О СЛОЖНОСТИ ВЫЧИСЛЕНИЙ ОДНОЧЛЕНОВ И НАБОРОВ СТЕПЕНЕЙ*)

В. В. Кочергин

В данной работе изучается вопрос о сложности вычисления одночленов и наборов степеней при различных моделях вычислений. Полученные результаты вместе с результатами работы [1] дают асимптотически точные решения двух известных задач.

А. Шольц [2] поставил задачу о сложности возведения в степень, т. е. задачу о нахождении величины $l(x^n)$ — минимального числа операций умножения, достаточного для вычисления x^n. Эту задачу (а также ее обобщения) часто рассматривают в аддитивной постановке (так называемая задача об аддитивных цепочках): найти минимально возможное число операций сложения для получения nx, при заданном x (или для получения числа n, имея только единицу) — см., например, [3, раздел 4.6.3].

А. Брауэр [4] (см. также [3, раздел 4.6.3; 5]) доказал верхнюю оценку

$$l(x^n) \leqslant \log n + \frac{\log n}{\log\log n} + O\Big(\frac{\log n \log\log\log n}{(\log\log n)^2}\Big),$$

из которой для величины $l(x^n)$ с учетом очевидной нижней оценки $l(x^n) \geqslant \log n$ следует асимптотическая формула $l(x^n) \sim \log n$. Здесь и далее $\log x = \log_2 x$.

П. Эрдеш [6] (см. также [3, раздел 4.6.3]) показал, что для почти всех чисел n справедливо равенство

$$l(x^n) = \log n + \frac{\log n}{\log\log n} + o\Big(\frac{\log n}{\log\log n}\Big).$$

Более точно этот факт можно сформулировать следующим образом. Существует функция $f(n)$ ($f(n) \to 0$ при $n \to \infty$) такая, что доля натуральных k, не превосходящих n и удовлетворяющих условию

$$\Big| l(x^k) - \log k - \frac{\log k}{\log\log k} \Big| \leqslant f(k)\frac{\log k}{\log\log k},$$

стремится к единице при $n \to \infty$.

Р. Беллман [7] поставил задачу о сложности вычисления одночлена от m переменных, т. е. нахождения величины $l(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m})$. Д. Кнут [3, с. 510, задача 32] поставил задачу о сложности вычисления m степеней одной переменной, т. е. нахождения величины $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$. Е. Страус [8] показал, что для любого фиксированного m

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

---

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 93-011-1527).

А. Яо [9] установил, что

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

для любого фиксированного m. Было показано (см., например, [10, 11; 1, лемма 2]), что на самом деле задачи о сложности реализации одночлена от m переменных и набора m степеней эквивалентны, а именно

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

Рассматривались также некоторые частные случаи задач Беллмана и Кнута. Например, в [12, 13] показано, что $l(x^{1^2}, x^{2^2}, \dots, x^{m^2}) \sim m$.

Н. Пиппенджер в [14] установил факт, из которого, в частности, следует, что

$$l(x^{n_1}, x^{n_2}, \dots, x^{n_m}),\ l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}) \leqslant \log(\max n_i) + \frac{m \log(\max n_i)}{\log(m \log(\max n_i))}(1 + o(1)) + O(m).$$

В [1] получена следующая верхняя оценка сложности вычисления набора m степеней (ввиду эквивалентности задач и для оценки сложности вычисления одночлена от m переменных):

$$l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \leqslant \log(\max n_i) + \frac{\log N}{\log\log N}\left(1 + O\left(\left(\frac{\log\log\log N}{\log\log N}\right)^{\frac{1}{2}}\right)\right) + O(m);$$

здесь и далее полагаем $N = n_1, n_2, \dots, n_m$. В настоящей работе показано, что для почти всех наборов $\tilde{n} = (n_1, n_2, \dots, n_m)$ эта оценка асимптотически не может быть улучшена, т. е. для почти всех наборов $\tilde{n}$ справедливо равенство

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

(точная формулировка результата дана ниже). Кроме того, получены аналогичные оценки сложности реализации одночлена $x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}$ и набора степеней $x^{n_1}, x^{n_2}, \dots, x^{n_m}$ для двух других вычислительных моделей. В первой модели (мультипликативная постановка) разрешается использовать операции умножения и деления, во второй модели (аддитивная постановка) — операции сложения и вычитания. Задачи о сложности вычислений в такой модели ставили П. Унгар (см., например [6]) и А. Ф. Сидоренко [10].

§ 1. Формулировка основного результата

Обозначим через $l_2(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m})$ ($l_2(x^{n_1}, x^{n_2}, \dots, x^{n_m})$) наименьшее число операций умножения и деления, достаточное для вычисления одночлена $x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}$ (набора степеней $x^{n_1}, x^{n_2}, \dots, x^{n_m}$). В [10, теорема 3] показано, что и в этой модели задачи о сложности вычисления одночлена $x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}$ и набора степеней $x^{n_1}, x^{n_2}, \dots, x^{n_m}$ эквивалентны, а именно

$$l_2(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}) + 1 = l_2(x^{n_1}, x^{n_2}, \dots, x^{n_m}) + m.$$

Последняя из рассматриваемых здесь моделей вычислений, введенная А. Ф. Сидоренко [10], заключается в том, что учитываются не только операции умножения (сложения), но и операции присвоения (пересылки). Ясно, что с прикладной точки зрения ими нельзя пренебрегать (время выполнения пересылки сравнимо с временем выполнения сложения). Обозначим через $l_{\text{пр}}(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m})$ (соответственно $l_{\text{пр}}(x^{n_1}, x^{n_2}, \dots, x^{n_m})$) длину (число команд) кратчайшей программы из операторов присвоения вида $z_i := z_j$ и двухадресных команд вида $z_i := z_i z_j$, которая вычисляет одночлен $x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}$ (набор степеней $x^{n_1}, x^{n_2}, \dots, x^{n_m}$); подробности см. в [1, 10]. В [10, теорема 3] показано, что

$$l_{\text{пр}}(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}) = l_{\text{пр}}(x^{n_1}, x^{n_2}, \dots, x^{n_m}).$$

Таким образом, во всех трех моделях вычислений задачи о сложности реализации одночлена $x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}$ и набора степеней $x^{n_1}, x^{n_2}, \dots, x^{n_m}$ эквивалентны. Поэтому в дальнейшем ограничимся только задачей вычисления наборов степеней и сформулируем для нее основное утверждение данной работы.

