

## О вычислении наборов степеней

© 1994 г. В. В. Кочергин

Исследуется известная задача [4, разд. 4.6.3, упр. 32] о сложности вычисления наборов значений  $x^{n_1}, \dots, x^{n_m}$  для различных наборов показателей  $(n_1, \dots, n_m)$ . Пусть  $l(x^{n_1}, \dots, x^{n_m})$  — наименьшее число операций умножения, достаточное для вычисления набора степеней  $x^{n_1}, \dots, x^{n_m}$ , а  $L(n_1, \dots, n_m) = \max l(x^{k_1}, \dots, x^{k_m})$ , где максимум берется по всем наборам  $(k_1, \dots, k_m)$ ,  $1 \leq k_i \leq n_i$ ,  $i = 1, \dots, m$ .

Доказано, что если последовательность наборов вида  $\tilde{n} = (n_1, \dots, n_m)$  удовлетворяет условию

$$m + \log_2(\max\{n_1, \dots, n_m\}) = o\left(\frac{\log_2 \prod_{i=1}^m n_i}{\log_2 \log_2 \prod_{i=1}^m n_i}\right),$$

то

$$L(n_1, \dots, n_m) \sim \frac{\log_2 \prod_{i=1}^m n_i}{\log_2 \log_2 \prod_{i=1}^m n_i},$$

причем

$$l(x^{k_1}, \dots, x^{k_m}) \sim \frac{\log_2 \prod_{i=1}^m k_i}{\log_2 \log_2 \prod_{i=1}^m k_i}$$

для почти всех наборов  $(k_1, \dots, k_m)$  таких, что  $1 \leq k_i \leq n_i$ ,  $i = 1, \dots, m$ .

## 1. Введение

В данной работе исследуется задача вычисления набора значений  $x^{n_1}, \dots, x^{n_m}$ , где  $n_i \in \mathbb{N}$ ,  $i = 1, \dots, m$ .

Обозначим через  $l(x^{n_1}, \dots, x^{n_m})$  наименьшее число операций умножения, достаточное для вычисления набора степеней  $x^{n_1}, \dots, x^{n_m}$ . В дальнейшем о сложности вычисления степеней будем говорить на языке схем из двуходовых элементов умножения (аналогично [1]). Таким образом,  $l(x^{n_1}, \dots, x^{n_m})$  — минимум сложностей  $l(S)$  всех схем из двуходовых элементов умножения, вычисляющих набор степеней  $x^{n_1}, \dots, x^{n_m}$ , где сложность  $l(S)$  схемы  $S$  — это число используемых в схеме  $S$  элементов умножения.

Положим  $L(n_1, \dots, n_m) = \max l(x^{k_1}, \dots, x^{k_m})$ , где максимум берется по всем наборам  $(k_1, \dots, k_m)$  таким, что  $1 \leq k_i \leq n_i$ ,  $i = 1, \dots, m$ .

В 1939 г. Брауэром [2] была установлена асимптотическая формула для вычисления одной степени

$$l(x^n) \sim L(n) \sim \log n,$$

а также была получена верхняя оценка

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

Заметим, что здесь и всюду в дальнейшем  $\log$  означает  $\log_2$ .

В 1960 г. Эрдеш [3] показал, что для почти всех  $n$  эта оценка величины  $l(x^n)$  асимптотически неулучшаема, и, следовательно,

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

В 1969 г. Кнут [4, раздел 4.6.3, упр. 32] поставил задачу о вычислении наборов степеней  $x^{n_1}, \dots, x^{n_m}$  для различных наборов  $\tilde{n} = (n_1, \dots, n_m)$ .

В 1976 г. Яо [5] доказал, что

$$l(x^{n_1}, \dots, x^{n_m}) \sim L(n_1, \dots, n_m) \sim \log \left( \max_{i=1, \dots, m} n_i \right)$$

для каждого фиксированного  $m$ .

