ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль—август 2008. Том 15, № 4. 44–56

УДК 519.713.2

НИЖНИЕ ОЦЕНКИ ДЛИНЫ КРАТЧАЙШИХ БЕРЕЖНО СИНХРОНИЗИРУЮЩИХ СЛОВ ДЛЯ ДВУХ- И ТРЁХБУКВЕННЫХ ЧАСТИЧНЫХ АВТОМАТОВ

П. В. Мартюгин

Аннотация. Описывается понятие слов, бережно синхронизирующих частичные конечные автоматы (ЧКА). Бережная синхронизируемость ЧКА является естественным обобщением синхронизируемости детерминированных конечных автоматов. В статье доказывается, что нижние оценки величин порога бережной синхронизации для множеств двух- и трёхбуквенных автоматов с данным количеством состояний растут быстрее любого полинома от количества состояний.

Ключевые слова: автоматы, синхронизируемость.

1. Определения и история вопроса

Частичным конечным автоматом (ЧКА) называется тройка (Q, Σ, δ), где Q — конечное множество состояний, Σ — конечный алфавит и δ — частичная функция из $Q \times \Sigma$ в Q (последнее означает, что функция δ может быть не определена на некоторых парах из $Q \times \Sigma$). Заметим, что в литературе часто детерминированные конечные автоматы определяются как частичные. Обозначим через 2^Q множество всех подмножеств множества Q, а через Σ^* — свободный Σ-порождённый моноид с пустым словом λ. Функция δ может быть естественным образом индуктивно продолжена из $2^Q \times \Sigma^*$ в 2^Q. Положим $\delta(q, \lambda) = q$ для всех $q \in Q$. Пусть $q \in Q$, $w \in \Sigma^*$, $a \in \Sigma$. Если значение функции δ определено на паре (q, w) и действие буквы a определено на состоянии $\delta(q, w)$, то положим $\delta(q, wa) = \delta(\delta(q, w), a)$. Если $S \subseteq Q$, $w \in \Sigma^*$ и функция $\delta(q, w)$ определена на всех состояниях $q \in S$, то положим $\delta(S, w) = \{\delta(q, w) \mid q \in S\}$. Иногда будем обозначать величину $\delta(S, w)$ через $S.w$.

ЧКА $\mathscr{A} = (Q, \Sigma, \delta)$ называется *бережно синхронизируемым*, если существует слово $w \in \Sigma^*$ такое, что значение $\delta(Q, w)$ определено и

$|\delta(Q, w)| = 1$. Про такое слово w будем говорить, что оно *бережно синхронизирует* автомат $\mathscr{A}$. Говоря другими словами, бережно синхронизирующее слово переводит все состояния автомата в одно. Обозначим через $\mathrm{Syn}(\mathscr{A})$ множество всех слов, бережно синхронизирующих автомат $\mathscr{A}$. Очевидно, что для каждого бережно синхронизируемого автомата найдется кратчайшее бережно синхронизирующее слово.

Зафиксируем натуральное число n. Встаёт естественный вопрос: насколько длинным может быть кратчайшее бережно синхронизирующее слово для ЧКА с n состояниями. Обозначим через $\omega_{\mathrm{car}}(n)$ максимальную длину такого слова:

$$\omega_{\mathrm{car}}(n) = \max\{\min\{|u| : u \in \mathrm{Syn}(\mathscr{A})\} : \mathscr{A} = (Q, \Sigma, \delta), |Q| = n\}.$$

Величина $\omega_{\mathrm{car}}(n)$ является *порогом бережной синхронизации* множества бережно синхронизируемых автоматов с n состояниями в том смысле, что для каждого автомата из этого класса в языке всех $\omega_{\mathrm{car}}(n)$-буквенных слов найдется бережно синхронизирующее его слово, и число $\omega_{\mathrm{car}}(n)$ наименьшее с таким свойством.

Бережная синхронизируемость ЧКА является естественным обобщением синхронизируемости детерминированных конечных автоматов (ДКА) со всюду определенной функцией переходов. Пусть $\mathscr{A} = (Q, \Sigma, \delta)$ — ДКА. Слово $w \in \Sigma^*$ *синхронизирует* автомат $\mathscr{A}$, если $|\delta(Q, w)| = 1$. Гипотеза, высказанная Черни (см. [2]), утверждает, что любой синхронизируемый автомат с n состояниями может быть синхронизирован словом длины не большей чем $(n-1)^2$. Предпринималось много попыток доказать эту гипотезу, но ни одна из них не увенчалась успехом. Гипотеза доказана только для некоторых частных видов автоматов [3, 4, 8]. В общем случае имеется только кубическая верхняя оценка [11]. Соответствующая нижняя оценка доказана Черни в [2].