Для произвольного набора $\tilde{n} = (n_1, n_2, \dots, n_m)$ натуральных чисел $n_1 < n_2 \dots < n_m$ положим $\mathfrak{M}(\tilde{n}) = \{(k_1, k_2, \dots, k_m) \mid k_1 < k_2 < \dots k_m, k_i \in N,\ 1 \leqslant k_i \leqslant n_i,\ i = 1, \dots, n\}$, и $K = k_1 k_2 \dots k_m$.

Теорема 1.1. *Пусть последовательность наборов*

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

удовлетворяет условиям

$$n_1(s) < n_2(s) < \dots < n_{m(s)}(s), \tag{1.1}$$

$$N(s) = \prod_{i=1}^{m(s)} n_i(s) \to \infty \text{ при } s \to \infty. \tag{1.2}$$

Тогда существуют положительные константы c, c_2, $c_{\text{пр}}$ и функции $f(x)$, $f_2(x)$, $f_{\text{пр}}(x)$ и $g_{\text{пр}}(x)$, стремящиеся к нулю при $x \to \infty$, такие, что доли $D(\tilde{n}(s))$, $D_2(\tilde{n}(s))$, $D_{\text{пр}}(\tilde{n}(s))$ наборов $(k_1, k_2, \dots, k_m)$ из $\mathfrak{M}(\tilde{n}(s))$, удовлетворяющих соответственно соотношениям

$$\left| l(x^{k_1}, x^{k_2}, \dots, x^{k_m}) - \left(\log k_m + \frac{\log K}{\log\log K} \right) \right| \leqslant f(K)\frac{\log K}{\log\log K} + cm, \tag{1.3}$$

$$\left| l_2(x^{k_1}, x^{k_2}, \dots, x^{k_m}) - \left(\log k_m + \frac{\log K}{\log\log K} \right) \right| \leqslant f_2(K)\frac{\log K}{\log\log K} + c_2 m, \tag{1.4}$$

$$\left| l_{\text{пр}}(x^{k_1}, x^{k_2}, \dots, x^{k_m}) - \left(\log k_m + \frac{\log K}{\log\log K} \right) \right| \leqslant f_{\text{пр}}(K)\frac{\log K}{\log\log K} + g_{\text{пр}}(K)\log k_m + c_{\text{пр}} m, \tag{1.5}$$

стремятся к единице при $s \to \infty$.

Замечание 1.1. В формулировке теоремы можно положить

$$f(x) = f_2(x) = f_{\text{пр}}(x) = \frac{2}{(\log\log x)^{1/2}}; \qquad g_{\text{пр}}(x) = \frac{2}{\log\log x}.$$

Верхние оценки из этой теоремы (причем для всех, а не почти всех наборов) доказаны в [1, теорема 1].

Нижняя оценка сложности реализации набора степеней будет доказана для вычислений в модели, в которой разрешается использовать операции как умножения, так и деления. Нижние оценки сложности вычислений набора степеней в двух других моделях будут следовать из очевидных неравенств

$$l_2(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \leqslant l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \leqslant l_{\text{пр}}(x^{n_1}, x^{n_2}, \dots, x^{n_m}).$$

Доказательство нижней оценки основано на обобщении доказательства из [6] нижней оценки сложности вычисления одной степени с использованием одной операции на случай реализации набора степеней с использованием двух операций. В доказательстве применяются также некоторые идеи работы [14].

§ 2. Вспомогательные утверждения

Пусть $\tilde{n} = (n_1, n_2, \dots, n_m)$ — набор различных натуральных чисел. Последовательность попарно различных целых чисел

$$1 = a_0, a_1, a_2, \dots, a_r \tag{2.1}$$

и r правил вида

$$a_i = a_j + a_k \text{ или } a_i = a_j - a_k \quad (1 \leqslant j < i,\ 1 \leqslant k < i; i = 1, \dots, r) \tag{2.2}$$

для получения этих чисел назовем $(\pm)$-*цепочкой* для набора $\tilde{n}$, если для любого t $(1 \leqslant t \leqslant m)$ найдется i $(0 \leqslant i \leqslant r)$ такое, что $n_t = a_i$.

Замечание 2.1. Данное определение $(\pm)$-цепочки отличается от обычного определения аддитивной цепочки не только тем, что разрешена операция вычитания, но и тем, что строго фиксируется правило получения очередного элемента по предыдущим.

Легко понять, что наименьшее значение r длины $(\pm)$-цепочки (2.1) для набора $\tilde{n} = (n_1, n_2, \dots, n_m)$ равно $l_2(x^{n_1}, x^{n_2}, \dots, x^{n_m})$.

- $(\pm)$-Цепочку (2.1) для набора $\tilde{n}$ назовем *положительной*, если все ее элементы положительны.

Лемма 2.1. *По всякой* $(\pm)$*-цепочке для произвольного набора* $\tilde{n}$ *можно построить положительную* $(\pm)$*-цепочку той же длины.*

- Для набора $\tilde{n}$ $(\pm)$-цепочку (2.1) будем называть *минимальной*, если не существует $(\pm)$-цепочки меньшей длины.

Каждому элементу a_i $(\pm)$-цепочки (2.1) поставим в соответствие два числа $P(a_i)$ и $Q(a_i)$ следующим образом. Если элемент a_i $(\pm)$-цепочки (2.1) определяется по правилам $a_i = a_j + a_k$ или $a_i = a_j - a_k$, то полагаем $P(a_i) = \max(j, k)$, $Q(a_i) = \min(j, k)$. Кроме того, будем считать, что $P(a_0) = Q(a_0) = -1$.

