Ан. А. Мучник, К. Ю. Горбунов, Алгоритмические аспекты декомпозиции и эквивалентности конечнозначных преобразователей, *Пробл. передачи информ.*, 2015, том 51, выпуск 3, 70–92

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 51 **2015** **Вып. 3**

УДК 621.391.1 : 519.7

© 2015 г. **Ан.А. Мучник**, **К.Ю. Горбунов**[1]

АЛГОРИТМИЧЕСКИЕ АСПЕКТЫ ДЕКОМПОЗИЦИИ И ЭКВИВАЛЕНТНОСТИ КОНЕЧНОЗНАЧНЫХ ПРЕОБРАЗОВАТЕЛЕЙ

Изучаются алгоритмические вопросы декомпозиции конечнозначного преобразователя в объединение однозначных и вложенности произвольного преобразователя в конечнозначный. Предлагаются алгоритмы, частично улучшающие оценки эффективности известных аналогичных алгоритмов.

§ 1. Введение

В настоящей статье исследуются алгоритмические вопросы декомпозиции конечнозначного преобразователя в объединение однозначных и вложенности произвольного преобразователя в конечнозначный. Эти вопросы изучались в работах Вебера [1–4], а также Сакаровича и де Соузы [5–8]. Там была доказана полиномиальная разрешимость вопроса о конечнозначности преобразователя, возможность декомпозиции конечнозначного преобразователя в объединение однозначных, предложен алгоритм проверки вложенности произвольного преобразователя в конечнозначный. Мы предлагаем более простые конструкции, частично улучшающие оценки предыдущих авторов. Полученные в результате декомпозиции однозначные преобразователи имеют размер порядка одной экспоненты от $\mathrm{poly}(n)$, где n – размер данного конечнозначного преобразователя; проверка вложенности произвольного преобразователя в конечнозначный производится с оценкой на размер используемой памяти в одну экспоненту. Заметим, что в [5,6] соответствующая оценка имеет порядок одной экспоненты не только от n, но и от k, где k – значность данного преобразователя (там k считается константой). Учитывая, что само k может быть эспоненциальным от n, эта оценка имеет порядок двух экспонент от n. Наша оценка не содержит k в показателе экспоненты, улучшая таким образом предыдущие. То же самое относится к проблеме проверки вложенности произвольного преобразователя в конечнозначный, которая в работе [8] решается с оценкой на размер памяти порядка $\exp(\mathrm{poly}(n,k))$, тогда как наша оценка имеет порядок $\exp(\mathrm{poly}(n))$. С другой стороны, в конструкциях из [4–6] число однозначных преобразователей равно значности данного конечнозначного преобразователя, что не следует из нашей конструкции. Таким образом, в каждой конструкции есть свои преимущества. Отметим также работу [9], содержащую подробное изложение теории автоматов и преобразователей.

В § 2 даются основные определения, примеры и утверждения, вводящие читателя в тему статьи. В § 3 излагаются конструкции, лежащие в основе декомпозиции конечнозначного преобразователя. В § 4 проводится сама декомпозиция. В § 5 рассматриваются вопросы о том, на какой минимальной длине входа и выхода может проявиться невложенность одного конечнозначного преобразователя в другой. Наконец, в § 6 приводятся результаты об алгоритмической проверке этой невложенности.

[1] Исследование выполнено в ИППИ РАН за счет гранта Российского научного фонда (проект № 14-50-00150).

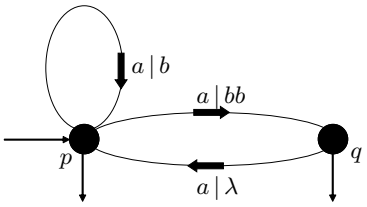

Рис. 1. Двузначный преобразователь: входу из i букв a соответствуют два выхода – из i букв b и из $(i+1)$ букв b

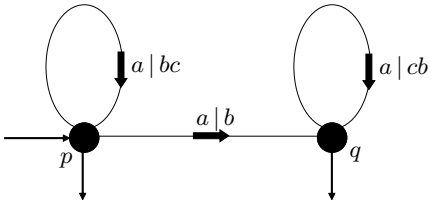

Рис. 2. Двузначный преобразователь: входу из i букв a соответствуют выходы из чередующихся букв b и c – оба выхода начинаются с b, один кончается на c, другой – на b

§ 2. Конечнозначные преобразователи

Конечным недетерминированным преобразователем $\mathfrak{A}$ называется шестерка $\langle A, B, Q, Q_0, F, \delta\rangle$, где A – (конечный) входной алфавит, B – выходной алфавит, Q – конечное множество состояний, $Q_0 \subseteq Q$ – множество начальных состояний, $F \subseteq Q$ – множество заключительных состояний, δ – множество переходов. Каждый переход – это четверка $\langle q_1, a, v, q_2\rangle$. Здесь q_1 – состояние до перехода, q_2 – состояние после перехода, $a \in A \cup \{\lambda\}$ (λ – пустое слово) – вход перехода, $v \in B^*$ – выход перехода. Будем представлять $\mathfrak{A}$ ориентированным графом, вершины которого являются состояниями, а ребра – переходами. Каждое ребро помечено входом и выходом соответствующего перехода. Путями в этом графе будем называть ориентированные пути. Слово, полученное конкатенацией входов вдоль некоторого пути l, назовем входом пути l и обозначим через $\mathrm{in}(l)$, а полученное конкатенацией выходов назовем выходом пути l и обозначим через $\mathrm{out}(l)$. Путь, начинающийся в начальном состоянии и заканчивающийся в заключительном, будем называть допускающим. Графиком $\Gamma(\mathfrak{A})$ преобразователя $\mathfrak{A}$ назовем множество пар $\langle u, v\rangle$, таких что $u = \mathrm{in}(l)$, $v = \mathrm{out}(l)$ для некоторого допускающего пути l. Будем говорить, что преобразователь $\mathfrak{A}_1$ вложен в преобразователь $\mathfrak{A}_2$, если $\Gamma(\mathfrak{A}_1) \subseteq \Gamma(\mathfrak{A}_2)$. Преобразователи $\mathfrak{A}_1$ и $\mathfrak{A}_2$ назовем эквивалентными, если $\Gamma(\mathfrak{A}_1) = \Gamma(\mathfrak{A}_2)$. Размером $|\mathfrak{A}|$ преобразователя $\mathfrak{A}$ будем называть сумму числа его состояний, переходов и длин их выходов. Очевидно, что по преобразователю $\mathfrak{A}$ можно за полиномиальное от $|\mathfrak{A}|$ время построить эквивалентный ему преобразователь, в котором через любое состояние проходит хотя бы один допускающий путь. Поэтому будем считать, что все рассматриваемые далее преобразователи обладают этим свойством.

Основным для дальнейшего изложения будет следующее

О п р е д е л е н и е. Преобразователь $\mathfrak{A}$ называется *конечнозначным*, если существует константа c, такая что для любого слова u существует не более c различных слов v, таких что $\langle u, v\rangle \in \Gamma(\mathfrak{A})$. Минимальное такое c называется *значностью* $\mathfrak{A}$. Если значность равна 1, то $\mathfrak{A}$ называется *однозначным*.

Например, преобразователи на рис. 1, 2 – двузначные, преобразователь на рис. 3 – четырехзначный.

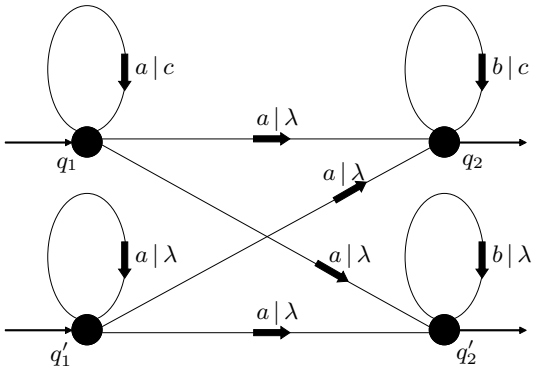

Рис. 3. Четырехзначный преобразователь: входу *aaab* соответствуют четыре выхода – λ, c, cc, ccc

Значность преобразователя может достигать значения, экспоненциального от его размера. Как показывает следующий пример, даже число различных длин выходов на одном входе может быть экспоненциальным.

Пример 1. Рассмотрим преобразователь $\mathfrak{B}$, имеющий $m+1$ пару состояний: $(q_1, q'_1), (q_2, q'_2), \ldots, (q_{m+1}, q'_{m+1})$. Начальные состояния – q_1, q'_1, заключительные – q_{m+1}, q'_{m+1}. Переходы следующие:

$$\langle q_i, u_i, \lambda, q_{i+1}\rangle, \quad \langle q_i, u_i, \lambda, q'_{i+1}\rangle, \quad \langle q'_i, u_i, \lambda, q_{i+1}\rangle,$$
$$\langle q'_i, u_i, \lambda, q'_{i+1}\rangle, \quad \langle q_i, u_i, c, q_i\rangle, \qquad \langle q'_i, u_i, \lambda, q'_i\rangle,$$

где $u_i = a$ при нечетном i и $u_i = b$ при четном, a, b, c – буквы (на рис. 3 изображен преобразователь $\mathfrak{B}$ в случае $m = 2$). Очевидно, что $\mathfrak{B}$ – конечнозначный. Пусть $f(k) = 2^{m-k}$. Тогда для входа $a^{f(0)}a\,b^{f(1)}b\,a^{f(2)}a\,b^{f(3)}b\ldots a^2a\,bb$ (считаем m четным) преобразователь $\mathfrak{B}$ может, очевидно, выдать любой выход c^k, где число k записывается в двоичной системе числом из не более m цифр. Таких чисел всего 2^m, т.е. экспонента от $|\mathfrak{B}|$.

Назовем преобразователь $\mathfrak{A}$ *редуцированным*, если у него ровно одно начальное и ровно одно конечное состояние, и все переходы с пустым входом идут из начального состояния в конечное. В [1] доказано следующее утверждение.

Лемма 1. *По преобразователю $\mathfrak{A}$ можно за полиномиальное время либо построить эквивалентный ему редуцированный преобразователь, либо констатировать бесконечнозначность $\mathfrak{A}$.*

Доказательство. Если преобразователь $\mathfrak{A}$ конечнозначный, в нем, очевидно, нет циклов с пустым входом и непустым выходом. Ясно, что проверка отсутствия указанных циклов выполняется за полиномиальное время. Если это условие не выполнено, констатируется бесконечнозначность $\mathfrak{A}$. Пусть оно выполнено.

Добавив не более двух состояний и не более $2|\mathfrak{A}|$ переходов, очевидным образом добьемся, чтобы в $\mathfrak{A}$ было ровно одно начальное состояние, из которого переходы только выходят, и ровно одно заключительное, куда переходы только входят. Далее, зададим на состояниях $\mathfrak{A}$ транзитивное отношение R: q_1Rq_2, если существует путь из q_1 в q_2 с пустым входом. Предположим, что q_1Rq_2 и q_2Rq_1. Тогда любой путь из q_1 в q_2 с пустым входом должен иметь пустой выход. Каждое максимальное множество состояний, на которых R тождественно истинно, естественным образом склеим в одно состояние. Удалим переходы-петли с пустым входом и пустым выходом. Получим преобразователь $\mathfrak{A}'$, который, очевидно, эквивалентен $\mathfrak{A}$. Пусть в $\mathfrak{A}'$ есть не начальное и не заключительное состояние q, такое что существует переход

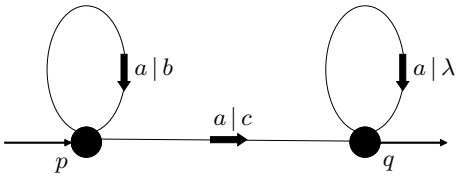

Рис. 4. Бесконечнозначный преобразователь: чем больше длина входа, тем больше вариантов выхода

с пустым входом, который входит в q или выходит из q. Выполним следующую операцию редукции. Для каждой пары переходов $\langle q_1, a_1, v_1, q\rangle, \langle q, a_2, v_2, q_2\rangle$, такой что $a_1 = \lambda$ или $a_2 = \lambda$, добавим переход $\langle q_1, a_1a_2, v_1v_2, q_2\rangle$. После этого удалим все переходы с пустым входом, входящие в q и выходящие из q. Очевидно, операция редукции не изменяет график преобразователя. Кроме того, если до нее у некоторого состояния q' не было инцидентных ему переходов с пустым входом, то и после нее их не будет. Поэтому не более чем за $|Q|$ операций редукции получим требуемый редуцированный преобразователь. ▲

Легко видеть, что для всех рассматриваемых далее задач наличие переходов с пустым входом в редуцированном преобразователе не является существенным. Поэтому будем считать, что таких переходов нет.

Замечание 1. Редуцированный преобразователь может быть бесконечнозначным. Таков, например, преобразователь, изображенный на рис. 4.

Сформулируем критерий конечнозначности преобразователя (теорема 1). Отметим, что сходный критерий сформулирован и доказан в [1].

