О задачах Беллмана и Кнута и их обобщениях

В. В. КОЧЕРГИН
Московский государственный университет им. М. В. Ломоносова,
Институт теоретических проблем микромира им. Н. Н. Боголюбова
e-mail: vvkoch@yandex.ru

УДК 519.7

Ключевые слова: аддитивные цепочки, векторные аддитивные цепочки, цепочки из сложений и вычитаний, цепочки слов, вычисление одночленов, вычисление степеней, задача Беллмана, задача Кнута.

Аннотация

Исследуются в асимптотической постановке различные обобщения классической задачи о наискорейшем возведении в степень, известной также как задача об аддитивных цепочках. Для двух наиболее известных обобщений — для задачи Ричарда Беллмана о сложности (наименьшем числе операций умножения) вычисления (исходя только из переменных) нормированного одночлена от m переменных и для задачи Дональда Кнута о сложности совместного вычисления системы из m степеней одной переменной — при слабых ограничениях предъявлено асимптотически точное решение. Кроме того, дан краткий обзор результатов по сложности вычислений, касающихся следующих трёх задач: вычисление системы из p нормированных одночленов от q переменных; аддитивные вычисления систем из p линейных форм от q переменных; вычисление системы из p элементов свободной абелевой группы с q порождающими.

Abstract

V. V. Kochergin, On Bellman's and Knuth's problems and their generalizations, Fundamentalnaya i prikladnaya matematika, vol. 20 (2015), no. 6, pp. 159—188.

Various generalizations of the classical problem of the fastest raising to a power (or the so-called problem on addition chains) are studied in the asymptotic sense. Under weak restrictions, we demonstrate asymptotically tight solutions of the two best known generalizations, namely, Bellman's problem on the computational complexity (on the minimal number of multiplication operations) of a normed monomial of several variables and Knuth's problem on the computational complexity of a powers system of one variable. We also briefly review some results on the computational complexity for three problems, namely, the computation of p-element systems of normed monomials in q variables, additive computations for systems of p integer linear forms over q variables, and the computation of p-element systems of the free Abelian group with q generators.

Фундаментальная и прикладная математика, 2015, том 20, № 6, с. 159—188.

1. Введение

В данной работе изучаются различные обобщения задачи о сложности возведения в степень, т. е. задачи о нахождении величины $l(x^n)$ — минимального числа операций умножения, достаточного для вычисления по переменной x величины x^n. Эту задачу (а также её обобщения) часто рассматривают в аддитивной постановке: это известная задача об аддитивных цепочках, которая формулируется следующим образом (см., например, [2, 31, 33, 46]).

Аддитивной цепочкой для натурального числа n называется последовательность натуральных чисел

$$a_0 = 1, a_1, \ldots, a_m = n,$$

удовлетворяющая следующему свойству: для каждого k, $1 \leqslant k \leqslant m$, найдутся два (не обязательно различных) числа i и j, $0 \leqslant i, j \leqslant k-1$, такие что $a_k = a_i + a_j$. Число r называется *длиной цепочки*. Очевидно, что минимальная длина аддитивной цепочки для n равна $l(x_n)$.

В 1939 А. Брауэром [27] была установлена асимптотическая формула для величины $l(x^n)$:

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

также была получена верхняя оценка

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

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

В 1960 г. П. Эрдёш [30] показал, что для почти всех n эта оценка величины $l(x^n)$ асимптотически неулучшаема.

В 1975 году А. Шёнхаге [42] установил нижнюю оценку

$$l(n) \geqslant \log n + \log s(n) - 2{,}13,$$

где $s(n)$ — число единиц в двоичной записи числа n.

В дальнейшем получили развитие многие обобщения задачи об аддитивных цепочках. Некоторые из них рассматриваются в данной работе в асимптотической постановке.

2. Вычисление одночленов и наборов степеней (задачи Беллмана и Кнута)

В 1963 г. Р. Беллман сформулировал [25] (а в 1964 г. Э. Страус обобщил [45]) задачу о сложности вычисления одночлена от q переменных, т. е. нахождения величины $l\left(x_1^{n_1} x_2^{n_2} \ldots x_q^{n_q}\right)$.

В 1969 г. Д. Кнут поставил [2, раздел 4.6.3, упр. 32] задачу о сложности вычисления p степеней одной переменной, т. е. нахождения величины $l\left(x^{n_1}, x^{n_2}, \ldots, x^{n_p}\right)$.

Э. Страус в 1964 г. показал [45], что для любого фиксированного q

$$l\bigl(x_1^{n_1}x_2^{n_2}\dots x_q^{n_q}\bigr)\sim\log(\max n_i).$$

В 1976 г. А. Яо установил [48], что для любого фиксированного p

$$l\bigl(x^{n_1},x^{n_2},\dots,x^{n_p}\bigr)\sim\log(\max n_i).$$

Д. Добкин и Р. Липтон доказали [28] асимптотическую формулу

$$l\bigl(x^{1^2},x^{2^2},\dots,x^{p^2}\bigr)\sim p.$$

В 1980 г. Н. Пиппенджер получил [41] результат, из которого, в частности, следует, что

$$l\bigl(x_1^{n_1}x_2^{n_2}\dots x_q^{n_q}\bigr)\leqslant\log(\max n_i)+\frac{m\,\log(\max n_i)}{\log\bigl(m\,\log(\max n_i)\bigr)}\bigl(1+o(1)\bigr)+O(q),$$

$$l\bigl(x^{n_1},x^{n_2},\dots,x^{n_p}\bigr)\leqslant\log(\max n_i)+\frac{m\,\log(\max n_i)}{\log\bigl(m\,\log(\max n_i)\bigr)}\bigl(1+o(1)\bigr)+O(p).$$

П. Доуни, Б. Леонг, Р. Сети в 1981 г. установили [29], что задача распознавания по набору натуральных чисел $(n_1,n_2,\dots,n_p,l)$ существования аддитивной цепочки, имеющей длину l и содержащей числа $n_1,n_2,\dots,n_p$, является NP-полной.

Также в 1981 г. было доказано [21, 34, 39] (см. также [1, лемма 2]), что на самом деле задачи о сложности вычисления одночлена от m переменных и набора m степеней эквивалентны:

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

и следовательно, достаточно исследовать одну из них.

2.1. Верхняя оценка

Теорема 1 [17]. *Пусть числовая функция $f(x)$ при $x\to\infty$ удовлетворяет условиям $f(x)\to\infty$ и $\log f(x)=o(\log x)$. Тогда для любой последовательности наборов натуральных чисел $\tilde n(s)=\bigl(n_1(s),n_2(s),\dots,n_{m(s)}(s)\bigr)$, $s=1,2,\dots$, удовлетворяющей при $s\to\infty$ условию*

$$N=\prod_{i=1}^{m(s)}n_i(s)\to\infty,$$

выполняются неравенства

$$l\bigl(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}\bigr)\leqslant\log(\max n_i)\bigl(1+o(1)\bigr)+$$
$$+\frac{\log N}{\log\log N}\bigl(1+o(1)\bigr)+\sum_{i=1}^{m}\left\{\frac{\log n_i}{\log m-2\log f(m)}\right\},$$

$$l\bigl(x^{n_1}, x^{n_2}, \ldots, x^{n_m}\bigr) \leqslant \log(\max n_i)\bigl(1 + o(1)\bigr) + \\ + \frac{\log N}{\log\log N}\bigl(1 + o(1)\bigr) + \sum_{i=1}^{m}\left\{\frac{\log n_i}{\log m - 2\log f(m)}\right\} - m,$$

где $\{x\}$ *— дробная часть числа* x.

Учитывая равенство

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

верхнюю оценку докажем только для величины $l\bigl(x_1^{n_1}x_2^{n_2}\ldots x_m^{n_m}\bigr)$.

Поставим в соответствие произвольному набору $\tilde{n} = (n_1, \ldots, n_m)$ (не ограничивая общности, в дальнейшем будем считать, что $n_1 < n_2 < \ldots < n_m$) таблицу $T_{\tilde{n}}$ из m булевых столбцов (вообще говоря, неодинаковой длины), где i-й столбец является двоичной записью числа n_i (младший разряд расположен в первой строке).

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

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

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

Оценим сверху сложность вычисления одночлена $x_1^{n_1}x_2^{n_2}\ldots x_m^{n_m}$ через сложность реализации вентильными схемами матрицы $A(T_{\tilde{n}})$ (вентильная схема реализует матрицу A, если число ориентированных цепей в схеме, ведущих от j-го входа к i-му выходу, равно элементу a_{ij} матрицы A; сложность $L_{\text{ВС}}(A)$ реализации вентильными схемами матрицы A — это минимальное число вентилей (рёбер) среди всех вентильных схем, реализующих матрицу A).

Лемма 1. *Справедливо неравенство*

$$l\bigl(x_1^{n_1}x_2^{n_2}\ldots x_m^{n_m}\bigr) \leqslant L_{\text{ВС}}\bigl(A(T_{\tilde{n}})\bigr) + 2\lceil\log(n_m + 1)\rceil - 2.$$

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

1. Припишем i-му входу вентильной схемы переменную x_i, $i = 1, \ldots, m$.

2. Пронумеруем все невходовые вершины вентильной схемы так, чтобы не оказалось путей от вершин с бóльшими номерами к вершинам с меньшими номерами. В порядке возрастания номеров каждую такую вершину вместе со всеми входящими в неё вентилями-рёбрами (а их в силу минимальности вентильной схемы должно быть не менее двух) заменим соответствующим образом на цепочку двувходовых элементов умножения.