Почему мы выбрали для синхронизации ЧКА термин «бережная»? Известно [10], что синхронизирующие слова играют важную роль в технике. Точнее говоря, они применимы при решении задач о правильной сортировке и сборке деталей. Пусть у нас есть одинаковые детали, которые должны быть одинаково ориентированы для правильной сборки. Пусть также имеется конечное количество устройств, которые умеют переворачивать деталь некоторым образом, зависящим от её текущей ориентации. Некоторые устройства могут сломать неправильно ориентированную деталь. Рассмотрим автомат с множеством состояний, равным множеству всех ориентаций детали, и алфавитом, совпадающим с множеством устройств. Частичная функция переходов определена неразру-

шающими (или бережными) действиями устройств. Тогда бережно синхронизирующее слово задаёт порядок, в котором должны быть использованы устройства так, чтобы правильно ориентировать деталь, не разрушив её.

Бережную синхронизацию ЧКА (как и синхронизацию ДКА) удобно себе представлять как передвижение фишек, стоящих на состояниях автомата. Пусть рассматривается бережно синхронизируемый ЧКА $\mathscr{A} = (Q, \Sigma, \delta)$ и $w \in \mathrm{Syn}(\mathscr{A})$. Представим себе, что в начальный момент времени на всех состояниях автомата стоит по фишке. Пусть $a \in \Sigma$ и на состоянии $q \in Q$ стоит фишка, тогда под действием буквы a эта фишка передвигается на состояние $\delta(q, a)$. Если несколько фишек оказываются на одном состоянии, то они склеиваются в одну. Если буква $a \in \Sigma$ не определена на состоянии $q \in Q$ и на состоянии q стоит фишка, то после действия буквы a фишка «умирает». Бережно синхронизирующее слово $w \in \Sigma^*$ переводит фишки со всех состояний автомата на одно таким образом, что ни одна из них не умирает. Это еще одно объяснение термина *бережная синхронизация*.

Задача оценки величины $\omega_{\mathrm{car}}(n)$ рассматривалась М. Ито и К. Сикисима-Цудзи в [6, 7] (в этих работах величина $\omega_{\mathrm{car}}(n)$ обозначалась через $d_3(n)$). Авторы рассматривали синхронизируемость недетерминированных конечных автоматов, и проблема оценки величины $\omega_{\mathrm{car}}(n)$ в этих работах была вспомогательной. Однако были получены следующие оценки величины $\omega_{\mathrm{car}}(n)$: $\omega_{\mathrm{car}}(n) \leqslant 2^n - 2^{n-2} - 1$; если $n = 2k$, то $2^{\frac{n}{2}} + 1 \leqslant \omega_{\mathrm{car}}(n)$; если $n = 2k+1$, то $3 \cdot 2^{\frac{n-3}{2}} + 1 \leqslant \omega_{\mathrm{car}}(n)$. В [9] автором данной статьи были улучшены нижние оценки, полученные Ито. А именно, было доказано:

$$\begin{array}{ll}
\text{если } n = 3k, & \text{то } \omega_{\mathrm{car}}(n) \geqslant 3 \cdot 3^{\frac{n}{3}} - 2, \\
\text{если } n = 3k+1, & \text{то } \omega_{\mathrm{car}}(n) \geqslant 4 \cdot 3^{\frac{n-1}{3}} - 2, \\
\text{если } n = 3k+2, & \text{то } \omega_{\mathrm{car}}(n) \geqslant 6 \cdot 3^{\frac{n-2}{3}} - 2, \\
\text{если } n = 3^r, & \text{то } \omega_{\mathrm{car}}(n) \geqslant 5 \cdot 3^{\frac{n}{3}} - o(3^{\frac{n}{3}}).
\end{array}$$

Заметим, что $2^{\frac{n}{2}} < 3^{\frac{n}{3}}$ для всех $n > 0$. Поэтому нижние оценки величины $\omega_{\mathrm{car}}(n)$ из [9] превосходят оценки, полученные в работах Ито.

Все только что приведённые нижние оценки величины $\omega_{\mathrm{car}}(n)$ были получены построением серий автоматов, в которых размер алфавита растёт с увеличением количества состояний. Но кроме этого интересен вопрос: как ведёт себя длина кратчайшего бережно синхронизирующего слова для ЧКА с фиксированным размером алфавита? Аналогично величине $\omega_{\mathrm{car}}(n)$ для автоматов над k-буквенным алфавитом может быть

определена следующая величина:

$$\omega_{\text{car}}^k(n) = \max\{\min\{|u| : u \in \text{Syn}(\mathscr{A})\} : \mathscr{A} = (Q, \Sigma, \delta), |Q| = n, \Sigma = k\}.$$

Величина $\omega_{\text{car}}^k(n)$ является порогом бережной синхронизации множества бережно синхронизируемых k-буквенных автоматов с n состояниями. Встаёт естественный вопрос о поиске величин $\omega_{\text{car}}^k(n)$ для различных k и n.

