, \alpha)$ следует $\overline{\psi}(q_1, \alpha) \neq \overline{\psi}(q_2, \alpha)$.

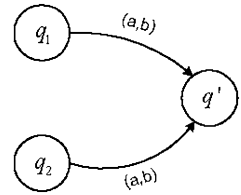

Рис. 4.

Далее нам понадобятся некоторые понятия из теории экспериментов с автоматами. Рассмотрим автомат $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ и подмножество его состояний $Q' \subseteq Q$.

Определение 3. *Простым безусловным диагностическим экспериментом* (далее п.б.д.э.) для Q' назовем такое слово α, что для любых двух различных состояний $q_1, q_2 \in Q'$ выполнено $\overline{\psi}(q_1, \alpha) \neq \overline{\psi}(q_2, \alpha)$.

Таким образом, если мы знаем диаграмму Мура автомата $\mathfrak{A}$ и подмножество возможных начальных состояний Q', но не знаем начального состояния автомата, то α позволяет определить это начальное состояние.

Определение 4. *Простым безусловным установочным экспериментом* (далее п.б.у.э) для подмножества Q' автомата $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ называется такое входное слово $\alpha \in A^*$, что для любых двух его состояний $q_1, q_2 \in Q'$ из $\overline{\psi}(q_1, \alpha) = \overline{\psi}(q_1, \alpha)$ следует, что $\varphi(q_1, \alpha) = \varphi(q_2, \alpha)$. Если $Q' = Q$, то мы говорим, что α — п.б.у.э. для $\mathfrak{A}$.

Таким образом, если мы знаем диаграмму Мура автомата $\mathfrak{A}$ и подмножество возможных начальных состояний Q', но не знаем в каком именно из них он находится, то α позволяет определить состояние автомата после эксперимента.

Замечание. Если α — п.б.у.э. для множества всех состояний автомата $\mathfrak{A}$, то любое слово вида $\beta\alpha$ также будет п.б.у.э. для $\mathfrak{A}$. Действительно, если для каких-нибудь двух различных состояний q_1, q_2 выполняется $\overline{\psi}(q_1, \beta\alpha) = \overline{\psi}(q_2, \beta\alpha)$, но $\varphi(q_1, \beta\alpha) \neq \varphi(q_2, \beta\alpha)$, то состояния $q_1' = \varphi(q_1, \beta)$, $q_2' = \varphi(q_2, \beta)$ различны и $\overline{\psi}(q_1', \alpha) = \overline{\psi}(q_2', \alpha)$, но $\varphi(q_1', \alpha) \neq \varphi(q_2', \alpha)$. Последнее противоречит тому, что α — п.б.у.э..

Обозначим через $\pi_\alpha^0(Q')$ разбиение $\{Q_1, \ldots, Q_s\}$ множества Q' по отношению отличимости словом α, то есть два состояния q_1, q_2 по-

падут в один класс разбиения только если $\overline{\psi}(q_1, \alpha) = \overline{\psi}(q_2, \alpha)$. Это разбиение мы будем называть *начальной неопределенностью* для Q' по отношению к α. Легко видеть, что слово α является п.б.д.э. для Q' в точности когда $\pi^0_\alpha(Q')$ состоит из одноэлементных множеств. Пусть также $\pi^1_\alpha(Q') = \{\varphi(Q'', \alpha) \mid Q'' \in \pi^0_\alpha(Q')\}$. Назовем $\pi^1_\alpha(Q')$ — *текущей неопределенностью* для Q' по отношению к α. Легко видеть, что слово α является п.б.у.э. для Q' в точности когда $\pi^1_\alpha(Q')$ состоит из одноэлементных множеств.

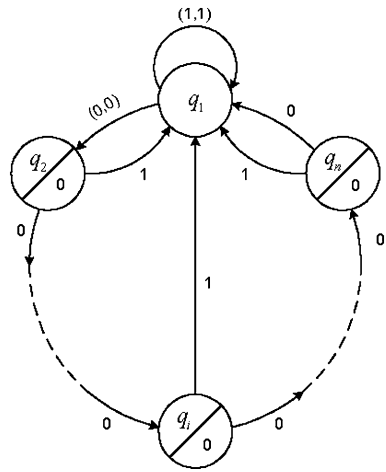

Рис. 5.

Легко показать [1], что п.б.у.э. для приведенного автомата $\mathfrak{A}$ существует всегда, в то время как п.б.д.э. удается построить не для всех приведенных автоматов. Рассмотрим следующий приведенный автомат $\mathfrak{A}$, диаграмма Мура которого изображена на рис. 5.

Легко видеть, что входной символ 1 не является корректным ни для какого трехэлементного подмножества состояний автомата $\mathfrak{A}$. Поскольку 0 не склеивает и не отличает никакие два различных состояния, то для любого трехэлементного множества состояний автомата $\mathfrak{A}$ не существует п.б.д.э.

Лемма 3. *Пусть у автомата* $\mathfrak{A} = (A, Q, B, \varphi, \psi)$, $|Q| = n$, $|B| \geqslant 2$, *для некоторого его* m*-элементного подмножества состояний* Q' *су-*

ществует п.б.д.э. и его минимальная длина равна l. Тогда можно доопределить $\mathfrak{A}$, добавив два новых состояния q_1, q_2 и $r = C_m^n$ входных символов $a_1, \ldots, a_r$ до автомата $\mathfrak{B} = (A \cup \{a_1, \ldots, a_r\}, Q \cup \{q_1, q_2\}, B, \varphi', \psi')$ такого, что q_1, q_2 1-кратно отличимы и минимальная длина 1-кратно отличающего слова для них равна $l + 1$.

Доказательство. Занумеруем все неупорядоченные пары состояний из Q': $Q_1, \ldots, Q_r$. Пусть b_1, b_2 — произвольные два различных входных символа из B. Доопределим функции переходов и выходов у автомата $\mathfrak{B}$ так, чтобы $\varphi'(\{q_1, q_2\}, a_j) = Q_j$, $\varphi'(q_i, a) = q_i$, $\varphi'(q, a_j) = q$; $\psi'(q_i, a) = b_i$, $\psi'(q_i, a_j) = b_1$, $\psi'(q, a_j) = b_1$, где $j = \overline{1, r}$, $i = \overline{1, 2}$, $q \in Q$, $a \in A$.

Докажем, что слово $\alpha = a_0\beta$, где a_0 — произвольный элемент из A, а β — кратчайший п.б.д.э. для Q', является кратчайшим 1-кратно отличающим словом для q_1, q_2. Поверим, что α 1-кратно отличает q_1, q_2. Действительно, если $\alpha' = a\beta'$, $\rho_H(\alpha, \alpha') \leqslant 1$, то либо $a = a_0$ и все доказано($\psi(q_1, a_0) \neq \psi(q_2, a_0)$), либо $a \neq a_0$, $\beta' = \beta$. В последнем случае если $a \in A$, то $\psi(q_1, a) \neq \psi(q_2, a)$ и все очевидно, если $a = a_i$, $i \in \{1, \ldots, r\}$, то $\varphi'(\{q_1, q_2\}, a_i) = Q_i$, и слово β отличает пару Q_i, а значит и α' отличает q_1, q_2.