3. Обозначим одночлен, вычисляемый j-м выходом полученной на предыдущем этапе схемы, через h_j, $j = 1, \ldots, \lceil\log(n_m + 1)\rceil$. Последняя часть схемы из

элементов умножения последовательно вычисляет одночлены

$$h^2_{\lceil\log(n_m+1)\rceil},\ h_{\lceil\log(n_m+1)\rceil-1}h^2_{\lceil\log(n_m+1)\rceil},\dots,$$
$$h_1\big(h_2\dots\big(h_{\lceil\log(n_m+1)\rceil-1}h^2_{\lceil\log(n_m+1)\rceil}\big)^2\dots\big)^2.$$

По построению справедливо равенство

$$h_1\big(h_2\dots\big(h_{\lceil\log(n_m+1)\rceil-1}h^2_{\lceil\log(n_m+1)\rceil}\big)^2\dots\big)^2 = x_1^{n_1}x_2^{n_2}\dots x_m^{n_m},$$

а число используемых в схеме умножений не превосходит величины

$$L_{\mathrm{BC}}\big(A(T_{\tilde{n}})\big) + 2\lceil\log(n_m+1)\rceil - 2.$$

Лемма 1 доказана. □

Обозначим

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

Лемма 2 [6]. *Выполняется неравенство*

$$l\big(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}\big) \leqslant \frac{\log N}{\log\log N}\left(1 + O\left(\left(\frac{\log\log\log N}{\log\log N}\right)^{1/2}\right)\right) + O(m+\log n_m).$$

Доказательство. Используя лемму 1, а также [4, теорема 3] (см. также [3]), получаем, что

$$\begin{aligned}
&l\big(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}\big) \leqslant\\
&\quad\leqslant \frac{H(T_{\tilde{n}})}{\log H(T_{\tilde{n}})}\left(1 + O\left(\left(\frac{\log\log H(T_{\tilde{n}})}{\log H(T_{\tilde{n}})}\right)^{1/2}\right)\right) + O(m+\log n_m) \leqslant\\
&\quad\leqslant \left(\frac{\log\prod\limits_{i=1}^{m} n_i}{\log\log\prod\limits_{i=1}^{m} n_i} + m\right)\left(1 + O\left(\left(\frac{\log\log\log\prod\limits_{i=1}^{m}(n_i+1)}{\log\log\prod\limits_{i=1}^{m} n_i}\right)^{1/2}\right)\right) +\\
&\quad + O(m+\log n_m) \leqslant\\
&\quad\leqslant \frac{\log N}{\log\log N}\left(1 + O\left(\left(\frac{\log\log\log N}{\log\log N}\right)^{1/2}\right)\right) + O(m+\log n_m).
\end{aligned}$$

Лемма 2 доказана. □

Лемма 3 [1]. *При любом натуральном t справедливо неравенство*

$$l\big(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}\big) \leqslant \log n_m + \frac{\log N}{t} + 2^t m.$$

Доказательство. Представим одночлен $x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}$ в следующем виде:

$$x_1^{n_1}x_2^{n_2}\dots x_m^{n_m} = g_1\big(g_2\dots\big(g_{r-1}g_r^{2^t}\big)^{2^t}\dots\big)^{2^t},$$

где $r \leqslant \lceil \lceil \log(n_m+1) \rceil / t \rceil$, а g_i, $i = 1, \ldots, r$, — одночлены с показателями степеней переменных из множества $\{1, \ldots, 2^t - 1\}$ (аналог схемы Горнера).

С помощью $m(2^t - 2)$ умножений вычислим все степени x_i^k, $i = 1, \ldots, m$, $k = 1, \ldots, 2^t - 1$; затем, используя не более

$$\lceil \lceil \log(n_1 + 1) \rceil / t \rceil + \ldots + \lceil \lceil \log(n_m + 1) \rceil / t \rceil - r$$

умножений, получим все одночлены g_j, $j = 1, \ldots, r$, и наконец, с помощью $(t+1)(r-1)$ умножений — одночлен $x_1^{n_1} x_2^{n_2} \ldots x_m^{n_m}$. Таким образом,

$$l\left(x_1^{n_1} x_2^{n_2} \ldots x_m^{n_m}\right) \leqslant m(2^t - 2) + \left(\frac{\log N}{t} + 2m - r\right) + (t+1)(r-1) \leqslant$$
$$\leqslant \log n_m + \frac{\log N}{t} + 2^t m.$$

Лемма 3 доказана. □

Лемма 4 [1]. *Пусть $N \to \infty$. Тогда*

$$l\left(x_1^{n_1} x_2^{n_2} \ldots x_m^{n_m}\right) \leqslant$$
$$\leqslant \log(\max n_i) + \frac{\log N}{\log\log N}\left(1 + O\left(\left(\frac{\log\log\log N}{\log\log N}\right)^{1/2}\right)\right) + O(m).$$

Доказательство. Положим

$$R = \sum_{i=1}^{m} \log n_i = \log N, \quad R_2(k) = \sum_{i=k+1}^{m} \log n_i, \quad k = 1, \ldots, m.$$

Определим число m_1 следующим образом. Если выполняется неравенство $\log n_1 \geqslant R/(\log R)^2$, то полагаем $m_1 = 0$; если же выполняется неравенство $\log n_1 < R/(\log R)^2$, то в качестве m_1 принимаем минимальное значение k, для которого выполняется неравенство

$$\frac{R_2(k)}{(\log R_2(k))^2} \leqslant \log n_{k+1}.$$

Такое значение найдётся и будет отлично от 0 и m, так как

$$\frac{R_2(0)}{(\log R_2(0))^2} = \frac{R}{(\log R)^2} > \log n_1, \quad \frac{R_2(m-1)}{(\log R_2(m-1))^2} = \frac{\log n_m}{(\log\log n_m)^2} < \log n_m,$$

Введём обозначения:

$$m_2 = m - m_1, \quad R_1 = \sum_{i=k+1}^{m_1} \log n_i, \quad R_2 = R_2(m).$$

Из леммы 2 следует, что

$$l\left(x_1^{n_1} x_2^{n_2} \ldots x_{m_1}^{n_{m_1}}\right) \leqslant \frac{R_1}{\log R_1}\left(1 + O\left(\left(\frac{\log\log R_1}{\log R_1}\right)^{1/2}\right)\right) + O\left(m + \frac{R}{\log R}\right);$$

по лемме 3 при $t = \lceil \log R_2 - 4 \log\log R_2 \rceil$ имеем

$$l\big(x_{m_1+1}^{n_{m_1+1}} \dots x_m^{n_m}\big) \leqslant \log n + \frac{R_2}{\lceil \log R_2 - 4\log\log R_2 \rceil} + \frac{2R_2}{(\log R_2)^4} m_2.$$

Так как

$$R_2(k) = \sum_{i=k+1}^{m} \log n_i \geqslant m_2 \log n_{m_1+1} \geqslant m_2 \frac{R_2}{(\log R_2)^2},$$

то $m_2 \leqslant (\log R_2)^2$ и, следовательно,

$$l(x_{m_1+1}^{n_{m_1+1}} \dots x_m^{n_m}) \leqslant \log n + \frac{R_2}{\log R_2} \left(1 + O\left(\left(\frac{\log\log R_2}{\log R_2}\right)^{1/2}\right)\right).$$

Складывая полученные оценки и применяя неравенство Йенсена

$$f(x_1) + f(x_2) \leqslant 2f\left(\frac{x_1 + x_2}{2}\right),$$

справедливое для выпуклой вверх функции, получаем, что при $R_i \geqslant x_0$, $i = 1, 2$, и $R \to \infty$ справедливы соотношения

$$\begin{aligned} l\big(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}\big) &\leqslant l\big(x_1^{n_1} x_2^{n_2} \dots x_{m_1}^{n_{m_1}}\big) + l\big(x_{m_1+1}^{n_{m_1+1}} \dots x_m^{n_m}\big) + 1 \leqslant \\ &\leqslant \log n + \frac{R_1 + R_2}{\log \frac{R_1+R_2}{2}} \left(1 + O\left(\left(\frac{\log\log \frac{R_1+R_2}{2}}{\log \frac{R_1+R_2}{2}}\right)^{1/2}\right)\right) + O\left(m + \frac{R}{(\log R)^2}\right) = \\ &= \log n + \frac{R}{\log R} \left(1 + O\left(\left(\frac{\log\log R}{\log R}\right)^{1/2}\right)\right) + O(m). \end{aligned}$$

Для завершения доказательства верхней оценки осталось отметить, что если $R_2 < R/(\log R)^2$, то

$$o(1) \log n = O(R_2) = O\left(\frac{R}{(\log R)^2}\right),$$

а если $R_2 > R/(\log R)^2$, то

$$\log n \left(1 + \frac{1}{\log R_2} + o\left(\frac{1}{\log R_2}\right)\right) = \log n \left(1 + \frac{1 + o(1)}{\log R_2}\right).$$

Лемма 4 доказана. □

Доказательство теоремы 1. Отдельно рассмотрим два случая: $\log N \geqslant \geqslant m \log m f(m)$ и $\log N < m \log m f(m)$.

Случай 1. Пусть выполняется неравенство

$$\log N \geqslant m \log m f(m).$$

Тогда

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

Применяя лемму 4 и используя это соотношение, получаем

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

Требуемая верхняя оценка в этом случае доказана.

Случай 2. Пусть выполняется неравенство

$$\log N < m \log m f(m).$$

В этом случае будем доказывать нужную оценку для задачи Кнута. Без ограничения общности можно считать, что все n_i различны. Тогда

$$\log N \geqslant \log(m!) \sim m \log m,$$

и поэтому в условиях случая 2, учитывая, что $\log f(m) = o(\log m)$, имеем

$$\log\log N \sim \log m.$$

Кроме того, из последних двух соотношений следует неравенство

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

Положим

$$I_1 = \big\{i \mid n_i < m^{f(m)}\big\}, \quad I_2 = \big\{i \mid n_i \geqslant m^{f(m)}\big\}.$$

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 следующие $d = \lceil f(m) \rceil + 1$ групп степеней:

$$\begin{aligned}
&\text{1-я группа:} \quad x^a, && a = 1, 2, \ldots, \left\lceil \frac{m}{(f(m))^2} \right\rceil;\\
&\text{2-я группа:} \quad x^{a\left(\left\lceil \frac{m}{(f(m))^2} \right\rceil\right)}, && a = 1, 2, \ldots, \left\lceil \frac{m}{(f(m))^2} \right\rceil;\\
&\ldots\\
&d\text{-я группа:} \quad x^{a\left(\left\lceil \frac{m}{(f(m))^2} \right\rceil\right)^{d-1}}, && a = 1, 2, \ldots, \left\lceil \frac{m}{(f(m))^2} \right\rceil.
\end{aligned}$$

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

Отметим, что в силу соотношений

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

справедливо неравенство

$$m^{f(m)} \leqslant \left(\left\lceil \frac{m}{(f(m))^2} \right\rceil\right)^d,$$

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

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

$$= o\left(\frac{\log N}{\log\log N}\right) + \sum_{i \in I_1} \frac{\log n_i}{\log\left(\frac{m}{(f(m))^2}\right)} +$$

$$+ \sum_{i \in I_1} \left(\lceil \log_{(m/(f(m))^2)} n_i \rceil - 1 - \log_{(m/(f(m))^2)} n_i\right) = \frac{\log \prod\limits_{i \in I_1} n_i}{\log m}\left(1 + o(1)\right) +$$

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

Используя лемму 4, получаем

$$l(\{x^{n_i} \mid i \in I_2\}) \leqslant \log\Big(\max_{i \in I_2} n_i\Big)\left(1 + o(1)\right) + \frac{\log \prod\limits_{i \in I_2} n_i}{\log\log \prod\limits_{i \in I_2} n_i}\left(1 + o(1)\right) + O(|I_2|).$$