Для алфавита, содержащего одну букву, ответ очевиден. Для однобуквенного ЧКА, содержащего n состояний, максимально возможная длина кратчайшего бережно синхронизирующего слова равна $n-1$, т. е. $\omega_{\text{car}}^1(n) = n-1$. Пример, обеспечивающий такую длину, представляет собой автомат $\mathscr{A} = (\{1, \ldots, n\}, \{a\}, \delta)$, где $\delta(q, a) = q + 1$ для $q \in \{1, \ldots, n-1\}$ и $\delta(n, a) = n$. Верхняя оценка следует из того, что бережно синхронизируемый ЧКА над однобуквенным алфавитом является ДКА, а для синхронизируемого ДКА $\mathscr{A} = (Q, \{a\}, \delta)$ выполняется $Q \supset Q.a \supset Q.a^2 \supset \ldots \supset Q.a^{s-1} = Q.a^s$ и $|Q.a^{s-1}| = 1$, где $s \leqslant n$. Для двух- и трёхбуквенных алфавитов не всё так очевидно. Непросто понять даже, какой будет зависимость величин $\omega_{\text{car}}^2(n)$ и $\omega_{\text{car}}^3(n)$ от n — полиномиальной или нет?

В разд. 2 построен пример, из которого становится понятным, почему величина $\omega_{\text{car}}^3(n)$ растёт быстрее, чем любой полином от n. В разд. 3 построен аналогичный пример для двухбуквенных автоматов и доказано, что величина $\omega_{\text{car}}^2(n)$ также растёт быстрее любого полинома степени n.

Введём еще несколько обозначений. Пусть $w \in \Sigma^*$, обозначим через $|w|$ длину слова w. Пусть $1 \leqslant k \leqslant |w|$, обозначим через $w[k]$ k-ю букву слова w. Пусть $1 \leqslant i < k \leqslant |w|$, обозначим через $w[i, k]$ слово $w[i] \ldots w[k]$.

2. Трёхбуквенный алфавит

Теорема 1. *Существует бесконечная последовательность* ЧКА

$$\left\{\mathscr{A}_{pfa}^3(n) \mid \mathscr{A}_{pfa}^3(n) = \{Q_n, \{a, b\}, \delta_n\}, |Q_n| = n\right\}$$

такая, что n пробегает бесконечную последовательность натуральных чисел и длина кратчайшего бережно синхронизирующего слова для автоматов $\mathscr{A}_{pfa}^3(n)$ растёт быстрее, чем любой полином от n.

Доказательство. Обозначим i-е простое число через p_i, т. е. $p_1 = 2$, $p_2 = 3$ и т. д. Построим автоматы $\mathscr{A}_{pfa}^3(n)$ для $n = \sum\limits_{i=1}^{r} p_i$. Определим ЧКА $\mathscr{A}_{pfa}^3(n) = \{Q_n, \{a, b, c\}, \delta_n\}$. Далее считаем, что число n зафиксировано,

и обозначим Q_n через Q и δ_n через δ. Положим

$$Q = \{v(i,k) \mid i \in \{1,\dots,r\}, k \in \{0, p_i - 1\}\}.$$

Определим функцию δ. Напомним, что для $q \in Q$, $\alpha \in \{a,b,c\}$ обозначаем $\delta(q,\alpha)$ через $q.\alpha$. Если для некоторых q и α значение $q.\alpha$ не определено, то будем записывать $q.\alpha = \mathrm{undef}$. Пусть $i \in \{1,\dots,r\}$, $k \in \{0, p_i - 1\}$, тогда

$$v(i,k).b = v(i,0), \quad v(i,k).a = \begin{cases} v(i,k+1), & k < p_i - 1, \\ v(i,0), & k = p_i - 1, \end{cases}$$

$$v(i,k).c = \begin{cases} v(1,1), & k = p_i - 1, \\ \mathrm{undef}, & k < p_i - 1. \end{cases}$$

Пример автомата $\mathscr{A}^3_{pfa}(n)$ для $r = 3$ (т. е. $\mathscr{A}^3_{pfa}(10)$) изображён на рис. 1. Действие буквы a изображено сплошными линиями, действие буквы b — пунктирными с короткими чёрточками, действие буквы c — пунктирными с длинными чёрточками.

Действие буквы a — это перестановка всего множества Q, которая распадается на циклы C_i, $i \in \{1,\dots,r\}$, длины которых являются последовательными простыми числами. Буква b переводит множество Q в состояния вида $v(i,0)$, т. е. в «нулевые» состояния циклов. Буква c определена только на состояниях вида $v(i, p_i - 1)$, т. е. на «последних» состояниях циклов.