Из определения автомата $\mathfrak{B}$ видно, что для любого 1-кратно отличающего состояния q_1, q_2 слова $\gamma = a(1)a(2)\ldots a(s)$ если мы изменим его первую букву $a(1)$ на a_i, то слово $a(2)\ldots a(s)$ должно отличать пару состояний Q_i. Тогда слово $a(2)\ldots a(s)$ должно отличать все пары состояний в Q', то есть является п.б.д.э. для Q' и $s \geqslant l + 1$. Лемма доказана.

Далее нам понадобится одна лемма, доказанная в [5].

Лемма 4. *Для любого $n > 1$ и $2 \leqslant m \leqslant \frac{n}{2}$ существует автомат $\mathfrak{A}$ с n состояниями такой, что для некоторого его m-элементного подмножества состояний существует п.б.д.э. и его минимальная длина равна C_{n-1}^{m-1}.*

Лемма 5. *Имеет место $\log_2 L^k(\mathcal{K}_n) \gtrsim n$ при $n \to \infty$.*

Доказательство. Пусть $k = 1$. По лемме 4 существует автомат $\mathfrak{A}$ с $n - 2$ состояниями у которого для некоторого подмножества состояний Q', $|Q'| = m$, есть п.б.д.э. длины $l = C_{n-3}^{m-1}$. Применив лемму 3 к

автомату $\mathfrak{A}$ мы получим автомат $\mathfrak{A}'$ с n состояниями такой, что для двух его состояний q_1, q_2 $l^1(\mathfrak{A}', q_1, q_2) \geqslant l+1$. Возьмем $m = \left[\frac{n}{2}\right]$, тогда $l = C_{n-3}^{\left[\frac{n}{2}\right]} \sim \frac{2^n}{\sqrt{n}}$ и $\log_2 l^1(\mathfrak{A}', q_1, q_2) \gtrsim n$ при $n \to \infty$. Таким образом, при $k = 1$ утверждение доказано. Допустим, что лемма верна для k. Докажем ее справедливость для $k+1$. Действительно по предположению индукции существует автомат $\mathfrak{B}$ с $n-2$ состояниями такой, что для двух его состояний q_1', q_2' выполняется $\log_2 l^k(\mathfrak{B}, q_1', q_2') \gtrsim n-2 \sim n$. Тогда по лемме 2 существует автомат $\mathfrak{B}'$ с двумя новыми состояниями q_1'', q_2'' такой, что $l^{k+1}(\mathfrak{B}', q_1'', q_2'') > l^k(\mathfrak{B}, q_1', q_2') \gtrsim n$. Лемма доказана.

Доказательство теоремы 1. Утверждение теоремы непосредственно следует из лемм 1 и 5. Теорема доказана.

Если ограничиться случаем $k = 1$, то справедлива более точная верхняя оценка величины $L^k(\mathcal{K}_n)$.

Теорема 2. *Имеет место* $\ln L^1(\mathcal{K}_n) < n \ln n$ *при* $n > 1$.

Доказательство. Пусть $\alpha = a(1)a(2)\dots a(l)$ — кратчайшее 1-кратно отличающее слово для состояний q_1, q_2 автомата $\mathfrak{A} = (A, Q, B, \varphi, \psi)$. Для доказательства леммы достаточно показать, что $|\alpha| < n^n$. Рассмотрим последовательность

$$(Q_0, \pi_0), (Q_1, \pi_1), \dots, (Q_{l-1}, \pi_{l-1}), \tag{2}$$

где $Q_0 = \{q_1, q_2\}$, $Q_i = \varphi(Q_0, \alpha_i)$, $\alpha_i = a(1)a(2)\dots a(i)$, если α_i не отличает q_1, q_2 и $Q_i = \varnothing$ иначе; π_i, $i = \overline{1, l-1}$, — разбиение множества состояний по отношению отличимости словом $\beta_i = a(i+1)a(i+2)\dots a(l)$, то есть два состояния q, q' попадают в один класс только если $\overline{\psi}(q, \beta_i) = \overline{\psi}(q', \beta_i)$. Допустим, что $|\alpha| \geqslant n^n$ Поскольку $n^n \geqslant (C_n^2 + 1)n! \geqslant (C_n^2 + 1)B_n$, где B_n — n-е число Белла, то есть число всевозможных разбиений n-элементного множества на непересекающиеся непустые подмножества, то в последовательности (2) найдутся два одинаковых элемента $(Q_i, \pi_i) = (Q_j, \pi_j)$, $i < j$. Рассмотрим слово $\gamma = \alpha_i\beta_j$ и докажем, что оно 1-кратно отличает q_1 и q_2. Для этого покажем, что любое слово $\gamma' = \alpha_i'\beta_j'$, $|\alpha_i| = |\alpha_i'|$, $|\beta_j| = |\beta_j'|$, $\rho_H(\gamma, \gamma') \leqslant 1$, отличает q_1, q_2. Возможны два случая.

1) $\rho_H(\alpha_i, \alpha_i') \leqslant 1$, $\beta_j = \beta_j'$. Тогда, либо α_i' отличает q_1, q_2 и все доказано, либо не отличает и переводит в пару состояний $Q' =$

$\varphi(Q_0, \alpha'_i)$. Причем склеить их α'_i не может, так как слово $\alpha'_i\beta_i$ обязано отличать q_1, q_2 ($\rho_H(\alpha, \alpha'_i\beta_i) \leqslant 1$). При этом β_i отличает пару состояний Q'. Вспомнив, что $\pi_i = \pi_j$ мы получаем, что и β_j отличает Q', а следовательно и слово $\gamma' = \alpha'_i\beta_j$ отличает q_1, q_2.

2) $\alpha_i = \alpha'_i$, $\rho_H(\beta_j, \beta'_j) \leqslant 1$. Тогда, либо α'_i отличает q_1, q_2 и все доказано, либо не отличает и переводит их в пару состояний Q_i. Слово α'_i не может склеить q_1, q_2 по той же причине, что и в пункте 1. Так как $\rho_H(\alpha, \alpha_j\beta'_j) \leqslant 1$ и $Q_i = Q_j \neq \varnothing$, то β'_j отличает Q_j и Q_i. Получаем, что $\gamma' = \alpha_i\beta'_j$ отличает q_1, q_2.

Теорема доказана.

Автомат, использованный для получения нижней оценки в теореме 1, имеет экспоненциальную от числа состояний мощность входного алфавита. Однако даже если ограничится классом $\mathcal{K}_{2,n,2}$ автоматов с n состояниями и двухбуквенным входным и выходным алфавитом, то, как показывает следующая теорема, нижняя оценка все равно растет быстрее чем любой полином от n.

