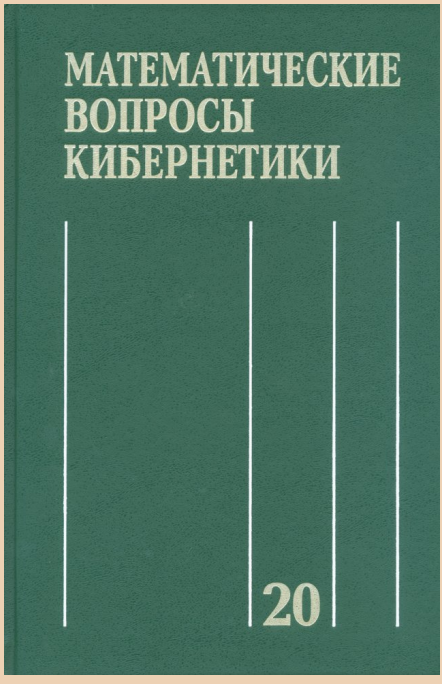
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 20



В. В. Кочергин

Задачи Беллмана, Кнута, Лупанова, Пиппенджера и их вариации как обобщения задачи об аддитивных цепочках

Рекомендуемая форма библиографической ссылки: Кочергин В. В. Задачи Беллмана, Кнута, Лупанова, Пиппенджера и их вариации как обобщения задачи об аддитивных цепочках // Математические вопросы кибернетики. Вып. 20. — М.: ФИЗМАТЛИТ, 2022. — С. 119–256. URL: http://library.keldysh.ru/mvk.asp?id=2022-119 DOI: 10.20948/mvk-2022-119

ЗАДАЧИ БЕЛЛМАНА, КНУТА, ЛУПАНОВА, ПИППЕНДЖЕРА И ИХ ВАРИАЦИИ КАК ОБОБЩЕНИЯ ЗАДАЧИ ОБ АДДИТИВНЫХ ЦЕПОЧКАХ*)

В. В. КОЧЕРГИН

(МОСКВА)

Оглавление

*) На заключительном этапе работа выполнялась при частичной финансовой поддержке Минобрнауки России в рамках реализации программы Московского центра фундаментальной и прикладной математики по соглашению № 075–15–2022–284.

DOI: 10.20948/mvk-2022-119

Введение

Данный текст написан по мотивам обзорного пленарного доклада, сделанного автором на XIX Международной конференции «Проблемы теоретической кибернетики», прошедшей в сентябре 2021 года на базе Казанского (Приволжского) федерального университета.

Отправной точкой является классическая задача о сложности возведения в степень, т. е. задача о нахождении величины $l(x^n)$ — минимального числа операций умножения, достаточного для вычисления по переменной x величины x^n (здесь и везде далее речь идет о так называемых «схемных» вычислениях — результаты промежуточных вычислений могут использоваться многократно). В работе предпринята попытка с единых позиций посмотреть на целый ряд задач, являющихся, с одной стороны, в том или ином смысле обобщениями этой задачи, а с другой — близких по постановке, хотя не всегда эта близость очевидна, и по используемым при их исследовании методам. Следует отметить, что данный обзор ни в коем случае не может претендовать на полноту и в значительной степени отражает научные интересы автора в рассматриваемой тематике. Более того, уже в процессе написания автор стал осознавать, что текст все более и более приобретает черты монографии.

При изучении задачи об эффективном возведении в степень природа переменной x не имеет никакого значения, а от бинарной операции, которую пока называем «умножением», по существу требуется только ассоциативность. В аддитивной постановке эта задача известна (см., например, [24]) как задача об аддитивных цепочках, по которой имеется огромное количество разнообразной литературы. Некоторым аспектам этой задачи, важным для дальнейшего, посвящен § 1.

Следующий параграф посвящен двум естественным обобщениям задачи об эффективном возведении в степень — задаче о сложности вычисления одночлена от m переменных, т. е. нахождения величины $l(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m})$, и задаче о сложности вычисления набора из m степеней одной переменной, т. е. нахождения величины $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$. Первую из этих задач, следуя [177, 188], будем называть *задачей Беллмана*, а вторую, сформулированную в [23, разд. 4.6.3, упр. 32], — *задачей Кнута*. Эти задачи сначала исследовались независимо, но на рубеже 70-х и 80-х годов прошлого века независимо сразу несколькими авторами было установлено, что эти задачи в некотором смысле эквивалентны. Последний факт позволяет говорить об этих двух задачах как об одной *задаче Беллмана — Кнута*.

При переходе от задачи об эффективном вычислении одной степени к задаче Беллмана неявно предполагалось, что операция умножения коммутативна. Модель, в которой используется одна коммутативная операция, будем называть *классической вычислительной моделью*. В случае неперестановочности произведения любых двух различных переменных возникает задача о сложности реализации элементов (слов) свободной полугруппы над алфавитом $\{x_1, x_2, \dots, x_m\}$. В качестве операции «умножения» в этом случае выступает операция конкатенации (склейки) слов, а под сложностью произвольного слова понимается минимальное число операций конкатенации, достаточное для его получения. Задачу нахождения такой сложности называют *задачей о сложности сборки слов схемами конкатенации*. Об этой задаче пойдет речь в § 3.

В § 4 рассматривается еще одна задача, близкая к задаче Беллмана и также имеющая алгебраическую природу. Эта задача может быть сформулирована таким образом. Пусть конечная абелева мультипликативная группа G задана базисом $B=\{a_1, a_2, \ldots, a_q\}$, т. е. группа G раскладывается в прямое произведение циклических подгрупп, порожденных элементами множества B: $G=\langle a_1\rangle\times\langle a_2\rangle\times\ldots\times\langle a_q\rangle$. Сложность $L(g; B)$ элемента g группы G в базисе B определяется как минимальное число операций умножения, достаточное для вычисления элемента g, исходя из элементов базиса B (разрешается многократное использование результатов промежуточных вычислений). Так же, как и в [60, 63], эту задачу и несколько тесно связанных с ней задач будем называть *задачей Лупанова о сложности вычисления элементов конечных абелевых групп*.

В классической вычислительной модели обобщением задач Беллмана и Кнута является *задача Пиппенджера* [177], заключающаяся в нахождении для системы одночленов

$$f_1=x_1^{a_{11}}x_2^{a_{12}}\ldots x_q^{a_{1q}},\quad f_2=x_1^{a_{21}}x_2^{a_{22}}\ldots x_q^{a_{2q}},\quad \ldots,\quad f_p=x_1^{a_{p1}}x_2^{a_{p2}}\ldots x_q^{a_{pq}}$$

сложности $l(f_1, f_2, \ldots, f_p)$ их совместного вычисления, под которой понимается минимально возможное число операций умножения, достаточное для вычисления по переменным $x_1, x_2, \ldots, x_q$ одночленов $f_1, f_2, \ldots f_p$. Понятно, что набор одночленов $f_1, f_2, \ldots f_p$ однозначно задается целочисленной матрицей $A=(a_{ij})$ размера $p\times q$ с неотрицательными коэффициентами без нулевых строк, и поэтому часто в задаче Пиппенджера вместо сложности реализации системы одночленов $f_1, f_2, \ldots f_p$ говорят о *сложности* $l(A)$ *матрицы* A. О различных аспектах задачи Пиппенджера речь идет в § 5.

В следующем параграфе рассматривается вычислительная модель, допускающая помимо операции умножения использование операции деления. В аддитивной постановке, для этой модели особенно естественной, аналог задачи Пиппенджера заключается в нахождении *сложности* $l(y_1, y_2, \ldots, y_p)$ *реализации системы целочисленных линейных форм* $y_i=a_{i1}x_1+a_{i2}x_2+\ldots+a_{iq}x_q$, $i=1, \ldots, p$, численно равной минимальному количеству операций сложения и вычитания, достаточному для получения этой системы по переменным $x_1, x_2, \ldots, x_q$. Такая мера сложности индуцирует меру $l_2(A)$ сложности порождения теперь уже произвольной целочисленной матрицы A. И, забегая вперед, скажем, что в исследовании именно этой меры сложности порождения матриц удалось продвинуться далее всего.

Предметом изучения § 7 является еще одна мера сложности порождения целочисленных матриц, соответствующая следующей вычислительной модели. Как и в классической модели, доступна только (коммутативная) операция умножения, но, помимо переменных, можно использовать и обратные к ним величины. Легко понять, что вычисления в этой модели имеют естественную алгебраическую трактовку как *вычисления систем элементов свободных абелевых групп*. Сложность $l_F(A)$ целочисленной матрицы A определяется как минимальное число операций умножения, достаточное для получения по образующим и обратным к ним элементам свободной абелевой группы системы элементов этой группы, представление через образующие которых задается матрицей A.

Параграф 8 посвящен еще одной мере сложности целочисленных матриц с неотрицательными элементами — сложности реализации *вентильными схемами* (ориентированными графами с предписанным числом путей).

Несмотря на то, что классическая вычислительная модель и модель вентильных схем сильно отличаются, — даже сложность в одной определяется как число операций умножения, а в другой как число ориентированных ребер (вентилей), — у этих моделей наблюдается некое внутреннее единство. Кроме того, в основе многих важных результатов для классической модели лежат результаты из теории вентильных схем.

В центре внимания последнего параграфа находится мера сложности вычисления одночленов в модели, основанной на использовании операции композиции. Операция композиции двух одночленов является обобщением операции умножения. Результатом композиции двух одночленов относительно третьего за счет выбора этого третьего одночлена может быть любой одночлен, у которого по каждой переменной показатель степени не менее показателей степени этой переменной в исходных одночленах и не более суммы этих показателей степеней. Тем самым множество доступных для использования в данной модели операций композиции бесконечно. Эта модель, называемая *схемами композиции*, с точки зрения сложности вычисления систем одночленов (или порождения целочисленных неотрицательных матриц) обладает рядом интересных свойств, которыми не обладают другие модели, или, по крайней мере, аналогичные свойства для других моделей неизвестны. Кроме того, исследования сложности реализации систем одночленов схемами композиции привели к важным продвижениям в классической модели.

§ 1. Задача об эффективном возведении в степень и ее некоторые обобщения

1.1. Задача об аддитивных цепочках. Считается [23], что задачу об эффективном возведении в степень или задачу о нахождении величины $l(x^n)$ — *сложности возведения в степень* n, т. е. минимального числа операций умножения, достаточного для вычисления по переменной x и натуральному n величины x^n, — поставил в 1894 г. Х. Деллак, хотя, по-видимому, еще в древних Египте и Индии был известен «бинарный» метод возведения в степень (см., например, [136]).

Этот метод заключается в следующем. Для возведения в степень n достаточно в двоичной записи числа n отбросить старшую (левую) единицу, заменить все нули на букву К, а единицы на пару букв КУ и применить к переменной x полученное слово таким образом: при считывании слева направо очередного символа в случае появления буквы К текущее значение возводится в квадрат, а в случае буквы У умножается на x. Например, для возведения в степень 100 бинарным методом слева направо двоичную запись 1100100_2 числа 100 преобразуем в «слово» КУККУКК, которому соответствует следующая последовательность вычислений: $x^2, x^3, x^6, x^{12}, x^{24}, x^{25}, x^{50}, x^{100}$. Можно использовать двоичное представление показателя степени для возведения в степень n и так: сначала вычислить все степени, у которых показатели являются степенями двойки, не превосходящими n, а потом перемножить степени, соответствующие единичным разрядам в двоичном представлении числа n. При вычислении x^{100}

получается, например, такая последовательность промежуточных результатов: $x^2, x^4, x^8, x^{16}, x^{32}, x^{64}, x^{96}, x^{100}$. Приведенные способы возведения в степень 100 имеют в некотором смысле двойственную природу. Соображения двойственности будут подробно обсуждаться в следующем параграфе, а пока отметим отличия двух предложенных методов с точки зрения количества ячеек памяти, необходимых при вычислении. В первом случае достаточно хранить текущую степень и саму переменную x, а во втором формально требуется растущее с ростом n число ячеек. Однако у второго способа есть вариант, называемый бинарным методом справа налево, требующий только две ячейки памяти: в одной хранится степень с текущей степенью двойки в показателе, а в другой — текущая «поправка». При получении x^{100} таким способом будет следующая последовательность степеней: x^2, x^4 (при этом x^4 помещается и во вторую ячейку), $x^8, x^{16}, x^{32}, x^{36}, x^{64}, x^{100}$.

Легко понять, что при возведении в n-ю степень любым из вариантов бинарного метода требуется*) $\lfloor \log n \rfloor + \nu(n) - 1$ операций умножения, где $\nu(n)$ — количество единичных разрядов в двоичной записи числа n.

Тем самым бинарный метод дает верхнюю оценку $l(x^n) \leqslant 2\lfloor \log n \rfloor$, которая вместе с нижней оценкой $l(x^n) \geqslant \lfloor \log n \rfloor$, легко доказываемой по индукции с использованием того очевидного факта, что добавление очередной операции увеличивает максимум показателей вычисленных степеней не более чем вдвое, устанавливает порядок роста величины $l(x^n)$ при $n \to \infty$.

Бинарный метод является оптимальным, например, для показателей степени вида $2^s + 2^t$, но в общем случае он не дает минимально возможное число умножений. Так, при возведении в 15-ю степень бинарным методом требуется 6 умножений, в то время как это можно сделать за 5 операций, последовательно вычисляя $x^2, x^4, x^5, x^{10}, x^{15}$. Экономию в одну операцию в этом случае дает использование также давно известного *метода множителей*, заключающегося в возведении в составную степень $n = ts$ путем возведения переменной в степень t с последующим возведением результата в степень s. В случае простого n вычисляется $(n-1)$-я степень переменной x с последующим домножением на x.

Метод множителей по числу операций в среднем лучше бинарного метода (но в отдельных случаях бывает и наоборот), но также, как бинарный метод, как обобщение бинарного метода — m-арный метод, как метод дерева степеней, как метод окон и как все другие известные методы (подробнее об этих методах см., например, [24, 121, 130, 131, 160, 162, 165, 166, 185]), не обеспечивает в общем случае минимально возможное число умножений.

Вообще задача нахождения точного значения величины $l(x^n)$ для произвольного n оказалась очень трудной. Ниже это еще будет обсуждаться, а пока заметим, что неизвестно, существует ли алгоритм полиномиальной сложности для вычисления по n значения $l(x^n)$. В 1939 А. Брауэром [129] для величины $l(x^n)$ при $n \to \infty$ была установлена асимптотическая формула**)

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

*) Здесь и далее запись $\log x$ без указания основания логарифма означает $\log_2 x$.

**) Для функций $f(m)$ и $g(m)$, заданных на множестве натуральных чисел, при $m \to \infty$ запись $f(m) \lesssim g(m)$ означает выполнение условия $\overline{\lim\limits_{m\to\infty}} \frac{f(m)}{g(m)} \leqslant 1$, запись $f(m) \gtrsim g(m)$ — выполнение условия $\underline{\lim\limits_{m\to\infty}} \frac{f(m)}{g(m)} \geqslant 1$ и, наконец, запись $f(m) \sim g(m)$ — выполнение условия $\lim\limits_{m\to\infty} \frac{f(m)}{g(m)} = 1$.

которая вытекает из следующей верхней оценки, которую приведем в силу ее важности с подробным доказательством.

Теорема 1 (А. Брауэр [129]). *Для любых натуральных n и d справедливо неравенство*

$$l(x^n) < \log n + \frac{\log n}{d} + 2^d.$$

Доказательство. Представим число n в системе счисления по основанию 2^d:

$$n = a_0 2^0 + a_1 2^d + a_2 2^{2d} + a_3 2^{3d} + \ldots + a_{s-1} 2^{(s-1)d} + a_s 2^{sd},$$

где $1 \leqslant a_s \leqslant 2^d - 1$ и для $i = 0, 1, \ldots, s-1$ коэффициенты a_i удовлетворяют неравенствам $0 \leqslant a_i \leqslant 2^d - 1$. Отметим справедливость неравенств

$$2^{sd} \leqslant n < 2^{(s+1)d}.$$

Докажем, что выполняется неравенство

$$l(x^n) \leqslant s(d+1) + 2^d - 2.$$

Предъявим даже два способа возведения в n-ю степень с использованием не более $s(d+1) + 2^d - 2$ операций умножения. В основе первого способа лежит метод А. Брауэра [129], в основе второго — метод Э. Ч. Яо [201].

Первый способ. Перепишем представление для n немного по-другому:

$$n = a_0 + 2^d(a_1 + 2^d(a_2 + 2^d(a_3 + 2^d(\ldots(a^{s-1} + 2^d a_s)\ldots)))).$$

Опишем процесс вычисления:

1. Сначала, используя $2^d - 2$ операции, вычисляем следующие степени:

$$x, x^2, x^3, x^4, \ldots, x^{2^d-2}, x^{2^d-1}.$$

Тем самым будут вычислены все степени x^{a_i}, $i = 0, 1, \ldots, a_s$.

2. Возводим x^{a_s} в квадрат d раз и домножаем на $x^{a_{s-1}}$; возводим $x^{a_s 2^d + a_{s-1}}$ в квадрат d раз и домножаем на $x^{a_{s-2}}$; возводим $x^{a_s 2^{2d} + a_{s-1} 2^d + a_{s-2}}$ в квадрат d раз и домножаем на $x^{a_{s-2}}$ и т. д.

Суммарное число операций не превосходит величины $2^d - 2 + s(d+1)$.

Второй способ. На первом этапе, использовав sd операций умножения, путем последовательного возведения в квадрат вычисляем степени

$$x^2,\ x^4,\ \ldots, x^{2^d},\ \ldots,\ x^{2^{2d}},\ \ldots,\ x^{2^{sd}}.$$

Положим

$$u_0 = x^{2^{0d}} = x,\ u_1 = x^{2^d},\ \ldots,\ u_s = x^{2^{sd}}.$$

Отметим, что все степени u_i, $i = 0, 1, \ldots, s$, вычислены на первом этапе.

Для $k = 1, \ldots, 2^d - 1$ положим

$$I_k = \{i \mid a_i = k\}, \quad J_k = \{j \mid a_j \geqslant k\}.$$

Справедливы такие представления вычисляемой степени:

$$x^n = u_0^{a_0} u_1^{a_1} \ldots u_s^{a_s} =$$

$$= \left(\prod_{i \in I_{2^d-1}} u_i\right)^{2^d-1} \left(\prod_{i \in I_{2^d-2}} u_i\right)^{2^d-2} \ldots \left(\prod_{i \in I_1} u_i\right)^1 =$$

$$= \left(\prod_{i \in J_{2^d-1}} u_i\right) \left(\prod_{i \in J_{2^d-2}} u_i\right) \ldots \left(\prod_{i \in J_1} u_i\right).$$

По уже вычисленным степеням $u_0, u_1, \ldots, u_s$ ввиду вложений

$$J_{2^d-1} \subseteq J_{2^d-2} \subseteq \ldots \subseteq J_1$$

произведения

$$\prod_{i \in J_{2^d-1}} u_i, \quad \prod_{i \in J_{2^d-2}} u_i, \quad \ldots, \quad \prod_{i \in J_1} u_i$$

можно последовательно вычислить, используя не более s операций умножения (по одной операции для «присоединения» каждой новой переменной u_i). Для перемножения этих произведений требуется не более $2^d - 2$ операций умножения.