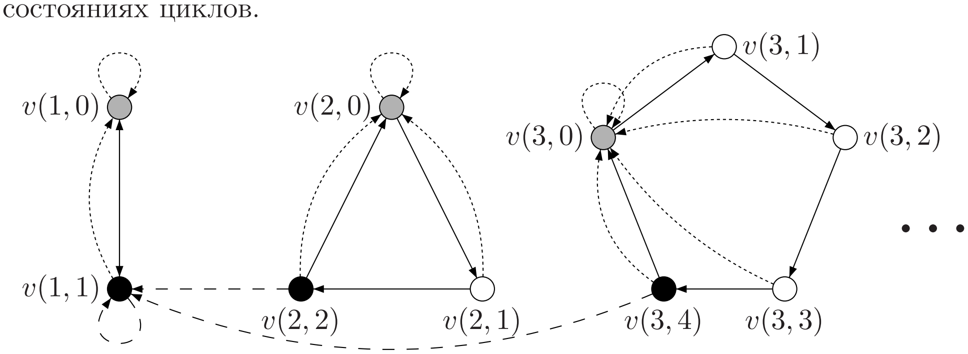

Рис. 1. Автомат $\mathscr{A}^3_{pfa}(n)$

Заметим, что $w = ba^{p_1\cdot\ldots\cdot p_r - 1}c \in \mathrm{Syn}\big(\mathscr{A}^3_{pfa}(n)\big)$. Действительно,

$$Q.b = \{v(i,0) \mid i \in \{1,\dots,r\}\}.$$

Для любого $i \in \{1,\dots,r\}$ под действием слова a^{p_i}, а значит, и под действием слова $a^{p_1\cdot\ldots\cdot p_i\cdot\ldots\cdot p_r}$ состояние $v(i,0)$ переходит само в себя. Поэтому

$$Q.ba^{p_1\cdot\ldots\cdot p_r - 1} = \{v(i, p_i - 1) \mid i \in \{1,\dots,r\}\},$$

и, следовательно, $Q.w = \{v(1,1)\}$, т. е. w бережно синхронизирует автомат $\mathscr{A}^3_{pfa}(n)$.

Докажем, что w — кратчайшее бережно синхронизирующее слово для автомата $\mathscr{A}^3_{pfa}(n)$. Пусть u — некоторое кратчайшее слово из $\mathrm{Syn}\big(\mathscr{A}^3_{pfa}(n)\big)$. Буквы a и b не могут перевести два состояния из разных циклов C_i в одно, поэтому в слове u присутствует буква c. Буква c переводит всю свою область определения в одноэлементное множество, поэтому $u[|u|] = c$ и буква c встречается в слове всего один раз. На всём множестве Q определены только буквы a и b, но $Q.a = Q$, поэтому $u[1] = b$ (иначе слово u не будет кратчайшим бережно синхронизирующим словом). Пусть $u[m] = b$ для некоторого $m \in \{1, \ldots, |u| - 1\}$. Для любого $i \in \{1, \ldots, r\}$ буквы a и b переводят состояния цикла C_i в состояния цикла C_i. Буквы c нет в слове $u[1, m-1]$, поэтому $Q.u[m-1] \cap C_i \neq \varnothing$. Следовательно,

$$Q.u[1, m-1].b = \{v(i, 0) \mid i \in \{1, \ldots, r\}\} = Q.b.$$

Из минимальности длины u следует, что буква b в слове u присутствует только на первом месте. Следовательно, $u = ba^t c$ для некоторого натурального t.

После применения буквы b в каждом из циклов C_i остаётся по одному состоянию $v(i, 0)$. Заметим, что $v(i, 0).a^x = v(i, p_i - 1)$ тогда и только тогда, когда $x \equiv p_i - 1 (\bmod p_i)$ для всех $i \in \{1, \ldots, r\}$. Мы получили систему из r линейных сравнений. Минимальным положительным решением этой системы является $x = p_1 p_2 \ldots p_r - 1$. Следовательно, $t = p_1 p_2 \ldots p_r - 1$ и слово $w = ba^{p_1 \cdot \ldots \cdot p_r - 1} c$ является кратчайшим словом из $\mathrm{Syn}\big(\mathscr{A}^3_{pfa}(n)\big)$.