Здесь и далее полагаем, что набор  $\tilde{n} = (n_1, \dots, n_m)$  —  $s$ -й член некоторой последовательности наборов, удовлетворяющих условию  $\prod_{i=1}^{m(s)} n_i(s) \rightarrow \infty$  при  $s \rightarrow \infty$ .

В 1980 г. Пиппенджер [6] получил результат, из которого следует, что если справедливо соотношение

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

то

$$L(\underbrace{n_1, \dots, n_m}_m) \sim \frac{\log n^m}{\log \log n^m}.$$

В данной работе будет доказано, что при выполнении условия

$$m + \log \left( \max_{i=1, \dots, m} n_i \right) = o\left(\frac{\log \prod_{i=1}^m n_i}{\log \log \prod_{i=1}^m n_i}\right)$$

справедливо асимптотическое равенство

$$L(n_1, \dots, n_m) \sim \frac{\log \prod_{i=1}^m n_i}{\log \log \prod_{i=1}^m n_i}.$$

Более того, если выполняется условие

$$m + \log \left( \max_{i=1, \dots, m} n_i \right) = o\left(\frac{\log \prod_{i=1}^m n_i}{\log \log \prod_{i=1}^m n_i}\right),$$

то для почти всех наборов  $(k_1, \dots, k_m)$  таких, что  $1 \leq k_i \leq n_i$ ,  $i = 1, \dots, m$ , справедливо асимптотическое равенство

$$l(x^{k_1}, \dots, x^{k_m}) \sim \frac{\log \prod_{i=1}^m k_i}{\log \log \prod_{i=1}^m k_i}.$$

## 2. Верхняя оценка

Сопоставим произвольному набору  $\tilde{n} = (n_1, \dots, n_m)$  (не ограничивая общности в дальнейшем будем считать, что  $n_1 < \dots < n_m$ ) таблицу  $T_{\tilde{n}}$  из  $m$  булевых строк, вообще говоря, неодинаковой длины, где  $i$ -я строка является двоичной записью числа  $n_i$  (младший разряд расположен в первом столбце).

Обозначим через  $H(T_{\tilde{n}})$  число элементов в таблице  $T_{\tilde{n}}$ , т. е.

$$H(T_{\tilde{n}}) = \sum_{i=1}^m \lfloor \log(n_i + 1) \rfloor.$$

Доопределим таблицу  $T_{\tilde{n}}$  нулями до матрицы размера  $m \times \lfloor \log(n_m + 1) \rfloor$ . Полученную матрицу обозначим через  $A(T_{\tilde{n}})$ .

Сведем задачу о верхней оценке сложности вычисления набора степеней  $x^{n_1}, \dots, x^{n_m}$  к задаче о верхней оценке сложности реализации вентильными схемами специального вида (0-1-вентильными схемами) матрицы  $A(T_{\tilde{n}})$  (необходимые определения даны в [7]).

**Лемма 1.**  $l(x^{n_1}, \dots, x^{n_m}) \leq L_{\text{BC}}(A(T_{\tilde{n}})) + \lfloor \log(n_m + 1) \rfloor - 1$ .

*Доказательство.* Преобразуем произвольную минимальную 0-1-вентильную схему, реализующую матрицу  $A(T_{\tilde{n}})$ , в схему из двувходовых элементов умножения следующим образом.

- (1) Построим подсхему, последовательно вычисляющую  $x, x^2, \dots, x^{2^{\lfloor \log(n_m + 1) \rfloor - 1}}$  (потребуется  $\lfloor \log(n_m + 1) \rfloor - 1$  элемент умножения).
- (2) Соединим выход элемента умножения, реализующего степень  $x^{2^{j-1}}$  с  $j$ -м входом 0-1-вентильной схемы,  $j = 1, \dots, \lfloor \log(n_m + 1) \rfloor$ .
- (3) Пронумеруем все невходовые вершины вентильной схемы так, чтобы не оказалось путей от вершин с большими номерами к вершинам с меньшими. В порядке возрастания номеров заменим каждую такую вершину вместе со всеми входящими в нее вентилями-ребрами (а их в силу минимальности вентильной схемы должно быть не менее двух) на цепочку элементов умножения, как показано на рис. 1.
- (4) Выходом с номером  $i$  схемы из элементов умножения,  $i = 1, \dots, m$ , будет выход последнего элемента умножения подсхемы, полученной преобразованием по правилу 2  $i$ -го выхода (с входящими в него вентилями) исходной вентильной схемы.