Окончательно для второго способа имеем:

$$l(x^n) \leqslant sd + s + 2^d - 2 = s(d+1) + 2^d - 2.$$

Таким образом, двумя способами доказано нужное неравенство. Из этой оценки ввиду справедливости соотношений $sd \leqslant \log n$ и $s \leqslant (\log n)/d$ получаем оценку

$$l(x^n) < \log n + \frac{\log n}{d} + 2^d.$$

Теорема Брауэра доказана.

Теперь, полагая в теореме Брауэра

$$d = \lfloor \log\log n - 2\log\log\log n \rfloor,$$

при $n \to \infty$ получаем следующую верхнюю оценку на число операций:

$$l(x^n) \leqslant \log n + \frac{\log n}{\log\log n \left(1 - \frac{2\log\log\log n + 1}{\log\log n}\right)} + \frac{\log n}{(\log\log n)^2} =$$
$$= \log n + \frac{\log n}{\log\log n}\left(1 + \frac{2\log\log\log n}{\log\log n} + \frac{2}{\log\log n} + o\left(\frac{1}{\log\log n}\right)\right).$$

На самом деле Брауэр рассматривал задачу не в мультипликативной, а в аддитивной постановке. В 1937 г. А. Шольц [181] переформулировал задачу о нахождении сложности возведения в степень на аддитивном языке, введя понятие аддитивной цепочки. *Аддитивной цепочкой* для натурального числа n называется всякая последовательность целых чисел

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

удовлетворяющая следующему свойству: для каждого k, $1 \leqslant k \leqslant m$, найдутся два целых числа (не обязательно различных) i и j, $0 \leqslant i, j \leqslant k-1$, таких, что $a_k = a_i + a_j$.

Минимальная длина m аддитивной цепочки для n называется *аддитивной сложностью* числа n и обозначается $l(n)$. Очевидно, что величины $l(n)$ и $l(x^n)$ совпадают. В дальнейшем при обсуждении задачи о сложности возведения в степень, а также ее обобщений, будем достаточно часто использовать язык аддитивных цепочек.

Возвращаясь к теореме Брауэра, остановимся на вопросе о точности этой верхней оценки. С одной стороны, как уже говорилось, вместе с почти очевидной нижней оценкой $l(x^n) \geqslant \lfloor \log n \rfloor$ эта теорема устанавливает

при $n \to \infty$ асимптотику роста величины $l(n)$. С другой стороны, если в двоичном представлении числа n единичных разрядов будет $o\left(\frac{\log n}{\log\log n}\right)$, то даже бинарный метод дает верхнюю оценку, существенно лучшую, нежели теорема Брауэра. Принципиальное решение этого вопроса получил в 1960 г. П. Эрдёш. Он показал [143], что для почти всех n справедливо асимптотическое равенство

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

Этот результат имеет существенное значение для дальнейшего, поэтому дадим его точную формулировку. Но сначала отметим, что в определении аддитивной цепочки можно считать, что все входящие в нее числа различны, так как если два числа в цепочке одинаковы, то одно из них может быть опущено. Более того, в произвольной аддитивной цепочке для числа n можно переупорядочить элементы в порядке возрастания и удалить члены, превосходящие n, не нарушая свойств аддитивной цепочки.

Теорема 2 (П. Эрдёш [143]). *Для любого положительного ε найдется такая константа c, $1 < c < 2$, что количество возрастающих аддитивных цепочек для чисел n, $n \leqslant N$, длины не более*

$$\log N + (1-\varepsilon)\frac{\log N}{\log\log N},$$

менее $c^{\log N}$ (и, следовательно, менее N) при всех достаточно больших значениях N.

Тем самым для любого положительного ε доля чисел n, $n \leqslant N$, удовлетворяющих условию

$$l(n) > \log N + (1-\varepsilon)\frac{\log N}{\log\log N},$$

а следовательно, и условию

$$l(n) > \log n + (1-\varepsilon)\frac{\log n}{\log\log n},$$

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

Стоит отметить принципиально разную природу слагаемых в правой части равенства $l(n) = \log n + \frac{\log n}{\log\log n} + o\left(\frac{\log n}{\log\log n}\right)$, справедливом для почти всех значений n. Слагаемое $\log n$ связано с величиной числа n и должно присутствовать для любого значения n, а «мощностное» (отношение логарифма количества чисел, не превосходящих n, к повторному логарифму) слагаемое зависит от «строения» числа n и присутствует для «почти всех» n. Однако, несмотря на то, что для почти всех значений n величина $l(n) - \log n$ достаточно велика, предъявить явным образом бесконечную последовательность таких значений не удается. Конструктивных нижних оценок, которые были бы качественно сильнее неравенства

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

(напомним, что $\nu(n)$ — число единиц в двоичной записи числа n), установленного в 1975 г А. Шёнхаге [182], до сих пор, по-видимому, не получено.

Такая ситуация (принципиальная разница между типичным значением сложности и известными нижними оценками сложности для конкретных представителей) характерна для схемных вычислений (см., например, [91, 97, 108]).

В 1980 г. Н. Пиппенджер получил [177] фундаментальный результат (он будет обсуждаться в §5), который, в частности, следующим образом усиливает нижнюю оценку Эрдёша: найдется такая положительная константа c, что для почти всех n выполняется неравенство

$$\log n + \frac{\log n}{\log\log n} - l(n) \leqslant c\frac{\log n \log\log\log n}{(\log\log n)^2}.$$

В свою очередь, этот результат усилен в работе [61].

Т е о р е м а 3 [61]. *Найдется такая функция $\gamma(n)$, удовлетворяющая условию $\gamma(n) \to 0$ при $n \to \infty$, что доля чисел n, $n \leqslant N$, удовлетворяющих неравенству*

$$\log n + \frac{\log n}{\log\log n} - l(n) \leqslant (2 + \gamma(n))\frac{\log n \log\log\log n}{(\log\log n)^2},$$

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

Таким образом, установлена нижняя оценка, имеющая для почти всех значений n отклонение от величины $\log n + (\log n)/(\log\log n)$ по абсолютной величине асимптотически такое же, как и отклонение в верхней оценке из теоремы Брауэра. При этом следует отметить, что авторы работы [61] ожидали в начале своих исследований по этой теме получить значительно более точную нижнюю оценку величины $l(n)$ для почти всех значений n.

Различным аспектам классической задачи об эффективном вычислении степеней (задачи о длине аддитивных цепочек) посвящено большое число публикаций — см., например, работы [13, 24, 56, 121, 126, 134, 147, 151, 188, 193, 194], являющиеся обзорами или содержащие обзорную часть. Кроме того, в связи с активным применением аппарата аддитивных цепочек в криптографических алгоритмах и других приложениях (см., например, [11, 103, 146]), в последние четверть века объем литературы по этой тематике серьезно увеличился. В значительной части публикаций приводятся разные эвристические алгоритмы возведения в степень (построения аддитивных цепочек), но принципиальных улучшений оценок величины $l(x^n)$, доказанных в середине прошлого века, практически не получено.

Из исследований задачи об аддитивных цепочках в направлениях, не имеющей явной связи с излагаемым далее материалом, стоит отметить опровержение правдоподобной гипотезы о том, что удвоение (степени) очень эффективный шаг, т. е. что $l(2n) = l(n) + 1$. Однако с помощью машинных вычислений установлено, что $l(191) = l(382)$. Более того, установлено [150], что при любом фиксированном натуральном m, не являющемся степенью двойки, величина $l(mn) - l(n)$ может быть сколь угодно большой. Кроме того, также стоит выделить исследования (см., например, обзоры [150, 191]), связанные с до сих пор не доказанной гипотезой Шольца — Брауэра, утверждающей, что $l(2^m - 1) \leqslant m - 1 + l(m)$.

1.2. Некоторые обобщения. Двойственность. В различных криптографических приложениях, в первую очередь в алгоритмах, связанных с быстрыми вычислениями на эллиптических кривых, помимо классических аддитивных цепочек, используется также аппарат цепочек из сложений и вычитаний (см., например, [141, 156, 157, 169, 198]).

Что такое цепочка из сложений и вычитаний, конечно, понятно и без всяких пояснений. Но чтобы, переходя от задачи к задаче, по нескольку раз не давать новых определений, которые незначительно обобщают предыдущие понятия, дадим несколько достаточно общих определений, которые в основном потребуются в последующих параграфах, но будут полезны и сейчас.

Назовем *векторной аддитивной цепочкой* (см., например, [119, 121, 140, 173, 188]) для целочисленной неотрицательной матрицы $A = (a_{ij})$ размера $p \times q$ последовательность q-мерных векторов (наборов) вида

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

начинающуюся с q единичных векторов и удовлетворяющую следующим условиям:

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

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

Число r называется длиной этой цепочки.

Определим *сложность* $l(A)$ матрицы A как минимальную длину векторной аддитивной цепочки для матрицы A.

Задача о поиске сложности целочисленных неотрицательных матриц относительно введенной меры сложности является аддитивным вариантом следующей задачи, поставленной в 1980 г. Н. Пиппенджером [177].

Пусть задана система из p нормированных одночленов от q переменных

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

описываемая целочисленной матрицей $A = (a_{ij})$ размера $p \times q$. Обозначим через $l(f_1, f_2, \ldots, f_p)$ минимальное число операций умножения, достаточное для вычисления по заданным переменным $x_1, x_2, \ldots, x_q$ системы одночленов $\{f_1, f_2, \ldots, f_p\}$ (разрешается многократное использование промежуточных результатов вычислений). Очевидно, что $l(f_1, f_2, \ldots, f_p) = l(A)$. В дальнейшем будем использовать оба этих обозначения.

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 [70, 91, 97]), 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.

Язык схем из функциональных элементов часто бывает удобен при исследовании обсуждаемых задач, и мы им будем пользоваться как для этой, так и для других вычислительных моделей.

Возвращаясь к цепочкам из сложений и вычитаний, отметим, что в мультипликативной постановке их можно интерпретировать как схемы из умножений и делений. Конечно, возможность использования дополнительной базисной операции может уменьшать общее число операций для возведения в степень: например, для возведения в степень $2^k - 1$ достаточно k умножений и одного деления, в то время как при использовании только умножений в силу нижней оценки Шёнхаге потребуется не менее $k + \log k - 2{,}13$ операций. Однако мощностные нижние оценки из работ [143] и [61] остаются справедливыми и в вычислительной модели с двумя операциями.

Если же рассматривать задачу об эффективном возведении в степень для вычислительной модели с одной операцией, но с операцией деления, а не с операцией умножения, асимптотика роста минимально возможного количества операций для возведения в n-ю степень будет другая. Нетрудно показать, что для этого потребуется не менее $\log_\varphi n$ делений, при этом верхняя оценка числа делений, как показано в [36, 51, 53], имеет вид

$$\log_\varphi n + \frac{\log n}{\log\log n}\left(1 + O\left(\frac{\log\log\log n}{\log\log n}\right)\right).$$

Теперь, возвращаясь к классической задаче возведения в степень, т. е. к обычным аддитивным цепочкам, объясним, почему для теоремы Брауэра приведено по сути два доказательства. Это сделано для того, чтобы проиллюстрировать соображения двойственности (дуальности), имеющие большое значение и для самой задачи об аддитивных цепочках, и для многих, но, правда, не всех ее обобщений. Два доказательства теоремы Брауэра при всех принципиальных отличиях на самом деле имеют одинаковую структуру, только в некотором смысле продвижение по этой структуре в методах Брауэра и Яо идет в противоположных направлениях.

Принцип двойственности (свойство двойственности, принцип транспонирования) является достаточно универсальным и в той или иной степени применим во многих вычислительных задачах. В частности, он используется при построении автоморфизмов конечных полей (см., например, [153]), при интерполяции многочленов (см., например, [125]), при построении схем для градиента рациональной функции [9, 99], при минимизации глубины формул и схем [8].

Касательно задач, обсуждаемых в настоящей работе, история принципа двойственности (или иначе — теоремы о дуальности, леммы о транспонировании), по-видимому, восходит к работам 1956 года О. Б. Лупанова [66] и, быть может, Дж. Бордевийка [127]. Интересный, но неоднозначный исторический обзор с критическим разбором многочисленных случаев переоткрывания принципа двойственности, которые продолжаются и поныне, содержится в [122].

Двойственность задачи Пиппенджера можно извлечь из более общего варианта принципа двойственности, предложенного в 1973 г. Ч. Фиддучиа [144]. В 1981 г. независимо А. Ф. Сидоренко [101], а также Д. Кнут

и К. Пападимитриу [155] в явном виде установили двойственность задачи Пиппенджера: сложность системы одночленов $\{f_1, f_2, \ldots, f_p\}$ от q переменных, заданной матрицей $A=(a_{ij})$ размера $p\times q$, и сложность двойственной системы одночленов $\{\widehat{f}_1, \widehat{f}_2, \ldots, \widehat{f}_q\}$ от p переменных, заданной транспонированной матрицей $A^T=(a_{ji})$ размера $q\times p$, для любой матрицы A без нулевых строк и столбцов связаны соотношением

$$l(f_1, f_2, \ldots, f_p)+p=l(\widehat{f}_1, \widehat{f}_2, \ldots, \widehat{f}_q)+q.$$

Различные варианты принципа двойственности также содержатся в работах [9–11, 83, 173, 197].

Для того, чтобы привести, по-видимому, самое простое из известных доказательств принципа двойственности для задачи Пиппенджера, определим еще одну вычислительную модель — вентильные схемы с кратными путями или графы с предписанным числом путей (см., например, [52, 55, 175]). Про эту и близкие модели подробнее речь пойдет в § 8.

Пусть $A=(a_{ij})$ — целочисленная матрица размера $p\times q$ с неотрицательными элементами. Ориентированный граф S без ориентированных циклов будем называть *вентильной схемой с кратными путями* (или *вентильной схемой с предписанным числом путей*), *реализующей матрицу* A, если: в S выделено p вершин — входных полюсов и q вершин — выходных полюсов; в S нет ориентированных путей от одного входа к другому, от одного выхода к другому, от выхода к входу; для любой пары (i, j), $1\leqslant i\leqslant p$, $1\leqslant j\leqslant q$, число ориентированных путей к i-му выходу от j-го входа равно в точности a_{ij}. Число ребер (вентилей) в схеме S назовем *сложностью вентильной схемы* S и обозначим через $l^{\text{кр}}_{\text{вс}}(S)$. *Сложностью реализации матрицы* A *вентильными схемами с кратными путями* назовем величину $l^{\text{кр}}_{\text{вс}}(A)=\min l^{\text{кр}}_{\text{вс}}(S)$, где минимум берется по всем схемам, реализующим матрицу A.

Т е о р е м а 4 (принцип двойственности для задачи Пиппенджера). *Для любой целочисленной матрицы A с неотрицательными элементами размера $p\times q$ без нулевых строк и столбцов выполняется равенство*

$$l(A)+p=l\left(A^T\right)+q,$$

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

Д о к а з а т е л ь с т в о. Пусть S — минимальная схема из элементов умножения, имеющая q входов, которым приписаны переменные $x_1, x_2, \ldots, x_q$, и p выходов, на которых реализуются одночлены $f_1, f_2, \ldots, f_p$, где $f_i=x_1^{a_{i1}}x_2^{a_{i2}}\ldots x_q^{a_{iq}}$, $i=1, 2, \ldots, p$.

Индукцией по номеру элемента в некоторой естественной (правильной) нумерации всех элементов схемы S легко установить, что если в вершине v схемы S вычисляется некоторый одночлен $x_1^{b_1}x_2^{b_2}\ldots v_q^{b_q}$, то для $j=1, 2, \ldots, q$ от j-го входа к вершине v ведет в точности b_j различных путей. Тем самым граф схемы S является вентильной схемой с кратными путями с q входами и p выходами, реализующей матрицу A. Обозначим эту вентильную схему через $S_{\text{вс}}$, а количество невходовых вершин схемы $S_{\text{вс}}$ через $V_+(S_{\text{вс}})$. В каждый элемент схемы S входят два ребра, поэтому при переходе от схемы S из элементов умножения к вентильной схеме $S_{\text{вс}}$ сложность, определяемая

сначала как число элементов умножения или число невходовых вершин, а потом как число ребер, увеличится на число невходовых вершин, т. е.

$$l^{\text{кр}}_{\text{вс}}(S_{\text{вс}}) = l(S) + V_+(S_{\text{вс}}).$$

Теперь в вентильной схеме $S_{\text{вс}}$ поменяем направления всех вентилей на противоположные. Получившуюся вентильную схему с кратными путями обозначим через $S^T_{\text{вс}}$. Очевидно, что вентильная схема $S^T_{\text{вс}}$ имеет p входов и q выходов, реализует матрицу A^T и для ее сложности выполняется равенство $l^{\text{кр}}_{\text{вс}}(S^T_{\text{вс}}) = l^{\text{кр}}_{\text{вс}}(S_{\text{вс}})$.

Наконец, перестроим вентильную схему $S^T_{\text{вс}}$ в схему S^T из элементов умножения, применяя следующие правила преобразования:

1) если в вершину v вентильной схемы $S^T_{\text{вс}}$ входит ровно один вентиль, то удаляем этот вентиль, а вершину v отождествляем с вершиной, из которой выходил этот вентиль;

2) если в вершину v вентильной схемы $S^T_{\text{вс}}$ входит ровно k вентилей, $k \geqslant 2$, то заменяем вершину v со входящими в нее вентилями на $k-1$ элемент умножения.

В схеме из элементов умножения S^T, имеющей p входов и q выходов, сохраняется следующее свойство вентильной схемы $S^T_{\text{вс}}$: для любой пары (i, j), $1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant q$, число ориентированных путей к j-му выходу от i-го входа равно в точности a_{ij}. Следовательно, схема S^T реализует систему одночленов, задаваемую матрицей A^T. Кроме того, справедливо равенство

$$l(S^T) = l^{\text{кр}}_{\text{вс}}(S^T_{\text{вс}}) - V_+(S^T_{\text{вс}}),$$

где $V_+(S^T_{\text{вс}})$ — количество невходовых вершин вентильной схемы $S^T_{\text{вс}}$.

Учитывая равенство $V_+(S_{\text{вс}}) - V_+(S^T_{\text{вс}}) = p - q$, окончательно получаем:

$$l(A^T) \leqslant l(S^T) = l^{\text{кр}}_{\text{вс}}(S^T_{\text{вс}}) - V_+(S^T_{\text{вс}}) = l^{\text{кр}}_{\text{вс}}(S_{\text{вс}}) - V_+(S^T_{\text{вс}}) = \\ = l(S) + V_+(S_{\text{вс}}) - V_+(S^T_{\text{вс}}) = l(A) + p - q.$$

Аналогично доказывается, что $l(A) = l\left((A^T)^T\right) \leqslant l(A^T) + q - p$.

Теорема 4 доказана.

Теперь, установив связь между схемами умножения и вентильными схемами с кратными путями, нетрудно показать, что вентильные схемы с одним входом и одним выходом, соответствующие схемам умножения, построенным для возведения в степень методами Брауэра и Яо, получаются друг из друга путем изменения направлений всех вентилей на противоположные.