Теорема 3. *Имеет место* $\ln L^k(\mathcal{K}_{2,n,2}) \gtrsim \sqrt{n \ln n}$ *при* $n \to \infty$.

Доказательству теоремы предпошлем лемму.

Лемма 6. *Для каждого натурального* $n > 1$ *существует автомат* $\mathfrak{A} = (\{0,1\}, Q, \{0,1\}, \varphi, \psi)$, $|Q| = n$, *такой, что у него найдутся два состояния* q_0, q_1 *для которых длина минимального* 1*-кратно отличающего слова есть* $e^{\sqrt{n \ln n}(1+o(1))}$ *при* $n \to \infty$.

Доказательство. Пусть $n \geqslant 4$ (для $n = 2, 3$ можно взять произвольный автомат у которого есть два состояния отличимые любым словом). Обозначим через p_i — i-е простое число. Найдем наибольшее такое $s = s(n)$, что

$$p_1 + \ldots + p_s + s \leqslant n - 1. \tag{3}$$

Определим автомат $\mathfrak{A}$. Положим $Q = Q_0 \cup Q_1 \cup \ldots \cup Q_s \cup Q'$, где $Q_0 = \{q_1, \ldots, q_s\}$, $Q_i = \{q_i^0, q_i^1, \ldots, q_i^{p_i - 1}\}$, $i = \overline{1, s}$ и Q' — произвольное множество из $n - p_1 - p_2 - \ldots - p_s - s$ элементов, один из которых

<table>
<tr><td colspan="3"></td><td colspan="2">$\varphi(q,a)$</td><td colspan="2">$\psi(q,a)$</td></tr>
<tr><td colspan="3"></td><td>$a=0$</td><td>$a=1$</td><td>$a=0$</td><td>$a=1$</td></tr>
<tr><td rowspan="4">q</td><td colspan="2">$q\in Q$</td><td colspan="2">q</td><td colspan="2">0</td></tr>
<tr><td rowspan="2">$q=q_i$</td><td>$i\neq s$</td><td>q_{i+1}</td><td rowspan="2">q_i^{i-s+1}</td><td colspan="2">0</td></tr>
<tr><td>$i=s$</td><td>q_0</td><td>1</td><td rowspan="2">0</td></tr>
<tr><td>$q=q_i^j$</td><td>$j\neq 0$</td><td>q_i^{j+1}</td><td>q_0</td><td>0</td></tr>
<tr><td></td><td>$j=0$</td><td colspan="2"></td><td>1</td></tr>
</table>

Таблица 1.

мы обозначим q_0. Обозначим через q_i^t, где $t\in\mathbb{Z}$ состояние $q_i^{t \bmod p_i}$. Возьмем в качестве $\mathfrak{A}$ автомат заданный в таблице 1, диаграмма Мура которого схематично изображена на рис. 6.

Заметим, что поскольку $\overline{\psi}(q_0,\beta)=0^{|\beta|}$ для любого $\beta\in\{0,1\}^*$, то отличимость q_0, q_1 эквивалентна тому, что слово $\overline{\psi}(q_1,\beta)$ содержит хотя бы одну единицу. Докажем, что любое слово α, 1-кратно отличающее q_0 и q_1, имеет длину $|\alpha|\geqslant s+p_1\cdot p_2\cdot\ldots\cdot p_s$. Сразу заметим, что α обязательно содержит 1, поскольку в противном случае, если изменить в нем первый символ на 1 мы получим слово α', которое не отличает q_0, q_1, но $\rho_H(\alpha,\alpha')=1$, чего быть не может. Покажем, что $a(1)=a(2)=\ldots=a(s)=0$. Допустим противное и пусть i_0 — такое число, что $a(1)=a(2)=\ldots a(i_0-1)=0$, $a(i_0)=1$, $1\leqslant i_0\leqslant s$. Рассмотрим два случая:

1) Пусть $i_0\neq s-1$. Тогда, как видно из определения автомата $\mathfrak{A}$, слово $a(1)a(2)\ldots a(i_0)$ не отличает q_0, q_1 и тем самым $l>i_0$. Рассмотрим слово $\alpha'=a'(1)a'(2)\ldots a'(l)$, причем $a'(i_0+1)=1$, $a'(i)=a(i)$, $i\neq i_0+1$. Тогда α' должно отличать q_0, q_1, поскольку α 1-кратно отличает q_0, q_1. Но как видно из построения автомата $\mathfrak{A}$: $\overline{\psi}(q_1,a'(1)\ldots a'(i_0+1)=0^{i_0+1}$, $\varphi(q_0,a'(1)\ldots a'(i_0+1))=\varphi(q_1,a'(1)\ldots a'(i_0+1))=q_0$, то есть слово α' не отличает q_0, q_1 и мы пришли к противоречию.
2) Пусть $i_0=s-1$. Тогда положим $\alpha'=a'(1)\ldots a'(l)$, где $a'(i_0{-}1)=1$, $a'(i)=a(i)$, $i\neq i_0{-}1$. Аналогично предыдущему пункту получаем, что с одной стороны α' должно отличать q_0, q_1 ($\rho_H(\alpha,\alpha')=1$), но с другой стороны из определения $\mathfrak{A}$ видно, что α' не отличает q_0, q_1. Опять приходим к противоречию.

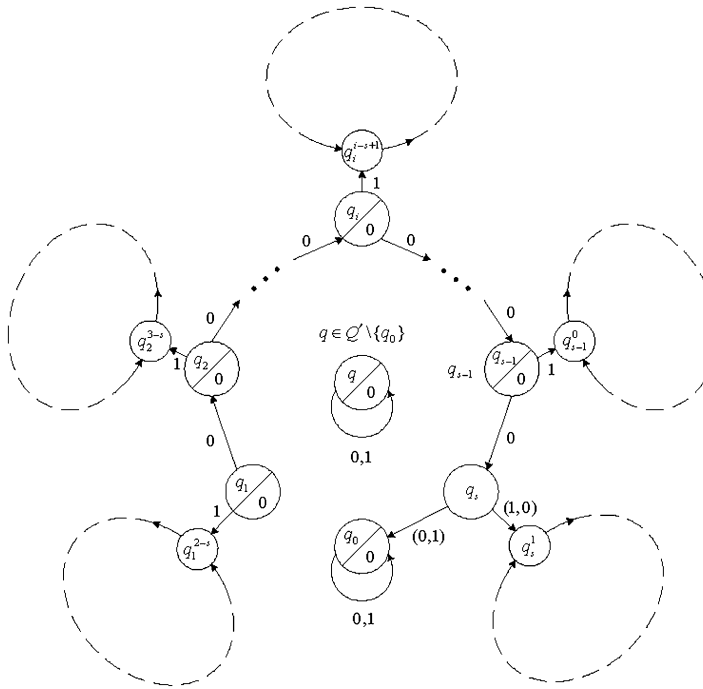

Рис. 6.

