

УДК 519.7

УТОЧНЕНИЕ ОЦЕНОК СЛОЖНОСТИ ВЫЧИСЛЕНИЯ  
ОДНОЧЛЕНОВ И НАБОРОВ СТЕПЕНЕЙ  
В ЗАДАЧАХ БЕЛЛМАНА И КНУТА <sup>\*)</sup>

*В. В. Кочергин*

**Аннотация.** Изучаются два обобщения классической задачи о наискорейшем возведении в степень — задача Беллмана о сложности (наименьшем числе операций умножения) вычисления исхода только из переменных нормированного одночлена от  $m$  переменных и задача Кнута о сложности совместного вычисления системы из  $m$  степеней одной переменной. Дается обзор некоторых результатов, связанных с этими задачами, а также уточняются асимптотические оценки сложности в задачах Беллмана и Кнута, когда поведение величины  $m$  сравнимо со сложностью (они имеют одинаковый порядок роста). Помимо того, что установленные верхние и нижние оценки сложности для задач Беллмана и Кнута для почти всех наборов степеней дают асимптотику роста сложности в широком диапазоне соотношений параметров (число переменных или вычисляемых степеней, значение максимального показателя степени и произведение всех показателей степеней), они ещё гарантируют при любом соотношении параметров превышение верхней оценки над нижней асимптотически не более, чем в  $5/3$  раза.

**Ключевые слова:** аддитивная цепочка, вычисление степени, вычисление одночлена, задача Беллмана, задача Кнута.

В работе рассматриваются обобщения известной задачи о сложности возведения в степень, т. е. задачи о нахождении величины  $l(x^n)$  — минимального числа операций умножения, достаточного для вычисления величины  $x^n$  по переменной  $x$ . Эту задачу (а также её обобщения) часто рассматривают в аддитивной постановке — в этом случае говорят про задачу об аддитивных цепочках, которая формулируется следующим образом (см., например, [2]).

---

<sup>\*)</sup>Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 11-01-00508 и 14-01-00598).

*Аддитивной цепочкой* для натурального числа  $n$  называется всякая последовательность целых чисел  $a_0 = 1, a_1, \dots, a_m = r$ , удовлетворяющая свойству: для каждого  $k, 1 \leq k \leq r$ , найдётся два целых числа (не обязательно различных)  $i$  и  $j, 0 \leq i, j \leq k-1$ , таких, что  $a_k = a_i + a_j$ . Минимальная длина  $r$  аддитивной цепочки для  $n$  называется *аддитивной сложностью* числа  $n$  и обозначается через  $l(n)$ .

Очевидно, что величины  $l(n)$  и  $l(x^n)$  совпадают.

В 1939 г. А. Брауэр [14] для величины  $l(n)$  при  $n \rightarrow \infty$  установил асимптотическую формулу<sup>1)</sup>

$$l(n) \sim \log n$$

и получил верхнюю оценку

$$l(n) \leq \log n + \frac{\log n}{\log \log n} + O\left(\frac{\log n \log \log \log n}{(\log \log n)^2}\right).$$

В 1960 г. П. Эрдёш [16] показал, что для почти всех  $n$  справедливо асимптотическое равенство

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

при этом стоит отметить разную природу слагаемых в правой части: слагаемое  $\log n$  связано с величиной числа  $n$  и должно присутствовать для любого значения  $n$ , а наличие «мощностного» слагаемого (отношения логарифма количества чисел, не превосходящих  $n$ , к повторному логарифму этого количества) зависит от «строения» числа  $n$  и присутствует для «почти всех»  $n$ .

После этого исследовались различные вопросы, связанные с задачей о наискорейшем возведении в степень (см., например, обзоры [17, 24], а также последние издания книги [2]).

В 1963 г. Р. Беллман в [13] (для случая  $m = 2$ ), а затем в 1964 г. Е. Страус в [23] (для произвольного  $m$ ) сформулировали задачу о сложности вычисления одночлена от  $m$  переменных, т. е. нахождения величины  $l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m})$ . В дальнейшем эту задачу, следуя [21, 24], будем называть *задачей Беллмана*, хотя логичнее было бы её называть задачей Беллмана — Страуса. Формально на языке аддитивных цепочек величина  $l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m})$  определяется как минимально возможная длина  $r$  последовательности  $m$ -мерных векторов (наборов)

<sup>1)</sup> Здесь и далее  $\log x$  означает  $\log_2 x$ , а запись  $f(n) \sim g(n)$  означает, что при  $n \rightarrow \infty$  отношение  $f(n)/g(n)$  стремится к 1.

$$\mathbf{v}_1 = (1, 0, \dots, 0), \mathbf{v}_2 = (0, 1, \dots, 0), \dots, \mathbf{v}_q = (0, 0, \dots, 1),$$

$$\mathbf{v}_{q+1}, \mathbf{v}_{q+2}, \dots, \mathbf{v}_{q+r} = (n_1, n_2, \dots, n_m),$$

начинающейся с  $m$  единичных векторов и удовлетворяющей условию: для каждого  $k$ ,  $q+1 \leq k \leq q+r$ , найдётся два натуральных числа (не обязательно различных)  $i$  и  $j$ ,  $1 \leq i, j \leq q-1$ , таких, что  $\mathbf{v}_k = \mathbf{v}_i + \mathbf{v}_j$  (сложение векторов покомпонентное).

В 1969 г. Д. Кнут [2, разд. 4.6.3, упр. 32] поставил задачу о сложности вычисления  $m$  степеней одной переменной, т. е. нахождения величины  $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$ . Эту задачу обычно называют (см., например, [20]) *задачей Кнута*. Очевидно, что величина  $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$  численно равна минимально возможной длине аддитивной цепочки для какого-либо числа  $n_i$  (например, для максимального из чисел  $n_1, \dots, n_m$ ), содержащей при этом все остальные числа из множества  $\{n_1, \dots, n_m\}$ .

Е. Страус [23] показал, что

$$l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}) \sim \log(\max_i n_i)$$

для любого фиксированного  $m$  при  $\sum n_i \rightarrow \infty$ .

А. Яо [25] для любого фиксированного  $m$  при  $\sum n_i \rightarrow \infty$  установил аналогичную формулу для сложности вычисления набора из  $m$  степеней:

$$l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \sim \log(\max_i n_i).$$

Стоит также выделить результат Т. Соузарда [22], который установил асимптотику роста сложности вычисления набора степеней для одного частного случая, упоминавшегося Д. Кнутом при постановке общей задачи, когда набор показателей степеней является последовательностью квадратов идущих подряд натуральных чисел, начиная с единицы:

$$l(x^{1^2}, x^{2^2}, \dots, x^{m^2}) \sim m, \quad m \rightarrow \infty.$$

В 1981 г. независимо А. Ф. Сидоренко [12], Дж. Оливос [19], а также Д. Кнут и К. Пападимитриу [18] доказали, что в действительности задачи о сложности вычисления одночлена от  $m$  переменных и набора  $m$  степеней двойственны (эквивалентны) и связаны равенством

$$l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}) + 1 = l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) + m,$$

следовательно, достаточно исследовать одну из них. На самом деле задачи Беллмана и Кнута можно рассматривать как частные случаи более

общей задачи — задачи о сложности вычисления системы из  $p$  одночленов от  $q$  переменных (подробнее про эту задачу см., например, [8, 9, 21]), для которой установлено [12, 18], что сложность вычисления двух систем одночленов, показатели степеней которых задаются матрицами, получающимися друг из друга транспонированием, отличаются на величину  $p - q$ , где  $p$  и  $q$  — размеры матриц.