§ 2. Задача Беллмана — Кнута

В этом параграфе речь пойдет о двух, наверное, самых естественных обобщениях задачи об эффективном возведении в степень.

В 1963 г. Р. Беллман [119] (для случая $m = 2$), а затем в 1964 г. Е. Штраус [187] (для произвольного m) сформулировали задачу о сложности вычисления одночлена от m переменных т. е. нахождения величины $l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m})$. В дальнейшем эту задачу, следуя [177, 188], будем называть *задачей Беллмана*, хотя логичнее было бы ее называть задачей

Беллмана — Штрауса. Формально на языке аддитивных цепочек величина $l(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m})$ определяется как минимально возможная длина r последовательности m-мерных векторов (наборов)

$$\boldsymbol{v}_1=(1,0,\dots,0),\ \boldsymbol{v}_2=(0,1,\dots,0),\ \dots,\ \boldsymbol{v}_m=(0,0,\dots,1),$$
$$\boldsymbol{v}_{m+1},\boldsymbol{v}_{m+2},\dots,\boldsymbol{v}_{m+r}=(n_1,n_2,\dots,n_m),$$

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

В 1969 г. Д. Кнут [23, разд. 4.6.3., упр. 32] поставил задачу о сложности вычисления m степеней одной переменной, т. е. нахождения величины $l(x^{n_1},x^{n_2},\dots,x^{n_m})$. Эту задачу обычно называют (см., например, [174]) *задачей Кнута*. Очевидно, что величина $l(x^{n_1},x^{n_2},\dots,x^{n_m})$ численно равна минимально возможной длине аддитивной цепочки для какого-либо числа n_i (например, для максимального из чисел $n_1,\dots,n_m$), содержащей при этом все остальные числа из множества $\{n_1,\dots,n_m\}$.

Отметим, что задачи Беллмана и Кнута, являясь обобщениями задачи об эффективном возведении в степень, в свою очередь, являются частными случаями поставленной несколько позже задачи о сложности вычисления системы из p одночленов от q переменных, о которой уже упоминалось и пойдет речь в § 5.

В 1964 г. Е. Штраус [187] показал, что для любого фиксированного m при $\sum n_i\to\infty$ справедлива асимптотическая формула

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

В 1976 г. А. Яо [201] для любого фиксированного m при $\sum n_i\to\infty$ установил аналогичную формулу для сложности вычисления набора из m степеней:

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

Верхняя оценка Штрауса получается естественным обобщением метода Брауэра, а верхнюю оценку Яо нетрудно восстановить по доказательству теоремы Брауэра методом Яо.

Как уже упоминалось, в 1981 г. независимо А. Ф. Сидоренко [101], Дж. Оливосом [173], а также Д. Кнутом и К. Пападимитриу [155] было явно установлено, что в действительности задачи о сложности вычисления одночлена от m переменных и набора m степеней двойственны (эквивалентны) — эти две величины сложности связаны равенством

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

и, следовательно, это по сути одна задача, которую естественно называть *задачей Беллмана — Кнута*.

Также в 1981 г. в работе [139] установлено, что задача распознавания по набору натуральных чисел $(n_1,n_2,\dots,n_m,l)$ существования аддитивной цепочки, имеющей длину l и содержащей числа $n_1,n_2,\dots,n_m$, при $m\geqslant 2$ является NP-полной. В связи с этим для задач Беллмана

и Кнута говорить о нахождении точного значения сложности не приходится. Поэтому естественно рассматривать эти задачи в асимптотической постановке — в этом случае требуется предложить такой метод вычисления одночлена $x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}$ или набора степеней $x^{n_1}, x^{n_2}, \dots, x^{n_m}$, при котором число используемых операций умножения в том или ином смысле близко к значению $l(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m})$ или $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$ соответственно; например, такой метод, что отношение числа операций умножения к значению $l(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m})$ или $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$ стремится к 1 при $(n_1 + n_2 + \dots + n_m) \to \infty$ для всех или «почти всех» наборов $(n_1, n_2, \dots, n_m)$.

Как уже было отмечено, при фиксированном m (числе переменных в одночлене или числе вычисляемых степеней соответственно) для задач Беллмана и Кнута асимптотически точное решение было найдено. Вопрос об асимптотике роста сложности в случае растущего числа переменных (степеней) долгое время оставался открытым. В этом направлении можно отметить, пожалуй, лишь два результата.

Первый получил Т. Соузард [184] — он установил асимптотику роста сложности вычисления набора степеней для одного частного случая, упоминавшегося Д. Кнутом при постановке общей задачи, когда набор показателей степеней является последовательностью квадратов идущих подряд, начиная с единицы, натуральных чисел:

$$l\left(x^{1^2}, x^{2^2}, \dots, x^{m^2}\right) \sim m$$

при $m \to \infty$.

Второй результат, полученный в 1976 г. Н. Пиппенджером [174], заключается в следующем асимптотическом равенстве:

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

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

Существенное продвижение в вопросе получения асимптотики сложности для задачи Беллмана — Кнута при растущем числе переменных или степеней получено в 1992 г. С. Б. Гашковым и автором [10] на базе основного результата работы [31]. И так же, как при доказательстве двойственности в задаче Пиппенджера, при получении этого результата важнейшую вспомогательную роль сыграли вентильные схемы с кратными ребрами, правда, в данном случае реализуемые ими матрицы — булевы, т. е. количество путей от произвольного входа к любому выходу равно либо 0, либо 1. В § 8 будет дан достаточно подробный обзор результатов по теории вентильных схем, а сейчас воспользуемся одним фактом из этого обзора.

Пусть $A = (a_{ij})$ — булева матрица размера $p \times q$. Для $j = 1, 2, \dots, q$ обозначим через p_j наибольший номер среди ненулевых элементов j-го столбца матрицы A. Таким образом,

$$p_j = \max\{i \mid a_{ij} \neq 0\}, \quad j = 1, 2, \dots, q.$$

Положим

$$H(A) = \sum_{j=1}^{q} p_j.$$

Отметим, что в матрице A среди pq элементов не менее $pq-H(A)$ элементов нулевые.

Сформулируем доказанное автором [30, 31] с использованием результатов Пиппенджера [174, 175], существенно опирающихся, в свою очередь, на работы [66, 85, 89], утверждение в виде леммы.

Лемма 1 [30,31]. *Для произвольной последовательности булевых матриц $A(n)$ размера $p(n)\times q(n)$, удовлетворяющей при $n\to\infty$ условию $H(A(n))\to\infty$, справедливо неравенство*

$$l^{кр}_{Вс}(A)\leqslant\frac{H(A(n))}{\log H(A(n))}\left(1+O\left(\left(\frac{\log\log H(A(n))}{\log H(A(n))}\right)^{1/2}\right)\right)+O(p+q).$$

На основе этого утверждения будем доказывать верхнюю оценку сложности для задачи Беллмана — Кнута.

Учитывая равенство

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

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

Сопоставим произвольному набору $\widetilde{n}=(n_1,\ldots,n_m)$ таблицу $T_{\tilde{n}}$ из m булевых столбцов, вообще говоря, неодинаковой высоты, где i-й столбец является двоичной записью числа n_i (младший разряд расположен в первой строке). Доопределим таблицу $T_{\tilde{n}}$ нулями до матрицы размера $\lceil\log(\max n_i+1)\rceil\times m$. Полученную матрицу обозначим через $A(T_{\tilde{n}})$. Тогда $H(A(T_{\tilde{n}}))=\sum\limits_{i=1}^{m}\lceil\log(n_i+1)\rceil$.

Оценим сверху сложность вычисления одночлена $x_1^{n_1}x_2^{n_2}\ldots x_m^{n_m}$ через сложность реализации вентильными схемами матрицы $A(T_{\tilde{n}})$.

Лемма 2. *Для любого набора натуральных чисел $n_1,n_2,\ldots,n_m$, выполняется неравенство*

$$l(x_1^{n_1}x_2^{n_2}\ldots x_m^{n_m})\leqslant l^{кр}_{Вс}(A(T_{\tilde{n}}))+2\lceil\log(\max n_i+1)\rceil-2.$$

Доказательство. Пусть $n_m=\max(n_1,n_2,\ldots,n_m)$. Преобразуем произвольную минимальную вентильную схему, реализующую матрицу $A(T_{\tilde{n}})$, в схему из двухвходовых элементов умножения следующим образом.

Припишем j-му входу вентильной схемы переменную x_j, $j=1,\ldots,m$. Пронумеруем все невходовые вершины вентильной схемы так, чтобы не оказалось путей от вершин с бóльшими номерами к вершинам с меньшими. В порядке возрастания номеров каждую такую вершину вместе со всеми входящими в нее вентилями-ребрами (а их в силу минимальности вентильной схемы для любой вершины, не являющейся выходом, должно быть не менее двух) заменим соответствующим образом на цепочку двухвходовых элементов умножения — если в вершину вентильной схемы входило ровно r ребер, то эту вершину вместе с входящими в нее ребрами заменяем на цепочку из $r-1$ двухвходового элемента умножения. Если в i-й выход исходной вентильной схемы входит более одного ребра, то i-м выходом схемы из элементов умножения объявляем последний элемент цепочки элементов

умножения, заменивший i-й выход вентильной схемы. Если в i-й выход исходной вентильной схемы входит ровно одно ребро, то i-м выходом схемы из элементов умножения объявляем последний элемент цепочки элементов умножения, полученной при преобразовании той вершины исходной вентильной схемы, из которой выходило единственное ребро, ведущее в i-й выход, при этом ребро удаляется.

Обозначим одночлен, вычисляемый i-м выходом полученной на предыдущем этапе схемы, $i=1,\ldots,\lceil\log(n_m+1)\rceil$, через h_i. Последняя часть схемы из элементов умножения последовательно вычисляет одночлены

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

В силу построения справедливо равенство

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

а число используемых умножений в построенной схеме не превосходит величины

$$L_{01}(A(T_{\tilde n}))+2\lceil\log(n_m+1)\rceil-2.$$

Лемма 2 доказана.

Положим

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

Т е о р е м а 5 [35]. *Для любой последовательности наборов натуральных чисел* $\tilde n(k)=\big(n_1(k),n_2(k),\ldots,n_{m(k)}(k)\big)$, $k=1,2,\ldots$, *удовлетворяющей условию*

$$\sum_{i=1}^{m(k)} n_i(k)\to\infty,$$

выполняется неравенство

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

где $N=n_1n_2\ldots n_m$.

Д о к а з а т е л ь с т в о. Пусть $n_m=\max(n_1,n_2,\ldots,n_m)$. Используя леммы 2 и 1, получаем:

$$l(x_1^{n_1}x_2^{n_2}\ldots x_m^{n_m})\leqslant\frac{H(A(T_{\tilde n}))}{\log H(A(T_{\tilde n}))}\left(1+O\left(\left(\frac{\log\log H(A(T_{\tilde n}))}{\log H(A(T_{\tilde n}))}\right)^{1/2}\right)\right)+$$
$$+O(m+\log n_m)\leqslant$$

$$\leqslant\left(\frac{\log\prod_{i=1}^m n_i}{\log\log\prod_{i=1}^m n_i}+m\right)\left(1+O\left(\left(\frac{\log\log\log\prod_{i=1}^m(n_i+1)}{\log\log\prod_{i=1}^m n_i}\right)^{1/2}\right)\right)+$$
$$+O(m+\log n_m)\leqslant$$

$$\leqslant \frac{\log N}{\log\log N}\left(1+O\left(\left(\frac{\log\log\log N}{\log\log N}\right)^{1/2}\right)\right)+O(m+\log n_m).$$

Теорема 5 доказана.

Теперь перейдем к доказательству того факта, что в верхней оценке из теоремы 5 слагаемое $O(\log n_m)$ можно заменить на $(1+o(1))\log n_m$.

Лемма 3. *При любом натуральном t справедливо неравенство*

$$l(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m})\leqslant \log\max n_i+\log N/t+2^t m,$$

где $N=n_1n_2\dots n_m$.

Доказательство. Пусть $n_m=\max(n_1,n_2,\dots,n_m)$. Представим одночлен $x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}$ в следующем виде:

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

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

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

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

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

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

Лемма 3 доказана.

Теперь можно перейти доказательству верхней оценки, установленной С. Б. Гашковым и автором в 1992 г.

Теорема 6 [10]. *Для любой последовательности наборов натуральных чисел $\widetilde{n}(k)=\big(n_1(k),n_2(k),\dots,n_{m(k)}(k)\big)$, $k=1,2,\dots$, удовлетворяющей условию*

$$\sum_{i=1}^{m(k)}n_i(k)\to\infty,$$

выполняется неравенство

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

где $N=n_1n_2\dots n_m$.

Доказательство. Без ограничения общности будем считать, что выполняются неравенства $n_1\leqslant n_2\leqslant\dots\leqslant n_m$. Утверждение теоремы в случае, когда величина n_m ограничена, очевидно. Далее будем считать, что $n_m\to\infty$.

Положим

$$R=\sum_{i=1}^{m}\log n_i=\log N;\qquad R_2(k)=\sum_{i=k+1}^{m}\log n_i,\quad k=0,1,\ldots,m.$$

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 найдется и будет отлично от 0 и m, так как

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

Введем обозначения: $m_2=m-m_1$, $R_1=\sum\limits_{i=1}^{m_1}\log n_i$, $R_2=R_2(m_1)$. Очевидно, что выполняется равенство $R=R_1+R_2$.

Из теоремы 5 следует, что

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

$$\leqslant\frac{R_1}{\log R_1}\left(1+O\left(\left(\frac{\log\log R_1}{\log R_1}\right)^{1/2}\right)\right)+O\left(m+\frac{R_2}{(\log R_2)^2}\right),$$

а в силу леммы 3 при $t=\lceil\log R_2-4\log\log R_2\rceil$ имеем:

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

Так как

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

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

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

Складывая полученные оценки и применяя неравенство Йенсена $f(x_1)+f(x_2)\leqslant 2f\left((x_1+x_2)/2\right)$, справедливое для выпуклой (при $x\geqslant x_0$ для некоторого x_0) вверх функции, получаем, что при $R_i\geqslant x_0$, $i=1,2$, и $R\to\infty$ справедливы соотношения

$$l(x_1^{n_1}x_2^{n_2}\ldots x_m^{n_m})\leqslant l(x_1^{n_1}x_2^{n_2}\ldots x_{m_1}^{n_{m_1}})+l(x_{m_1+1}^{n_{m_1+1}}\ldots x_m^{n_m})+1\leqslant$$

$$\leqslant\log n+\frac{R_1+R_2}{\log\frac{R_1+R_2}{2}}\left(1+O\left(\left(\frac{\log\log\frac{R_1+R_2}{2}}{\log\frac{R_1+R_2}{2}}\right)^{1/2}\right)\right)+O\left(m+\frac{R}{(\log R)^2}\right)=$$

$$= \log n + \frac{R}{\log R}\left(1 + O\left(\left(\frac{\log\log R}{\log R}\right)^{1/2}\right)\right) + O(m).$$

Эта оценка остается справедливой и в случае, когда $R_1 < x_0$ или $R_2 < x_0$. Теорема 6 доказана.

Верхняя оценка из теоремы 6 вместе с простыми нижними оценками

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

$$l(x_1^{n_1}, x^{n_2}, \dots, x^{n_m}) \geqslant \log(\max n_i),$$

справедливыми для всех наборов $(n_1, n_2, \dots, n_m)$, а также с «мощностной» нижней оценкой (см., например, [70]), дают асимптотику роста сложности в задачах Беллмана и Кнута для «почти всех» наборов при достаточно широком диапазоне соотношения параметров. Однако в случае, когда величины $\log(\max n_i)$ и $\frac{\log N}{\log\log N}$ имеют одинаковый порядок роста, эти нижние оценки не совпадают асимптотически с верхней.

В 1994 г. в работе [32] удалось восполнить это пробел, в некотором смысле объединив в одну нижнюю оценку «мощностную» оценку и оценку через $\log(\max n_i)$.

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

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

Т е о р е м а 7 [32]. *Существуют такие положительная константа c и функция $f(x)$, стремящаяся к 0 при $x \to \infty$, что для любой последовательности наборов*

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

различных натуральных чисел, удовлетворяющей при $s \to \infty$ условию

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

доля наборов $(k_1, k_2, \dots, k_m)$ из $\mathfrak{M}\left(\widetilde{n}(s)\right)$, для которых выполняются соотношения

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

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

Доказательство этой теоремы, являющейся обобщением результатов из [61, 143], ввиду громоздкости и значительных технических трудностей здесь не приводится.

Замечание 1. В формулировке теоремы 7 можно положить

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

Замечание 2. Теорема 7 остается справедливой, если рассматривать доли наборов не из множества $\mathfrak{M}\left(\widetilde{n}(s)\right)$, а из множества $\mathfrak{N}\left(\widetilde{n}(s)\right)$, где

$$\mathfrak{N}\left(\widetilde{n}\right) = \{(k_1, k_2, \ldots, k_m) \mid k_i \in \mathbb{N},\ 1 \leqslant k_i \leqslant n_i,\ i = 1, 2, \ldots, m\}.$$

Такой подход является более логичным при изучении задачи Беллмана. Отличия в подходах связаны с соображениями следующего толка: при вычислениях одночлены $x_1^{n_1}x_2^{n_2}$ и $x_1^{n_2}x_2^{n_1}$ естественно считать разными, а наборы степеней (x^{n_1}, x^{n_2}) и (x^{n_2}, x^{n_1}) — одинаковыми. Стоит отметить, что в изначальной формулировке результат в некотором смысле является более тонким.

Содержательно из теорем 6 и 7 следует, что при выполнении дополнительного условия

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

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

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

$$(1-\varepsilon)\log\left(\max_i n_i\right) + \frac{\log N}{\log\log N} \leqslant l\left(x^{k_1}, x^{k_2}, \ldots, x^{k_m}\right) \leqslant$$
$$\leqslant (1+\varepsilon)\log\left(\max_i n_i\right) + \frac{\log N}{\log\log N},$$

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

$$l(x_1^{k_1}x_2^{k_2}\ldots x_m^{k_m}) \sim \log\left(\max_i n_i\right) + \frac{\log N}{\log\log N},$$

$$l\left(x^{k_1}, x^{k_2}, \ldots, x^{k_m}\right) \sim \log\left(\max_i n_i\right) + \frac{\log N}{\log\log N},$$

из которых в силу справедливости для всех наборов теоремы 6 следует и выполнение для почти всех наборов соотношений

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

где $K = k_1k_2\ldots k_m$.

Таким образом, теоремы 6 и 7 дают окончательное асимптотически точное решение задач Беллмана и Кнута: действительно, при стандартном условии «сложность (число операций) существенно больше числа полюсов

(суммы «входов» и «выходов» — в данном случае $m+1$)» для почти всех исследуемых объектов (наборов) верхняя оценка асимптотически совпадает с нижней.