Т е о р е м а 1. *Преобразователь* $\mathfrak{A}$ *размера* n *конечнозначен тогда и только тогда, когда для любых двух его состояний* s_1, s_2 (*не обязательно различных*) *и любых трех путей* p_1, p_2, p_3 *с одним и тем же входом* u, *таких что* p_1 *начинается в* s_1 *и кончается в* s_1, p_2 *начинается в* s_1 *и кончается в* s_2, *а* p_3 *начинается в* s_2 *и кончается в* s_2, *выполняются следующие два условия*:
(1) *Если* $\operatorname{out}(p_1) \neq \lambda$, *то* $\operatorname{out}(p_2)$ *является началом бесконечного слова* $(\operatorname{out}(p_1))^\infty$.
(2) *Для любого* $u' \subseteq u$ *выполняется* $|d(p_1, p_2, u')| \leqslant n^4$.

П р и м е р 2. Для преобразователя на рис. 4 не выполнено условие (1), хотя выполнено условие (2). Если в нем заменить букву c на λ, будет не выполнено условие (2), но выполнено условие (1). В обоих случаях преобразователь – бесконечнозначный.

Докажем необходимость сформулированного критерия. Пусть $\mathfrak{A}$ – конечнозначный преобразователь.

Докажем условие (1). Пусть $k > c$, где c – значность $\mathfrak{A}$. Рассмотрим множество $\{p_1^{i-1}p_2p_3^{k-i} \mid i = 1, \ldots, k\}$ путей из s_1 в s_2. Легко видеть, что все эти пути имеют один и тот же вход u^k. Выбор k гарантирует существование такого $j > 0$, что $(\operatorname{out}(p_1))^j \operatorname{out}(p_2) = \operatorname{out}(p_2)(\operatorname{out}(p_3))^j$. Отсюда

$$(\operatorname{out}(p_1))^{2j} \operatorname{out}(p_2) = (\operatorname{out}(p_1))^j \operatorname{out}(p_2)(\operatorname{out}(p_3))^j =$$
$$= \operatorname{out}(p_2)(\operatorname{out}(p_3))^j(\operatorname{out}(p_3))^j = \operatorname{out}(p_2)(\operatorname{out}(p_3))^{2j},$$

и аналогично $(\operatorname{out}(p_1))^{tj} \operatorname{out}(p_2) = \operatorname{out}(p_2)(\operatorname{out}(p_3))^{tj}$ для любого t, откуда ясно, что $\operatorname{out}(p_2)$ – начало $(\operatorname{out}(p_1))^\infty$.

Докажем от противного условие (2). Предположим, что $|d(p_1, p_2, u')| > n^4$ для какого-то $u' \subseteq u$. Пусть $\lambda = u_0, u_1, u_2, \ldots$ – все начала слова u. Заметим, что $|d(p_1, p_2, u_i) - d(p_1, p_2, u_{i+1})| \leqslant n$ для любого i, при этом $d(p_1, p_2, u_0) = 0$, следователь-

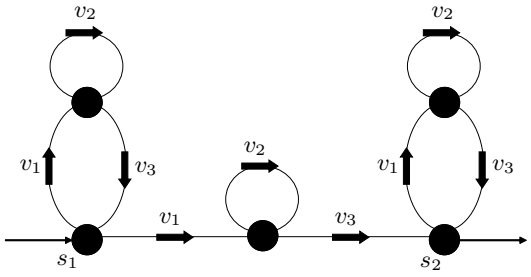

Рис. 5. Схема путей из доказательства теоремы 1. Указаны только входы

но, среди u_i найдется хотя бы n^3+1 начал u_{i_k} с различными $d(p_1,p_2,u_{i_k})$. Каждому u_{i_k} соответствует тройка состояний, в которых кончаются пути $p_1(u_{i_k}), p_2(u_{i_k})$, $p_3(u_{i_k})$. Возьмем такие $u_{i'}$ и $u_{i''}$ $(u_{i'} \subset u_{i''})$, которым соответствует одна и та же тройка. Таким образом, $u = v_1v_2v_3$, где $v_1 = u_{i'}$, $v_1v_2 = u_{i''}$ (см. рис. 5).

По построению $|\mathrm{out}(p_1(v_2))| \neq |\mathrm{out}(p_2(v_2))|$, так как

$$d(p_1,p_2,v_1) = |\mathrm{out}(p_1(v_1))| - |\mathrm{out}(p_2(v_1))| \neq$$
$$\neq |\mathrm{out}(p_1(v_1))| + |\mathrm{out}(p_1(v_2))| - |\mathrm{out}(p_2(v_1))| - |\mathrm{out}(p_2(v_2))| = d(p_1,p_2,v_1v_2).$$

Если $|\mathrm{out}(p_1)| \neq |\mathrm{out}(p_3)|$, то длины выходов путей $p_1^{i-1}p_2p_3^{k-i}$, очевидно, попарно различны, что противоречит выбору k. Если

$$|\mathrm{out}(p_1(v_1))| + |\mathrm{out}(p_1(v_3))| \neq |\mathrm{out}(p_3(v_1))| + |\mathrm{out}(p_3(v_3))|,$$

то такое же противоречие дают пути $[p_1(v_1)p_1(v_3)]^{i-1}p_2(v_1)p_2(v_3)[p_3(v_1)p_3(v_3)]^{k-i}$. Если же в обоих случаях выполняются равенства, рассмотрим различные пути из s_1 в s_2 с входом $v_1v_2v_3v_1v_2v_2v_3\ldots v_1v_2^kv_3$, проходящие по p_1,p_2,p_3. Легко видеть, что длина выхода этих путей монотонно зависит от того, какой блок $v_1v_2^iv_3$ приходится на путь p_2, что противоречит выбору k. Условие (2) и необходимость критерия доказаны. Достаточность критерия будет доказана в § 4 вместе с теоремой 3.

В [1] доказана следующая

Теорема 2. *Существует полиномиальный алгоритм, который по произвольному преобразователю решает, конечнозначный он или нет.*

Доказательство. Этот результат следует из леммы 1, критерия конечнозначности (теорема 1) и того, что по произвольному преобразователю $\mathfrak{A}$ без пустых входов можно за полиномиальное время решить, удовлетворяет ли он критерию. Покажем, как это сделать. Перебираем пары состояний $\langle s_1,s_2\rangle$. Для каждой пары сначала проверим, выполняется ли условие (2). Для этого построим следующий недетерминированный автомат A_1. Его состояния – упорядоченные четверки $\langle q_1,q_2,q_3,m\rangle$, где q_1,q_2,q_3 – состояния $\mathfrak{A}$, а m – либо целое число, такое что $|m| \leqslant n^4$, либо символ $*$. Переход из состояния $\langle q_1,q_2,q_3,m\rangle$ в состояние $\langle q_1',q_2',q_3',m'\rangle$ с входом a существует тогда и только тогда, когда, во-первых, для каждого $i=1,2,3$ существует переход в $\mathfrak{A}$ из q_i в q_i' с входом a (обозначим его выход через v_i), и во-вторых, если m – число и $|m+|v_1|-|v_2|| \leqslant n^4$, то $m' = m+|v_1|-|v_2|$, в противном случае $m' = *$. Начальное состояние A_1 равно $\langle s_1,s_1,s_2,0\rangle$, заключительное – $\langle s_1,s_2,s_2,*\rangle$. В m вычисляется разность между длинами выходов p_1 и p_2, а символ $*$ указывает, что ее модуль превысил n^4.

Очевидно, что из существования допускающего пути в A_1 следует существование указанных в критерии путей p_1,p_2,p_3, таких что на некотором начале u' их общего входа $|d(p_1,p_2,u')| > n^4$. Обратно, из существования таких путей вытекает, очевидно, существование допускающего пути в A_1. Таким образом, выполненность

условия (2) для s_1, s_2 эквивалентна отсутствию в A_1 допускающего пути, что, очевидно, проверяется за полиномиальное время.

Скажем, что два слова *согласованы*, если одно из них является началом другого.

Теперь проверим для s_1, s_2 выполненность условия (1), предполагая, что условие (2) для них выполнено. Сначала заметим, что условие (1) эквивалентно следующему условию (1′): слова $\mathrm{out}(p_1)$ и $\mathrm{out}(p_2)$ согласованы. Действительно, если (1′) не выполняется, то и (1), очевидно, тоже. Наоборот, если (1) нарушается для путей p_1, p_2, p_3, то для путей $p_1' = p_1^k$, $p_2' = p_2 p_3^{k-1}$, $p_3' = p_3^k$, где k достаточно велико, нарушается условие (1′).

Построим следующий автомат A_2. Его состояния делятся на три множества: Q_1, Q_2, Q_3. В Q_1 это пятерки $\langle q_1, q_2, q_3, m, a\rangle$, здесь q_1, q_2, q_3 так же, как в A_1, соответствуют последним состояниям угадываемых путей p_1, p_2, p_3, в m вычисляется разность длин выходов p_1 и p_2. При этом требуется, чтобы $|m| \leqslant n^4$, и если это неравенство нарушается, переход отсутствует. В a естественным образом вычисляется последняя буква того пути из p_1, p_2, выход которого в данный момент строго длиннее (если $|m| > 0$), а если $m = 0$, то $a = \lambda$. Начальное состояние – $\langle s_1, s_1, s_2, 0, \lambda\rangle$, заключительных состояний в Q_1 нет.

Находясь в произвольном состоянии $\langle q_1, q_2, q_3, m, a\rangle \in Q_1$ $(m \neq 0)$, A_2 может "предположить", что именно в указанной букве a произойдет рассогласованность $\mathrm{out}(p_1)$ и $\mathrm{out}(p_2)$ (назовем ее сбоем), и перейти (с пустым входом и выходом) в состояние из Q_2, имеющее вид $\langle q_1, q_2, q_3, a, k\rangle$, где k сначала равно m. Здесь в q_1, q_2, q_3 вычисляется обычная информация, a – буква предполагаемого сбоя, k указывает, на сколько букв надо нарастить "короткий" выход, чтобы проверить, действительно ли в указанном месте произойдет сбой. Переходы между состояниями в Q_2 очевидным образом уменьшают $|k|$ по мере нарастания "короткого" выхода, знак k определяет путь с "коротким" выходом. Когда на "коротком" выходе появляется буква, в которой по предположению должен быть сбой, проверяется, действительно ли эта буква не равна a. Если это так, A_2 может перейти в состояние из Q_3, которое имеет вид $\langle q_1, q_2, q_3\rangle$. Если, находясь в состоянии $\langle q_1, q_2, q_3, 0, \lambda\rangle \in Q_1$, A_2 обнаруживает при очередном переходе несогласованность выходов p_1 и p_2, то он тоже может перейти в $\langle q_1', q_2', q_3'\rangle \in Q_3$. Нахождение в состоянии из Q_3 означает, что сбой произошел, и теперь осталось достроить пути p_1, p_2, p_3 до конца. Переходы в Q_3 определяются естественным образом, заключительное состояние – $\langle s_1, s_2, s_2\rangle$. Очевидно, что условие (1′) выполнено для s_1, s_2 тогда и только тогда, когда не существует допускающего пути в A_2. ▲

В силу теоремы 2 вопрос о вложенности произвольного преобразователя в конечнозначный сводится за полиномиальное время к вопросу о вложенности одного конечнозначного преобразователя в другой. Действительно, проверим конечнозначность первого преобразователя. Если он бесконечнозначный, то, очевидно, не может быть вложен в конечнозначный.

Частным случаем однозначных преобразователей являются автоматы, т.е. преобразователи с пустым выходом. Даже для них невложенность может проявляться лишь на входе экспоненциальной длины. Это сразу следует из того, что для любого n существует недетерминированный автомат A размера $\mathrm{poly}(n)$, который не допускает некоторое слово w длины $\exp(\mathrm{poly}(n))$, но допускает все слова меньшей длины. Действительно, возьмем в качестве w конкатенацию записей всех n-разрядных двоичных чисел (младшие разряды слева), расположенных в порядке возрастания, начиная от слова из одних нулей и кончая словом из одних единиц. Автомат A в процессе работы "угадывает" причину, по которой читаемое слово не равно w. Причины могут быть такими: первое слово не нулевое; некоторое последующее число не равно предыдущему, увеличенному на 1 (в этом случае угадывается номер разряда, который в следующем слове не соответствует w); длина всего слова не кратна n; последнее слово

не единичное. В состояниях A (до угадывания) хранится номер последнего прочитанного разряда, его значение и информация о том, есть ли левее него нули в текущем числе. Этой информации достаточно для определения того, каким должен быть соответствующий разряд в следующем слове. Дальнейшие детали очевидны.

§ 3. Диаграммы путей и их свойства

Для декомпозиции конечнозначного преобразователя мы собираемся каждому допускающему пути в нем сопоставить такую информацию, которая была бы не слишком большой, допускала бы не слишком много вариантов, но в то же время однозначно определяла выход при данном входе. Здесь мы опишем соответствующие конструкции и докажем необходимые леммы.