Очевидно, что  $i$ -й выход полученной схемы из элементов умножения вычисляет  $x^{n_i}$ ,  $i = 1, \dots, m$ , а сложность этой схемы не превосходит величины  $L_{\text{BC}}(A(T_{\tilde{n}})) + \lfloor \log(n_m + 1) \rfloor - 1$ . Лемма 1 доказана.

Обозначим  $N = N(\tilde{n}) = \prod_{i=1}^m n_i$ .

**Лемма 2.** Справедлива оценка

$$l(x^{n_1}, \dots, x^{n_m}) \leq \frac{\log N}{\log \log N} \left( 1 + O \left( \left( \frac{\log \log \log N}{\log \log N} \right)^{1/2} \right) \right) + O(m + \log n_m).$$

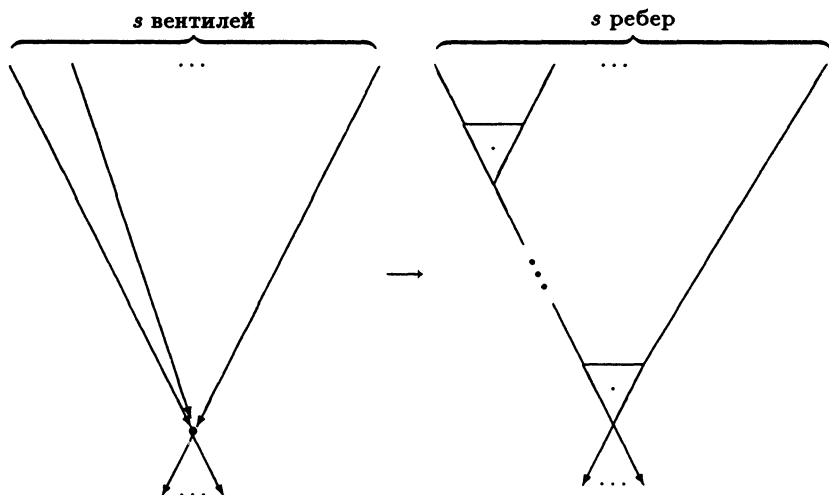


Рис. 1

*Доказательство.* Используя лемму 1, а также лемму 2 и теорему 3 из [7], получаем, что

$$\begin{aligned}
 l(x^{n_1}, \dots, x^{n_m}) &\leq \frac{\log H(T_{\tilde{n}})}{\log \log H(T_{\tilde{n}})} \left( 1 + O \left( \left( \frac{\log \log \log H(T_{\tilde{n}})}{\log \log H(T_{\tilde{n}})} \right)^{1/2} \right) \right) + O(m + \log n_m) \\
 &\leq \left( \frac{\log \prod_{i=1}^m n_i}{\log \log \prod_{i=1}^m n_i} + m \right) \left( 1 + O \left( \left( \frac{\log \log \log \prod_{i=1}^m (n_i + 1)}{\log \log \prod_{i=1}^m n_i} \right)^{1/2} \right) \right) \\
 &\quad + O(m + \log n_m) \\
 &= \frac{\log N}{\log \log N} \left( 1 + O \left( \left( \frac{\log \log \log N}{\log \log N} \right)^{1/2} \right) \right) + O(m + \log n_m).
 \end{aligned}$$

Лемма 2 доказана.