Оценим сверху величину $|I_2|$. Из неравенств

$$N \geqslant \prod_{i \in I_2} n_i \geqslant \left(m^{f(m)}\right)^{|I_2|},$$

следует, что

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

Таким образом,

$$l(\{x^{n_i} \mid i \in I_2\}) \leqslant \log(\max n_i)\left(1 + o(1)\right) + \frac{\log \prod\limits_{i \in I_2} n_i}{\log\log \prod\limits_{i \in I_2} n_i}\left(1 + o(1)\right) + o\left(\frac{\log N}{\log\log N}\right).$$

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

$$l\left(x^{n_1}, x^{n_2}, \ldots, x^{n_m}\right) \leqslant \log(\max n_i)\left(1 + o(1)\right) + \frac{\log \prod\limits_{i \in I_1} n_i}{\log m}\left(1 + o(1)\right) +$$

$$+ \frac{\log \prod\limits_{i \in I_2} n_i}{\log\log \prod\limits_{i \in I_2} n_i}\left(1 + o(1)\right) +$$

$$+ \sum_{i=1}^{m} \left(\lceil \log_{(m/(f(m))^2)} n_i \rceil - \log_{(m/(f(m))^2)} n_i\right) - m + o\left(\frac{\log N}{\log\log N}\right).$$

Отметим, что в случае выполнения неравенства

$$\log \prod_{i\in I_2} n_i \geqslant \frac{\log N}{(\log\log N)^2}$$

справедливы соотношения

$$\log\log \prod_{i\in I_2} n_i \geqslant \log\log N - 2\log\log\log N \sim \log\log N \sim f(m),$$

и следовательно,

$$\frac{\log \prod\limits_{i\in I_2} n_i}{\log\log \prod\limits_{i\in I_2} n_i} \leqslant \frac{\log\log N}{\log m}\big(1+o(1)\big).$$

Если же выполняется неравенство

$$\log \prod_{i\in I_2} n_i < \frac{\log N}{(\log\log N)^2}$$

то, очевидно,

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

Таким образом, в обоих случаях

$$\frac{\log \prod\limits_{i\in I_1} n_i}{\log m}\big(1+o(1)\big) + \frac{\log \prod\limits_{i\in I_2} n_i}{\log\log \prod\limits_{i\in I_2} n_i}\big(1+o(1)\big) \leqslant$$

$$\leqslant \frac{\log N}{\log m}\big(1+o(1)\big) = \frac{\log N}{\log\log N}\big(1+o(1)\big)$$

Поэтому окончательно получаем

$$l(x^{n_1}, x^{n_2}, \ldots, x^{n_m}) \leqslant \log(\max n_i)\big(1+o(1)\big) + \frac{\log N}{\log\log N}\big(1+o(1)\big) +$$

$$+ \sum_{i=1}^{m}\big(\lceil \log_{(m/(f(m))^2)} n_i\rceil - \log_{(m/(f(m))^2)} n_i\big) - m.$$

Для завершения доказательства верхней оценки осталось использовать равенство

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

Теорема 1 доказана. □

Следствие 1. *Для любой последовательности наборов натуральных чисел*

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

удовлетворяющей при $s \to \infty$ условию

$$N = \prod_{i=1}^{m(s)} n_i(s) \to \infty,$$

выполняются неравенства

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

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

2.2. Нижняя оценка

Верхняя оценка теоремы 1 асимптотически неулучшаема для почти всех наборов $\tilde{n} = (n_1, n_2, \dots, n_m)$, т. е. для почти всех наборов $\tilde{n}$ справедливы асимптотические равенства

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

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

Аккуратно сформулируем этот факт.

Теорема 2 [7]. *Пусть последовательность наборов*

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

удовлетворяет при $s \to \infty$ условию

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

Тогда существуют такие положительные константа c и функция $f(x)$, стремящаяся к нулю при $x \to \infty$, что доля наборов $(k_1, k_2, \dots, k_m)$, $k_i \leqslant n_i$, удовлетворяющих соотношению

$$l(x^{k_1}, x^{k_2}, \dots, x^{k_m}) \geqslant \log\max k_i + \frac{\log K}{\log\log K} - f(K)\frac{\log K}{\log\log K} - cm,$$

где $K = k_1 k_2 \dots k_m$, стремится к единице при $s \to \infty$.

Учитывая равенство

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

нижнюю оценку докажем только для величины $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$.

Последовательность натуральных чисел $1 = a_0, a_1, \dots, a_r$ и r правил вида $a_i = a_j + a_k$, где $1 \leqslant j < i$, $1 \leqslant k < i$, $i = 1, \dots, r$, для получения этих чисел называются *аддитивной цепочкой* для набора $\tilde{n} = (n_1, \dots, n_m)$, если

для любого t, $t = 1, \dots, m$, найдётся i, $1 \leqslant i \leqslant r$, $i = 1, \dots, i$, такое что $n_t = a_i$. Без ограничения общности можно считать все аддитивные цепочки возрастающими. Легко понять, что наименьшее значение r длины аддитивной цепочки для набора $\tilde{n}$ равно $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$.

Аддитивную цепочку для набора $\tilde{n}$ будем называть *минимальной*, если не существует аддитивной цепочки для набора $\tilde{n}$ меньшей длины.

Обозначим через $H(\lambda, \varepsilon, \nu)$ число возрастающих минимальных аддитивных цепочек (указанного выше вида), удовлетворяющих условиям

$$\lfloor \log a_r \rfloor \geqslant \lambda, \quad r \leqslant \lambda + \frac{(1-\varepsilon)\nu}{\log \nu}.$$

Лемма 5. *Пусть $\lambda \leqslant \nu \log \nu$ и $\varepsilon(\nu) = 1/(\log \nu)^{1/2}$. Тогда при всех достаточно больших ν выполняется неравенство*

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

Эта лемма доказывается аналогично соответствующему неравенству при доказательстве нижней оценки величины $l(x^n)$ из [30] (см. также [2, раздел 4.6.3]). В усиленном виде эта лемма доказана в [7, лемма 2.3].

Перейдём к непосредственному доказательству нижней оценки (см. также [7]).

Положим

$$M(\tilde{n}) = \{k_1, k_2, \dots, k_m \mid k_1 < k_2 < \dots < k_m,\ k_i \in \mathbb{N},\ 1 \leqslant k_i \leqslant n_i,\ i = 1, \dots, m\}.$$

Обозначим $K = k_1 k_2 \dots k_m$. Покажем, что для любой последовательности наборов $\tilde{n}(s) = \big(n_1(s), n_2(s), \dots, n_{m(s)}(s)\big)$, $s = 1, 2, \dots$, удовлетворяющей условию $N(s) \to \infty$ при $s \to \infty$, доля $D\big(\tilde{n}(s)\big)$ наборов $(k_1, k_2, \dots, k_m)$ из множества $M\big(\tilde{n}(s)\big)$, удовлетворяющих соотношению

$$\left(\log k_m + \frac{\log K}{\log \log K}\right) - l(x^{k^1}, x^{k^2}, \dots, x^{k^m}) \leqslant f(K)\frac{\log K}{\log \log K} + cm$$

(здесь $f(x) = 2/(\log \log K)^{1/2}$, c — некоторая константа больше 4), стремится к единице при $s \to \infty$.

Положим

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

В случае когда выполняется неравенство

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

непосредственной проверкой нетрудно убедиться, что $D\big(\tilde{n}(s)\big) \to \infty$ при $s \to \infty$.

В случае когда выполняется неравенство

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

полагая $\nu = \log N - 4m\log m$ и применяя лемму 5, также получаем, что $D\big(\tilde{n}(s)\big) \to \infty$ при $s \to \infty$. Нижняя оценка доказана.

Тем самым при слабых ограничениях даны асимптотически точные (для почти всех наборов $\tilde{n} = (n_1, n_2, \ldots, n_m)$) решения задач Р. Беллмана и Д. Кнута.

3. Одно применение задачи Кнута

В этом разделе изучается задача порождения (сборки) слов с помощью операции конкатенации.

Конкатенацией слов $\tilde{\alpha}$ и $\tilde{\beta}$ конечной длины над произвольным алфавитом называется слово $\tilde{\alpha}\tilde{\beta}$, полученное приписыванием к слову $\tilde{\alpha}$ справа слова $\tilde{\beta}$. Далее будут рассматриваться только слова из алфавита $\{0, 1\}$.

Последовательность S двоичных слов (наборов)

$$\tilde{\tau}_{-1} = 0,\ \tilde{\tau}_0 = 1,\ \tilde{\tau}_1, \ldots,\ \tilde{\tau}_r = \tilde{\alpha}$$

называется *цепочкой слов* (см., например, [24]) или *схемой конкатенации* (см., например, [19]), реализующей (вычисляющей) слово (набор) $\tilde{\alpha}$, если для каждого i, $i = 1, 2, \ldots, r$, слово $\tilde{\tau}_i$ можно представить в виде $\tilde{\tau}_i = \tilde{\tau}_j\tilde{\tau}_m$, где индексы j и m удовлетворяют условиям $-1 \leqslant j, m \leqslant i - 1$. *Сложностью* $l_{\mathrm{c}}(S)$ данной схемы S, реализующей слово $\tilde{\alpha}$, назовём число r. Положим $l_{\mathrm{c}}(\tilde{\alpha}) = \min l_{\mathrm{c}}(S)$, где минимум берётся по всем схемам конкатенации, реализующим слово $\tilde{\alpha}$. Величину $l_{\mathrm{c}}(\tilde{\alpha})$ назовём *мультипликативной сложностью* слова (набора) $l_{\mathrm{c}}(\tilde{\alpha})$. Отметим, что схему конкатенации можно рассматривать как схему из функциональных элементов (комбинационную схему) (см., например, [18,22]), имеющую два входа, на которые подаются соответственно 0 и 1, а каждый элемент схемы реализует конкатенацию наборов, подаваемых на его входы. Аналогичным образом можно ввести понятие мультипликативной сложности системы двоичных слов (наборов). Для этого надо потребовать, чтобы в последовательности S содержались все слова из реализуемой системы.

Обозначим через A_n^k множество всех двоичных наборов (слов) длины n, содержащих ровно k единиц. Положим

$$l_{\mathrm{c}}(k, n) = \max_{\tilde{\alpha} \in A_n^k} l_{\mathrm{c}}(\tilde{\alpha}), \quad k = 0, 1, \ldots, n.$$

Очевидно, что при $k = 0$ и при $k = n$ задача о мультипликативной сложности эквивалентна задаче о минимальной длине аддитивной цепочки. Кроме того, как показано в [44], при значениях k, «близких» к $n/2$,

$$l_{\mathrm{c}}(k, n) = \big(1 + o(1)\big)\frac{n}{\log n}.$$

Теорема 3 [8]. *Пусть последовательность пар* (k_m, n_m), $m = 1, 2, \ldots$, *при* $m \to \infty$ *удовлетворяет условиям*

1) $0 \leqslant k_m \leqslant n_m$;
2) $n_m \to \infty$.