Пусть дан преобразователь $\mathfrak{A}$, удовлетворяющий критерию конечнозначности из теоремы 1. Пусть q_1 и q_2 – состояния $\mathfrak{A}$. Скажем, что $q_1 \geqslant q_2$, если существует путь из q_1 в q_2. Назовем состояния q_1 и q_2 эквивалентными, если $q_1 \geqslant q_2$ и $q_2 \geqslant q_1$. Тогда множество состояний Q разбивается на классы эквивалентных состояний. Переход $\langle q_1, a, v, q_2\rangle$ будем называть *переходом в состояниях*, если q_1 не эквивалентно q_2.

Лемма 2. *Пусть в $\mathfrak{A}$ два состояния q_1 и q_2 эквивалентны. Тогда для любых двух путей l_1 и l_2 из q_1 в q_2, таких что* $\mathrm{in}(l_1) = \mathrm{in}(l_2)$, *выполняется* $\mathrm{out}(l_1) = \mathrm{out}(l_2)$. *Для любого начала u' слова $u = \mathrm{in}(l_1)$ выполняется $|d(l_1, l_2, u')| \leqslant n^4$.*

Доказательство. Обозначим $w_1 = \mathrm{out}(l_1)$, $w_2 = \mathrm{out}(l_2)$. В силу эквивалентности q_1 и q_2 существует путь l из q_2 в q_1. Если $|w_1| = |w_2|$, применим условие (1) теоремы 1, где $s_1 = s_2 = q_1$, $p_1 = l_1 l$, $p_2 = p_3 = l_2 l$. Получим, что $\mathrm{out}(l_1 l) = \mathrm{out}(l_2 l)$, откуда следует $w_1 = w_2$. Пусть $|w_1| \neq |w_2|$. Будем считать, что $|w_1| > 0$. Получаем противоречие с условием (2), положив в нем $s_1 = s_2 = q_1$, $p_1 = (l_1 l)^k$, $p_2 = p_3 = (l_2 l)^k$ для $k > n^4$. Последнее утверждение леммы следует из условия (2) теоремы 1. ▲

Пусть Q_1 и Q_2 – подмножества Q. Скажем, что Q_2 достигается из Q_1 на слове w, если существует множество L путей из Q_1 в Q_2 с входом w, такое что для любого $q_1 \in Q_1$ существует путь из L, начинающийся в q_1, а для любого $q_2 \in Q_2$ существует путь из L, кончающийся в q_2. Скажем, что $Q_1 \geqslant Q_2$, если существует слово, на котором Q_2 достигается из Q_1. Очевидно, что введенное отношение транзитивно и продолжает уже введенное на состояниях: $q_1 \geqslant q_2$ тогда и только тогда, когда $\{q_1\} \geqslant \geqslant \{q_2\}$. Назовем множества Q_1 и Q_2 эквивалентными, если $Q_1 \geqslant Q_2$ и $Q_2 \geqslant Q_1$. Тогда множество подмножеств Q разбивается на классы эквивалентных подмножеств.

Лемма 3. *По двум подмножествам Q_1 и Q_2 можно за время* $\exp(\mathrm{poly}(n))$ *выяснить, выполняется ли $Q_1 \geqslant Q_2$.*

Доказательство. Построим автомат, проверяющий достижимость Q_2 из Q_1. Его состояния – кортежи подмножеств множества Q длины $m = |Q_1|$. Каждое подмножество соответствует "своему" элементу множества Q_1, начальное состояние – кортеж одноэлементных подмножеств "своих" элементов. Переход с входом a идет из кортежа $\langle P_1, P_2, \ldots, P_m\rangle$ в кортеж $\langle R_1, R_2, \ldots, R_m\rangle$, если для каждого i все переходы из P_i с входом a ведут в R_i и для каждого состояния из R_i существует ведущий в него переход из P_i с входом a. Конечные состояния автомата – такие кортежи $\langle R_1, R_2, \ldots, R_m\rangle$, что каждое R_i имеет непустое пересечение с Q_2 и Q_2 содержится в объединении всех R_i. Очевидно, что $Q_1 \geqslant Q_2$ тогда и только тогда, когда в автомате существует допускающий путь. Легко видеть, что построение автомата и проверка этого условия требуют не более экспоненциального времени. ▲

Пусть есть слово u, и $u' \subseteq u$. Множеством *двусторонней достижимости* $M_u(u')$ назовем множество таких состояний q, для которых существует допускающий путь l, такой что $\mathrm{in}(l) = u$ и путь $l(u')$ кончается в q. Легко видеть, что если $u_1 \subseteq u_2 \subseteq u$, то $M_u(u_1) \geqslant M_u(u_2)$. Пусть на допускающем пути l есть переход p и l_1 – начало l, кончающееся непосредственно до p, а l_2 – начало l, кончающееся сразу после p. Будем

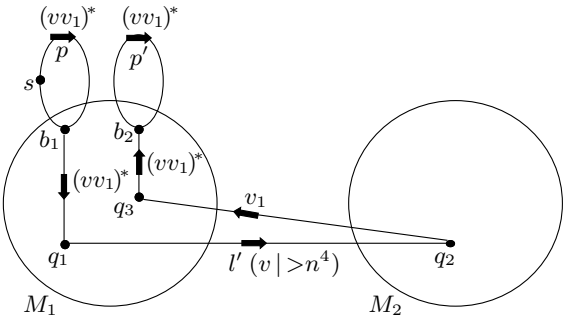

Рис. 6. Схема путей из доказательства леммы 4. Символ $*$ означает натуральное число (в каждом месте свое)

называть p *переходом в множествах* на l, если $M_u(u_1)$ не эквивалентно $M_u(u_2)$, где $u_1 = \mathrm{in}(l_1)$, $u_2 = \mathrm{in}(l_2)$.

Лемма 4. *Пусть M_1, M_2 – произвольные эквивалентные множества состояний, $q_1 \in M_1$, $q_2 \in M_2$, l' – путь из q_1 в q_2, такой что M_2 достигается из M_1 на слове $v = \mathrm{in}(l')$ и $|\mathrm{out}(l')| > n^4$. Тогда для любых двух путей l_1, l_2 из q_1 в q_2 с входом v слова $\mathrm{out}(l_1)$ и $\mathrm{out}(l_2)$ согласованы, и для любого $v' \subseteq v$ выполняется $|d(l_1, l_2, v')| \leqslant 2n^4$.*

Доказательство. Будем считать, что q_1 не эквивалентно q_2, иначе утверждение сразу следует из леммы 2. Из эквивалентности M_1 и M_2 следует, что M_1 достигается из M_2 на некотором слове v_1. Тогда M_1 достигается из самого себя на слове vv_1. Поэтому существует бесконечная последовательность состояний из M_1: $q_0, q_{-1}, q_{-2} \ldots$, такая что для любого $i \leqslant 0$ существует путь γ_i из q_i в q_{i+1} с входом vv_1. Зафиксируем состояние $b_1 = q_i = q_j$ для некоторых $i < j \leqslant 1$. Получим замкнутый путь из b_1 в b_1, который обозначим через p (рис. 6). Кроме того, существует бесконечная последовательность состояний из M_1: $q_3, q_4, \ldots$, такая что существует путь γ_2 из q_2 в q_3 с входом v_1, и для любого $i \geqslant 3$ есть путь γ_i из q_i в q_{i+1} с входом vv_1. Здесь $q_i \neq q_j$ для всех $i \leqslant 1$, $j \geqslant 2$ в силу неэквивалентности q_1 и q_2. Зафиксировав $b_2 = q_i = q_j$ для некоторых $3 \leqslant i < j$, получим замкнутый путь из b_2 в b_2, который обозначим через p' (рис. 6).

Путь из b_1 в b_2, состоящий из трех отрезков – из b_1 в q_1 по путям γ_i ($i \leqslant 0$), из q_1 в q_2 по l' и из q_2 в b_2 по путям γ_i ($i \geqslant 2$) – обозначим через γ. Очевидно, $|\mathrm{in}(p)| = kn_1$, $|\mathrm{in}(\gamma)| = kn_2$, $|\mathrm{in}(p')| = kn_3$, где $k = |vv_1|$, а n_1, n_2, n_3 – натуральные числа. Возьмем на p состояние s, такое что путь, начинающийся в s, идущий все время по циклу p и имеющий длину $k(n_1n_2n_3 - n_2)$, оканчивается в b_1, обозначим этот путь через γ'. Рассмотрим три пути: путь p_1 из s в s, совершающий n_2n_3 оборотов по циклу p, путь p_2 из s в b_2, равный $\gamma'\gamma$, и путь p_3 из b_2 в b_2, совершающий n_1n_2 оборотов по циклу p'. Очевидно, что $\mathrm{in}(p_1) = \mathrm{in}(p_2) = \mathrm{in}(p_3) = kn_1n_2n_3$. Так как $|\mathrm{out}(p_2)| \geqslant$ $\geqslant |\mathrm{out}(l')| > n^4$, то по условию (2) теоремы 1 $|\mathrm{out}(p_1)| > 0$. Путь p_2 можно провести по l_1 или l_2 вместо l'. По условию (1) выходы любого из этих трех возможных вариантов пути p_2 являются началами слова $(\mathrm{out}(p_1))^\infty$. Отсюда следует, что слова $\mathrm{out}(l_1)$ и $\mathrm{out}(l_2)$ согласованы. Из условия (2) легко видеть, что $|d(l_1, l_2, v')| \leqslant 2n^4$. ▲

Если l – допускающий путь в $\mathfrak{A}$ с входом u, а l_1 – его начало с входом u_1, будем называть множество $M_u(u_1)$ множеством двусторонней достижимости пути l относительно l_1 и обозначать через $M(l, l_1)$. Очевидным следствием леммы 4 является следующее утверждение.

Следствие. *Пусть l – допускающий путь в $\mathfrak{A}$, l_1 и l_2 – два его начала (l_1 – более короткое) и $M(l, l_1)$ эквивалентно $M(l, l_2)$. Обозначим через l' отрезок пути l, дополняющий l_1 до l_2, а через q_1 и q_2 – начальное и конечное состояния l' соот-*

ветственно. Пусть $|\mathrm{out}(l')| > n^4$. *Тогда для любых двух путей* p_1, p_2 *из* q_1 *в* q_2 *с входом* $v = \mathrm{in}(l')$ *слова* $\mathrm{out}(p_1)$ *и* $\mathrm{out}(p_2)$ *согласованы, и для любого* $v' \subseteq v$ *выполняется* $|d(p_1, p_2, v')| \leqslant 2n^4$.

Пусть l – допускающий путь в $\mathfrak{A}$. Каждому началу l' пути l соответствует пара (q, M), где $q \in M$ – состояние, в котором оканчивается l', а $M = M(l, l')$. Будем отмечать пары, соответствующие некоторым началам пути l. Отметим пары, соответствующие пустому началу и всему пути. Для каждого перехода в состояниях на l, который не является переходом в множествах на l, возьмем ближайшие слева и справа на l (мы представляем l направленным слева направо) переходы в множествах (если они есть). Для каждого из этих двух переходов отметим по две пары, соответствующие началам пути l, кончающимся непосредственно до перехода и сразу после него. Для каждого перехода в состояниях, который является и переходом в множествах на l, отметим две указанные пары, соответствующие этому переходу.

Обозначим через D последовательность всех отмеченных пар, расположенных в порядке возрастания соответствующих им начал. Легко видеть, что для любых двух соседних в D пар (q_1, M_1), (q_2, M_2) возможны следующие три случая:

1) q_1 эквивалентно q_2;
2) Начала l, соответствующие этим парам, различаются на один переход пути l, который является переходом и в состояниях, и в множествах;
3) M_1 эквивалентно M_2, q_1 не эквивалентно q_2.

Если имеет место i-й случай, будем говорить, что отрезок $[(q_1, M_1), (q_2, M_2)]$ имеет i-й тип. Отрезку первого типа не приписывается никакой информации, кроме номера его типа. Отрезку второго типа приписывается слово, являющееся выходом соответствующего перехода. Для отрезка третьего типа пусть l' – участок пути l между положениями (q_1, M_1) и (q_2, M_2), $v = \mathrm{in}(l')$, $w = \mathrm{out}(l')$. Возможны два случая. Если $|w| \leqslant n^4$, скажем, что отрезок имеет первый подтип и припишем ему само слово w. Если $|w| > n^4$, скажем, что отрезок имеет второй подтип и припишем ему число k, равное разности между $|w|$ и минимальной длиной выхода среди выходов всех путей из q_1 в q_2 с входом v. По следствию 1 $k \leqslant 2n^4$. Кроме того, среди отрезков выделяем такие, где пары (q_1, M_1) и (q_2, M_2) соответствуют двум началам пути l, различающимся на один переход. Эти отрезки называем *короткими*.

Последовательность D с приписанной отрезкам указанной информацией будем называть *диаграммой* пути l и обозначать через $D(l)$. Информация включает также номер типа отрезка и (для третьего типа) номер подтипа, а также указание, является ли он коротким. Поскольку переходов в состояниях не больше n, диаграммы всех допускающих путей в $\mathfrak{A}$ имеют длину не больше $4n$.