- $(\pm)$-Цепочку (2.1) назовем *приведенной*, если ее элементы расположены в порядке неубывания величины $P(a_i)$, причем в случае равенства величин $P(a_1), \dots, P(a_n)$ — в порядке неубывания величин $Q(a_1), \dots, Q(a_n)$, а в случае, когда $P(a_1) = \dots = P(a_n)$ и $Q(a_1) = \dots = Q(a_n)$ (что возможно только для элементов, полученных по правилам $a_{i_1} = a_j + a_k$ и $a_{i_2} = a_j - a_k$ соответственно), элемент a_{i_1} предшествует элементу a_{i_2}.

Лемма 2.2. *Для произвольного набора $\tilde{n}$ по всякой* $(\pm)$*-цепочке можно построить положительную приведенную* $(\pm)$*-цепочку той же самой длины.*

Произвольной $(\pm)$-цепочке (2.1) сопоставим последовательность $1 = b_0, b_1, b_2, \ldots, b_r$, где

$$b_i = \max_{0 \leqslant t \leqslant i} |a_t|. \tag{2.3}$$

Обозначим через $H(\lambda, \varepsilon, \nu)$ число положительных приведенных минимальных $(\pm)$-цепочек (2.1), удовлетворяющих условиям

$$\lfloor \log b_r \rfloor \geqslant \lambda, \tag{2.4}$$

$$r \leqslant \lambda + (1-\varepsilon)\nu / \log \nu. \tag{2.5}$$

Отметим, что по лемме 2.2 среди минимальных $(\pm)$-цепочек (2.1), вычисляющих произвольный набор, найдется по крайней мере одна положительная приведенная $(\pm)$-цепочка.

Лемма 2.3. *Пусть* $\lambda \leqslant \nu \log \nu$ *и*

$$\varepsilon(\nu) = 1/(\log \nu)^{1/2}. \tag{2.6}$$

Тогда при при всех достаточно больших ν *выполняется неравенство*

$$H(\lambda, \varepsilon(\nu), \nu) < 2^{\nu}/(2^{\varepsilon(\nu)/4})^{\nu}. \tag{2.7}$$

Доказательство. Положим

$$\delta = \delta(\nu) = 2^{\varepsilon(\nu)/4} - 1. \tag{2.8}$$

Поскольку $\delta \to 0$ при $\nu \to \infty$, будем считать, что

$$\delta < \sqrt{2} - 1. \tag{2.9}$$

Разобьем r шагов произвольной положительной приведенной минимальной $(\pm)$-цепочки (2.1), удовлетворяющей условиям (2.4), (2.5), на три класса.

Шаг i отнесем к *первому классу*, если этот шаг является удвоением, т. е. $b_i = 2b_{i-1}$. (Заметим, что тогда $b_i > b_{i-1}$ и, следовательно, $a_i = b_i$.)

Шаг i отнесем ко *второму классу*, если

$$b_i < 2b_{i-1},$$

$$b_i \geqslant (1+\delta)^{i-j} b_j \text{ для всех } j \quad (0 \leqslant j < i). \tag{2.10}$$

Шаг i отнесем к *третьему классу*, если

$$b_i < 2b_{i-1},$$

$$b_i < (1+\delta)^{i-j} b_j \text{ для некоторого } j \quad (0 \leqslant j < i). \tag{2.11}$$

Обозначим через u_1, u_2, u_3 количество шагов, отнесенных соответственно к первому, второму и третьему классам. Очевидно, что

$$u_1 + u_2 + u_3 = r. \tag{2.12}$$

Оценим сверху величину $u_2 + u_3$.

Если шаг i отнесен к второму или третьему классу, то $b_i \neq 2b_{i-1}$, т. е. $b_i \leqslant b_{i-1} + b_{i-2} \leqslant 3b_{i-2}$. Используя (2.4) и (2.9), получаем

$$2^\lambda \leqslant b_r < 3^{(u_2+u_3)/2}2^{u_1} = \frac{2^{u_1+u_2+u_3}}{(4/3)^{(u_2+u_3)/2}} = \frac{2^r}{2^{(u_2+u_3)\log(2/\sqrt{3})}}.$$

Поэтому в силу (2.5)

$$u_2 + u_3 < \frac{1}{\log(2/\sqrt{3})}(r-\lambda) \leqslant \frac{1-\varepsilon}{\log(2/\sqrt{3})}\frac{\nu}{\log\nu} < 5(1-\varepsilon)\frac{\nu}{\log\nu}. \tag{2.13}$$

Покажем, что

$$u_3 \leqslant (1-\varepsilon/2)\nu/\log\nu. \tag{2.14}$$

Для каждого шага i_s $(s = 1, \ldots, u_3)$ из третьего класса при соответствующем j_s $(0 \leqslant j_s \leqslant i_s)$ в силу (2.11) выполняется неравенство $b_{i_s} < b_{j_s}(1+\delta)^{i_s-j_s}$. Пусть $I_1, \ldots, I_{u_3}$ — полуинтервалы $(j_1, i_1], \ldots, (j_{u_3}, i_{u_3}]$, где $(j, i]$ — множество целых чисел ρ таких, что $j < \rho \leqslant i$. Построим систему неперекрывающихся полуинтервалов $J_1 = (j'_1, i'_1], \ldots, J_h = (j'_h, i'_h]$ такую, что

$$I_1 \cup \ldots \cup I_{u_3} = J_1 \cup \ldots \cup J_h,$$

$$b_{i'_s} < b_{j'_s}(1+\delta)^{2(i'_s-j'_s)} \text{ для } 1 \leqslant s \leqslant h.$$

Пусть $i_1 < i_2 < \ldots < i_{u_3}$. Удалим все полуинтервалы I_t, которые можно удалить, не изменяя объединения $I_1 \cup \ldots \cup I_{u_3}$. Теперь каждую систему перекрывающихся полуинтервалов $(j_c, i_c], \ldots, (j_d, i_d]$ объединим в один полуинтервал $(j', i'] = (j_c, i_d]$. Заметим, что

$$b_{i'} < b_{j'}(1+\delta)^{i_c-j_c+\ldots+i_d-j_d} \leqslant b_{j'}(1+\delta)^{2(i'-j')}, \tag{2.15}$$

так как каждая точка полуинтервала $(j', i']$ покрыта полуинтервалами $(j_c, i_c], \ldots, (j_d, i_d]$ не более чем дважды.