Таким образом, мы доказали, что слово α имеет вид $\alpha = 0^s\beta$, где $\beta = b(1)\dots b(m)$ содержит 1. Пусть j_0 — наименьшее такое j, что $b(j) = 1$. Докажем, что j кратно p_i для всех $i \in \{1, \dots, s\}$. Пусть $\alpha_i = 0^{i-1}10^{s-i}\beta$, $i = \overline{1,s}$. Если j не кратно p_i, то

$$\varphi(q_1, 0^{i-1}10^{s-i}0^{j-1}) = \varphi(q_i^1, 0^{j-1}) = q_i^j \neq q_i^0,$$

поэтому слово $0^{i-1}10^{s-i}0^{j-1}1$ склеивает q_0, q_1, но не различает их, а значит и α_i, $\rho_H(\alpha, \alpha_i) = 1$, не отличает q_0, q_1. Последнее противоречит тому, что α 1-кратно отличает q_0, q_1. Таким образом, мы доказали, что j кратно всем p_i, $i = \overline{1,s}$ и следовательно $j \geqslant p_1 \cdot p_2 \cdot \ldots \cdot p_s$, откуда $|\alpha| \geqslant s + p_1 \cdot p_2 \cdot \ldots \cdot p_s$. Легко проверить, что слово 0^m1, где $m = s + p_1 \cdot \ldots \cdot p_s - 1$, 1-кратно отличает q_0, q_1. Следовательно минимальная длина l_n 1-кратно отличающего слова для q_0, q_1 есть $l_n = s + p_1 \cdot \ldots \cdot p_s$. Оценим произведение $p_1 \cdot \ldots \cdot p_s$. Для этого вспомним,

что s является функцией от n и $s(n)$ есть максимальное такое s, что выполняется 3.

Пусть $x(n) = p_{s(n)+1} - 1$. Тогда

$$\ln(p_1 \cdot \ldots \cdot p_{s(n)}) = \sum_{p_i \leqslant x(n)} \ln p_i \sim x(n)$$

при $n \to \infty$. Здесь мы воспользовались известным соотношением [7] $\sum_{p_i \leqslant x} \ln p_i \sim x$ при $x \to \infty$. Оценим величину $x(n)$. Перепишем условие 3 в виде

$$\sum_{p_i \leqslant x(n)} p_i + \pi(x(n)) + 1 \leqslant n,$$

где $\pi(x)$ — число простых чисел не превосходящих x. Положим

$$F(x) = \sum_{p_i \leqslant x} p_i + \pi(x) + 1.$$

Легко видеть, что $F(x)$ — неубывающая на промежутке $[0, +\infty)$ функция. Как известно [7] $\pi(x) \sim \frac{x}{\ln x}$ при $x \to \infty$ и $p_i \sim i \ln i$ при $i \to \infty$.

Поэтому

$$\sum_{p_i \leqslant x} p_i \sim \sum_{i=1}^{\pi(x)} i \ln i \sim \frac{\pi^2(x)}{2} \ln \pi(x) \sim \frac{x^2}{2 \ln^2 x} \ln \frac{x}{\ln x} \sim \frac{x^2}{2 \ln x}$$

при $x \to \infty$. Таким образом, $F(x) \sim \frac{x^2}{2 \ln x}$ при $x \to \infty$. Поскольку $x(n)$ — максимальное такое целое x, что $F(x(n)) \leqslant n$, то получаем

$$F(x(n)) \leqslant n < F(x(n) + 1)$$

и поскольку $F(x(n)) \sim F(x(n) + 1)$, то $F(x(n)) \sim n$ при $n \to \infty$.

Таким образом,

$$\frac{x^2(n)}{2 \ln x(n)} \sim n,$$
$$x^2(n) \sim 2n \ln x(n). \tag{4}$$

Прологарифмировав последнее соотношение получаем

$$2\ln x(n) = \ln n + \ln 2 + \ln\ln x(n) + o(1),$$
$$\ln x(n) \sim \frac{1}{2}\ln n. \tag{5}$$

Используя 4 и 5 получаем

$$x^2(n) \sim 2n\ln x(n) \sim n\ln n,$$
$$x(n) \sim \sqrt{n\ln n}.$$

Таким образом, мы доказали, что $\ln(p_1 \cdot \ldots \cdot p_{s(n)}) \sim \sqrt{n\ln n}$ и тем самым $l_n = p_1 \cdot \ldots \cdot p_{s(n)} + s(n) \sim e^{\sqrt{n\ln n}(1+o(1))}$ при $n \to \infty$, что и требовалось. Лемма доказана.

Доказательство теоремы 3. При $k = 1$ утверждение является переформулировкой леммы 6. Допустим, что лемма верна для k. Докажем ее для $k+1$. Действительно, по предположению индукции существует автомат $\mathfrak{A} \in \mathcal{K}_{2,n-2,2}$ такой, что для двух его состояний q_1, q_2 выполняется $\ln l^k(\mathfrak{A}, q_1, q_2) \gtrsim \sqrt{(n-2)\ln(n-2)} \sim \sqrt{n\ln n}$. Тогда по лемме 2 существует автомат $\mathfrak{A}' \in \mathcal{K}_{2,n,2}$ с двумя новыми состояниями q_1', q_2' такой, что $l^{k+1}(\mathfrak{A}', q_1', q_2') \gtrsim \sqrt{n\ln n}$. Теорема доказана.

Определение 5. Два состояния q_1, q_2 автомата $\mathfrak{A}$ называются *ω-кратно отличимыми*, если они k-кратно отличимы для любого $k \geqslant 0$.

Теорема 4. *Если два состояния q_1, q_2 автомата $\mathfrak{A} \in \mathcal{K}_n$ k-кратно отличимы, где $k \geqslant \frac{n(n-1)}{2}$, то они ω-кратно отличимы.*

Доказательству предпошлем несколько лемм.

Лемма 7. *Если для двух различных состояний q_1, q_2 автомата $\mathfrak{A} \in K_n$ существует некорректное слово, то существует и некорректное слово α, $|\alpha| \leqslant \frac{n(n-1)}{2}$.*

Доказательство. Допустим, что утверждение не верно и $\alpha = a(1)\ldots a(l)$ — кратчайшее некорректное слово для q_1, q_2. Тогда $l > \frac{n(n-1)}{2}$ и мы рассмотрим пары состояний $Q_0 = \{q_1, q_2\}$, $Q_i = \varphi(Q_0, a(1)\ldots a(i))$, $i = 1, \ldots, l-1$. Очевидно, что найдутся целые

i и j, где $0 \leqslant i < j \leqslant n-1$ такие, что $Q_i = Q_j$. Тогда слово $\alpha' = a(1)\dots a(i)a(j+1)\dots a(l)$ — некорректно для q_1, q_2, но $|\alpha'| < |\alpha|$, что противоречиво. Лемма доказана.