Диаграммой (не относящейся ни к какому заранее указанному пути) назовем последовательность пар вида (q, M), где каждым двум соседним парам приписан один из трех типов отрезков (для третьего типа – еще подтип) с соответствующей информацией и указанием, является ли отрезок коротким. Диаграмму D назовем *корректной*, если

1) Ее первая пара равна $\langle q_0, \{q_0\}\rangle$, где q_0 – начальное состояние $\mathfrak{A}$; последняя пара равна $\langle f, \{f\}\rangle$, где f – заключительное состояние $\mathfrak{A}$. Для каждой пары (q, M) из D выполняется $q \in M$;

2) Длина D не превышает $4n$;

3) Для каждого отрезка $[(q_1, M_1), (q_2, M_2)]$ первого типа состояния q_1 и q_2 эквивалентны;

4) Каждый отрезок $[(q_1, M_1), (q_2, M_2)]$ второго типа помечен как короткий, q_1 не эквивалентно q_2, M_1 не эквивалентно M_2, слово, сопоставленное отрезку, является выходом некоторого перехода из q_1 в q_2;

5) Для каждого отрезка $[(q_1, M_1), (q_2, M_2)]$ третьего типа множества M_1 и M_2 эквивалентны, состояния q_1 и q_2 не эквивалентны. Для первого подтипа сопостав-

ленное слово w имеет длину не больше n^4, для второго подтипа сопоставленное число не превышает $2n^4$;

6) Каждая пара (q, M) (кроме, возможно, начальной и конечной) является началом или концом короткого отрезка $[(q_1, M_1), (q_2, M_2)]$, у которого множества M_1 и M_2 не эквивалентны (это свойство гарантирует, в частности, что отрезки первого и третьего типов всегда разделены в D отрезком второго типа).

Лемма 5. *Диаграмма любого допускающего пути корректна. Всего корректных диаграмм не более* $\exp(\mathrm{poly}(n))$. *По диаграмме можно за время* $\exp(\mathrm{poly}(n))$ *проверить ее корректность.*

Доказательство. Первые два утверждения леммы очевидны. В третьем нетривиален лишь алгоритм проверки эквивалентности двух множеств. Он легко следует из леммы 3. ▲

Скажем, что допускающий путь l удовлетворяет корректной диаграмме $D = (q_1, M_1), (q_2, M_2), \ldots, (q_m, M_m)$, если в нем можно выделить последовательность возрастающих начал $l_1, l_2, \ldots, l_m$, такую что l_i оканчивается в состоянии q_i для каждого i, $M(l, l_i) = M_i$, все короткие отрезки соответствуют одному переходу, на каждом отрезке второго типа или третьего типа первого подтипа выход совпадает с указанным в D, на каждом отрезке третьего типа второго подтипа выход имеет длину больше n^4 и превышает по длине минимальный выход (среди выходов всех путей из q_1 в q_2 с тем же входом) на указанную в D величину. Очевидно, любой допускающий путь l удовлетворяет диаграмме $D(l)$.

Лемма 6. *Пусть l_1 и l_2 – допускающие пути в $\mathfrak{A}$ с одним и тем же входом, удовлетворяющие одной и той же корректной диаграмме D. Тогда* $\mathrm{out}(l_1) = \mathrm{out}(l_2)$.

Доказательство. По свойству 6) любая не крайняя пара из D соответствует положению пути, удовлетворяющему D, непосредственно до или после перехода в множествах, причем из D видно, какой из этих случаев имеет место. Любое множество двусторонней достижимости M, о котором известно, что оно соответствует положению пути непосредственно слева (или справа) от перехода в множествах, однозначно определяет начало u' слова $u = \mathrm{in}(l_1) = \mathrm{in}(l_2)$, такое что $M = M_u(u')$. Поэтому пары из D однозначно разбивают вход u на соответствующие участки, и достаточно доказать равенство выходов l_1 и l_2 на каждом участке входа. Если отрезок диаграммы имеет первый тип, то совпадение выходов на соответствующем участке входа следует из леммы 2. Для отрезка второго типа или первого подтипа третьего типа выход указан непосредственно в диаграмме. На отрезке второго подтипа третьего типа выходы l_1 и l_2 согласованы (см. следствие), и одинаковая разность длин с одним и тем же числом обеспечивает их совпадение. ▲

§ 4. Декомпозиция конечнозначного преобразователя

Скажем, что конечнозначный преобразователь $\mathfrak{A}$ *разлагается в декомпозицию* однозначных преобразователей $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_K$, если $\Gamma(\mathfrak{A}) = \bigcup_{i=1}^{K} \Gamma(\mathfrak{A}_i)$. В [2] доказано, что любой конечнозначный преобразователь $\mathfrak{A}$ можно эффективно разложить в декомпозицию ровно k однозначных преобразователей за время $\exp(\exp(\mathrm{poly}(n)))$, где k – значность преобразователя $\mathfrak{A}$. При этом размер каждого однозначного преобразователя не более $\exp(\exp(\mathrm{poly}(n)))$. В работе [5] оценка на время и размер компонент улучшена до одной экспоненты, но в показателе экспоненты присутствует k, которое само может быть экспоненциально от n (см. пример 1 в § 2). Мы предлагаем в следующей теореме способ декомпозиции с “чисто” экспоненциальными оценками, который, правда, не гарантирует, что число однозначных преобразователей будет ровно k.

Теорема 3. *Существует алгоритм, который по любому конечнозначному преобразователю* $\mathfrak{A}$ *размера* n *вычисляет за время, не превосходящее* $\exp(\mathrm{poly}(n))$, *его декомпозицию на не более чем* $\exp(\mathrm{poly}(n))$ *однозначных преобразователей размера не более* $\exp(\mathrm{poly}(n))$.

Доказательство. Как и в § 3, будем предполагать вместо конечнозначности $\mathfrak{A}$ выполненность критерия конечнозначности (см. теорему 1). Поскольку из возможности декомпозиции преобразователя следует его конечнозначность, вместе с теоремой 3 будет доказана достаточность критерия.

В силу леммы 5 для доказательства теоремы 3 достаточно для каждой корректной диаграммы D построить за экспоненциальное время преобразователь $\mathfrak{A}(D)$, график которого состоит из тех и только тех элементов $\Gamma(\mathfrak{A})$, которые реализуются путями, удовлетворяющими диаграмме D. По лемме 6 преобразователь $\mathfrak{A}(D)$ будет однозначным.

Множеством левосторонней достижимости для слова u назовем множество таких состояний q, что существует путь из начального состояния в q с входом u. Если дана диаграмма D, то множеством локальной двусторонней достижимости на отрезке $[(q_1, M_1), (q_2, M_2)]$ диаграммы D для входа u и его начала u' назовем множество таких состояний q, что существует путь l из q_1 в q_2, такой что $\mathrm{in}(l) = u$ и путь $l(u')$ кончается в q. Множеством локальной левосторонней достижимости на этом отрезке для входа u назовем множество таких состояний q, что существует путь из q_1 в q с входом u.

Опишем $\mathfrak{A}(D)$. Состояниями $\mathfrak{A}(D)$ будут совокупности вида $\langle Q_1, Q_2, q, L\rangle$. Здесь в Q_1 будет вычисляться множество левосторонней достижимости для прочитанного начала входа, в $Q_2 \subseteq Q_1$ – множество двусторонней достижимости для всего входа и текущего начала входа, в $q \in Q_2$ – текущее состояние угадываемого пути в $\mathfrak{A}$. Очевидно, что множество Q_2 однозначно определяет текущий отрезок $[(q_1, M_1), (q_2, M_2)]$ диаграммы D первого или третьего типа, такой что $M_1 \geqslant Q_2 \geqslant M_2$, если он существует. L непусто тогда и только тогда, когда этот отрезок существует и имеет третий тип. В случае первого подтипа L – число m, принимающее все значения от 0 до длины указанного в D выхода (в m будет вычисляться длина выхода на отрезке). В случае второго подтипа L – совокупность $\langle Q'_1, Q'_2, P\rangle$. Здесь в Q'_1 будет вычисляться множество локальной левосторонней достижимости на текущем отрезке, в Q'_2 – множество локальной двусторонней достижимости, $q \in Q'_2 \subseteq Q'_1$. P – это множество пар $\langle q', m\rangle$, по одной для каждого состояния $q' \in Q'_2$, где $0 \leqslant m \leqslant 2n^4$, и еще одна текущая пара с q', равным текущему состоянию q. Обозначим через u_t отрезок входа, прочтенный к текущему моменту в $\mathfrak{A}(D)$ на рассматриваемом отрезке. В текущей паре $\langle q, m\rangle$ в m будет вычисляться разность между длиной выхода угадываемого пути на отрезке входа u_t и минимальной длиной выхода среди выходов всех путей с входом u_t из q_1 в множество Q'_2. Чтобы следить за этой минимальной длиной, в каждой не текущей паре $\langle q', m\rangle$ в m будет вычисляться разность между минимальной длиной выхода среди выходов всех путей из q_1 в q' с входом u_t и минимальной длиной выхода среди выходов всех путей с входом u_t из q_1 в множество Q'_2. Начальными состояниями $\mathfrak{A}(D)$ являются такие, в которых $Q_1 = Q_2 = \{q_0\}$, $q = q_0$; если первый отрезок диаграммы имеет третий тип, то L непусто, при первом подтипе $L = 0$, при втором $Q'_1 = Q'_2 = \{q_0\}$ и обе пары равны $\langle q_0, 0\rangle$. Текущая пара – $\langle q, 0\rangle$. Заключительными состояниями $\mathfrak{A}(D)$ являются такие, где $Q_2 = \{f\}$, $q = f$; если последний отрезок в D имеет третий тип, то L непусто, при первом подтипе число m равно длине указанного в D выхода, при втором подтипе $Q'_2 = \{f\}$, и текущая пара равна $\langle f, m\rangle$, где m – число, указанное в D.

Опишем переходы $\mathfrak{A}(D)$. Скажем, что состояние q'' из $\mathfrak{A}$ является последователем состояния q' по букве a, если есть переход из q' в q'' с входом a. Переход из состояния s_1 в состояние s_2 с входной буквой a и выходным словом v существует тогда и только тогда, когда выполнены все следующие условия:

1) $Q_1(s_2)$ (так обозначаем компоненту Q_1 в состоянии s_2) есть множество всех последователей состояний из $Q_1(s_1)$ по a. Таким образом, компонента Q_1 вычисляется детерминированно;

2) Существует переход в $\mathfrak{A}$ из $q(s_1)$ в $q(s_2)$ с входом a и выходом v;

3) Для каждого состояния q' из $Q_2(s_1)$ хотя бы один из его последователей по a принадлежит $Q_2(s_2)$. Для каждого состояния q' из $Q_1(s_1) \setminus Q_2(s_1)$ все его последователи по a не принадлежат $Q_2(s_2)$;

4) В D существует отрезок R: $[(q_1, M_1), (q_2, M_2)]$ либо типа 1 или 3, такой что $M_1 \geqslant Q_2(s_1) \geqslant M_2$, $M_1 \geqslant Q_2(s_2) \geqslant M_2$, (очевидно, такой отрезок может быть лишь один), либо типа 2, такой что $M_1 = Q_2(s_1)$, $M_2 = Q_2(s_2)$, $q_1 = q(s_1)$, $q_2 = q(s_2)$, v равно выходу, указанному при R. В этом последнем случае, если предыдущий отрезок D (до (q_1, M_1)) имеет третий тип, то должно выполняться: $Q'_2(s_1) = \{q_1\}$, m в $L(s_1)$ равно длине указанного в D выхода (для первого подтипа) или m в текущей паре равно указанному в D числу (для второго подтипа). Аналогично, если последующий отрезок D (от (q_2, M_2)) имеет третий тип, то должны выполняться очевидные начальные условия. В случае, когда R имеет третий тип, должны выполняться перечисленные в следующем абзаце условия.

Множество $Q'_1(s_2)$ состоит из всех последователей состояний из $Q'_1(s_1)$ по a. Для каждого состояния q' из $Q'_2(s_1)$ хотя бы один из его последователей по a принадлежит $Q'_2(s_2)$. Для каждого состояния q' из $Q'_1(s_1) \setminus Q'_2(s_1)$ все его последователи по a не принадлежат $Q'_2(s_2)$. В случае первого подтипа выход v продолжает начало длины $m(s_1)$ указанного в D выхода, и $m(s_2) = m(s_1) + |v|$. В случае второго подтипа $P(s_2)$ получается по следующим правилам. Сначала сопоставим каждому $q' \in Q'_2(s_2)$ минимальное число среди всех сумм $m + |w|$, таких что для некоторого q'' $\langle q'', m\rangle \in P(s_1)$ и существует переход из q'' в q' с входом a и выходом w. Среди всех сопоставленных чисел возьмем минимальное число k. Если $k \neq 0$, уменьшим все эти числа на k. При этом все получившиеся числа не превышают $2n^4$. Эти числа в парах с соответствующими им состояниями составляют $P(s_2)$. В текущей паре $m(s_2) = m(s_1) + |v| - k \leqslant 2n^4$.

Наконец, если отрезок R короткий, то $M_1 = Q_2(s_1)$, $M_2 = Q_2(s_2)$, $q_1 = q(s_1)$, $q_2 = q(s_2)$.