Положим $q = (i'_1 - j'_1) + \ldots + (i'_h - j'_h)$. В силу (2.4), неравенств $b_i \leqslant 2b_{i-1}$ для всех шагов, номера i которых не принадлежат интервалам $J_1, \ldots, J_h$, условия (2.9) и неравенства $q \geqslant u_3$ имеем

$$2^\lambda \leqslant b_r \leqslant 2^{r-q}(1+\delta)^{2q} = 2^r((1+\delta)^2/2)^q \leqslant 2^r((1+\delta)^2/2)^{u_3}.$$

Отсюда и из (2.4), (2.8) получаем

$$u_3 \leqslant \frac{r-\lambda}{1-2\log(1+\delta)} = \frac{r-\lambda}{1-\varepsilon/2} \leqslant \frac{1-\varepsilon}{1-\varepsilon/2}\frac{\nu}{\log\nu} \leqslant (1-\varepsilon/2)\frac{\nu}{\log\nu}.$$

Таким образом, если для произвольной положительной приведенной минимальной $(\pm)$-цепочки (2.1) выполняются неравенства (2.4) и (2.5), то эта цепочка удовлетворяет следующим условиям:

$$\begin{aligned} u_3 &\leqslant (1-\varepsilon/2)\nu/\log\nu, \\ u_2 + u_3 &< 5(1-\varepsilon)\nu/\log\nu, \\ u_1 + u_2 + u_3 &\leqslant \lambda + (1-\varepsilon)\nu/\log\nu. \end{aligned} \tag{2.16}$$

Пусть теперь заданы u_1, u_2, u_3, удовлетворяющие условиям (2.16). Тогда существует не более

$$\binom{r}{u_2+u_3}\binom{u_2+u_3}{u_2} \tag{2.17}$$

способов отнесения каждого шага к тому или иному классу шагов. После того как распределение шагов задано, оценим число возможностей выбора самих шагов.

Сначала оценим сверху число способов выбора шагов, отнесенных к второму классу. Если i-й шаг отнесен к второму классу, то в силу (2.9) выполняется неравенство $b_i \geqslant (1+\delta)b_{i-1}$. Пусть $a_i = a_j + a_k$ или $a_i = a_j - a_k$. Тогда

$$\delta b_{i-1} \leqslant b_j \leqslant b_{i-1}, \quad \delta b_{i-1} \leqslant b_k \leqslant b_{i-1}. \tag{2.18}$$

Кроме того, в силу (2.9)

$$\begin{aligned} b_j &\leqslant b_i/(1+\delta)^{i-j} \leqslant 2b_{i-1}/(1+\delta)^{i-j}, \\ b_k &\leqslant b_i/(1+\delta)^{i-k} \leqslant 2b_{i-1}/(1+\delta)^{i-k}. \end{aligned} \tag{2.19}$$

Из (2.18) и (2.19) получаем

$$\delta \leqslant 2/(1+\delta)^{i-j}, \quad \delta \leqslant 2/(1+\delta)^{i-k}. \tag{2.20}$$

Пусть для натурального β выполняется неравенство $\delta \leqslant 2/(1+\delta)^{\beta}$. Тогда $\delta(1+\beta\delta) \leqslant 2$. Отсюда в силу (2.8) получаем

$$\beta \leqslant \frac{2-\delta}{\delta^2} \leqslant \frac{2}{\delta^2} = \frac{2}{(2^{\varepsilon/4}-1)^2} \leqslant \frac{2}{(\varepsilon/4)^2(\ln 2)^2} = \frac{128}{\varepsilon^2}.$$

Таким образом, имеется не более

$$(3\beta^2)^{u_2} \leqslant (16/\varepsilon)^{4u_2}. \tag{2.21}$$

возможностей для выбора шагов из второго класса.

Теперь оценим сверху число способов выбора шагов, отнесенных к первому и третьему классам. Так как каждая из r^2 пар индексов (j,k), $0 \leqslant j, k \leqslant r$, может быть использована не более двух раз, то имеется не более

$$\binom{2r^2}{u_3} \tag{2.22}$$

возможностей выбора u_3 пар индексов $(j_1,k_1),\ldots,(j_{u_3},k_{u_3})$ для шагов из третьего класса.

В порядке возрастания номера i для каждого шага из первого и третьего классов определим j и k, соответствующие этому шагу, следующим образом.

1. Если i-й шаг отнесен к первому классу, то $a_i = a_j + a_j$, где j однозначно определяется из условия $a_j = b_{i-1}$.
2. Если i-й шаг отнесен к третьему классу, то используем пару (j_h,k_h) из множества $(j_1,k_1),\ldots,(j_{u_3},k_{u_3})$, удовлетворяющую условиям
   (а) $j_h < i$, $k_h < i$;
   (б) величина $\max(j_h,k_h)$ принимает наименьшее значение среди всех пар индексов, не использовавшихся для предыдущих шагов из третьего класса и удовлетворяющих условию (а);
   (в) величина $\min(j_h,k_h)$ принимает наименьшее значение среди всех пар индексов, не использовавшихся для предыдущих шагов из третьего класса и удовлетворяющих условиям (а) и (б).

Если такой пары индексов не существует, то мы не получим никакой $(\pm)$-цепочки. С другой стороны, любая приведенная минимальная $(\pm)$-цепочка с шагами из третьего класса на предписанных местах должна удовлетворять второму правилу выбора шага, отнесенного к третьему классу.