Лемма 8. *Если для пары различных состояний q_1, q_2 автомата $\mathfrak{A}$ существует некорректное слово α, то q_1, q_2 не являются k-кратно отличимыми для всех $k \geqslant |\alpha|$.*

Доказательство. Пусть $\alpha = a(1)\dots a(l)$ — некорректное для состояний q_1, q_2 автомата $\mathfrak{A}$ слово. Допустим, что для q_1, q_2 существует k-кратно отличающее слово $\beta = b(1)\dots b(l')$, где $k \geqslant l$. Если $l' < l$, то положим $\beta' = a(1)\dots a(l')$, если $l' \geqslant l$, то $\beta' = a(1)\dots a(l)b(l+1)\dots b(l')$. Очевидно, что в обоих случаях β' отличается от β не более чем в k позициях и $\overline{\psi}(q_1, \beta') = \overline{\psi}(q_2, \beta')$. Таким образом, состояния q_1, q_2 не являются k-кратно отличимыми. Лемма доказана.

Далее нам понадобится лемма Хиббарда [1], касающуюся существования и сложности п.б.у.э. для подмножеств состояний приведенного автомата.

Лемма 9 (Хиббард [1]). *Для любого подмножества состояний Q', $|Q'| = k$, $k \geqslant 2$, автомата $\mathfrak{A} \in \mathcal{K}_n$ существует п.б.у.э. α, причем $|\alpha| \leqslant \frac{(2n-k)(k-1)}{2}$.*

Лемма 10. *Если все входные слова корректны для пары различных состояний q_1, q_2 автомата $\mathfrak{A} \in K_n$, то для любого целого $k \geqslant 0$ они k-кратно отличимы словом α_k, $|\alpha_k| \leqslant n - 1 + k\frac{n(n-1)}{2}$.*

Доказательство. Докажем индукцией по k. При $k = 0$ k-кратная отличимость совпадает с обычной отличимостью состояний и утверждение следует из теоремы Мура [2].

Пусть лемма верна для k и слово α_k, $|\alpha_k| \leqslant n - 1 + k\frac{n(n-1)}{2}$, k-кратно отличает q_1, q_2. Докажем ее для $k+1$. По лемме 9 существует п.б.у.э. α, $|\alpha| \leqslant \frac{n(n-1)}{2}$. для автомата $\mathfrak{A}$. Рассмотрим слово $\alpha_{k+1} = \alpha_k\alpha$, $|\alpha_{k+1}| = |\alpha_k| + |\alpha| \leqslant n - 1 + (k+1)\frac{n(n-1)}{2}$, и докажем, что оно $(k+1)$-кратно отличает состояния q_1, q_2. Действительно, пусть слово $\alpha'_{k+1} = \alpha'_k\alpha'$, где $|\alpha'_k| = |\alpha_k|$, $|\alpha'| = |\alpha|$, отличается от α_{k+1} не более чем в $(k+1)$-ой позиции. Тогда возможны два случая:

1) α'_k отличается от α_k не более чем в k позициях. Тогда $\overline{\psi}(q_1, \alpha'_k) \neq \overline{\psi}(q_2, \alpha'_k)$, поскольку α_k k-кратно отличает q_1, q_2.
2) α'_k отличается от α_k ровно в $(k+1)$ позиции. Если $\overline{\psi}(q_1, \alpha'_k) \neq \overline{\psi}(q_2, \alpha'_k)$, то все доказано. Пусть $\overline{\psi}(q_1, \alpha'_k) = \overline{\psi}(q_2, \alpha'_k)$. Рассмотрим состояния $q'_1 = \varphi(q_1, \alpha'_k)$, $q'_2 = \varphi(q_2, \alpha'_k)$. Так как $\alpha' = \alpha$ — п.б.у.э. для $\mathfrak{A}$, то $\overline{\psi}(q'_1, \alpha') \neq \overline{\psi}(q'_2, \alpha')$. Действительно, в противном случае $\overline{\psi}(q'_1, \alpha') = \overline{\psi}(q'_2, \alpha')$ и $\varphi(q'_1, \alpha') = \varphi(q'_2, \alpha')$, то есть слово α'_{k+1} — некорректное для q_1, q_2. Таким образом, мы пришли к противоречию и $\overline{\psi}(q'_1, \alpha') \neq \overline{\psi}(q'_2, \alpha')$.

Как видно в обоих случаях $\overline{\psi}(q_1, \alpha'_{k+1}) \neq \overline{\psi}(q_2, \alpha'_{k+1})$, что и требовалось доказать. Лемма доказана.

Доказательство теоремы 4. Пусть состояния q_1, q_2 автомата $\mathfrak{A} \in K_n$ k-кратно отличимы, где $k \geqslant \frac{n(n-1)}{2}$. Допустим, что существует некорректное слово для q_1, q_2. Пусть α — самое короткое такое слово. Из леммы 7 следует, что $|\alpha| \leqslant \frac{n(n-1)}{2}$. Тогда по лемме 8 получаем, что q_1, q_2 не могут быть k-кратно отличимыми. Следовательно наше предположение не верно и для q_1, q_2 все входные слова корректны. Тогда по лемме 10 состояния q_1, q_2 — k-кратно отличимы для любого целого $k \geqslant 0$, то есть ω-отличимы. Теорема доказана.

Теорема 5. *Для каждого целого n, $n \geqslant 2$, существует автомат $\mathfrak{A} \in \mathcal{K}_n$ такой, что для любого $k \in \{0, 1, \ldots, \frac{n(n-1)}{2} - 1\}$ найдется пара состояний q_1, q_2, которая k-кратно отличима, но не $(k+1)$-кратно отличима.*

Доказательство. Рассмотрим автомат $\mathfrak{A} = (\{0,1,2\}, Q, Q, \varphi, \psi)$, $Q = \{q^0, \ldots, q^{n-1}\}$, где $\psi(q, 3) = q$, $\psi(q, a) = q^0$, $a \in \{0, 1\}$, $\varphi(q, 3) = q$, $q \in Q$. Функция переходов $\varphi(q, a)$, для $a \in \{0, 1\}$ задана на диаграмме Мура, изображенной на рис. 7. В работе [6] доказывается (теорема 1), что для пары состояний $Q_0 = \{q^0, q^{[\frac{n}{2}]}\}$ существует склеивающее слово $\alpha = a(1) \ldots a(l) \in \{0,1\}^*$, $l = \frac{n(n-1)}{2}$. Причем, никакое более короткое слово этим свойством не обладает. Рассмотрим последовательность $Q_0, Q_1, \ldots, Q_{l-1}$, где $Q_i = \varphi(Q_0, a(1) \ldots a(i))$. Очевидно, что для Q_i кратчайшим склеивающим словом будет слово $\alpha_i = a(i+1) \ldots a(l)$,

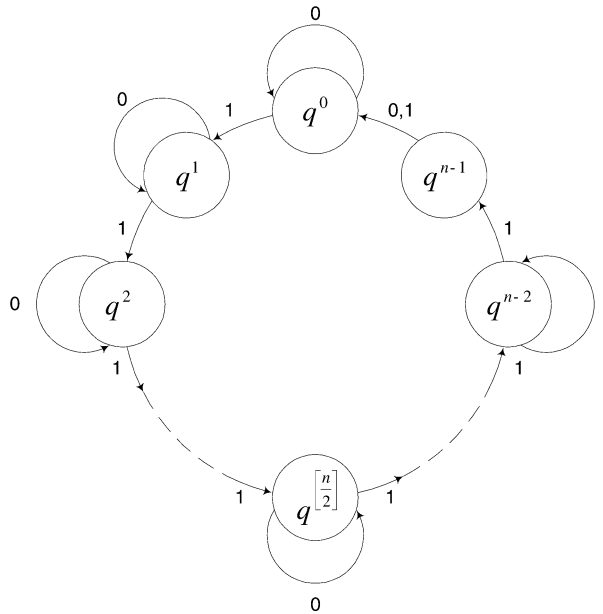

Рис. 7.

