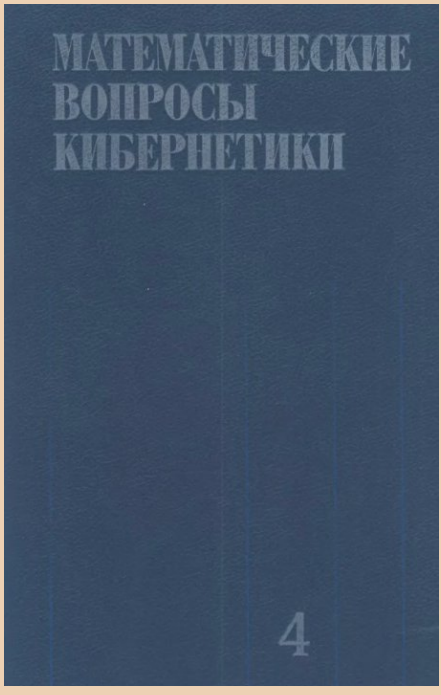
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 4



В. В. Кочергин

О сложности вычислений в конечных абелевых группах

Рекомендуемая форма библиографической ссылки: Кочергин В. В. О сложности вычислений в конечных абелевых группах // Математические вопросы кибернетики. Вып. 4. — М.: Физматлит, 1992. — С. 178–217. URL: http://library.keldysh.ru/mvk.asp?id=1992-178

О СЛОЖНОСТИ ВЫЧИСЛЕНИЙ В КОНЕЧНЫХ АБЕЛЕВЫХ ГРУППАХ

В. В. КОЧЕРГИН

(МОСКВА)

Введение

Пусть G — абелева группа. Будем считать, что групповая операция — умножение.

Множество $Б_G = \{g_1, g_2, \ldots, g_q\}$ элементов конечнопорожденной абелевой группы G будем называть базисом в G, если G есть прямое произведение циклических групп, порожденных элементами $g_1, g_2, \ldots, g_q$:

$$G = \langle g_1\rangle \times \langle g_2\rangle \times \ldots \times \langle g_q\rangle.$$

Объект изучения — *схемы из функциональных элементов умножения*; на входы схем подаются базисные элементы группы G, а сами схемы состоят из двухвходовых элементов, которые по двум представителям группы G, поступающим на входы, реализуют их произведение.

Пусть S — такая схема. Обозначим через $L(S)$ *сложность схемы* S, т. е. суммарное число функциональных элементов.

Через $L(g, Б_G)$ обозначим *сложность реализации* элемента g *конечной абелевой группы* G *в базисе* $Б_G$, определяемую равенством $L(g, Б_G) = \min L(S)$, где минимум берется по всем схемам S в базисе $Б_G$, реализующим g. Будем считать (это не принципиально), что $L(e, Б_G) = 0$, где e — единица группы G.

Сложность $L(G, Б_G)$ *конечной абелевой группы* G *в базисе* $Б_G$ определим так: $L(G, Б_G) = \max\limits_{g\in G} L(g, Б_G)$.

Обозначим множество всех базисов конечной абелевой группы G через $\mathfrak{B}_G$.

Для каждой конечной абелевой группы G введем понятие *сложности* этой *группы* $L(G)$, уже не зависящее от выбора базиса:

$$L(G) = \max_{Б_G\in\mathfrak{B}_G} L(G, Б_G).$$

Далее, определим функцию Шеннона сложности реализации конечных абелевых групп следующим образом:

$$L(n) = \max L(G),$$

где максимум берется по всем абелевым группам порядка n.

В § 1 работы исследуется вопрос о поведении функции $L(G, Б_G)$ при $|G| \to \infty$. Доказано, что *)

$$L(G, Б_G) = \frac{\log|G|}{\log\log|G|}\left(1 + O\left(\left(\frac{\log\log\log|G|}{\log\log|G|}\right)^{1/2}\right)\right) + O(\max(p, q)),$$

*) Здесь и далее $\log x$ означает $\log_2 x$.

где p — логарифм значения максимального порядка среди элементов базиса $Б_G$, а q — число элементов базиса $Б_G$. В частности, если выполнено условие

$$\frac{\max(p, q)\log(\max(p, q))}{\log|G|} \to 0,$$

то

$$L(G, Б_G) \sim \frac{\log|G|}{\log\log|G|}.$$

В ходе доказательства этих утверждений получены некоторые оценки сложности реализации двоичных ступенчатых матриц (таблиц) вентильными схемами специального вида.

В § 2 изучается асимптотическое поведение функции Шеннона. С использованием результатов § 1 доказано, что

$$L(n) - \log n \sim \frac{\log n}{\log\log n}.$$

§ 1. Исследование функции $L(G, Б_G)$

Нижняя оценка. Пусть $Б_G = \{g_1, g_2, \ldots, g_q\}$ — базис конечной абелевой группы G, причем порядки базисных элементов равны соответственно $k_1, k_2, \ldots, k_q$ (далее будем считать, что элементы базиса упорядочены по возрастанию своих порядков, т. е. $k_1 \leqslant k_2 \leqslant \ldots \leqslant k_q$). Тогда $G = \langle g_1\rangle_{k_1} \times \langle g_2\rangle_{k_2} \times \ldots \times \langle g_q\rangle_{k_q}$.

Введем обозначения:

$$p_i = [\log(k_i - 1)] + 1, \tag{1}$$

$$p = [\log(\max_{1\leqslant i\leqslant q} k_i - 1)] + 1 = [\log(k_q - 1)] + 1. \tag{2}$$

Теорема 1. $L(G, Б_G) \geqslant p + q - 2$.

Доказательство. Обозначим $g_0 = g_1 g_2 \ldots g_{q-1} g_q^{2^{p-1}}$. Заметим, что

$$L(g_0, Б_G) \geqslant L\left(g_q^{2^{p-1}}, Б_G\right) + q - 1, \tag{3}$$

так как из любой схемы, реализующей элемент $g_i g_{i+1} \ldots g_q^{2^{p-1}}$, можно получить схему сложности, по крайней мере, на единицу меньше, реализующую элемент $g_{i+1} g_{i+2} \ldots g_q^{2^{p-1}}$, последовательно удалив все элементы умножения, на оба входа которых подаются некоторые степени g_i, а также все элементы умножения, на один вход которых подается степень элемента g_i, а на другой — элемент группы G, порожденный только базисными элементами $g_{i+1}, g_{i+2}, \ldots, g_q$.

Кроме того,

$$L\left(g_q^{2^{p-1}}, Б_G\right) \geqslant p - 1, \tag{4}$$

так как s-й элемент умножения в занумерованной в естественном порядке схеме, реализующей элемент $g_q^{2^{p-1}}$, вычисляет элемент $f(g_1, g_2, \ldots, g_{q-1}) g_q^r$, где $r \leqslant 2^s$.

Используя (3) и (4), получаем $L(g_0, Б_G) \geqslant p + q - 2$.

Теорема доказана.

Теорема 2. *Для произвольного* $\varepsilon > 0$ *найдется* $m(\varepsilon) > 0$ *такое, что для любой конечной абелевой группы* G, *удовлетворяющей условию* $|G| > m(\varepsilon)$, *в произвольном базисе* $Б_G$ *справедлива оценка*

$$L(G, Б_G) \geqslant \frac{\log|G|}{\log\log|G|}\left(1 + (1 - \varepsilon)\frac{\log\log\log|G|}{\log\log|G|}\right).$$

Доказательство. Утверждение теоремы будем доказывать мощностным методом.

Схему, реализующую элемент $g \in G$ в базисе $Б_G$, будем называть минимальной, если не существует схемы в базисе $Б_G$, реализующей g с меньшей сложностью.

Введем обозначения:

$N(G, Б_G, L)$ — число элементов группы G, которые можно реализовать схемами из элементов умножения в базисе $Б_G$ со сложностью не более L;

$n(Б_G, L)$ — число различных минимальных схем из элементов умножения в базисе $Б_G$ сложности не более L;

$n'(Б_G, l)$ — число различных минимальных схем из элементов умножения в базисе $Б_G$ сложности l.

Оценим $n'(Б_G, l)$, $l \geqslant 1$. Каждой схеме в базисе $Б_G$ сложности l сопоставим $l!$ таблиц размера $l \times 2$ следующим образом. Занумеруем все элементы схемы ($l!$ вариантов). Клетка в i-й строке ($1 \leqslant i \leqslant l$) на j-м месте ($j = 1, 2$) заполняется в зависимости от того, что подается на j-й вход элемента с номером i — базисный элемент g_s или выход элемента умножения с номером t. В первом случае в клетке будет g_s, а во втором — t. Строка, соответствующая элементу умножения, выход которого совпадает с выходом схемы, помечается звездочкой. На рис. 1 показан пример построения таблицы по занумерованной схеме.

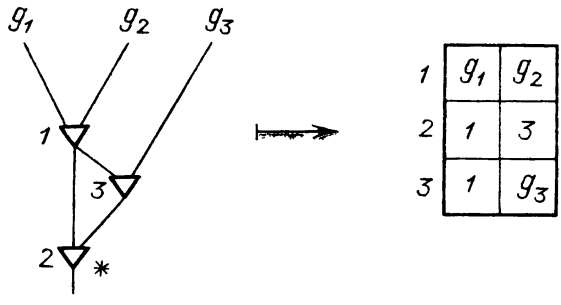


Рис. 1

Очевидно, что все $l!$ таблиц, соответствующих одной минимальной схеме, различны, и разным схемам соответствуют различные таблицы.

Всего таблиц такого вида не более $(q+l)^{2l} \cdot l$. Поэтому $n'(Б_G, l) \leqslant (q+l)^{2l} l/l!$. Тогда при $L \geqslant 2$

$$N(G, Б_G, L) \leqslant n(Б_G, L) \leqslant$$

$$\leqslant q + 1 + \sum_{l=1}^{L} n'(Б_G, l) \leqslant q + 1 + \sum_{l=1}^{L} \frac{(q+l)^{2l} l}{l!} \leqslant \frac{L^2 (q+l)^{2L}}{L!}.$$

Отсюда, используя неравенство $n! \geqslant (n/3)^n$ и теорему 1, получаем:

$$N(G, Б_G, L(G, Б_G)) \leqslant$$

$$\leqslant L^2(G, Б_G)(q + L(G, Б_G))^{2L(G, Б_G)} \cdot \left(\frac{3}{L(G, Б_G)}\right)^{L(G, Б_G)} \leqslant$$

$$\leqslant L^2(G, Б_G)(2L(G, Б_G) + 1)^{2L(G, Б_G)} \cdot \left(\frac{3}{L(G, Б_G)}\right)^{L(G, Б_G)} \leqslant$$

$$\leqslant (27 L(G, Б_G))^{L(G, Б_G)+2}$$

Далее, с одной стороны, из определения $N(G, Б_G, L)$ следует, что

$$N(G, Б_G, L(G, Б_G)) = |G|. \tag{5}$$

Предположим, что

$$L(G, Б_G) \leqslant \frac{\log |G|}{\log \log |G|} \left(1 + (1 - \varepsilon) \frac{\log \log \log |G|}{\log \log |G|}\right) \tag{6}$$

Тогда, с другой стороны,

$$\log \frac{N(G, Б_G, L(G, Б_G))}{|G|} \leqslant$$

$$\leqslant \left(\frac{\log|G|}{\log\log|G|}\left(1+(1-\varepsilon)\frac{\log\log\log|G|}{\log\log|G|}\right)+2\right)\log\frac{27\cdot 2\log|G|}{\log\log|G|}-\log|G|\leqslant$$

$$\leqslant (3\log 3+1)\left(\frac{\log|G|}{\log\log|G|}+(1-\varepsilon)\frac{\log|G|\log\log\log|G|}{(\log\log|G|)^2}+2\right)+$$

$$+2\log\log|G|-\varepsilon\frac{\log|G|\log\log\log|G|}{\log\log|G|}.$$

Последнее выражение стремится к $-\infty$ при $|G|\to\infty$. Поэтому найдется $m(\varepsilon)>0$ такое, что для любой конечной абелевой группы G, удовлетворяющей условию $|G|>m(\varepsilon)$, выполняется неравенство $\log(N(G, Б_G, L(G, Б_G))/|G|)<0$, что противоречит равенству (5).

Следовательно, для любой конечной абелевой группы G, удовлетворяющей условию $|G|>m(\varepsilon)$, в любом базисе $Б_G$ предположение (6) неверно, т. е.

$$L(G, Б_G)>\frac{\log|G|}{\log\log|G|}\left(1+(1-\varepsilon)\frac{\log\log\log|G|}{\log\log|G|}\right).$$

Теорема доказана.

Верхняя оценка. Доказательство верхней оценки сводится к доказательству аналогичной оценки сложности реализации двоичных ступенчатых матриц (таблиц) вентильными схемами специального вида.

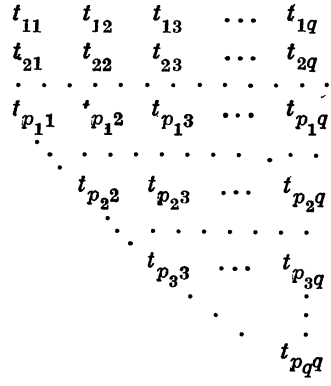


Рис. 2

Будем называть двоичную таблицу указанного на рис. 2 вида *ступенчатой матрицей* или просто *таблицей* размера $p\times q$, если $1\leqslant p_1\leqslant p_2\leqslant\ldots\leqslant p_q=p$.

Обозначим длину i-й строки таблицы через q_i. Тогда

$$q=q_1\geqslant q_2\geqslant\ldots\geqslant q_p\geqslant 1. \tag{7}$$

Кроме того, площадь таблицы T (т. е. величину $|\{t_{ij}|t_{ij}\in T\}|$) обозначим $H(T)$, число строк таблицы $T-p(T)$, число столбцов таблицы $T-q(T)$. Далее, если не может возникнуть неопределенность, иногда будем писать просто H, p, q.

Заметим, что

$$H=\sum_{i=1}^{p}q_i=\sum_{j=1}^{q}p_j. \tag{8}$$

Каждая таблица T размера $p\times q$ порождает двоичную матрицу $A(T)=(a_{ij})_{p\times q}$ по правилу:

$$a_{ij}=\begin{cases}t_{ij}, & \text{если } 1\leqslant i\leqslant p_j,\\ 0, & \text{если } p_j<i\leqslant p.\end{cases} \tag{9}$$

Введем понятие 0-1-вентильной схемы.

Ориентированный граф S будем называть 0-1-*вентильной схемой, реализующей двоичную матрицу* A *размера* $p \times q$, если:

1) в S выделено q вершин — входных полюсов и p вершин — выходных полюсов;

2) в S нет ориентированных путей от одного входа к другому, от одного выхода к другому, от выхода к входу;

3) для любой пары (j, i), $1 \leqslant j \leqslant q$, $1 \leqslant i \leqslant p$, число ориентированных путей от j-го входа к i-му выходу равно a_{ij}.

Обозначим через $L_{\text{вс}}(S)$ *сложность* 0-1-*вентильной схемы* S, т. е. число ребер (вентилей) схемы S. Определим *сложность* $L_{\text{вс}}(A)$ *реализации двоичной матрицы* A 0-1-*вентильными схемами* так: $L_{\text{вс}}(A) = \min L_{\text{вс}}(S)$, где минимум берется по всем 0-1-вентильным схемам S, реализующим матрицу A.

Покажем теперь, как можно свести задачу о верхней оценке сложности реализации абелевой группы схемами из функциональных элементов умножения к задаче о верхней оценке сложности реализации 0-1-вентильными схемами матриц, специальным образом построенных по элементам абелевой группы.

Рассмотрим абелеву группу $G = \langle g_1 \rangle_{k_1} \times \langle g_2 \rangle_{k_2} \times \ldots \times \langle g_q \rangle_{k_q}$. Пусть g — произвольный элемент G. Его можно представить в таком виде:

$$g = g_1^{t_1} g_2^{t_2} \ldots g_q^{t_q}, \quad t_1 \leqslant k_1 - 1, \ldots, t_q \leqslant k_q - 1. \tag{10}$$

Так как $t_j \leqslant k_j - 1$, $1 \leqslant j \leqslant q$, то, вследствие (1), каждое t_j можно представить в следующем виде:

$$t_j = t_{1j} \cdot 2^0 + t_{2j} \cdot 2^1 + \ldots + t_{p_j j} \cdot 2^{p_j - 1}, \quad t_{ij} \in \{0, 1\}. \tag{11}$$

Теперь элементу g сопоставим таблицу $T_g^{B_G}$ из определенных выше элементов t_{ij} (j-й столбец таблицы имеет высоту p_j), аналогичную таблице, показанной на рис. 2.

Заметим, что в силу (1),

$$H\left(T_g^{B_G}\right) = \sum_{j=1}^{q} p_j = \sum_{j=1}^{q} [\log (k_j - 1)] + 1 \leqslant \sum_{j=1}^{q} \log k_j + q = \log |G| + q, \tag{12}$$

$$H\left(T_g^{B_G}\right) = \sum_{j=1}^{q} [\log (k_j - 1)] + 1 \geqslant \sum_{j=1}^{q} \log k_j = \log |G|. \tag{13}$$

Лемма 1. *Для любого элемента* g *произвольной конечной абелевой группы* G, *заданной своим базисом* B_G, *справедливо неравенство*

$$L(g, B_G) \leqslant L_{\text{вс}}\left(A\left(T_g^{B_G}\right)\right) + 2p - 2.$$

Доказательство. Преобразуем произвольную минимальную 0-1-вентильную схему $S_{\text{вс}}$, реализующую матрицу $A\left(T_g^{B_G}\right)$, в схему из функциональных элементов $S_{\text{сфэ}}$ над базисом B_G по следующим правилам:

1) j-му входу вентильной схемы припишем базисный элемент g_j, $1 \leqslant j \leqslant q$.

2) Каждый фрагмент вентильной схемы, состоящий из вершины, не являющейся входом, и всех инцидентных ей ребер, преобразуем как показано на рис. 3.

3) i-м выходом, $1 \leqslant i \leqslant p$, схемы из функциональных элементов будет выход последнего элемента умножения среди тех, которые получены

путем преобразования по правилу 2) пучка вентилей, входящего в i-й выход исходной вентильной схемы.

Из минимальности исходной 0-1-вентильной схемы и того, что в ней для любой пары из входа и выхода существует не более одного пути, ведущего от первого ко второму, следует, что также, как и в исходной вентильной схеме, в схеме, полученной после всех преобразований по

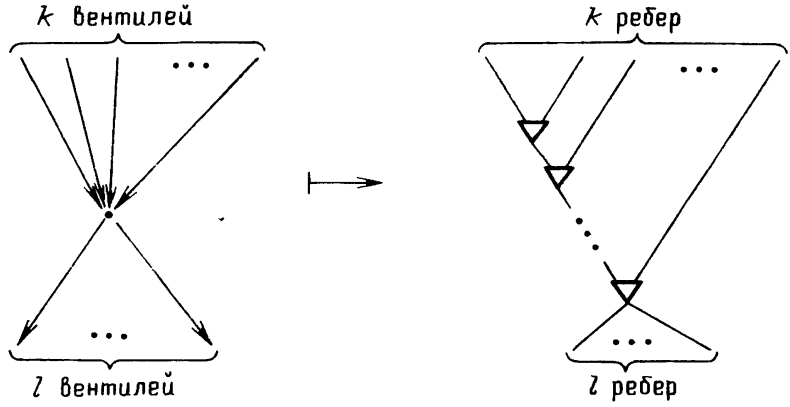


Рис. 3

правилам 1)—3), не будет ориентированных циклов, т. е. получится действительно схема из функциональных элементов.