Тогда

$$l_{\mathrm{c}}(k_m, n_m) \sim \log n_m + \frac{\log C_{n_m}^{k_m}}{\log\log C_{n_m}^{k_m}}.$$

(*Будем считать, что* $\log x/\log\log x = 0$ *при* $x \leqslant 4$.)

Доказательство. Верхняя оценка. Отметим, что в силу очевидного равенства $l_{\mathrm{c}}(k,n) = l_{\mathrm{c}}(n-k,n)$ можно считать, что $k \leqslant n/2$.

Пусть $\tilde{\alpha}_n^k$ — некоторый набор из множества A_n^k, имеющий наибольшую мультипликативную сложность среди наборов из этого множества, т. е. удовлетворяющий условию $l_{\mathrm{c}}(\tilde{\alpha}_n^k) = l_{\mathrm{c}}(k,n)$. Для набора $\tilde{\alpha}_n^k$ обозначим через n_i, $i = 0, 1, \ldots, k$, число нулей между i-й и $(i+1)$-й единицами. Таким образом,

$$n = \sum_{i=0}^{k} n_i + k.$$

Случай 1. Пусть выполняется неравенство $k \leqslant n^{1/\log\log n}$.

Сведём задачу о верхней оценке сложности порождения слов схемами конкатенации к задаче о верхней оценке сложности вычисления набора степеней одной переменной.

Будем считать, что $n_i > 0$, $i = 0, 1, \ldots, k$. Очевидно, что

$$l_{\mathrm{c}}(\tilde{\alpha}_n^k) \leqslant l(x^{n_0}, x^{n_1}, \ldots, x^{n_k}) + 2k.$$

Используя лемму 4, получаем

$$l_{\mathrm{c}}(k,n) = l_{\mathrm{c}}(\tilde{\alpha}_n^k) \leqslant \log \max_{0\leqslant i\leqslant k} n_i + \frac{\log \prod\limits_{i\colon n_i\neq 0} n_i}{\log\log \prod\limits_{i\colon n_i\neq 0} n_i}\bigl(1+o(1)\bigr) + O(k).$$

Тогда при $k \geqslant 1$ имеем

$$\begin{aligned}
&\frac{\log \prod\limits_{i\colon n_i\neq 0} n_i}{\log\log \prod\limits_{i\colon n_i\neq 0} n_i} \leqslant \frac{\log(n/s)^s}{\log\log(n/s)^s} \leqslant \frac{\log\bigl(n/(k+1)\bigr)^{k+1}}{\log\log\bigl(n/(k+1)\bigr)^{k+1}} \leqslant \\
&\quad\leqslant \frac{\log(n/k)^{k+1}}{\log\log(n/k)^{k+1}} \leqslant \frac{\log(n/k)^{k+1}}{\log\log(n/k)^k} \leqslant \frac{\log(n/k)^k}{\log\log(n/k)^k} + O\left(\frac{\log n}{\log\log n}\right) \leqslant \\
&\quad\leqslant \frac{\log C_n^k}{\log\log C_n^k}\bigl(1+o(1)\bigr) + O\left(\frac{\log n}{\log\log n}\right), \\
&k = \frac{\log k + \log\log(n/k)}{\log n - \log k}\,\frac{\log(n/k)^k}{\log\log(n/k)^k} \leqslant \\
&\quad\leqslant \frac{\log k}{\log n - \log k}\,\frac{\log C_n^k}{\log\log C_n^k}\bigl(1+o(1)\bigr) = o\left(\frac{\log C_n^k}{\log\log C_n^k}\right).
\end{aligned}$$

Поэтому окончательно в условиях случая 1 получаем

$$l_{\mathrm{c}}(k,n) \leqslant \log n\big(1+o(1)\big) + \frac{\log C_n^k}{\log\log C_n^k}\big(1+o(1)\big) =$$
$$= \log n\big(1+o(1)\big) + \frac{\log(n/k)^k}{\log\log(n/k)^k}\big(1+o(1)\big) =$$
$$= \log n\big(1+o(1)\big) + \frac{k\log n}{\log(k\log n)}\big(1+o(1)\big).$$

Случай 2. Пусть выполняется неравенство $n^{1/\log\log n} \leqslant k \leqslant n^{1-1/\log\log n}$. Этот случай достаточно трудный, при его разборе используется специальная техника. Полное доказательство содержится в [8].

Случай 3. Пусть выполняется неравенство $n^{1-1/\log\log n} < k \leqslant n/2$.

Доказательство верхней оценки в этом случае во многом аналогично доказательству асимптотически точной верхней оценки реализации класса булевых (двоичных) матриц с заданной долей единиц (заданной густоты) вентильными схемами глубины 2 (см. [20, теорема 1.4]).

Следуя [20], для произвольного двоичного набора $\tilde\alpha$ обозначим через $I(\tilde\alpha)$ величину $\log C_{|\tilde\alpha|}^{\|\tilde\alpha\|}$, где $|\tilde\alpha|$ — длина набора $\tilde\alpha$, а $\|\tilde\alpha\|$ — число единиц в наборе $\tilde\alpha$.

Пусть $\tau = \tau(k,n)$ и $t = t(k,n)$ — некоторые параметры, удовлетворяющие условиям $\tau < 1$, $t < (1-\tau)\log\log C_n^k$. Точные значения этих параметров укажем позже.

Разобьём исследуемый набор $\tilde\alpha_n^k$ на поднаборы $\tilde\alpha(1), \tilde\alpha(2), \ldots, \tilde\alpha(s)$, «отрезая» слева на i-м шаге, $i = 1, 2, \ldots, s$, кусок $\tilde\alpha(i)$ максимально возможной длины, удовлетворяющий условиям

$$I\big(\tilde\alpha(i)\big) < (1-\tau)\log\log C_n^k, \quad |\tilde\alpha(i)| \leqslant 2^t.$$

Оценим число операций конкатенации, достаточное для реализации системы наборов $\tilde\alpha(1), \tilde\alpha(2), \ldots, \tilde\alpha(s)$. Число различных наборов среди них не превосходит величины $(2^t)^2\, 2^{(1-\tau)\log\log C_n^k}$, так как длина каждого набора, а также и число единиц в наборе, не превосходит 2^t, а число различных наборов фиксированной длины a с фиксированным числом единиц b не превосходит величины $C_a^b < 2^{(1-\tau)\log\log C_n^k}$. Таким образом, учитывая, что для реализации одного набора требуется не более 2^t операций конкатенации, получаем, что сложность реализации системы наборов $\tilde\alpha(1), \tilde\alpha(2), \ldots, \tilde\alpha(s)$ не превосходит величины $(2^t)^3\, 2^{(1-\tau)\log\log C_n^k}$. Но тогда

$$l_{\mathrm{c}}(k,n) = l_{\mathrm{c}}(\tilde\alpha_n^k) \leqslant s + (2^t)^3\, 2^{(1-\tau)\log\log C_n^k}.$$

Оценим сверху величину s. Положим

$$R = \{i \mid 1 \leqslant i \leqslant s,\ |\tilde\alpha(i)| \leqslant 2^t - 1\}.$$

Пусть $i \in R$, т. е. выполняется неравенство $|\tilde\alpha| \leqslant 2^t - 1$. Обозначим $|\tilde\alpha| = a$, $\|\tilde\alpha\| = b$.

Отметим, что в наборе $\tilde{\alpha}(i)$ есть хотя бы один ноль и хотя бы одна единица, так как иначе выполнялись бы соотношения

$$\log C_{a+1}^1 = \log C_{a+1}^a = \log(a+1) \leqslant t < (1-\tau)\log\log C_n^k,$$

что противоречит максимальности набора $\tilde{\alpha}(i)$.

Из соотношений

$$\left(1-\frac{b}{a}\right) C_{a+1}^b \leqslant C_a^b, \quad \frac{b}{a}\, C_{a+1}^{b+1} \leqslant C_a^b$$

следует неравенство

$$\min\left(1-\frac{b}{a}\right) \max\bigl(C_{a+1}^b, C_{a+1}^{b+1}\bigr) \leqslant C_a^b.$$

Поэтому

$$\log\max\bigl(C_{a+1}^b, C_{a+1}^{b+1}\bigr) \leqslant \log C_a^b - \log\min\left(1-\frac{b}{a}\right) \leqslant \log C_a^b + t.$$

С другой стороны, учитывая максимальность набора $\tilde{\alpha}(i)$, получаем, что выполняется неравенство $\max\bigl(C_{a+1}^b, C_{a+1}^{b+1}\bigr) \geqslant (1-\tau)\log\log C_n^k$. Следовательно, если $i \in R$, то справедлива оценка $I\bigl(\tilde{\alpha}(i)\bigr) \geqslant (1-\tau)\log\log C_n^k - t$.

Теперь, с одной стороны, имеем соотношения

$$\sum_{i=1}^{s} I\bigl(\tilde{\alpha}(i)\bigr) \geqslant \sum_{i\in R} I\bigl(\tilde{\alpha}(i)\bigr) \geqslant |R|\bigl((1-\tau)\log\log C_n^k - t\bigr),$$

а с другой, учитывая неравенство $C_{a_1}^{b_1} C_{a_2}^{b_2} \dots C_{a_s}^{s_1} \leqslant C_{a_1+a_2+\dots+a_s}^{b_1+b_2+\dots+b_s}$ (которое получается из сравнения коэффициентов при $x^{b_1+b_2+\dots+b_s}$ в левой и правой частях тождества $(1+x)^{a_1}(1+x)^{a_2}\dots(1+x)^{a_s} = (1+x)^{a_1+a_2+\dots+a_s}$), — соотношения

$$\sum_{i=1}^{s} I\bigl(\tilde{\alpha}(i)\bigr) = \log\Bigl(C_{|\tilde{\alpha}(1)|}^{\|\tilde{\alpha}(1)\|} C_{|\tilde{\alpha}(2)|}^{\|\tilde{\alpha}(2)\|} \dots C_{|\tilde{\alpha}(s)|}^{\|\tilde{\alpha}(s)\|}\Bigr) \leqslant$$

$$\leqslant \log\Bigl(C_{|\tilde{\alpha}(1)|+|\tilde{\alpha}(2)|+\dots+|\tilde{\alpha}(s)|}^{\|\tilde{\alpha}(1)\|+\|\tilde{\alpha}(2)\|+\dots+\|\tilde{\alpha}(s)\|}\Bigr) = \log C_n^k.$$

Следовательно,

$$|R| \leqslant \frac{\log C_n^k}{(1-\tau)\log\log C_n^k - t}.$$

Кроме того, если $i \in R$, то $|\tilde{\alpha}(i)| = 2^t$. Поэтому $s - |R| \leqslant n/2^t$.