$|\alpha_i| = l - i$. Рассмотрим произвольное $k \in \{0, 1, \ldots, l-1\}$. Пара состояний Q_{l-k-1} не является $(k+1)$-кратно отличимой, поскольку слово α_{l-k-1}, $|\alpha_{l-k-1}| = k+1$, склеивает эту пару состояний и, как видно из построения автомата, не отличает ее. Таким образом, по лемме 8 пара состояний Q_{l-k-1} не является $(k+1)$-кратно отличимой. В тоже время, слово $\alpha = 3^{k+1}$ k-кратно отличает пару Q_{l-k-1}. Действительно, если α' отличается от α не более чем в k-позициях, то α' останется хотя бы одно вхождение символа 3. Тогда $\alpha' = \beta 3 \gamma$, где β не содержит вхождений символа 3. Поскольку $|\beta| < k+1$, оно не может склеить пару Q_{l-k-1}. Значит слово $\beta 3$, как видно из построения автомата, отличает эту пару. Таким образом, мы доказали, что α k-кратно отличает пару состояний Q_{l-k-1}. Теорема доказана.

При проектировании автомата мы обычно хотим быть уверены, что у него нет состояний неотличимых с точки зрения внешнего поведения. На этом пути возникло понятие приведенного автомата. Если при этом на входе автомата могут происходит искажения, то ма-

ло потребовать его приведенности. Разумно потребовать, чтобы все его состояния были попарно ω-отличимы, то есть при любом числе k искажений на входе у автомата не будет k-кратно неотличимых состояний.

Определение 6. Автомат называется *кратно-приведенным*, если любая его пара отличимых состояний 1-кратно отличима.

Как показывает следующая теорема класс $\mathcal{C}$ кратно-приведенных автоматов в точности удовлетворяет нашим требованиям.

Теорема 6. *Если автомат $\mathfrak{A}$ кратно-приведенный, то все его состояния ω-кратно отличимы.*

Доказательству предпошлем лемму.

Лемма 11. *Следующие свойства приведенного автомата $\mathfrak{A}=(A, Q, B, \varphi, \psi)$ эквивалентны*

1) *Все входные символы $a \in A$ корректны для Q.*
2) *Все входные слова $\alpha \in A^*$ корректны для Q.*
3) *Любой п.б.у.э. для $\mathfrak{A}$ является п.б.д.э. для него.*
4) *Автомат $\mathfrak{A}$ — кратно-приведенный.*

Доказательство. Докажем 1) $\Rightarrow$ 2). Допустим противное, тогда 1) выполнено, но существует такое слово α и состояния q_1, q_2, что $\varphi(q_1, \alpha) = \varphi(q_2, \alpha)$ и $\overline{\psi}(q_1, \alpha) = \overline{\psi}(q_2, \alpha)$. Рассмотрим кратчайшее его начало $\alpha' = a(1) \dots a(l)$ такое, что $\varphi(q_1, \alpha') = \varphi(q_2, \alpha')$. В силу свойства 1) $|\alpha'| > 1$. Состояния $q_1' = \varphi(q_1, a(1) \dots a(l-1))$ и $q_2' = \varphi(q_2, a(1) \dots a(l-1))$ различны в силу минимальности α'. Поэтому для пары состояний q_1', q_2' получаем $\varphi(q_1', a(l)) = \varphi(q_2', a(l))$, $\psi(q_1', a(l)) = \psi(q_2', a(l))$, что противоречит условию 1). Таким образом, наше предположение не верно и мы доказали 1) $\Rightarrow$ 2).

Докажем 2) $\Rightarrow$ 3). Пусть 2) выполнено и α — п.б.у.э. для $\mathfrak{A}$. Предположим, что α не является п.б.д.э. для $\mathfrak{A}$. Тогда для каких-нибудь различных состояний q_1, q_2 выполнено $\overline{\psi}(q_1, \alpha) = \overline{\psi}(q_2, \alpha)$, и поскольку α — п.б.у.э. это влечет за собой $\varphi(q_1, \alpha) = \varphi(q_2, \alpha)$. Таким образом, мы пришли к противоречию с пунктом 2) и доказали 2) $\Rightarrow$ 3).

Докажем 3) $\Rightarrow$ 4). Действительно, пусть q_1, q_2 — различные состояния автомата $\mathfrak{A}$. Поскольку он приведенный, то существует слово α_0, отличающее их. В силу пункта 3) и леммы 9 существует п.б.д.э. β для $\mathfrak{A}$. Тогда слово $\alpha_1 = \alpha_0\beta$ будет 1-кратно отличать состояния q_1, q_2. Действительно, если слово $\alpha_1' = \alpha_0'\beta'$, $|\alpha_0'| = |\alpha_0|$, $|\beta'| = |\beta|$, отличается от α_1 в одной позиции, то возможны два случая:

1) α_0' $=$ α_0, β' отличается от β в одной позиции. Тогда $\overline{\psi}(q_1, \alpha_0') \neq \overline{\psi}(q_2, \alpha_0')$, то есть α_1' отличает q_1, q_2.
2) α_0' отличается от α_0 в одной позиции, $\beta' = \beta$. Тогда, согласно замечанию к определению п.б.у.э., слово $\alpha_1' = \alpha_0'\beta$ — п.б.у.э. для $\mathfrak{A}$, а в силу 3) еще и п.б.д.э. для $\mathfrak{A}$. Таким образом, мы опять доказали, что α_1' отличает q_1, q_2.

Докажем 4) $\Rightarrow$ 1). Пусть q_1, q_2 — произвольная пара различных состояний автомата $\mathfrak{A}$, и a — любой входной символ. Тогда из 4) следует, что существует слово $\alpha = a(1)\dots a(l)$, которое 1-кратно отличает q_1, q_2. Рассмотрим слово $\alpha' = aa(2)\dots a(l)$, отличающееся от него не более чем в одной позиции. Оно отличает q_1 и q_2. Значит либо $\varphi(q_1, a) \neq \varphi(q_2, a)$, либо $\psi(q_1, a) \neq \psi(q_2, a)$, что и требовалось доказать. Лемма доказана.