Оценим скорость роста длины слова w в зависимости от количества состояний автомата $\mathscr{A}^3_{pfa}(n)$, равного $p_1 + \ldots + p_r$. Из теоремы Чебышёва о распределении простых чисел получаем

$$\alpha \cdot i \ln(i) < p_i < \beta \cdot i \ln(i),$$

где $0,9 < \alpha < \beta < 1,2$ — некоторые константы. Имеем (см. [5])

$$\lim_{r \to \infty} \left(\prod_{i=1}^{r} p_i \right)^{1/p_r} = e.$$

Следовательно, для достаточно больших r получаем

$$|u| > \prod_{i=1}^{r} p_i > e^{\alpha r \ln r}.$$

С другой стороны (см. [1]),

$$\sum_{i=1}^{r} p_i \sim \frac{1}{2} r^2 \ln r.$$

Следовательно,

$$n = \sum_{i=1}^{r} p_i < \frac{1}{2} r^{2+\varepsilon}$$

для любого $\varepsilon > 0$ и достаточно больших r. Отсюда $r > \sqrt[2+\varepsilon]{2n}$. Таким образом,

$$|u| > e^{\alpha \sqrt[2+\varepsilon]{2n} \ln(\sqrt[2+\varepsilon]{2n})} > e^{0{,}9 \sqrt[2+\varepsilon]{2n}}.$$

Поэтому длина слова w растёт быстрее любого многочлена от n. Теорема 1 доказана.

Из только что доказанной теоремы следует, что величина $\omega^3_{\mathrm{car}}(n)$ растёт быстрее любого многочлена от n. Аналогичный автомат можно построить для произвольного n, не обязательно равного сумме простых чисел, добавив несколько новых состояний, которые под действием буквы b переходят в состояние $v(1, 0)$.

3. Двухбуквенный алфавит

Серия двухбуквенных автоматов, обеспечивающая нижнюю оценку величины $\omega^2_{\mathrm{car}}(n)$, строится аналогично серии $\mathscr{A}^3_{pfa}(n)$, но конструкция является более сложной.

Теорема 2. *Существует бесконечная последовательность* ЧКА

$$\left\{\mathscr{A}^2_{pfa}(n) \mid \mathscr{A}^2_{pfa}(n) = \{Q_n, \{a, b\}, \delta_n\}, |Q_n| = n\right\}$$

такая, что n пробегает бесконечную последовательность натуральных чисел и длина кратчайшего бережно синхронизирующего слова для автоматов $\mathscr{A}^2_{pfa}(n)$ растёт быстрее любого многочлена от n.

Доказательство. Обозначим i-е простое число через p_i. Построим автоматы $\mathscr{A}^2_{pfa}(n)$ для $n = 2\sum\limits_{i=1}^{r} p_i$. Определим ЧКА $\mathscr{A}^2_{pfa}(n) = \{Q_n,\ \{a, b\}, \delta_n\}$. Далее будем считать, что число n зафиксировано, и обозначать Q_n через Q, а δ_n через δ. Положим

$$Q = \{v(m, i, k) \mid m \in \{0, 1\}, i \in \{1, \ldots, r\}, k \in \{0, p_i - 1\}\}.$$

Определим функцию δ. Пусть $i \in \{1, \ldots, r\},\ k \in \{0, p_i - 1\}$, тогда

$$v(0,i,k).b = v(0,i,0), \quad v(1,i,k).b = v(0,i,k),$$
$$v(0,i,k).a = \begin{cases} v(1,i,k+1), & k < p_i - 1, \\ v(1,i,0), & k = p_i - 1, \end{cases}$$
$$v(1,i,k).a = \begin{cases} v(1,1,1), & k = p_i - 1, \\ \text{undef}, & k < p_i - 1. \end{cases}$$

Пример автомата $\mathscr{A}^2_{pfa}(n)$ для $r = 3$ (т. е. $\mathscr{A}^2_{pfa}(20)$) изображён на рис. 2. Действие буквы a изображено сплошными линиями, действие буквы b — пунктирными. Состояния автомата могут быть изображены в виде таблицы из 2-х горизонтальных рядов и r вертикальных колонок, причем i-я колонка состоит из p_i подколонок. Обозначим m-й ряд через R_m, т. е. $R_m = \{v(m,i,k) \mid i \in \{1, \ldots, r\}, k \in \{0, p_i - 1\}\}$. Обозначим i-ю колонку через $K_i = \{v(m,i,k) \mid m \in \{0,1\}, k \in \{0, p_i - 1\}\}$.