Таким образом, окончательно получаем, что

$$l_{\mathrm{c}}(k,n) \leqslant \frac{\log C_n^k}{(1-\tau)\log\log C_n^k - t} + \frac{n}{2^t} + 2^{3t} 2^{(1-\tau)\log\log C_n^k},$$

где $\tau < 1$, $t < (1-\tau)\log\log C_n^k$.

Положим

$$\tau = \left(\frac{3(\log n - \log\log C_n^k) + 4\log\log\log C_n^k}{\log\log C_n^k}\right)^{1/2}, \quad t = \frac{1}{2}\log\frac{n(\log\log C_n^k)^{2/3}}{(\log C_n^k)^{1-\tau/3}}.$$

Тогда в условиях случая 3 имеем оценку

$$l_{\mathrm{c}}(k,n) \leqslant \bigl(1+o(1)\bigr)\frac{\log C_n^k}{\log\log C_n^k}.$$

Верхняя оценка доказана.

Нижняя оценка находится аналогично доказательству нижней оценки сложности вычисления набора степеней путём «объединения» очевидной оценки $l_{\mathrm{c}}(k,n) \geqslant \log n$ и «мощностной» оценки

$$l_{\mathrm{c}}(k,n) \geqslant \bigl(1+o(1)\bigr)\frac{\log C_n^k}{\log\log C_n^k}\bigl(1+o(1)\bigr). \qquad \square$$

4. Обобщения задач Беллмана и Кнута

4.1. Определения

1. Вычисление систем одночленов

Пусть задана система из p нормированных одночленов от q переменных

$$\begin{aligned} f_1 &= x_1^{a_{11}} x_2^{a_{12}} \dots x_q^{a_{1q}}, \\ f_2 &= x_1^{a_{21}} x_2^{a_{22}} \dots x_q^{a_{2q}}, \\ &\dots \\ f_p &= x_1^{a_{p1}} x_2^{a_{p2}} \dots x_q^{a_{pq}}, \end{aligned}$$

описываемая целочисленной матрицей $A = (a_{ij})$ размера $p \times q$. Обозначим через $l_2(y_1, y_2, \dots, y_p)$ (будем использовать также обозначение $l_2(A)$) минимальное число операций умножения, достаточное для вычисления по заданным переменным $x_1, x_2, \dots, x_q$ системы одночленов $\{f_1, f_2, \dots, f_p\}$ (разрешается многократное использование промежуточных результатов вычислений).

Величину $l(A)$ можно также определить на языке аддитивных цепочек. Назовём *векторной аддитивной цепочкой* (см., например, [25, 26, 39, 46]) для целочисленной неотрицательной матрицы $A = (a_{ij})$ размера $p \times q$ последовательность q-мерных векторов (наборов) вида

$$\mathbf{v}_1 = (1,0,\dots,0),\ \mathbf{v}_2 = (0,1,\dots,0),\dots,\ \mathbf{v}_q = (0,0,\dots,1),\ \mathbf{v}_{q+1},\ \mathbf{v}_{q+2},\ \dots,\ \mathbf{v}_{q+r},$$

начинающуюся с q единичных векторов и удовлетворяющую следующим условиям:

1) для каждого k, $q+1 \leqslant k \leqslant q+r$, найдётся два натуральных числа (не обязательно различных) i и j, $1 \leqslant i \leqslant k-1$, $1 \leqslant j \leqslant k-1$, таких что $\mathbf{v}_k = \mathbf{v}_i + \mathbf{v}_j$ (сложение векторов покомпонентное);

2) $\{(a_{11}, a_{12}, \ldots, a_{1q}), (a_{21}, a_{22}, \ldots, a_{2q}), \ldots, (a_{p1}, a_{p2}, \ldots, a_{pq})\} \subseteq \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{q+r}\}$.

Число r называется длиной этой цепочки. Определим *сложность* $l(A)$ матрицы A как минимальную длину векторных аддитивных цепочек для матрицы A.

Величину $l(f_1, f_2, \ldots, f_p)$ (или $l(A)$) можно также интерпретировать как минимально возможную сложность (число элементов) схемы из функциональных элементов или комбинационной схемы (необходимые определения можно найти в [18,22]), на входы которой подаются функции $x_1, x_2, \ldots, x_q$, на выходах схемы вычисляются функции

$$x_1^{a_{11}} x_2^{a_{12}} \ldots x_q^{a_{1q}},\ x_1^{a_{21}} x_2^{a_{22}} \ldots x_q^{a_{2q}}, \ldots,\ x_1^{a_{p1}} x_2^{a_{p2}} \ldots x_q^{a_{pq}}$$

задаваемые целочисленной неотрицательной матрицей наборов показателей степеней A размера $p \times q$, а сама схема состоит из двухвходовых элементов, реализующих произведение функций, подаваемых на входы элемента.

Задача исследования роста величины $l(f_1, f_2, \ldots, f_p)$ поставлена в [41].

2. Аддитивные вычисления целочисленных линейных форм

Пусть задана система из p линейных форм от q переменных

$$\begin{aligned} y_1 &= a_{11}x_1 + a_{12}x_2 + \ldots + a_{1q}x_q, \\ y_2 &= a_{21}x_1 + a_{22}x_2 + \ldots + a_{2q}x_q, \\ &\ldots \\ y_p &= a_{p1}x_1 + a_{p2}x_2 + \ldots + a_{pq}x_q, \end{aligned}$$

определяемая целочисленной матрицей $A = (a_{ij})$ размера $p \times q$. Обозначим через $l_2(y_1, y_2, \ldots, y_p)$ (будем использовать также обозначение $l_2(A)$) минимальное число операций сложения и вычитания, достаточное для вычисления системы линейных форм $\{y_1, y_2, \ldots, y_p\}$ от переменных $x_1, x_2, \ldots, x_q$ (разрешается многократное использование промежуточных результатов вычислений).

Величину $l_2(A)$ можно определить также на языке аддитивных цепочек (см., например, [32, 35, 36, 38, 47]). *Цепочкой из сложений и вычитаний* (*векторов*) для матрицы $A = (a_{ij})$ размера $p \times q$ назовём последовательность q-мерных векторов (наборов) вида

$$\mathbf{v}_1 = (1, 0, \ldots, 0),\ \mathbf{v}_2 = (0, 1, \ldots, 0), \ldots,\ \mathbf{v}_q = (0, 0, \ldots, 1),\ \mathbf{v}_{q+1},\ \mathbf{v}_{q+2},\ \ldots,\ \mathbf{v}_{q+r},$$

начинающуюся с q единичных векторов и удовлетворяющую следующим условиям:

1) для каждого k, $q+1 \leqslant k \leqslant q+r$, найдётся два натуральных числа (не обязательно различных) i и j, $1 \leqslant i \leqslant k-1$ and $1 \leqslant j \leqslant k-1$, таких что $\mathbf{v}_k = \mathbf{v}_i + \mathbf{v}_j$ или $\mathbf{v}_k = \mathbf{v}_i - \mathbf{v}_j$ (сложение и вычитание векторов покомпонентное);
2) $\{(a_{11}, a_{12}, \ldots, a_{1q}), (a_{21}, a_{22}, \ldots, a_{2q}), \ldots, (a_{p1}, a_{p2}, \ldots, a_{pq})\} \subseteq \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{q+r}\}$.

Число r называется длиной цепочки. Определим l_2-*сложность* $l_2(A)$ матрицы A как минимальную длину цепочек из сложения и вычитания для матрицы A.

Величину $l_2(y_1, y_2, \ldots, y_p)$ (или $l_2(A)$) можно также интерпретировать как минимально возможную сложность схемы из функциональных элементов, на входы которой подаются функции $x_1, x_2, \ldots, x_q$, на выходах схемы вычисляются функции

$$a_{11}x_1+a_{12}x_2+\ldots+a_{1q}x_q,\ a_{21}x_1+a_{22}x_2+\ldots+a_{2q}x_q, \ldots,\ a_{p1}x_1+a_{p2}x_2+\ldots+a_{pq}x_q,$$

задаваемые целочисленной матрицей коэффициентов A размера $p\times q$; сама схема состоит из двухвходовых элементов, реализующих сумму или разность функций, подаваемых на входы элемента.

Отметим, что эта задача может быть сформулирована не только в аддитивной, но и в мультипликативной форме. В мультипликативном случае через $l_2(z_1, z_2, \ldots, z_p)$ обозначим минимальное число операций умножения и деления, достаточное для вычисления системы функций

$$z_1 = x_1^{a_{11}}x_2^{a_{12}}\ldots x_q^{a_{1q}},\ z_2 = x_1^{a_{21}}x_2^{a_{22}}\ldots x_q^{a_{2q}}, \ldots,\ z_p = x_1^{a_{p1}}x_2^{a_{p2}}\ldots x_q^{a_{pq}}$$

с целочисленными показателями степеней a_{ij} $(i = 1, 2, \ldots, p,\ j = 1, 2, \ldots, q)$ по данным $x_1, x_2, \ldots, x_q$. Очевидно, что

$$l_2(z_1, z_2, \ldots, z_p) = l_2(A).$$

Задача исследования роста величины $l(y_1, y_2, \ldots, y_p)$ поставлена в [21].

3. Вычисления элементов свободной абелевой группы

Пусть свободная абелева группа G (групповую операцию будем называть умножением) задана конечным множеством свободных образующих $\{x_1, x_2, \ldots, x_q\}$. Тогда произвольная система элементов этой группы

$$\begin{aligned} g_1 &= x_1^{a_{11}}x_2^{a_{12}}\ldots x_q^{a_{1q}},\\ g_2 &= x_1^{a_{21}}x_2^{a_{22}}\ldots x_q^{a_{2q}},\\ &\ldots\\ g_p &= x_1^{a_{p1}}x_2^{a_{p2}}\ldots x_q^{a_{pq}} \end{aligned}$$

определяется целочисленной матрицей $A = (a_{ij})$ размера $p\times q$. Обозначим через $l_{\mathrm{F}}(f_1, f_2, \ldots, f_p)$ (будем также использовать обозначение $l_{\mathrm{F}}(A)$) минимальное число операций умножения, достаточное для вычисления системы элементов $\{g_1, g_2, \ldots, g_p\}$ по множеству $\{x_1, x_1^{-1}x_2, x_2^{-1}, \ldots, x_q, x_q^{-1}\}$, состоящему из образующих и обратных к ним элементов, при этом разрешается многократное использование промежуточных результатов вычислений.