Заметим, что после выбора соответствующей пары индексов (j_h, k_h) для определения самого шага, отнесенного к третьему классу, остается не более двух возможностей. Учитывая это, получаем, что величина

$$2^{u_3}\binom{2r^2}{u_3} \tag{2.23}$$

дает верхнюю оценку для числа вариантов выбора шагов, отнесенных к первому и третьему классам. Таким образом, число положительных приведенных минимальных $(\pm)$-цепочек с заданным количеством u_1, u_2 и u_3 шагов, отнесенных соответственно к первому, второму и третьему классам, не больше произведения величин (2.17), (2.21), (2.23), т. е. величины

$$\binom{u_1+u_2+u_3}{u_2+u_3}\binom{u_2+u_3}{u_2}(16/\varepsilon)^{4u_2}2^{u_3}\binom{2(u_1+u_2+u_3)^2}{u_3}.$$

Поэтому

$$H(\lambda,\varepsilon(\nu),\nu) \leqslant \sum \binom{u_1+u_2+u_3}{u_2+u_3}\binom{u_2+u_3}{u_2} \times (16/\varepsilon)^{4u_2}2^{u_3}\binom{2(u_1+u_2+u_3)^2}{u_3}, \tag{2.24}$$

где сумма берется по всем u_1, u_2 и u_3, удовлетворяющим условиям (2.16).

- Функцию $h(\nu)$ называем *допустимой*, если $\log h(\nu) = O\left(\frac{\nu \log\log\nu}{\log\nu}\right)$ при $\nu \to \infty$.

Легко понять, что число слагаемых в правой части неравенства (2.24) — допустимая функция. Заменив каждый множитель в этих слагаемых на максимально возможный, с учетом (2.16), (2.6) и неравенства $\lambda \leqslant \nu\log\nu$ приходим к оценкам

$$2^{u_3} < 2^{\nu/\log\nu} = h_1(\nu),$$

$$\binom{u_2+u_3}{u_2} \leqslant 2^{u_2+u_3} \leqslant 2^{5\nu/\log\nu} = h_2(\nu),$$

$$(16/\varepsilon(\nu))^{4u_2} \leqslant (16(\log\nu)^{1/2})^{20\nu/\log\nu} = 2^{(20\nu/\log\nu)\log(16(\log\nu)^{1/2}} = h_3(\nu),$$

где $h_1(\nu)$, $h_2(\nu)$, $h_3(\nu)$ — допустимые функции;

$$\binom{u_1+u_2+u_3}{u_2+u_3} \leqslant \binom{\lceil 2\nu\log\nu\rceil}{\lceil 5\nu/\log\nu\rceil} \leqslant \frac{(\lceil 2\nu\log\nu\rceil)^{\lceil 5\nu/\log\nu\rceil}}{(\lceil 5\nu/\log\nu\rceil)!} \leqslant \left(\frac{3\lceil 2\nu\log\nu\rceil}{\lceil 5\nu/\log\nu\rceil}\right)^{\lceil 5\nu/\log\nu\rceil} = h_4(\nu),$$

где $h_4(\nu)$ — допустимая функция, так как

$$\log(h_4(\nu)) = \frac{6\nu\log\log\nu}{\log\nu}(1+o(1)) = O\left(\frac{\nu\log\log\nu}{\log\nu}\right);$$

$$\binom{2(u_1+u_2+u_3)^2}{u_3} \leqslant \binom{\lceil 4\nu^2\log^2\nu\rceil}{u_3} \leqslant \frac{(\lceil 4\nu^2\log^2\nu\rceil)^{u_3}}{(u_3)!} \leqslant (3\lceil 4\log^2\nu\rceil)^{u_3}(\nu^2/u_3)^{u_3},$$

где $(3\lceil 4\log^2\nu\rceil)^{u_3}$ — допустимая функция, так как в силу (2.14)

$$\log((3\lceil 4\log^2\nu\rceil)^{u_3}) \leqslant \frac{2\nu\log\log\nu}{\log\nu}(1+o(1)) = O\Big(\frac{\nu\log\log\nu}{\log\nu}\Big).$$

Теперь оценим сверху величину $(\nu^2/u_3)^{u_3}$. Если $u_3 \leqslant \nu/\log^2\nu$, то

$$(\nu^2/u_3)^{u_3} \leqslant \nu^{2\nu/\log^2\nu} = 2^{2\nu/\log\nu} = h_5(\nu),$$

где $h_5(\nu)$ — допустимая функция. Если $u_3 \geqslant \nu/\log^2\nu$, то в силу (2.14)

$$(\nu^2/u_3)^{u_3} \leqslant (\nu^2/(\nu/\log^2\nu))^{(1-\varepsilon(\nu)/2)\nu/\log\nu} \leqslant 2^{((1-\varepsilon(\nu)/2)\nu/(\log\nu))(\log\nu+2\log\log\nu)} = 2^{(1-\varepsilon(\nu)/2)\nu}h_6(\nu),$$

где $h_6(\nu)$ — допустимая функция. Следовательно, в любом случае

$$(\nu^2/u_3)^{u_3} \leqslant 2^{(1-\varepsilon(\nu)/2)\nu}h_7(\nu),$$

где $h_7(\nu)$ — некоторая допустимая функция.

Таким образом, из (2.24) и полученных оценок имеем

$$H(\lambda,\varepsilon(\nu),\nu) \leqslant 2^{(1-\varepsilon(\nu)/2)\nu}h(\nu).$$

где $h(\nu)$ — допустимая функция (как произведение допустимых функций). Тогда в силу (2.6) при всех достаточно больших ν справедливо неравенство $H(\lambda,\varepsilon(\nu),\nu) < 2^{\nu-\nu\varepsilon(\nu)/4}$. Лемма 2.3 доказана.

§ 3. Доказательство теоремы 1.1

Положим

$$f(x) = f_2(x) = f_{\text{пр}}(x) = 2/(\log\log x)^{1/2}, \tag{3.1}$$

$$g_{\text{пр}}(x) = 2/(\log\log x). \tag{3.2}$$

Верхняя оценка для всех трех вычислительных моделей при соответствующем выборе констант c, c_2 и $c_{\text{пр}}$ в силу теоремы 1 из [1] верна для всех наборов из $\mathfrak{M}(\tilde{n}(s))$. Здесь и далее полагаем, что s (следовательно, $N(s)$) достаточно велико для того, чтобы все соотношения, справедливые при всех достаточно больших s (или N), можно было считать выполненными.