Доказательство теоремы 6. Пусть $\mathfrak{A}$ — кратно-приведенный. Поскольку у $\mathfrak{A}$ все состояния попарно 1-кратно отличимы, то согласно лемме 11 все входные слова корректны для него. Тогда из леммы 10 следует, что все его состояния попарно ω-отличимы. Теорема доказана.

Следствие 1. *Если для автомата $\mathfrak{A} \in K_n$ существует слово, k-кратно отличающее все пары его различных состояний и $k > 0$, то всегда найдется такое слово длины не более $(k+1)\frac{n(n-1)}{2}$.*

Доказательство. Действительно, поскольку все пары состояний автомата $\mathfrak{A}$ 1-кратно отличимы, то он кратно-приведенный. Пусть β — п.б.у.э. для $\mathfrak{A}$. По лемме 9 он всегда существует и $|\beta| \leqslant \frac{n(n-1)}{2}$. Из пункта 3 леммы 11 β также п.б.д.э. для $\mathfrak{A}$. Докажем, что слово $\alpha_k = (\beta)^{k+1}$ k-кратно отличает любую пару состояний q_1, q_2 автомата $\mathfrak{A}$. Для этого рассмотрим произвольное слово $\alpha_k' = \beta_1 \dots \beta_{k+1}$,

$|\beta_i| = |\beta|$, $i = \overline{1, k+1}$, $\rho_H(\alpha'_k, \alpha_k) \leqslant k$. Очевидно, что для некоторого $s \in \{1, \ldots, k+1\}$ $\beta_s = \beta$. Тогда слово $\beta_1 \ldots \beta_{s-1}$ либо отличает q_1, q_2, либо переводит их в различные состояния (пункт 2, лемма 11). В последнем случае слово $\beta_1 \ldots \beta_{s-1}\beta$ отличает их. Таким образом, слово α_k k-кратно отличает q_1, q_2, причем $|\alpha_k| \leqslant (k+1)\frac{n(n-1)}{2}$. Следствие доказано.

Обозначим через $\mathcal{C}_n$ — множество кратно-приведенных автоматов с не более чем n состояниями. Рассмотрим для этого класса функцию Шеннона $L^k(\mathcal{C}_n)$ k-кратной отличимости двух состояний.

Теорема 7. *Имеет место равенство*

$$L^k(\mathcal{C}_n) = n - 1 + k\frac{n(n-1)}{2}.$$

Доказательство. Если автомат $\mathfrak{A} \in \mathcal{C}_n$, то согласно условию 2) из леммы 11 для любой его пары различных состояний все входные слова будут корректными. Поэтому к нему применима лемма 10 и мы доказали, что

$$L^k(\mathcal{C}_n) \leqslant n - 1 + k\frac{n(n-1)}{2}.$$

Для завершения доказательства теоремы нам осталось привести кратно-приведенный автомат и такие два его k-кратно отличимых состояния на которых достигается верхняя оценка. Рассмотрим автомат $\mathfrak{A} = (A, Q, B, \varphi, \psi)$, где $A = \{0, 1, \ldots, n-1\}$, $Q = \{q_0, q_1, \ldots, q_{n-1}\}$, $B = \{0, 1\}$, а функции переходов определена так: $\varphi(q_i, i) = q_{i+1}$, $\varphi(q_{i+1}, i) = q_i$, $i = \overline{1, n-2}$, и $\varphi(q, a) = q$ во всех остальных случаях. Функция выходов определена следующим образом: $\psi(q_{n-1}, n-1) = 1$ и $\psi(q, a) = 0$ во всех остальных случаях. Диаграмма Мура для этого автомата приведена на рис. 8. Фактически такой же автомат был введен в работе [1] для доказательства нижней оценки функции Шеннона для сложности п.б.у.э. Единственное отличие в том, что в автомате $\mathfrak{A}$ вводится дополнительный входной символ 0. В работе [1] доказывается лемма, которая без труда переносится и на автомат $\mathfrak{A}$.

Лемма 12. *Для любого входного слова α, $|\alpha| < \frac{n(n-1)}{2}$, существует такое $i \in \{1, \ldots, n-1\}$, что $\overline{\psi}(q_0, \alpha) = \overline{\psi}(q_i, \alpha)$.*

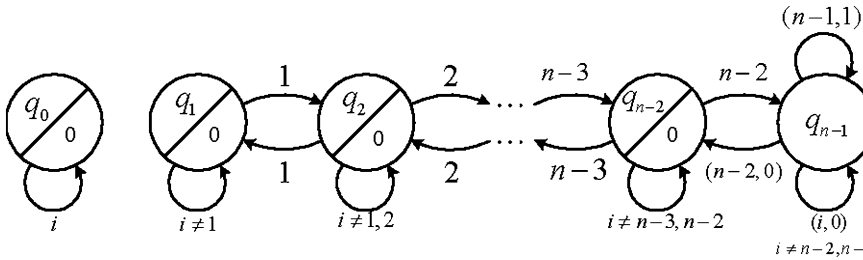

Рис. 8.

Доказательство. Пусть для некоторого слова $\alpha = a(1)\dots a(l)$, $l < \frac{n(n-1)}{2}$, утверждение не верно. Тогда $\overline{\psi}(q_0,\alpha) \neq \overline{\psi}(q_i,\alpha)$, $i = 1,\dots,n-1$. Чтобы α отличало q_0 и q_i, необходимо чтобы q_i под действием некоторого начала слова α попадало в q_{n-1}. При этом, как видно из диаграммы Мура, мы обязаны пройти через все состояния $q_i, q_{i+1},\dots,q_{n-1}$. Таким образом, для каждого j существует начало $\alpha_{ij} = a(1)\dots a(l_{ij})$ слова α, такое, что $\varphi(q_i, a(1)\dots a(l_{ij}-1)) = q_j$ и $a(l_{ij}) = j$. Докажем, что все α_{ij}, $1 \leqslant i \leqslant j \leqslant n-1$, различны. Действительно, пусть $\alpha_{ij} = \alpha_{sp}$, тогда $j = a(l_{ij}) = a(l_{sp}) = p$. Как видно из диаграммы Мура автомат $\mathfrak{A}$ — *перестановочный*, то есть для любой входной буквы $a \in A$ отображение $q \mapsto \varphi(q,a)$ задает перестановку на множестве состояний Q. Очевидно, что в этом случае и для любого входного слова $\alpha \in A^*$ отображение $q \mapsto \varphi(q,\alpha)$ задает перестановку на Q. Тогда так как $\varphi(q_i,\alpha_{ij}) = \varphi(q_s,\alpha_{ij})$, то $s = i$. Таким образом, все α_{ij}, $1 \leqslant i \leqslant j \leqslant n-1$, различные и $|\alpha| \geqslant n-1+n-2+\ldots+1 = \frac{n(n-1)}{2}$. Лемма доказана.