Также в 1981 г. в [15] установлено, что задача распознавания по набору натуральных чисел  $(n_1, n_2, \dots, n_m, l)$  существования аддитивной цепочки, имеющей длину  $l$  и содержащей числа  $n_1, n_2, \dots, n_m$ , является NP-полной. В связи с этим для задач Беллмана и Кнута говорить о нахождении точного значения сложности не приходится. Поэтому естественно рассматривать эти задачи в асимптотической постановке — в этом случае требуется предложить метод вычисления одночлена  $x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}$  или набора степеней  $x^{n_1}, x^{n_2}, \dots, x^{n_m}$  такой, что число используемых операций умножения в том или ином смысле близко к значению  $l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m})$  или  $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$  соответственно, например, такой метод, что отношение числа операций умножения к значению  $l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m})$  или  $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$  стремится к 1 при  $(n_1 + n_2 + \dots + n_m) \rightarrow \infty$  для всех или «почти всех» наборов  $(n_1, n_2, \dots, n_m)$ .

Как отмечено, при фиксированном  $m$  (числе переменных в одночлене или числе вычисляемых степеней соответственно) для задач Беллмана и Кнута асимптотически точное решение было найдено. Вопрос об асимптотике роста сложности в случае растущего числа переменных (степеней) долгое время оставался открытым. В этом направлении можно отметить, пожалуй, лишь результат Н. Пиппенджера [20] 1976 г.:

$$\max l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) = \log n + (1 + o(1)) \frac{m \log n}{\log(m \log n)} + O(m),$$

где максимум ищется по всем наборам  $(n_1, n_2, \dots, n_m)$ , каждая компонента которых не превосходит заданной величины  $n$ .

В 1992 г. С. Б. Гашковым и автором [1] на базе основного результата из [3] (см. также [4, 5]) установлены следующие верхние оценки сложности для задач Беллмана и Кнута.

**Утверждение 1** [1]. Для любой последовательности наборов натуральных чисел  $\tilde{n}(s) = (n_1(s), n_2(s), \dots, n_{m(s)}(s))$ ,  $s = 1, 2, \dots$ , удовлетво-

ряющей условию  $\sum_{i=1}^{m(s)} n_i(s) \rightarrow \infty$ , выполняются неравенства

$$l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \leq l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m})$$

$$\leq \log \max_{1 \leq i \leq m} n_i + \frac{\log N}{\log \log N} \left( 1 + O \left( \left( \frac{\log \log \log N}{\log \log N} \right)^{1/2} \right) \right) + O(m),$$

где  $N = n_1 n_2 \dots n_m$ .

Эти верхние оценки вместе с простыми нижними оценками (некоторое усиление которых сформулировано ниже в лемме 1)

$$l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}) \geq \log(\max_i n_i) + m - 1, \quad l(x_1^{n_1}, x_2^{n_2}, \dots, x_m^{n_m}) \geq \log(\max_i n_i),$$

справедливыми для всех наборов  $(n_1, n_2, \dots, n_m)$ , а также с «мощностной» нижней оценкой (см., например, [10]), дают асимптотику роста сложности в задачах Беллмана и Кнута для «почти всех» наборов при достаточно широком диапазоне соотношения параметров. Однако в случае, когда величины  $\log(\max_i n_i)$  и  $\frac{\log N}{\log \log N}$  имеют одинаковый порядок роста, эти нижние оценки асимптотически не совпадают с верхней.

В 1994 г. в [6] удалось восполнить этот пробел, в некотором смысле объединив в одну нижнюю оценку «мощностную» оценку и оценку через  $\log(\max_i n_i)$ .

Прежде чем дать точную формулировку этого результата, для произвольного набора  $\tilde{n} = (n_1, n_2, \dots, n_m)$  различных натуральных чисел через  $\sigma$  обозначим перестановку, упорядочивающую набор  $\tilde{n}$  по возрастанию:  $n_{\sigma(1)} < n_{\sigma(2)} < \dots < n_{\sigma(m)}$ , и положим

$$\mathfrak{M}(\tilde{n}) = \{ (k_1, k_2, \dots, k_m) \mid k_1 < k_2 < \dots < k_m, \\ k_i \in \mathbb{N}, \quad 1 \leq k_i \leq n_{\sigma(i)}, \quad i = 1, 2, \dots, m \}.$$

**Утверждение 2** [6]. Пусть последовательность наборов

$$\tilde{n}(s) = (n_1(s), n_2(s), \dots, n_m(s)), \quad s = 1, 2, \dots,$$

различных натуральных чисел такова, что  $N(s) = \prod_{i=1}^{m(s)} n_i(s) \rightarrow \infty$  при  $s \rightarrow \infty$ . Тогда существуют положительная константа  $c$  и функция  $f(x)$ , стремящаяся к 0 при  $x \rightarrow \infty$ , такие, что доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{M}(\tilde{n}(s))$ , удовлетворяющих соотношениям

$$l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \geq l(x^{k_1}, x^{k_2}, \dots, x^{k_m}) \\ \geq \left( \log \max_i n_i + \frac{\log N}{\log \log N} \right) - \left( f(N) \frac{\log N}{\log \log N} + cm \right),$$

стремится к единице при  $s \rightarrow \infty$ .

**Замечание 1.** В формулировке утверждения 2 можно положить

$$f(x) = \frac{2}{(\log \log x)^{1/2}}.$$

**Замечание 2.** Утверждение 2 остаётся справедливым, если рассматривать доли наборов не из множества  $\mathfrak{M}(\tilde{n}(s))$ , а из множества  $\mathfrak{N}(\tilde{n}(s))$ , где  $\mathfrak{N}(\tilde{n}) = \{(k_1, k_2, \dots, k_m) \mid k_i \in \mathbb{N}, 1 \leq k_i \leq n_i, i = 1, 2, \dots, m\}$ . Такой подход является более логичным при изучении задачи Беллмана. Отличия в подходах связаны с соображениями следующего толка: при вычислениях одночлены  $x_1^{n_1} x_2^{n_2}$  и  $x_1^{n_2} x_2^{n_1}$  естественно считать разными, а наборы степеней  $(x^{n_1}, x^{n_2})$  и  $(x^{n_2}, x^{n_1})$  — одинаковыми. Стоит отметить, что в изначальной формулировке результат в некотором смысле является более тонким.