Заметим, что сложность полученной схемы из функциональных элементов не превосходит числа вентилей в исходной вентильной схеме

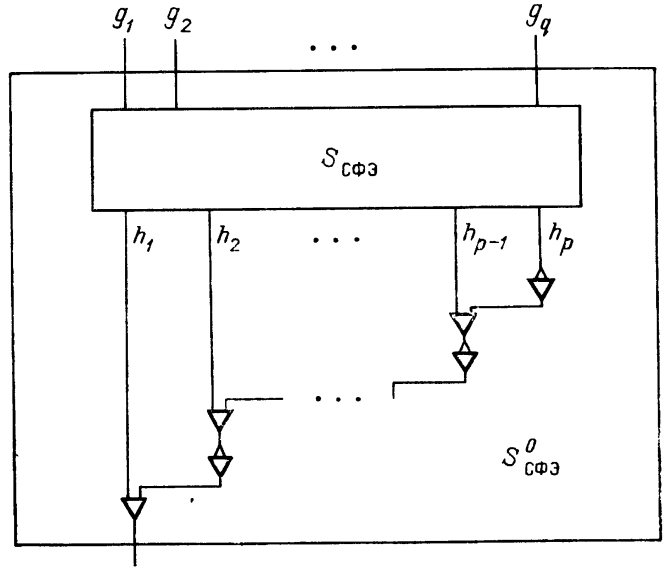


Рис. 4

(точнее равна разности числа вентилей и числа невходовых вершин вентильной схемы).

Очевидно, что на i-м выходе $S_{\text{сфэ}}$ будет реализовываться элемент

$$h_i = g_1^{a_{i1}} g_2^{a_{i2}} \dots g_q^{a_{iq}}. \tag{14}$$

Построим схему $S^0_{\text{сфэ}}$, как показано на рис. 4. Обозначим элемент группы G, реализуемый схемой $S^0_{\text{сфэ}}$, через g_0. Из построения схемы $S^0_{\text{сфэ}}$

и (14), (9), (11), (10) следует, что

$$g_0 = (\ldots((h_p^2 h_{p-1})^2 \cdot h_{p-2})^2 \ldots h_2)^2 \cdot h_1 = \prod_{i=1}^{p} h_i^{2^{i-1}} =$$

$$= \prod_{i=1}^{p} \left(\prod_{j=1}^{q} g_j^{a_{ij}} \right)^{2^{i-1}} = \prod_{i=1}^{p} \prod_{j=1}^{q} g_j^{a_{ij} \cdot 2^{i-1}} = \prod_{j=1}^{q} \prod_{i=1}^{p} g^{a_{ij} \cdot 2^{i-1}} =$$

$$= \prod_{j=1}^{q} g_j^{\sum_{i=1}^{p} a_{ij} 2^{i-1}} = \prod_{j=1}^{q} g_j^{\sum_{i=1}^{p_j} t_{ij} \cdot 2^{i-1}} = \prod_{j=1}^{q} g_j^{t_j} = g.$$

Поэтому

$$L(g, Б_G) \leqslant L(S^0_{\text{сфэ}}) \leqslant L_{\text{вс}}(A(T_g^{Б_G})) + 2p - 2.$$

Лемма доказана.

Замечание. Для любого элемента g произвольной конечнопорожденной абелевой группы G, представимого в базисе $Б_G$ в виде произведения неотрицательных степеней элементов базиса, можно также определить таблицу $\widehat{T}_g^{Б_G}$, выписав по столбцам двоичные записи степеней базисных элементов из такого представления в порядке возрастания этих степеней. Дословно повторяя доказательство леммы 1, легко убедиться в справедливости неравенства

$$L(g, Б_G) \leqslant L_{\text{вс}}(A(\widehat{T}_g^{Б_G})) + p(\widehat{T}_g^{Б_G}) - 2.$$

Теперь будем оценивать сверху сложность реализации 0-1-вентильными схемами двоичных матриц вида $A(T)$, где T — некоторая таблица.

Обозначим через $A^* = (a^*_{ij})_{m \times n}$ матрицу, полученную из матрицы $A = (a_{ij})_{n \times m}$ транспонированием.

Лемма 2. *Для любой двоичной матрицы A*

$$L_{\text{вс}}(A^*) = L_{\text{вс}}(A).$$

Доказательство. Утверждение леммы следует из того, что при изменении направлений всех ребер 0-1-вентильной схемы, реализующей матрицу A, на противоположные получается 0-1-вентильная схема, реализующая матрицу A^*, и наоборот. Лемма доказана.

Введем функцию

$$\overline{\log} x = \begin{cases} \log x, & \text{при } x \geqslant 2, \\ 1, & \text{при } x < 2. \end{cases}$$

Заметим, что эта функция монотонна.

Лемма 3. *Существуют положительные c_1 и c_2 такие, что для любой таблицы T, удовлетворяющей условиям*

$$q(T) \geqslant p(T), \tag{15}$$

$$H(T) \geqslant p(T) \cdot q^{1/3}(T), \tag{16}$$

справедливо неравенство

$$L_{\text{вс}}(A(T)) \leqslant c_1 \frac{H(T)}{\overline{\log} H(T)} + c_2 q(T).$$

Доказательство основано на использовании конструкции О. Б. Лупанова асимптотически наилучшего метода синтеза вентильных схем глубины 2 ([2]).

Разобьем матрицу $A(T)$ по строкам на $]p/r[$ полос, каждая из которых имеет q столбцов и не более, чем r строк (рис. 5). Обозначим высоту s-й полосы, $1 \leqslant s \leqslant]p/r[$, через $\rho(s)$. Очевидно, что

$$\rho(s) = \begin{cases} r & \text{при } 1 \leqslant s <]p/r[, \\ r' = p - r(\,]p/r[- 1) & \text{при } s =]p/r[. \end{cases} \tag{17}$$

Множество столбцов каждой полосы разобьем на группы одинаковых (см. рис. 5); для каждой полосы получится не более 2^r групп.

Сопоставим каждому ненулевому столбцу полосы вентиль, выходящей из входного полюса, имеющего номер, равный номеру этого столбца.

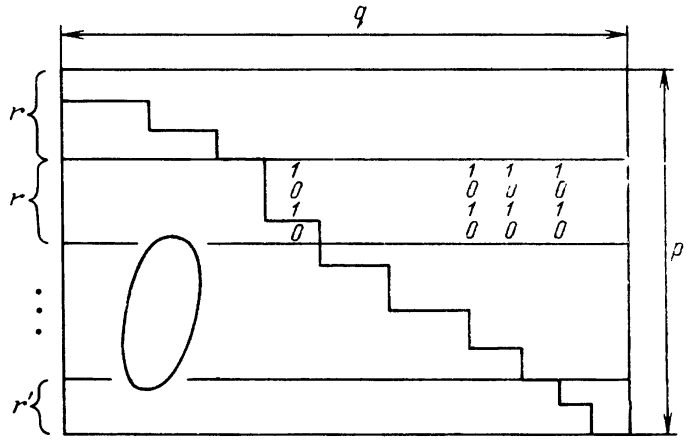


Рис. 5

Выходы всех вентилей, сопоставленных столбцам одной группы, объединим в один узел. Каждый узел соединим пучком из не более чем r вентилей с выходными полюсами, имеющими номера, равные номерам строк, в которых расположены единицы соответствующих столбцов. Полученная 0-1-вентильная схема глубины 2 реализует матрицу $A(T)$ и вследствие (7), (17), (8) содержит вентилей не более чем

$$\sum_{s=1}^{]p/r[} (q_{(s-1)r+1} + r \cdot 2^r) = \frac{1}{r} \sum_{s=1}^{]p/r]} r \cdot q_{(s-1)r+1} + \left]\frac{p}{r}\right[r2^r \leqslant$$

$$\leqslant \frac{1}{r} \sum_{s=1}^{]p/r[} \left(\sum_{i=1}^{\rho(s)} q_{(s-1)r+i} + r\,(q_{(s-1)r+1} - q_{(s-1)r+\rho(s))}) \right) + \left]\frac{p}{r}\right[r \cdot 2^r \leqslant$$

$$\leqslant \frac{1}{r} \sum_{i=1}^{p} q_i + q + (p + r)\,2^r = \frac{H}{r} + q + (p + r)\,2^r.$$

Используя (15), получаем соотношение $H \leqslant pq \leqslant q^2$ и, следовательно,

$$\left[\frac{1}{6}\overline{\log q}\right] + 1 \geqslant \frac{1}{12}\overline{\log H}. \tag{18}$$

Положим

$$r = \left[\frac{1}{6}\overline{\log q}\right] + 1. \tag{19}$$

Заметим, что найдется $c_1' > 0$ такое, что для любого $x \geqslant 1$ справедливо неравенство

$$\frac{1}{x^{1/12}} \leqslant c_1' \frac{1}{\overline{\log x}}. \tag{20}$$

Учитывая (19), (18), (15), (16) и (20), имеем:

$$L_{\text{вс}}(A(T)) \leqslant \frac{H}{\left[\frac{1}{6}\overline{\log q}\right]+1} + q + \left(p + \left[\frac{1}{6}\overline{\log q}\right] + 1\right)\cdot 2^{\left[\frac{1}{6}\overline{\log q}\right]+1} \leqslant$$

$$\leqslant \frac{H}{\frac{1}{12}\overline{\log H}} + q + 4pq^{1/6} + \frac{1}{3}\overline{\log q}\cdot q^{1/6} \leqslant 12\frac{H}{\overline{\log H}} + 2q + 4pq^{1/6} =$$

$$= 12\frac{H}{\overline{\log H}} + 2q + 4\frac{pq^{1/3}}{q^{1/6}} \leqslant 12\frac{H}{\overline{\log H}} + 2q + 4\frac{pq^{1/3}}{(pq)^{1/12}} \leqslant$$

$$\leqslant 12\frac{H}{\overline{\log H}} + 2q + 4c_1'\frac{H}{\overline{\log (pq)}} \leqslant (12 + 4c_1')\frac{H}{\overline{\log H}} + 2q.$$

Лемма доказана.

Лемма 3′. *Существуют положительные c_1 и c_2 такие, что для любой таблицы T, удовлетворяющей условиям*

$$p(T) \geqslant q(T), \tag{21}$$

$$H(T) \geqslant q(T)p^{1/3}(T), \tag{22}$$

справедливо неравенство

$$L_{\text{вс}}(A(T)) \leqslant c_1\frac{H(T)}{\overline{\log H(T)}} + c_2 p(T).$$

Доказательство следует из лемм 2 и 3.

Лемма 4. *Существуют положительные c_3 и c_4 такие, что для любой таблицы T справедливо неравенство*

$$L_{\text{вс}}(A(T)) \leqslant c_3\frac{H(T)}{\overline{\log H(T)}} + c_4\max(p(T), q(T)).$$

Доказательство. Рассмотрим произвольную таблицу T. В силу леммы 2 можно считать, что

$$q(T) \geqslant p(T). \tag{23}$$

Рассмотрим два случая: $H \geqslant p\cdot q^{1/3}$ и $H < p\cdot q^{1/3}$.

Случай 1°.

$$H(T) \geqslant p(T)q^{1/3}(T).$$

Так как $q \geqslant p$, выполняются условия (15) и (16) леммы 3. Применяя ее, получаем:

$$L_{\text{вс}}(A(T)) \leqslant c_1\frac{H}{\overline{\log H}} + c_2 q.$$

Случай 2°.

$$H(T) < p(T)q^{1/3}(T). \tag{24}$$

Обозначим

$$q' =]q^{2/3}[, \quad p' =]p/q^{1/3}[. \tag{25}$$

Рассмотрим матрицу $A(T)$. Элемент a_{ij}, где $i = p'$, $j = q - q' + 1$, не принадлежит таблице T, так как тогда в силу (25) и (24) была бы справедлива цепочка неравенств $H \geqslant q'p' \geqslant q^{2/3}\cdot\frac{p}{q^{1/3}} = p\cdot q^{1/3} > H$ — противоречие. Таким образом, все элементы таблицы T расположены в первых p' строках и последних q' столбцах матрицы $A(T)$.

В матрице $A(T)$ выделим две подматрицы — A_1 размера $p' \times (q - q')$ и A_2 размера $p \times q'$, как показано на рис. 6. Обозначим ту часть таблицы T, которая принадлежит матрице A_1, через T_1, а часть, принадлежащую A_2,— через T_2. Тогда T_1 и T_2 являются в свою очередь таблицами.

Реализуем 0-1-вентильными схемами отдельно матрицы A_1 и A_2, а затем отождествим первые p' выходов схемы, реализующей матрицу A_2 с выходами схемы, реализующей матрицу A_1.

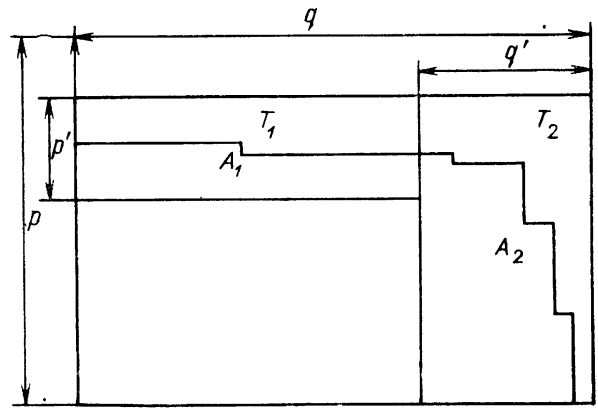


Рис. 6

а) Оценим сложность реализации матрицы A_1 размера $p' \times (q - q')$. Вместо матрицы A_1 рассмотрим матрицу $A_1' = A(T_1')$, где T_1' — таблица, полученная из таблицы, как показано на рис. 7. Очевидно, что

$$H(T_1') \leqslant H(T). \qquad (26)$$

По таблице T_1' построим таблицу $T_1'' \subseteq A_1'$, содержащую все элементы таблицы T_1' и обладающую свойством:

$$H(T_1'') = H(T). \qquad (27)$$

Из (26) и того, что $H(A_1') = p'q \geqslant p/q^{1/3} \cdot q \geqslant pq^{1/3} > H(T)$, следует, что такую таблицу T_1'' всегда можно построить.

Заметим, что в силу предположения (23) выполняется соотношение

$$\frac{p+q-1}{q^{1/3}} \geqslant \left]\frac{p}{q^{1/3}}\right[, \qquad (28)$$

которое очевидно при $q \geqslant 3$ (так как тогда $q - 1 \geqslant q^{1/3}$), а в случае $1 \leqslant p \leqslant q \leqslant 2$ оно проверяется непосредственно.

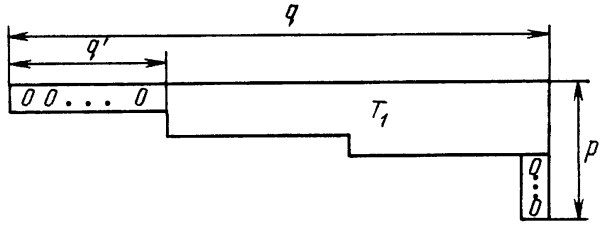


Рис. 7

Таблица T_1'' удовлетворяет условиям (15) и (16) леммы 3, так как в силу (27), (28) и (25) $q(T_1'') = q(T) \geqslant p(T) \geqslant p(T_1'')$ и

$$H(T_1'') = H(T) \geqslant p + q - 1 = \frac{p+q-1}{q^{1/3}} \geqslant \left]\frac{p}{q^{1/3}}\right[q^{1[3} =$$

$$= p' \cdot q^{1/3} = p(T_1'') q^{1/3}(T_1'').$$

Поэтому, используя лемму 3 и (27), получаем:

$$L_{\text{вс}}(A_1) = L_{\text{вс}}(A_1') = L_{\text{вс}}(A(T_1'')) \leqslant$$

$$\leqslant c_1 \frac{H(T_1'')}{\log H(T_1'')} + c_2 q(T_1'') = c_1 \frac{H(T)}{\log H(T)} + c_2 q(T). \qquad (29)$$

б) Оценим сложность реализации матрицы A_2 размера $p \times q'$. Так как $pq^{1/3} > H \geqslant q$, то $p > q^{2/3}$ и, следовательно,

$$p \geqslant]q^{2/3}[= q'. \tag{30}$$

По таблице T_2 построим таблицу $T_2' \subseteq A_2$, содержащую все элементы таблицы T_2 и обладающие свойством:

$$H(T_2') = H(T). \tag{31}$$

Это сделать можно, так как из (30) с учетом (23) следует, что

$$H(A_2) = p]q^{2/3}[\geqslant (]q^{2/3}[)^2 \geqslant q^{4/3} \geqslant p \cdot q^{1/3} > H(T).$$

Заметим, что в условиях случая 2° выполняется соотношение

$$\frac{p+q-1}{p^{1/3}} \geqslant \left]\frac{q}{p^{1/3}}\right[. \tag{32}$$

Оно очевидно при $p \geqslant 3$ (так как тогда $p - 1 \geqslant p^{1/3}$) и $p = 1$, а при $p = 2$ в силу (24) и (30) $q = 2$, и в этом случае соотношение (32) проверяется непосредственно.

Теперь, используя (31), (32), (23) и (25), получаем:

$$H(T_2') = H(T) \geqslant p + q - 1 =$$

$$= \frac{p+q-1}{p^{1/3}} p^{1/3} \geqslant \left]\frac{q}{p^{1/3}}\right[p^{1/3} \geqslant]q^{2/3}[p^{1/3} = q' \cdot p^{1/3}.$$

Поэтому

$$H(T_2') \geqslant q(T_2') p^{1/3}(T_2'). \tag{33}$$

Из (30) и (33) следует, что таблица T_2' удовлетворяет условиям (21) и (22) леммы 3′.

Используя эту лемму, (31) и (23), получаем:

$$L_{\text{вс}}(A_2) = L_{\text{вс}}(A(T_2')) \leqslant c_1 \frac{H(T_2')}{\overline{\log} H(T_2)} + c_2 p(T_2') \leqslant c_1 \frac{H(T)}{\overline{\log} H(T)} + c_2 q(T). \tag{34}$$

Для сложности реализации всей матрицы $A(T)$, используя оценки (29) и (34), в случае 2° получаем:

$$L_{\text{вс}}(A(T)) \leqslant L_{\text{вс}}(A_1) + L_{\text{вс}}(A_2) \leqslant 2c_1 \frac{H(T)}{\overline{\log} H(T)} + 2c_2 q(T).$$

Лемма доказана.

Лемма 5. *Существуют положительные c_5 и c_6 такие, что для любой таблицы T, удовлетворяющей для некоторых H_0 и a, $H_0 \in \mathbf{N}$, $0 < a \leqslant 1$, условию*

$$H(T) \leqslant \frac{H_0}{(\overline{\log} H_0)^a}, \tag{35}$$

справедливо неравенство

$$L_{\text{вс}}(A(T)) \leqslant c_5 \frac{H_0}{(\overline{\log} H_0)^{1+a}} + c_6 \max(p(T), q(T)).$$

Доказательство. Заметим, что функция $x/\overline{\log} x$ монотонно возрастает при $x > e$. Поэтому найдется $c_2' > 0$ такое, что для любой пары (x_1, x_2), $x_1 \in \mathbf{N}$, $x_2 \in \mathbf{N}$, если $x_1 \leqslant x_2$, то

$$x_1/\overline{\log} x_1 \leqslant c_2' x_2/\overline{\log} x_2. \tag{36}$$

Также заметим, что найдется $0<c_3'<1$ такое, что для любого $x\in\mathbf{N}$

$$x^{c_3'}\geqslant \overline{\log}\, x. \tag{37}$$

Применяя к таблице T, удовлетворяющей условию (35), лемму 4 и используя (36), (37) и неравенство $a\leqslant 1$, получаем *):

$$L_{\text{вс}}(A(T))\leqslant c_3\frac{H(T)}{\overline{\log}\, H(T)}+c_4\max(p(T),q(T))\leqslant$$

$$\leqslant c_3c_2'\frac{\left]\frac{H_0}{(\overline{\log}\, H_0)^a}\right[}{\overline{\log}\left(\left]\frac{H_0}{(\overline{\log}\, H_0)^a}\right[\right)}+c_4\max(p(T),q(T))\leqslant$$

$$\leqslant c_3c_2'\frac{H_0}{(\overline{\log}\, H_0)^a}\frac{1}{\overline{\log}\frac{H_0^{1-c_3'}H_0^{c_3'}}{\overline{\log}\, H_0}}+(c_4+c_3c_2')\max(p(T),q(T))\leqslant$$

$$\leqslant c_3c_2'\frac{1}{1-c_3'}\frac{H_0}{(\overline{\log}\, H_0)^{1+a}}+(c_4+c_3c_2')\max(p(T),q(T)).$$

Лемма доказана.