### 3. Нижняя оценка

Введем следующие обозначения: пусть

$$\mathfrak{M}(n_1, \dots, n_m) = \{(k_1, \dots, k_m) \mid k_1 < \dots < k_m; k_i \in \mathbb{N}, 1 \leq k_i \leq n_i, i = 1, \dots, m\};$$

$V(n_1, \dots, n_m; D)$  — число наборов  $k_1, \dots, k_m \in \mathfrak{M}(n_1, \dots, n_m)$  с  $l(x^{k_1}, \dots, x^{k_m}) \leq D$ ;

$v(n_1, \dots, n_m; D)$  — число различных минимальных схем сложности не более  $D$ , реализующих наборы степеней  $x^{k_1}, \dots, x^{k_m}$ , где  $(k_1, \dots, k_m) \in \mathfrak{M}(n_1, \dots, n_m)$ ;

$v'(n_1, \dots, n_m; d)$  — число различных минимальных схем сложности  $d$ , реализующих наборы степеней  $x^{k_1}, \dots, x^{k_m}$ , где  $(k_1, \dots, k_m) \in \mathfrak{M}(n_1, \dots, n_m)$ .

**Лемма 3.** *Справедлива оценка*

$$|\mathfrak{M}(n_1, \dots, n_m)| \geq \frac{n_1(n_2 - 1) \dots (n_m - m + 1)}{m!}.$$

**Лемма 4** (см. [8]). *Справедлива оценка*

$$V(n_1, \dots, n_m; D) \leq (3(D+1))^{D+m+1}.$$

*Доказательство.* Каждая минимальная схема из  $d$  пронумерованных в произвольном порядке двуходовых элементов умножения, реализующая набор степеней  $x^{k_1}, \dots, x^{k_m}$ , где  $(k_1, \dots, k_m) \in \mathcal{M}(n_1, \dots, n_m)$ , полностью определяется списком из  $d$  пар, каждая из которых показывает, что подается на оба входа элемента умножения с соответствующим номером (подается либо  $x$ , либо выход элемента умножения с другим номером), а также указанием тех  $t$  из  $d$  элементов умножения, выходы которых являются выходами схемы.

Заметим, что все  $d!$  списков, соответствующих всем возможным способам нумерации элементов умножения одной минимальной схемы, различны, и разным минимальным схемам соответствуют различные списки. Поэтому

$$v'(n_1, \dots, n_m; d) \leq \frac{(d+1)^{2d} C_d^m}{d!}.$$

Отсюда

$$\begin{aligned} V(n_1, \dots, n_m; D) &\leq v(n_1, \dots, n_m; D) \leq 1 + \sum_{d=1}^D v'(n_1, \dots, n_m; d) \\ &\leq (D+1) \frac{(D+1)^{2D} C_D^m}{D!} = \frac{(D+1)^{2(D+1)} C_D^m}{D!}. \end{aligned}$$

Используя неравенство  $n! \geq (n/3)^n$ , получаем, что

$$V(n_1, \dots, n_m; D) \leq (3(D+1))^{D+1} D^m \leq (3(D+1))^{D+m+1}.$$

Лемма 4 доказана.

**Лемма 5.** Пусть  $m = o(\log N / \log \log N)$ . Тогда найдется функция  $g(n) > 0$  такая, что

$$(1) \quad g(n) \rightarrow 0 \text{ при } n \rightarrow \infty;$$

$$(2) \quad V(n_1, \dots, n_m; (1 - g(N)) \log N / \log \log N) / |\mathcal{M}(n_1, \dots, n_m)| \rightarrow 0 \text{ при } N \rightarrow \infty.$$

*Доказательство.* Так как  $m = o(\log N / \log \log N)$ , найдется такая функция  $f(n)$ , что  $f(n) \rightarrow 0$  при  $n \rightarrow \infty$  и при всех достаточно больших  $N$  выполняется неравенство  $m \leq f(N) \log N / \log \log N$ .