Содержательно из утверждений 1 и 2 следует, что при выполнении дополнительного условия

$$m = o\left(\log(\max_i n_i) + \frac{\log N}{\log \log N}\right)$$

для любого  $\varepsilon > 0$  доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{M}(\tilde{n}(s))$  (или из  $\mathfrak{N}(\tilde{n})$ ), удовлетворяющих соотношениям

$$\begin{aligned} (1 - \varepsilon) \log(\max_i n_i) + \frac{\log N}{\log \log N} &\leq l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \\ &\leq (1 + \varepsilon) \log(\max_i n_i) + \frac{\log N}{\log \log N}, \end{aligned}$$

$$\begin{aligned} (1 - \varepsilon) \log(\max_i n_i) + \frac{\log N}{\log \log N} &\leq l(x^{k_1}, x^{k_2}, \dots, x^{k_m}) \\ &\leq (1 + \varepsilon) \log(\max_i n_i) + \frac{\log N}{\log \log N}, \end{aligned}$$

стремится к единице, или, короче, при указанном условии для почти всех наборов из  $\mathfrak{M}(\tilde{n})$  (или из  $\mathfrak{N}(\tilde{n})$ ) справедливы асимптотические равенства

$$\begin{aligned} l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) &\sim \log(\max_i n_i) + \frac{\log N}{\log \log N}, \\ l(x^{k_1}, x^{k_2}, \dots, x^{k_m}) &\sim \log(\max_i n_i) + \frac{\log N}{\log \log N}, \end{aligned}$$

из которых в силу справедливости для всех наборов утверждения 1 следует и выполнение для почти всех наборов соотношений

$$l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \sim l(x^{k_1}, x^{k_2}, \dots, x^{k_m}) \sim \log(\max_i k_i) + \frac{\log K}{\log \log K},$$

где  $K = k_1 k_2 \dots k_m$ .

Таким образом в [1, 6] получено асимптотически точное решение задач Беллмана и Кнута. Действительно, при стандартном условии, что сложность (число операций) существенно больше числа полюсов (суммы «входов» и «выходов» — в данном случае  $m + 1$ ), для почти всех исследуемых объектов (наборов) верхняя оценка асимптотически совпадает с нижней.

В данной работе уточняются оценки сложности в задачах Беллмана и Кнута в случае, когда количество переменных в одночлене или соответственно количество вычисляемых степеней сравнимо со сложностью (имеют одинаковый порядок роста). Отметим, что в этом случае отличие оценок сложности для задач Беллмана и Кнута на величину  $m - 1$  становится существенным. Часть предложенных здесь результатов анонсирована ещё в [7].

Обозначим через  $\{x\}$  дробную часть числа  $x$ .

**Теорема 1.** Пусть числовая функция  $f(x)$  при  $x \rightarrow \infty$  удовлетворяет условиям  $f(x) \rightarrow \infty$ ,  $\log f(x) = o(\log x)$ . Тогда для любой последовательности наборов натуральных чисел  $\tilde{n}(s) = (n_1(s), n_2(s), \dots, n_{m(s)}(s))$ ,  $s = 1, 2, \dots$ , удовлетворяющей условию  $\sum_{i=1}^{m(s)} n_i(s) \rightarrow \infty$ , выполняются неравенства

$$\begin{aligned} l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}) &\leq \log(\max_i n_i)(1 + o(1)) + \frac{\log N}{\log \log N}(1 + o(1)) \\ &\quad + \sum_{i=1}^m \frac{\log n_i}{\log m - 2 \log f(m)}, \\ l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) &\leq \log(\max_i n_i)(1 + o(1)) + \frac{\log N}{\log \log N}(1 + o(1)) \\ &\quad + \sum_{i=1}^m \frac{\log n_i}{\log m - 2 \log f(m)} - m, \end{aligned}$$

где  $N = n_1 n_2 \dots n_m$ .

**ДОКАЗАТЕЛЬСТВО.** Возможны два случая:  $\log N \geq m \log m f(m)$  и  $\log N < m \log m f(m)$ .

СЛУЧАЙ 1. Пусть выполняется неравенство  $\log N \geq m \log mf(m)$ . Тогда  $m = o\left(\frac{\log N}{\log \log N}\right)$ . Применяя утверждение 1 и используя это соотношение, получаем

$$\begin{aligned} l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) &\leq l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}) \leq \log(\max_i n_i)(1 + o(1)) \\ &+ \frac{\log N}{\log \log N}(1 + o(1)) + O(m) \sim \log(\max_i n_i) + \frac{\log N}{\log \log N}. \end{aligned}$$

Требуемая верхняя оценка в этом случае доказана.

СЛУЧАЙ 2. Пусть выполняется неравенство  $\log N < m \log mf(m)$ . В этом случае будем доказывать нужную оценку для задачи Кнута. Без ограничения общности можно считать, что все  $n_i$  различны. Тогда  $\log N \geq \log(m!) \sim m \log m$ . С учётом того, что  $\log f(m) = o(\log m)$ , имеем  $\log \log N \sim \log m$ . Из последних двух соотношений следует неравенство

$$m \leq \frac{\log N}{\log \log N}(1 + o(1)).$$

Положим  $I_1 = \{i \mid n_i < m^{f(m)}\}$ ,  $I_2 = \{i \mid n_i \geq m^{f(m)}\}$ . Отдельно оценим сверху сложность вычисления наборов степеней  $\{x^{n_i} \mid i \in I_1\}$  и  $\{x^{n_i} \mid i \in I_2\}$ .

Для получения набора степеней  $\{x^{n_i} \mid i \in I_1\}$  сначала последовательно реализуем  $d$  групп ( $d = \lceil f(m) \rceil + 1$ ) степеней:

1-я группа:  $x^a$ ,  $a = 1, 2, \dots, \lceil \frac{m}{(f(m))^2} \rceil$ ;

2-я группа:  $x^{a(\lceil \frac{m}{(f(m))^2} \rceil)}$ ,  $a = 1, 2, \dots, \lceil \frac{m}{(f(m))^2} \rceil$ ;

...

$d$ -я группа:  $x^{a(\lceil \frac{m}{(f(m))^2} \rceil)^{d-1}}$ ,  $a = 1, 2, \dots, \lceil \frac{m}{(f(m))^2} \rceil$ .

Очевидно, что для вычисления этих степеней требуется  $O(m/f(m))$  умножений.

Отметим, что в силу соотношений

$$d \log \left( \left\lceil \frac{m}{(f(m))^2} \right\rceil \right) \geq (\lceil f(m) \rceil + 1) (\log m - 2 \log f(m)) \geq f(m) \log m$$

справедливо неравенство  $m^{f(m)} \leq \left( \left\lceil \frac{m}{(f(m))^2} \right\rceil \right)^d$ , из которого, в свою очередь, следует, что любую степень  $x^{n_i}$ ,  $i \in I_1$ , можно получить, используя вычисленные  $d$  групп степеней, затратив не более  $\lceil \log_{(m/(f(m))^2)} n_i \rceil - 1$  умножений.