В свете получения асимптотически точного решения задач Беллмана и Кнута интересно отметить такой момент. В знаменитом многотомнике Д. Е. Кнута «Искусство программирования», во втором томе первого издания которого была сформулирована задача о сложности вычисления набора степеней [23, разд. 4.6.3, упр. 32], есть очень много упражнений самого разного уровня сложности, начиная от простых задачек «для разогрева» и заканчивая открытыми проблемами. Трудность каждого упражнения оценена по числовой шкале от 0 до 50. Так, в первом издании числом 50 были отмечены Великая теорема Ферма и задача о сложности вычисления набора степеней, но в третьем издании эта оценка для первой задачи «девальвировала» до 45, так как к этому моменту ее доказательство уже перестало быть открытой проблемой, а вторая и вовсе исчезла из списка упражнений.

Однако, несмотря на получение асимптотически точного решения задач Беллмана и Кнута, эти задачи в случае, когда условие «число переменных или степеней существенно меньше суммы логарифма максимальной степени и мощностного слагаемого» не выполняется, остались. Значительным продвижением в этом направлении стала следующая теорема, в предварительном виде представленная [40] в 2000 г. и получившая окончательный вид [56] в 2014 г. Отметим, что в этой теореме отличие оценок сложности для задач Беллмана и Кнута на величину $m-1$ становится существенным.

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

Т е о р е м а 8 [56]. *Пусть числовая функция $f(x)$ при $x\to\infty$ удовлетворяет условиям $f(x)\to\infty$, $\log f(x)=o(\log x)$. Тогда для любой последовательности наборов натуральных чисел*

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

удовлетворяющей условию

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

выполняются неравенства

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

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

где $N=n_1n_2\ldots n_m$.

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

Случай 1. Пусть выполняется неравенство $\log N \geqslant m \log mf(m)$. Тогда

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

Далее, применяя теорему 6 и используя это соотношение, получаем:

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

Требуемая верхняя оценка в этом случае доказана.

Случай 2. Пусть выполняется неравенство $\log N < m \log mf(m)$. В этом случае будем доказывать нужную оценку для задачи Кнута. Без ограничения общности можно считать, что все n_i различны. Тогда имеем:

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

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

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

Положим

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

Отдельно оценим сверху сложность вычисления наборов степеней $\{x^{n_i} \mid i \in I_1\}$ и $\{x^{n_i} \mid i \in I_2\}$.

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

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

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

...

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

Очевидно, что для вычисления этих степеней требуется $O\left(\frac{m}{f(m)}\right)$ умножений.

Отметим, что в силу соотношений

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

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

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

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

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

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

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

Перейдем к оценке величины $l\left(\{x^{n_i} \mid i \in I_2\}\right)$ (а также оценим величину $|I_2|$). Используя теорему 6, получаем:

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

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,

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

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

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

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

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

Отметим, что в случае выполнения неравенства

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

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,

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

Если же выполняется неравенство

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

то, очевидно,

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

Итак, в обоих случаях имеем:

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

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

Поэтому окончательно получаем:

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

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

Для завершения доказательства верхней оценки осталось использовать равенство

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

Теорема 8 доказана.

Следствие 1. *Для любой последовательности наборов натуральных чисел* $\widetilde{n}(k)=\left(n_1(k),n_2(k),\ldots,n_{m(k)}(k)\right)$, $k=1,2,\ldots$, *удовлетворяющей условию*

$$\sum_{i=1}^{m(k)}n_i(k)\to\infty,$$

выполняются неравенства

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

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

Доказательство. Для получения из теоремы 8 этого утверждения достаточно учесть неравенства

$$0\leqslant\sum_{i=1}^{m}\left(\lceil\log_{(m/(f(m))^2)}n_i\rceil-\log_{(m/(f(m))^2)}n_i\right)<m.$$

Теперь на элементарном примере проиллюстрируем, во-первых, различия в формулировке самой теоремы 8 и следствия 1 из нее, а во-вторых, метод доказательства теоремы 8.

Пример 1. Исследуем асимптотический рост при $m\to\infty$ величины $l(x^{n_1},x^{n_2},\dots,x^{n_m})$ в случае, когда на показатели степеней наложены следующие ограничения: все n_i различны и ограничены сверху величиной $m^2/\log\log m$.

В силу наложенных ограничений выполняются соотношения

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

Поэтому, применяя следствие 1, получаем оценку

$$l(x^{n_1},x^{n_2},\dots,x^{n_m})\leqslant 2m+o(m).$$

С другой стороны, в случае, когда почти все показатели степени «близки» к $m^2/\log\log m$, положив $f(x)=(\log\log m)^{1/2}$ в теореме 8, получаем оценку $l(x^{n_1},x^{n_2},\dots,x^{n_m})\leqslant m+o(m)$, которая, в силу очевидного факта — на каждую степень надо использовать хотя бы одну операцию умножения, — является асимптотически не улучшаемой.

Метод доказательства оценки из теоремы 8 в данном примере может быть проинтерпретирован следующим образом. Заметим, что каждое из чисел n_i является двухразрядным в системе счисления с основанием $\lceil m/(\log\log m)^{1/2}\rceil$. Сначала вычислим все степени с показателями, имеющими одноразрядную запись по этому основанию, а затем — все степени с показателями, имеющими двухразрядную запись с нулем в младшем разряде. На это потребуется $O\left(m/(\log\log m)^{1/2}\right)$ операций умножения. После этого для вычисления каждой степени x^{n_i} потребуется не более одной операции умножения.

Далее для сокращения записи будем выписывать оценки только для задачи Беллмана (оценки для задачи Кнута автоматически выписываются из соотношения двойственности). Кроме того, будем считать, что все степени n_i, $i=1,\dots,m$, различны и отличны от 0, так как если $\{n_1,n_2,\dots,n_m\}=\{r_1,r_2,\dots,r_s\}$ и все числа r_i, $i=1,\dots,r_s$, различны и отличны от 0, то, очевидно,

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

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

Положим

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

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

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

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

Далее, при выполнении условия $\frac{\log N}{\log \log N} = o\left(\log \max_i n_i + m\right)$ в силу теоремы 8 и неравенства

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

справедлива асимптотика

$$l\left(x_1^{n_1} x_2^{n_2} \ldots x_m^{n_m}\right) \sim \log \max_i n_i + m \sim V(n_1, n_2, \ldots, n_m).$$

В общем случае, дополнительно учитывая неравенство

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

получаем, что для почти всех наборов $(k_1, k_2, \ldots, k_m)$ из $\mathfrak{M}\left(\widetilde{n}\right)$ справедливы асимптотические соотношения

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

В 2014 г. в работе [56] такое уточнение оценок сложности в случае, когда рост величины m сравним с ростом суммы $\log \max_i n_i + \frac{\log N}{\log \log N}$.

Т е о р е м а 9 [56]. *Пусть последовательность наборов*

$$\widetilde{n}(s) = \left(n_1(s), n_2(s), \ldots, n_{m(s)}(s)\right), \quad s = 1, 2, \ldots,$$

различных натуральных чисел при $s \to \infty$ удовлетворяет условию

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

Тогда для любого $\varepsilon > 0$ доля наборов $(k_1, k_2, \ldots, k_m)$ из $\mathfrak{N}\left(\widetilde{n}(s)\right)$, для которых выполняются неравенства

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

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

Верхняя оценка теоремы 9 следует из теоремы 8, а нижняя устанавливается путем комбинирования пяти разных нижних оценок.

Следствие 2. *Пусть последовательность наборов*

$$\widetilde{n}(s) = \left(n_1(s), n_2(s), \ldots, n_{m(s)}(s)\right), \quad s = 1, 2, \ldots,$$

различных натуральных чисел при $s \to \infty$ *удовлетворяет условию*

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

Тогда для любого $\varepsilon > 0$ *доля наборов* $(k_1, k_2, \ldots, k_m)$ *из* $\mathfrak{M}\left(\widetilde{n}(s)\right)$, *для которых выполняются неравенства*

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

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

Замечание. Последовательность наборов

$$\widetilde{n}(s) = \left(s^2, s^2 + 1, \ldots, s^2 + s - 1, 2^s, 2^s + 1, \ldots, 2^s + \lfloor \log s \rfloor\right), \quad s = 1, 2, \ldots,$$

дает пример, когда «разрыв» в 5/3 раза между асимптотикой верхней и нижней оценок устранить не удается. Верхняя оценка, устанавливаемая теоремой 8, асимптотически равна $5s$, в то время как все пять нижних оценок из доказательства теоремы 9 асимптотически не превосходят $3s$.

В заключение несколько усилим формулировку теоремы 8, а точнее, следствия 1 к ней, избавившись от множителя $1 + o(1)$ у слагаемого $\log(\max n_i)$. Это, казалось бы, непринципиальное изменение поможет доказать один интересный факт о сравнении оценок сложности для задач Беллмана и Лупанова в § 4.

Теорема 10. *Для любой последовательности наборов натуральных чисел* $\widetilde{n}(s) = (n_1(s), n_2(s), \ldots, n_{m(s)}(s))$, $s = 1, 2, \ldots$, *такой, что*

$$\prod_{i=1}^{m(s)} (n_i(s) + 1) \to \infty \quad \textit{при} \quad s \to \infty,$$

выполняется неравенство

$$l\left(x_1^{n_1} x_2^{n_2} \ldots x_m^{n_m}\right) \leqslant \log \max_i n_i + \frac{\log\left(\prod (n_i + 1)\right)}{\log\log\left(\prod (n_i + 1)\right)} (1 + o(1)) + m.$$

Доказательство. Положим

$$N = (n_1 + 1)(n_2 + 1) \ldots (n_m + 1);$$

$$I_1 = \left\{ i \mid \log n_i \geqslant \frac{\log N}{(\log\log N)^2} \right\}, \quad I_2 = \left\{ i \mid \log n_i < \frac{\log N}{(\log\log N)^2} \right\};$$

$$U_1 = \prod_{i \in I_1} x_i^{n_i}, \quad U_2 = \prod_{i \in I_2} x_i^{n_i}; \quad N_1 = \prod_{i \in I_1} n_i, \quad N_2 = \prod_{i \in I_2} n_i.$$

Для оценки сложности вычисления одночленов U_1 и U_2 применим, соответственно, теорему 6 и следствие 1 к теореме 8:

$$l(U_1) \leqslant \log \max_i n_i + \frac{\log N_1}{\log\log N_1} (1 + o(1)) + O(|I_1|),$$

$$l(U_2) \leqslant \frac{\log N}{(\log\log N)^2} (1 + o(1)) + \frac{\log N_2}{\log\log N_2} (1 + o(1)) + |I_2|,$$

откуда, учитывая соотношения

$$|I_1| \leqslant (\log\log N)^2, \quad |I_2| \leqslant m, \quad \frac{\log N_1}{\log\log N_1} + \frac{\log N_2}{\log\log N_2} \leqslant \frac{\log N}{\log\log N} (1 + o(1)),$$

получаем требуемую оценку. Теорема 10 доказана.

§ 3. Сборка слов схемами конкатенации

Давайте теперь зададимся вопросом, как изменится задача Беллмана, если отказаться от коммутативности используемой операции. В этом случае будет вычисляться не одночлен $x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}$, а некоторый элемент полугруппы с порождающими $x_1, x_2, \dots, x_n$, допускающий представление, включающее для каждого i, $i = 1, 2, \dots, m$, ровно n_i вхождений порождающего элемента x_i.

Задачи такого типа естественным образом возникают в алгебре (см., например, [14]), но в этих задачах, как правило, речь идет о «формульной» сложности, когда полученный промежуточный результат может быть использован один раз. Однако и «схемная» сложность, когда промежуточный результат может быть использован многократно, также представляет большой интерес [81, 111, 186].

Будем рассматривать один из наиболее естественных случаев задачи о сложности вычисления элементов полугрупп — случай, когда порождающие $x_1, x_2, \dots, x_m$ являются образующими свободной полугруппы. В этом случае множество порождающих элементов полугруппы обычно называется *алфавитом*, сами порождающие — *буквами*, а полугрупповая операция — конкатенацией. *Конкатенацией слов* $\widetilde{\alpha}$ и $\widetilde{\beta}$ конечной длины над произвольным алфавитом называется слово $\widetilde{\alpha}\widetilde{\beta}$, полученное приписыванием к слову $\widetilde{\alpha}$ справа слова $\widetilde{\beta}$.

В работах [18, 137] введена мера сложности порождения слов с помощью операции конкатенации, которой будем придерживаться в данной работе и которая с небольшими модификациями известна и как длина цепочек слов (см., например, [117, 118, 123, 128, 178]), и как мультипликативная сложность слов [39, 41, 79, 80, 158], и как аддитивная сложность слов [82, 95, 96, 168].

Последовательность S слов (наборов) из конечного алфавита $\mathfrak{A}$

$$\widetilde{\tau}_1, \quad \widetilde{\tau}_2, \quad \dots, \quad \widetilde{\tau}_r = \widetilde{\alpha}$$

назовем *схемой конкатенации* [78], реализующей (вычисляющей) слово (набор) $\widetilde{\alpha}$, если для каждого i, $i = 1, 2, \dots, r$, слово $\widetilde{\tau}_i$ можно представить в виде $\widetilde{\tau}_i = \widetilde{\beta}_{i_1}\widetilde{\beta}_{i_2}$, где для $j = 1, 2$ либо β_{i_j} — буква из алфавита $\mathfrak{A}$, либо $\beta_{i_j} = \tau_m$ для некоторого m, удовлетворяющего условию $m \leqslant i - 1$. *Сложностью* $l^c_{\mathfrak{A}}(S)$ данной схемы S, реализующей слово $\widetilde{\alpha}$, назовем число r. Положим $l^c_{\mathfrak{A}}(\widetilde{\alpha}) = \min l^c_{\mathfrak{A}}(S)$, где минимум берется по всем схемам конкатенации, реализующим слово $\widetilde{\alpha}$ в алфавите $\mathfrak{A}$. Величину $l^c_{\mathfrak{A}}(\widetilde{\alpha})$ назовем *мультипликативной сложностью* слова (набора) $\widetilde{\alpha}$ в алфавите $\mathfrak{A}$. Будем также называть величину $l^c_{\mathfrak{A}}(\widetilde{\alpha})$ *сложностью сборки слова* $\widetilde{\alpha}$ *схемами конкатенации* над алфавитом $\mathfrak{A}$.

Схему конкатенации в алфавите $\mathfrak{A}$ можно рассматривать как схему из функциональных элементов, имеющую $|\mathfrak{A}|$ входов, на которые подаются, соответственно, буквы из алфавита $\mathfrak{A}$, а каждый элемент схемы реализует конкатенацию наборов, подаваемых на его входы. Заметим также, что аналогичным образом можно ввести понятие *сложности* $l^c_{\mathfrak{A}}(M)$ *сборки системы слов* M *схемами конкатенации*: для этого надо потребовать, чтобы в последовательности S содержались все слова из множества M.

Отметим, что, с одной стороны, к задаче о сборке слов схемами конкатенации мы пришли, отталкиваясь от задачи Беллмана, а с другой стороны, аддитивные цепочки, по существу, можно рассматривать как частный случай схем конкатенации — случай однобуквенного алфавита $\mathfrak{A}$, и, таким образом, задача Кнута — это задача о сборке системы слов схемами конкатенации над однобуквенным алфавитом.

В исследованиях по сложности сборки слов схемами конкатенации выделим два направления. Первое из них связано с уточнением асимптотического поведения соответствующей функции Шеннона, характеризующей сложность сборки самого сложного слова заданной длины, а второе — с изучением сложности двоичных слов с заданным соотношением нулей и единиц. Именно этим двум направлениям и посвящен данный параграф.

Прежде чем перейти к первому из них, заметим, что большинство обсуждаемых не только в этом параграфе, но и во всей работе вопросов так или иначе относится к асимптотической теории сложности [75], важнейшей частью которой, в частности, является изучение асимптотического поведения функционалов, характеризующих меру сложности самых труднореализуемых объектов из заданных классов и называемых обычно функциями Шеннона. Часть из уже описанных результатов можно было бы сформулировать именно на таком языке, но в данной работе соответствующие теоремы сформулированы без использования понятия функции Шеннона. Дальнейшее изложение уже настоятельно требует введения соответствующих понятий.

Заходя издалека, напомним, что в моделях с конечным набором базисных операций для нахождения сложности реализации заданного объекта (функции) существует тривиальный переборный алгоритм. Однако реально воспользоваться им чаще всего невозможно, так как с ростом числа элементов в схемах количество схем растет очень быстро и применение тривиального метода становится практически неосуществимым. На самом деле большая трудоемкость решения задачи синтеза в общем виде присуща всем алгоритмам, предназначенным для ее решения, — к этому выводу одним из первых пришел С. В. Яблонский [114]. С тех пор эта точка зрения стала общепринятой, получив много косвенных подтверждений своей справедливости. В силу этого обычно рассматривают некоторые ослабления рассматриваемой задачи. Одно из таких ослаблений заключается в приближенном решении задачи, т. е. в построении не обязательно минимальных, а «достаточно экономных» схем. Но и эта задача при поиске «достаточно точного» решения, вообще говоря, остается очень трудной. Поэтому часто рассматривают задачу построения асимптотически оптимальных схем. Постановка этой задачи, скажем, для классического случая вычисления булевых функций такова. Каждой схеме S ставится в соответствие неотрицательное число $L(S)$ (сложность схемы S), например, число элементов схемы. Считается, что схема тем лучше, чем меньше величина $L(S)$. Через $L(f)$ обозначается сложность схемы заданного типа, которая реализует f и имеет минимальную сложность. Вводится функция $L(n) = \max L(f)$, где максимум берется по всем рассматриваемым функциям от n переменных. Требуется найти метод синтеза схем, позволяющий для любой рассматриваемой функции f от n переменных стоить схему, которая реализует функцию f и имеет сложность, не превосходящую или мало превосходящую (например, асимптотически не превосходящую) величину $L(n)$. Такой подход был предложен

К. Шенноном [183] в 1949 г. при исследовании контактных схем и может быть перенесен на другие классы управляющих систем. Функцию $L(n)$ принято называть *функцией Шеннона*.

Фундаментальные основы асимптотической теории синтеза и сложности управляющих систем были заложены О. Б. Лупановым. Им были предложены асимптотически оптимальные методы синтеза и получены асимптотически точные оценки сложности для важнейших классов управляющих систем: вентильных схем глубины 2, контактно-вентильных схем, схем из функциональных элементов, контактных схем, схем из функциональных элементов без ветвления выходов (формул) и с ограниченным ветвлением (формул с частичной памятью), формул ограниченной глубины, параллельно-последовательных контактных схем, релейно-контактных схем и др. (см., например, [66, 70, 75, 92]). При изучении этих модельных классов управляющих систем О. Б. Лупановым были выявлены новые эффекты и закономерности, в числе которых было явление, названное эффектом Шеннона: при реализации в большинстве исследованных им классов управляющих систем почти все функции имеют почти одинаковую сложность, асимптотически равную сложности наиболее сложных функций.

К асимптотической теории сложности относится и большинство вопросов, обсуждаемых в данной работе. В частности, относительно задачи о сложности сборки слов схемами конкатенации речь пойдет об исследовании асимптотического поведения соответствующих функций Шеннона.

Обозначим через $W_{\mathfrak{A}}(n)$ множество всех слов в алфавите $\mathfrak{A}$ длины n. Положим $L^c_{\mathfrak{A}}(n) = \max l^c(\widetilde{\alpha})$, где максимум берется по всем словам $\widetilde{\alpha}$ из множества $W_{\mathfrak{A}}(n)$.