Очевидно, что если в $\mathfrak{A}$ есть допускающий путь l, удовлетворяющий диаграмме D, то в $\mathfrak{A}(D)$ существует допускающий путь l', такой что $\mathrm{in}(l) = \mathrm{in}(l')$, $\mathrm{out}(l) = \mathrm{out}(l')$. Пусть, наоборот, в $\mathfrak{A}(D)$ есть допускающий путь l'. Покажем, что соответствующий ему путь l в $\mathfrak{A}$ удовлетворяет диаграмме D. Компонента Q_1 вычисляется верно, так как она детерминирована. Покажем, что Q_2 тоже вычисляется верно. Пусть это не так. Пусть Q_2 в некоторый момент имеет лишнее состояние. Тогда в силу того, что элементы Q_2 имеют хотя бы одного последователя в Q_2 на каждом шаге, в конце компонента Q_2 не может состоять лишь из заключительного состояния, что приводит к противоречию. Пусть Q_2 не содержит некоторого состояния, которое на самом деле входит в множество двусторонней достижимости. Так как все последователи состояний из $Q_1 \setminus Q_2$ не принадлежат Q_2, то в конце заключительное состояние f должно не принадлежать Q_2, что невозможно. Аналогично доказывается правильность вычисления Q'_1 и Q'_2 на отрезках третьего типа. Переходы $\mathfrak{A}(D)$ устроены так, что находясь в D на каком-либо отрезке первого или третьего типа, можно уйти с него только по переходу, соответствующему следующему отрезку второго типа, и лишь тогда, когда информация о первом отрезке соответствует D. Правильность вычисления этой информации очевидна. Построение $\mathfrak{A}(D)$, очевидно, производится за экспоненциальное время. Теорема 3 и достаточность критерия конечнозначности доказаны. ▲

Замечание 2. Изложенную конструкцию можно применять к конечнозначным преобразователям без пустых входов, у которых не обязательно одно начальное и

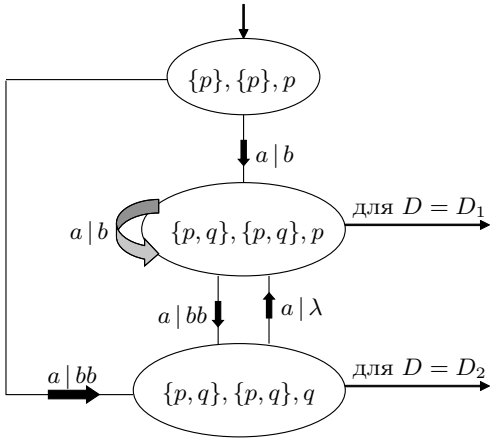

Рис. 7. Однозначные преобразователи, получившиеся в результате декомпозиции двузначного преобразователя на рис. 1, различаются лишь конечными состояниями. Компоненты состояний показаны в последовательности Q_1, Q_2, q. Среднее состояние – конечное для $\mathfrak{A}(D_1)$, нижнее – для $\mathfrak{A}(D_2)$, где $D_1 = \langle p, \{p\}\rangle, \langle p, \{p, q\}\rangle$, $D_2 = \langle p, \{p\}\rangle, \langle q, \{p, q\}\rangle$

одно конечное состояние (т.е. не редуцируя их). Единственные изменения относятся к виду начальной пары корректной диаграммы (теперь там множество M – подмножество множества начальных состояний Q_0), к виду конечной пары корректной диаграммы (там M – подмножество множества конечных состояний Q_f) и к определению начальных и конечных состояний преобразователя $\mathfrak{A}(D)$. У него в начальных состояниях $Q_1 = Q_0$, в заключительных – множество $Q_1 \setminus Q_2$ не содержит состояний из Q_f.

Замечание 3. Если из каких-либо соображений известно, что на любом отрезке третьего типа все пути с одним входом имеют согласованные выходы (например, выходы всех переходов в $\mathfrak{A}$ – слова в однобуквенном алфавите), то, очевидно, можно ограничиться лишь диаграммами, в которых все отрезки третьего типа имеют второй подтип.

Замечание 4. После описанного построения всех преобразователей $\mathfrak{A}(D)$ из них следует удалить состояния, через которые не проходит допускающий путь. При этом часто уменьшается как размер этих преобразователей, так и их количество.

Пример 3. В преобразователе, изображенном ни рис. 1, состояния p и q эквивалентны, возможные множества $\{p\}$ и $\{p, q\}$ двусторонней достижимости также эквивалентны. Легко видеть, что возможны лишь две диаграммы допускающих путей – $\langle p, \{p\}\rangle, \langle p, \{p, q\}\rangle$ и $\langle p, \{p\}\rangle, \langle q, \{p, q\}\rangle$, состоящие из одного отрезка первого типа. Учитывая замечания 2 и 4, видим, что итоговая декомпозиция состоит из двух преобразователей, различающихся лишь конечным состоянием (см. рис. 7).

Пример 4. В преобразователе, изображенном ни рис. 2, состояния p и q не эквивалентны, возможные множества $\{p\}$ и $\{p, q\}$ двусторонней достижимости эквивалентны. С учетом замечания 3 легко видеть, что возможны лишь две диаграммы допускающих путей – $\langle p, \{p\}\rangle, \langle p, \{p, q\}\rangle$ и $\langle p, \{p\}\rangle, \langle q, \{p, q\}\rangle$, состоящие из одного отрезка третьего типа второго подтипа с приписанным ему числом $k = 0$. Учитывая замечания 2 и 4, видим, что итоговая декомпозиция состоит из двух преобразователей, изображенных на рис. 8 и 9.

Пример 5. В преобразователе, изображенном ни рис. 3, все состояния не эквивалентны, возможные множества $\{q_1, q_1'\}$ и $\{q_2, q_2'\}$ двусторонней достижимости также не эквивалентны. Легко видеть, что возможны лишь четыре диаграммы до-

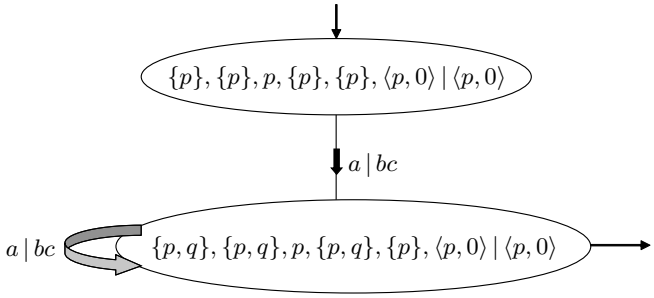

Рис. 8. Однозначный преобразователь, соответствующий диаграмме $\langle p,\{p\}\rangle, \langle p,\{p,q\}\rangle$ $(k=0)$ при декомпозиции двузначного преобразователя, изображенного на рис. 2. Компоненты его состояний показаны в последовательности $Q_1, Q_2, q, Q_1', Q_2', P$, текущая пара отделена вертикальной чертой

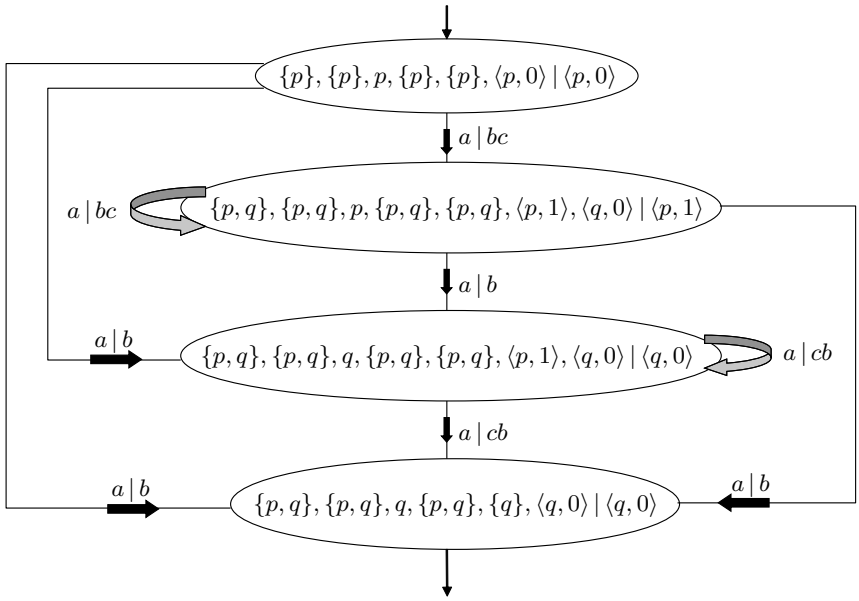

Рис. 9. Однозначный преобразователь, соответствующий диаграмме $\langle p,\{p\}\rangle, \langle q,\{p,q\}\rangle$ $(k=0)$ при декомпозиции двузначного преобразователя, изображенного на рис. 2

пускающих путей – $\langle q_1,\{q_1,q_1'\}\rangle, \langle q_2,\{q_2,q_2'\}\rangle$; $\langle q_1,\{q_1,q_1'\}\rangle, \langle q_2',\{q_2,q_2'\}\rangle$; $\langle q_1',\{q_1,q_1'\}\rangle$, $\langle q_2,\{q_2,q_2'\}\rangle$ и $\langle q_1',\{q_1,q_1'\}\rangle, \langle q_2',\{q_2,q_2'\}\rangle$, состоящие из одного отрезка второго типа. Учитывая замечания 2 и 4, видим, что итоговая декомпозиция состоит из четырех преобразователей, различающихся лишь парой текущих состояний. На рис. 10 изображен преобразователь для первой диаграммы.

Укажем одно следствие наших построений.

Теорема 4. *Для любого слова u в $\mathfrak{A}$ существует множество $M(u)$, состоящее из* $\exp(\mathrm{poly}(n))$ *допускающих путей с входом u, такое что для любого допускающего пути l с входом u существует путь $l' \in M(u)$, такой что* $\mathrm{out}(l') = \mathrm{out}(l)$, *и для любого $u' \subseteq u$ выполняется $|d(l,l',u')| \leqslant 2n^4$.*

В частности, как доказано в [1], значность конечнозначного преобразователя размера n не превосходит $\exp(\mathrm{poly}(n))$.

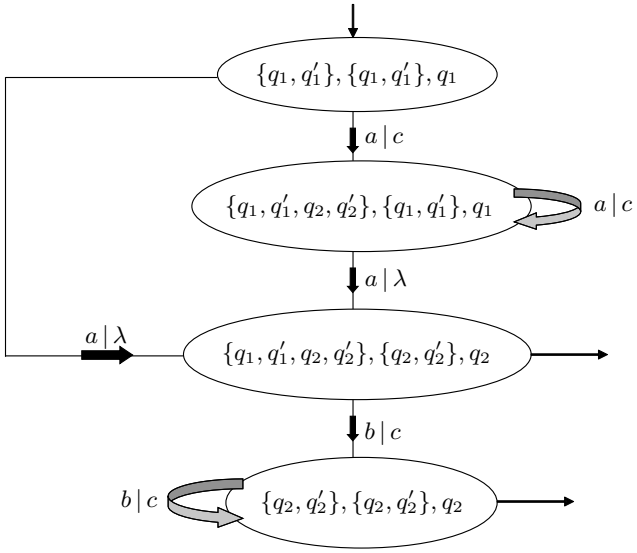

Рис. 10. Однозначный преобразователь, получившийся в результате декомпозиции четырехзначного преобразователя, изображенного на рис. 3, для диаграммы $\langle q_1, \{q_1, q_1'\}\rangle, \langle q_2, \{q_2, q_2'\}\rangle$ (компоненты состояний показаны в последовательности Q_1, Q_2, q). Три других преобразователя получаются из него заменой пары (q_1, q_2) текущих состояний на одну из трех других пар

Для доказательства теоремы 4 возьмем в качестве $M(u)$ по одному пути с каждой возможной диаграммой. Ее утверждение легко следует из лемм 2, 6 и следствия леммы 4.

§ 5. Тест на вложенность

Рассмотрим вопросы о тесте на вложенность, т.е. о том, какую длину входов и выходов достаточно проверить, чтобы убедиться, что произвольный преобразователь $\mathfrak{A}_1$ вложен в конечнозначный преобразователь $\mathfrak{A}_2$. В силу леммы 1 можно считать, что $\mathfrak{A}_1$ и $\mathfrak{A}_2$ не имеют пустых входов. Следующая лемма утверждает, что если $\mathfrak{A}_1$ не вложен в $\mathfrak{A}_2$, то это проявляется на выходах экспоненциальной длины.