Оценим сверху величину  $\log(V(n_1, \dots, n_m; D) / |\mathcal{M}(n_1, \dots, n_m)|)$ :

$$\begin{aligned} \log \frac{V(n_1, \dots, n_m; D)}{|\mathcal{M}(n_1, \dots, n_m)|} &\leq \log \frac{(3(D+1))^{D+m+1}}{n_1(n_2-1) \dots (n_m-m+1)/m!} \\ &\leq \log \frac{(3(D+1))^{D+m+1} m!}{(n_1/1)(n_2/2) \dots (n_m/m)} \\ &= (D+m+1)(\log(D+1) + \log 3) - \log N + 2 \log(m!). \end{aligned}$$

Положим  $g(n) = \max(\sqrt{f(n)}, (\log \log m)^{-1/2})$ . Подставляя вместо  $D$  величину  $(1 - g(N)) \log N / \log \log N$ , получаем, что

$$\begin{aligned}
 & \log \frac{V(n_1, \dots, n_m; (1 - g(N)) \log N / \log \log N)}{|\mathfrak{M}(n_1, \dots, n_m)|} \\
 & \leq \left( (1 - g(N)) \frac{\log N}{\log \log N} + m + 1 \right) \left( \log \left( (1 - g(N)) \frac{\log N}{\log \log N} + 1 \right) + \log 3 \right) \\
 & \quad - \log N + 2m \log m \\
 & = \left( \frac{\log N}{\log \log N} - g(N) \frac{\log N}{\log \log N} + O(m) \right) (\log \log N - \log \log \log N + O(1)) \\
 & \quad - \log N + O(m \log m) \\
 & \leq -g(N) \log N + O \left( \frac{\log N}{\log \log N} \right) + O \left( g(N) \frac{\log N \log \log \log N}{\log \log N} \right) \\
 & \quad + O(m \log \log N) + O(m \log m) \\
 & \leq -g(N) \log N + O \left( \frac{\log N}{\log \log N} \right) + O \left( g(N) \frac{\log N \log \log \log N}{\log \log N} \right) + O(f(N) \log N).
 \end{aligned}$$

Последнее выражение стремится к  $-\infty$  при  $N \rightarrow \infty$ , так как выполняются следующие соотношения:

$$g(N) > 0; \quad \lim_{N \rightarrow \infty} \frac{1}{g(N) \log \log N} = 0; \quad \lim_{N \rightarrow \infty} \frac{f(N)}{g(N)} = 0.$$

Лемма 5 доказана.

#### 4. Объединение верхней и нижней оценок

**Теорема 1.** Пусть  $m + \log n_m = o(\log N / \log \log N)$ . Тогда справедливо асимптотическое равенство

$$L(n_1, \dots, n_m) \sim \frac{\log N}{\log \log N}.$$

*Доказательство.* Верхняя оценка непосредственно следует из леммы 2. Рассмотрим оценку снизу. Так как  $V(n_1, \dots, n_m; L(n_1, \dots, n_m)) = |\mathfrak{M}(n_1, \dots, n_m)|$ , в силу леммы 5 выполняется неравенство

$$L(n_1, \dots, n_m) \geq (1 - g(N)) \frac{\log N}{\log \log N}$$

для некоторой функции  $g(n)$  такой, что  $g(n) \rightarrow 0$  при  $n \rightarrow \infty$ . Теорема 1 доказана.

Значение величины  $l(x^{n_1}, \dots, x^{n_m})$  может, вообще говоря, сильно отличаться от значения  $L(n_1, \dots, n_m)$ . Например, при  $m = \lfloor \log n_1 \rfloor$ , с одной стороны,

$$l(x^{n_1}, x^{n_1+1}, \dots, x^{n_1+m-1}) \sim \log n_1 + m \sim 2 \log n_1,$$

а с другой, так как  $\log N \sim (\log n_1)^2$  и  $m + \log(n_1 + m - 1) = o(\log N / \log \log N)$ , справедливо соотношение

$$L(n_1, n_1 + 1, \dots, n_1 + m - 1) \sim \frac{\log N}{\log \log N} \sim \frac{(\log n_1)^2}{2 \log \log n_1}.$$

Однако, для величины  $l(x^{n_1}, \dots, x^{n_m})$  справедливо следующее утверждение.