Задача нахождения асимптотики роста функции Шеннона $L^c_{\mathfrak{A}}(n)$, характеризующей сложность сборки самого сложного слова длины n в алфавите $\mathfrak{A}$, является по существу «фольклорной», а ее решение впервые опубликовано, по-видимому, в [186], где установлено, что

$$L^c_{\mathfrak{A}}(n) \sim \log |\mathfrak{A}| \frac{n}{\log n}.$$

Особую важность исследованию схем конкатенации придает тот факт, что асимптотически точную нижнюю оценку функции Шеннона $L^c_{\mathfrak{A}}(n)$ можно не только получить применением стандартного мощностного метода, но и предъявив конкретное слово (начальный отрезок последовательности де Брёйна, о которой см., например, [107, 132]), что просто немыслимо для большинства других вычислительных схем (моделей).

При существенно более детальном исследовании задачи о сложности сборки слов схемами конкатенации удалось выявить еще один эффект, не имеющий места или, по крайней мере, пока не обнаруженный, для других вычислительных моделей. Перейдем к его описанию.

3.1. Уточнение асимптотического поведения функции Шеннона сложности сборки слов. Как уже отмечалось, О. Б. Лупановым [67–69] найдена асимптотика роста функции Шеннона для сложности булевых функций во всех основных классах схем, включая классы формул и схем из функциональных элементов, построенных из элементов произвольного конечного полного базиса. С. А. Ложкиным [64] многие из этих оценок усилены: в частности установлены так называемые асимптотические оценки

высокой степени точности (которые условно можно трактовать как оценки, дающие не только асимптотику функции Шеннона, но и асимптотику остаточного члена) для класса формул, а также для схем из функциональных элементов в базисах специального вида. В случае класса схем из функциональных элементов над полным конечным базисом B установлены следующие нижняя и верхняя оценки [64] функции Шеннона $L_B(n)$:

$$\rho_B \frac{2^n}{n}\left(1+(1+o(1))\frac{\log n}{n}\right) \leqslant L_B(n) \leqslant \rho_B \frac{2^n}{n}\left(1+(1+\varkappa_B+o(1))\frac{\log n}{n}\right), \quad (*)$$

где ρ_B — приведенный вес базиса [75], $\varkappa_B = 1$ в случае, когда базис B симметричный [64], и $\varkappa_B = 0$ в остальных случаях. Приведенные оценки не дают ответа на вопрос, может ли коэффициент при $(\log n)/n$ в нижней оценке быть асимптотически равен 2 (или хотя бы асимптотически превышать $1+\varepsilon$ для некоторого $\varepsilon > 0$).

Покажем, что задача сборки слов схемами конкатенации для аналогичной нижней оценки функции Шеннона (с учетом поправки на масштаб, связанный с количеством объектов в классе, по которому берется максимум) дает положительный ответ на этот вопрос.

Аккуратно применяя известные методы для функции Шеннона сложности сборки слов схемами конкатенации, можно получить следующие оценки:

$$\log|\mathfrak{A}|\frac{n}{\log n}\left(1+(1+o(1))\frac{\log\log n}{\log n}\right) \leqslant L^c_{\mathfrak{A}}(n) \leqslant$$
$$\leqslant \log|\mathfrak{A}|\frac{n}{\log n}\left(1+(2+o(1))\frac{\log\log n}{\log n}\right). \quad (**)$$

Если в оценках из $(*)$ величину n представить как $\log\log|P(n)|$ (здесь $P(n)$ — множество всех булевых функций от n фиксированных переменных), а в оценках из $(**)$ величину n представить как $(\log|W_{\mathfrak{A}}(n)|)/\log|\mathfrak{A}|$, то соотношения $(*)$ для симметричного базиса и соотношения $(**)$ дадут совершенно одинаковые*) оценки соответствующих функций Шеннона через мощности исследуемых классов, причем в обоих случаях нижняя и верхняя оценки отличаются лишь коэффициентами при втором слагаемом в скобках — асимптотически равными 1 и 2 соответственно. В 2016 г. автором и Д. В. Кочергиным для функции Шеннона сложности сборки слов схемами конкатенации этот «зазор» устранен: установлена [59] нижняя оценка, имеющая точно такой же вид, что и верхняя оценка в соотношениях $(**)$.

Теорема 11 [59]. *При $n \to \infty$ для функции Шеннона сложности сборки слов схемами конкатенации в конечном алфавите $\mathfrak{A}$ справедливо равенство*

$$L^c_{\mathfrak{A}}(n) = \log|\mathfrak{A}|\frac{n}{\log n}\left(1+(2+o(1))\frac{\log\log n}{\log n}\right).$$

Доказательство. Сначала для полноты картины установим оценки $(**)$, а затем усилим нижнюю оценку до оценки требуемого вида. Пусть $\mathfrak{A} = \{a_1, \ldots, a_s\}$.

*) С точностью до наличия множителя ρ_B в неравенствах из $(*)$. При этом если в задаче сборки слов схемами конкатенации разрешить использование многовходовых операций конкатенации с приписанными таким операциям весами или стоимостями, то аналогичный мультипликативный коэффициент появится и в соотношениях $(**)$.

Верхняя оценка. Пусть t — натуральный параметр, значение которого определим позже. Построим схему конкатенации, вычисляющую некоторое слово $\widetilde{\alpha}$ над алфавитом $\mathfrak{A}$ длины n, удовлетворяющее условию $l^c(\widetilde{\alpha}) = L^c_{\mathfrak{A}}(n)$.

Первая часть схемы вычисляет все слова длины t. Для этого потребуется не более $(t-1)s^t$ операций конкатенации. Вторая часть, склеивая полученные слова длины t, вычисляет все множество из s^{2t} слов длины $2t$ за s^{2t} операций (по одной операции конкатенации на слово). Третья часть схемы собирает слово $\widetilde{\alpha}$ из заготовок длины $2t$ и букв исходного алфавита с использованием не более $\lfloor n/(2t)\rfloor + 2t - 1$ операций конкатенации. Таким образом, $L^c_{\mathfrak{A}}(n) \leqslant (t-1)s^t + s^{2t} + \lfloor n/(2t)\rfloor + 2t - 1$. Положив $t = \lfloor (\log_s n - 2\log_s \log n)/2\rfloor$, при $n \to \infty$ получаем:

$$L^c_{\mathfrak{A}}(n) \leqslant \frac{n}{\log_s n}\left(1 + 2\frac{\log\log n}{\log n} + O\left(\frac{1}{\log n}\right)\right).$$

Верхняя оценка доказана.

Нижняя оценка. При доказательстве нижней оценки под схемами конкатенации будем понимать схемы из функциональных элементов, на входы которых подаются буквы алфавита $\mathfrak{A}$, а каждый элемент схемы реализует конкатенацию подаваемых на его входы слов. Схему конкатенации как обычно будем называть *минимальной*, если никакая схема меньшей сложности не вычисляет то же самое слово. Обозначим через $N_{\mathfrak{A}}(l)$ число минимальных схем конкатенации со входами $a_1, \ldots, a_s$ сложности не более l. Верхние оценки на число схем из функциональных элементов, реализующих булевы функции (см., например, § 3 из [71]), легко переносятся на случай схем конкатенации.

Лемма 4. *Существует такая константа c (зависящая только от числа букв в алфавите $\mathfrak{A}$), что для любого натурального l справедливо неравенство $N_{\mathfrak{A}}(l) \leqslant (cl)^l$.*

С использованием леммы 4 стандартным образом устанавливается мощностная нижняя оценка функции Шеннона.

Лемма 5. *Для любого $\varepsilon > 0$ при всех достаточно больших значениях n справедливо неравенство*

$$L^c_{\mathfrak{A}}(n) \geqslant \frac{n}{\log_s n}\left(1 + (1-\varepsilon)\frac{\log\log n}{\log n}\right).$$

Доказательство. Положим $l_\varepsilon = \frac{n}{\log_s n}\left(1 + (1-\varepsilon)\frac{\log\log n}{\log n}\right)$. Установим, что $\lim\limits_{n\to\infty} \frac{N_{\mathfrak{A}}(l_\varepsilon)}{s^n} = 0$. В силу леммы 4 при всех достаточно больших значениях n выполняются соотношения

$$\log_s \frac{N_{\mathfrak{A}}(l_\varepsilon)}{s^n} \leqslant \frac{n}{\log_s n}\left(1 + (1-\varepsilon)\frac{\log\log n}{\log n}\right)\left(\log_s n - \log_s \log n + \log_s(2c)\right) - n =$$
$$= (-\varepsilon + o(1))\frac{n\log\log n}{\log n}.$$

Неравенство $N_{\mathfrak{A}}(l_\varepsilon) < s^n$ влечет оценку $L^c_{\mathfrak{A}}(n) > l_\varepsilon$. Лемма 5 доказана.

Нижняя оценка из (**) непосредственно следует из леммы 5 в силу произвольности ε.

Уточнение нижней оценки проведем для двухбуквенного алфавита $\{0, 1\}$, общий случай рассматривается аналогично. Будем в этом случае в обозначении функции Шеннона опускать нижний индекс.

Положим $k=k(n)=\min\{t\,|\,2^t+t-1\geqslant n\}$. В случае когда $n=2^{k(n)}+k(n)-1$, обозначим через $B(n)$ множество всех двоичных слов де Брёйна [107] порядка $k(n)$ (т. е. множество всех слов длины $2^{k(n)}+k(n)-1$, в которых все $2^{k(n)}$ подслов длины $k(n)$ различны). Известно [132] (см. также, например, [107]), что $|B\left(2^k+k-1\right)|=2^{2^{k-1}}$. Теперь при условии $n\neq 2^{k(n)}+k(n)-1$ определим множество $B(n)$ как множество всех слов длины n, в которых все $n-k(n)+1$ слов длины $k(n)$ различны. Отметим, что множество $B(n)$ содержит множество всех подслов длины n во всех словах множества $B\left(2^{k(n)}+k(n)-1\right)$.

Лемма 6. *При всех натуральных n выполняется неравенство $|B(n)|\geqslant 2^{n/2-\log n}$.*

Доказательство. Очевидно, $2^{k(n)-1}+k(n)-1\leqslant n\leqslant 2^{k(n)}+k(n)-1$. Если $2^{k(n)}\leqslant n\leqslant 2^{k(n)}+k(n)-1$, то $|B(n)|=2^{2^{k(n)-1}}$. В этом случае нужная оценка следует из соотношений

$$2^{k(n)-1}=\frac{1}{2}\left(2^{k(n)}+k(n)-1\right)-\frac{1}{2}(k(n)-1)\geqslant\frac{1}{2}n-\frac{1}{2}\log n+\frac{1}{2}>\frac{1}{2}n-\frac{1}{2}\log n.$$

При $2^{k(n)-1}+k(n)-1\leqslant n<2^{k(n)}$ требуемая оценка извлекается из рассуждений, используемых при доказательстве теоремы 9.3.2 из [107].

Лемма 6 доказана.

Для произвольного натурального $r\geqslant 2$ определим величину $r'=r'(r)$ равенством $r'=r/2$ в случае, когда r является степенью двойки, и равенством $r'=\lfloor r/2\rfloor+1$ в противном случае. Среди всех бинарных корневых деревьев с r листьями (вершинами степени 1) выделим какое-либо дерево, в котором ровно r' вершин смежны с листьями. Назовем это выделенное дерево *каноническим*.

Пусть $\widetilde{\alpha}\in B(n)$, а S — некоторая минимальная схема конкатенации для слова $\widetilde{\alpha}$. Рассматривая S как схему из функциональных элементов, каждую из вершин v схемы отнесем к одному из двух множеств в зависимости от длины $\lambda(v)$ вычисляемого в вершине (входе схемы или функциональном элементе) v слова:

$$V_1=\{v\in S\,|\,\lambda(v)\leqslant k(n)-1\},\quad V_2=\{v\in S\,|\,\lambda(v)\geqslant k(n)\}.$$

Обозначим через $R=R(S)$ число всех ребер в схеме S, у которых начальная вершина лежит в множестве V_1, а конечная — в V_2. В силу определения множества $B(n)$ из каждой (отличной от выхода) вершины множества V_2 до выхода существует единственный ориентированный путь. Поэтому соединения множества вершин V_2 в схеме образуют бинарное корневое дерево с R листьями, находящимися во множестве V_1, при этом листья могут быть «склеенными», т. е. из одной вершины, лежащей в множестве V_1, может идти несколько ребер в вершины множества V_2. Очевидно, что справедливо равенство $|V_2|=R-1$. При изменении структуры этого бинарного корневого дерева с сохранением порядка «подключения» к листьям получается другая минимальная схема для слова $\widetilde{\alpha}$. Теперь среди всех получающихся таким образом минимальных схем выделим схему, в которой множество вершин V_2 образуют каноническое бинарное корневое дерево с R листьями. Такую схему будем также называть *канонической*.

В канонической схеме S множество вершин (функциональных элементов) V_2 разобьем на два подмножества V_2' и V_2'': к множеству V_2' отнесем

вершины, смежные с вершинами из множества V_1, а к множеству V_2'' — все остальные вершины из V_2.

Лемма 7. *При всех достаточно больших значениях n для любой минимальной схемы S, вычисляющей слово из множества $B(n)$, справедливы неравенства*

$$\frac{n}{\log n} \leqslant R(S) \leqslant \frac{n}{\log n} + 3\frac{n \log\log n}{\log^2 n}.$$

Доказательство. Верхняя оценка непосредственно следует из соотношений $R(S) = |V_2| + 1 \leqslant L^c(S)$ и установленной верхней оценки функции Шеннона. Нижняя оценка следует из неравенств $R(S) \geqslant \frac{n}{k(n)-1}$ и $n \geqslant 2^{k(n)-1} + k(n) - 2$. Лемма 7 доказана.

Обозначим через $N(l, n, r)$ множество схем конкатенации S, удовлетворяющих следующим свойствам: 1) схема S вычисляет некоторое слово из множества $B(n)$; 2) схема S является минимальной; 3) схема S является канонической; 4) выполняется неравенство $L^c(S) \leqslant l$; 5) выполняется равенство $R(S) = r$, а через $N(l, n, r)$ — множество схем, удовлетворяющих первым четырем из этих свойств.

Лемма 8. *Найдется такая константа $c > 0$, что при всех достаточно больших значениях n справедливо неравенство*

$$|N(l, n, r)| \leqslant \left(\frac{cn \log\log n}{\log^2 n}\right)^l \left(\frac{\log n}{n}\right)^{r/2}.$$

Доказательство. Учитывая лемму 7 и верхнюю оценку функции Шеннона, без ограничения общности можно считать, что выполняются соотношения $\frac{n}{\log n} \leqslant r \leqslant l \leqslant \frac{n}{\log n} + 3\frac{n \log\log n}{\log^2 n}$, а также неравенство $l - r \geqslant (\log\log n)/2$.

Сначала оценим сверху величину $|N'(l, n, r)|$, где $N'(l, n, r)$ — подмножество схем S из множества $N(l, n, r)$, удовлетворяющих условию $L^c(S) = l$.

Пусть $S \in N'(l, n, r)$. Для этой схемы информация о том, выходы каких элементов подаются на произвольный элемент из множества V_2'', однозначно определяется значением параметра r, а на входы всех остальных элементов (кроме, быть может, одного входа одного элемента из множества V_2') подаются либо выходы функциональных элементов из множества V_1, либо входы схемы (также входящие в множество V_1).

Занумеруем произвольным образом числами от 1 до $|V_1| - 2$ функциональные элементы из множества V_1, а числами от $|V_1| - 1$ до $|V_1| + |V_2'| - 2$ — все элементы из множества V_2'. Схеме S с введенной нумерацией невходовых вершин из множества $V_1 \cup V_2'$ сопоставим таблицу из $|V_1| + |V_2'| - 2$ строк и двух столбцов, указав на пересечении i-й строки и j-го столбца выход какого элемента или какой вход подается на j-й вход i-го элемента. При различных нумерациях описанного вида получаются разные таблицы.

Поэтому, учитывая равенства $|V_2| = r-1$, $|V_1| = l-r+3$, $|V_2'| = r'(r)$ и $|V_2''| = r - r'(r) - 1$, имеем:

$$|N'(l,n,r)| \leqslant \frac{(|V_1|)^{2(|V_1|+|V_2'|-2)}}{(|V_1|-2)!\,(|V_2'|)!} = \frac{(l-r+3)^{2(l-r+r'+1)}}{(l-r+1)!(r')!} \leqslant$$

$$\leqslant \frac{c_1^l (l-r)^{2(l-(r/2))}}{\frac{(l-r)^{l-r}}{3^{l-r}}\,\frac{(r/2)^{r/2}}{3^{r/2}}} \leqslant \frac{c_2^l (l-r)^l}{r^{r/2}} \leqslant \frac{c_3^l \left(\frac{n\log\log n}{\log^2 n}\right)^l}{\left(\frac{n}{\log n}\right)^{r/2}},$$

где c_1, c_2, c_3 — некоторые константы. Просуммировав оценки на величину $|N'(l',n,r)|$ по всем l', не превосходящим l, получаем требуемую оценку. Лемма 8 доказана.

Лемма 9. *При всех достаточно больших значениях n для любой минимальной схемы конкатенации S, вычисляющей слово из множества $B(n)$, справедливо неравенство*

$$R(S) \geqslant \frac{n}{\log n} + \left(1 - 4\frac{\log\log\log n}{\log\log n}\right)\frac{n\log\log n}{\log^2 n}.$$

Доказательство. В минимальной схеме конкатенации S, вычисляющей некоторое слово из множества $B(n)$, множество вершин (функциональных элементов) V_1 разобьем на два подмножества V_1' и V_1'': к множеству V_2' отнесем вершины, смежные с вершинами из множества V_2, а к множеству V_1'' — все остальные вершины из V_1. В свою очередь, множество вершин V_1' разобьем на два подмножества $V_1'(1)$ и $V_1'(2)$ в зависимости от длины $\lambda(v)$ вычисляемого в вершине v слова:

$$V_1'(1) = \{v \in V_1' \mid \lambda(v) \geqslant \lambda_0\}, \quad V_1'(2) = \{v \in V_1' \mid \lambda(v) < \lambda_0\},$$

где $\lambda_0 = \log n - \log\log n + 3\log\log\log n$.