Лемма 7. *Если преобразователь $\mathfrak{A}_1$ не вложен в конечнозначный преобразователь $\mathfrak{A}_2$, то существует пара $\langle u, v\rangle$, такая что $\langle u, v\rangle \in \Gamma(\mathfrak{A}_1)$, $\langle u, v\rangle \notin \Gamma(\mathfrak{A}_2)$ и $|v| \leqslant \exp(p_1(n))$, где $p_1(n)$ – некоторый полином.*

Доказательство. Рассмотрим допускающий путь l_1 в $\mathfrak{A}_1$ с выходом минимальной длины, такой что $\langle u, v_1\rangle \in \Gamma(\mathfrak{A}_1)$, $\langle u, v_1\rangle \notin \Gamma(\mathfrak{A}_2)$, где $u = \mathrm{in}(l_1)$, $v_1 = \mathrm{out}(l_1)$. Предположим, что $|v_1| > \exp(p_1(n))$, где степень $p_1(n)$ достаточно велика. Здесь и далее под выражениями типа "достаточно много" будем подразумевать величину $\exp(\mathrm{poly}(n))$, где степень полинома настолько велика, что можно выполнить все описываемые действия. Под выражением "фиксированная экспонента" понимаем величину $\exp(p(n))$, где $p(n)$ – полином, существование которого либо очевидно, либо доказано ранее. Если $\langle u, v_2\rangle \in \Gamma(\mathfrak{A}_2)$, $|v_1| = |v_2|$, но $v_1 \neq v_2$, то назовем левым (соответственно, правым) *сбоем* между v_1 и v_2 первую слева (соответственно, справа) пару неравных букв слов v_1 и v_2, равноотстоящих от начала (соответственно, конца). По теореме 4 количество различных v_2, таких что $\langle u, v_2\rangle \in \Gamma(\mathfrak{A}_2)$ – фиксированная экспонента, поэтому и букв на v_1, в которых имеет место левый или правый сбой между v_1 и каким-нибудь из таких v_2, тоже мало. Возьмем в слове v_1 достаточно

большое подслово r, в которое не попадает ни один сбой и которое лежит от ближайшего сбоя на расстоянии, в достаточно большое число раз превышающем $|r|$.

Выделим достаточно много начал u' входа u (а значит, и начал $l_1(u')$ пути l_1) так, чтобы выполнялись следующие три условия:

1. Слова $\mathrm{out}(l_1(u'))$ для всех выделенных слов u' заканчиваются внутри r и различны.

2. Состояние, в котором кончается путь $l_1(u')$, одно и то же для всех выделенных u'.

3. Для всех выделенных слов u' множества левосторонней и правосторонней достижимости в $\mathfrak{A}_2$ одни и те же (множеством правосторонней достижимости для u' мы называем множество состояний, из которых существует путь в заключительное состояние с входом u'', где $u'u'' = u$).

План доказательства следующий. Поскольку путь l_1 много раз проходит через одно и то же состояние, из него можно (причем, многими способами) выбросить набор его отрезков, получив допускающий путь с более коротким входом и выходом. Тогда в $\mathfrak{A}_2$ существует допускающий путь с тем же входом и выходом. Свойство 3 позволяет "нарастить" этот путь до пути с входом u (далее будем называть полученный путь *восстановленным*). Сложность в том, чтобы добиться еще и выхода, равного v_1, получив очевидное противоречие. Для этого сначала создадим некоторый "запас" допускающих путей в $\mathfrak{A}_2$ с входом u, чтобы найти среди них такие, к которым (или к их частям) удобно применять критерий конечнозначности.

Будем следующим образом сужать по шагам множество выделенных слов и одновременно строить в $\mathfrak{A}_2$ множество отмеченных состояний. На очередном шаге для каждого неотмеченного состояния q из $\mathfrak{A}_2$ проверяем, существует ли допускающий путь в $\mathfrak{A}_2$ с входом u, у которого начала $l(u')$ кончаются в q для не менее чем $m/\exp(n)$ выделенных слов u', где m – количество выделенных слов на данный момент. Если существует, то отмечаем q, ставим ему в соответствие один из описанных путей, а множество выделенных слов уменьшаем в $\exp(n)$ раз, чтобы все выделенные начала кончались в q. Путь, поставленный в соответствие отмеченному состоянию q, будем обозначать $l(q)$ и называть отмеченным. Когда на очередном шаге ни одно неотмеченное состояние не будет отмечено, процесс останавливается. Так как шагов не более n, в конце процесса количество выделенных слов достаточно велико. Каждый путь $l(q)$ во всех выделенных входах находится в состоянии q.

Разделим все выделенные слова на три примерно равные части из идущих по возрастанию слов, а между левой и средней частью зафиксируем одно из выделенных слов u_b, которое будем называть граничным (см. рис. 11, *а*). Каждому выделенному слову u' из средней части сопоставим множество, состоящее из всех таких наборов $\langle q, q_1, q_2, d\rangle$, что в $\mathfrak{A}_2$ существует путь l из q_1 в q_2 с входом u'', где $u' = u_b u''$, q – отмеченное состояние и разность между $|\mathrm{out}(l)|$ и длиной выхода $l(q)$ на отрезке входа u'' равна d, причем $|d| \leqslant 2n^4$. Число описанных множеств – фиксированная экспонента, поэтому в средней части существует много выделенных слов, которым соответствует одно и то же множество. В этой части считаем выделенными только эти слова.

Так как все выделенные начала пути l_1 оканчиваются в одном состоянии, можно выбросить любое множество отрезков между ними и получить укороченный допускающий путь l_1' в $\mathfrak{A}_1$ с некоторым входом $\bar{u}$. В силу выбора l_1 существует допускающий путь l_2' в $\mathfrak{A}_2$, такой что $\mathrm{in}(l_2') = \mathrm{in}(l_1') = \bar{u}$, $\mathrm{out}(l_2') = \mathrm{out}(l_1')$. Пусть выбросы отрезков произведены в средней части. Под выделенными началами $\bar{u}'$ входа $\bar{u}$ будем понимать его начала, получившиеся из начал первоначального входа u совершением этих выбросов. Покажем, что хотя бы для одного выделенного $\bar{u}'$ из левой и правой частей путь $l_2'(\bar{u}')$ оканчивается в отмеченном состоянии. Будем обозначать через $q(t)$ состояние, в котором оканчивается путь $l_2'(t)$. Рассмотрим на $\mathrm{in}(l_2')$ нача-

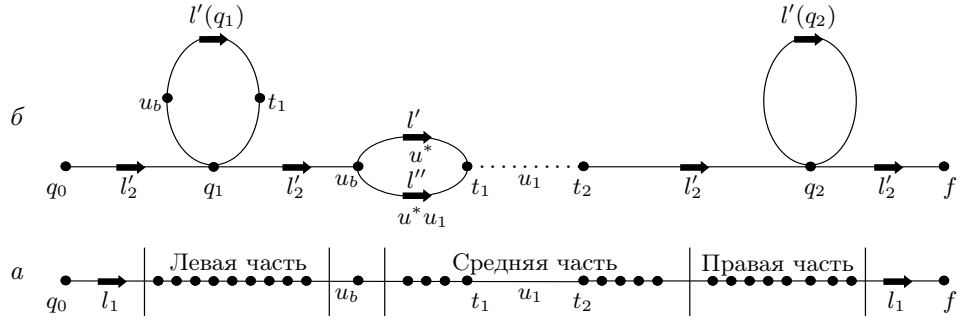

Рис. 11. Обеспечение контролируемой длины выхода восстановленного пути: *а* – структура пути l_1 в преобразователе $\mathfrak{A}_1$. Все состояния, соответствующие точкам (жирным кружочкам), одинаковы; *б* – схема восстановления пути l_2 из пути l'_2 в преобразователе $\mathfrak{A}_2$. Вставляется выброшенный отрезок u_1, так что точки t_1 и t_2 соответствуют одному и тому же состоянию

ло t, соответствующее самому правому выброшенному отрезку. В силу совпадения множеств правосторонней достижимости для всех выделенных слов существует путь из $q(t)$ в заключительное состояние, вход которого равен $u'u''$, где u' – вход самого правого выброшенного отрезка, а u'' – вход l'_2 от t до конца. Соединив старое начало с новым концом, получим новый допускающий путь в $\mathfrak{A}_2$, на входе которого одним выброшенным отрезком меньше. Таким же образом вставим остальные выброшенные отрезки и получим допускающий путь с входом u. В левой части выделенных начал он проходит через некоторое состояние q_1, которое встречается в примерно $1/(3n)$ количества всех выделенных начал. Если бы q_1 не было отмеченным, это противоречило бы завершенности построения отмеченных состояний. Аналогично (вставкой отрезков слева направо) показывается, что в правой части существует выделенное начало пути l'_2, оканчивающееся в отмеченном состоянии q_2.

Итак, мы обнаружили в $\mathfrak{A}_2$ пути $l(q_1)$ и $l(q_2)$ с входом u, находящиеся в удобной (для применения критерия конечнозначности) конфигурации с путем l'_2, который мы умеем восстанавливать до пути с входом u, но пока не умеем обеспечивать выход v_1. Сперва добьемся, чтобы длина выхода восстановленного пути была в некотором смысле определенной.

Так как пути $l(q_1)$ и $l(q_2)$ во всех выделенных началах проходят через q_1 и q_2, то из этих путей можно сделать выбросы на тех же отрезках входа, что и для l_1. Будем обозначать пути с такими выбросами через $l'(q_1)$ и $l'(q_2)$. Из условия (2) теоремы 1 (при $s_1 = q_1$, $s_2 = q_2$, p_1, p_2, p_3 – участки путей $l'(q_1)$, l'_2, $l'(q_2)$ соответственно) следует, что разность длин выходов пути l'_2 на отрезке от u_b до любого выделенного среднего начала u' и пути $l'(q_1)$ на том же участке входа, не превосходит по модулю $2n^4$. Если же на этом участке нет выбросов, то путь $l'(q_1)$ совпадает на нем с путем $l(q_1)$. Учитывая это, рассмотрим следующий процесс восстановления l'_2 до пути с входом u (см. рис. 11, *б*). Пусть самый левый выброшенный отрезок расположен между началами t_1 и t_2 и его вход обозначен через u_1. Обозначим через l' участок пути l'_2 от u_b до t_1, а его вход – через u^*. По построению (совпадение множеств наборов $\langle q, q_1, q_2, d\rangle$ для средних выделенных начал) существует путь l'' из $q(u_b)$ в $q(t_1)$, такой что $\mathrm{in}(l'') = u^*u_1$, а разность $|\mathrm{out}(l'')| - |\mathrm{out}(l')|$ равна длине выхода пути $l(q_1)$ на отрезке входа u_1. Вход нового допускающего пути, получающегося заменой в l'_2 участка l' на l'', содержит на один выброшенный отрезок меньше. Можно сказать, что мы вставили отрезок на входе и при этом выход удлинился на длину выхода пути $l(q_1)$ на вставленном отрезке входа. После этого таким же образом вставляем второй слева отрезок и так далее. В конце получим восстановленный путь с входом u.

Итак, мы взяли под контроль длину выхода восстановленного пути. Теперь обеспечим, чтобы она была равна $|v_1|$.

Выбросом называем удаление из u множества отрезков между выделенными началами вместе с удалением из v_1 соответствующих отрезков выхода пути l_1. Для выброса α будем обозначать через $l'_2(\alpha)$ некоторый допускающий путь с выбросом α в $\mathfrak{A}_2$; через $l_2(\alpha)$ – некоторый восстановленный путь с входом u, построенный описанным выше процессом; $q_1(\alpha)$ – некоторое отмеченное состояние, через которое проходит в левой части выделенных начал путь $l'_2(\alpha)$; $t_1(\alpha)$ – некоторое выделенное начало в левой части, в котором $l_2(\alpha)$ находится в $q_1(\alpha)$; $q_2(\alpha)$ и $t_2(\alpha)$ – то же самое для правой части; $l'_\alpha(q_1)$ – путь $l(q_1)$ с выбросом α; $|\alpha|$ – сумма длин выходов выбрасываемых из l_1 отрезков.

Любой отрезок между двумя соседними выделенными началами из средней части имеет относительно каждого отмеченного состояния q один из трех типов: длина выхода $l(q)$ на этом отрезке может быть больше длины выхода пути l_1 на нем (положительный тип), меньше этой длины (отрицательный тип) или равна ей (нулевой тип). Таким образом, каждому такому отрезку сопоставляется набор пар $\langle q, \text{тип}\rangle$. Всего таких наборов – фиксированная экспонента. Выберем достаточно много непересекающихся отрезков, которым соответствует один и тот же набор. Упорядочим их слева направо и рассмотрим последовательность S выбросов, в которой m-й выброс состоит из первых m отрезков. Каждому выбросу α из S поставим в соответствие пару $\langle q, v\rangle$, где $q = q_1(\alpha)$, $v = \text{out}(l_2(\alpha))$. По теореме 4 количество таких пар – фиксированная экспонента. Пусть α_1 и α_2 – два различных выброса из S, которым соответствует одна и та же пара $\langle q, v\rangle$. Если бы тип всех отрезков относительно q был ненулевым, то, очевидно, разности между длинами выходов восстановленных путей и $|v_1|$ были бы различны для α_1 и α_2, значит, эти выходы тоже были бы различны. Полученное противоречие показывает, что тип всех отрезков относительно q нулевой, что с учетом конструкции вставки дает для α_1 (как и для α_2) равенство $|v| = |v_1|$, где $v = \text{out}(l_2(\alpha_1))$.