Пусть  $m + \log n_m = o(\log N / \log \log N)$  и  $K = \prod_{i=1}^m k_i$ . Тогда для почти всех наборов  $(k_1, \dots, k_m) \in \mathcal{M}(n_1, \dots, n_m)$  справедливо асимптотическое равенство

$$l(x^{k_1}, \dots, x^{k_m}) \sim \frac{\log K}{\log \log K},$$

Сформулируем это утверждение более строго.

Обозначим через  $U(n_1, \dots, n_m; h)$ , где  $h(n)$  – некоторая функция, число наборов  $(k_1, \dots, k_m) \in \mathcal{M}(n_1, \dots, n_m)$  таких, что

$$\left| l(x^{k_1}, \dots, x^{k_m}) - \frac{\log K}{\log \log K} \right| < h(K) \frac{\log K}{\log \log K}.$$

**Теорема 2.** Пусть  $m + \log n_m = o(\log N / \log \log N)$ . Тогда найдется функция  $h(n) > 0$  такая, что

$$(1) \quad h(n) \rightarrow 0 \text{ при } n \rightarrow \infty;$$

$$(2) \quad U(n_1, \dots, n_m; h) / |\mathcal{M}(n_1, \dots, n_m)| \rightarrow 1 \text{ при } N \rightarrow \infty.$$

*Доказательство.* В силу леммы 2 найдутся положительные  $c_1$  и  $c_2$  такие, что для любого набора  $(k_1, \dots, k_m)$ ,  $k_1 < \dots < k_m$ , справедливо неравенство

$$l(x^{k_1}, \dots, x^{k_m}) \leq \frac{\log K}{\log \log K} + c_1 \frac{\log K (\log \log \log K)^{1/2}}{(\log \log K)^{3/2}} + c_2 (m + \log k_m).$$

Так как  $m + \log n_m = o(\log N / \log \log N)$ , найдется функция  $f(n)$  такая, что  $f(n) \rightarrow 0$  при  $n \rightarrow \infty$  и при всех достаточно больших  $N$  выполняется неравенство  $m + \log n_m \leq f(N) \log N / \log \log N$ . Без ограничения общности можно считать, что функция  $f(n)$  невозрастающая.

Пусть  $g(n)$  – функция, о существовании которой говорится в лемме 5. Тогда найдется  $c_3 > 0$  такое, что для всех достаточно больших  $n$  выполняются неравенства

$$0 \leq \frac{1 + c_1}{1 - g(n) - c_2 f(n)} \leq c_3.$$

Далее, если набор  $(k_1, \dots, k_m)$  удовлетворяет условию

$$l(x^{k_1}, \dots, x^{k_m}) \geq (1 - g(N)) \frac{\log N}{\log \log N},$$

то справедливы соотношения

$$\begin{aligned} (1 - g(N)) \frac{\log N}{\log \log N} &\leq \frac{\log K}{\log \log K} + c_1 \frac{\log K (\log \log \log K)^{1/2}}{(\log \log K)^{3/2}} + c_2 (m + \log k_m) \\ &\leq (1 + c_1) \frac{\log K}{\log \log K} + c_2 f(N) \frac{\log N}{\log \log N}, \end{aligned}$$

и, следовательно, если  $N$  достаточно велико,

$$\frac{\log N}{\log \log N} \leq c_3 \frac{\log K}{\log \log K}.$$

Положим  $h_0(n) = \max \left( g(n), c_1 (\log \log \log n / \log \log n)^{1/2} + c_2 c_3 f(n) \right)$ . Теперь определим функцию  $h(n)$  таким образом:  $h(n) = \max_{i \geq n} h_0(i)$ . Очевидно, что

- (1)  $h(n)$  — невозрастающая функция;
- (2)  $h(n) \rightarrow 0$  при  $n \rightarrow \infty$ ;
- (3)  $h(n) \geq h_0(n) \geq g(n)$ .