Для каждой вершины v схемы S обозначим через $d(v)$ степень ветвления выхода расположенного в этой вершине элемента (т. е. полустепень исхода этой вершины). Тогда

$$n = \sum_{v\in V_1'} d(v)\lambda(v) \leqslant \left(\sum_{v\in V_1'(1)} d(v)\right)(k(n)-1) + \left(\sum_{v\in V_1'(2)} d(v)\right)\lambda_0 \leqslant$$

$$\leqslant \left(\sum_{v\in V_1'(1)} d(v)\right)\log n + \left(\sum_{v\in V_1'(2)} d(v)\right)\lambda_0.$$

Кроме того,

$$R(S) = \sum_{v\in V_1'(1)} d(v) + \sum_{v\in V_1'(2)} d(v).$$

Введя обозначение

$$T = \left(\sum_{v\in V_1'(1)} d(v)\right) \Big/ \left(\sum_{v\in V_1'(2)} d(v)\right),$$

получаем:

$$\sum_{v\in V_1'(1)} d(v) \geqslant \frac{n}{\log n + \lambda_0 T^{-1}}, \quad R(S) = \frac{T+1}{T}\sum_{v\in V_1'(1)} d(v).$$

Следовательно,

$$R(S) \geqslant \frac{n(T+1)}{T\log n + \lambda_0}.$$

Для произвольной вершины v из множества V_1' выполняется неравенство $d(v) \leqslant 2^{k(n)-\lambda(v)}$, так как любое слово длины λ, $\lambda < k$, встречается в слове де Брёйна порядка k ровно $2^{k-\lambda}$ раз. С использованием указанного неравенства получаем:

$$|V_1'(1)| \geqslant \frac{\sum\limits_{v\in V_1'(1)} d(v)}{2^{k(n)-\lambda_0}} \geqslant \frac{n}{2^{k(n)}} \frac{2^{\lambda_0} T}{T\log n + \lambda_0} \geqslant \frac{2^{\lambda_0} T}{2(T\log n + \lambda_0)}.$$

Теперь докажем, что при всех достаточно больших значениях n справедливо неравенство $T \leqslant (\log\log n)^{-1}$. С использованием леммы 7 имеем:

$$L^c(S) \geqslant |V_1'(1)| + |V_2| + 1 = |V_1'(1)| + R(S) \geqslant \frac{n}{\log n} + \frac{T(\log\log n)^2}{2(T+1)} \frac{n\log\log n}{\log^2 n}.$$

Но последняя сумма при выполнении противоположного неравенства $T > (\log\log n)^{-1}$ противоречит установленной верхней оценке теоремы, что и доказывает нужное неравенство.

Теперь утверждение леммы следует из справедливости при всех достаточно больших n цепочки соотношений

$$R(S) - \frac{n}{\log n} \geqslant \frac{n(T+1)}{T\log n + \lambda_0} - \frac{n}{\log n} = \frac{n(\log n - \lambda_0)}{\log n(T\log n + \lambda_0)} \geqslant$$
$$\geqslant \frac{n\log\log n(\log\log n - 3\log\log\log n)}{\log^2 n(\log\log n + 1)} \geqslant \frac{n\log\log n}{\log^2 n}\left(1 - 4\frac{\log\log\log n}{\log\log n}\right).$$

Лемма 9 доказана.

Переходя к непосредственному доказательству нижней оценки теоремы 11, положим $L^c(B(n)) = \max L^c(\widetilde{\alpha})$, где максимум берется по всем словам $\widetilde{\alpha}$ из множества $B(n)$. В силу очевидного неравенства $L^c(n) \geqslant L^c(B(n))$ достаточно получить требуемую нижнюю оценку для величины $L^c(B(n))$.

Для произвольного положительного ε положим

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

Установим, что $\lim\limits_{n\to\infty} \frac{N(l_\varepsilon, n)}{|B(n)|} = 0$. С использованием лемм 6–9 получаем:

$$\log \frac{N(l_\varepsilon, n)}{|B(n)|} \leqslant$$
$$\leqslant \frac{n}{\log n}\left(1 + (2-\varepsilon)\frac{\log\log n}{\log n}\right)\left(\log n - 2\log\log n + \log\log\log n + \log(2c)\right) +$$
$$+ \frac{1}{2}\left(\frac{n}{\log n} + \left(1 - 4\frac{\log\log\log n}{\log\log n}\right)\frac{n\log\log n}{\log^2 n}\right)(\log\log n - \log n) - \left(\frac{n}{2} - \log n\right) =$$
$$= (-\varepsilon + o(1))\frac{n\log\log n}{\log n}.$$

Неравенство $N(l_\varepsilon, n) < |B(n)|$ влечет оценку $L^c(B(n)) > l_\varepsilon$. Отсюда в силу произвольности ε следует окончательная оценка.

Нижняя оценка теоремы 11, а с ней и вся теорема доказана.

3.2. Сложность сборки схемами конкатенации двоичных слов с заданной долей единиц. Вторая задача, на которой остановимся, обсуждая вопросы сложности сборки слов схемами конкатенации, заключается в исследовании асимптотического поведения функции Шеннона сложности сборки двоичных слов (наборов) с заданным числом единиц, определяемой при $0 \leqslant k \leqslant n$ равенством

$$L^c(k, n) = \max_{\widetilde{\alpha} \in A_n^k} l^c(\widetilde{\alpha}),$$

где максимум берется по множеству всех двоичных наборов (слов) длины n, содержащих ровно k единиц.

Очевидно, что при $k = 0$ и при $k = n$ эта задача превращается в задачу об аддитивных цепочках. Кроме того, при значениях k, «близких» к $n/2$, из [186] следует, что

$$L^c(k, n) = (1 + o(1))\frac{n}{\log n}.$$

Т е о р е м а 12 [39]. *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**)

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

Д о к а з а т е л ь с т в о. Полное доказательство этой теоремы содержится в [39]. Здесь дадим изложение его наиболее важных и интересных, но при этом достаточно простых частей, имеющих и самостоятельное значение.

Верхняя оценка. Отметим, что в силу очевидного равенства $L^c(k, n) = L^c(n-k, n)$ можно считать, что $k \leqslant n/2$.

Пусть $\widetilde{\alpha}_n^k$ — некоторый двоичный набор длины n, содержащий k единиц и удовлетворяющий условию $l^c(\widetilde{\alpha}_n^k) = L^c(k, n)$. Обозначим в наборе $\widetilde{\alpha}_n^k$ через n_i, $i = 0, 1, \ldots, k$, число нулей между i-й и $(i+1)$-й единицами. Таким образом, $n = \sum\limits_{i=0}^{k} n_i + k$.

С л у ч а й 1. Пусть выполняется неравенство $k \leqslant n^{1/\log\log n}$.

Сведем задачу о верхней оценке сложности порождения слов схемами конкатенации к задаче о верхней оценке сложности вычисления набора степеней одной переменной, т. е. к задаче Кнута.

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

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

Используя теорему 6, получаем:

$$L^c(k, n) = l^c(\widetilde{\alpha}_n^k) \leqslant \log \max_{0 \leqslant i \leqslant k} n_i + \frac{\log \prod\limits_{i: n_i \neq 0} n_i}{\log \log \prod\limits_{i: n_i \neq 0} n_i}(1 + o(1)) + O(k).$$

---

*) Будем считать, что $\dfrac{\log x}{\log \log x} = 0$ при $x \leqslant 4$.

Тогда при $k \geqslant 1$ имеем:

$$\frac{\log \prod\limits_{i:n_i\neq 0} n_i}{\log\log \prod\limits_{i:n_i\neq 0} n_i} \leqslant \frac{\log \left(\frac{n}{s}\right)^s}{\log\log \left(\frac{n}{s}\right)^s} \leqslant \frac{\log \left(\frac{n}{k+1}\right)^{k+1}}{\log\log \left(\frac{n}{k+1}\right)^{k+1}} \leqslant \frac{\log \left(\frac{n}{k}\right)^{k+1}}{\log\log \left(\frac{n}{k}\right)^{k+1}} \leqslant \frac{\log \left(\frac{n}{k}\right)^{k+1}}{\log\log \left(\frac{n}{k}\right)^{k}} \leqslant$$

$$\leqslant \frac{\log \left(\frac{n}{k}\right)^{k}}{\log\log \left(\frac{n}{k}\right)^{k}} + O\left(\frac{\log n}{\log\log n}\right) \leqslant \frac{\log C_n^k}{\log\log C_n^k}(1+o(1)) + O\left(\frac{\log n}{\log\log n}\right);$$

$$k = \frac{\log k + \log\log \frac{n}{k}}{\log n - \log k} \frac{\log \left(\frac{n}{k}\right)^k}{\log\log \left(\frac{n}{k}\right)^k} \leqslant \frac{\log k}{\log n - \log k} \frac{\log C_n^k}{\log\log C_n^k}(1+o(1)) =$$

$$= o\left(\frac{\log C_n^k}{\log\log C_n^k}\right).$$

Поэтому окончательно в условиях случая 1 получаем:

$$L^c(k,n) \leqslant \log n\ (1+o(1)) + \frac{\log C_n^k}{\log\log C_n^k}(1+o(1)) =$$

$$= \log n\ (1+o(1)) + \frac{\log \left(\frac{n}{k}\right)^k}{\log\log \left(\frac{n}{k}\right)^k}(1+o(1)) =$$

$$= \log n\ (1+o(1)) + \frac{k\log n}{\log(k\log n)}(1+o(1)).$$

С л у ч а й 2. Пусть выполняется неравенство $n^{1/\log\log n} \leqslant k \leqslant n^{1-1/\log\log n}$. Этот случай достаточно тяжелый, при его разборе используется специальная техника. Полное доказательство содержится в работе [39].

С л у ч а й 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 [89, теорема 1.4].

Следуя [89], для произвольного двоичного набора $\widetilde{\alpha}$ обозначим через $I(\widetilde{\alpha})$ величину $\log C_{|\widetilde{\alpha}|}^{||\widetilde{\alpha}||}$, где $|\widetilde{\alpha}|$ — длина набора $\widetilde{\alpha}$, а $||\widetilde{\alpha}||$ — число единиц в наборе $\widetilde{\alpha}$.

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.

Разобьем исследуемый набор $\widetilde{\alpha}_n^k$ на поднаборы $\widetilde{\alpha}(1)$, $\widetilde{\alpha}(2), \ldots, \widetilde{\alpha}(s)$, «отрезая» слева на i-м шаге, $i = 1, 2, \ldots, s$, кусок $\widetilde{\alpha}(i)$ максимально возможной длины, удовлетворяющий условиям:

$$I(\widetilde{\alpha}(i)) < (1-\tau)\log\log C_n^k,$$
$$|\widetilde{\alpha}(i)| \leqslant 2^t.$$

Оценим число операций конкатенации, достаточное для реализации системы наборов $\widetilde{\alpha}(1)$, $\widetilde{\alpha}(2), \ldots, \widetilde{\alpha}(s)$. 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, сложность реализации системы наборов $\widetilde{\alpha}(1)$, $\widetilde{\alpha}(2), \ldots, \widetilde{\alpha}(s)$ не превосходит величины $(2^t)^3\ 2^{(1-\tau)\log\log C_n^k}$. Но тогда

$$L^c(k,n) = l_c(\widetilde{\alpha}_n^k) \leqslant s + (2^t)^3\ 2^{(1-\tau)\log\log C_n^k}.$$

Оценим сверху величину s. Положим $R = \{i \mid 1 \leqslant i \leqslant s, |\widetilde{\alpha}| \leqslant 2^t - 1\}$. Пусть $i \in R$, т.е. выполняется неравенство $|\widetilde{\alpha}| \leqslant 2^t - 1$. Обозначим $|\widetilde{\alpha}| = a$, $||\widetilde{\alpha}|| = b$.

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

Из соотношений

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

следует неравенство

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

Поэтому

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

С другой стороны, учитывая максимальность набора $\widetilde{\alpha}(i)$, выполняется неравенство $\max\left(C_{a+1}^b, C_{a+1}^{b+1}\right) \geqslant (1-\tau)\log\log C_n^k$. Следовательно, если $i \in R$, то справедлива оценка

$$I(\widetilde{\alpha}(i)) \geqslant (1-\tau)\log\log C_n^k - t.$$

Теперь, с одной стороны, имеем соотношения

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

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

$$\sum_{i=1}^{s} I(\widetilde{\alpha}(i)) = \log\left(C_{|\widetilde{\alpha}(1)|}^{||\widetilde{\alpha}(1)||} C_{|\widetilde{\alpha}(2)|}^{||\widetilde{\alpha}(2)||} \ldots C_{|\widetilde{\alpha}(s)|}^{||\widetilde{\alpha}(s)||}\right) \leqslant$$

$$\leqslant \log\left(C_{|\widetilde{\alpha}(1)|+|\widetilde{\alpha}(2)|+\ldots+|\widetilde{\alpha}(s)|}^{||\widetilde{\alpha}(1)||+||\widetilde{\alpha}(2)||+\ldots+||\widetilde{\alpha}(s)||}\right) = \log C_n^k.$$

Следовательно,

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

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

Таким образом, окончательно получаем:

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

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

Положим

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

Тогда в условиях случая 3 имеем оценку:

$$L^c(k,n) \leqslant (1+o(1))\frac{\log C_n^k}{\log\log C_n^k}.$$

Верхняя оценка доказана.

Нижняя оценка проводится аналогично доказательству нижней оценки сложности вычисления набора степеней (см. теорему 7) путем «объединения» очевидной оценки $l_c(k,n) \geqslant \log n$ и «мощностной» оценки $l_c(k,n) \geqslant \frac{\log C_n^k}{\log\log C_n^k}(1+o(1))$. Теорема 12 доказана.

§ 4. Задача Лупанова

Этот параграф, посвященный задаче о сложности реализации элементов конечных абелевых групп, начнем не так, как большинство других параграфов, в которых прежде всего обсуждается связь исследуемой задачи с остальными. Постановку задачи о сложности вычислений в конечных абелевых группах дадим независимо, а уже потом поговорим о ее связи с другими задачами. Кроме того, в этом параграфе будет немного нарушен общий подход к введению обозначений, принятый в настоящей работе: сложность реализации отдельных объектов обозначается строчной буквой «l» с различными индексами, а различные функции Шеннона — прописными буквами «L». Все это связано прежде всего с тем, что интерес автора к тематике, затрагиваемой в обзоре, начался именно с этой задачи, и хотелось сохранить и постановку задачи, и даже обозначения в первоначальном виде.

Отправной точкой для изложения результатов в этом параграфе и основой для введения новых обозначений являются обнаруженные несколько лет назад три листочка [104] с записями Олега Борисовича Лупанова, датированные, по-видимому, весной 1988 года. В этих листочках О. Б. Лупанов ставил автору задачу о сложности вычисления элементов конечных абелевых групп. Начав с этой задачи, автор постепенно переключился на исследование близких вопросов — задач Беллмана, Кнута и Пиппенджера. Однако представлялось важным вернуться к задаче именно в исходной постановке, поскольку решению задач в изначальной постановке О. Б. Лупанов придавал

большое значение. И за последние примерно девять лет удалось получить ответы по многим аспектам этой задачи, которую будем далее называть *задачей Лупанова*.

4.1. Постановка задачи. Пусть G — конечная абелева группа (групповую операцию будем называть умножением). Подмножество $B = \{a_1, \ldots, a_q\}$ элементов группы будем называть *базисом* в группе G, если G раскладывается в прямое произведение циклических подгрупп, порожденных элементами множества B:

$$G = \langle a_1 \rangle_{u_1} \times \ldots \times \langle a_q \rangle_{u_q},$$

где u_i — порядок элемента a_i, $i = 1, \ldots, q$.

Для каждого элемента g группы G определим его *сложность реализации над базисом* B, обозначаемую через $L(g; B)$, как минимальное число операций умножения, достаточное для вычисления элемента g с использованием элементов множества B, при этом все уже вычисленные элементы могут быть использованы многократно.

Стоит сказать, что, помимо изучения такой, «схемной» сложности элементов конечных групп, немало работ посвящено и исследованию «формульной» сложности (см., например, обзор [14]), однако в настоящей работе рассматривается только схемная сложность. Отметим также, что в алгебре под задачей вычислений в группе понимают, как правило, совсем другую задачу, а именно, задачу распознавания равенства слов в группе (см., например, [93]).

Так же, как и в других задачах, сложность реализации элемента g группы G над базисом B можно интерпретировать на языке схем из функциональных элементов, как это сделано, например, в [31]: на входы схем подаются базисные элементы группы G, сами схемы состоят из двухвходовых элементов, которые по двум представителям группы G, поступающим на входы, реализуют их произведение; под сложностью схемы понимается число функциональных элементов в схеме (т. е. операций умножения), а сложность реализации $L(g; B)$ элемента g группы G над базисом B численно равна минимальной сложности схем, реализующих элемент g над базисом B.

По аналогии с аддитивными цепочками дадим еще такое эквивалентное определение величины $L(g; B)$.

Вычислительной цепочкой S для элемента g конечной абелевой группы G над базисом $B = \{a_1, \ldots, a_q\}$ будем называть последовательность $a_1, \ldots, a_q, h_1, h_2, \ldots, h_r = g$ элементов группы G, удовлетворяющую свойству: для каждого k, $1 \leqslant k \leqslant r$, найдутся два элемента (не обязательно различных) h_{k1} и h_{k2} из множества $\{a_1, \ldots, a_q, h_1, h_2, \ldots, h_{k-1}\}$ (т. е. лежащих в этой последовательности левее элемента h_k) таких, что $h_k = h_{k1} h_{k2}$. Число r называется *длиной вычисления* S для элемента g над базисом B, минимальная длина вычисления элемента g над базисом B совпадает с величиной $L(g; B)$ и называется *сложностью реализации* (*вычисления*) элемента g над базисом B.

Сложность $L(G, B)$ *конечной абелевой группы* G *над базисом* B определим так:

$$L(G, B) = \max_{g \in G} L(g; B).$$

Положим

$$LM(G)=\max_{B\colon B-\text{базис } G} L(G,B),\quad Lm(G)=\min_{B\colon B-\text{базис } G} L(G,B).$$

Так как конечная абелева группа G полностью определяется вектором $\boldsymbol{v}=(v_1,\ldots,v_q)$ порядков примарных циклических подгрупп группы G, то вместо обозначения $LM(G)$ можно использовать обозначение $M(\boldsymbol{v})$, а вместо $Lm(G)$ — $m(\boldsymbol{v})$.

Для абелевой группы, порядки примарных циклических подгрупп которой задаются вектором $\boldsymbol{v}$, будем использовать обозначение $G_{\boldsymbol{v}}$.

Для вектора $\boldsymbol{v}=(v_1,\ldots,v_q)$ обозначим через $\|\boldsymbol{v}\|$ величину $v_1v_2\ldots v_q$. Положим

$$M(n)=\max_{\boldsymbol{v}\colon \|\boldsymbol{v}\|\leqslant n} M(\boldsymbol{v}),\quad m(n)=\max_{\boldsymbol{v}\colon \|\boldsymbol{v}\|\leqslant n} m(\boldsymbol{v}).$$

Кроме того, введем функции $M_{\text{ср}}(n)$ и $m_{\text{ср}}(n)$, характеризующие средние значения соответствующих мер сложности абелевых групп порядка n, определив их равенствами:

$$M_{\text{ср}}(n)=\frac{\sum LM(G)}{A(n)},\quad m_{\text{ср}}(n)=\frac{\sum Lm(G)}{A(n)},$$

где суммы берутся по всем различным (с точностью до изоморфизма) абелевым группам G порядка n, а $A(n)$ — количество попарно неизоморфных абелевых групп порядка n.

Задача заключается в том, чтобы, во-первых, найти числовые функции $f_1(\boldsymbol{v})$ и $f_2(\boldsymbol{v})$, определенные на векторах $\boldsymbol{v}$, характеризующих порядки примарных циклических групп, с помощью которых выражались бы величины $M(\boldsymbol{v})$ и $m(\boldsymbol{v})$ (хотя бы асимптотически или с точностью до порядка при условии, что порядок всей группы стремится к бесконечности); во-вторых, исследовать рост функций $M(n)$ и $m(n)$, а также функций $M_{\text{ср}}(n)$ и $m_{\text{ср}}(n)$, при $n\to\infty$.