Лемма 6. *Пусть $f(x)$ непрерывна и выпукла вверх на $[x_0,\infty)$. Тогда для любого набора чисел $(x_1, x_2, \ldots, x_k)$, где $x_i\geqslant x_0$, $1\leqslant i\leqslant k$, выполняется неравенство*

$$\sum_{i=1}^{k}f(x_i)\leqslant kf\left(\frac{\sum_{i=1}^{k}x_i}{k}\right).$$

Утверждение леммы следует из неравенства Йенсена (подробнее см., например, [3, с. 90—93]).

Лемма 7. *Найдется $c_4'>4$ такое, что функции*

$$x/\overline{\log}\, x \quad \text{и} \quad x(\overline{\log}\,\overline{\log}\, x)^{1/2}/(\overline{\log}\, x)^{3/2}$$

выпуклы вверх на $[c_4',\infty)$.

Утверждение леммы легко проверяется вычислением вторых производных этих функций.

Лемма 8. *Существуют положительные c_7 и c_8 такие, что для любой двоичной матрицы A размера $p\times q$ справедливо неравенство*

$$L_{\text{вс}}(A)\leqslant\frac{H(A)}{\overline{\log}\, H(A)}+c_7\frac{H(A)(\overline{\log}\,\overline{\log}\, H(A))^{1/2}}{(\overline{\log}\, H(A))^{3/2}}+c_8p+c_8q.$$

Утверждение леммы непосредственно следует из основного результата статьи Н. Пиппенджера [6] (при $K=1$).

Лемма 9. *Существуют положительные c_9, c_{10} и c_{11} такие, что для любой таблицы T справедливо неравенство*

$$L_{\text{вс}}(A(T))\leqslant\left(1+\frac{1}{(\overline{\log}\, H(T))^{1/2}}\right)\frac{H(T)}{\overline{\log}\frac{H^2(T)}{2p(T)\,q(T)\,(\overline{\log}\, H(T))^{1/2}}}+$$

$$+c_9\frac{H(T)(\overline{\log}\,\overline{\log}\, H(T))^{1/2}}{\left(\overline{\log}\frac{H^2(T)}{2p(T)\,q(T)\,(\overline{\log}\, H(T))^{1/2}}\right)^{3/2}}+c_{10}q(T)+c_{11}\frac{p^2(T)\,q(T)\,(\overline{\log}\, H(T))^{1/2}}{H(T)}.$$

*) Для доказательства последнего неравенства в цепочке следует рассмотреть два случая: $H_0=1$ и $H_0\geqslant 2$.

Доказательство. Рассмотрим таблицу T и матрицу $A(T)$. По таблице T однозначно находятся индексы $1 = i_1 < i_2 < i_3 < \ldots < i_k < i_{k+1} = q + 1$, которые определяются из условий:

а) если $i \in [i_j, i_{j+1} - 1]$, то $p_i - p_{i_j} \leqslant \frac{H}{q(\overline{\log} H)^{1/2}}$,

б) $p_{i_{j+1}} - p_{i_j} > \frac{H}{q(\overline{\log} H)^{1/2}}$.

Тогда

$$p = p_q = p_q - p_{i_k} + \sum_{j=2}^{k} (p_{i_j} - p_{i_{j-1}}) + p_{i_1} \geqslant$$

$$\geqslant \sum_{j=2}^{k} (p_{i_j} - p_{i_{j-1}}) \geqslant \left]\frac{H}{q(\overline{\log} H)^{1/2}}\right[(k-1),$$

и поэтому

$$k \leqslant \frac{p}{\left]\frac{H}{q(\overline{\log} H)^{1/2}}\right[} + 1 \leqslant \frac{pq(\overline{\log} H)^{1/2}}{H} + 1 \leqslant \frac{2pq(\log H)^{1/2}}{H}. \quad (38)$$

Теперь рассмотрим таблицу $T' \subseteq A(T)$ такую, что

$$T' = \bigcup_{j=1}^{k} A_j, \quad (39)$$

где A_j — матрица размера $p(A_j) \times (i_{j+1} - i_j)$, полученная из первых $p(A_j) = \min\left(p, p_{i_j} + \left[H/q(\overline{\log} H)^{1/2}\right]\right)$ элементов столбцов матрицы $A(T)$ с номерами s, $i_j \leqslant s < i_{j+1}$ (см. рис. 8).

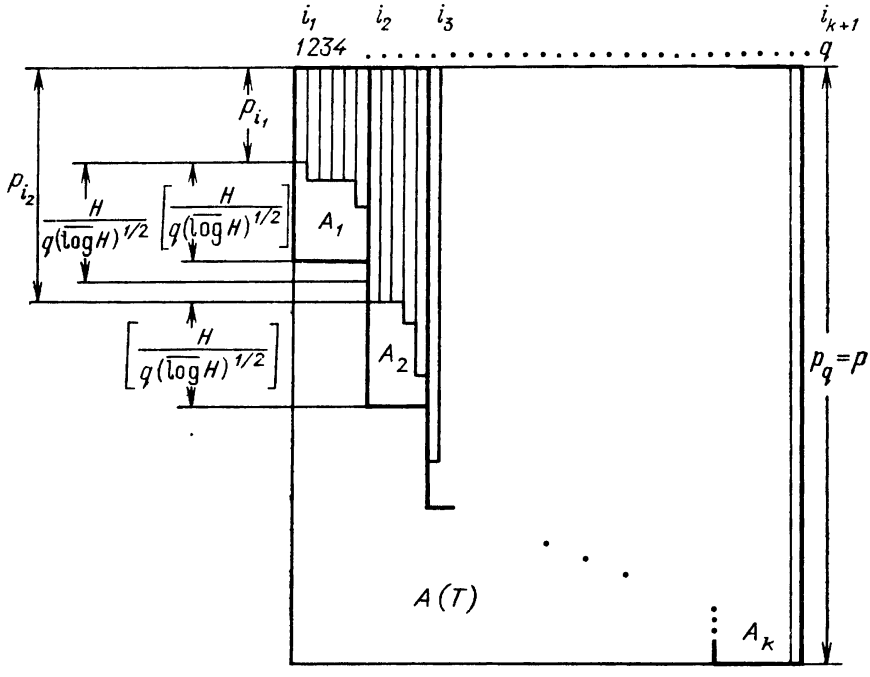


Рис. 8

Таблица T' обладает следующими свойствами:

$$p(T') = p(T), \quad q(T') = q(T); \quad (40)$$

$$A(T') = A(T); \quad (41)$$

$$H(T) \leqslant H(T') \leqslant H(T) + q\left[\frac{H(T)}{q(\overline{\log} H(T))^{1/2}}\right] \leqslant \left(1 + \frac{1}{(\overline{\log} H(T))^{1/2}}\right) H(T). \quad (42)$$

Пусть

$$\mathcal{K}_1 = \{1 \leqslant j \leqslant k \mid H(A_j) \geqslant c_4'\}, \quad \mathcal{K}_2 = \{1 \leqslant j \leqslant k \mid H(A_j) < c_4'\}. \tag{43}$$

Обозначим

$$k_1 = |\mathcal{K}_1|, \quad H_1 = \sum_{j \in \mathcal{K}_1} H(A_j); \tag{44}$$

$$k_2 = |\mathcal{K}_2|, \quad H_2 = \sum_{j \in \mathcal{K}_2} H(A_j). \tag{45}$$

Тогда

$$\frac{H_1}{k_1} - \frac{H(T')}{k} = \frac{H_1}{k_1} - \frac{H_1 + H_2}{k_1 + k_2} = \frac{H_1 k_1 + H_1 k_2 - H_1 k_1 - H_2 k_1}{k_1 (k_1 + k_2)} =$$

$$= \frac{H_1 k_2 - H_2 k_1}{k_1 (k_1 + k_2)} \geqslant \frac{c_4' k_1 k_2 - c_4' k_2 k_1}{k_1 (k_1 + k_2)} = 0,$$

т. е.

$$\frac{H(T')}{k} \leqslant \frac{H_1}{k_1}. \tag{46}$$

Перейдем к оценке сложности реализации матрицы $A(T)$. В силу (41), (39) и (43) имеем:

$$L_{\text{вс}}(A(T)) = L_{\text{вс}}(A(T')) \leqslant \sum_{j=1}^{k} L_{\text{вс}}(A_j) = \sum_{j \in \mathcal{K}_1} L_{\text{вс}}(A_j) + \sum_{j \in \mathcal{K}_2} L_{\text{вс}}(A_j). \tag{47}$$

Если $k_1 \neq 0$, то для оценки сложности реализации матриц A_j, $j \in \mathcal{K}_1$, применяем лемму 8:

$$L_{\text{вс}}(A_j) \leqslant \frac{H(A_j)}{\overline{\log} H(A_j)} + c_7 \frac{H(A_j)(\overline{\log}\,\overline{\log} H(A_j))^{1/2}}{(\overline{\log} H(A_j))^{3/2}} + c_8 (i_{j+1} - i_j) + c_8 p.$$

Поэтому

$$\sum_{j \in \mathcal{K}_1} L_{\text{вс}}(A_j) \leqslant \sum_{j \in \mathcal{K}_1} \frac{H(A_j)}{\overline{\log} H(A_j)} + c_7 \sum_{j \in \mathcal{K}_1} \frac{H(A_j)(\overline{\log}\,\overline{\log} H(A_j))^{1/2}}{(\overline{\log} H(A_j))^{3/2}} + c_8 q + c_8 p k. \tag{48}$$

Из (43), (44), лемм 6 и 7, (39) и (46) следует, что

$$\sum_{j \in \mathcal{K}_1} \frac{H(A_j)}{\overline{\log} H(A_j)} \leqslant k_1 \frac{\frac{H_1}{k_1}}{\overline{\log} \frac{H_1}{k_1}} \leqslant \frac{H(T')}{\overline{\log} \frac{H_1}{k_1}} \leqslant \frac{H(T')}{\overline{\log} \frac{H(T')}{k}}; \tag{49}$$

$$\sum_{j \in \mathcal{K}_1} \frac{H(A_j)(\overline{\log}\,\overline{\log} H(A_j))^{1/2}}{(\overline{\log} H(A_j))^{3/2}} \leqslant k_1 \frac{\frac{H_1}{k_1}\left(\overline{\log}\,\overline{\log} \frac{H_1}{k_1}\right)^{1/2}}{\left(\overline{\log} \frac{H_1}{k_1}\right)^{3/2}} \leqslant$$

$$\leqslant \frac{H(T')(\overline{\log}\,\overline{\log} H(T'))^{1/2}}{\left(\overline{\log} \frac{H_1}{k_1}\right)^{3/2}} \leqslant \frac{H(T')(\overline{\log}\,\overline{\log} H(T'))^{1/2}}{\left(\overline{\log} \frac{H(T')}{k}\right)^{3/2}}. \tag{50}$$

Для сложности реализации первой группы матриц $(A_j,\ j \in \mathcal{K}_1)$ окончательно, используя (48), (49) и (50), имеем следующую оценку:

$$\sum_{j \in \mathcal{K}_1} L_{\text{вс}}(A_j) \leqslant \frac{H(T')}{\overline{\log} \frac{H(T')}{k}} + c_7 \frac{H(T')(\overline{\log}\,\overline{\log} H(T'))^{1/2}}{\left(\overline{\log} \frac{H(T')}{k}\right)^{3/2}} + c_8 q + c_8 p k. \tag{51}$$

Заметим, что эта оценка остается справедливой и при $k_1 = 0$.

Матрицы A_j, $j \in \mathcal{K}_2$, будем реализовывать тривиальным способом — вентильными схемами глубины 1.

Из (43) и (45) следует:

$$\sum_{j \in \mathcal{K}_2} L_{\text{вс}}(A_j) \leqslant \sum_{j \in \mathcal{K}_2} H(A_j) \leqslant c_4' k_2 \leqslant c_4' k. \tag{52}$$

Теперь, подставляя (51) и (52) в (47) и используя (42) и (38), получаем:

$$L_{\text{вс}}(A(T)) \leqslant \frac{H(T')}{\overline{\log} \frac{H(T')}{k}} + c_7 \frac{H(T') (\overline{\log}\, \overline{\log} H(T'))^{1/2}}{\left(\overline{\log} \frac{H(T')}{k}\right)^{3/2}} + c_8 q + c_8 pk + c_4' k \leqslant$$

$$\leqslant \left(1 + \frac{1}{(\overline{\log} H(T))^{1/2}}\right) \frac{H(T)}{\overline{\log} \frac{H^2(T)}{2pq (\overline{\log} H(T))^{1/2}}} + 4c_7 \frac{H(T) (\overline{\log}\, \overline{\log} H(T))^{1/2}}{\left(\overline{\log} \frac{H^2(T)}{2pq (\overline{\log} H(T))^{1/2}}\right)^{3/2}} +$$

$$+ c_8 q + 2(c_8 + c_4') \frac{p^2 q (\overline{\log} H(T))^{1/2}}{H(T)}.$$

Лемма доказана.

Лемма 9′. *Существуют положительные* c_9, c_{10} *и* c_{11} *такие, что для любой таблицы* T *справедливо неравенство*

$$L_{\text{вс}}(A(T)) \leqslant \left(1 + \frac{1}{(\overline{\log} H(T))^{1/2}}\right) \frac{H(T)}{\overline{\log} \frac{H^2(T)}{2p(T) q(T) (\overline{\log} H(T))^{1/2}}} +$$

$$+ c_9 \frac{H(T) (\overline{\log}\, \overline{\log} H(T))^{1/2}}{\left(\overline{\log} \frac{H^2(T)}{2p(T) q(T) (\overline{\log} H(T))^{1/2}}\right)^{3/2}} + c_{10} p(T) + c_{11} \frac{q^2(T) p(T) (\overline{\log} H(T))^{1/2}}{H(T)}.$$

Доказательство следует из лемм 2 и 9.

Лемма 10. *Существуют положительные* c_{12} *и* c_{13} *такие, что для любой таблицы* T, *удовлетворяющей условию*

$$q(T) \geqslant p(T) \tag{53}$$

и хотя бы одному из двух следующих условий

$$\frac{H(T)}{\overline{\log}^4 H(T)} \geqslant q(T); \tag{54}$$

$$p(T) \leqslant \frac{q(T)}{\overline{\log}^2 H(T)}, \tag{55}$$

справедливо неравенство

$$L_{\text{вс}}(A(T)) \leqslant \frac{H(T)}{\overline{\log} \frac{H^{3/2}(T)}{2 (p(T) q(T))^{1/2} (\overline{\log} H(T))^2}} + c_{12} \frac{H(T) (\overline{\log}\, \overline{\log} H(T))^{1/2}}{(\overline{\log} H(T))^{3/2}} + c_{13} q(T).$$

Доказательство. Рассмотрим два случая соотношения параметров H, p и q произвольной таблицы T:

$$H \overline{\log} H \geqslant pq \quad \text{и} \quad H \overline{\log} H < pq.$$

Случай 1°.

$$H(T) \overline{\log} H(T) \geqslant p(T) q(T). \tag{56}$$

Применяя лемму 9 и используя (56), получаем:

$$L_{\text{вс}}(A(T)) \leqslant \left(1+\frac{1}{(\overline{\log} H)^{1/2}}\right)\frac{H}{\overline{\log}\frac{H^2}{2pq\,(\overline{\log} H)^{1/2}}} + c_9\frac{H\,(\overline{\log}\,\overline{\log} H)^{1/2}}{\left(\overline{\log}\frac{H^2}{2pq\,(\overline{\log} H)^{1/2}}\right)^{3/2}} +$$

$$+ c_{10}q + c_{11}\frac{p^2q\,(\overline{\log} H)^{1/2}}{H} \leqslant \left(1+\frac{1}{(\overline{\log} H)^{1/2}}\right)\frac{H}{\overline{\log}\frac{H}{2\,(\overline{\log} H)^{3/2}}} +$$

$$+ c_9\frac{H\,(\overline{\log}\,\overline{\log} H)^{1/2}}{\left(\overline{\log}\frac{H}{2\,(\overline{\log} H)^{3/2}}\right)^{3/2}} + c_{10}q + c_{11}p\,(\overline{\log} H)^{3/2}. \quad (57)$$

Заметим, что найдется $c_5'>0$ такое, что для любого $x\in\mathbf{N}$ выполняется неравенство $\overline{\log}^4 x \leqslant c_5' x$. Поэтому, учитывая (56) и (53), имеем:

$$p\,(\overline{\log} H)^{3/2} \leqslant \frac{H\,(\overline{\log} H)^{5/2}}{q} = \frac{H}{(\overline{\log} H)^{3/2}}\cdot\frac{(\overline{\log} H)^4}{q} \leqslant$$

$$\leqslant 2^4\frac{H}{(\overline{\log} H)^{3/2}}\frac{\overline{\log}^4 q}{q} \leqslant 2^4c_5'\frac{H}{(\overline{\log} H)^{3/2}}. \quad (58)$$

Кроме того, найдется $c_6'>0$ такое, что для любого $x\in\mathbf{N}$

$$c_6'\,\overline{\log}\frac{x}{2\,(\overline{\log} x)^{3/2}} \geqslant \overline{\log} x. \quad (59)$$

Из (57), учитывая (58) и (59), получаем:

$$L_{\text{вс}}(A(T)) \leqslant \frac{H}{\overline{\log}\frac{H}{2\,(\overline{\log} H)^{3/2}}} + \left(c_6' + (c_6')^{3/2}c_9 + 2^4c_5'c_{11}\right)\frac{H\,(\overline{\log}\,\overline{\log} H)^{1/2}}{(\overline{\log} H)^{3/2}} + c_{10}q \leqslant$$

$$\leqslant \frac{H}{\overline{\log}\frac{H^{3/2}}{2\,(pq)^{1/2}\,(\overline{\log} H)^{3/2}}} + \left(c_6' + (c_6')^{3/2}c_9 + 2^4c_5'c_{11}\right)\frac{H\,(\overline{\log}\,\overline{\log} H)^{1/2}}{(\overline{\log} H)^{3/2}} + c_{10}q. \quad (60)$$

Случай 2°.

$$H(T)\,\overline{\log} H(T) < p(T)\,q(T). \quad (61)$$

Обозначим

$$p' = \left[\left(H\,\overline{\log} H\,\frac{p}{q}\right)^{1/2}\right], \quad q' = \left[\left(\frac{H}{\overline{\log} H}\,\frac{q}{p}\right)^{1/2}\right]. \quad (62)$$

Из (61) и (62) имеем:

$$p' \leqslant p, \quad q' \leqslant q. \quad (63)$$

Заметим, что все элементы таблицы T расположены в первых p' строках и последних q' столбцах матрицы $A(T)$, так как иначе бы элемент a_{ij} матрицы $A(T)$, где $i=p'+1$, $j=q-q'$, принадлежал таблице T, и тогда, вследствие (62), выполнялась бы цепочка неравенств

$$H \geqslant (q'+1)(p'+1) > \left(\frac{Hq}{\overline{\log} Hp}\right)^{1/2}\left(\frac{H\,\overline{\log} Hp}{q}\right)^{1/2} = H \text{ — противоречие.}$$

Выделим в матрице $A(T)$ две подматрицы — A_1 размера $p'\times(q-q')$ и A_2 размера $p\times q'$, как показано на рис. 6. Обозначим через T_i, $i=1, 2$, часть таблицы T, принадлежащую матрице A_i. Эти части таблицы T, в свою очередь, являются таблицами. Очевидно, что

$$L_{\text{вс}}(A(T)) \leqslant L_{\text{вс}}(A_1) + L_{\text{вс}}(A_2). \quad (64)$$

Отдельно оценим сложность реализации матриц A_1 и A_2. Заметим, что

$$L_{\text{вс}}(A_i) = L_{\text{вс}}(A(T_i)), \quad i = 1, 2, \tag{65}$$

хотя равенство $A_1 = A(T_1)$ может не выполняться.