Нижняя оценка. Будем считать, что

$$c \geqslant 4, \quad c_2 \geqslant 4, \quad c_{\text{пр}} \geqslant 4. \tag{3.3}$$

Отметим также, что ввиду (1.1) и (1.2)

$$n_{m(s)}(s) \to \infty \text{ при } s \to \infty. \tag{3.4}$$

В силу очевидных неравенств

$$l_2(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \leqslant l(x^{n_1}, x^{n_2}, \dots, x^{n_m}) \leqslant l_{\text{пр}}(x^{n_1}, x^{n_2}, \dots, x^{n_m})$$

достаточно доказать соответствующее утверждение о нижней оценке для величины $l_2(x^{n_1}, x^{n_2}, \dots, x^{n_m})$. Положим

$$\lambda = \lambda(\tilde{n}) = \max\{\log n_m - \log N/(\log\log N)^{3/2}, 0\}. \tag{3.5}$$

Обозначим через $\mathfrak{M}(\tilde{n}, \lambda)$ множество наборов $(k_1, k_2, \dots, k_m)$ из $\mathfrak{M}(\tilde{n})$ таких, что $\log k_m \geqslant \lambda$, а через $\mathfrak{M}^+(\tilde{n})$ — множество наборов $(k_1, k_2, \dots, k_m)$ из $\mathfrak{M}(\tilde{n})$, удовлетворяющих условию

$$l_2(x^{k_1}, x^{k_2}, \dots, x^{k_m}) \geqslant \log n_m + (1 - f_2(N)) \log N/(\log\log N) - c_2 m.$$

Тогда $\mathfrak{M}^+(\tilde{n}, \lambda) = \mathfrak{M}^+(\tilde{n}) \cap \mathfrak{M}(\tilde{n}, \lambda)$. Заметим, что при всех достаточно больших значениях s для любого набора $(k_1, k_2, \dots, k_m) \in \mathfrak{M}(\tilde{n}(s))$ выполняется неравенство

$$\log n_m + (1 - f_2(N)) \log N (\log\log N)^{-1} - c_2 m \geqslant \log k_m + (1 - f_2(K)) \log K (\log\log K)^{-1} - c_2 m.$$

Отсюда с учетом справедливости верхней оценки для всех наборов из $\mathfrak{M}(\tilde{n}(s))$ получаем

$$D_2(\tilde{n}) \geqslant \frac{|\mathfrak{M}^+(\tilde{n})|}{|\mathfrak{M}(\tilde{n})|}. \tag{3.6}$$

Рассмотрим два случая.

Случай 1: верно неравенство

$$\log N \leqslant 4m \log m + \frac{\log N}{(\log\log N)^{1/2}}. \tag{3.7}$$

Тогда для любого набора $(k_1, k_2, \dots, k_m) \in \mathfrak{M}(\tilde{n}, \lambda)$ в силу (3.1), (3.3), (3.5) и (3.7) справедливы соотношения

$$\begin{aligned} l_2(x^{k_1}, x^{k_2}, \dots, x^{k_m}) &\geqslant \lambda \geqslant \log n_m - \frac{\log N}{(\log\log N)^{3/2}} \\ &= \log n_m + (1 - f_2(N)/2) \frac{\log N}{\log\log N} - \frac{\log N}{\log\log N} \\ &\geqslant \log n_m + (1 - f_2(N)/2) \frac{\log N}{\log\log N} - \frac{4m \log m}{\log\log N} - \frac{\log N}{(\log\log N)^{1/2}} \\ &\geqslant \log n_m + (1 - f_2(N)) \frac{\log N}{\log\log N} - c_2 m. \end{aligned}$$

Таким образом, справедливо равенство $|\mathfrak{M}(\tilde{n}, \lambda)| = |\mathfrak{M}^+(\tilde{n}, \lambda)|$. Поэтому в силу (3.6) $D_2(\tilde{n}(s)) = 1$ при всех достаточно больших s.

Случай 2: верно неравенство

$$\log N > 4m\log m + \frac{\log N}{(\log\log N)^{1/2}}. \tag{3.8}$$

Заметим, что

$$\frac{|\mathfrak{M}^+(\tilde{n})|}{|\mathfrak{M}(\tilde{n})|} \geqslant \frac{|\mathfrak{M}^+(\tilde{n},\lambda)|}{|\mathfrak{M}(\tilde{n})|} = \frac{|\mathfrak{M}(\tilde{n},\lambda)|}{|\mathfrak{M}(\tilde{n})|} - \frac{|\mathfrak{M}(\tilde{n},\lambda)\setminus\mathfrak{M}^+(\tilde{n},\lambda)|}{|\mathfrak{M}(\tilde{n})|}. \tag{3.9}$$

Оценим снизу величину $|\mathfrak{M}(\tilde{n},\lambda)|\,/\,|\mathfrak{M}(\tilde{n})|$. Для этого выпишем все наборы из множества $\mathfrak{M}(\tilde{n})\setminus\mathfrak{M}(\tilde{n},\lambda)$ и объединим их в группы с одинаковыми первыми $m-1$ элементами. Каждой такой группе (она содержит не более 2^λ наборов) можно сопоставить не менее $n_m - 2^\lambda - 1$ наборов из множества $\mathfrak{M}(\tilde{n},\lambda)$ с теми же первыми $m-1$ элементами. Следовательно,

$$|\mathfrak{M}(\tilde{n},\lambda)| \geqslant \frac{n_m - 2^\lambda - 1}{2^\lambda}\,|\mathfrak{M}(\tilde{n})\setminus\mathfrak{M}(\tilde{n},\lambda)| = \frac{n_m - 2^\lambda - 1}{2^\lambda}\,(|\mathfrak{M}(\tilde{n})| - |\mathfrak{M}(\tilde{n},\lambda)|).$$

Поэтому

$$\frac{|\mathfrak{M}(\tilde{n},\lambda)|}{|\mathfrak{M}(\tilde{n})|} \geqslant \frac{n_m - 2^\lambda - 1}{n_m - 1}. \tag{3.10}$$