Лемма 13. *Пусть слово α отличает состояния q_0, q_1 автомата $\mathfrak{A}$, причем никакое собственное начало α их не отличает. Тогда для каждого i, $1 \leqslant i \leqslant n-1$ существует слово α', $\rho_H(\alpha,\alpha') \leqslant 1$, такое, что $\overline{\psi}(q_0,\alpha') = \overline{\psi}(q_1,\alpha')$ и $\varphi(q_1,\alpha') = q_i$.*

Доказательство. Пусть $\alpha = a(1)\dots a(l)$. Тогда поскольку никакое собственное начало α не отличает q_0 и q_1, то $a(l) = n-1$ и $\varphi(q,a(1)\dots a(l-1)) = q_{n-1}$. Тогда для $i = n-1$ положим $\alpha' = a(1)\dots a(l-1)0$. Очевидно, что оно удовлетворяет условию леммы.

Пусть теперь $i < n-1$. Поскольку автомат $\mathfrak{A}$ — перестановочный, то существует единственное такое j, $j > 1$, что $\varphi(q_j, \alpha) = q_i$. Пусть $s_0 = 1$, $p_0 = j$ и $q_{s_t} = \varphi(q_{s_0}, a(1)\dots a(t))$, $q_{p_t} = \varphi(q_{p_0}, a(1)\dots a(t))$, $t = 1, \dots, l$.

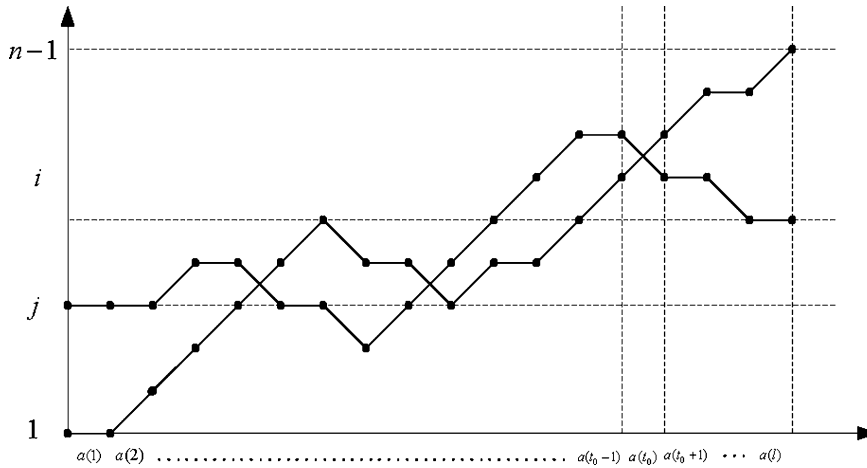

Рис. 9.

Таким образом, мы получим две целочисленные последовательности $s_0 = 1, s_1, \dots, s_{l-1}, s_l = n-1$ и $p_0 = j, p_1, \dots, p_{l-1}, p_l = i$ обладающие тем свойством, что каждый последующий член отличается от предыдущего не более чем на единицу. Причем в силу перестановочности $\mathfrak{A}$ имеем $s_t \neq p_t$, $t = 1, \dots, l$. Поскольку $s_0 - p_0 < 0$, $s_l - p_l > 0$, то существует такое t_0, что $s_{t_0} - p_{t_0} < 0$, а $s_t - p_t > 0$, для $t > t_0$ (рис. 9). Причем в силу свойств этих целочисленных последовательностей $p_{t_0} - s_{t_0} = 1$, $s_{t_0+1} - p_{t_0+1} = 1$, $s_{t_0} = p_{t_0+1}$, $s_{t_0+1} = p_{t_0}$. Рассмотрим слово $\alpha' = a(1)\dots a(t_0)0a(t_0+2)\dots a(l)$. Подавая его на состояние q_1 получим следующую последовательность состояний $q_{s_0} = q_1, q_{s_1}, \dots, q_{s_{t_0}}, q_{p_{t_0}+1}, \dots, q_{p_l} = q_j$. Очевидно, что среди $q_{p_{t_0+2}}, \dots, q_{p_l}$ нет состояния q_{n-1}. Следовательно $\overline{\psi}(q_1, \alpha') = 0^l = \overline{\psi}(q_0, \alpha')$ и $\varphi(q_1, \alpha') = q_i$. Лемма доказана.

Докажем индукцией по k, что для состояний q_0, q_1 автомата $\mathfrak{A}$ любое k-кратно отличающее слово α имеет длину

$|\alpha| \geqslant n-1+(k-1)\frac{n(n-1)}{2}$. При $k=0$ это легко видеть из диаграммы Мура. Допустим утверждение справедливо для k. Докажем его для $k+1$. Пусть $\alpha = a(1)\dots a(l)$ — минимальное по длине $(k+1)$-кратно отличающее слово для q_0, q_1 и β — минимальное по длине его начало, k-кратно отличающее состояния q_0, q_1. Тогда $\alpha = \beta\gamma$ и $|\beta| \geqslant n-1+(k-1)\frac{n(n-1)}{2}$ по предположению индукции. Легко видеть, что существует слово β', отличающееся от β в не более чем k позициях такое, что слова $\overline{\psi}(q_0,\beta')$ и $\overline{\psi}(q_1,\beta')$ отличаются в последней позиции. Действительно, в противном случае, β не было бы минимальным по длине. Очевидно, что слово β' удовлетворяет лемме 13 и для каждого i, $1 \leqslant i \leqslant n-1$, существует слово β_i, отличающееся от β' не более чем в $(k+1)$-позиции такое, что $\overline{\psi}(q_0,\beta_i) = \overline{\psi}(q_1,\beta_i)$ и $\varphi(q_1,\beta_i) = q_i$, $\varphi(q_0,\beta_i) = q_0$. Таким образом, поскольку α $(k+1)$-кратно отличает q_0, q_1, то необходимо, чтобы выполнялось $\overline{\psi}(q_0,\gamma) \neq \overline{\psi}(q_i,\gamma)$. Значит по лемме 12 получаем $|\beta| \geqslant \frac{n(n-1)}{2}$ и $|\alpha| = |\beta| + |\gamma| \geqslant n-1+k\frac{n(n-1)}{2}$. Теорема 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] Hibbard T. H. Least upper bounds on minimal terminal state experiments for two classes of sequential machines // J. Assoc. Comp. 1961. № 4. P. 601–612. [Русский перевод см. Кибернитический сборник (новая серия). 1966. Вып. 2. С. 7–23.]

[2] Moore E. F. Gedanken-experiments on sequential machines // Automata Studies. 1956. P. 129–153. [Русский перевод см. Автоматы (сб. статей). 1956. ИЛ. С. 179–210.]

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

[4] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Элементы теории автоматов. М.: Наука, 1985.

[5] Соколовский М. Н. О диагностических экспериментах с автоматами // Кибернетика. № 6. 1971. С. 44–49.

[6] Пантелеев П. А. Об отличимости состояний автоматов // Дискретная математика. 2003. Т. 15. Вып. 3. С. 76–90.

[7] Прахар К. Распределение простых чисел. М.: Мир, 1967.