а) Если $H(T_i) < H(T)/(\overline{\log} H(T))^{1/2}$, $i = 1$ или 2, то в силу (65), леммы 5, (53) и (63), имеем:

$$L_{\text{вс}}(A_i) \leqslant c_5 \frac{H(T)}{(\overline{\log} H(T))^{3/2}} + c_6 q(T). \tag{66}$$

б) Пусть выполняется соотношение

$$H(T_1) \geqslant \frac{H(T)}{(\overline{\log} H(T))^{1/2}}. \tag{67}$$

Тогда из (62), (67), (53), (54) и (55) следует:

$$\frac{p^2(T_1)\, q(T_1) (\overline{\log} H(T_1))^{1/2}}{H(T_1)} \leqslant \frac{(p')^2 q (\overline{\log} H(T))^{1/2}}{H(T_1)} \leqslant \frac{H(T)\, p \overline{\log} H(T)\, q \overline{\log} H(T)}{qH(T)} \leqslant$$

$$\leqslant p \overline{\log}^2 H(T) \leqslant \begin{cases} q \overline{\log}^2 H(T) \leqslant \dfrac{H(T)}{\overline{\log}^2 H(T)}, & \text{если (54)}, \\ q, & \text{если (55)}. \end{cases} \tag{68}$$

Применяем к таблице T_1 лемму 9, учитывая (65), (62), (68) и (67):

$$L_{\text{вс}}(A_1) = L_{\text{вс}}(A(T_1)) \leqslant$$

$$\leqslant \left(1 + \frac{1}{(\overline{\log} H(T_1))^{1/2}}\right) \frac{H(T_1)}{\overline{\log} \dfrac{H^2(T_1)}{2(H(T)\, pq \overline{\log} H(T))^{1/2} (\overline{\log} H(T_1))^{1/2}}} +$$

$$+ c_9 \frac{H(T_1) (\overline{\log} \overline{\log} H(T_1))^{1/2}}{\left(\overline{\log} \dfrac{H^2(T_1)}{2(H(T)\, pq \overline{\log} H(T))^{1/2} (\overline{\log} H(T_1))^{1/2}}\right)^{3/2}} + c_{10} q + c_{11} \frac{H(T)}{\overline{\log}^2 H(T)} +$$

$$+ c_{11} q \leqslant \left(1 + \frac{\sqrt{2}}{(\overline{\log} H(T))^{1/2}}\right) \frac{H(T_1)}{\overline{\log} \dfrac{H^{3/2}(T)}{2(pq)^{1/2} (\overline{\log} H(T))^2}} +$$

$$+ c_9 \frac{H(T) (\overline{\log} \overline{\log} H(T))^{1/2}}{\left(\overline{\log} \dfrac{H^{3/2}(T)}{2(pq)^{1/2} (\overline{\log} H(T))^2}\right)^{3/2}} + c_{11} \frac{H(T)}{(\overline{\log} H(T))^2} + (c_{10} + c_{11}) q. \tag{69}$$

Заметим, что найдется $c_7' > 0$ такое, что для любого $x \in \mathbf{N}$ выполняется неравенство

$$c_7' \overline{\log} \frac{x^{1/2}}{2 \overline{\log}^2 x} \geqslant \overline{\log} x. \tag{70}$$

С учетом (70) и того, что $H^2(T) \geqslant pq$, из (69) следует:

$$L_{\text{вс}}(A_1) \leqslant \frac{H(T_1)}{\overline{\log} \dfrac{H^{3/2}(T)}{2(pq)^{1/2} (\overline{\log} H(T))^2}} +$$

$$+ \left(\sqrt{2} c_7' + c_9 (c_7')^{3/2} + c_{11}\right) \frac{H(T) (\overline{\log} \overline{\log} H(T))^{1/2}}{(\overline{\log} H(T))^{3/2}} + (c_{10} + c_{11}) q. \tag{71}$$

в) Пусть выполняется соотношение

$$H(T_2) \geqslant \frac{H(T)}{(\overline{\log} H(T))^{1/2}}. \tag{72}$$

Тогда из (72) и (62) имеем:

$$\frac{q^2(T_2)\,p(T_2)(\overline{\log}\,H(T_2))^{1/2}}{H(T_2)} \leqslant \frac{(q')^2\,p(\overline{\log}\,H(T))^{1/2}}{H(T_2)} \leqslant \frac{H(T)\,qp\,\overline{\log}\,H(T)}{p\,\overline{\log}\,H(T)\,H(T)} = q. \quad (73)$$

Применяем к таблице T_2 лемму 9′, учитывая (65), (62), (73), (72), (70) и (53):

$$L_{\text{вс}}(A_2) = L_{\text{вс}}(A(T_2)) \leqslant \left(1 + \frac{1}{(\overline{\log}\,H(T_2))^{1/2}}\right) \times$$

$$\times \frac{H(T_2)}{\overline{\log}\dfrac{H^2(T_2)}{2\left(\dfrac{H(T)\,pq}{\overline{\log}\,H(T)}\right)^{1/2}(\overline{\log}\,H(T_2))^{1/2}}} + c_9 \frac{H(T_2)(\overline{\log}\,\overline{\log}\,H(T_2))^{1/2}}{\left(\overline{\log}\dfrac{H^2(T_2)}{2\left(\dfrac{H(T)\,pq}{\overline{\log}\,H(T)}\right)^{1/2}(\overline{\log}\,H(T_2))^{1/2}}\right)^{3/2}} +$$

$$+ c_{10}p + c_{11}q \leqslant \left(1 + \frac{\sqrt{2}}{(\overline{\log}\,H(T))^{1/2}}\right) \frac{H(T_2)}{\overline{\log}\dfrac{H^{3/2}(T)}{2(pq)^{1/2}(\overline{\log}\,H(T))^2}} +$$

$$+ c_9 \frac{H(T)(\overline{\log}\,\overline{\log}\,H(T))^{1/2}}{\left(\overline{\log}\dfrac{H^{3/2}}{2(pq)^{1/2}(\overline{\log}\,H(T))^2}\right)^{3/2}} + c_{10}p + c_{11}q \leqslant \frac{H(T_2)}{\overline{\log}\dfrac{H^{3/2}(T)}{2(pq)^{1/2}(\overline{\log}\,H(T))^2}} +$$

$$+ \left(\sqrt{2}\,c_7' + c_9(c_7')^{3/2}\right) \frac{H(T)(\overline{\log}\,\overline{\log}\,H(T))^{1/2}}{(\overline{\log}\,H(T))^{3/2}} + (c_{10} + c_{11})q. \quad (74)$$

Окончательно, в случае 2°, складывая оценки из б), в) и две из а), получаем, используя (64), (66), (71), (74) и равенство $H(T_1) + H(T_2) = H(T)$, такую оценку для $L_{\text{вс}}(A(T))$:

$$L_{\text{вс}}(A(T)) \leqslant \frac{H(T)}{\overline{\log}\dfrac{H^{3/2}(T)}{2(pq)^{1/2}(\overline{\log}\,H(T))^2}} + \left(2c_5 + 2\sqrt{2}\,c_7' + 2c_9(c_7')^{3/2} + c_{11}\right) \times$$

$$\times \frac{H(T)(\overline{\log}\,\overline{\log}\,H(T))^{1/2}}{(\overline{\log}\,H(T))^{3/2}} + (2c_6 + 2c_{10} + 2c_{11})q. \quad (75)$$

Положим

$$c_{12} = \max\left(c_6' + (c_6')^{3/2}c_9 + 2^4 c_5' c_{11},\ 2c_5 + 2\sqrt{2}\,c_7' + 2c_9(c_7')^{3/2} + c_{11}\right),$$

$$c_{13} = 2c_6 + 2c_{10} + 2c_{11}.$$

Тогда из (60) и (75) следует утверждение леммы в обоих случаях. Лемма доказана.

Лемма 10′. *Существуют положительные c_{12} и c_{13} такие, что для любой таблицы T, удовлетворяющей условию*

$$q(T) \leqslant p(T) \quad (76)$$

и хотя бы одному из двух следующих условий

$$\frac{H(T)}{\overline{\log}^4 H(T)} \geqslant p(T); \quad (77)$$

$$q(T) \leqslant \frac{p(T)}{\overline{\log}^2 H(T)}, \quad (78)$$

справедливо неравенство

$$L_{\text{вс}}(A(T)) \leqslant \frac{H(T)}{\overline{\log}\dfrac{H^{3/2}(T)}{2(p(T)\,q(T))^{1/2}(\overline{\log}\,H(T))^2}} + c_{12}\frac{H(T)(\overline{\log}\,\overline{\log}\,H(T))^{1/2}}{(\overline{\log}\,H(T))^{3/2}} +$$

$$+ c_{13}p(T).$$

Доказательство следует из лемм 2 и 10.

Лемма 11. *Существуют положительные* c_{14} *и* c_{15} *такие, что для любой таблицы* T *справедливо неравенство*

$$L_{\text{вс}}(A(T)) \leqslant \frac{H(T)}{\overline{\log}\dfrac{H^{3/2}(T)}{2(p(T)\,q(T))^{1/2}(\overline{\log} H(T))^3}} + c_{14}\frac{H(T)(\overline{\log}\,\overline{\log} H(T))^{1/2}}{(\overline{\log} H(T))^{3/2}} + c_{15}\max(p(T), q(T)).$$

Доказательство. Пусть T — некоторая таблица. Без ограничения общности (в силу леммы 2) можно считать, что

$$q(T) \geqslant p(T). \tag{79}$$

Рассмотрим различные случаи соотношения параметров H, p и q таблицы T.

1°. $\dfrac{H}{\overline{\log}^4 H} \leqslant q$ и $p \geqslant \dfrac{q}{\overline{\log}^2 H}$:

1.1°. $\overline{\log}^6 H \leqslant p^{1/2}$;

1.2°. $\overline{\log}^6 H > p^{1/2}$.

2°. $\dfrac{H}{\overline{\log}^4 H} > q$ или $p < \dfrac{q}{\overline{\log}^2 H}$.

Переходим к изучению каждого случая.

Случай 1°.

$$\frac{H(T)}{(\overline{\log} H(T))^4} \leqslant q(T), \tag{80}$$

$$p(T) \geqslant \frac{q(T)}{(\overline{\log} H(T))^2}. \tag{81}$$

Подслучай 1.1°.

$$(\overline{\log} H(T))^6 \leqslant p^{1/2}(T). \tag{82}$$

Обозначим

$$p' = \left[\left(H\frac{p}{q}\right)^{1/2}\right], \quad q' = \left[\left(H\frac{q}{p}\right)^{1/2}\right]. \tag{83}$$

Из (83) и неравенства $H \leqslant pq$ следует, что

$$p' \leqslant p, \quad q' \leqslant q. \tag{84}$$

Заметим, что все элементы таблицы T расположены в первых p' строках и последних q' столбцах матрицы $A(T)$, так как иначе бы элемент a_{ij} матрицы $A(T)$, где $i = p' + 1$, $j = q - q'$ принадлежал таблице T, и тогда вследствие (83), выполнялась бы цепочка неравенств

$$H \geqslant (q'+1)(p'+1) > (Hq/p)^{1/2}(Hp/q)^{1/2} = H \text{ — противоречие.}$$

Выделим в матрице $A(T)$ две подматрицы — A_1 размера $p' \times (q - q')$ и A_2 размера $p \times q'$, как показано на рис. 6. Обозначим через T_i, $i = 1, 2$, часть таблицы T, принадлежащую матрице A_i. Эти части таблицы в свою очередь тоже являются таблицами.

Вместо таблицы T_1 будем рассматривать таблицу T_1', полученную из таблицы T_1, как показано на рис. 7.

Будем считать, что $T_2' = T_2$.

Тогда имеем следующую оценку:

$$L_{\text{вс}}(A(T)) \leqslant L_{\text{вс}}(A_1) + L_{\text{вс}}(A_2) = L_{\text{вс}}(A(T_1')) + L_{\text{вс}}(A(T_2')). \tag{85}$$

Заметим, что в силу (84)

$$H(T_1') + H(T_2') \leqslant H(T) + p' + q' \leqslant H(T) + p + q. \tag{86}$$

Отдельно оценим $\overline{L_{\text{вс}}}(\overline{A}(T_1'))$ и $L_{\text{вс}}(A(T_2'))$.

а) Если $H(T_i) < H(T)/(\overline{\log} H(T))^{1/2}$, $i = 1$ или 2, то в силу леммы 5, (84) и (79), получаем:

$$L_{\text{вс}}(A(T_i')) \leqslant c_5 \frac{H(T)}{(\overline{\log} H(T))^{3/2}} + c_6 q(T). \tag{87}$$

б) Пусть выполняется соотношение

$$H(T_1') \geqslant \frac{H(T)}{(\overline{\log} H(T))^{1/2}}. \tag{88}$$

Тогда в силу (83), (80), (79) и (82) получаем:

$$p(T_1') = p' \leqslant \left(H(T)\frac{p}{q}\right)^{1/2} \leqslant (p(\overline{\log} H(T))^4)^{1/2} =$$

$$= \frac{p}{(\overline{\log} H(T))^2} \cdot \frac{(\overline{\log} H(T))^4}{p^{1/2}} \leqslant \frac{q}{(\overline{\log} H(T))^2} \leqslant \frac{q(T_1')}{(\overline{\log} H(T_1'))^2}. \tag{89}$$

Из (79) и (89) следует, что для таблицы T_1' выполняются условия (53) и (55) леммы 10. Применяя ее, получаем (используя (83) и (88)):

$$L_{\text{вс}}(A(T_1')) \leqslant \frac{H(T_1')}{\log \frac{H^{3/2}(T_1')}{2(p(T_1')q(T_1'))^{1/2}(\overline{\log} H(T_1'))^2}} + c_{12}\frac{H(T_1')(\overline{\log}\,\overline{\log} H(T_1'))^{1/2}}{(\overline{\log} H(T_1'))^{3/2}} +$$

$$+ c_{13} q(T_1') \leqslant \frac{H(T_1')}{\log \frac{H^{3/2}(T)}{2(H(T)pq)^{1/4}(\overline{\log} H(T))^3}} + c_{12}(\sqrt{2})^3 \frac{H(T)(\overline{\log}\,\overline{\log} H(T))^{1/2}}{(\overline{\log} H(T))^{3/2}} +$$

$$+ c_{13} q \leqslant \frac{H(T_1')}{\log \frac{H^{3/2}(T)}{2(pq)^{1/2}(\overline{\log} H(T))^3}} + 3c_{12}\frac{H(T)(\overline{\log}\,\overline{\log} H(T))^{1/2}}{(\overline{\log} H(T))^{3/2}} + c_{13} q. \tag{90}$$

в) Пусть выполняется соотношение

$$H(T_2') \geqslant \frac{H(T)}{(\overline{\log} H(T))^{1/2}}. \tag{91}$$

Тогда в силу (83), (81), (80), (79) и (82)

$$q(T_2') = q' \leqslant \left(H(T)\frac{q}{p}\right)^{1/2} \leqslant (H(T)(\overline{\log} H(T))^2)^{1/2} \leqslant (q(\overline{\log} H(T))^6)^{1/2} =$$

$$= \frac{q}{(\overline{\log} H(T))^2} \frac{(\overline{\log} H(T))^5}{q^{1/2}} \leqslant p \frac{(\overline{\log} H(T))^5}{p^{1/2}} \leqslant p = p(T_2'). \tag{92}$$

Если $H(T_2')/(\overline{\log} H(T_2'))^4 > p(T_2')$, то для таблицы $\overline{T}_2'$ выполняется условие (77) леммы 10′.

Если же $H(T_2')/(\overline{\log} H(T_2'))^4 \leqslant p(T_2')$, то в силу (91), (81) и (82), имеем:

$$q(T_2') = q' \leqslant \left(H(T)\frac{q}{p}\right)^{1/2} \leqslant \left(H(T_2')(\overline{\log} H(T))^{1/2}\frac{q}{p(T_2')}\right)^{1/2} \leqslant$$

$$\leqslant (q(\overline{\log} H(T))^{1/2}(\overline{\log} H(T_2'))^4)^{1/2} \leqslant (p(\overline{\log} H(T))^2(\overline{\log} H(T))^5)^{1/2} \leqslant$$

$$\leqslant \frac{p}{(\overline{\log} H(T))^2}\frac{(\overline{\log} H(T))^6}{p^{1/2}} \leqslant \frac{p(T_2')}{(\overline{\log} H(T_2'))^2},$$

т. е. для таблицы T_2' выполняется условие (78) леммы 10′.

Таким образом, для таблицы T_2', учитывая (92), выполняются оба условия (76) и ((77) или (78)) леммы 10′. Применяя ее и используя (83), (91) и (79), получаем:

$$L_{\text{вс}}(A(T_2')) \leqslant \frac{H(T_2')}{\overline{\log}\,\dfrac{H^{3/2}(T_2')}{2(p(T_2')q(T_2'))^{1/2}(\overline{\log}\,H(T_2'))^2}} +$$

$$+ c_{12}\frac{H(T_2')(\overline{\log}\,\overline{\log}\,H(T_2'))^{1/2}}{(\overline{\log}\,H(T_2'))^{3/2}} + c_{13}p(T_2') \leqslant$$

$$\leqslant \frac{H(T_2')}{\overline{\log}\,\dfrac{H^{3/2}(T)}{2(H(T)\,pq)^{1/4}(\overline{\log}\,H(T))^3}} + c_{12}(\sqrt{2})^3\frac{H(T)(\overline{\log}\,\overline{\log}\,H(T))^{1/2}}{(\overline{\log}\,H(T))^{3/2}} + c_{13}p \leqslant$$

$$\leqslant \frac{H(T_2')}{\overline{\log}\,\dfrac{H^{3/2}(T)}{2(pq)^{1/2}(\overline{\log}\,H(T))^3}} + 3c_{12}\frac{H(T)(\overline{\log}\,\overline{\log}\,H(T))^{1/2}}{(\overline{\log}\,H(T))^{3/2}} + c_{13}q. \quad (93)$$

Окончательную оценку для $L_{\text{вс}}(A(T))$ в случае 1.1° получаем из (85), (87), (90), (93) и (86), складывая оценки из б), в) и две из а):

$$L_{\text{вс}}(A(T)) \leqslant \frac{H(T)}{\overline{\log}\,\dfrac{H^{3/2}(T)}{2(pq)^{1/2}(\overline{\log}\,H(T))^3}} +$$

$$+ (2c_5 + 6c_{12})\frac{H(T)(\overline{\log}\,\overline{\log}\,H(T))^{1/2}}{(\overline{\log}\,H(T))^{3/2}} + (2c_6 + 2c_{13} + 2)q(T). \quad (94)$$

Подслучай 1.2°.

$$(\overline{\log}\,H(T))^6 > p^{1/2}(T). \quad (95)$$

Обозначим через c_8' наибольший корень уравнения $2^7\log^7 x = \sqrt{x}$. Тогда при $q > c_8'$, используя (79) и (81), имеем:

$$\log^6 H \leqslant \log^6(q^2) = 2^6\log^6 q \leqslant q^{1/2}/(2\log q) \leqslant (p\log^2 H)^{1/2}/\log H = p^{1/2},$$

что противоречит (95). Таким образом, при выполнении условия (95) справедливо неравенство $q \leqslant c_8'$ и, следовательно, в случае 1.2°, используя (79), получаем такую оценку:

$$L_{\text{вс}}(A(T)) \leqslant H(T) \leqslant q^2 \leqslant (c_8')^2. \quad (96)$$

Случай 2°.

$$\frac{H(T)}{(\overline{\log}\,H(T))^4} > q(T) \quad \text{или} \quad p(T) < \frac{q(T)}{(\overline{\log}\,H(T))^2}.$$

Это условие вместе с (79) влечет выполнение условий (53) и ((54) или (55)) леммы 10 для таблицы T. Применяя эту лемму, имеем:

$$L_{\text{вс}}(A(T)) \leqslant$$

$$\leqslant \frac{H(T)}{\overline{\log}\,\dfrac{H^{3/2}(T)}{2(pq)^{1/2}(\overline{\log}\,H(T))^2}} + c_{12}\frac{H(T)(\overline{\log}\,\overline{\log}\,H(T))^{1/2}}{(\overline{\log}\,H(T))^{3/2}} + c_{13}q \leqslant$$

$$\leqslant \frac{H(T)}{\overline{\log}\,\dfrac{H^{3/2}(T)}{2(pq)^{1/2}(\overline{\log}\,H(T))^3}} + c_{12}\frac{H(T)(\overline{\log}\,\overline{\log}\,H(T))^{1/2}}{(\overline{\log}\,H(T))^{3/2}} + c_{13}q. \quad (97)$$

Теперь положим

$$c_{14} = 2c_5 + 6c_{12}, \quad c_{15} = \max\left(2c_6 + 2c_{13} + 2, (c_8')^2\right).$$

Тогда из (94), (96) и (97) следует утверждение леммы во всех случаях. Лемма доказана.