Величина $l_{\mathrm{F}}(A)$ может быть определена также на языке аддитивных цепочек. *Аддитивной F-цепочкой* (см., например, [14, 15]) для целочисленной матрицы $A = (a_{ij})$ размера $p\times q$ назовём последовательность q-мерных векторов (наборов)

вида

$$\mathbf{v}_1 = (1, 0, \ldots, 0),\ \mathbf{v}_2 = (0, 1, \ldots, 0),\ \ldots,\ \mathbf{v}_q = (0, 0, \ldots, 1),$$
$$\mathbf{v}_{q+1} = (-1, 0, \ldots, 0),\ \mathbf{v}_{q+2} = (0, -1, \ldots, 0),\ \ldots,\ \mathbf{v}_{2q} = (0, 0, \ldots, -1),$$
$$\mathbf{v}_{2q+1},\ \mathbf{v}_{2q+2},\ \ldots,\ \mathbf{v}_{2q+r},$$

начинающуюся с $2q$ единичных и противоположных им векторов и удовлетворяющую следующим условиям:

1) для каждого k, $2q+1 \leqslant k \leqslant 2q+r$, найдётся два натуральных числа (не обязательно различных) i и j, $1 \leqslant i \leqslant k-1$, $1 \leqslant j \leqslant k-1$, таких что $\mathbf{v}_k = \mathbf{v}_i + \mathbf{v}_j$ (сложение векторов покомпонентное);
2) $\{(a_{11}, a_{12}, \ldots, a_{1q}), (a_{21}, a_{22}, \ldots, a_{2q}), \ldots, (a_{p1}, a_{p2}, \ldots, a_{pq})\} \subseteq \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2q+r}\}$.

Число r называется длиной этой цепочки. Определим l_{F}-*сложность* $l_{\mathrm{F}}(A)$ матрицы A как как минимальную длину аддитивных F-цепочек для матрицы A.

Величину $l_{\mathrm{F}}(g_1, g_2, \ldots, g_p)$ (или $l_{\mathrm{F}}(A)$) можно также интерпретировать как минимально возможную сложность схемы из функциональных элементов, на входы которой подаются функции $x_1, x_1^{-1}x_2, x_2^{-1}, \ldots, x_q, x_q^{-1}$, на выходах схемы вычисляются функции

$$x_1^{a_{11}} x_2^{a_{12}} \ldots x_q^{a_{1q}},\ x_1^{a_{21}} x_2^{a_{22}} \ldots x_q^{a_{2q}}, \ldots,\ x_1^{a_{p1}} x_2^{a_{p2}} \ldots x_q^{a_{pq}}$$

задаваемые целочисленной матрицей A наборов показателей степеней размера $p \times q$; сама схема состоит из двухвходовых элементов, реализующих произведение элементов группы, подаваемых на входы функциональных элементов.

Задача исследования роста величины $l(f_1, f_2, \ldots, f_p)$ поставлена в [14].

Стоит отметить, что при всем формальном сходстве в определениях, введённые меры сложности l, l_2 и l_{F} существенно отличаются друг от друга.

В данной работе поведение величин $l(A)$, $l_2(A)$ и $l_{\mathrm{F}}(A)$ исследуется в следующей асимптотической постановке. Пусть последовательность $\{A(n) = (a_{ij}(n))\}$ целочисленных $\big(p(n) \times q(n)\big)$-матриц при $n \to \infty$ удовлетворяет условию

$$\max_{a_{ij} \in A(n)} a_{ij} \to \infty.$$

Ставится задача нахождения асимптотического роста функционалов сложности $l(A)$, $l_2(A)$ и $l_{\mathrm{F}}(A)$ при $n \to \infty$.

4.2. Двойственность

Теорема 4 [21, 34, 39]. *Для произвольной неотрицательной целочисленной матрицы A размера $p \times q$ без нулевых строк и столбцов справедливо равенство*

$$l(A) + p = l\big(A^{\mathrm{T}}\big) + q,$$

где A^{T} — матрица, получающаяся из матрицы A транспонированием.

В частности, из теоремы 4 следует, что задача Беллмана эквивалентна задаче Кнута:

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

Теорема 5 [21]. *Для произвольной целочисленной матрицы A размера $p\times q$ справедливы соотношения*

$$-q\leqslant l_2\big(A^{\mathrm{T}}\big)-l_2(T)\leqslant p.$$

Подобные соотношения для величины $l_{\mathrm{F}}(A)$, вообще говоря, неверны. Действительно,

$$l_{\mathrm{F}}\big((2^k,-2^k)\big)=k+1,\quad l_{\mathrm{F}}\big((2^k,-2^k)^{\mathrm{T}}\big)=2k.$$

4.3. Функции Шеннона

В общем виде задача нахождения асимптотики роста величин $l(A)$, $l_2(A)$ и $l_{\mathrm{F}}(A)$ (в случае роста максимума абсолютных величин элементов матрицы) представляется очень трудной задачей. В этом разделе исследуются функции Шеннона для мер сложности l, l_2 и l_{F}.

Положим

$$L(p,q,K)=\max l(A),$$

где максимум берётся по всем целочисленным матрицам $A=(a_{ij})$ размера $p\times q$, удовлетворяющим условиям $0\leqslant a_{ij}\leqslant K-1$, $i=1,\dots,p$, $j=1,\dots,q$. Таким образом, $L(p,q,K)$ — максимум сложностей систем из p одночленов от q переменных по всем системам, в которых все показатели степеней во всех одночленах не превосходят $K-1$.

Теорема 6 [41]. *Пусть $pq\log K\to\infty$. Тогда*

$$L(p,q,K)=\min(p,q)\log K+$$
$$+\frac{pq\log K}{\log(pq\log K)}\left(1+O\left(\left(\frac{\log\log(pq\log K)}{\log(pq\log K)}\right)^{1/2}\right)\right)+O\big(\max(p,q)\big).$$

Положим

$$L_2(p,q,K)=\max l_2(A),$$

где максимум берётся по всем целочисленным матрицам $A=(a_{ij})$ размера $p\times q$, удовлетворяющим условиям $|a_{ij}|\leqslant K-1$, $i=1,\dots,p$, $j=1,\dots,q$. Следовательно, $L_2(p,q,K)$ — наименьшее число операций сложения и вычитания, достаточное для вычисления любой системы из p линейных форм от q переменных с коэффициентами из множества $\{0,\pm1,\dots,\pm(K-1)\}$.

Теорема 7 [5]. *Пусть $pq\log K\to\infty$. Тогда*

$$L_2(p,q,K)=\min(p,q)\log K+$$
$$+\frac{pq\log(2K-1)}{\log(pq\log K)}\left(1+O\left(\left(\frac{\log\log(pq\log K)}{\log(pq\log K)}\right)^{1/2}\right)\right)+O\big(\max(p,q)\big).$$

Отметим, что при доказательстве верхней оценки предложен метод вычисления произвольной системы линейных форм, дающий нужную оценку, при котором используется всего лишь одна операция вычитания.

Положим

$$L_F(p,q,K) = \max l_{\mathrm{F}}(A),$$

где максимум берётся по всем целочисленным матрицам $A = (a_{ij})$ размера $p \times q$, удовлетворяющим условиям $|a_{ij}| \leqslant K-1$, $i = 1,\dots,p$, $j = 1,\dots,q$. Таким образом, $L_F(p,q,K)$ — максимально возможная сложность системы из p элементов свободной абелевой группы с q образующими среди всех систем, у которых в представлении элементов через образующие ни один показатель степени не превосходит по абсолютной величине значения $K-1$.

Теорема 8 [14]. *Пусть $pq\log K \to \infty$. Тогда*

$$L_F(p,q,K) \leqslant \min(p,q+1)\log K + \\ + \frac{pq\log(2K-1)}{\log(pq\log K)}\left(1 + O\left(\left(\frac{\log\log(pq\log K)}{\log(pq\log K)}\right)^{1/2}\right)\right) + O\big(\max(p,q)\big);$$

$$L_F(p,q,K) \geqslant \max\left(\min(p,q+1)\log K,\ \frac{pq\log(2K-1)}{\log(pq\log K)}\right) + O\big(\max(p,q)\big).$$

Указанная в теореме нижняя оценка при одинаковом по порядку росте величин

$$\min(p,\ q+1)\log K \quad \text{и} \quad \frac{pq\log(2K-1)}{\log(pq\log K)}$$

асимптотически не совпадает с верхней оценкой (правда, и отличается асимптотически не более чем в 2 раза). Однако если модифицировать рассуждения случая 2 при доказательстве нижней оценки из [41] с учётом утверждений лемм 1 и 2 из [14], то можно получить оценку

$$L_F(p,q,K) \geqslant \min(p,\ q+1)\log K + \\ + \frac{pq\log(2K-1)}{\log(pq\log K)}\left(1 + O\left(\frac{\log\log(pq\log K)}{\log(pq\log K)}\right)\right) + O\big(\max(p,q)\big).$$

4.4. Универсальная нижняя оценка

Пусть A — матрица размера $p \times q$ с элементами a_{ij}, $i = 1,2,\dots,p$, $j = 1,2,\dots,q$, а число k удовлетворяет неравенствам $1 \leqslant k \leqslant \min(p,q)$. Для наборов индексов $(i_1,i_2,\dots,i_k)$ и $(j_1,j_2,\dots,j_k)$, таких что $1 \leqslant i_1 < i_2 < \dots < i_k \leqslant p$, $1 \leqslant j_1 < j_2 < \dots < j_k \leqslant q$, обозначим через $A(i_1,i_2,\dots,i_k;j_1,j_2,\dots,j_k)$ квадратную матрицу размера k, состоящую из элементов, находящихся на пересечении k строк с номерами $i_1,i_2,\dots,i_k$ и k столбцов с номерами $j_1,j_2,\dots,j_k$.

Положим

$$D(A) = \max_{k:\ 1\leqslant k\leqslant\min(p,q)}\Big(\max_{(i_1,i_2,\dots,i_k;j_1,j_2,\dots,j_k)} |\det A(i_1,i_2,\dots,i_k;j_1,j_2,\dots,j_k)|\Big).$$

Таким образом, $D(A)$ — это максимум абсолютных величин миноров матрицы A, где максимум берётся по всем минорам.

Теорема 9 [9, 10, 12, 15, 37]. *Для любой ненулевой целочисленной матрицы A выполняются соотношения*

$$l(A) \geqslant \log D(A), \quad l_2(A) \geqslant \log D(A), \quad l_{\mathrm{F}}(A) \geqslant \log D(A).$$

4.5. Вычисление систем целочисленных линейных форм

Теорема 10 [10]. *Пусть последовательность целочисленных матриц $A(n) = \big(a_{ij}(n)\big)_{p(n)\times q(n)}$ при $n \to \infty$ удовлетворяет условию*

$$\frac{p+q}{\big(\log\log D(A)\big)^{1/2}} \to 0.$$

Тогда

$$l_2\big(A(n)\big) \sim \log D\big(A(n)\big).$$

Таким образом, при любых фиксированных (и даже слабо растущих) размерах матриц, задающих системы целочисленных линейных форм, верхняя оценка сложности вычисления этой системы аддитивными операциями асимптотически совпадает с универсальной нижней оценкой.