Таким образом величину  $l(\{x^{n_i} \mid i \in I_1\})$  можно оценить так:

$$l(\{x^{n_i} \mid i \in I_1\}) \leq O(m/f(m)) + \sum_{i \in I_1} (\lceil \log_{(m/(f(m))^2)} n_i \rceil - 1)$$



$$\begin{aligned}
&= o\left(\frac{\log N}{\log \log N}\right) + \sum_{i \in I_1} \frac{\log n_i}{\log(m/(f(m))^2)} \\
&+ \sum_{i \in I_1} (\lceil \log_{(m/(f(m))^2)} n_i \rceil - 1 - \log_{(m/(f(m))^2)} n_i) = \frac{\log \prod_{i \in I_1} n_i}{\log m} (1 + o(1)) \\
&+ \sum_{i=1}^m (\lceil \log_{(m/(f(m))^2)} n_i \rceil - \log_{(m/(f(m))^2)} n_i) - m + O(|I_2|) + o\left(\frac{\log N}{\log \log N}\right).
\end{aligned}$$

Перейдём к оценке величины  $l(\{x^{n_i} \mid i \in I_2\})$  (а также оценим величину  $|I_2|$ ). Используя утверждение 1, получаем

$$l(\{x^{n_i} \mid i \in I_2\}) \leq \log(\max_{i \in I_2} n_i)(1 + o(1)) + \frac{\log \prod_{i \in I_2} n_i}{\log \log \prod_{i \in I_2} n_i} (1 + o(1)) + O(|I_2|).$$

Оценим сверху величину  $|I_2|$ . Из неравенств  $N \geq \prod_{i \in I_2} n_i \geq (m^{f(m)})^{|I_2|}$  следует, что

$$|I_2| \leq \frac{\log N}{f(m) \log m} \sim \frac{1}{f(m)} \frac{\log N}{\log \log N} = o\left(\frac{\log N}{\log \log N}\right).$$

Таким образом,

$$\begin{aligned}
l(\{x^{n_i} \mid i \in I_2\}) &\leq \log(\max_i n_i)(1 + o(1)) + \frac{\log \prod_{i \in I_2} n_i}{\log \log \prod_{i \in I_2} n_i} (1 + o(1)) \\
&+ o\left(\frac{\log N}{\log \log N}\right).
\end{aligned}$$

Далее, объединяя оценки для  $l(\{x^{n_i} \mid i \in I_1\})$  и  $l(\{x^{n_i} \mid i \in I_2\})$ , получаем

$$\begin{aligned}
l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) &\leq \log(\max_i n_i)(1 + o(1)) + \frac{\log \prod_{i \in I_1} n_i}{\log m} (1 + o(1)) \\
&+ \frac{\log \prod_{i \in I_2} n_i}{\log \log \prod_{i \in I_2} n_i} (1 + o(1)) + \sum_{i=1}^m (\lceil \log_{(m/(f(m))^2)} n_i \rceil - \log_{(m/(f(m))^2)} n_i)
\end{aligned}$$

$$-m + o\left(\frac{\log N}{\log \log N}\right).$$

Отметим, что если  $\log \prod_{i \in I_2} n_i \geq \frac{\log N}{(\log \log N)^2}$ , то справедливы соотношения  $\log \log \prod_{i \in I_2} n_i \geq \log \log N - 2 \log \log \log N \sim \log \log N \sim f(m)$ , следовательно,

$$\frac{\log \prod_{i \in I_2} n_i}{\log \log \prod_{i \in I_2} n_i} \leq \frac{\log \log N}{\log m} (1 + o(1)).$$

Если  $\log \prod_{i \in I_2} n_i < \frac{\log N}{(\log \log N)^2}$ , то очевидно, что

$$\frac{\log \prod_{i \in I_2} n_i}{\log \log \prod_{i \in I_2} n_i} = o\left(\frac{\log N}{\log \log N}\right) = o\left(\frac{\log N}{\log m}\right).$$

Таким образом, в обоих случаях имеем

$$\begin{aligned} \frac{\log \prod_{i \in I_1} n_i}{\log m} (1 + o(1)) + \frac{\log \prod_{i \in I_2} n_i}{\log \log \prod_{i \in I_2} n_i} (1 + o(1)) \\ \leq \frac{\log N}{\log m} (1 + o(1)) = \frac{\log N}{\log \log N} (1 + o(1)). \end{aligned}$$

Поэтому

$$\begin{aligned} l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \leq \log(\max_i n_i) (1 + o(1)) + \frac{\log N}{\log \log N} (1 + o(1)) \\ + \sum_{i=1}^m (\lceil \log_{(m/(f(m))^2)} n_i \rceil - \log_{(m/(f(m))^2)} n_i) - m. \end{aligned}$$

Для завершения доказательства верхней оценки осталось использовать равенство

$$l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}) + 1 = l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) + m.$$

Теорема 1 доказана.

**Следствие.** Для любой последовательности наборов натуральных чисел  $\tilde{n}(s) = (n_1(s), n_2(s), \dots, n_{m(s)}(s))$ ,  $s = 1, 2, \dots$ , такой, что

$$\sum_{i=1}^{m(s)} n_i(s) \rightarrow \infty,$$

выполняются неравенства

$$l(x_1^{n_1} x_2^{n_2} \dots, x_m^{n_m}) \leq \log(\max_i n_i)(1 + o(1)) + \frac{\log N}{\log \log N}(1 + o(1)) + m,$$

$$l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \leq \log(\max_i n_i)(1 + o(1)) + \frac{\log N}{\log \log N}(1 + o(1)).$$

Для получения этого следствия из теоремы 1 достаточно оценить сверху единицей каждую дробную часть.

Теперь на элементарном примере проиллюстрируем, во-первых, различия в формулировке самой теоремы 1 и следствия из неё, а во-вторых, метод доказательства теоремы 1.

Исследуем асимптотический рост при  $m \rightarrow \infty$  величины  $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$  в случае, когда на показатели степеней наложены следующие ограничения: все степени  $n_i$  различны и ограничены сверху величиной  $m^2 / \log \log m$ .

В силу наложенных ограничений выполняются соотношения

$$\log \max_i n_i = o(m), \quad \log N \leq 2m \log m, \quad \frac{\log N}{\log \log N} \leq 2m.$$

Поэтому, применяя следствие, получаем оценку  $l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \leq 2m + o(m)$ .

С другой стороны, положив  $f(x) = (\log \log m)^{1/2}$  в теореме 1, получаем оценку  $l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \leq m + o(m)$ , которая в силу того очевидного факта, что на каждую степень надо использовать хотя бы одну операцию умножения, асимптотически неупрощаема.

Метод доказательства оценки из теоремы 1 в данном примере может быть проинтерпретирован следующим образом. Заметим, что каждое из чисел  $n_i$  является не более чем двухразрядным в системе счисления с основанием  $\lceil m/(\log \log m)^{1/2} \rceil$ . Сначала вычислим все степени с показателями, имеющими одноразрядную запись по этому основанию, а затем — все степени с показателями, имеющими двухразрядную запись с нулём в младшем разряде. На это потребуется  $O(m/(\log \log m)^{1/2})$  операций умножения. После этого для вычисления каждой степени  $x^{n_i}$ ,  $i = 1, 2, \dots, m$ , потребуется не более одной операции умножения.

Переходя к уточнению нижних оценок, начнём с простейших из них.