Теорема 3. *Существуют положительные* c_{16} *и* c_{17} *такие, что для любой таблицы* T *справедливо неравенство*

$$L_{\text{вс}}(A(T)) \leqslant \frac{H(T)}{\overline{\log} H(T)}\left(1 + c_{16}\left(\frac{\overline{\log}\,\overline{\log} H(T)}{\overline{\log} H(T)}\right)^{1/2}\right) + c_{17}\max(p(T), q(T)).$$

Доказательство. Рассмотрим такую последовательность таблиц $\{T\}_n$: сначала выпишем все таблицы площади 1 (их 2), затем — все таблицы площади 2 (их 8), 3 (их 24) и т. д. Заметим, что $H(T) \to \infty$.

Для доказательства теоремы достаточно установить, что для членов этой последовательности верна следующая оценка:

$$L_{\text{вс}}(A(T)) \leqslant \frac{H(T)}{\overline{\log} H(T)} + O\left(\frac{H(T)(\overline{\log}\,\overline{\log} H(T))^{1/2}}{(\overline{\log} H(T))^{3/2}}\right) + O(\max(p(T), q(T))). \quad (98)$$

В силу леммы 2 можно ограничиться таблицами, удовлетворяющими неравенству

$$q(T) \geqslant p(T). \quad (99)$$

Рассмотрим два случая соотношения параметров H, p и q: $H 2^{(\overline{\log} H \overline{\log}\overline{\log} H)^{1/2}} > pq$ и $H 2^{(\overline{\log} H \overline{\log}\overline{\log} H)^{1/2}} \leqslant pq$.

Случай 1°.

$$H(T)\cdot 2^{(\overline{\log} H(T)\overline{\log}\overline{\log} H(T))^{1/2}} > p(T)q(T). \quad (100)$$

Применяя лемму 11, в силу (99) и (100) получаем:

$$L_{\text{вс}}(A(T)) \leqslant \frac{H}{\overline{\log}\dfrac{H^{3/2}}{2(pq)^{1/2}(\overline{\log} H)^3}} + c_{14}\frac{H(\overline{\log}\,\overline{\log} H)^{1/2}}{(\overline{\log} H)^{3/2}} + c_{15}q \leqslant$$

$$\leqslant \frac{H}{\overline{\log} H}\cdot\frac{\overline{\log} H}{\overline{\log}\dfrac{H}{2\left(2^{(\overline{\log} H \overline{\log}\overline{\log} H)^{1/2}}\right)^{1/2}(\overline{\log} H)^3}} +$$

$$+ c_{14}\frac{H(\overline{\log}\,\overline{\log} H)^{1/2}}{(\overline{\log} H)^{3/2}} + c_{15}q \leqslant \frac{H}{\overline{\log} H}\cdot\frac{1}{1 - O\left(\dfrac{(\overline{\log}\,\overline{\log} H\,\overline{\log} H)^{1/2}}{(\overline{\log} H)^{1/2}}\right)} +$$

$$+ O\left(\frac{H(\overline{\log}\,\overline{\log} H)^{1/2}}{(\overline{\log} H)^{3/2}}\right) + O(q) = \frac{H}{\overline{\log} H} + O\left(\frac{H(\overline{\log}\,\overline{\log} H)^{1/2}}{(\overline{\log} H)^{3/2}}\right) + O(q). \quad (101)$$

Случай 2°.

$$H(T)\cdot 2^{(\overline{\log} H(T)\overline{\log}\overline{\log} H(T))^{1/2}} \leqslant p(T)q(T). \quad (102)$$

Для оценки $L_{\text{вс}}(A(T))$ в этом случае рассмотрим специальные множества таблиц $\mathbf{T}_{\text{п}}$ («промежуточные» таблицы), $\mathbf{T}_{\text{м}}$ («малые» таблицы), $\mathbf{T}_{\text{б}}$ («большие» таблицы) и $\mathbf{T}_{\text{U}}$ (таблицы «из объединения»), которые будем определять поэтапно. Всего будет k шагов, где k — параметр, зависящий от площади таблицы T (его значение определим ниже).

Первый этап. Обозначим

$$p' = \left[\left(H(T)\frac{p(T)}{q(T)}\right)^{1/2}\right], \quad q' = \left[\left(H(T)\frac{q(T)}{p(T)}\right)^{1/2}\right]. \quad (103)$$

Тогда в силу неравенства $H \leqslant pq$ имеем $p' \leqslant p$ и $q' \leqslant q$, причем все элементы таблицы T расположены в первых p' строках и последних q'

столбцах матрицы $A(T)$, так как иначе бы элемент a_{ij} матрицы $A(T)$, где $i=p'+1$, $j=q-q'$, принадлежал таблице T и тогда, вследствие (103) выполнялась бы цепочка неравенств

$$H \geqslant (p'+1)(q'+1) > \left(H\frac{q}{p}\right)^{1/2}\left(H\frac{p}{q}\right)^{1/2} = H \text{ — противоречие.}$$

Матрицу $A(T)$ разобьем на две части — A_1 размера $p' \times (q-q')$ и A_2 размера $p \times q'$, как показано на рис. 9. Обозначим через $\widehat{T}_i$, $i=1, 2$,

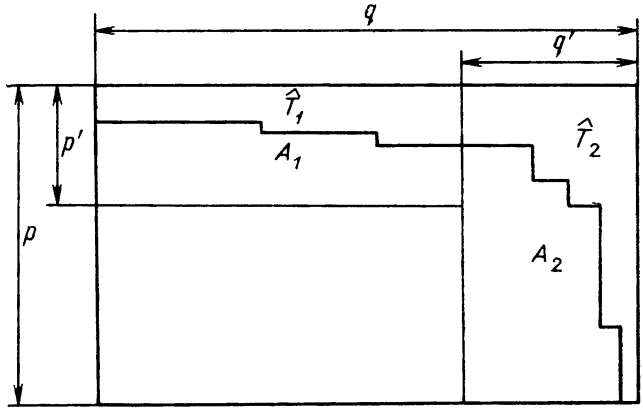


Рис. 9

часть таблицы, принадлежащую матрице A_i. Эти части таблицы T в свою очередь являются таблицами. По таблице $\widehat{T}_1$ построим таблицу T_1 как показано на рис. 10. Будем считать, что $T_2 = \widehat{T}_2$.

Таблицы T_1 и T_2 обладают следующими свойствами:

$$p(T_1) = \left[\left(H(T)\frac{p(T)}{q(T)}\right)^{1/2}\right], \quad q(T_1) = q(T); \tag{104}$$

$$p(T_2) = p(T), \quad q(T_2) = \left[\left(H(T)\frac{q(T)}{p(T)}\right)^{1/2}\right]; \tag{105}$$

$$L_{\text{вс}}(A(T)) \leqslant L_{\text{вс}}(A(T_1)) + L_{\text{вс}}(A(T_2)); \tag{106}$$

$$H(T_1) + H(T_2) \leqslant H(T) + p(T_1) + q(T_2). \tag{107}$$

Включаем таблицы T_1 и T_2 в $\mathbf{T}_\text{п}$. Если таблица T_{i_1} ($i_1 = 1, 2$) удовлетворяет неравенству $H(T_{i_1}) \leqslant \frac{H(T)}{\log H(T)}$, то включаем таблицу T_{i_1} еще и в $\mathbf{T}_\text{м}$.

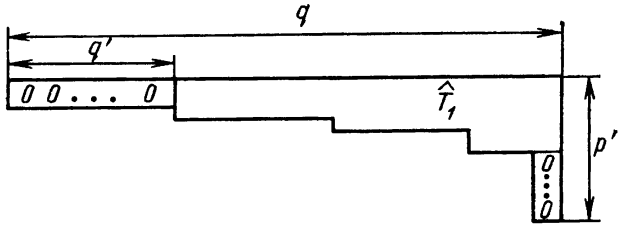


Рис. 10

s-й этап ($s=2, \ldots, k$). По каждой таблице $T_{i_1 \ldots i_{s-1}}$, полученной на предыдущем этапе и не включенной во множество $\mathbf{T}_\text{м}$ (т. е. удовлетворяющей неравенству $H(T_{i_1 \ldots i_{s-1}}) > \frac{H(T)}{\log H(T)}$), аналогично первому этапу строим таблицы $T_{i_1 \ldots i_{s-1} 1}$ и $T_{i_1 \ldots i_{s-1} 2}$, которые обладают следующими свойствами:

$$p(T_{i_1 \ldots i_{s-1} 1}) = \left[\left(H(T_{i_1 \ldots i_{s-1}})\frac{p(T_{i_1 \ldots i_{s-1}})}{q(T_{i_1 \ldots i_{s-1}})}\right)^{1/2}\right], \tag{108}$$

$$q(T_{i_1 \ldots i_{s-1} 1}) = q(T_{i_1 \ldots i_{s-1}});$$

$$p(T_{i_1\dots i_{s-1}2}) = p(T_{i_1\dots i_{s-1}}), \tag{109}$$

$$q(T_{i_1\dots i_{s-1}2}) = \left[\left(H(T_{i_1\dots i_{s-1}})\frac{q(T_{i_1\dots i_{s-1}})}{p(T_{i_1\dots i_{s-1}})}\right)^{1/2}\right];$$

$$L_{\text{вс}}(A(T_{i_1\dots i_{s-1}}) \leqslant L_{\text{вс}}(A(T_{i_1\dots i_{s-1}1})) + L_{\text{вс}}(A(T_{i_1\dots i_{s-1}2})); \tag{110}$$

$$H(T_{i_1\dots i_{s-1}1}) + H(T_{i_1\dots i_{s-1}2})) \leqslant$$

$$\leqslant H(T_{i_1\dots i_{s-1}}) + p(T_{i_1\dots i_{s-1}}) + q(T_{i_1\dots i_{s-1}}). \tag{111}$$

Включаем таблицы $T_{i_1\dots i_{s-1}1}$ и $T_{i_1\dots i_{s-1}2}$ в $\mathbf{T}_{\text{п}}$. Если $T_{i_1\dots i_{s-1}i_s}$ $(i_s = 1, 2)$ удовлетворяет неравенству $H(T_{i_1\dots i_s}) \leqslant H(T)/\sqrt{\log H(T)}$, то включаем таблицу $T_{i_1\dots i_s}$ еще и в $\mathbf{T}_{\text{м}}$.

Кроме того, если $s = k$, то все таблицы $T_{i_1\dots i_k}$, полученные на k-м этапе и не вошедшие во множество $\mathbf{T}_{\text{м}}$, включаем в $\mathbf{T}_{\text{б}}$. Обозначим

$$\mathbf{T}_{\cup} = \mathbf{T}_{\text{м}} \cup \mathbf{T}_{\text{б}}. \tag{112}$$

Построение множеств $\mathbf{T}_{\text{п}}$, $\mathbf{T}_{\text{м}}$, $\mathbf{T}_{\text{б}}$ и $\mathbf{T}_{\cup}$ закончено.

Укажем некоторые свойства этих множеств:

$$\mathbf{T}_{\cup} \subseteq \mathbf{T}_{\text{п}}. \tag{113}$$

$$|\mathbf{T}_{\cup}| \leqslant 2^k. \tag{114}$$

$$|\mathbf{T}_{\text{п}}| < 2^{k+1}. \tag{115}$$

Для любой таблицы $T_{\text{п}} \in \mathbf{T}_{\text{п}}$

$$H(T_{\text{п}}) \leqslant H(T) + 2kq(T) \leqslant (2k+1)H(T). \tag{116}$$

(Следует из построения множества $\mathbf{T}_{\text{п}}$, (107), (101) и неравенств $q(T_{\text{п}}) \leqslant q(T)$ и $p(T_{\text{п}}) \leqslant p(T) \leqslant q(T)$ для произвольной таблицы $T_{\text{п}} \in \mathbf{T}_{\text{п}}$.)

Для любой таблицы $T_{\text{б}} \in \mathbf{T}_{\text{б}}$

$$p(T_{\text{б}})q(T_{\text{б}}) \leqslant ((2k+1)H(T))^{1+1/2^k}. \tag{117}$$

Докажем это свойство. Заметим, что если таблица $T_{\text{б}}$ принадлежит множеству $\mathbf{T}_{\text{б}}$, то она имеет и обозначение такого вида: $T_{i_1\dots i_k}$. Поэтому, в силу (108), (109), (116), (104) и (105), получаем:

$$p(T_{\text{б}})q(T_{\text{б}}) = p(T_{i_1\dots i_k})q(T_{i_1\dots i_k}) =$$

$$= \left\{\begin{array}{ll} \left[\left(H(T_{i_1\dots i_{k-1}})\dfrac{p(T_{i_1\dots i_{k-1}})}{q(T_{i_1\dots i_{k-1}})}\right)^{1/2}\right] q(T_{i_1\dots i_{k-1}}), & i_k = 1 \\ p(T_{i_1\dots i_{k-1}})\cdot\left[\left(H(T_{i_1\dots i_{k-1}})\dfrac{q(T_{i_1\dots i_{k-1}})}{p(T_{i_1\dots i_{k-1}})}\right)^{1/2}\right], & i_k = 2 \end{array}\right\} \leqslant$$

$$\leqslant ((2k+1)H(T)\,p(T_{i_1\dots i_{k-1}})\,q(T_{i_1\dots i_{k-1}}))^{1/2} \leqslant \dots$$

$$\dots \leqslant ((2k+1)H(T))^{1/2+1/4+\dots+1/2^k}(p(T)\,q(T))^{1/2^k} \leqslant$$

$$\leqslant ((2k+1)H(T))^{1-1/2^k}(H(T))^{1/2^k-1} \leqslant ((2k+1)H(T))^{1+1/2^k}.$$

Свойство (117) доказано. Вернемся к оценке $(L_{\text{вс}}A(T))$. Из построения множеств $\mathbf{T}_{\text{м}}$ и $\mathbf{T}_{\text{б}}$, (106) и (110) следует:

$$L_{\text{вс}}(A(T)) \leqslant \sum_{T_{\text{м}} \in \mathbf{T}_{\text{м}}} L_{\text{вс}}(A(T_{\text{м}})) + \sum_{T_{\text{б}} \in \mathbf{T}_{\text{б}}} L_{\text{вс}}(A(T_{\text{б}})). \tag{118}$$

Для произвольной таблицы $T_{\text{м}} \in \mathbf{T}_{\text{м}}$ из построения множества $\mathbf{T}_{\text{м}}$ следует,

что $H(T_м) \leqslant H(T)/\overline{\log} H(T)$, и поэтому в силу леммы 5

$$L_{вс}(A(T_м)) \leqslant c_5 \frac{H(T)}{(\overline{\log} H(T))^2} + c_6 p(T_м) + c_6 q(T_м). \tag{119}$$

Для произвольной таблицы $T_б \in \mathbf{T}_б$ выполняется неравенство

$$H(T_б) > \frac{H(T)}{\overline{\log} H(T)}. \tag{120}$$

Применяя лемму 11 и используя (120), (117), (112), (113), (116) и (37), получаем:

$$L_{вс}(A(T_б)) \leqslant \frac{H(T_б)}{\overline{\log} \frac{H^{3/2}(T_б)}{2(p(T_б)q(T_б))^{1/2}(\overline{\log} H(T_б))^3}} + c_{14}\frac{H(T_б)(\overline{\log}\,\overline{\log} H(T_б))^{1/2}}{(\overline{\log} H(T_б))^{3/2}} +$$

$$+ c_{15}q(T_б) + c_{15}p(T_б) \leqslant \frac{H(T_б)}{\overline{\log} \frac{H^{3/2}(T)/(\overline{\log} H(T))^{3/2}}{2((2k+1)H(T))^{1/2+1/2^{k+1}}(\overline{\log}((2k+1)H(T)))^3}} +$$

$$+ c_{14}\frac{H(T_б)(\overline{\log}\,\overline{\log}((2k+1)H(T)))^{1/2}}{\left(\overline{\log}\frac{H(T)}{\overline{\log} H(T)}\right)^{3/2}} + c_{15}q(T_б) + c_{15}p(T_б) \leqslant$$

$$\leqslant \frac{H(T_б)}{\overline{\log} \frac{H(T)}{2(2k+1)(H(T))^{1/2^{k+1}}(\overline{\log}((2k+1)H(T)))^5}} +$$

$$+ \frac{c_{14}}{(1-c_3')^{3/2}}\frac{H(T_б)(\overline{\log}\,\overline{\log}((2k+1)H(T)))^{1/2}}{(\overline{\log} H(T))^{3/2}} + c_{15}q(T_б) + c_{15}p(T_б). \tag{121}$$

Положим

$$k = \left[\overline{\log}\left(\left(\frac{\overline{\log} H(T)}{\overline{\log}\,\overline{\log} H(T)}\right)^{1/2}\right)\right] - 1. \tag{122}$$