Пусть $A = (a_{ij})_{p\times q}$. Через $l_{\{-\}}(A)$ обозначим наименьшее число операций вычитания, достаточное для вычисления системы из p линейных форм от q переменных с множеством коэффициентов, задаваемым матрицей A.

Положим

$$\varphi = \frac{\sqrt{5}+1}{2}.$$

Теорема 11 [10]. *Пусть последовательность целочисленных матриц $A(n) = \big(a_{ij}(n)\big)_{p(n)\times q(n)}$ при $n \to \infty$ удовлетворяет условию*

$$\frac{p+q}{\big(\log\log D(A)\big)^{1/2}} \to 0.$$

Тогда

$$l_{\{-\}}(A) \sim \log_\varphi D\big(A(n)\big).$$

4.6. Вычисление систем одночленов

Изучение асимптотического поведения величины $l(A)$ в общем случае является достаточно трудной задачей. В настоящее время известна асимптотика роста только для некоторых частных случаев.

Теорема 12 [9, 11]. *Пусть последовательность матриц*

$$A(n) = \big(a_{ij}(n)\big)_{p(n)\times 2}, \quad n = 1, 2, \ldots,$$

с неотрицательными целыми элементами и без нулевых строк при $n \to \infty$ *удовлетворяет условию*

$$\max_{a_{ij} \in A(n)} a_{ij}(n) \to \infty.$$

Тогда

$$\log D\big(A(n)\big) \leqslant l\big(A(n)\big) \leqslant \log D\big(A(n)\big) + o\left(\frac{p(n) \log \max a_{ij}(n)}{\log \log \max a_{ij}(n)}\right).$$

Теорема 13 [12]. *Пусть последовательность матриц*

$$A(n) = \big(a_{ij}(n)\big)_{3\times 3}, \quad n = 1, 2, \ldots,$$

с неотрицательными целыми элементами и без нулевых строк при $n \to \infty$ *удовлетворяет условию*

$$\max_{a_{ij} \in A(n)} a_{ij}(n) \to \infty.$$

Тогда

$$l\big(A(n)\big) \sim \log D\big(A(n)\big).$$

Верхняя оценка, асимптотически совпадающая с нижней оценкой из теоремы 9, была последовательно получена для следующих случаев:

а) матриц размера 2×2;

б) матриц размера $2 \times q(n)$ и матриц размера $p(n) \times 2$ (двойственный случай) при ограниченных или слабо растущих значениях $p(n)$ и $q(n)$;

в) матриц размера 3×3.

Эти результаты естественным образом приводят к предположению о том, что для матриц любого фиксированного размера $p \times q$ в рамках асимптотической постановки задачи справедливо соотношение $l(A) \sim \log D(A)$. Косвенным доводом в пользу справедливости этой гипотезы является результат теоремы 10.

Тем не менее предположение о справедливости асимптотической формулы $l(A) \sim \log D(A)$ для матриц любого фиксированного размера $p \times q$ оказывается неверным уже для матриц размера 4×4: можно привести пример последовательности матриц размера $2t \times 2t$, для которой нижнюю оценку из теоремы 9 можно усилить в $2t/(t+1)$ раз.

Обозначим через $A(t, n)$ матрицу размера $2t \times 2t$, определяемую следующим образом. Первой строкой матрицы $A(t, n)$ является набор длины $2t$, первая половина разрядов которого равна n, а вторая половина — 0. Остальные $2t-1$ строки матрицы $A(t, n)$ получаются из первой строки последовательным циклическим сдвигом на один разряд вправо. Тогда элементы a_{ij} матрицы $A(t, n)$ задаются равенствами

$$a_{ij} = \begin{cases} n, & \text{если } 0 \leqslant j - i \leqslant t - 1 \text{ или } j - i \leqslant -(t+1), \\ 0, & \text{если } j - i \geqslant t \text{ или } -t \leqslant j - i \leqslant -1, \end{cases}$$

$$i = 1, 2, \ldots, 2t, \quad j = 1, 2, \ldots, 2t.$$

Для примера выпишем матрицу $A(t,n)$ при $t=3$:

$$A(3,n)=\begin{pmatrix} n & n & n & 0 & 0 & 0\\ 0 & n & n & n & 0 & 0\\ 0 & 0 & n & n & n & 0\\ 0 & 0 & 0 & n & n & n\\ n & 0 & 0 & 0 & n & n\\ n & n & 0 & 0 & 0 & n \end{pmatrix}.$$

Для удобства договоримся под a_{ij} при $j>2t$ и $1\leqslant i\leqslant 2t$ понимать элемент a_{ir}, где r определяется из условий $1\leqslant r\leqslant 2t$, $r\equiv j\,(\mathrm{mod}\,2t)$. Теперь можно утверждать, что для любого i $(1\leqslant i\leqslant 2t)$ среди элементов a_{ij} и $a_{i,j+t}$ один является нулевым, а другой равен n.

Если аналогичным образом под x_j при $j>2t$ понимать переменную x_r, где r определяется из условий $1\leqslant r\leqslant 2t$, $r\equiv j\,(\mathrm{mod}\,2t)$, то задаваемые матрицей $A(t,n)$ одночлены $f_i=x_1^{a_{i1}}x_2^{a_{i2}}\ldots x_q^{a_{iq}}$, $i=1,2,\ldots,2t$, можно представить следующим образом: $f_i=x_i^n x_{i+1}^n\ldots x_{i+t-1}^n$.

Теорема 14 [16]. *При условии $t=o(\log n)$ справедливо асимптотическое равенство*

$$l\big(A(t,n)\big)\sim 2t\log n.$$

Теорема 15 [16]. *Пусть*

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

Тогда

$$l\big(A(t,n)\big)\sim\frac{2t}{t+1}\log D\big(A(t,n)\big).$$

4.7. Вычисление систем элементов свободных абелевых групп

В общем виде задача нахождения асимптотики роста величины $l_{\mathrm{F}}(A)$ (с ростом, например, максимума абсолютных значений элементов матрицы) представляется очень трудной, заведомо труднее, чем поиск асимптотики роста величины $l_2(A)$, и, по-видимому, труднее, чем поиск асимптотического поведения величины $l(A)$. Так, при некоторых ограничениях эта задача решена для меры сложности l_2 (теорема 10), а для меры сложности l установлена асимптотика в случае, когда выполняется хотя бы одно из условий $p=2$ или $q=2$ (теорема 12), в то время как для меры сложности l_{F} асимптотика роста установлена только для случая $p=2$ и для случая $p=3$, $q=2$.

Отметим также, что для меры сложности l_{F} нижняя оценка из теоремы 9 может быть усилена вдвое:

$$l_{\mathrm{F}}\left((2^k,2^{-k})^{\mathrm{T}}\right)=2\log D\left((2^k,2^{-k})^{\mathrm{T}}\right).$$

Пусть A — целочисленная матрица размера $p\times q$. Положим

$$T(A)=\max_{j\colon 1\leqslant j\leqslant q}\big\{\max\{a_{1j},a_{2j},\ldots,a_{pj},0\}\,|\,\min\{a_{1j},a_{2j},\ldots,a_{pj},0\}|\big\}.$$

Теорема 16 [13]. *Пусть последовательность целочисленных матриц* $A(n) = \big(a_{ij}(n)\big)_{2\times q(n)}$ *при* $n \to \infty$ *удовлетворяет условию*

$$\frac{q(n)}{\log\log \max\limits_{i,j} |a_{ij}(n)|} \to 0.$$

Тогда

$$l_{\mathrm{F}}\big(A(n)\big) \sim \log \max\big\{D\big(A(n)\big), T\big(A(n)\big)\big\}.$$

Пусть матрица A имеет размеры 3×2. Для удобства под a_{st} при $s > 3$ и/или $t > 2$ будем понимать элемент a_{ij}, где i и j определяются из условий $1 \leqslant i \leqslant 3$, $i \equiv s \pmod 3$; $1 \leqslant j \leqslant 2$, $j \equiv t \pmod 2$.

Элемент a_{ij} матрицы A размера 3×2 назовём *особым*, если выполняются следующие условия:

$$a_{ij} \neq 0, \quad a_{ij}a_{i+1,j} \leqslant 0, \quad a_{ij}a_{i+2,j} \leqslant 0, \quad |a_{i+1,j}| + |a_{i+2,j}| \neq 0.$$

Для матрицы A размера 3×2 положим

$$A(s,t) = \begin{pmatrix} a_{s1} & a_{s2} \\ a_{t1} & a_{t2} \end{pmatrix}.$$

Пусть a_{ij} — особый элемент матрицы A размера 3×2. Определим величину $r(a_{ij})$ следующим образом:

1) если выполняются неравенства $\det A(i+1, i+2) \det A(i+2, i) \geqslant 0$ и $\det A(i+1, i+2) \det A(i, i+1) \geqslant 0$, то полагаем

$$r(a_{ij}) = |a_{ij} \det A(i+1, i+2)|;$$

2) если выполняется неравенство $\det A(i+1, i+2) \det A(i+2, i) < 0$, то полагаем

$$r(a_{ij}) = |a_{ij} \det A(i+1, i+2)| \frac{\max\{|a_{i1}|, |a_{i2}|, |a_{i+2,1}|, |a_{i+2,2}|\}}{D\big(A(i+2, i)\big)};$$

3) если выполняется неравенство $\det A(i+1, i+2) \det A(i, i+1) < 0$, то полагаем

$$r(a_{ij}) = |a_{ij} \det A(i+1, i+2)| \frac{\max\{|a_{i1}|, |a_{i2}|, |a_{i+1,1}|, |a_{i+1,2}|\}}{D\big(A(i, i+1)\big)}.$$

Для элементов a_{ij}, не являющихся особыми в целочисленной матрице A размера 3×2, положим $r(a_{ij}) = 0$. Для матрицы A определим величину $R(A)$ равенством

$$R(A) = \max_{a_{ij} \in A} r(a_{ij}).$$

Теорема 17 [15]. *Для произвольной последовательности целочисленных матриц* $A(n) = \big(a_{ij}(n)\big)$ *размера* 3×2, *удовлетворяющей при* $n \to \infty$ *условию*

$$\max_{a_{ij} \in A(n)} |a_{ij}(n)| \to 0,$$

справедливо асимптотическое равенство

$$l_{\mathrm{F}}\big(A(n)\big) \sim \log \max\big\{D\big(A(n)\big), T\big(A(n)\big), R\big(A(n)\big)\big\}.$$

4.8. Соотношения между мерами сложности вычисления систем одночленов

Для любого фиксированного t, $t \geqslant 2$, можно привести пример последовательности матриц размера $2t \times 2t$, для которых сложность вычисления систем одночленов, задаваемых этими матрицами, может быть снижена асимптотически в $2t/(t+1)$ раз в случае, если в вычислениях разрешить использование, помимо переменных, и обратных к ним величин.