Итак, мы обеспечили нужную длину выхода v восстановленного пути. Осталось добиться, чтобы v совпадал с v_1. Если бы замена выхода при восстановлении всегда происходила на том же отрезке r, где по построению расположены выбросы выхода пути l_1, это было бы легко. Действительно, в этом случае (если выходы не совпадают) мы рассмотрели бы левый сбой между v и v_1. Тогда при совершении выбросов изменения выходов в $\mathfrak{A}_1$ и $\mathfrak{A}_2$ происходили бы с одной и той же стороны от сбоя, а значит, и после выбросов выходы не могли бы стать равными. Однако соответствие между входом и выходом на пути l'_2 может быть сильно “искривлено” по сравнению с этим соответствием на пути l_1, тогда замены на выходе могут быть расположены, например, в зоне возможных сбоев. Эта проблема решается следующим образом. Сначала обеспечим, чтобы при восстановлении пути замены выходов были именно вставками, и внесем определенность в содержание этих вставок.

Скажем, что выброс α является выбросом нулевого типа, если тип всех отрезков из α относительно $q_1(\alpha)$ нулевой. Ранее мы показали, что на любом участке средней части с достаточно большим количеством выделенных начал существует достаточно много выбросов нулевого типа: $\alpha_1, \alpha_2, \ldots, \alpha_k$, где все $|\alpha_i|$ различны. Поэтому можно взять достаточно много выбросов на средней части так, чтобы выполнялись следующие условия:

1. Выбросы упорядочены, т.е. каждый отрезок одного из любых двух выбросов лежит строго левее каждого отрезка другого и не пересекается с ним.
2. Все выбросы являются выбросами нулевого типа.
3. Для любых двух различных выбросов α_i, α_j выполнено $|\alpha_i| \neq |\alpha_j|$.
4. Для всех выбросов α состояния $q_1(\alpha)$ и $q_2(\alpha)$ одни и те же (обозначим их через q_1 и q_2).

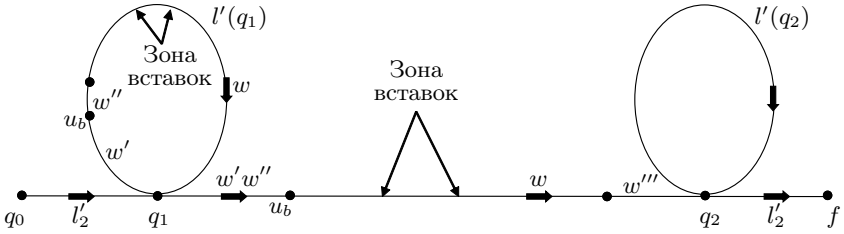

Рис. 12. Обеспечение "вставочного" характера восстановления выходов и уточнение содержания вставок. Показан случай, когда выходы пути $l'_2(\alpha)$ на входах от $t_1(\alpha)$ до u_b и от $t_1(\alpha)$ до $t_2(\alpha)$ длиннее соответствующих выходов пути от $l'_2(\alpha)$. Здесь $w'w''$ и w''' – начала выхода w, $|w''| < n^4$, $|w'''| < n^4$

5. Для всех α разности между длиной выхода $l'_2(\alpha)$ на отрезке от $t_1(\alpha)$ до u_b и длиной выхода $l'_\alpha(q_1)$ на том же отрезке одинаковы (из условия (2) теоремы 1 следует, что эта разность по модулю не превосходит n^4).
6. У всех $l_2(\alpha)$ (а значит, и всех $l'_2(\alpha)$) одинаковый выход от начала до u_b.
7. Все $\mathrm{out}(l_2(\alpha))$ одинаковы (обозначим этот выход через v_2).

Из условия 2 вытекает, что выход пути $l(q_1)$ не пуст на любом отрезке, входящем в выбросы. Тогда из условий (1), (2) теоремы 1 и того, что разность выходов путей $l'_2(\alpha)$ и $l'_\alpha(q_1)$ на отрезке от $t_1(\alpha)$ до $t_2(\alpha)$ не меняется после вставки, следует, что для всех α (кроме, возможно, n^4 самых левых и самых правых) $\mathrm{out}(l_2(\alpha))$ получается из $\mathrm{out}(l'_2(\alpha))$ вставкой выходов пути $l(q_1)$ на отрезках из α (см. рис. 12). Действительно, если w и w_1 – выходы путей $l'_\alpha(q_1)$ и $l(q_1)$ на отрезке от $t_1(\alpha)$ до $t_2(\alpha)$, то выход $l'_2(\alpha)$ на этом отрезке является началом слова w^∞, оканчивающимся в n^4-окрестности конца первого w, а выход $l_2(\alpha)$ на том же отрезке является оканчивающимся в аналогичной окрестности началом слова w_1^∞, где w_1 получается из w вставками, произведенными вне n^4-окрестностей начала и конца.

Таким образом, мы внесли определенность в содержание вставок на выходе. Теперь внесем определенность в расположение этих вставок, чтобы обеспечить их местонахождение вне района сбоев. После этого используем условие 3 для получения противоречия с тем, что $v_1 \neq v_2$.

Из условия 5 следует, что для всех α (кроме, возможно, n^4 самых левых) выходы всех $l'_2(\alpha)$ после начала u_b повторяют выходы путей $l'_\alpha(q_1)$ с одного и того же места на общем начале выходов $l'_\alpha(q_1)$. Учитывая условие 6, заключаем, что если выброс α_i строго левее, чем α_j, то и вставка на выходе для α_i происходит строго левее (считая по длине всего выхода) вставки для α_j. Назовем это свойство монотонностью. Напомним, что $|v_1| = |v_2|$ (в силу условия 2) и для любого выброса, если из v_1 и v_2 выбросить соответствующие отрезки, они станут равными. В силу монотонности существует много таких выбросов, для которых участок выбросов из v_2 не содержит ни левого ни правого сбоя между v_1 и v_2. Возьмем два таких выброса: α_i и α_j, где α_i левее α_j. Напомним, что участок выбросов из v_1 не содержит сбоев по построению отрезка r. Легко видеть, что для того чтобы после выброса α_i слова v_1 и v_2 могли стать равными, необходимо, чтобы выбросы из v_1 и v_2 лежали по разные стороны от обоих сбоев. Пусть выбросы из v_1 лежат слева от левого сбоя, тогда выбросы из v_2 лежат справа от правого сбоя (см. рис. 13, *а*; симметричный случай рассматривается аналогично). Сделаем выброс α_i, сдвинув начало слова v_1 вправо на $|\alpha_i|$, а конец слова v_2 – влево на $|\alpha_i|$ (см. рис. 13, *б*). Обозначим через a букву левого сбоя в v_1, а через b – букву этого сбоя в v_2.

Очевидно, что начало слова v, в которое превратились оба слова v_1 и v_2 после совершения выброса $|\alpha_i|$, периодично с периодом $|\alpha_i|$. Этот период нарушается в точности на расстоянии $|\alpha_i|$ справа от a в букве a' (см. рис. 13, *б*). Действительно,

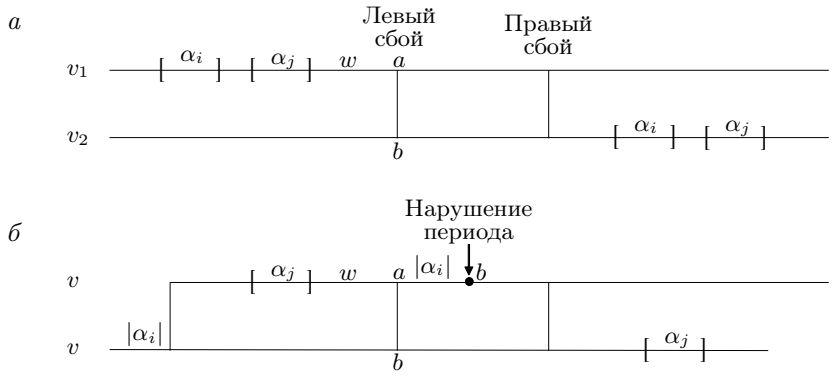

Рис. 13. Схема доказательства равенства выходов пути l_1 и восстановленного пути: *а* – расположение выбросов α_i и α_j относительно сбоев ($a \neq b$) на выходах v_1 и v_2; *б* – после совершения выброса α_i слова v_1 и v_2 превратились в одно и то же слово v, имеющее период длины $|\alpha_i|$ от начала до $b \neq a$

если бы он не нарушался в этой букве, то сбой бы не исчез, а если бы нарушался раньше, сбой появился бы левее. В частности, то же самое утверждение про период выполняется для суффикса w слова v, начинающегося от правого конца α_2. Действительно, по построению подслова r длина начала слова w до сбоя a намного больше величин $|\alpha_i|$, $|\alpha_j|$ и даже их произведения. Проведя те же рассуждения для выброса α_j, получим, что начало слова w периодично с периодом $|\alpha_j|$ и этот период нарушается в точности на расстоянии $|\alpha_j|$ справа от a. Но тогда начало слова w периодично с периодом длины $|\alpha_i||\alpha_j|$. Нарушение этого большого периода является нарушением обоих малых периодов, а нарушение одного из малых периодов является нарушением и большого. Так как $|\alpha_i| \neq |\alpha_j|$ (условие 3), получаем противоречие с тем, что нарушения этих двух периодов произошли в разных местах. ▲

Для полноты изложения рассмотрим также оценку на $|u|$ в условиях доказанной леммы. В [2] доказано, что если преобразователь $\mathfrak{A}_1$ не вложен в конечнозначный преобразователь $\mathfrak{A}_2$, то существует пара $\langle u, v\rangle \in \Gamma(\mathfrak{A}_1)$, $\langle u, v\rangle \notin \Gamma(\mathfrak{A}_2)$, где $|u| \leqslant \exp(\exp(\mathrm{poly}(n)))$. Покажем, как это утверждение можно вывести из леммы 7. Рассмотрим пару $\langle u, v\rangle$, существование которой доказано в лемме 7, с минимальной $|u|$ при данном v. Предположим, что $|u| > \exp(\exp(\mathrm{poly}(n)))$, где степень полинома достаточно велика. Так как $|v| \leqslant \exp(p_1(n))$, то на допускающем пути l_1 из $\mathfrak{A}_1$ с входом u и выходом v существует достаточно длинный (две экспоненты) отрезок с пустым выходом. Выделим на этом отрезке много начал слова u, в которых l_1 находится в одном состоянии. Каждому выделенному началу u' поставим в соответствие множество пар вида $\langle q, v'\rangle$, где $v' \subseteq v$, q – состояние из $\mathfrak{A}_2$, такое что в $\mathfrak{A}_2$ существует путь из начального состояния q_0 в q с входом u' и выходом v'. Из теоремы 4 следует, что количество таких множеств – фиксированная двойная экспонента, поэтому можно выбрать два начала u_1 и u_2, которым соответствует одно и то же множество. По построению в $\mathfrak{A}_2$ существует допускающий путь l_2 с входом, получающимся из u выбрасыванием отрезка от u_1 до u_2, и выходом v. Пусть q – состояние, в котором кончается $l_2(u_1)$. В силу совпадения соответствующих множеств, в $\mathfrak{A}_2$ существует путь l_2' из q_0 в q, такой что $\mathrm{in}(l_2') = u_2$, $\mathrm{out}(l_2') = \mathrm{out}(l_2(u_1))$. Соединяя путь l_2' с продолжением пути l_2, получим допускающий путь в $\mathfrak{A}_2$ с входом u и выходом v. Это противоречит тому, что $\langle u, v\rangle \notin \Gamma(\mathfrak{A}_2)$. Оценка на $|u|$ доказана.

Нижняя оценка на длину выхода v в формулировке леммы 7 экспоненциальна (т.е. невложенность может проявиться лишь на выходах экспоненциальной длины). Эта оценка легко следует из существования описанного в конце § 2 автомата A, который допускает не все слова, но все “экспоненциально короткие”. Достаточно снаб-

дить фиксированным однобуквенным выходом все переходы автомата A с непустым входом, а также автомата, допускающего все слова.

Замечание 5. Авторам не известен ответ на вопрос, существует ли двухэкспоненциальная нижняя оценка на длину входа u в формулировке леммы 7.

§ 6. Разрешимость вложенности преобразователей

Перейдем к вопросам, связанным с разрешимостью вложенности одного преобразователя в другой. В [10] доказана разрешимость выяснения вопроса о вложенности произвольного преобразователя $\mathfrak{A}_1$ в конечнозначный преобразователь $\mathfrak{A}_2$ без оценки на время алгоритма. В [2] доказана разрешимость этого вопроса за время $\exp(\exp(\mathrm{poly}(n)))$, где n – сумма размеров $\mathfrak{A}_1$ и $\mathfrak{A}_2$. Размер используемой памяти у этого алгоритма также имеет порядок двойной экспоненты. В [8] эти оценки улучшены до одной экспоненты, в показателе которой присутствует величина k – значность преобразователя $\mathfrak{A}_2$. Как известно, сама k может быть экспоненциальной от n. Докажем теорему, усиливающую этот результат, построив алгоритм с "чисто" экспоненциальной памятью.