Заметим, что тогда найдется $c_9' > 0$ такое, что для любого значения $H(T)$ выполняется неравенство

$$\overline{\log}((2k+1)H(T)) \leqslant c_9' \overline{\log} H(T). \tag{123}$$

Из (118), (119) и (121), используя (123), (112), (114) и (122), получаем:

$$L_{вс}(A(T)) \leqslant \frac{\sum\limits_{T_б \in \mathbf{T}_б} H(T_б)}{\overline{\log} \frac{H(T)}{(c_9')^6(2k+1)(H(T))^{1/2^{k+1}}(\overline{\log} H(T))^5}} +$$

$$+ 3c_{14}\frac{1}{(1-c_3')^{3/2}}\left(\sum_{T_б \in \mathbf{T}_б} H(T_б)\right)\frac{(\overline{\log}\,\overline{\log} H(T))^{1/2}}{(\overline{\log} H(T))^{3/2}} + |\mathbf{T}_м| c_5 \frac{H(T)}{(\overline{\log} H(T))^2} +$$

$$+ c_6 \sum_{T_м \in \mathbf{T}_м} q(T_м) + c_6 \sum_{T_м \in \mathbf{T}_м} p(T_м) + c_{15} \sum_{T_б \in \mathbf{T}_б} q(T_б) + c_{15} \sum_{T_б \in \mathbf{T}_б} p(T_б) \leqslant$$

$$\leqslant \frac{H(T)}{\overline{\log} \frac{H(T)}{(c_9')^6(2k+1)(H(T))^{1/2^{k+1}}(\overline{\log} H(T))^5}} + \frac{3c_{14}}{(1-c_3')^{3/2}}\frac{H(T)(\overline{\log}\,\overline{\log} H(T))^{1/2}}{(\overline{\log} H(T))^{3/2}} +$$

$$+ c_5 2^k \frac{H(T)}{(\overline{\log} H(T))^2} + \left(1 + \frac{3c_{14}}{(1-c_3')^{3/2}}\right)\left(\sum_{T_\cup \in \mathbf{T}_\cup} H(T_\cup) - H(T)\right) +$$

$$+(c_6+c_{15})\sum_{T_U\in\mathbf{T}_U} q(T_0)+(c_6+c_{15})\sum_{T_U\in\mathbf{T}_U} p(T_U)=$$

$$=\frac{H(T)}{\overline{\log}\,H(T)}\,\frac{\overline{\log}\,H(T)}{\overline{\log}\,H(T)-O\left(\dfrac{\overline{\log}\,H(T)}{\left(\dfrac{\overline{\log}\,H(T)}{\overline{\log}\,\overline{\log}\,H(T)}\right)^{1/2}}\right)}+$$

$$+O\left(\frac{H(T)\,(\overline{\log}\,\overline{\log}\,H(T))^{1/2}}{(\overline{\log}\,H(T))^{3/2}}\right)+O\left(\frac{H(T)}{(\overline{\log}\,H(T))^{3/2}\,(\overline{\log}\,\overline{\log}\,H(T))^{1/2}}\right)+$$

$$+O\left(\sum_{T_U\in\mathbf{T}_U} H(T_U)-H(T)\right)+O\left(\sum_{T_U\in\mathbf{T}_U} q(T_U)\right)+O\left(\sum_{T_U\in\mathbf{T}_U} p(T_U)\right)=$$

$$=\frac{H(T)}{\overline{\log}\,H(T)}\,\frac{1}{1-O\left(\left(\dfrac{\overline{\log}\,\overline{\log}\,H(T)}{\overline{\log}\,H(T)}\right)^{1/2}\right)}+O\left(\frac{H(T)\,(\overline{\log}\,\overline{\log}\,H(T))^{1/2}}{(\overline{\log}\,H(T))^{3/2}}\right)+$$

$$+O\left(\sum_{T_U\in\mathbf{T}_U} H(T_U)-H(T)\right)+O\left(\sum_{T_U\in\mathbf{T}_U} q(T_U)\right)+O\left(\sum_{T_U\in\mathbf{T}_U} p(T_U)\right)=$$

$$=\frac{H(T)}{\overline{\log}\,H(T)}+O\left(\frac{H(T)\,(\overline{\log}\,\overline{\log}\,H(T))^{1/2}}{(\overline{\log}\,H(T))^{3/2}}\right)+O\left(\sum_{T_U\in\mathbf{T}_U} H(T_U)-H(T)\right)+$$

$$+O\left(\sum_{T_U\in\mathbf{T}_U} q(T_U)\right)+O\left(\sum_{T_U\in\mathbf{T}_U} p(T_U)\right). \quad (124)$$

Осталось оценить величины $\sum\limits_{T_U\in\mathbf{T}_U} q(T_U)$, $\sum\limits_{T_U\in\mathbf{T}_U} p(T_U)$ и $\sum\limits_{T_U\in\mathbf{T}_U} H(T_U)-H(T)$.

Заметим, что из построения множества $\mathbf{T}_U$ следует, что для любой таблицы $T_{i_1\ldots i_r}$ из $\mathbf{T}_U$, у которой не все индексы $i_1, \ldots, i_r$ равны 1, выполняется неравенство $q(T_{i_1\ldots i_r})\leqslant q\left(T_{\underbrace{1\ldots12}_{\mu}}\right)$, где μ — номер первой по счету двойки среди индексов $i_1, \ldots, i_r\left(T_{\underbrace{1\ldots12}_{\mu}}\in\mathbf{T}_\Pi\right)$.

Аналогично для любой таблицы $T_{i_1\ldots i_r}\in\mathbf{T}_U$, у которой не все индексы $i_1, \ldots, i_r$ равны 2, выполняется неравенство $p(T_{i_1\ldots i_r})\leqslant p\left(T_{\underbrace{2\ldots21}_{\nu}}\right)$, где ν — номер первой по счету единицы среди индексов $i_1, \ldots, i_r\left(T_{\underbrace{2\ldots21}_{\nu}}\in\mathbf{T}_\Pi\right)$.

Поэтому в силу (104), (105), (108), (109) и (114) имеем:

$$\sum_{T_U\in\mathbf{T}_U} q(T_U)\leqslant q(T_{1\ldots1})+(|\,\mathbf{T}_U\,|-1)\max_{T_{1\ldots12}\in\mathbf{T}_\Pi}\{q(T_{1\ldots12})\}\leqslant$$

$$\leqslant q(T)+2^k\max_{T_{1\ldots12}\in\mathbf{T}_\Pi}\{q(T_{1\ldots12})\}; \quad (125)$$

$$\sum_{T_U\in\mathbf{T}_U} p(T_U)\leqslant p(T_{2\ldots2})+(|\,\mathbf{T}_U\,|-1)\max_{T_{2\ldots21}\in\mathbf{T}_\Pi}\{p(T_{2\ldots21})\}\leqslant$$

$$\leqslant p(T)+2^k\max_{T_{2\ldots21}\in\mathbf{T}_\Pi}\{p(T_{2\ldots21})\}. \quad (126)$$

Кроме того, из (107), (111) и (115) следует, что

$$\sum_{T_U\in\mathbf{T}_U} H(T_U)-H(T)\leqslant\sum_{\substack{T_{i_1\ldots i_r}\in\mathbf{T}_\Pi,\\ i_r=2}} q(T_{i_1\ldots i_r})+\sum_{\substack{T_{i_1\ldots i_r}\in\mathbf{T}_\Pi,\\ i_r=1}} p(T_{i_1\ldots i_r})\leqslant$$

$$\leqslant \frac{|\mathbf{T}_{\text{п}}|}{2} \max_{T_{1\ldots12}\in\mathbf{T}_{\text{п}}} \{q(T_{1\ldots12})\} + \frac{|\mathbf{T}_{\text{п}}|}{2} \max_{T_{2\ldots21}\in\mathbf{T}_{\text{п}}} \{p(T_{2\ldots21})\} \leqslant$$

$$\leqslant 2^k \max_{T_{1\ldots12}\in\mathbf{T}_{\text{п}}} \{q(T_{1\ldots12})\} + 2^k \max_{T_{2\ldots21}\in\mathbf{T}_{\text{п}}} \{p(T_{2\ldots21})\}. \quad (127)$$

Оценим величины $q(T_{1\ldots12})$, $T_{1\ldots12}\in\mathbf{T}_{\text{п}}$. Заметим, что если $T_{\underbrace{1\ldots12}_{s}}\in$ $\in\mathbf{T}_{\text{п}}$, то для таблиц T_1, T_{11}, $\ldots$, $T_{\underbrace{1\ldots1}_{s-1}}$ выполняется неравенство

$$H(T_{1\ldots1}) \geqslant \frac{H(T)}{\overline{\log} H(T)}. \quad (128)$$

В силу (104), (108), (128), (109) и (116) получаем:

$$q(T_1) = q(T), \quad p(T_1) = \left[\left(H(T)\frac{p(T)}{q(T)}\right)^{1/2}\right] \geqslant \frac{(H(T))^{1/2}(p(T))^{1/2}}{4^{1/2}(q(T))^{1/2}};$$

$$q(T_{11}) = q(T), \quad p(T_{11}) = \left[\left(H(T_1)\frac{p(T_1)}{q(T_1)}\right)^{1/2}\right] \geqslant$$

$$\geqslant \frac{(H(T_1))^{1/2}(p(T_1))^{1/2}}{4^{1/2}(\overline{\log} H(T_1))^{1/2}(q(T))^{1/2}} \geqslant \frac{(H(T))^{1/2+1/4}(p(T))^{1/4}}{4^{1/2+1/4}(\overline{\log} H(T))^{1/2}(q(T))^{1/2+1/4}}$$

. . . . . .

$$q\left(T_{\underbrace{1\ldots1}_{s-1}}\right) = q(T), \quad p\left(T_{\underbrace{1\ldots1}_{s-1}}\right) \geqslant$$

$$\geqslant \frac{(H(T))^{1/2+1/4+\ldots+1/2^{s-1}}(p(T))^{1/2^{s-1}}}{4^{1/2+1/4+\ldots+1/2^{s-1}}(\overline{\log} H(T))^{1/2+\ldots+1/2^{s-2}}(q(T))^{1/2+1/4+\ldots+1/2^{s-1}}} =$$

$$= \frac{(H(T))^{1-1/2^{s-1}}(p(T))^{1/2^{s-1}}}{4^{1-1/2^{s-1}}(\overline{\log} H(T))^{1-1/2^{s-2}}(q(T))^{1-1/2^{s-1}}};$$

$$q\left(T_{\underbrace{1\ldots12}_{s}}\right) = \left[\left[H\left(T_{\underbrace{1\ldots1}_{s-1}}\right)\frac{q\left(T_{\underbrace{1\ldots1}_{s-1}}\right)}{p\left(T_{\underbrace{1\ldots1}_{s-1}}\right)}\right]^{1/2}\right] \leqslant$$

$$\leqslant \frac{(2k+1)^{1/2}(H(T))^{1/2^s}(q(T))^{1-1/2^s}4^{1/2}(\overline{\log} H(T))^{1/2-1/2^{s-1}}}{(p(T))^{1/2^s}} \leqslant$$

$$\leqslant q(T)\left(\frac{H(T)}{p(T)q(T)}\right)^{1/2^s} 4^{1/2}(2k+1)^{1/2}(\overline{\log} H(T))^{1/2}. \quad (129)$$

Из (129), (102) и (122) следует, что

$$2^k \max_{T_{1\ldots12}\in\mathbf{T}_{\text{п}}} \{q(T_{1\ldots12})\} \leqslant$$

$$\leqslant 2^{k+1} q(T)\left(\frac{1}{2^{(\overline{\log} H(T)\,\overline{\log}\,\overline{\log} H(T))^{1/2}}}\right)^{1/2^k}(2k+1)^{1/2}(\overline{\log} H(T))^{1/2} =$$

$$= q(T)\,2^{k+1-\frac{1}{2^k}(\overline{\log} H(T)\,\overline{\log}\,\overline{\log} H(T))^{1/2}+\frac{1}{2}\overline{\log}(2k+1)+\frac{1}{2}\overline{\log}\,\overline{\log} H(T)} =$$

$$= q(T)\cdot O\left(2^{\frac{1}{2}\overline{\log}\,\overline{\log} H(T)-\frac{1}{2}\overline{\log}\,\overline{\log}\,\overline{\log} H(T)+\frac{1}{2}\overline{\log}\,\overline{\log} H(T)} \times\right.$$

$$\left.\times 2^{-(\overline{\log} H(T)\,\overline{\log}\,\overline{\log} H(T))^{1/2}\Big/\left(\frac{1}{2}\left(\frac{\overline{\log} H(T)}{\overline{\log}\,\overline{\log} H(T)}\right)^{1/2}\right)+\frac{1}{2}\log(3\overline{\log}\,\overline{\log} H(T))}\right) =$$

$$= q(T)\,O\left(2^{\overline{\log}\,\overline{\log}\,H(T)+\overline{\log}\,\overline{\log}\,\overline{\log}\,H(T)-2\,\overline{\log}\,\overline{\log}\,H(T)}\right) =$$

$$= q(T)\,O\left(2^{-\frac{1}{2}\overline{\log}\,\overline{\log}\,H(T)}\right) = q(T)o(1) = o(q(T)). \quad (130)$$

Аналогично доказывается, что

$$2^k \max_{T_{2\ldots21}\in \mathbf{T}_\Pi}\{p(T_{2\ldots21})\} = o(p(T)). \quad (131)$$

Таким образом, из (125), (126), (127), (130), (131) и (99) следует:

$$\sum_{T_\cup\in\mathbf{T}_\cup} q(T_\cup) + \sum_{T_\cup\in\mathbf{T}_\cup} p(T_\cup) + \sum_{T_\cup\in\mathbf{T}_\cup} H(T_\cup) - H(T) \leqslant q(T) + p(T) +$$

$$+ 2\cdot 2^k \max_{T_{1\ldots12}\in\mathbf{T}_\Pi}\{q(T_{1\ldots12})\} + 2\cdot 2^k \max_{T_{2\ldots21}\in\mathbf{T}_\Pi}\{p(T_{2\ldots21})\} = o(q(T)). \quad (132)$$

Окончательную оценку для $L_{\text{вс}}(A(T))$ в случае 2° получаем из (124) и (132):

$$L_{\text{вс}}(A(T)) \leqslant \frac{H(T)}{\overline{\log}\,H(T)} + O\left(\frac{H(T)\,(\overline{\log}\,\overline{\log}\,H(T))^{1/2}}{(\log H(T))^{3/2}}\right) + O(q(T)). \quad (133)$$

Из (107), (133) и (99) следует утверждение (98). Теорема доказана.

Теорема 4. *Существуют положительные* c_{18} *и* c_{19} *такие, что для любой конечной абелевой группы* G *с базисом* $Б_G$ *справедливо неравенство*

$$L(G, Б_G) \leqslant \frac{\overline{\log}\,|G|}{\overline{\log}\,\overline{\log}\,|G|} + c_{18}\,\frac{\overline{\log}\,|G|\,(\overline{\log}\,\overline{\log}\,\overline{\log}\,|G|)^{1/2}}{(\overline{\log}\,\overline{\log}\,|G|)^{3/2}} + c_{19}\max(p, q).$$

Доказательство. Пусть $g \in G$. Тогда в силу (12) и (13) $\overline{\log}\,|G| \leqslant H\left(T_g^{Б_G}\right) \leqslant \overline{\log}\,|G| + q$. Поэтому из леммы 1 и теоремы 3 следует, что

$$L(g, Б_G) \leqslant L_{\text{вс}}\left(A\left(T_g^{Б_G}\right)\right) + 2p \leqslant \frac{H\left(T_g^{Б_G}\right)}{\overline{\log}\,H\left(T_g^{Б_G}\right)} +$$

$$+ c_{16}\,\frac{H\left(T_g^{Б_G}\right)\left(\overline{\log}\,\overline{\log}\,H\left(T_g^{Б_G}\right)\right)^{1/2}}{\left(\overline{\log}\,H\left(T_g^{Б_G}\right)\right)^{3/2}} + c_{17}\max\left(p\left(T_g^{Б_G}\right), q\left(T_g^{Б_G}\right)\right) + 2p \leqslant$$

$$\leqslant \frac{\overline{\log}\,|G|}{\overline{\log}\,\overline{\log}\,|G|} + q + 2c_{16}\,\frac{\overline{\log}\,|G|\,(\overline{\log}\,\overline{\log}\,\overline{\log}\,|G|)^{1/2}}{(\overline{\log}\,\overline{\log}\,|G|)^{3/2}} +$$

$$+ 2c_{16}q + c_{17}\max(p, q) + 2p \leqslant \frac{\overline{\log}\,|G|}{\overline{\log}\,\overline{\log}\,|G|} + 2c_{16}\,\frac{\overline{\log}\,|G|\,(\overline{\log}\,\overline{\log}\,\overline{\log}\,|G|)^{1/2}}{(\overline{\log}\,\overline{\log}\,|G|)^{3/2}} +$$

$$+ (2c_{16} + c_{17} + 3)\max(p, q).$$

Положим $c_{18} = 2c_{16}$, $c_{19} = 2c_{16} + c_{17} + 3$. Тогда для любого элемента $g \in G$ справедлива оценка

$$L(g, Б_G) \leqslant \frac{\overline{\log}\,|G|}{\overline{\log}\,\overline{\log}\,|G|} + c_{18}\,\frac{\overline{\log}\,|G|\,(\overline{\log}\,\overline{\log}\,\overline{\log}\,|G|)^{1/2}}{(\overline{\log}\,\overline{\log}\,|G|)^{3/2}} + c_{19}\max(p, q).$$

Теорема доказана.

Замечание. Из теорем 2 и 3 следует, что для произвольной последовательности конечных абелевых групп $\{G\}_n$, заданных последова-

тельностью базисов $\{Б_G\}_n$, при выполнении условия $\frac{\max(p, q)\log(\max(p, q))}{\log|G|} \to 0$ $\left(\text{оно равносильно условию } \frac{\max(p, q)\log\log|G|}{\log|G|} \to 0\right)$ справедливо асимптотическое равенство

$$L(G, Б_G) \sim \frac{\log|G|}{\log\log|G|}.$$

§ 2. Асимптотика функции $L(n)$ и остаточного члена

В этом параграфе изучается поведение функции Шеннона $L(n)$ при $n \to \infty$. Порядок $L(n)$ устанавливается просто. С одной стороны, для циклической группы $\langle g\rangle_n$ порядка n справедлива оценка

$$L(\langle g\rangle_n) \geqslant L(\langle g\rangle_n, \{g\}) \geqslant L(g^{n-1}, \{g\}) \geqslant [\log(n-1)] \sim \log n.$$

Отсюда

$$L(n) \gtrsim \log n. \tag{134}$$

С другой стороны, для произвольной абелевой группы G порядка n в любом базисе $Б_G$ справедливо

$$L(G, Б_G) \leqslant q - 1 + \sum_{i=1}^{q} 2\log k_i < q + 2\log\left(\prod_{i=1}^{q} k_i\right) \leqslant 3\log|G| = 3\log n.$$

Следовательно,

$$L(n) \leqslant 3\log n. \tag{135}$$

Из (134) и (135) получаем, что $L(n) \asymp \log n$.

Верхняя оценка, асимптотически равная нижней оценке (134), устанавливается уже заметно сложнее. Здесь же доказывается

Теорема 5. $L(n) - \log n \sim \frac{\log n}{\log\log n}$.

Верхняя оценка. Рассмотрим задачу о вычислении одночленов от многих переменных. Обозначим через $l(x_1^{k_1}x_2^{k_2}\dots x_q^{k_q})$ сложность вычисления $x_1^{k_1}x_2^{k_2}\dots x_q^{k_q}$, т. е. наименьшее число операций умножения, достаточное для вычисления $x_1^{k_1}x_2^{k_2}\dots x_q^{k_q}$.

Лемма 12. *Пусть даны целые*

$$k_i \geqslant 2, \quad 1 \leqslant i \leqslant q. \tag{136}$$

Тогда

$$l(x_1^{k_1}x_2^{k_2}\dots x_q^{k_q}) \leqslant \log n + \frac{\log n}{\log\log n} + o\left(\frac{\log n}{\log\log n}\right),$$

где $n = k_1k_2\dots k_q$.

Доказательство. Без ограничения общности можно считать, что

$$k_1 \geqslant k_2 \geqslant \dots \geqslant k_q. \tag{137}$$

Кроме того, будем считать, что n достаточно большое (т. е. все используемые неравенства, выполняющиеся при всех достаточно больших n, верны).

Положим

$$\varphi(n) = A\log\left(\frac{\log n}{\log\log n}\right), \tag{138}$$

где A — некоторая положительная константа, значение которой определим ниже.

Разобьем множество всех переменных $X = \{x_1, x_2, \dots, x_q\}$ на четыре группы (среди которых могут быть и пустые) — X_1, X_2, X_3 и X_4 следующим образом.