**Лемма 1.** Если все степени  $n_i$ ,  $i = 1, \dots, m$ , различны и не равны 0, то справедливы неравенства

$$l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}) \geq \max(\log(\max_i n_i), m-1) + m-1,$$

$$l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \geq \max(\log(\max_i n_i), m-1).$$

**Доказательство.** В силу того, что с помощью  $k$  операций умножения степень с показателем, бóльшим  $2^k$ , получить невозможно (этот факт легко устанавливается индукцией по  $k$ ), справедливо неравенство  $l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \geq \log \max_i n_i$ , которое вместе с очевидным соотношением  $l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \geq m-1$  даёт второе неравенство леммы. Первое неравенство леммы следует из второго и двойственности задач Беллмана и Кнута. Лемма 1 доказана.

Теперь аккуратно сформулируем нижнюю оценку обычного шенноновского типа, получающуюся из мощностных соображений.

**Лемма 2.** Пусть последовательность наборов

$$\tilde{n}(s) = (n_1(s), n_2(s), \dots, n_{m(s)}(s)), \quad s = 1, 2, \dots,$$

удовлетворяет условию  $N(\tilde{n}(s)) = N(s) = \prod_{i=1}^{m(s)} n_i(s) \rightarrow \infty$  при  $s \rightarrow \infty$ .

Тогда для любого  $\varepsilon > 0$  доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$ , удовлетворяющих соотношению

$$l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \geq \frac{\log N}{\log \log N} \left( 1 + (1 - \varepsilon) \frac{\log \log \log N}{\log \log N} \right),$$

стремится к единице при  $s \rightarrow \infty$ .

Заметим, что величина  $l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m})$  численно равна минимальной сложности (определяемой как число элементов) схем из функциональных элементов (определения см., например, в [10, 11]), обладающих следующими свойствами: (i) на входы схемы подаются переменные  $x_1, x_2, \dots, x_m$ ; (ii) все функциональные элементы схемы являются двухвходовыми и каждый из них вычисляет произведение поступающих на его входы функций (одночленов); (iii) на выходе схемы вычисляется одночлен  $x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}$ . Теперь для доказательства леммы 2 достаточно сослаться, скажем, на [11, § Д.3, § Д.4].

В силу двойственности задач Беллмана и Кнута из леммы 2 вытекает

**Следствие.** Пусть последовательность наборов

$$\tilde{n}(s) = (n_1(s), n_2(s), \dots, n_{m(s)}(s)), \quad s = 1, 2, \dots,$$

удовлетворяет условию  $N(\tilde{n}(s)) = N(s) = \prod_{i=1}^{m(s)} n_i(s) \rightarrow \infty$  при  $s \rightarrow \infty$ .

Тогда для любого  $\varepsilon > 0$  доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$ , удовлетворяющих соотношению

$$l(x^{k_1}, x^{k_2}, \dots, x^{k_m}) \geq \frac{\log N}{\log \log N} \left( 1 + (1 - \varepsilon) \frac{\log \log \log N}{\log \log N} \right) - m,$$

стремится к единице при  $s \rightarrow \infty$ .

Отметим, что пример, иллюстрирующий метод доказательства теоремы 1, показывает, что избавиться от вычитания величины  $m$  в оценке из этого следствия, вообще говоря, нельзя.

Далее для сокращения записи будем выписывать оценки только для задачи Беллмана (оценки для задачи Кнута автоматически выписываются из соотношения двойственности). Кроме того, будем считать, что все степени  $n_i$ ,  $i = 1, \dots, m$ , различны и отличны от нуля, так как если  $\{n_1, n_2, \dots, n_m\} = \{r_1, r_2, \dots, r_s\}$  и все числа  $r_i$ ,  $i = 1, \dots, s$ , различны и отличны от нуля, то, очевидно,

$$l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}) = l(x_1^{r_1} x_2^{r_2} \dots x_s^{r_s}) + m - s.$$

Поэтому далее без ограничения общности считаем, что  $1 \leq n_1 < n_2 < \dots < n_m$ .

Положим

$$V(n_1, n_2, \dots, n_m) = \log \max_i n_i + \frac{\log N}{\log \log N} + m,$$

где по-прежнему  $N = n_1 n_2 \dots n_m$ .

При выполнении условия  $m = o\left(\log \max_i n_i + \frac{\log N}{\log \log N}\right)$ , как отмечалось, для почти всех наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{M}(\tilde{n})$  (или из  $\mathfrak{N}(\tilde{n})$ ) верны асимптотические равенства

$$l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \sim V(k_1, k_2, \dots, k_m) \sim V(n_1, n_2, \dots, n_m).$$

При выполнении условия  $\frac{\log N}{\log \log N} = o(\log \max_i n_i + m)$  в силу теоремы 1 и леммы 1

$$l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \sim \log \max_i n_i + m \sim V(n_1, n_2, \dots, n_m).$$

В общем случае из теоремы 1 и леммы 1 с учётом очевидного неравенства

$$\max \left\{ \log \max_i n_i + m, \frac{\log N}{\log \log N} \right\} \geq \frac{1}{2} \left( \log \max_i n_i + \frac{\log N}{\log \log N} + m \right)$$

следует, что для почти всех наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{M}(\tilde{n})$  выполняются асимптотические соотношения

$$\frac{1}{2} V(n_1, n_2, \dots, n_m) \lesssim l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \lesssim V(n_1, n_2, \dots, n_m).$$

**Теорема 2.** Пусть последовательность наборов

$$\tilde{n}(s) = (n_1(s), n_2(s), \dots, n_{m(s)}(s)), \quad s = 1, 2, \dots,$$

различных натуральных чисел такова, что  $N(s) = \prod_{i=1}^{m(s)} n_i(s) \rightarrow \infty$  при  $s \rightarrow \infty$ . Тогда для любого  $\varepsilon > 0$  доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$ , удовлетворяющих неравенствам

$$\left( \frac{3}{5} - \varepsilon \right) V(n_1, n_2, \dots, n_m) \leq l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \leq (1 + \varepsilon) V(n_1, n_2, \dots, n_m),$$

стремится к единице при  $s \rightarrow \infty$ .

**Доказательство.** Справедливость верхней оценки при всех достаточно больших номерах  $s$  для всех наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$  непосредственно вытекает из следствия к теореме 1.

При доказательстве нижней оценки без ограничения общности будем считать, что выполняются неравенства

$$n_1 < n_2 < \dots < n_m.$$

Пусть  $g(x) = \log \log x$ . При каждом  $s = 1, 2, \dots$  разобьём множество индексов переменных на два множества  $J_1(s)$  и  $J_2(s)$  следующим образом (аргумент  $s$  в скобках будем, как правило, опускать):

$$J_1 = \{i \mid n_i < m^{g(m)}\}, \quad |J_1| = m_1; \quad J_2 = \{i \mid n_i \geq m^{g(m)}\}, \quad |J_2| = m_2.$$

В соответствии с этим разбиением разобьём и набор  $\tilde{n}$  на два поднабора:  $\tilde{n}_1 = (n_1, n_2, \dots, n_{m_1})$  и  $\tilde{n}_2 = (n_{m_1+1}, n_{m_1+2}, \dots, n_m)$ . Далее положим

$$H_1 = \frac{\log \prod_{i \in J_1} n_i}{\log \log \prod_{i \in J_1} n_i}, \quad H_2 = \frac{\log \prod_{i \in J_2} n_i}{\log \log \prod_{i \in J_2} n_i}, \quad H = \frac{\log \prod_{i \in J_1 \cup J_2} n_i}{\log \log \prod_{i \in J_1 \cup J_2} n_i}$$

(здесь и далее под функцией  $\log \log x$  понимаем функцию, переопределённую или доопределённую таким образом, что при  $1 \leq x < 4$  она равна единице). При выполнении условия  $m_i = 0$  ( $i = 1$  или  $i = 2$ ) полагаем  $H_i = 0$ .