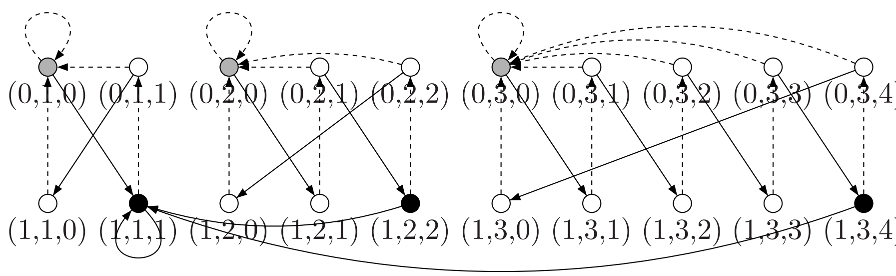

Рис. 2. Автомат $\mathscr{A}^2_{pfa}(n)$

Лемма 1. *Слово* $w = b^2(ab)^{p_1 \cdot \ldots \cdot p_r - 2}a^2$ *принадлежит* $\mathrm{Syn}\big(\mathscr{A}^2_{pfa}(n)\big)$.

Доказательство. Пусть в начале синхронизации на каждом состоянии автомата стоит по фишке. Имеем

$$Q.b^2 = \{v(0,i,0) \mid i \in \{1, \ldots, r\}\}.$$

После применения слова b^2 в каждой колонке остаётся по одной фишке, причём все фишки стоят в нулевом ряду. Слово ab переводит фишку с $v(0,i,k)$ на $v(0,i,(k+1) \bmod p_i)$ для всех $i \in \{1, \ldots, r\},\ k \in \{0, p_i - 1\}$. Поэтому для любого $i \in \{1, \ldots, r\}$ слово $(ab)^{p_1 \cdot \ldots \cdot p_r - 2}$ переведёт фишку с состояния $v(0,i,0)$ на состояние $v(0,i,p_i - 2)$. Далее, $v(0,i,p_i - 2).a = v(1,i,p_i - 1)$. Поэтому буква a определена на множестве $Q.b^2(ab)^{p_1 \cdot \ldots \cdot p_r - 2}a$ и $Q.w = v(1,1,0)$. Лемма 1 доказана.

Пусть u — некоторое кратчайшее слово из $\mathrm{Syn}\big(\mathscr{A}^2_{pfa}(n)\big)$. Докажем, что $|u| = |w|$. Выясним, какой вид может иметь слово u.

Лемма 2. *Слово u имеет вид $b^2(ab)^t a^2$ для некоторого $t > 0$.*

Доказательство. Буква a определена не на всем множестве Q, поэтому $u[1] = b$. Если $u[2] = a$, то на множестве $Q.u[1,2]$ определена только буква b, поэтому $u[3] = b$. В этом случае $Q.u[1,3] = Q.bab = Q.b$ и из слова u можно безболезненно выкинуть первые две буквы, что противоречит минимальности длины u. Следовательно, $u[1,2] = b^2$.

Пусть в начале синхронизации на каждом состоянии автомата стоит по фишке. После применения слова $u[1,2] = b^2$ все фишки оказываются на состояниях ряда R_0. Заметим, что $R_0.a \subseteq R_1$, $R_0.b \subseteq R_0$, $R_1.b \subseteq R_0$, и если все фишки находятся в ряду R_1 так, что буква a определена на всех состояниях с фишками, то под действием буквы a все фишки перейдут на состояние $v(1,1,1)$. Следовательно, для $k \geqslant 2$ множество $Q.u[1,k]$ содержится либо в R_0, либо в R_1. Фишки из разных колонок K_i могут быть склеены только под действием буквы a. При этом они все должны находиться в некотором подмножестве P ряда R_1. В этом случае $P.a = \{v(1,1,1)\}$, т. е. P переходит в одноэлементное множество. Следовательно, $Q.u[1,|u|-1] = P$ и $u[|u|] = a$.

После применения слова b^2 в каждой колонке K_i, $i \in \{1,\ldots,r\}$, находится одна фишка, и при применении букв слова u, кроме последней, эта фишка так и останется в колонке K_i. Поэтому если для некоторого $2 < k < |u|$ множество $Q.u[1,k-1]$ содержится в ряду R_0 и $u[k] = b$, то $Q.u[1,k] = Q.b^2$. В этом случае слово $u[1,k]$ может быть заменено на b^2, что противоречит минимальности длины u. Поэтому если после применения $u[1,k-1]$ фишки стоят в ряду R_0, то $u[k] = a$. Если для некоторого $2 < k < |u|$ множество $Q.u[1,k-1]$ содержится в ряду R_1, то буква a не определена на этом множестве и $u[k] = b$. Следовательно, начиная с третьей буквы слова u, буквы a и b применяются по очереди до тех пор, пока не появится возможность применить букву a, в момент, когда фишки находятся в ряду R_1. Следовательно, слово u имеет вид $b^2(ab)^t a^2$ для некоторого t. Лемма 2 доказана.

Лемма 3. $u = b^2(ab)^{p_1\cdot\ldots\cdot p_r - 2}a^2 = w$.