Теорема 5. *Существует детерминированный алгоритм, использующий память размера* $\exp(\mathrm{poly}(n))$, *который по произвольному преобразователю* $\mathfrak{A}_1$ *и конечнозначному преобразователю* $\mathfrak{A}_2$ *решает вопрос о вложенности* $\mathfrak{A}_1$ *в* $\mathfrak{A}_2$.

Доказательство. Опишем недетерминированный алгоритм, подтверждающий невложенность $\mathfrak{A}_1$ в $\mathfrak{A}_2$ и работающий на экспоненциальной памяти. Сначала алгоритм угадывает выход v, где $|v| \leqslant \exp(p_1(n))$, и записывает v на ленте. После этого по шагам угадывается вход и путь в $\mathfrak{A}_1$. В каждый момент на ленте указано $v_1 \subseteq v$ – выход угаданного начала пути в $\mathfrak{A}_1$ и множество пар $\langle v', q\rangle$, где $v' \subseteq v$, q – состояние из $\mathfrak{A}_2$, такое что существует путь из начального состояния в q с угаданным к данному моменту входом и выходом v'. На очередном шаге угадывается очередная буква a входа и очередной переход в $\mathfrak{A}_1$ с входом a. Алгоритм проверяет, что выход у этого перехода продолжает v_1 вдоль v, и дописывает его к v_1. Затем для каждой пары $\langle v', q\rangle$ и каждого перехода в $\mathfrak{A}_2$ из q с входом a и выходом, который продолжает v' вдоль v и не выводит за его пределы, естественным образом строится новая пара. Повторяющиеся пары удаляются из получившегося нового множества. Алгоритм работает до тех пор, пока v_1 – начало v и множество пар непусто. Если $v_1 = v$ и в множестве пар нет пары $\langle v, f\rangle$, где f – заключительное состояние, то алгоритм обнаруживает невложенность $\mathfrak{A}_1$ в $\mathfrak{A}_2$. Правильность работы и экспоненциальная память этого алгоритма очевидны. По теореме Сэвича (см. [11, с. 489]) недетерминированный алгоритм, использующий память размера S, может быть переделан в детерминированный, распознающий тот же язык и использующий память размера S^2. Отсюда следует существование искомого алгоритма. ▲

Конструкция выбросов, использованная для доказательства теоремы 5, позволяет получить следующий результат.

Теорема 6. *Пусть* $\mathfrak{A}_1$ *и* $\mathfrak{A}_2$ *– конечнозначные преобразователи без пустых входов и* $\mathfrak{A}_1$ *вложен в* $\mathfrak{A}_2$. *Тогда для любого допускающего пути* l_1 *в* $\mathfrak{A}_1$ *с входом* u *и выходом* v *существует допускающий путь* l_2 *в* $\mathfrak{A}_2$ *с тем же входом и выходом, такой что для любого* $u' \subseteq u$ *выполняется* $|d(l_1, l_2, u')| \leqslant \exp(\mathrm{poly}(n))$.

Доказательство. Обозначим через $M_1(u, v)$ и $M_2(u, v)$ множества допускающих путей с входом u и выходом v в $\mathfrak{A}_1$ и $\mathfrak{A}_2$ соответственно. Предположим вопреки утверждению теоремы, что существует путь $l_1 \in M_1(u, v)$, такой что для любого пути $l_2 \in M_2(u, v)$ существует $u' \subseteq u$, такое что $|d(l_1, l_2, u')| > k \geqslant \exp(\mathrm{poly}(n))$, где степень полинома достаточно велика. По теореме 4 в $\mathfrak{A}_2$ существует не более чем экспоненциальное множество M путей из $M_2(u, v)$, такое что для любого пути $l \in M_2(u, v)$

существует $l' \in M$, такой что для любого $u' \subseteq u$ имеем $|d(l, l', u')| \leqslant 2n^4$. Рассмотрим множество P допускающих путей l в $\mathfrak{A}_1$, обладающих следующим свойством: на входе l существует множество T из не более $|M|$ начал, такое что для любого пути $l' \in M_2(\mathrm{in}(l), \mathrm{out}(l))$ существует начало $u' \in T$, такое что $|d(l, l', u')| > k_1 = k - 2n^4$. Легко видеть, что $l_1 \in P$, поэтому P не пусто. Пусть l_0 – путь из P с минимальной длиной выхода, обозначим $u_0 = \mathrm{in}(l_0)$, $v_0 = \mathrm{out}(l_0)$. Соответствующее ему множество начал обозначим через T_0. Из наших предположений следует, что $|v_0| > k_1$. Поэтому существует отрезок r пути l_0 с достаточно большим выходом, не содержащий начал из T_0. Для r повторим всю конструкцию выбросов, описанную в доказательстве леммы 7 (обозначениям l_1, u, v_1 из леммы 7 теперь соответствуют l_0, u_0, v_0). Единственное отличие будет состоять в том, что в качестве пути l'_2 в $\mathfrak{A}_2$ для пути l'_0 в $\mathfrak{A}_1$ с выбросами будем брать не произвольный путь, а такой что для любого начала $u' \in T_0$ выполняется $|d(l'_0, l'_2, u')| \leqslant k_1$. Этот путь существует в силу условия выбора l_0 и того, что $|\mathrm{out}(l'_0)| < |\mathrm{out}(l_0)|$. Повторив соответствующее рассуждение, легко доказать, что существует такой выброс нулевого типа из пути l_0, что для восстановленного пути l_2 в $\mathfrak{A}_2$ выполнено $\mathrm{in}(l_2) = u_0$, $\mathrm{out}(l_2) = v_0$. Последнее равенство следует из того, что при доказательстве леммы 7 мы получили противоречие, предполагая, что для всех выбросов α выполнено $\mathrm{out}(l_2(\alpha)) \neq v_0$. Легко видеть, что в силу нулевого типа и конструкции вставки, при вставке отрезка отклонение $d(l'_0, l'_2, u')$ пути в $\mathfrak{A}_1$ от пути в $\mathfrak{A}_2$ может меняться только для u', лежащих между граничным началом u_b и вставляемым на входе отрезком (точнее, $d(l''_0, l''_2, u'') = d(l'_0, l'_2, u')$, где l''_0, l''_2 – пути до вставки, l'_0, l'_2 – пути после вставки, $u' = u''$, если u' оканчивается левее вставки, и $u' = (u''$ с вставкой), если правее). Следовательно, за пределами отрезка r, и в частности, на всех началах $u' \in T_0$ выполняется $|d(l_0, l_2, u')| \leqslant k_1$. Получили противоречие с тем, что $l_0 \in P$. ▲

В одном частном случае результат теоремы 5 можно усилить. Будем говорить, что преобразователь $\mathfrak{A}$ *имеет конечную задержку*, если существует такое натуральное c, что для любого пути l из условия $|\mathrm{in}(l)| \geqslant c$ следует $|\mathrm{out}(l)| > 0$. Очевидно, что $c \leqslant \mathrm{poly}(n)$, где $n = |\mathfrak{A}|$ (если преобразователь конечнозначный и редуцированный, то его конечная задержка, очевидно, эквивалентна отсутствию циклов с пустым выходом).

Теорема 7. *Существует недетерминированный алгоритм, который за недетерминированное время* $\exp(\mathrm{poly}(n))$ *подтверждает невложенность произвольного преобразователя* $\mathfrak{A}_1$ *в конечнозначный преобразователь* $\mathfrak{A}_2$, *где* $\mathfrak{A}_2$ *имеет конечную задержку.*

Для доказательства теоремы нам потребуется следующая лемма, усиливающая в этом частном случае лемму 7.

Лемма 8. *Если преобразователь* $\mathfrak{A}_1$ *не вложен в конечнозначный преобразователь* $\mathfrak{A}_2$ *с конечной задержкой, то существует пара* $\langle u, v\rangle \in \Gamma(\mathfrak{A}_1)$, $\langle u, v\rangle \notin \Gamma(\mathfrak{A}_2)$, *такая что* $|u| \leqslant \exp(p_2(n))$, *где* $p_2(n)$ – *некоторый полином.*

Доказательство. Пусть l_1 – допускающий путь в $\mathfrak{A}_1$ минимальной длины, такой что $\langle \mathrm{in}(l_1), \mathrm{out}(l_1)\rangle \notin \Gamma(\mathfrak{A}_2)$. Обозначим $u = \mathrm{in}(l_1)$, $v_1 = \mathrm{out}(l_1)$. Предположим, что $|u|$ достаточно велико. Возможны два случая.

Случай 1. $|v_1| > \exp(p_1(n))$, где $p_1(n)$ – полином из леммы 7. В этом случае приводим это предположение к противоречию точно так же, как в доказательстве леммы 7.

Случай 2. $|v_1| \leqslant \exp(p_1(n))$. В этом случае существует достаточно длинный участок r пути l_1 с пустым выходом. На нем будем делать выбросы так же, как в доказательстве леммы 7, только вместо требования, чтобы выход выбрасываемых отрезков был непуст, потребуем, чтобы длина входа каждого выбрасываемого отрезка была больше c. Повторив соответствующее рассуждение, докажем существование выброса α нулевого типа. Но в силу свойства конечной задержки выход любого от-

меченного пути в $\mathfrak{A}_2$ непустой на выбрасываемых отрезках входа. Это противоречит тому, что выход участка r пустой. ▲

Доказательство теоремы 7. Опишем требуемый алгоритм. Он угадывает вход u и выход v, где $|u| \leqslant \exp(p_2(n))$, $|v| \leqslant n|u|$. После этого детерминированно определяется, есть ли в $\mathfrak{A}_1$ и $\mathfrak{A}_2$ допускающий путь с входом u и выходом v. Для этого для каждого $u' \subseteq u$, где u' увеличивается побуквенно, находится множество пар $\langle v', q\rangle$, где $v' \subseteq v$, q – состояние, такое что существует путь из начального состояния в q с входом u' и выходом v'. Подробности очевидны. Алгоритм обнаруживает невложенность $\mathfrak{A}_1$ в $\mathfrak{A}_2$, если $\langle u, v\rangle \in \Gamma(\mathfrak{A}_1)$, $\langle u, v\rangle \notin \Gamma(\mathfrak{A}_2)$. Очевидно, время работы этого алгоритма примерно $n|u||v|$. ▲

Второй из авторов выражает благодарность Ю.Л. Притыкину и рецензенту, которые внимательно прочитали текст и высказали много полезных замечаний, способствовавших существенному улучшению статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Weber A.* Über die Mehrdeutigkeit und Wertigkeit von endlichen Automaten und Transducern: Dissertation. Goethe-Universität Frankfurt am Main, Germany, 1987.
2. *Weber A.* A Decomposition Theorem for Finite Valued Transducers and an Application to the Equivalence Problem // Proc. 13th Int. Sympos. on Mathematical Foundations of Computer Science (MFCS'88). Carlsbad, Czechoslovakia. August 29 – September 2, 1988. Lect. Notes Comput. Sci. V. 324. Berlin: Springer, 1988. P. 552–562.
3. *Weber A.* On the Valuedness of Finite Transducers // Acta Inform. 1990. V. 27. № 8. P. 749–780.
4. *Weber A.* Decomposing a k-Valued Transducer into k Unambiguous Ones // RAIRO Inform. Théor. Appl. 1996. V. 30. № 5. P. 379–413.
5. *Sakarovitch J., de Souza R.* On the Decomposition of k-Valued Rational Relations // Proc. 25th Int. Sympos. on Theoretical Aspects of Computer Science (STACS'2008). Bordeaux, France. February 21–23, 2008. Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2008. P. 621–632.
6. *Sakarovitch J., de Souza R.* Lexicographic Decomposition of k-Valued Transducers // Theory Comput. Syst. 2010. V. 47. № 3. P. 758–785.
7. *Sakarovitch J., de Souza R.* On the Decidability of Bounded Valuedness for Transducers // Proc. 33rd Int. Sympos. on Mathematical Foundations of Computer Science (MFCS'2008). Toruń, Poland. August 25–29, 2008. Lect. Notes Comput. Sci. V. 5162. Berlin: Springer, 2008. P. 588–600.
8. *de Souza R.* On the Decidability of the Equivalence for k-Valued Transducers // Proc. 12th Int. Conf. on Developments in Language Theory (DLT'2008). Kyoto, Japan. September 16–19, 2008. Lect. Notes Comput. Sci. V. 5257. Berlin: Springer, 2008. P. 252–263.
9. *Sakarovitch J.* Elements of Automata Theory. Cambridge: Cambridge Univ. Press, 2009.
10. *Culik K., II, Karhumäki J.* The Equivalence of Finite Valued Transducers (on HDT0L Languages) is Decidable // Theoret. Comput. Sci. 1986. V. 47. № 1. P. 71–84.
11. *Хопкрофт Д.Э., Мотвани Р., Ульман Д.Д.* Введение в теорию автоматов, языков и вычислений. М.: Издательский дом "Вильямс", 2002.

Мучник Андрей Альбертович
(24.02.1958 – 18.03.2007)
Горбунов Константин Юрьевич
Институт проблем передачи информации
им А.А.Харкевича РАН
gorbunov@iitp.ru

Поступила в редакцию
12.02.2014
После переработки
03.06.2015