Очевидно, что  $m_1 + m_2 = m$ . Кроме того, справедливо асимптотическое равенство  $H_1 + H_2 \sim H$ . Действительно, неравенство  $H_1 + H_2 \geq H$  очевидно, а соотношение  $H_1 + H_2 = H + o(H)$ , по существу, установлено в ходе доказательства теоремы 1. Отметим, что последовательность, получающаяся из последовательности  $H_2(s)$ ,  $s = 1, 2, \dots$ , путём вычеркивания всех нулевых членов, либо конечна, либо стремится к бесконечности.

Теперь отдельно сформулируем четыре нижние оценки.

ОЦЕНКА 1. Доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$ , удовлетворяющих неравенству

$$l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \geq H,$$

стремится к единице при  $s \rightarrow \infty$ .

Это утверждение непосредственно следует из леммы 2.

ОЦЕНКА 2. Для любого  $\varepsilon > 0$  доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$ , удовлетворяющих неравенству

$$l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \geq (1 - \varepsilon)H_1 + \log \max_i n_i - 2g(m) \log m,$$

стремится к единице при  $s \rightarrow \infty$ .

ДОКАЗАТЕЛЬСТВО. Если выполняется условие  $H_1 \leq m - 1$ , то оно непосредственно следует из леммы 1.

Пусть выполняется условие  $H_1 > m - 1$ . Если при этом справедливо неравенство  $m \leq H/(\log H)$ , то доказываемая оценка непосредственно следует из утверждения 2. Поэтому без ограничения общности можно считать, что  $H_1 \rightarrow \infty$  при  $s \rightarrow \infty$ . Каждому набору  $\tilde{k} = (k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$  сопоставим какую-либо минимальную схему  $S_{\tilde{k}}$  из элементов умножения, вычисляющую одночлен  $x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}$ . Перестроим схему  $S_{\tilde{k}}$  в схему  $S_{\tilde{k}}^1$  следующим образом. Сначала подадим вместо переменных  $x_{m_1+1}, x_{m_2+1}, \dots, x_m$  единицу, а затем удалим все элементы умножения, хотя бы на один вход которых подаётся единица (при этом на те элементы, на входы которых подавался выход удалённого элемента, подадим одночлен, подаваемый на другой вход удаляемого элемента).

Очевидно, что, во-первых,  $S_{\tilde{k}}^1$  вычисляет одночлен  $x_1^{k_1} x_2^{k_2} \dots x_{m_1}^{k_{m_1}}$ , во-вторых, на входы схемы подаются только переменные  $x_1, x_1, \dots, x_{m_1}$ ,

в-третьих, степень любой переменной одночлена, вычисляемого в произвольной вершине (произвольным элементом) схемы  $S_k^1$ , не превосходит величины  $m^{g(m)}$ .

Отметим, что добавление к схеме одного элемента умножения (и, возможно, нового входа) может увеличить максимум показателей степеней среди всех переменных всех вычисляемых элементами схемы одночленов не более чем в 2 раза. Поэтому, обозначая через  $l(S)$  число элементов (умножения) в схеме  $S$ , имеем

$$l(S_k^1) - l(S_k^1) \geq \log \max(k_{m_1+1}, k_{m_1+2}, \dots, k_m) - g(m) \log m.$$

Таким образом для любого  $\varepsilon > 0$ , с одной стороны, доля наборов  $(k_1, k_2, \dots, k_{m_1})$  из  $\mathfrak{N}(\widetilde{n}_1(s))$ , удовлетворяющих неравенству

$$l(x_1^{k_1} x_2^{k_2} \dots x_{m_1}^{k_{m_1}}) \geq (1 - \varepsilon) H_1,$$

стремится к единице при  $s \rightarrow \infty$ , а с другой стороны, при условии  $H_2(s) \neq 0$  доля наборов  $(k_{m_1+1}, k_{m_1+2}, \dots, k_m)$  из  $\mathfrak{N}(\widetilde{n}_2(s))$ , удовлетворяющих неравенству

$$\log \max(k_{m_1+1}, k_{m_1+2}, \dots, k_m) - g(m) \log m \geq \log n_m - 2g(m) \log m,$$

стремится (в случае бесконечности ненулевых элементов в последовательности  $H_2(s)$ ) к единице при  $s \rightarrow \infty$ .

Следовательно, в любом случае для любого  $\varepsilon > 0$  доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\widetilde{n}(s))$ , удовлетворяющих неравенству

$$l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \geq (1 - \varepsilon) H_1 + \log \max_i n_i - 2g(m) \log m,$$

стремится к единице при  $s \rightarrow \infty$ . Оценка 2 доказана.

**ОЦЕНКА 3.** Для любого  $\varepsilon > 0$  доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\widetilde{n}(s))$ , удовлетворяющих неравенству

$$l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \geq \left(\frac{3}{2} - \varepsilon\right) m_1 + \log \max_i n_i - 2g(m) \log m,$$

стремится к единице при  $s \rightarrow \infty$ .

**ДОКАЗАТЕЛЬСТВО.** Если  $m_1(s) \leq m(s)/(\log m(s))$ , то требуемая оценка следует из леммы 1. Если выполняется условие  $m(s) \leq H/(\log H)$ , то оценка 3 вытекает из замечания 2 к утверждению 2. Поэтому далее считаем, что  $m_1(s) > m(s)/(\log m(s))$  и  $m(s) > H/(\log H)$ . Отметим, что тогда  $m_1(s) \rightarrow \infty$ .



Нетрудно показать, что для любого  $\varepsilon > 0$  доля наборов  $(k_1, k_2, \dots, k_{m_1})$  из  $\mathfrak{N}(\tilde{n}_1(s))$ , удовлетворяющих неравенству

$$|\{k_1, k_2, \dots, k_{m_1}\}| \geq \left(\frac{1}{2} - \varepsilon\right) m_1,$$

стремится к единице при  $s \rightarrow \infty$ , следовательно, доля наборов, удовлетворяющих неравенству

$$l(x_1^{k_1} x_2^{k_2} \dots x_{m_1}^{k_{m_1}}) \geq \left(\frac{3}{2} - \varepsilon\right) m_1,$$

также стремится к единице.