Доказательство. После применения слова b^2 в каждой из колонок K_i, $i \in \{1,\ldots,r\}$, остаётся по одной фишке, стоящей на состоянии $v(0,i,0)$. Заметим, что $v(0,i,0).(ab)^x a = v(1,i,p_i - 1)$ тогда и только тогда, когда $x \equiv p_i - 2 (\operatorname{mod} p_i)$ для всех $i \in \{1,\ldots,r\}$. Мы получили систему из r сравнений. Минимальным положительным решением этой системы является $x = p_1 p_2 \ldots p_r - 2$. Следовательно, $t = p_1 p_2 \ldots p_r - 2$ и слово $w = b^2(ab)^{p_1\cdot\ldots\cdot p_r - 2}a^2$ является кратчайшим в $\mathrm{Syn}(\mathscr{A}^2_{pfa}(n))$. Лемма 3 доказана.

Оценим скорость роста длины слова w в зависимости от числа состояний автомата $\mathscr{A}^2_{pfa}(n)$, равного $2(p_1 + \ldots + p_r)$. Из теоремы Чебышёва о распределении простых чисел получаем

$$\alpha \cdot i \ln(i) < p_i < \beta \cdot i \ln(i),$$

где $0,9 < \alpha < \beta < 1,2$ — некоторые константы. Имеем (см. [5])

$$\lim_{r\to\infty} \left(\prod_{i=1}^{r} p_i \right)^{1/p_r} = e.$$

Следовательно, для достаточно больших r получаем

$$|u| > 2 \cdot \prod_{i=1}^{r} p_i > 2 \cdot e^{\alpha r \ln r}.$$

С другой стороны (см. [1]),

$$\sum_{i=1}^{r} p_i \sim \frac{1}{2} r^2 \ln r.$$

Значит,

$$n = 2 \cdot \sum_{i=1}^{r} p_i < r^{2+\varepsilon}$$

для любого $\varepsilon > 0$ и достаточно больших r. Отсюда получаем $r > \sqrt[2+\varepsilon]{n}$. Таким образом,

$$|u| > 2e^{\alpha \sqrt[2+\varepsilon]{n} \ln(\sqrt[2+\varepsilon]{2n})} > 2e^{0,9 \sqrt[2+\varepsilon]{n}}.$$

Следовательно, длина слова w растёт быстрее любого полинома от n. Теорема 2 доказана.

Из теоремы 2 следует, что величина $\omega^2_{\mathrm{car}}(n)$ растёт быстрее любого полинома от n. Аналогичный автомат можно построить для произвольного n, не обязательно равного удвоенной сумме простых чисел, добавив несколько новых состояний, которые под действием буквы b переходят в состояние $v(0,1,0)$. Заметим, что длина кратчайшего бережно синхронизирующего слова для автомата $\mathscr{A}^2_{pfa}(n)$ меньше аналогичной длины для автомата $\mathscr{A}^3_{pfa}(n)$ с тем же количеством состояний.

4. Компьютерные эксперименты

При малых значениях числа n автомат $\mathscr{A}^2_{pfa}(n)$ даёт слишком маленькую длину кратчайшего бережно синхронизирующего слова. Поэтому были проведены компьютерные эксперименты по поиску максимально возможной длины такого слова. Для $n = 2, 3, 4, 5$ максимальную длину слова дали автоматы из известной серии Черни (см. [2]) со всюду определенной функцией переходов. Функция переходов автомата Черни $\mathscr{C} = (Q, \{a, b\}, \delta)$ задаётся следующим образом: для $i \in \{1, \dots, n-1\}$

$$\delta(i, b) = i + 1, \ \ \delta(i, a) = i, \ \ \delta(n, a) = \delta(n, b) = 1.$$

Длина кратчайшего синхронизирующего слова для автомата Черни с n состояниями равна $(n-1)^2$.

Для $n > 5$ была построена другая серия двухбуквенных ЧКА, которая при малых n даёт оптимальную оценку величины $\omega^2_{\mathrm{car}}(n)$. Рассмотрим для произвольного натурального n автомат $\mathscr{B}^2_{pfa}(n) = (Q, \{a, b\}, \delta)$. Пусть $Q = \{0, \dots, n-1\}$. Определим функцию δ. Для $i \in \{1, \dots, n-2\}$

$$\delta(i, a) = i, \ \ \delta(i, b) = i + 1, \ \ \delta(0, a) = \delta(0, b) = 1,$$

$$\delta(n-1, a) = 0, \ \ \delta(n-1, b) = \mathrm{undef}.$$

Автомат $\mathscr{B}^2_{pfa}(n)$ изображён на рис. 3. Буква b определена на всех состояниях, буква a не определена на состоянии $n-1$. В табл. 1 приведены длины кратчайших бережно синхронизирующих слов для $\mathscr{B}^2_{pfa}(n)$ при малых n.