Докажем, что функция  $h(n)$  удовлетворяет и условию 2 теоремы. Действительно, если для набора  $(k_1, \dots, k_m) \in \mathfrak{M}(n_1, \dots, n_m)$  выполняется неравенство

$$l(x^{k_1}, \dots, x^{k_m}) \geq (1 - h(N)) \frac{\log N}{\log \log N},$$

то тем более выполняется неравенство

$$l(x^{k_1}, \dots, x^{k_m}) \geq (1 - g(N)) \frac{\log N}{\log \log N},$$

и поэтому, учитывая, что функция  $f(n)$  невозрастающая, получаем, что

$$\begin{aligned} l(x^{k_1}, \dots, x^{k_m}) &\leq \frac{\log K}{\log \log K} + c_1 \frac{\log K (\log \log \log K)^{1/2}}{(\log \log K)^{3/2}} + c_2 (m + \log k_m) \\ &\leq \frac{\log K}{\log \log K} \left( 1 + c_1 \left( \frac{\log \log \log K}{\log \log K} \right)^{1/2} \right) + c_2 f(N) \frac{\log N}{\log \log N} \\ &\leq \frac{\log K}{\log \log K} \left( 1 + c_1 \left( \frac{\log \log \log K}{\log \log K} \right)^{1/2} \right) + c_2 c_3 f(K) \frac{\log K}{\log \log K} \\ &\leq \frac{\log K}{\log \log K} (1 + h(K)). \end{aligned}$$

Следовательно, так как для любого набора  $(k_1, \dots, k_m) \in \mathfrak{M}(n_1, \dots, n_m)$  справедливо неравенство

$$(1 - h(K)) \frac{\log K}{\log \log K} \leq (1 - h(N)) \frac{\log N}{\log \log N},$$

находим, что

$$\begin{aligned} \frac{U(n_1, \dots, n_m; h)}{|\mathfrak{M}(n_1, \dots, n_m)|} &\geq \frac{|\mathfrak{M}(n_1, \dots, n_m)| - V(n_1, \dots, n_m; (1 - h(N)) \log N / \log \log N)}{|\mathfrak{M}(n_1, \dots, n_m)|} \\ &\geq 1 - \frac{V(n_1, \dots, n_m; (1 - g(N)) \log N / \log \log N)}{|\mathfrak{M}(n_1, \dots, n_m)|}. \end{aligned}$$

В силу выбора функции  $g(n)$  (см. лемму 5), получаем, что

$$\frac{U(n_1, \dots, n_m; h)}{|\mathfrak{M}(n_1, \dots, n_m)|} \rightarrow 1$$

при  $N \rightarrow \infty$ . Теорема 2 доказана.

**Добавление при корректуре.** После написания данной статьи, С. Б. Гашковым и автором этой работы показано [9], что для вычисления набора степеней  $x^{n_1}, \dots, x^{n_m}$  в любом случае достаточно

$$\log(\max n_i) + \frac{\log N}{\log \log N} (1 + o(1)) + O(m)$$

операций умножения.



## Список литературы

1. Кочергин В. В. О сложности вычислений в конечных абелевых группах. *ДАН СССР* (1991) **317**, №2, 291–294.
2. Brauer A. On addition chains. *Bull. Amer. Math. Soc.* (1939) **45**, 736–739.
3. Erdős P. Remarks on number theory III. On addition chains. *Acta Arithm.* (1960) **6**, 77–81.
4. Кнут Д. Е. *Искусство программирования для ЭВМ*, т. 2. Мир, Москва, 1977.
5. Yao A. C.-C. On the evaluation of powers. *SIAM J. Comput.* (1976) **5**, 100–103.
6. Pippenger N. On evaluation of powers and monomials. *SIAM J. Comput.* (1980) **9**, 230–250.
7. Кочергин В. В. О сложности вычислений в конечных абелевых группах. *Математические вопросы кибернетики* (1992) №4, 177–216.
8. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования. *Проблемы кибернетики* (1965) №14, 31–110.
9. Гашков С. Б., Кочергин В. В. Об аддитивных цепочках векторов, вентиляных схемах и сложности вычисления степеней *Методы дискретного анализа в теории графов и сложности* (1992) №52, 22–40.

Статья поступила 15.05.92.