Если  $n_m \leq m^{g(m)}$ , то для почти всех наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$  справедливы соотношения

$$\begin{aligned} l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) &\geq l(x_1^{k_1} x_2^{k_2} \dots x_{m_1}^{k_{m_1}}) \geq \left(\frac{3}{2} - \varepsilon\right) m_1 \\ &\geq \left(\frac{3}{2} - \varepsilon\right) m_1 + \log n_m - g(m) \log m. \end{aligned}$$

Пусть  $n_m > m^{g(m)}$ . В этом случае так же, как и при доказательстве оценки 2, каждому набору  $\tilde{k} = (k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$  сопоставим какую-либо минимальную схему  $S_{\tilde{k}}$ , вычисляющую одночлен  $x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}$ , и аналогичным образом перестроим схему  $S_{\tilde{k}}$  в схему  $S_{\tilde{k}}^1$ . Тогда

$$\begin{aligned} l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) &= l(S_{\tilde{k}}^1) + l(S_{\tilde{k}}) - l(S_{\tilde{k}}^1) \\ &\geq l(x_1^{k_1} x_2^{k_2} \dots x_{m_1}^{k_{m_1}}) + \log \max_{m_1+1 \leq i \leq m} k_i - g(m) \log m. \end{aligned}$$

Поэтому доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$ , удовлетворяющих неравенству

$$l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \geq \left(\frac{3}{2} - \varepsilon\right) m_1 + \log \max_i n_i - 2g(m) \log m,$$

стремится к единице при  $s \rightarrow \infty$ . Оценка 3 доказана.

**ОЦЕНКА 4.** Для любого  $\varepsilon > 0$  доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$ , удовлетворяющих неравенству

$$l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \geq H_2 + \log \max_i n_i + m_1 - \varepsilon H,$$

стремится к единице при  $s \rightarrow \infty$ .

ДОКАЗАТЕЛЬСТВО. Каждому набору  $\tilde{k} = (k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$  сопоставим какую-либо минимальную схему  $S_{\tilde{k}}$  из элементов умножения, вычисляющую одночлен  $x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}$ . Перестроим схему  $S_{\tilde{k}}$  в схему  $S_{\tilde{k}}^2$  следующим образом. Сначала подадим единицу вместо переменных  $x_1, x_2, \dots, x_{m_1}$ , а затем удалим все элементы умножения, хотя бы на один вход которых подаётся единица (при этом на те элементы, на входы которых подавался выход удалённого элемента, подадим одночлен, подаваемый на другой вход удаляемого элемента).

Очевидно, что схема  $S_{\tilde{k}}^2$  вычисляет одночлен  $x_{m_1+1}^{k_{m_1+1}} x_{m_1+2}^{k_{m_1+2}} \dots x_m^{k_m}$ . В силу замечания 2 к утверждению 2 и неравенства  $l(S_{\tilde{k}}) - l(S_{\tilde{k}}^2) \geq m_1$  справедлив следующий факт: для некоторой положительной константы  $c$  доля наборов  $\tilde{k} = (k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$ , удовлетворяющих неравенству

$$l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \geq (1 - \varepsilon/2)H_2 + \log \max_i n_i - cm_2 + m_1,$$

стремится к единице при  $s \rightarrow \infty$ . Далее, в силу справедливости соотношения  $(m^{g(m)})^{m_2} \leq N$  имеем

$$m_2 \leq \frac{\log N}{g(m) \log m}.$$

Отсюда если  $\log m > \log \log N - 2 \log \log \log N$ , то

$$m_2 \leq \frac{2 \log N}{g(m) \log \log N}$$

при достаточно больших значениях  $N$ , а в противном случае

$$m_2 \leq m \leq 2^{\log \log N - \log \log \log N} = \frac{\log N}{(\log \log N)^2}.$$

Таким образом,  $cm_2 \leq \frac{\varepsilon}{2}H$  при всех достаточно больших значениях  $N$ . Оценка 4 доказана.

Прежде чем непосредственно перейти к завершению доказательства теоремы 2, на базе оценок 2 и 3 получим ещё одну оценку.

ОЦЕНКА 5. Для любого  $\varepsilon > 0$  доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$ , удовлетворяющих неравенству

$$l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \geq \left(\frac{1}{2} - \varepsilon\right) H_1 + (1 - \varepsilon) m_1 + \log \max_i n_i - 2g(m) \log m,$$

стремится к единице при  $s \rightarrow \infty$ .

ДОКАЗАТЕЛЬСТВО. Если  $H_1 \leq (1 + \delta)m_1$ , то, применяя оценку 3, получаем, что для почти всех наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$  справедливы соотношения

$$\begin{aligned} l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) &\geq \left(\frac{3}{2} - \varepsilon\right) m_1 + \log \max_i n_i - 2g(m) \log m \\ &\geq \frac{H_1}{2(1 + \delta)} + (1 - \varepsilon) m_1 + \log \max_i n_i - 2g(m) \log m \\ &\geq \left(\frac{1}{2} - \frac{\delta}{2}\right) H_1 + (1 - \varepsilon) m_1 + \log \max_i n_i - 2g(m) \log m. \end{aligned}$$

Если  $H_1 > (1 + \delta)m_1$ , то справедливы соотношения  $(1 + \delta)m_1 \log m_1 < H_1 \log m_1 \leq \log N_1$ , следовательно,  $N_1 \geq (m_1^{1+\delta})^{m_1}$ . Тогда для любого  $\varepsilon > 0$  доля наборов  $(k_1, k_2, \dots, k_{m_1})$  из  $\mathfrak{N}(\tilde{n}_1(s))$ , удовлетворяющих неравенству

$$|\{k_1, k_2, \dots, k_{m_1}\}| \geq (1 - \varepsilon) m_1,$$

стремится к единице при  $s \rightarrow \infty$ , стало быть, доля наборов, удовлетворяющих неравенству

$$l(x_1^{k_1} x_2^{k_2} \dots x_{m_1}^{k_{m_1}}) \geq (2 - \varepsilon) m_1,$$

также стремится к единице.

Повторяя доказательство оценки 3, получаем, что доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$ , удовлетворяющих неравенству

$$l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \geq (2 - \varepsilon) m_1 + \log \max_i n_i - 2g(m) \log m,$$

стремится к единице при  $s \rightarrow \infty$ .

Используя эту оценку и оценку 2, получаем, что для почти всех наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$  выполняются соотношения

$$\begin{aligned} l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) &\geq \frac{1}{2}((2 - \varepsilon)m_1 + \log \max_i n_i - 2g(m) \log m + (1 - \varepsilon)H_1 \\ &\quad + \log \max_i n_i - 2g(m) \log m) = \left(\frac{1}{2} - \frac{\varepsilon}{2}\right) H_1 \\ &\quad + \left(1 - \frac{\varepsilon}{2}\right) m_1 + \log \max_i n_i - 2g(m) \log m. \end{aligned}$$

Оценка 5 доказана.