Положим

$$X_1 = \{x_i \in X \mid k_i > 2^{\log n/\varphi(n)\log\log n}\}. \tag{139}$$

Обозначим

$$\alpha = |X_1|, \quad n_1 = \prod_{i:\, x_i \in X_1} k_i. \tag{140}$$

Будем считать, что $n_1 = 1$, если $X_1 = \varnothing$.

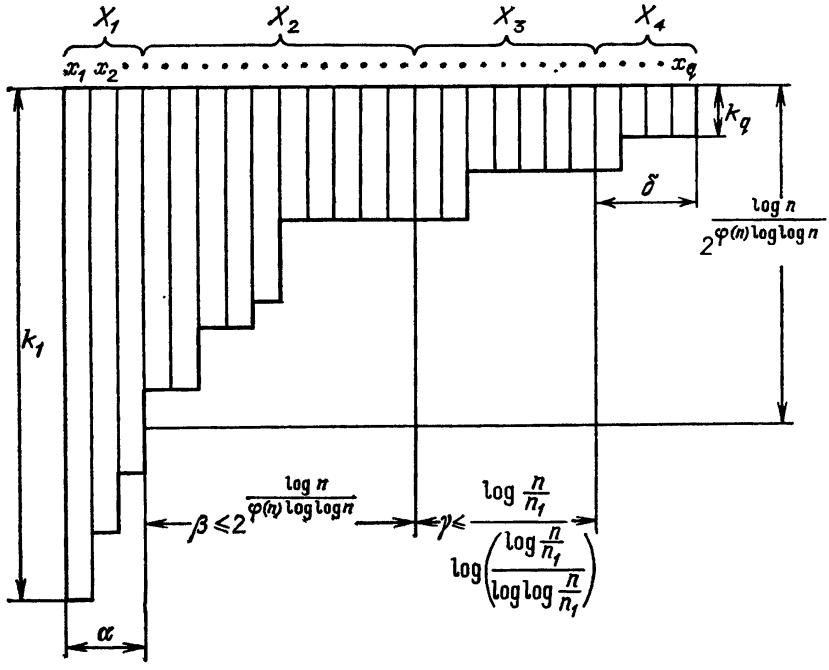


Рис. 11

Вторую группу определим так:

$$X_2 = \left\{x_i \in X \mid \alpha < i \leqslant \alpha + \frac{\log n}{\varphi(n)\log\log n}\right\}. \tag{141}$$

Обозначим

$$\beta = |X_2|, \quad n_2 = \prod_{i:\, x_i \in X_2} k_i. \tag{142}$$

В третью группу отнесем такие переменные:

$$X_3 = \left\{x_i \in X \mid \alpha + \beta < i \leqslant \alpha + \beta + \frac{\log \frac{n}{n_1}}{\log\left(\frac{\log \frac{n}{n_1}}{\log\log \frac{n}{n_1}}\right)}\right\}. \tag{143}$$

Обозначим

$$\gamma = |X_3|, \quad n_3 = \prod_{i:\, x_i \in X_3} k_i. \tag{144}$$

Оставшиеся переменные попадают в четвертую группу:

$$X_4 = X \setminus (X_1 \cup X_2 \cup X_3) = \{x_i \in X \mid \alpha + \beta + \gamma < i \leqslant q\}. \tag{145}$$

Обозначим

$$\delta = |X_4|, \quad n_4 = \prod_{i:\, x_i \in X_4} k_i. \tag{146}$$

Это разбиение переменных на группы схематично показано на рис. 11.

Очевидно, что

$$l\left(x_1^{k_1}\dots x_q^{k_q}\right)\leqslant l\left(x_1^{k_1}\dots x_\alpha^{k_\alpha}\right)+l\left(x_{\alpha+1}^{k_{\alpha+1}}\dots x_{\alpha+\beta}^{k_{\alpha+\beta}}\right)+l\left(x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}}\dots x_q^{k_q}\right)+2. \tag{147}$$

Оценим (на языке схем из функциональных элементов умножения) сверху каждое слагаемое в предположении, что каждое n_i, $i=1, 2, 3, 4$, соответствующее непустому множеству X_i, достаточно велико (т. е. все используемые неравенства, справедливые для всех достаточно больших n_i, верны). В случае малых n_i, $i=1, 2, 3, 4$, достаточно тривиальной оценки $l\left(y_1^{r_1}\dots y_s^{r_s}\right)\leqslant\sum_{i=1}^{s} r_i-1$.

1. Вычисление $x_1^{k_1}\dots x_\alpha^{k_\alpha}$. Вычисление основано на использовании метода Брауэра [4] (см. также [1, с. 494—495]) асимптотически оптимального вычисления степеней. Запишем каждый показатель k_i, $1\leqslant i\leqslant\alpha$, в 2^{l_i}-арной системе счисления (значения l_i, $1\leqslant i\leqslant\alpha$, выберем позже):

$$k_i=d_{0i}\left(2^{l_i}\right)^{t_i}+d_{1i}\left(2^{l_i}\right)^{t_i-1}+\dots+d_{t_i-1,i}\left(2^{l_i}\right)^{1}+d_{t_i,i}. \tag{148}$$

Блоки B_i, $1\leqslant i\leqslant\alpha$, будут вычислять $x_i^{k_i}$ (рис. 12). Используя эти блоки, построим схему S_1, реализующую $x_1^{k_1}x_2^{k_2}\dots x_\alpha^{k_\alpha}$ (рис. 13).

Подсчитав число элементов умножения в схеме S_1, получаем:

$$l\left(x_1^{k_1}\dots x_\alpha^{k_\alpha}\right)\leqslant\sum_{i=1}^{\alpha}\left(2^{l_i}-2+l_it_i+t_i\right)+\alpha-1\leqslant\sum_{i=1}^{\alpha}\left(2^{l_i}+l_it_i+t_i\right). \tag{149}$$

Положим

$$l_i=\rfloor\log\log k_i-2\log\log\log k_i\lfloor. \tag{150}$$

Из (148) следует, что $k_i\geqslant 2^{l_it_i}$ и, следовательно, учитывая (150),

$$t_i\leqslant\frac{\log k_i}{l_i}=\frac{\log k_i}{\rfloor\log\log k_i-2\log\log\log k_i\lfloor}. \tag{151}$$

Подставляя (150), (151) в (149) и учитывая (139), (140) и (141), получаем:

$$l\left(x_1^{k_1}\dots x_\alpha^{k_\alpha}\right)\leqslant$$

$$\leqslant\sum_{i=1}^{\alpha}\left(\frac{2\log k_i}{(\log\log k_i)^2}+\log k_i+\frac{\log k_i}{\log\log k_i-2\log\log\log k_i}\right)\leqslant$$

$$\leqslant\left(\sum_{i=1}^{\alpha}\log k_i\right)\left(1+\frac{2}{\left(\log\frac{\log n}{\varphi(n)\log\log n}\right)^2}+\frac{1}{\log\frac{\log n}{\varphi(n)\log\log n}-2\log\log\frac{\log n}{\varphi(n)\log\log n}}\right)=$$

$$=\log n_1\left(1+\frac{1}{\log\log n-\log\varphi(n)-\log\log\log n-2\log\log\log n+2\log\log\varphi(n)+2\log\log\log\log n}+\right.$$

$$\left.+\frac{2}{(\log\log n-\log\varphi(n)-\log\log\log n)^2}\right)=\log n_1+\frac{\log n_1}{\log\log n}+$$

$$+o\left(\frac{\log n_1}{\log\log n}\right)=\log n_1+\frac{\log n_1}{\log\log n}+o\left(\frac{\log n}{\log\log n}\right). \tag{152}$$

2. Вычисление $x_{\alpha+1}^{k_{\alpha+1}}\dots x_{\alpha+\beta}^{k_{\alpha+\beta}}$ ($\beta\geqslant 1$). Выпишем по столбцам в таблицу T_β двоичные записи чисел $k_{\alpha+1}$, $k_{\alpha+2}$, …, $k_{\alpha+\beta}$ (младшие разряды сверху). Полученная таблица имеет длину β и высоту $[\log k_{\alpha+1}]+1$. По

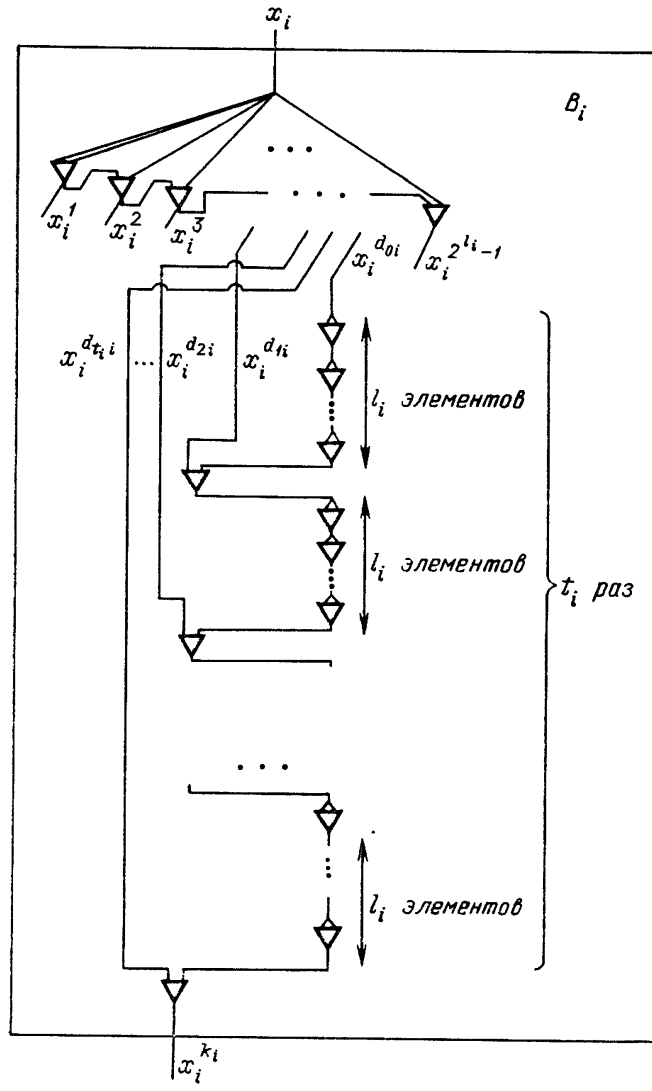

x_i
B_i
x_i^1
x_i^2
x_i^3
$x_i^{d_{0i}}$
$x_i^{2^{l_i-1}}$
$x_i^{d_{t_i i}}$
$x_i^{d_{2i}}$
$x_i^{d_{1i}}$
l_i элементов
l_i элементов
t_i раз
l_i элементов
$x_i^{k_i}$

Рис. 12

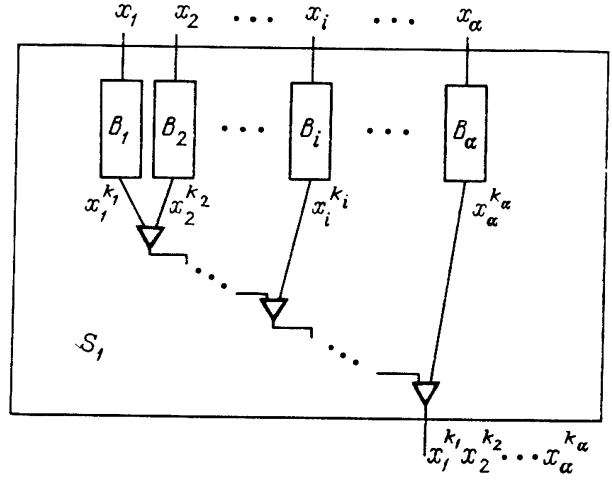

x_1 x_2 ... x_i ... x_α
B_1 B_2 ... B_i ... B_α
$x_1^{k_1}$ $x_2^{k_2}$ $x_i^{k_i}$ $x_\alpha^{k_\alpha}$
S_1
$x_1^{k_1} x_2^{k_2} \ldots x_\alpha^{k_\alpha}$

Рис. 13

теореме 3 имеем:

$$L_{\text{вс}}(A(T_\beta)) \leqslant$$

$$\leqslant \frac{H(T_\beta)}{\overline{\log} H(T_\beta)}\left(1 + c_{16}\left(\frac{\overline{\log}\,\overline{\log} H(T_\beta)}{\overline{\log} H(T_\beta)}\right)^{1/2}\right) + c_{17}\max(\beta, [\log k_{\alpha+1}] + 1) \leqslant$$

$$\leqslant \frac{H(T_\beta)}{\overline{\log} H(T_\beta)} + c_{16}\frac{H(T_\beta)(\overline{\log}\,\overline{\log} H(T_\beta))^{1/2}}{(\overline{\log} H(T_\beta))^{3/2}} + c_{17}\beta + c_{17}\log k_{\alpha+1}. \quad (153)$$

В силу построения таблицы T_β, используя (142), получаем:

$$H(T_\beta) = \sum_{i=\alpha+1}^{\alpha+\beta}([\log k_i] + 1) \leqslant \sum_{i=\alpha+1}^{\alpha+\beta}\log k_i + \beta = \log n_2 + \beta; \quad (154)$$

$$H(T_\beta) \geqslant \sum_{i=\alpha+1}^{\alpha+\beta}\log k_i = \log n_2. \quad (155)$$

Из (153) с учетом (154) и (155) следует, что

$$L_{\text{вс}}(A(T_\beta)) \leqslant \frac{\log n_2 + \beta}{\log\log n_2} + c_{16}(\log n_2 + \beta)\frac{(\log\log(\log n_2 + \beta))^{1/2}}{(\log\log n_2)^{3/2}} +$$

$$+ c_{17}\beta + c_{17}\log k_{\alpha+1} \leqslant \frac{\log n_2}{\log\log n_2} + 2c_{16}\frac{\log n_2(\log\log\log n_2)^{1/2}}{(\log\log n_2)^{3/2}} +$$

$$+ (1 + 2c_{16} + c_{17})\beta + c_{17}\log k_{\alpha+1}. \quad (156)$$

Рассматривая произведение $x_{\alpha+1}^{k_{\alpha+1}} \ldots x_{\alpha+\beta}^{k_{\alpha+\beta}}$ как элемент конечнопорожденной абелевой группы $\langle x_{\alpha+1}\rangle_\infty \times \langle x_{\alpha+2}\rangle_\infty \times \ldots \times \langle x_{\alpha+\beta}\rangle_\infty$, применяя замечание к лемме 1 и используя (156), (141), (142), неравенство $k_{\alpha+1} \leqslant 2^{\log n/\varphi(n)\log\log n}$ и (138), получаем:

$$l\left(x_{\alpha+1}^{k_{\alpha+1}} \ldots x_{\alpha+\beta}^{k_{\alpha+\beta}}\right) \leqslant L_{\text{вс}}(A(T_\beta)) + 2([\log k_{\alpha+1}] + 1) - 2 \leqslant$$

$$\leqslant \frac{\log n_2}{\log\log n_2} + 2c_{16}\frac{\log n_2(\log\log\log n_2)^{1/2}}{(\log\log n_2)^{3/2}} + (1 + 2c_{16} + c_{17})\beta +$$

$$+ (c_{17} + 2)\log k_{\alpha+1} \leqslant \frac{\log n_2}{\log\log n_2} + 2c_{16}\frac{\log n_2(\log\log\log n_2)^{1/2}}{(\log\log n_2)^{3/2}} +$$

$$+ (2c_{16} + c_{17} + 3)\frac{\log n}{\varphi(n)\log\log n} \leqslant \frac{\log n_2}{\log\log n_2} + o\left(\frac{\log n_2}{\log\log n_2}\right) +$$

$$+ o\left(\frac{\log n}{\log\log n}\right) = \frac{\log n_2}{\log\log n_2} + o\left(\frac{\log n}{\log\log n}\right). \quad (157)$$

3. Вычисление $x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}} \ldots x_q^{k_q}$. Пусть B — некоторая положительная константа, значение которой определим ниже. Рассмотрим два случая.

Случай 1°.

$$q - (\alpha + \beta) = \gamma + \delta \leqslant \log\frac{n}{n_1} - B\frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}}. \quad (158)$$

Отдельно реализуем $x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}} \ldots x_{\alpha+\beta+\gamma}^{k_{\alpha+\beta+\gamma}}$ и $x_{\alpha+\beta+\gamma+1}^{k_{\alpha+\beta+\gamma+1}} \ldots x_q^{k_q}$. Очевидно, что

$$l\left(x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}} \ldots x_q^{k_q}\right) \leqslant$$

$$\leqslant l\left(x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}} \ldots x_{\alpha+\beta+\gamma}^{k_{\alpha+\beta+\gamma}}\right) + l\left(x_{\alpha+\beta+\gamma+1}^{k_{\alpha+\beta+\gamma+1}} \ldots x_q^{k_q}\right) + 1. \quad (159)$$

а) *Вычисление* $x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}} \dots x_{\alpha+\beta+\gamma}^{k_{\alpha+\beta+\gamma}}$. Аналогично таблице T_β определим T_γ как таблицу из столбцов двоичных записей чисел $k_{\alpha+\beta+1}, \dots, k_{\alpha+\beta+\gamma}$. Таблица T_γ имеет длину γ и высоту $[\log k_{\alpha+\beta+1}]+1$.