Отсюда и из (3.6), (3.9), (3.10) следует, что

$$1 \geqslant D_2(\tilde{n}) \geqslant \frac{n_m - 2^\lambda - 1}{n_m - 1} - \frac{|\mathfrak{M}(\tilde{n},\lambda)\setminus\mathfrak{M}^+(\tilde{n},\lambda)|}{|\mathfrak{M}(\tilde{n})|}, \tag{3.11}$$

где в силу (1.2), (3.4) и (3.5)

$$\frac{n_m - 2^\lambda - 1}{n_m - 1} \to 1 \text{ при } s \to \infty. \tag{3.12}$$

Отметим также, что

$$|\mathfrak{M}(\tilde{n})| \geqslant \frac{n_1(n_2-1)\ldots(n_m-m+1)}{m!} \geqslant \frac{N}{(m!)^2}. \tag{3.13}$$

Положим

$$\nu = \log N - 4m\log m. \tag{3.14}$$

Тогда в силу (3.8) справедливо неравенство

$$\nu > \frac{\log N}{(\log\log N)^{1/2}}. \tag{3.15}$$

Каждому набору $(k_1, k_2, \ldots, k_m)$, принадлежащему $|\mathfrak{M}(\tilde{n},\lambda)\setminus\mathfrak{M}^+(\tilde{n},\lambda)|$ и, следовательно, удовлетворяющему условиям

$$k_1 < k_2 < \ldots < k_m, \qquad \log k_m \geqslant \lambda,$$

$$l_2(x^{k_1}, x^{k_2}, \ldots, x^{k_m}) \geqslant \log n_m + (1 - f_2(N))\frac{\log N}{\log\log N} - c_2 m,$$

сопоставим какую-либо положительную приведенную минимальную ($\pm$)-цепочку (2.1), вычисляющую набор $(k_1, k_2, \dots, k_m)$ (следовательно, удовлетворяющую условию $\log b_r \geqslant \lambda$) и такую, что

$$r \leqslant \lambda + \Big(1 - \frac{1}{(\log \nu)^{1/2}}\Big) \frac{\nu}{\log \nu}.$$

Такое сопоставление сделать можно, так как при всех достаточно больших N в силу (3.1), (2.14), неравенства $\nu < N$ и (3.3) имеем

$$\begin{aligned}
&\log n_m + (1 - f_2(N)) \frac{\log N}{\log\log N} - c_2 m \\
&\qquad \leqslant \lambda + \frac{\log N}{\log\log N} - \frac{\log N}{(\log\log N)^{3/2}} - c_2 m \\
&\qquad \leqslant \lambda + \frac{\nu}{\log \nu} + \frac{4m \log m}{\log\log N} - \frac{\nu}{(\log \nu)^{3/2}} - c_2 m \\
&\qquad \leqslant \lambda + \Big(1 - \frac{1}{(\log \nu)^{1/2}}\Big) \frac{\nu}{\log \nu}.
\end{aligned}$$

Очевидно, что каждая положительная приведенная минимальная ($\pm$)-цепочка (2.1) будет сопоставлена не более

$$\Big(\lambda + \Big(1 - \frac{1}{(\log \nu)^{1/2}}\Big) \frac{\nu}{\log \nu}\Big)^m \leqslant (2 \log N)^m \tag{3.16}$$

наборам $(k_1, k_2, \dots, k_m) \in \mathfrak{M}(\tilde{n}, \lambda) \setminus \mathfrak{M}^+(\tilde{n}, \lambda)$. Отметим также, что в силу (3.15) справедливы соотношения

$$l \leqslant \log N \leqslant \nu (\log\log N)^{1/2} \leqslant \nu \log \nu.$$

Таким образом, выполнено условие леммы 2.3. Учитывая (3.16) и применяя леммы 2.2, 2.3, получаем

$$|\mathfrak{M}(\tilde{n}, \lambda) \setminus \mathfrak{M}^+(\tilde{n}, \lambda)| \leqslant (2 \log N)^m H(\lambda, \varepsilon(\nu), \nu) \leqslant \frac{(2 \log N)^m 2^\nu}{(2^{\varepsilon(\nu)/4})^\nu}, \tag{3.17}$$

где $\varepsilon(\nu)$ берется из (2.6). Используя (2.6), (3.13) и (3.17), имеем

$$\begin{aligned}
&\log \Big(\frac{|\mathfrak{M}(\tilde{n}, \lambda) \setminus \mathfrak{M}^+(\tilde{n}, \lambda)|}{|\mathfrak{M}(\tilde{n})|}\Big) \\
&\qquad \leqslant m \log(\log N + 1) + \nu - \frac{\nu}{4(\log \nu)^{1/2}} - \log N + 2m \log m.
\end{aligned} \tag{3.18}$$

Если

$$m \leqslant \log N / (\log\log N)^3, \tag{3.19}$$

то из (3.15), (3.18), (3.19) и неравенства $\nu < \log N$ следует, что

$$\log \Big(\frac{|\mathfrak{M}(\tilde{n}, \lambda) \setminus \mathfrak{M}^+(\tilde{n}, \lambda)|}{|\mathfrak{M}(\tilde{n})|}\Big) < -\frac{\log N}{4 \log\log N} + O\Big(\frac{\log N}{(\log\log N)^2}\Big). \tag{3.20}$$

Если

$$m > \log N / (\log\log N)^3, \tag{3.21}$$

то $m\log(\log N+1)\leqslant 2m\log m$ и, учитывая (3.14) и (3.15), имеем

$$\log\Big(\frac{|\mathfrak{M}(\tilde{n},\lambda)\setminus\mathfrak{M}^{+}(\tilde{n},\lambda)|}{|\mathfrak{M}(\tilde{n})|}\Big)\leqslant-\frac{\nu}{4(\log\nu)^{1/2}}\leqslant-\frac{\log N}{4\log\log N}. \tag{3.22}$$

Таким образом, в силу (3.20) и (3.22) при любых соотношениях между m и $\log N$

$$\frac{|\mathfrak{M}(\tilde{n},\lambda)\setminus\mathfrak{M}^{+}(\tilde{n},\lambda)|}{|\mathfrak{M}(\tilde{n})|}\to 0 \text{ при } s\to\infty.$$

Используя (3.11) и (3.12), получаем, что $D_2(\tilde{n}(s))\to 1$ при $s\to\infty$. Теорема 1.1 доказана.