Теорема 18 [16]. *При условии $t = o(\log n)$ справедливо асимптотическое равенство*

$$\frac{l\big(A(t,n)\big)}{l_{\mathrm{F}}\big(A(t,n)\big)} \sim \frac{2t}{t+1}.$$

Более того, из теоремы 18 непосредственно вытекает следующий факт.

Следствие 2. *Пусть при $n \to \infty$ выполняются условия $t \to \infty$ и $t = o(\log n)$. Тогда справедливо асимптотическое равенство*

$$\frac{l\big(A(t,n)\big)}{l_{\mathrm{F}}\big(A(t,n)\big)} \sim 2.$$

Существует пример последовательности систем элементов свободной абелевой группы, для которой возможность использования, помимо операции умножения, операции деления приводит к снижению сложности вычисления асимптотически вдвое.

Положим

$$B(k) = \begin{pmatrix} 2^k \\ -2^k \end{pmatrix}.$$

Тогда

$$\frac{l_{\mathrm{F}}\big(B(k)\big)}{l_2\big(B(k)\big)} = \frac{2k}{k+1}.$$

В заключение отметим один любопытный факт, который легко получается с использованием теорем 10 и 15: в отдельных случаях при вычислении систем одночленов использование операции деления может быть более эффективно, чем использование операции умножения.

Теорема 19. *Для любого фиксированного t, $t \geqslant 3$, выполняется неравенство*

$$\lim_{n\to\infty} \frac{l\big(A(t,n)\big)}{l_{\{-\}}\big(A(t,n)\big)} > 1.$$

Работа выполнена при финансовой поддержке РФФИ (проект 14-01-00598).

Литература

[1] Гашков С. Б., Кочергин В. В. Об аддитивных цепочках векторов, вентильных схемах и сложности вычисления степеней // Методы дискрет. анализа в теории графов и сложности. — 1992. — Вып. 52. — С. 22—40.

[2] Кнут Д. Е. Искусство программирования для ЭВМ. Т. 2. — М.: Мир, 1977.

[3] Кочергин В. В. О сложности вычислений в конечных абелевых группах // ДАН СССР. — 1991. — Т. 317, № 2. — С. 291—294.

[4] Кочергин В. В. О сложности вычислений в конечных абелевых группах // Матем. вопр. кибернет. — 1992. — Вып. 4. — С. 178—217.

[5] Кочергин В. В. Об аддитивных вычислениях систем целочисленных линейных форм // Вестн. Моск. ун-та. Сер. 1. Математика, механика. — 1993. — № 6. — С. 97—101.

[6] Кочергин В. В. О вычислении наборов степеней // Дискрет. матем. — 1994. — Т. 6, № 2. — С. 129—137.

[7] Кочергин В. В. О сложности вычислений одночленов и наборов степеней // Дискретный анализ. — Новосибирск: Изд-во Ин-та матем. СО РАН, 1994. — (Тр. РАН. Сиб. отделение. Ин-т матем.; Т. 27). — С. 94—107.

[8] Кочергин В. В. О мультипликативной сложности двоичных слов с заданным числом единиц // Матем. вопр. кибернет. — 1999. — Вып. 8. — С. 63—76.

[9] Кочергин В. В. О сложности вычисления пары одночленов от двух переменных // Дискрет. матем. — 2005. — Т. 17, № 4. — С. 116—142.

[10] Кочергин В. В. Об асимптотике сложности аддитивных вычислений систем целочисленных линейных форм // Дискрет. анализ и исслед. операций. Сер. 1. — 2006. — Т. 13, № 2. — С. 38—58.

[11] Кочергин В. В. О сложности вычисления систем одночленов от двух переменных // Тр. VII Междунар. конф. «Дискретные модели в теории управляющих систем» (Покровское, 4—6 марта 2006 г.). — М.: МАКС Пресс, 2006. — С. 185—190.

[12] Кочергин В. В. О сложности вычисления системы из трёх одночленов от трёх переменных // Матем. вопр. кибернет. — 2006. — Вып. 15. — С. 79—155.

[13] Кочергин В. В. О сложности совместного вычисления двух элементов свободной абелевой группы // Материалы XVI Междунар. школы-семинара «Синтез и сложность управляющих систем» (Санкт-Петербург, 26—30 июня 2006 г.). — М.: Изд-во мех.-мат. ф-та МГУ, 2006. — С. 54—59.

[14] Кочергин В. В. О максимальной сложности совместного вычисления систем элементов свободной абелевой группы // Вестн. Моск. ун-та. Сер. 1. Математика, механика. — 2007. — № 3. — С. 14—19.

[15] Кочергин В. В. О сложности совместного вычисления трёх элементов свободной абелевой группы с двумя образующими // Дискрет. анализ и исслед. операций. Сер. 1. — 2008. — Т. 15, № 2. — С. 23—64.

[16] Кочергин В. В. Об одном соотношении двух мер сложности вычисления систем одночленов // Вестн. Моск. ун-та. Сер. 1. Математика, механика. — 2009. — № 4. — С. 8—13.

[17] Кочергин В. В. Уточнение оценок сложности вычисления одночленов и наборов степеней в задачах Беллмана и Кнута // Дискрет. анализ и исслед. операций. — 2014. — Т. 21, № 6. — С. 51—72.

[18] Лупанов О. Б. О синтезе некоторых классов управляющих систем // Пробл. кибернет. — 1963. — Вып. 10. — С. 63—97.

[19] Мерекин Ю. В. Нижняя оценка сложности для схем конкатенации слов // Дискрет. анализ и исслед. операций. — 1996. — Т. 3, № 1. — С. 52—56.

[20] Нечипорук Э. И. О топологических принципах самокорректирования // Пробл. кибернет. — 1969. — Вып. 21. — С. 5—102.

[21] Сидоренко А. Ф. Сложность аддитивных вычислений семейств целочисленных линейных форм // Зап. науч. сем. ЛОМИ АН СССР. — 1981. — Т. 105. — С. 53—61.

[22] Сэвидж Д. Е. Сложность вычислений. — М.: Факториал, 1998.

[23] Althöfer I. Tight lower bounds on the length of word chains // Inform. Process. Lett. — 1990. — Vol. 34, no. 5. — P. 275—276.

[24] Arnold A., Brlek S. Optimal word chains for the Thue—Morse word // Inform. Comput. — 1989. — Vol. 83, no. 2. — P. 140—151.

[25] Bellman R. E. Addition chains of vectors (Advanced problem 5125) // Amer. Math. Monthly. — 1963. — Vol. 70. — P. 765.

[26] Bernstein D. J. Pippenger's exponentiation algorithm. — 2002. — `http://cr.yp.to/papers/pippenger.pdf`.

[27] Brauer A. On addition chains // Bull. Amer. Math. Soc. — 1939. — Vol. 45. — P. 736—739.

[28] Dobkin D., Lipton R. J. Addition chain methods for the evaluation of specific polynomials // SIAM J. Comput. — 1980. — Vol. 9, no. 1. — P. 121—125.

[29] Downey P., Leong B., Sethi R. Computing sequences with addition chains // SIAM J. Comput. — Vol. 10. — 1981. — P. 638—646.

[30] Erdős P. Remarks on number theory, III: On addition chains // Acta Arith. — 1960. — Vol. 6. — P. 77—81.

[31] Gordon D. M. A survey of fast exponentiation methods // J. Algorithms. — 1998. — Vol. 27. — P. 129—146.

[32] Goundar R. R., Shiota K., Toyonaga M. New strategy for doubling-free short addition-subtraction chain // Appl. Math. Inform. Sci. — 2008. — Vol. 2, no. 2. — P. 123—133.

[33] Hebb K. R. Some results on addition chains // Not. Amer. Math. Soc. — 1974. — Vol. 21. — P. A-294.

[34] Knuth D. E., Papadimitriou C. H. Duality in addition chains // Bull. European Assoc. Theoret. Comput. Sci. — 1981. — Vol. 13. — P. 2—4.

[35] Kunihiro N., Yamamoto H. Window and extended window methods for addition chain and addition-subtraction chain // IEICE Trans. Fundam. Electron. Commun. Comput. Sci. — 1998. — Vol. E81-A, no. 1. — P. 72—81.

[36] Morain F., Olivos J. Speeding up the computation on an eliptic curve using addition-subtraction chains // Inform. Théor. Appl. — 1990. — Vol. 24. — P. 531—544.

[37] Morgenstern J. Note on a lower bound of the linear complexity of the fast Fourier transform // J. Assoc. Comput. Mach. — 1973. — Vol. 20. — P. 305—306.

[38] Nedjah N., Mourelle L. Minimal addition-subtraction chains using genetic algorithm // Advances in Information Systems. — Berlin: Springer, 2002. — (Lect. Notes Comput. Sci.; Vol. 2457). — P. 303—313.

[39] Olivos J. On vectorial addition chains // J. Algorithms. — 1981. — Vol. 2, no. 1. — P. 13—21.

[40] Pippenger N. The minimum number of edges in graphs with prescribed paths // Math. Systems Theory. — 1979. — Vol. 12, no. 4. — P. 325—346.

[41] Pippenger N. On evaluation of powers and monomials // SIAM J. Comput. — 1980. — Vol. 9, no. 2. — P. 230—250.

[42] Schönhage A. A lower bound for the length of addition chains // Theor. Comput. Sci. — 1975. — Vol. 1, no. 1. — P. 1—12.

[43] Southard T. H. Addition chains for the first N squares: Tech. Rep. CNA-84. — Univ. of Texas at Austin, 1974.

[44] Strassen V. Berechnungen in partiellen Algebren endlichen Typs // Computing. — 1973. — Vol. 11. — P. 181—196.

[45] Straus E. G. Addition chains of vectors // Amer. Math. Monthly. — 1964. — Vol. 71. — P. 806—808.

[46] Subbarao M. V. Addition chains — some results and problems // Number Theory and Applications / R. A. Mollin, ed. — Dordrecht: Kluwer Academic, 1989. — (NATO Adv. Sci. Inst. Ser.: Ser. C; Vol. 265). — P. 555—574.

[47] Volger H. Some results on addition/subtraction chains // Inform. Proc. Lett. — 1985. — Vol. 20. — P. 155—160.

[48] Yao A. C.-C. On the evaluation of powers // SIAM J. Comput. — 1976. — Vol. 5. — P. 100—103.