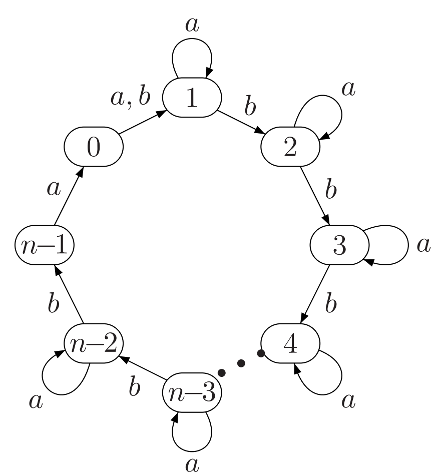

Рис. 3. Автомат, $\mathscr{B}^2_{pfa}(n)$

Таблица 1.

Длины кратчайших слов из $\mathrm{Syn}\big(\mathscr{B}^2_{pfa}(n)\big)$

n	6	7	8	9	10	11	12
Длина слова	26	39	55	73	93	116	141

Несложно показать, что слово

$$w = a^2b(ab)^{n-3}a^2b^2(ab)^{n-4}a^2b^3(ab)^{n-5}\dots a^2b^{n-3}(ab)a^2$$

будет бережно синхронизировать автомат $\mathscr{B}^2_{pfa}(n)$, поэтому длина кратчайшего слова из $\mathrm{Syn}\big(\mathscr{B}^2_{pfa}(n)\big)$ не превосходит $\frac{(n-2)(3n-5)}{2}$ (хотя на самом деле она меньше), т. е. является полиномом от n. Поэтому при больших n кратчайшее слово из $\mathrm{Syn}(\mathscr{A}^2_{pfa}(n))$ будет длиннее, чем кратчайшее слово из $\mathrm{Syn}\big(\mathscr{B}^2_{pfa}(n)\big)$. Однако полный перебор всех двухбуквенных ЧКА с не более чем 8 состояниями показал, что автомат $\mathscr{B}^2_{pfa}(n)$ даёт максимально возможную длину кратчайшего бережно синхронизирующего слова среди автоматов с n состояниями для $n = 6, 7, 8$. Для $n > 8$ перебрать все ЧКА не удалось, однако можно предположить, что для n, не намного превосходящих 8, автомат $\mathscr{B}^2_{pfa}(n)$ будет по-прежнему обеспечивать максимум длины кратчайшего бережно синхронизирующего слова.

ЛИТЕРАТУРА

1. **Bach E., Shallit J.** Algorithmic number theory, Vol. 1: Efficient Algorithms. — Cambridge, MA: MIT Press, 1996. — 506 p.
2. **Černý J.** Poznámka k homogénnym eksperimentom s konecnými avtomatami // Mat.-Fyz. Cas. Slovensk. Akad. Vied. — 1964. — Vol. 14. — P. 208–216.
3. **Dubuc L.** Sur les automates circulaires et la conjecture de Černý // RAIRO Inform. Theor. Appl. — 1998. — Vol. 32. — P. 21–34.
4. **Eppstein D.** Reset sequences for monotonic automata // SIAM J. Comput. — 1990. Vol. 19. — P. 500–510.
5. **Finch S. R.** Mathematical constants. — Cambridge: Cambridge University Press, 2003. — 602 p.
6. **Ito M.** Algebraic theory of automata and languages. — Singapore: World Scientific, 2004. — 199 p.
7. **Ito M., Shikishima-Tsuji K.** Some results on directable automata // Theory is forever. Essays dedicated to Arto Salomaa on the occasion of his 70th birthday. — Berlin; Heidelberg; New York: Springer-Verl., 2004. — P. 125–133. — (Lect. Notes Comp. Sci.; Vol. 3113).

8. **Kari J.** Synchronizing finite automata on Eulerian digraphs // Math. foundations comput. Sci. 26th Internat. symp. (Marianske Lazne, 2001). — P. 432–438. — (Lect. Notes Comput. Sci.; Vol. 2136).
9. **Martyugin P. V.** Lower bounds for length of shortest carefully synchronizing words // CSR 2006, Workshop on Words and Automata. CD Proceedings. — St. Petersburg, 2006.
10. **Natarajan B. K.** Some paradigms for the automated design of parts feeders // Internat. J. Robotics Research. — 1989. — Vol. 8, N 6. — P. 89–109.
11. **Pin J.-E.** On two combinatorial problems arising from automata theory // Ann. Discrete Math. — 1983. — Vol. 17. — P. 535–548.

Мартюгин Павел Владимировaич,
e-mail: martugin@mail.ru

Статья поступила
18 апреля 2008 г.

Переработанный вариант —
13 мая 2008 г.