Именно в таком виде Олег Борисович Лупанов ставил автору, тогда еще студенту-пятикурснику, задачу о сложности вычисления элементов конечных абелевых групп. С тех пор в этом и близких направлениях был получен ряд результатов, постановки задач видоизменялись, расширялись, переосмысливались, так или иначе все дальше удаляясь от исходной. Однако здесь сделана попытка по возможности наиболее полно ответить как раз на изначально поставленные вопросы.

4.2. Первые продвижения и следствия из результатов для задачи Беллмана. Нахождение точных формул для введенных мер сложности вычислений в конечных абелевых группах представляется нереальной задачей, что подтверждается, в частности, уже обсуждавшейся NP-полнотой [139] задачи Беллмана. Поэтому далее будем говорить только об асимптотических (с ростом порядка группы) оценках (по возможности асимптотически точных или хотя бы точных по порядку).

Достаточно серьезное продвижение в решении этих задач было получено в 1991 г. в работе [31] (см. также краткий вариант [30]). Помимо двух простых нижних оценок (одна из которых стандартная мощностная) сложности конечной абелевой группы над заданным базисом, была получена важная верхняя оценка. Прежде чем сформулировать эти результаты, введем следующие обозначения.

Пусть $G = \langle a_1 \rangle_{u_1} \times \ldots \times \langle a_q \rangle_{u_q}$. Тогда для базиса $B = \{a_1, \ldots, a_q\}$ положим $k(B) = \max\limits_{1 \leqslant i \leqslant q} u_i$. Кроме того, для произвольного базиса B конечной абелевой группы положим $q(B) = |B|$. Иногда будем вместо $q(B)$ использовать обозначение q (если при этом не возникает коллизий).

Итак, в работе [31] установлены следующие нижние оценки:

1) для произвольной конечной абелевой группы G и любого базиса B этой группы справедливо неравенство

$$L(G, B) \geqslant \lfloor \log(k(B) - 1) \rfloor + q(B) - 1;$$

2) для произвольного положительного ε найдется такое положительное $m(\varepsilon)$, что для сложности любой конечной абелевой группы G над базисом B при выполнении условия $|G| > m(\varepsilon)$ справедлива оценка

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

Сформулируем верхнюю оценку для величины $L(G, B)$ из [31] и отметим, что эта оценка впоследствии стала основой для получения асимптотически точного решения задачи Беллмана.

Т е о р е м а 13 [31]. *Существуют такие положительные константы c_1 и c_2, что для произвольной конечной абелевой группы G и любого базиса B этой группы справедливо неравенство*

$$L(G, B) \leqslant \frac{\log |G|}{\log \log |G|} \left(1 + c_1 \left(\frac{\log \log \log |G|}{\log \log |G|}\right)^{1/2}\right) + c_2 \max(\log k(B), q(B)).$$

Здесь стоит отметить, что извлекаемые из доказательства теоремы 13 значения констант c_1 и c_2 достаточно велики.

Тем не менее эти нижние и верхняя оценки устанавливают порядок роста величины $L(G, B)$: при условии $|G| \to \infty$ справедливо равенство

$$L(G, B) = \Theta\left(\frac{\log |G|}{\log \log |G|} + \log k(B) + q(B)\right).$$

Кроме того, в работе [31] исследовался асимптотический рост функции $L(n)$, определяемой равенством $L(n) = \max LM(G)$, где максимум берется по всем абелевым группам G порядка n.

Т е о р е м а 14 [31]. *При $n \to \infty$ справедливо равенство*

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

Тем самым фактически была решена задача об асимптотике роста величины $M(n)$ (несколько подробнее об этом будет сказано ниже).

Собственно, на этом результаты, формально относящиеся к данному направлению, надолго прерываются. Были еще две работы автора [34, 37], являющиеся в некотором смысле логическим продолжением статьи [31], но они посвящены задачам сложности вычислений (в том же самом смысле) в конечных нильпотентных и разрешимых группах и в них новых результатов для класса конечных абелевых групп практически не содержится.

Однако задачи, поставленные О. Б. Лупановым, имеют тесную связь с задачей Беллмана.

Очевидно, что для произвольного элемента $a_1^{n_1}a_2^{n_2}\dots a_m^{n_m}$ абелевой группы $\langle a_1\rangle\times\langle a_2\rangle\times\dots\times\langle a_m\rangle$ справедливо неравенство

$$L\left(a_1^{n_1}a_2^{n_2}\dots a_m^{n_m},\{a_1,a_2,\dots,a_m\}\right)\leqslant l\left(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}\right).$$

Поэтому верхняя оценка сложности в задаче Беллмана — Кнута автоматически дает верхнюю оценку в задаче о сложности вычисления элементов конечных абелевых групп.

С использованием следствия 1 из теоремы 8 или применяя теорему 10, один из результатов работы [31] можно значительно усилить следующим образом.

Т е о р е м а 15. *Пусть* $G=\langle a_1\rangle_{u_1}\times\dots\times\langle a_q\rangle_{u_q}$, $B=\{a_1,\dots,a_q\}$. *Тогда при* $|G|\to\infty$ *справедливы соотношения*

$$\max\left(\frac{\log|G|}{\log\log|G|},\ \log(\max_i u_i)+q\right)\lesssim L(G,B)\lesssim\frac{\log|G|}{\log\log|G|}+\log(\max_i u_i)+q.$$

С получением нижних оценок сложности вычисления элементов конечных абелевых групп через нижние оценки для задачи Беллмана — Кнута, конечно, все не так однозначно. Приведем два примера.

П р и м е р 2. С одной стороны, справедливо равенство $l(x^{31})=7$ (см., например, [23]), а с другой стороны, в группе $\langle a\rangle_{33}$, очевидно, выполняется соотношение $L(a^{31},\{a\})=6$.

Обобщая, получаем, с одной стороны, неравенство

$$l(x^{2^n-1})\geqslant n+\log n-2{,}13,$$

вытекающее из основного результата статьи [182], а с другой, для группы $\langle a\rangle_{2^n+1}$, — равенство

$$L\left(a^{2^n-1},\{a\}\right)=n+1.$$

Таким образом,

$$l(x^{2^n-1})-L\left(a^{2^n-1},\{a\}\right)\geqslant\log n-3{,}13.$$

П р и м е р 3. Для произвольного m обозначим через $(n_1,n_2,\dots,n_m)$ набор, удовлетворяющий двум условиям:

1) $n_i\leqslant 2^m$, $i=1,2,\dots,m$;

2) $l\left(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}\right)=\max l\left(x_1^{t_1}x_2^{t_2}\dots x_m^{t_m}\right)$, где максимум берется по всем наборам $(t_1,t_2,\dots,t_m)$ с целыми неотрицательными компонентами, не превышающими величины 2^m.

Из стандартных мощностных соображений (см., например, [35] или более сильную теорему 7 из настоящей работы) при всех достаточно больших значениях m следует такое неравенство:

$$l\left(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}\right)\geqslant\frac{m^2}{2\log m}.$$

Теперь положим $n=\max\limits_{j=1,2,\dots,m}n_j$, $r_i=2n+1-n_i$ $(i=1,2,\dots,m)$. Отметим, что при всех i, $1\leqslant i\leqslant m$, выполняются неравенства $n_i<r_i$. Рассмотрим группу $\langle a_1\rangle_{r_1}\times\langle a_2\rangle_{r_2}\times\dots\times\langle a_m\rangle_{r_m}$. В этой группе справедлива цепочка равенств:

$$(a_1a_2\dots a_m)^{2n+1}=\prod_{i=1}^m a_i^{2n+1-n_i+n_i}=\prod_{i=1}^m\left(a_i^{r_i}a_i^{n_i}\right)=a_1^{n_1}a_2^{n_2}\dots a_m^{n_m}.$$

Поэтому, используя теорему Брауэра, при $m \to \infty$ получаем следующую оценку:

$$L\left(a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}, \{a_1, a_2, \dots a_m\}\right) \leqslant \log n + o(\log n) + m \lesssim 2m.$$

Следовательно,

$$l\left(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}\right) \gtrsim \frac{\left(L\left(a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}, \{a_1, a_2, \dots a_m\}\right)\right)^2}{8 \log L\left(a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}, \{a_1, a_2, \dots a_m\}\right)},$$

т. е. отличие в порядках роста сложности с увеличением параметра m для двух задач почти квадратичное.

Таким образом, сами нижние оценки, полученные при исследовании задачи Беллмана — Кнута, не могут быть напрямую применены для получения нижних оценок сложности вычислений элементов конечных абелевых групп. Тем не менее почти дословно повторяя рассуждения из работы [32], можно установить следующий факт, аналогичный теореме 7.

Т е о р е м а 16. *Пусть B — базис конечной абелевой группы G. Если выполняется условие*

$$q(B) = o\left(\frac{\log |G|}{\log \log |G|} + \log k(B)\right)$$

при $|G| \to \infty$, то справедлива асимптотическая оценка

$$L(G, B) \gtrsim \frac{\log |G|}{\log \log |G|} + \log k(B).$$

4.3. Задача Лупанова: основные результаты. Изложение результатов, большинство из которых получено в [57], стоит начать с формулировки ответа на первую часть задачи: по большому счету он фактически содержится еще в [31].

Т е о р е м а 17 [57]. *При $n \to \infty$ справедливы равенства*

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

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

Д о к а з а т е л ь с т в о. Справедливость первого равенства следует из теоремы 14 и соотношения

$$M(n) = \max_{1 \leqslant m \leqslant n} L(m).$$

Верхняя оценка второго равенства следует из первого равенства и неравенства $m(n) \leqslant M(n)$. Докажем нижнюю оценку. Воспользуемся теоремой Бертрана — Чебышёва о распределении простых чисел (см., например, [109]), в силу которой найдется простое p, удовлетворяющее условиям $\lceil n/2 \rceil < p < 2\lceil n/2 \rceil$, а следовательно, и неравенствам $n/2 < p \leqslant n$. Тогда

$$m(n) \geqslant L\left(\langle a \rangle_p, \{a\}\right),$$

а доказательство соотношения

$$L\left(\langle a \rangle_m, \{a\}\right) - \log m \gtrsim \frac{\log m}{\log \log m}$$

при $m \to \infty$ содержится в доказательстве нижней оценки теоремы 5 из [31], по существу и составляя это доказательство.

Теорема 17 доказана.

Тем самым решена одна из поставленных О. Б. Лупановым задач: найдена асимптотика роста функций $M(n)$ и $m(n)$ (на самом деле не только асимптотика, но и асимптотика остаточного члена).

Теперь перейдем к исследованию асимптотики роста величин $M(\boldsymbol{v})$ и $m(\boldsymbol{v})$.

Функцию $h(n)$ натурального аргумента будем называть *допустимой*, если выполняется следующее свойство: для любых двух последовательностей натуральных чисел $\{d_n^{(1)}\}$ и $\{d_n^{(2)}\}$, удовлетворяющих условиям:

1) $d_n^{(1)} \to \infty$;

2) $d_n^{(2)}/2 \leqslant d_n^{(1)} \leqslant 2d_n^{(2)}$ для всех достаточно больших значениях n,

при $n \to \infty$ справедливо асимптотическое равенство $h\left(d_n^{(1)}\right) \sim h\left(d_n^{(2)}\right)$.

Заметим, что замена коэффициентов $1/2$ и 2, фигурирующих во втором условии определения, на произвольные константы $1/c$ и c, где $c > 1$, приводит к эквивалентному определению допустимой функции. Поэтому допустимую функцию можно определить как функцию натурального аргумента, допускающую доопределение до медленно меняющейся на бесконечности функции (см., например, [98]).

Т е о р е м а 18 [57]. *При $\|\boldsymbol{v}\| \to \infty$ выполняются соотношения*

$$\frac{\log \|\boldsymbol{v}\|}{\log\log \|\boldsymbol{v}\|} \lesssim m(\boldsymbol{v}) \leqslant M(\boldsymbol{v}) \lesssim \log \|\boldsymbol{v}\|,$$

причем для любых допустимых функций $h_1(n)$ и $h_2(n)$, удовлетворяющих при $n \to \infty$ условиям

$$\frac{\log n}{\log\log n} \lesssim h_1(n) \lesssim h_2(n) \lesssim \log n,$$

найдется последовательность векторов $\boldsymbol{v}_s$, удовлетворяющая условию $\|\boldsymbol{v}_s\| \to \infty$, для которой справедливы соотношения

$$m(\boldsymbol{v}_s) \sim h_1(\|\boldsymbol{v}_s\|), \qquad M(\boldsymbol{v}_s) \sim h_2(\|\boldsymbol{v}_s\|).$$

Д о к а з а т е л ь с т в о. Асимптотическое неравенство

$$m(\boldsymbol{v}) \gtrsim \frac{\log \|\boldsymbol{v}\|}{\log\log \|\boldsymbol{v}\|}$$

следует непосредственно из нижней оценки теоремы 15, соотношения $m(\boldsymbol{v}) \leqslant M(\boldsymbol{v}) \leqslant M(\|\boldsymbol{v}\|)$ очевидны, а для завершения доказательства цепочки соотношений из утверждения теоремы остается применить теорему 17.

Теперь установим существование требуемой последовательности.

Без ограничения общности можно считать, что функции $h_1(n)$ и $h_2(n)$ при всех достаточно больших n удовлетворяют неравенствам

$$\frac{\log n}{\log\log n} \leqslant h_1(n) \leqslant h_2(n) \leqslant \log n + \frac{\log n}{\log\log n}.$$

Действительно, если это не так, то от функций $h_1(n)$ и $h_2(n)$ можно перейти к функциям $\widehat{h}_1(n)$ и $\widehat{h}_2(n)$, определяемым следующим образом:

$$\widehat{h}_1(n) = \max\left\{\frac{\log n}{\log\log n},\ \min\left\{h_1(n),\ h_2(n),\ \log n + \frac{\log n}{\log\log n}\right\}\right\};$$

$$\widehat{h}_2(n) = \min\left\{\max\left\{\frac{\log n}{\log\log n},\ h_1(n),\ h_2(n)\right\},\ \log n + \frac{\log n}{\log\log n}\right\}.$$

Функции $\widehat{h}_1(n)$ и $\widehat{h}_2(n)$ асимптотически равны функциям $h_1(n)$ и $h_2(n)$ соответственно, являются допустимыми и удовлетворяют соотношениям

$$\frac{\log n}{\log\log n} \leqslant \widehat{h}_1(n) \leqslant \widehat{h}_2(n) \leqslant \log n + \frac{\log n}{\log\log n}.$$

Положим

$$t = t(s) = \left\lceil \max\left\{h_1(2^s) - \frac{s}{\log s},\ \frac{s}{(\log s)^2}\right\}\right\rceil,$$

$$d_1 = d_1(s) = \left\lceil \frac{s - \lfloor h_2(2^s) - h_1(2^s)\rfloor}{t}\right\rceil.$$

Тогда, с одной стороны, справедливо неравенство $d_1 \leqslant (\log s)^2 + 1$, а с другой, в силу соотношений

$$s - \lfloor h_2(2^s) - h_1(2^s)\rfloor \geqslant s - h_2(2^s) + h_1(2^s) \geqslant h_1(2^s) - \frac{s}{\log s},$$

выполняется условие $d_1 \geqslant 1$.

Пусть p_1 — максимальное простое число, не превосходящее $2^{\lceil s/(\log s)^2\rceil}$, p_2 — предшествующее числу p_1 простое число (т. е. p_2 — максимальное простое число, меньшее p_1), p_3 — предшествующее числу p_2 простое число и т. д. Определим параметр $d_2 = d_2(s)$ из условия

$$p_1 p_2 \dots p_{d_2-1} < 2^{\lfloor h_2(2^s) - h_1(2^s)\rfloor} \leqslant p_1 p_2 \dots p_{d_2-1} p_{d_2}.$$

Установим корректность определения d_2. В силу теоремы Бертрана — Чебышёва о распределении простых чисел (см., например, [109]) выполняются неравенства

$$p_i \geqslant \frac{2^{\lceil s/(\log s)^2\rceil}}{2^i}, \quad i = 1, 2, \dots \lceil s/(\log s)^2\rceil - 1.$$

Поэтому при $j = \lceil 2(\log s)^2\rceil$ справедливы соотношения

$$\prod_{i=1}^{j} p_i \geqslant \frac{2^{j\lceil s/(\log s)^2\rceil}}{2^1 2^2 \dots 2^j} \geqslant 2^{js/(\log s)^2 - j(j+1)/2} > 2^s \geqslant 2^{\lfloor h_2(2^s) - h_1(2^s)\rfloor}.$$

Следовательно, значение d_2 с требуемыми свойствами существует, причем $d_2 \leqslant \lceil 2(\log s)^2\rceil$.

Теперь определим вектор $\boldsymbol{v}_s = \big(v_1(s), \dots, v_{d_1+d_2}(s)\big)$, положив

$$v_1 = v_2 = \dots = v_{d_1-1} = 2^t, \quad v_{d_1} = 2^{s - \lfloor h_2(2^s) - h_1(2^s)\rfloor - (d_1-1)t},$$

$$v_{d_1+1} = p_1, v_{d_1+2} = p_2, \dots, v_{d_1+d_2-1} = p_{d_2-1}, \quad v_{d_1+d_2} = p_0,$$

где p_0 — наименьшее из простых чисел p, отличных от двух и удовлетворяющих условию

$$p_1 p_2 \dots p_{d_2-1} p \geqslant 2^{\lfloor h_2(2^s) - h_1(2^s)\rfloor}.$$

Тогда выполняются соотношения

$$2^s \leqslant \|\boldsymbol{v}_s\| \leqslant 3 \cdot 2^s, \quad d_1 + d_2 \leqslant 4(\log s)^2 \leqslant 4(\log\log \|\boldsymbol{v}_s\|)^2.$$

Поэтому для любого базиса B группы $G_{\boldsymbol{v}_s}$ выполняется неравенство $q(B) \leqslant (\log\log \|\boldsymbol{v}_s\|)^2$ и, следовательно, в силу теорем 15 и 16, справедливо асимптотическое равенство

$$L(G_{\boldsymbol{v}_s}, B) \sim \frac{\log \|\boldsymbol{v}_s\|}{\log\log \|\boldsymbol{v}_s\|} + \log k(B)$$

в предположении, что $s \to \infty$.

Таким образом, при $s \to \infty$ имеем:

$$m(\boldsymbol{v}_s) \sim \frac{\log \|\boldsymbol{v}_s\|}{\log\log \|\boldsymbol{v}_s\|} + \log v_1 \sim$$

$$\sim \frac{s}{\log s} + \max\left\{h_1(2^s) - \frac{s}{\log s}, \ \frac{s}{(\log s)^2}\right\} \sim h_1\left(2^s\right) \sim h_1(\|\boldsymbol{v}_s\|),$$

$$M(\boldsymbol{v}_s) \sim \frac{\log \|\boldsymbol{v}_s\|}{\log\log \|\boldsymbol{v}_s\|} + \log(v_1 v_{d_1+1} v_{d_1+2} \ldots v_{d_1+d_2}) \sim$$

$$\sim \frac{s}{\log s} + \max\left\{h_1(2^s) - \frac{s}{\log s}, \ \frac{s}{(\log s)^2}\right\} + h_2(2^s) - h_1(2^s) \sim h_2\left(2^s\right) \sim h_2(\|\boldsymbol{v}_s\|).$$

Теорема 18 доказана.