Замечание 3.1. В формулировке теоремы соотношения (1.3) и (1.4) можно заменить соотношениями

$$\Big|l(x^{k_1},x^{k_2},\dots,x^{k_m})-\Big(\log n_m+\frac{\log N}{\log\log N}\Big)\Big|\leqslant f(N)\frac{\log N}{\log\log N}+cm,$$

$$\Big|l_2(x^{k_1},x^{k_2},\dots,x^{k_m})-\Big(\log n_m+\frac{\log N}{\log\log N}\Big)\Big|\leqslant f_2(N)\frac{\log N}{\log\log N}+c_2m,$$

$$\Big|l_{\text{пр}}(x^{k_1},x^{k_2},\dots,x^{k_m})-\Big(\log n_m+\frac{\log N}{\log\log N}\Big)\Big|$$
$$\leqslant f_{\text{пр}}(N)\frac{\log N}{\log\log N}+g_{\text{пр}}(N)\log n_m+c_{\text{пр}}m.$$

При этом изменении верхние оценки тем более выполняются, а нижние (для почти всех наборов), по существу, доказаны в таком усиленном виде.

Замечание 3.2. Положим

$$L(n_1,n_2,\dots,n_m)=\max l(x^{k_1},x^{k_2},\dots,x^{k_m}),$$
$$L_2(n_1,n_2,\dots,n_m)=\max l_2(x^{k_1},x^{k_2},\dots,x^{k_m}),$$
$$L_{\text{пр}}(n_1,n_2,\dots,n_m)=\max l_{\text{пр}}(x^{k_1},x^{k_2},\dots,x^{k_m}),$$

где максимум берется по всем наборам из $\mathfrak{M}(\tilde{n})$. Тогда для любой последовательности наборов $\tilde{n}(s)$ $(s=1,2,\dots)$ при выполнении условия

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

справедливы асимптотические соотношения

$$L\sim L_2\sim L_{\text{пр}}\sim\log(\max_i n_i)+\frac{\log N}{\log\log N}.$$

Замечание 3.3. Пусть $\tilde{z}=(z_1,z_2,\dots,z_m)$ — набор целых чисел. Тогда для определяемой естественным образом величины $l_2(x^{z_1},x^{z_2},\dots,x^{z_m})$ справедливы следующие оценки:

$$l_2(x^{|z_1|},x^{|z_2|},\dots,x^{|z_m|})\leqslant l_2(x^{z_1},x^{z_2},\dots,x^{z_m})$$
$$\leqslant l_2(x^{|z_1|},x^{|z_2|},\dots,x^{|z_m|})+[m/2]+2.$$

Замечание 3.4. Пусть G — конечная абелева группа (по умножению), а $B_G = \{g_1, g_2, \ldots, g_q\}$ — базис этой группы, т. е.

$$G = \langle g_1 \rangle_{d_1} \times \langle g_2 \rangle_{d_2} \times \ldots \times \langle g_q \rangle_{d_q},$$

где $\langle g \rangle_d$ — циклическая группа порядка d, порожденная элементом g. Обозначим через $L(G, B)$ наименьшее число операций умножения, достаточное для получения любого элемента группы G, исходя из элементов базиса B_G. В [15] (см. также [16]) доказано, что

$$L(G, B_G) = \frac{\log |G|}{\log \log |G|}(1 + o(1)) + O(\log(\max_i d_i)) + O(q).$$

Этот результат можно усилить следующим образом:

$$L(G, B_G) = \log(\max_i d_i) + \frac{\log |G|}{\log \log |G|}(1 + o(1)) + O(q).$$

Верхняя оценка следует из [1, замечание 3], а доказательство нижней оценки полностью аналогично приведенному выше.

В заключение автор выражает признательность В. Б. Алексееву за замечания, способствовавшие улучшению текста работы.

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. **Scholz A.** Jahresbericht der Deutschen Mathematiker. // Vereiningung (11). 1937. Bd. 47, S. 41–42.
3. **Кнут Д. Е.** Искусство программирования для ЭВМ. М.: Мир, 1977. Т. 2.
4. **Brauer A.** On addition chains // Bull. Amer. Math. Soc. 1939. V. 45, P. 736–739.
5. **Вальский Р. Э.** О наименьшем числе умножений для возведения в данную степень // Проблемы кибернетики. М.: Физматгиз, 1959. Вып. 2. С. 73–74
6. **Erdos P.** Remarks on number theory, III: On addition chains // Acta Arith. 1960. V. 6, P. 77–81.
7. **Bellman R. E.** Addition chains of vectors // Amer. Math. Monthly. 1963. V. 70, P. 765.
8. **Straus E. G.** Addition chains of vectors // Amer. Math. Monthly. 1964. V. 71, P. 806–808.
9. **Yao A. C.-C.** On the evaluation of powers // SIAM J. Comput. 1976. V. 5, N 1. P. 100–103.
10. **Сидоренко А. Ф.** Сложность аддитивных вычислений семейств целочисленных линейных форм // Зап. науч. семинаров ЛОМИ. 1981. Т. 105. С. 53–61.
11. **Olivos J.** On vectorial addition chains // J. Algorithms. 1981. V. 2, N 1. P. 13–21.
12. **Southard T. H.** Addition chains for the first N squares // Tech. Rep. CNA-84, Univ. of Texas at Austin, 1974.
13. **Dobkin D., Lipton R. J.** Addition chains methods for the evaluation of specific polynomials // SIAM J. Comput. 1980. V. 9, N 1. P. 121–125.
14. **Pippenger N.** On the evaluation of powers and monomials // SIAM J. Comput. 1980. V. 9, N 2. P. 230–250.
15. **Кочергин В. В.** О сложности вычислений в конечных абелевых группах // Математические вопросы кибернетики. 1992. Вып. 4. С. 178–217.
16. **Кочергин В. В.** О сложности вычислений в конечных абелевых группах // Докл. АН СССР. 1991. Т. 317, № 2. С. 291–294.