Применяя замечание к лемме 1 и теорему 3, получаем:

$$l\left(x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}} \dots x_{\alpha+\beta+\gamma}^{k_{\alpha+\beta+\gamma}}\right) \leqslant \frac{H(T_\gamma)}{\overline{\log} H(T_\gamma)} + c_{16}\frac{H(T_\gamma)\left(\overline{\log}\,\overline{\log} H(T_\gamma)\right)^{1/2}}{\left(\overline{\log} H(T_\gamma)\right)^{3/2}} +$$
$$+ c_{17}\max(\gamma, [\log k_{\alpha+\beta+1}]+1) + 2([\log k_{\alpha+\beta+1}]+1) - 2. \quad (160)$$

В силу построения таблицы T_γ, используя (144), имеем:

$$H(T_\gamma) = \sum_{i=\alpha+\beta+1}^{\alpha+\beta+\gamma}([\log k_i]+1) \leqslant \sum_{i=\alpha+\beta+1}^{\alpha+\beta+\gamma}\log k_i + \gamma = \log n_3 + \gamma; \quad (161)$$

$$H(T_\gamma) \geqslant \sum_{i=\alpha+\beta+1}^{\alpha+\beta+\gamma}\log k_i = \log n_3. \quad (162)$$

Кроме того,

$$k_{\alpha+\beta+1} \leqslant k_{\alpha+1} \leqslant 2^{\frac{\log n}{\varphi(n)\log\log n}}. \quad (163)$$

Из (160) с учетом (161), (162), (163) и (138) следует, что

$$l\left(x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}} \dots x_{\alpha+\beta+\gamma}^{k_{\alpha+\beta+\gamma}}\right) \leqslant \frac{\log n_3+\gamma}{\log\log n_3} +$$
$$+ c_{16}(\log n_3+\gamma)\frac{(\log\log(\log n_3+\gamma))^{1/2}}{(\log\log n_3)^{3/2}} + c_{17}\gamma + (c_{17}+2)\log k_{\alpha+\beta+1} \leqslant$$
$$\leqslant \frac{\log n_3}{\log\log n_3} + 2c_{16}\frac{\log n_3(\log\log\log n_3)^{1/2}}{(\log\log n_3)^{3/2}} + (1+2c_{16}+c_{17})\gamma +$$
$$+ (c_{17}+2)\frac{\log n}{\varphi(n)\log\log n} = \frac{\log n_3}{\log\log n_3} + (1+2c_{16}+c_{17})\gamma +$$
$$+ o\left(\frac{\log n_3}{\log\log n_3}\right) + o\left(\frac{\log n}{\log\log n}\right) = \frac{\log n_3}{\log\log n_3} + (1+2c_{16}+c_{17})\gamma + o\left(\frac{\log n}{\log\log n}\right). \quad (164)$$

б) *Вычисление* $x_{\alpha+\beta+\gamma+1}^{k_{\alpha+\beta+\gamma+1}} \dots x_q^{k_q}$. Будем считать, что $\delta = q-(\alpha+\beta+\gamma) \geqslant 1$. Тогда в силу определения множеств X_3 и X_4

$$\gamma = \frac{\log\frac{n}{n_1}}{\log\left(\frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}}\right)}. \quad (165)$$

Поэтому

$$(k_{\alpha+\beta+\gamma+1})^{\log\frac{n}{n_1}\Big/\log\left(\frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}}\right)} = (k_{\alpha+\beta+\gamma+1})^{\gamma} \leqslant$$
$$\leqslant \prod_{i=1}^{\gamma}(k_{\alpha+\beta+i}) = \prod_{i:x_i\in X_3} k_i = n_3 \leqslant \frac{n}{n_1}.$$

Следовательно, $\log(k_{\alpha+\beta+\gamma+1}) \leqslant \log\left(\dfrac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}}\right)$. Отсюда

$$k_{\alpha+\beta+\gamma+1} \leqslant \frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}}. \tag{166}$$

На основе схемы, последовательно реализующей все степени до $k_{\alpha+\beta+\gamma+1}$ включительно, можно построить схему из $\delta - 1 + k_{\alpha+\beta+\gamma+1} - 1$ элементов умножения, реализующую $x_{\alpha+\beta+\gamma+1}^{k_{\alpha+\beta+\gamma+1}} \dots x_q^{k_q}$. Учитывая (166), получаем:

$$l\left(x_{\alpha+\beta+\gamma+1}^{k_{\alpha+\beta+\gamma+1}} \dots x_q^{k_q}\right) \leqslant \delta + \frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}}. \tag{167}$$

Таким образом, в случае 1°, т. е. при выполнении условия (158), из (153), (164) и (167), учитывая (159) и (165), следует такая оценка:

$$l\left(x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}} \dots x_q^{k_q}\right) \leqslant \frac{\log n_3}{\log\log n_3} + (\gamma+\delta) + (2c_{16}+c_{17})\gamma +$$

$$+ \frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}} + o\left(\frac{\log n}{\log\log n}\right) \leqslant \frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}} + \log\frac{n}{n_1} - B\frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}} +$$

$$+ (2c_{16}+c_{17})\frac{\log\frac{n}{n_1}}{\log\left(\dfrac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}}\right)} + \frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}} + o\left(\frac{\log n}{\log\log n}\right) =$$

$$= \log\frac{n}{n_1} + (2-B)\frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}} + (2c_{16}+c_{17})\frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}}\cdot\frac{1}{1-\dfrac{\log\log\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}}} +$$

$$+ o\left(\frac{\log n}{\log\log n}\right) = \log\frac{n}{n_1} + (2 + 2c_{16} + c_{17} - B)\frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}} + o\left(\frac{\log n}{\log\log n}\right). \tag{168}$$

Случай 2.

$$q - (\alpha+\beta) = \gamma + \delta > \log\frac{n}{n_1} - B\frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}}. \tag{169}$$

Тогда в силу определения множеств X_2, X_3 и X_4 $\beta = \dfrac{\log n}{\varphi(n)\log\log n}$. Отсюда,

учитывая (137), (144), (146), (136) и (169), получаем:

$$(k_{\alpha+\beta+1})^{\frac{\log n}{\varphi(n)\log\log n}} = (k_{\alpha+\beta+1})^{\beta} \leqslant \prod_{i=1}^{\beta} k_{\alpha+i} = \prod_{i:\, x_i \in X_2} k_i =$$

$$= n_2 = \frac{n}{n_1 n_3 n_4} \leqslant \frac{n/n_1}{2^{\gamma+\delta}} < 2^{B\frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}}}.$$

Следовательно,

$$\log(k_{\alpha+\beta+1}) \leqslant \frac{B\dfrac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}}}{\dfrac{\log n}{\varphi(n)\log\log n}} \leqslant B\varphi(n). \tag{170}$$

На основе схемы, последовательно реализующей все степени до $k_{\alpha+\beta+1}$ включительно, можно построить схему из $\gamma+\delta-1+k_{\alpha+\beta+1}-1$ элементов умножения, вычисляющую $x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}} \ldots x_q^{k_q}$. Отсюда, учитывая (170), имеем:

$$l\left(x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}} \ldots x_q^{k_q}\right) \leqslant \gamma + \delta + 2^{B\varphi(n)}. \tag{171}$$

Таким образом, в случае 2°, т. е. при выполнении условия (169), из (171), учитывая (136), (144) и (146), получаем следующую оценку:

$$l\left(x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}} \ldots x_q^{k_q}\right) \leqslant \log(n_3 n_4) + 2^{B\varphi(n)} \leqslant \log\frac{n}{n_1} + 2^{B\varphi(n)}. \tag{172}$$

Из неравенств (168) и (172) вытекает, что и в случае 1°, и в случае 2° справедлива такая оценка:

$$l\left(x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}} \ldots x_q^{k_q}\right) \leqslant \log\frac{n}{n_1} + \max(2 + 2c_{16} + c_{17} - B, 0)\frac{\log\frac{n}{n_1}}{\log\log\frac{n}{n_1}} +$$

$$+ 2^{B\varphi(n)} + o\left(\frac{\log n}{\log\log n}\right). \tag{173}$$

Положим

$$B = 2 + 2c_{16} + c_{17}, \tag{174}$$

$$A = \frac{1}{2(2 + 2c_{16} + c_{17})}. \tag{175}$$

Подставляя (138), (174) и (175) в (173), получаем:

$$l\left(x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}} \ldots x_q^{k_q}\right) \leqslant \log\frac{n}{n_1} + 2^{1/2\log\left(\frac{\log n}{\log\log n}\right)} + o\left(\frac{\log n}{\log\log n}\right) =$$

$$= \log\frac{n}{n_1} + o\left(\frac{\log n}{\log\log n}\right). \tag{176}$$

Теперь, имея оценки (152), (157) и (176) сложности вычисления соответственно $x_1^{k_1} \ldots x_\alpha^{k_\alpha}$, $x_{\alpha+1}^{k_{\alpha+1}} \ldots x_{\alpha+\beta}^{k_{\alpha+\beta}}$ и $x_{\alpha+\beta+1}^{k_{\alpha+\beta+1}} \ldots x_q^{k_q}$, можем оце-

нить, используя (147), и сложность вычисления $x_1^{k_1} \dots x_q^{k_q}$:

$$l\left(x_1^{k_1} \dots x_q^{k_q}\right) \leqslant$$

$$\leqslant \log n_1 + \frac{\log n_1}{\log\log n} + \frac{\log n_2}{\log\log n_2} + \log\frac{n}{n_1} + o\left(\frac{\log n}{\log\log n}\right) =$$

$$= \log n + \frac{\log n_1}{\log\log n} + \frac{\log n_2}{\log\log n_2} + o\left(\frac{\log n}{\log\log n}\right). \quad (177)$$

Осталось оценить сверху $\frac{\log n_2}{\log\log n_2}$. Если $\log n_2 \leqslant \frac{\log n}{(\log\log n)^2}$, то

$$\frac{\log n_2}{\log\log n_2} = o\left(\frac{\log n}{\log\log n}\right).$$

Если $\log n_2 > \frac{\log n}{(\log\log n)^2}$, то

$$\frac{\log n_2}{\log\log n_2} \leqslant \frac{\log n_2}{\log\frac{\log n}{(\log\log n)^2}} = \frac{\log n_2}{\log\log n}\,\frac{1}{1 - \frac{2\log\log\log n}{\log\log n}} =$$

$$= \frac{\log n_2}{\log\log n} + o\left(\frac{\log n}{\log\log n}\right)$$

Таким образом, в любом случае

$$\frac{\log n_2}{\log\log n_2} \leqslant \frac{\log n_2}{\log\log n} + o\left(\frac{\log n}{\log\log n}\right). \quad (178)$$

Подставляя (178) в (177), получаем:

$$l\left(x_1^{k_1} \dots x_q^{k_q}\right) \leqslant \log n + \frac{\log n_1}{\log\log n} + \frac{\log n_2}{\log\log n} + o\left(\frac{\log n}{\log\log n}\right) \leqslant$$

$$\leqslant \log n + \frac{\log n}{\log\log n} + o\left(\frac{\log n}{\log\log n}\right).$$

Лемма доказана.

Вернемся к доказательству верхней оценки теоремы 5. Пусть G — произвольная абелева группа порядка n, а $Б_G = \{g_1, g_2, \dots, g_q\}$ — ее базис. Тогда $G = \langle g_1\rangle_{k_1} \times \langle g_2\rangle_{k_2} \times \dots \times \langle g_q\rangle_{k_q}$, где k_i — порядок базисного элемента g_i, $1 \leqslant i \leqslant q$, причем $\prod\limits_{i=1}^{q} k_i = n$.

Произвольный элемент $g \in G$ можно представить в виде $g = g_1^{t_1} g_2^{t_2} \dots g_q^{t_q}$, $t_i \leqslant k_i - 1$ $(1 \leqslant i \leqslant q)$. Выделим среди показателей степени t_i, $1 \leqslant i \leqslant q$, нулевые и единичные. Без ограничения общности можно считать, что это первые r показателей. Обозначим

$$m = 2^r \prod_{i=r+1}^{q} t_i. \quad (179)$$

Очевидно, что

$$m \leqslant n. \quad (180)$$

Для сложности элемента g в базисе $Б_G$ справедлива оценка:

$$L(g, Б_G) = L\left(g_1^{t_1} g_2^{t_2} \dots g_q^{t_q}, Б_G\right) \leqslant l\left(x_1^{t_1} \dots x_r^{t_r} x_{r+1}^{t_{r+1}} \dots x_q^{t_q}\right) \leqslant$$

$$\leqslant l\left(x_1^2 \dots x_r^2 x_{r+1}^{t_{r+1}} \dots x_q^{t_q}\right). \quad (181)$$

Для оценки сложности вычисления $x_1^2 \dots x_r^2 x_{r+1}^{t_{r+1}} \dots x_q^{t_q}$ применяем лемму 12, учитывая (179):

$$l\left(x_1^2 \dots x_r^2 x_{r+1}^{t_{r+1}} \dots x_q^{t_q}\right) \leqslant \log m + \frac{\log m}{\log\log m} + o\left(\frac{\log m}{\log\log m}\right). \qquad (182)$$

Из (181) и (182), используя (180), получаем:

$$L(g, Б_G) \leqslant \log m + \frac{\log m}{\log\log m} + o\left(\frac{\log m}{\log\log m}\right) \leqslant \log n + \frac{\log n}{\log\log n} + o\left(\frac{\log n}{\log\log n}\right).$$

Отсюда в силу произвольности группы G, базиса $Б_G$ и элемента g, непосредственно следует асимптотическое неравенство

$$L(n) - \log n \lesssim \frac{\log n}{\log\log n}.$$

Верхняя оценка теоремы 5 доказана.

Нижняя оценка. Нижняя оценка нужного вида будет доказана для циклической группы $\langle g\rangle_n$ порядка n в базисе, состоящем из одного элемента $\{g\}$, являющегося порождающим элементом группы.

В основе доказательства — мощностные рассуждения.

Напомним некоторые определения (подробнее см., например, [1, с. 482—498]).

Возрастающей аддитивной цепочкой для натурального числа n называется последовательность натуральных чисел

$$1 = a_0 < a_1 < a_2 < \dots < a_r = n, \qquad (183)$$

обладающих тем свойством, что $a_i = a_j + a_l$ при некоторых $j \leqslant l < i$ для всех $1 \leqslant i \leqslant r$.

Наименьшее значение r длины возрастающих аддитивных цепочек для n называется *аддитивной сложностью числа n* и обозначается $l(n)$.

Индукцией по i легко показать, что $a_i \leqslant 2^i$, и поэтому для любой возрастающей аддитивной цепочки (183) справедливо неравенство

$$\log n \leqslant r. \qquad (184)$$

Заметим, что

$$l(n) = l(x^n), \qquad (185)$$

так как по возрастающей аддитивной цепочке (183) естественным образом строится схема для вычисления x^n, использующая ровно r операций умножения, причем i-й элемент схемы вычисляет x^{a_i}, и наоборот, по схеме просто строится аддитивная цепочка той же сложности, которую можно легко сделать возрастающей.

Пусть $m \geqslant 2$, $0 < \varepsilon \leqslant 1$.

Обозначим через $N(m, \varepsilon)$ число возрастающих аддитивных цепочек (183), удовлетворяющих соотношениям

$$2^m \leqslant n < 2^{m+1}; \qquad (186)$$

$$r \leqslant m + (1 - \varepsilon)\, m/\log m. \qquad (187)$$

Через $\tilde{N}(m, \varepsilon)$ обозначим число возрастающих аддитивных цепочек (183), удовлетворяющих соотношениям

$$n \geqslant 2^m; \qquad (188)$$

$$r \leqslant m + (1 - \varepsilon)\, m/\log m. \qquad (189)$$

П. Эрдеш [5] (см. также [1, с. 495—498]) доказал следующее свойство $N(m, \varepsilon)$:

Лемма 13. *Для всякого* $0<\varepsilon\leqslant 1$ *найдется* $b=b(\varepsilon)>1$ *такое, что при всех достаточно больших* m

$$N(m,\ \varepsilon)<2^m/b^m.$$

Другими словами, для больших m величина $N(m,\ \varepsilon)$ существенно меньше количества чисел n, удовлетворяющих условию (186).

С использованием леммы 13 докажем аналогичное свойство $\widetilde{N}(m,\ \varepsilon)$.

Лемма 14. *Для всякого* $0<\varepsilon\leqslant 1$ *найдется* $c=c(\varepsilon)>1$ *такое, что при всех достаточно больших* m

$$\widetilde{N}(m,\ \varepsilon)<\frac{2^m}{c^m}.$$

Доказательство. Любая аддитивная цепочка (183), удовлетворяющая условию (189), в силу (184) удовлетворяет и соотношению

$$n\leqslant 2^{m+\frac{(1-\varepsilon)m}{\log m}}. \tag{190}$$

Кроме того, для целых $m\geqslant 2$ и $i\geqslant 0$ справедливо неравенство

$$(m+i)+\frac{(1-\varepsilon)(m+i)}{\log(m+i)}\geqslant m+\frac{(1-\varepsilon)m}{\log m}. \tag{191}$$

В силу определения $\widetilde{N}(m,\ \varepsilon)$ и $N(m,\ \varepsilon)$, (190) и (191), имеем:

$$\widetilde{N}(m,\ \varepsilon))\leqslant \sum_{i=0}^{(1-\varepsilon)m/\log m} N(m+i,\ \varepsilon).$$

Тогда, применяя лемму 13, получаем, что найдется $1<b=b(\varepsilon)<2$ такое, что при всех достаточно больших m выполняется соотношение

$$\widetilde{N}(m,\ \varepsilon)\leqslant \sum_{i=0}^{(1-\varepsilon)m/\log m}\frac{2^{m+i}}{b^{m+i}}\leqslant\left(\frac{2}{b}\right)^m\frac{\left(\frac{2}{b}\right)^{\frac{(1-\varepsilon)m}{\log m}+1}}{2/b-1}\leqslant$$

$$\leqslant\frac{b}{2-b}\left(\frac{2}{b}\right)^{m+\frac{(1-\varepsilon)m}{\log m}+1}. \tag{192}$$

Обозначим $c=c(\varepsilon)=\dfrac{1+b(\varepsilon)}{2}$. Тогда, учитывая, что $1<b<2$, имеем:

$$1<c<b<2. \tag{193}$$

Поэтому при всех достаточно больших m выполняется неравенство

$$\frac{b}{2-b}\left(\frac{2}{b}\right)^{m+\frac{(1-\varepsilon)m}{\log m}+1}<\frac{2^m}{c^m}, \tag{194}$$

так как оно равносильно неравенствам

$$\left(1+\frac{1-\varepsilon}{\log m}+\frac{1}{m}\right)(1-\log b)+\frac{\log\frac{b}{2-b}}{m}<1-\log c$$

и

$$\left(1+\frac{1-\varepsilon}{\log m}+\frac{1}{m}\right)\frac{1-\log b}{1-\log c}+\frac{\log\frac{b}{2-b}}{m(1-\log c)}<1,$$

а последнее из них при достаточно больших m в силу (193) выполняется.

Окончательно из (192) и (194) следует, что при всех достаточно больших m выполнено $\tilde{N}(m, \varepsilon) < \frac{2^m}{c^m}$, где вследствие (193) $c = c(\varepsilon) > 1$. Лемма доказана.

Теперь вернемся к получению нижней оценки.

Лемма 15. *Для всякого* $\varepsilon > 0$ *при всех достаточно больших* n *выполняется неравенство*

$$L(\langle g\rangle_n, \{g\}) > [\log(n-1)] - 1 + \frac{(1-\varepsilon)([\log(n-1)]-1)}{\log([\log(n-1)]-1)}.$$

Доказательство. Каждой минимальной схеме из элементов умножения, реализующей $g^s \in \langle g_n\rangle$, $s \leqslant n-1$, естественным образом можно поставить в соответствие возрастающую аддитивную цепочку для t, где t имеет вид $t = s + l \cdot n$, $l \geqslant 0$, причем сложность схемы, реализующей g^s, будет равна аддитивной сложности числа t. Схемам, реализующим разные элементы g^{s_1} и g^{s_2} группы $\langle g\rangle_n$ (т. е. $0 \leqslant s_1 < s_2 \leqslant n-1$) будут соответствовать разные аддитивные цепочки, так как их последние члены будут сравнимы по модулю n соответственно с s_1 и s_2.

Положим

$$m = [\log(n-1)] - 1. \tag{195}$$

Предположим, что

$$L(\langle g\rangle_n, \{g\}) \leqslant m + \frac{(1-\varepsilon)m}{\log m}. \tag{196}$$

Рассмотрим аддитивные цепочки, соответствующие минимальным схемам для элементов g^{2^m}, g^{2^m+1}, ..., g^{n-1} группы $\langle g\rangle_n$. Их не менее чем $n-1-2^m$ штук, причем в силу (196) все они удовлетворяют условиям (188) и (189). Поэтому $\tilde{N}(m, \varepsilon) \geqslant n-1-2^m$. Отсюда, учитывая (195), получаем, что $\tilde{N}(m, \varepsilon) \geqslant 2^m$.

Но, с другой стороны, при всех достаточно больших m (а следовательно, в силу (195) и при всех достаточно больших n) по лемме 14 $\tilde{N}(m, \varepsilon) < 2^m$.

Таким образом, при всех достаточно больших n предположение (196) неверно. Лемма доказана.

Следствие. $L(n) - \log n \gtrsim \frac{\log n}{\log\log n}$.

Доказана нижняя оценка (а с ней и вся теорема).

В заключение автор выражает искреннюю благодарность научному руководителю О. Б. Лупанову за внимание к работе и ценные советы.

СПИСОК ЛИТЕРАТУРЫ

1. Кнут Д. Искусство программирования для ЭВМ. Т. 2.— М.: Мир, 1977.
2. Лупанов О. Б. О вентильных и контактно-вентильных схемах // ДАН СССР.— 1956.— 111, № 6.— С. 1171—1174.
3. Харди Г. Г., Литтлвуд Дж. Е., Полиа Г. Неравенства.— М.: ГИИЛ, 1948.
4. Brauer A. On addition chains // Bull. Amer. Math. Soc.— 1939.— V. 45.— P. 736—739.
5. Erdös P. Remarks on number theory, III: On addition chains // Acta Arith.— 1960.— V. 6.— P. 77—81.
6. Pippenger N. The minimum number of edges in graphs with prescribed path // Math. Systems Theory.— 1979.— V. 12.— P. 325—346.

Поступило в редакцию 14.IV.90