Наконец, используя оценки 1, 4 и 5, получаем, что доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{N}(\tilde{n}(s))$ , для которых справедлива цепочка соотношений

$$\begin{aligned} l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) &\geq \max \left\{ H, H_2 + \log \max_i n_i + m_1 - \varepsilon H, \right. \\ &\quad \left( \frac{1}{2} - \varepsilon \right) H_1 + (1 - \varepsilon) m_1 + \log \max_i n_i - 2g(m) \log m \left. \right\} \\ &\geq \frac{2}{5} H + \frac{1}{5} (H_2 + \log \max_i n_i + m_1 - \varepsilon H) \\ &\quad + \frac{2}{5} \left( \left( \frac{1}{2} - \varepsilon \right) H_1 + (1 - \varepsilon) m_1 + \log \max_i n_i - 2g(m) \log m \right) \\ &\geq \left( \frac{3}{5} - \varepsilon \right) (H + \log n_m + m) = \left( \frac{3}{5} - \varepsilon \right) V(n_1, n_2, \dots, n_m), \end{aligned}$$

стремится к единице при  $s \rightarrow \infty$ . Теорема 2 доказана.

**Следствие.** Пусть последовательность наборов

$$\tilde{n}(s) = (n_1(s), n_2(s), \dots, n_{m(s)}(s)t), \quad s = 1, 2, \dots,$$

различных натуральных чисел такова, что  $N(s) = \prod_{i=1}^{m(s)} n_i(s) \rightarrow \infty$  при  $s \rightarrow \infty$ . Тогда для любого  $\varepsilon > 0$  доля наборов  $(k_1, k_2, \dots, k_m)$  из  $\mathfrak{M}(\tilde{n}(s))$ , удовлетворяющих неравенствам

$$\left( \frac{3}{5} - \varepsilon \right) V(k_1, k_2, \dots, k_m) \leq l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}) \leq (1 + \varepsilon) V(k_1, k_2, \dots, k_m)$$

стремится к единице при  $s \rightarrow \infty$ .

Действительно, верхняя оценка следует из теоремы 1, а нижняя — из теоремы 2.

**Замечание.** Следующий пример показывает, что уменьшить «разрыв» в  $5/3$  раза между асимптотикой верхней и нижней оценок с помощью только использованных при доказательстве теоремы 2 методов, вообще говоря, нельзя. Итак, пусть

$$\tilde{n}(s) = (s^2, s^2 + 1, \dots, s^2 + s - 1, 2^s, 2^s + 1, \dots, 2^s + \lfloor \log s \rfloor), \quad s = 1, 2, \dots,$$

Тогда  $m(s) = s + \lfloor \log s \rfloor + 1$ ,  $\log \max_i n_i = s + o(1)$ ,  $H(s) \sim 3s$ . Соответственно верхняя оценка, устанавливаемая теоремой 1, асимптотически равна  $5s$ , а все нижние оценки из доказательства теоремы 2 асимптотически не превосходят  $3s$ .

## ЛИТЕРАТУРА

1. **Гашков С. Б., Кочергин В. В.** Об аддитивных цепочках векторов, вентильных схемах и сложности вычисления степеней // Методы дискретного анализа в теории графов и сложности. — Новосибирск, 1992. — Вып. 52. — С. 22–40.
2. **Кнут Д. Е.** Искусство программирования для ЭВМ. — М.: Мир, 1977. — Т. 2. — 724 с.
3. **Кочергин В. В.** О сложности вычислений в конечных абелевых группах // Мат. вопросы кибернетики. — М.: Наука, 1992. — Вып. 4. — С. 178–217.
4. **Кочергин В. В.** О сложности вычислений в конечных абелевых группах // Докл. АН СССР. — 1991. — Т. 317, № 2. — С. 291–294.
5. **Кочергин В. В.** О вычислении наборов степеней // Дискрет. математика. — Т. 6, вып. 2. — 1994. — С. 129–137.
6. **Кочергин В. В.** О сложности вычислений одночленов и наборов степеней // Дискретный анализ. — Новосибирск: Изд-во Института математики СО РАН, 1994. — С. 94–107. (Тр. РАН. Сиб. отд-ние. Ин-т математики; Т. 27)
7. **Кочергин В. В.** О двух обобщениях задачи об аддитивных цепочках // Тр. IV Междунар. конф. «Дискретные модели в теории управляющих систем» (Москва, 19–25 июня 2000 г.). — М.: МАКС Пресс, 2000. — С. 55–59.
8. **Кочергин В. В.** О сложности вычисления пары одночленов от двух переменных // Дискрет. математика. — Т. 17, вып. 4. — 2005. — С. 116–142.
9. **Кочергин В. В.** О сложности вычисления системы из трех одночленов от трех переменных // Мат. вопросы кибернетики. — М.: Наука, 2006. — Вып. 15. — С. 79–155.
10. **Лупанов О. Б.** О синтезе некоторых классов управляющих систем // Пробл. кибернетики. — 1963. — Вып. 10. — С. 63–97.
11. **Лупанов О. Б.** Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Пробл. кибернетики — 1965. — Вып. 14. — С. 31–110.
12. **Сидоренко А. Ф.** Сложность аддитивных вычислений семейств целочисленных линейных форм // Зап. науч. семинаров ЛОУИ. — 1981. — Т. 105. — С. 53–61.
13. **Bellman R. E.** Addition chains of vectors (advanced problem 5125) // Amer. Math. Monthly. — 1963. — Vol. 70. — P. 765.
14. **Brauer A.** On addition chains // Bull. Amer. Math. Soc. — 1939. — Vol. 45. — P. 736–739.
15. **Downey P., Leong B., Sethi R.** Computing sequences with addition chains // SIAM J. Comput. — Vol. 10. — 1981. — P. 638–646.

16. **Erdős P.** Remarks on number theory. III: On addition chains // *Acta Arith.* — 1960. — Vol. 6. — P. 77–81.
17. **Gordon D. M.** A survey of fast exponentiation methods // *J. Algorithms.* — 1998. — Vol. 27. — P. 129–146.
18. **Knuth D. E., Papadimitriou C. H.** Duality in addition chains // *Bull. Eur. Assoc. Theor. Comput. Sci.* — 1981. — Vol. 13. — P. 2–4.
19. **Olivos J.** On vectorial addition chains // *J. Algorithms.* — 1981. — Vol. 2, N 1. — P. 13–21.
20. **Pippenger N.** On evaluation of powers and related problems // *Proc. 17th Ann. IEEE Symp. Found. Comput. Sci. (Houston, TX, 25–27 Oct. 1976).* — P. 258–263.
21. **Pippenger N.** On evaluation of powers and monomials // *SIAM J. Comput.* — 1980. — Vol. 9, N 2. — P. 230–250.
22. **Southard T. H.** Addition chains for the first  $N$  squares // *Tech. Rep. CNA-84*, Univ. Texas, Austin, 1974.
23. **Straus E. G.** Addition chains of vectors // *Amer. Math. Monthly.* — 1964. — Vol. 71. — P. 806–808.
24. **Subbarao M. V.** Addition chains — some results and problems // *Number Theory and Applications. NATO Adv. Sci. Inst. Ser.: Ser. C.* — Kluwer Acad. Publ. Group, 1989. — Vol. 265. — P. 555–574.
25. **Yao A. C.-C.** On the evaluation of powers // *SIAM J. Comput.* — 1976. — Vol. 5. — P. 100–103.

Кочергин Вадим Васильевич,  
e-mail: vvkoch@yandex.ru

Статья поступила  
18 февраля 2014 г.

Переработанный вариант —  
20 мая 2014 г.