Перейдем к более подробному исследованию величины $M(\boldsymbol{v})$. Пусть группа G представлена как прямое произведение своих примарных циклических компонент:

$$G = \langle a_1\rangle_{v_1} \times \ldots \times \langle a_q\rangle_{v_q}.$$

Обозначим через $q(\boldsymbol{v})$ размерность (число координат) вектора $\boldsymbol{v}$. Далее для каждого простого делителя p_i величины $\|\boldsymbol{v}\|$ обозначим через $P_i(\boldsymbol{v})$ максимальный из порядков примарных циклических подгрупп, являющихся степенями числа p_i. Теперь положим $P(\boldsymbol{v}) = \prod P_i(\boldsymbol{v})$, где произведение берется по всем простым делителям числа $\|\boldsymbol{v}\|$. Легко заметить, что величина $P(\boldsymbol{v})$ численно равна максимальному значению порядка среди всех элементов группы G. Кроме того, всегда найдется базис B_1 группы G, для которого справедливо равенство $k(B_1) = P(\boldsymbol{v})$.

Очевидно, что справедливы оценки $M(\boldsymbol{v}) \geqslant q(\boldsymbol{v}) - 1$, $M(\boldsymbol{v}) \geqslant \log(P(\boldsymbol{v}) - 1)$, но «объединить» их в одно неравенство, подобно неравенству

$$L(G, B) \geqslant \lfloor \log(k(B) - 1)\rfloor + q(B) - 1,$$

не удается. Однако справедлива

Т е о р е м а 19 [57]. *При $\|\boldsymbol{v}\| \to \infty$ справедливо асимптотическое неравенство*

$$M(\boldsymbol{v}) \gtrsim q(\boldsymbol{v}) + \log P(\boldsymbol{v}).$$

Д о к а з а т е л ь с т в о. Отдельно рассмотрим несколько случаев.

С л у ч а й 1. Пусть выполняется неравенство

$$q(\boldsymbol{v}) \leqslant \frac{\log P(\boldsymbol{v})}{\log\log\log \|\boldsymbol{v}\|}.$$

Тогда

$$M(\boldsymbol{v}) \geqslant \log(P(\boldsymbol{v})-1) \gtrsim q(\boldsymbol{v}) + \log P(\boldsymbol{v}).$$

Случай 2. Пусть выполняется неравенство

$$\log P(\boldsymbol{v}) \leqslant \frac{q(\boldsymbol{v})}{\log\log\log\|\boldsymbol{v}\|}.$$

Тогда

$$M(\boldsymbol{v}) \geqslant q(\boldsymbol{v}) - 1 \gtrsim q(\boldsymbol{v}) + \log P(\boldsymbol{v}).$$

Случай 3. Пусть выполняются неравенства

$$q(\boldsymbol{v}) \geqslant \frac{\log P(\boldsymbol{v})}{\log\log\log\|\boldsymbol{v}\|}, \quad \log P(\boldsymbol{v}) \geqslant \frac{q(\boldsymbol{v})}{\log\log\log\|\boldsymbol{v}\|}.$$

Рассмотрим базис B', имеющий среди всех базисов B, удовлетворяющих равенству $k(B)=P(\boldsymbol{v})$, наибольшее значение величины $q(B)$.

Случай 3.1. Пусть выполняется неравенство

$$q(\boldsymbol{v}) - q(B') \leqslant \frac{q(\boldsymbol{v})}{\log\log\log\|\boldsymbol{v}\|}.$$

Тогда, обозначив абелеву группу, задаваемую вектором $\boldsymbol{v}$, через G, получаем:

$$M(\boldsymbol{v}) \geqslant L(G,B') \geqslant q(B') + \log(k(B')-1) - 1 \geqslant$$

$$\geqslant q(\boldsymbol{v}) + \log(P(\boldsymbol{v})-1) - \frac{q(\boldsymbol{v})}{\log\log\log\|\boldsymbol{v}\|} - 1 \sim q(\boldsymbol{v}) + \log P(\boldsymbol{v}).$$

Случай 3.2. Пусть выполняется неравенство

$$q(\boldsymbol{v}) - q(B') > \frac{q(\boldsymbol{v})}{\log\log\log\|\boldsymbol{v}\|}.$$

Тогда в силу определения базиса B', вектор, составленный из порядков элементов базиса B', выглядит (с точностью до перестановки координат) следующим образом. Величина одной из координат равна $k(B')=P(\boldsymbol{v})$, для оставшихся $q(B')-1$ координат существует взаимнооднозначное отображение на $q(B')-1$ координат вектора $\boldsymbol{v}$, сохраняющее величины координат, при этом величины оставшихся $q(\boldsymbol{v})-q(B')+1$ координат вектора $\boldsymbol{v}$ попарно различны. Поэтому

$$P(\boldsymbol{v}) = k(B') \geqslant \prod_{i=1}^{q(\boldsymbol{v})-q(B')+1} (i+1).$$

Следовательно,

$$\log P(\boldsymbol{v}) = k(B') \geqslant \sum_{i=1}^{q(\boldsymbol{v})-q(B')+1} \log(i+1) \geqslant \frac{q(\boldsymbol{v})-q(B')}{2} \log\frac{q(\boldsymbol{v})-q(B')}{2} \geqslant$$

$$\geqslant \frac{1}{4}\frac{q(\boldsymbol{v})}{\log\log\log\|\boldsymbol{v}\|}(\log q(\boldsymbol{v}) - \log\log\log\log\|\boldsymbol{v}\|).$$

Тогда справедливо неравенство

$$q(\boldsymbol{v}) \leqslant 2^{5(\log\log\log\|\boldsymbol{v}\|)^2}.$$

Действительно, если это не так, то из предыдущей цепочки соотношений следует, что при всех достаточно больших значениях $\|\boldsymbol{v}\|$ выполняется неравенство

$$\log P(\boldsymbol{v}) > q(\boldsymbol{v}) \log\log\log \|\boldsymbol{v}\|,$$

что противоречит условиям случая 3.

Таким образом, применяя теорему 18 и учитывая условия случая 3, при $\|\boldsymbol{v}\| \to \infty$ получаем:

$$M(\boldsymbol{v}) \gtrsim \frac{\log \|\boldsymbol{v}\|}{\log\log \|\boldsymbol{v}\|} = \frac{2^{2^{\log\log\log |\boldsymbol{v}|}}}{2^{\log\log\log \|\boldsymbol{v}\|}} > q(\boldsymbol{v}) + q(\boldsymbol{v}) \log\log\log \|\boldsymbol{v}\| \geqslant q(\boldsymbol{v}) + \log P(\boldsymbol{v}).$$

Теорема 19 доказана.

Следующая теорема дает ответ еще на одну часть исходной задачи Лупанова.

Т е о р е м а 20 [57]. *При $\|\boldsymbol{v}\| \to \infty$ выполняются соотношения*

$$\max\left(\frac{\log \|\boldsymbol{v}\|}{\log\log \|\boldsymbol{v}\|},\ q(\boldsymbol{v}) + \log P(\boldsymbol{v})\right) \lesssim M(\boldsymbol{v}) \lesssim \frac{\log \|\boldsymbol{v}\|}{\log\log \|\boldsymbol{v}\|} + q(\boldsymbol{v}) + \log P(\boldsymbol{v}).$$

Д о к а з а т е л ь с т в о. Нижняя оценка непосредственно следует из мощностной нижней оценки и теоремы 19. Для доказательства верхней оценки обозначим для группы G, определяемой вектором $\boldsymbol{v}$, через B_M базис, удовлетворяющий условию $M(\boldsymbol{v}) = L(G, B_M)$. Тогда с использованием верхней оценки теоремы 1 и неравенств $k(B_M) \leqslant P(\boldsymbol{v})$ и $q(B_M) \leqslant q(\boldsymbol{v})$ имеем:

$$M(\boldsymbol{v}) = L(G, B_M) \lesssim \frac{\log |G|}{\log\log |G|} + \log k(B_M) + q(B_M) \leqslant \frac{\log \|\boldsymbol{v}\|}{\log\log \|\boldsymbol{v}\|} + q(\boldsymbol{v}) + \log P(\boldsymbol{v}).$$

Теорема 20 доказана.

Эта теорема устанавливает порядок роста величины $M(\boldsymbol{v})$, причем верхняя оценка может превышать нижнюю асимптотически не более чем в два раза. Кроме того, в случае когда одна из величин $\dfrac{\log \|\boldsymbol{v}\|}{\log\log \|\boldsymbol{v}\|}$ или $q(\boldsymbol{v}) + \log P(\boldsymbol{v})$ растет существенно быстрее другой, т. е. выполняется условие

$$\frac{\log \|\boldsymbol{v}\|}{\log\log \|\boldsymbol{v}\| (\log P(\boldsymbol{v}) + q(\boldsymbol{v}))} + \frac{\log\log \|\boldsymbol{v}\| (\log P(\boldsymbol{v}) + q(\boldsymbol{v}))}{\log \|\boldsymbol{v}\|} \to \infty,$$

теорема 20 устанавливает следующую асимптотику роста функционала сложности $M(\boldsymbol{v})$:

$$M(\boldsymbol{v}) \sim \frac{\log \|\boldsymbol{v}\|}{\log\log \|\boldsymbol{v}\|} + \log P(\boldsymbol{v}) + q(\boldsymbol{v}).$$

Для формулировки оценок асимптотического роста величины $m(\boldsymbol{v})$ введем обозначения. Пусть B — базис конечной абелевой группы G. Положим

$$r(B) = \lfloor \log(k(B) - 1) \rfloor + q(B), \quad r(\boldsymbol{v}) = \min_{B:\ B - \text{базис } G_{\boldsymbol{v}}} r(B).$$

Т е о р е м а 21 [57]. *С одной стороны, при $\|\boldsymbol{v}\| \to \infty$ выполняется верхняя оценка*

$$m(\boldsymbol{v}) \lesssim \frac{\log \|\boldsymbol{v}\|}{\log\log \|\boldsymbol{v}\|} + r(\boldsymbol{v});$$

с другой стороны, при всех достаточно больших значениях $\|\boldsymbol{v}\|$ *справедлива нижняя оценка*

$$m(\boldsymbol{v}) \geqslant \max\left(\frac{\log\|\boldsymbol{v}\|}{\log\log\|\boldsymbol{v}\|},\ r(\boldsymbol{v})-1\right).$$

Нижняя оценка непосредственно следует из двух самых первых нижних оценок, а верхняя — из верхней оценки теоремы 15.

Эта теорема устанавливает порядок роста величины $m(\boldsymbol{v})$, причем опять верхняя оценка может превышать нижнюю асимптотически не более чем в два раза. В случае когда одна из величин $\frac{\log\|\boldsymbol{v}\|}{\log\log\|\boldsymbol{v}\|}$ или $r(\boldsymbol{v})$ растет существенно быстрее другой, т. е. выполняется условие

$$\frac{\log\|\boldsymbol{v}\|}{(\log\log\|\boldsymbol{v}\|)r(\boldsymbol{v})}+\frac{(\log\log\|\boldsymbol{v}\|)r(\boldsymbol{v})}{\log\|\boldsymbol{v}\|}\to\infty,$$

теорема 21 устанавливает следующую асимптотику роста функционала сложности $m(\boldsymbol{v})$:

$$m(\boldsymbol{v})\sim\frac{\log\|\boldsymbol{v}\|}{\log\log\|\boldsymbol{v}\|}+r(\boldsymbol{v}).$$

Перейдем к описанию асимптотического поведения функций $M_{\text{ср}}(n)$ и $m_{\text{ср}}(n)$, характеризующих средние значения соответствующих мер сложности абелевых групп порядка n.

Т е о р е м а 22 [57]. *При* $n\to\infty$ *выполняются соотношения*

$$\frac{\log n}{\log\log n}\lesssim m_{cp}(n)\leqslant M_{cp}(n)\lesssim\log n,$$

причем для любых допустимых функций $h_1(n)$ *и* $h_2(n)$, *удовлетворяющих при* $n\to\infty$ *условиям*

$$\frac{\log n}{\log\log n}\lesssim h_1(n)\lesssim h_2(n)\lesssim\log n,$$

найдется последовательность $\{n_s\}$, *удовлетворяющая условию* $n_s\to\infty$ *при* $s\to\infty$, *для которой справедливы соотношения*

$$m_{cp}(n_s)\sim h_1(n_s);\quad M_{cp}(n_s)\sim h_2(n_s).$$

Д о к а з а т е л ь с т в о. Универсальные соотношения из первой части теоремы непосредственно следуют из теоремы 18, поэтому сразу перейдем к доказательству существования требуемой последовательности.

Также как и при доказательстве теоремы 18 без ограничения общности можно считать, что функции $h_1(n)$ и $h_2(n)$ при всех достаточно больших n удовлетворяют неравенствам

$$\frac{\log n}{\log\log n}\leqslant h_1(n)\leqslant h_2(n)\leqslant\log n+\frac{\log n}{\log\log n}.$$

Положим

$$H_1=H_1(s)=\left\lceil\max\left\{h_1(2^s)-\frac{s}{\log s},\ \frac{s}{(\log s)^2}\right\}\right\rceil;$$

$$H_2 = H_2(s) = \left\lceil \max \left\{ h_2(2^s) - \frac{s}{\log s},\ \frac{s}{(\log s)^2} \right\} \right\rceil .$$

Отметим, что выполняется неравенство $H_2 \leqslant s$.

Пусть p_1 — максимальное простое число, меньшее 2^{H_1}, p_2 — предшествующее числу p_1 простое число (т. е. p_2 — максимальное простое число, меньшее p_1), p_3 — предшествующее числу p_2 простое число и т. д. Определим параметр $d = d(s)$ из условия

$$p_1 p_2 \ldots p_{d-1} < 2^{H_2} \leqslant p_1 p_2 \ldots p_{d-1} p_d.$$

Установим корректность определения d. В силу теоремы Бертрана — Чебышёва о распределении простых чисел (см., например, [109]) выполняются неравенства

$$p_i \geqslant \frac{2^{\lceil s/(\log s)^2 \rceil}}{2^i}, \quad i = 1, 2, \ldots, \lceil s/(\log s)^2 \rceil - 1.$$

Поэтому при $j = \lceil 2(\log s)^2 \rceil$ справедливы соотношения

$$\prod_{i=1}^{j} p_i \geqslant \frac{2^{j\lceil s/(\log s)^2 \rceil}}{2^1 2^2 \ldots 2^j} \geqslant 2^{js/(\log s)^2 - j(j+1)/2} > 2^s \geqslant 2^{H_2}.$$

Следовательно, значение d с требуемыми свойствами существует, причем $d \leqslant \lceil 2(\log s)^2 \rceil$.

Отметим также справедливость неравенства $d \geqslant 2$, вытекающего из соотношений $p_1 < 2^{H_1} \leqslant 2^{H_2}$.

Обозначим через p'_d наименьшее из простых чисел x, отличных от двух и удовлетворяющих условию

$$p_1 p_2 \ldots p_{d-1} x \geqslant 2^{H_2}.$$

Тем самым справедливы неравенства

$$2^{H_2} \leqslant p_1 p_2 \ldots p_{d-1} p'_d < 3 \cdot 2^{H_2}.$$

Теперь положим

$$t = t(s) = s - H_2,$$
$$n_s = 2^t p_1 p_2 \ldots p_{d-1} p'_d.$$

Тогда выполняются неравенства

$$2^s \leqslant n_s < 3 \cdot 2^s.$$

В силу теоремы 16 имеем:

$$m_{\text{ср}}(n_s) \gtrsim \frac{\log n_s}{\log \log n_s} + \log p_1,$$

$$M_{\text{ср}}(n_s) \gtrsim \frac{\log n_s}{\log \log n_s} + \log \left(p_1 p_2 \ldots p_{d-1} p'_d \right).$$

Перейдем к получению верхних оценок величин $m_{\text{ср}}(n_s)$ и $M_{\text{ср}}(n_s)$.

Отметим, что число всех попарно неизоморфных абелевых групп порядка n_s равно числу всех попарно неизоморфных абелевых групп порядка $2^{t(s)}$ и, в свою очередь, равно числу неупорядоченных разбиений числа $t(s)$ на натуральные слагаемые (см., например, [107, 113]). Обозначим это число через $\varrho(t(s))$. Для произвольной абелевой группы G порядка n_s обозначим через B_G^m некоторый базис этой группы, удовлетворяющий условию $Lm(G) = L(G, B_G^m)$, а через B_G^M — некоторый базис, удовлетворяющий условию $LM(G) = L(G, B_G^M)$. Тогда

$$m_{\text{ср}}(n_s) = \frac{\sum L(G, B_G^m)}{\varrho(t(s))}, \quad M_{\text{ср}}(n_s) = \frac{\sum L(G, B_G^M)}{\varrho(t(s))},$$

где суммы берутся по всем $\varrho(t(s))$ различным (с точностью до изоморфизма) абелевым группам G порядка n_s.

Для оценки величин $L(G, B_G^m)$ и $L(G, B_G^M)$ используем справедливую при $|G| \to \infty$ верхнюю оценку из теоремы 15:

$$L(G, B) \lesssim \frac{\log |G|}{\log\log |G|} + \log k(B) + q(B).$$

Рассмотрим два случая.

Случай 1. Пусть выполняется неравенство $t \leqslant \frac{\log n_s}{(\log\log n_s)^2}$. Тогда для любой группы G порядка n_s при $s \to \infty$ выполняются соотношения

$$L(G, B_G^m) \lesssim \frac{\log n_s}{\log\log n_s} + \log(2^t p_1) + (t + d) \sim \frac{\log n_s}{\log\log n_s} + \log p_1;$$

$$L(G, B_G^M) \lesssim \frac{\log n_s}{\log\log n_s} + \log(2^t p_1 p_2 \dots p_{d-1} p'_d) + (t + d) \sim$$
$$\sim \frac{\log n_s}{\log\log n_s} + \log(p_1 p_2 \dots p_{d-1} p'_d).$$

Поэтому

$$m_{\text{ср}}(n_s) \lesssim \frac{\log n_s}{\log\log n_s} + \log p_1; \quad M_{\text{ср}}(n_s) \lesssim \frac{\log n_s}{\log\log n_s} + \log\left(p_1 p_2 \dots p_{d-1} p'_d\right).$$

Случай 2. Пусть выполняется неравенство $t > \frac{\log n_s}{(\log\log n_s)^2}$. Тогда $t \to \infty$ при $s \to \infty$.

Обозначим через $a(t)$ число различных (с точностью до изоморфизма) абелевых групп порядка 2^t, у которых есть примарная компонента порядка не менее $2^{t/(\log t)^2}$, а через $b(t)$ — число различных (с точностью до изоморфизма) абелевых групп порядка 2^t, у которых число примарных компонент не менее $t/(\log t)^2$.

Тогда, учитывая, что $t \leqslant s \leqslant \log n_s$ и $d \leqslant \lceil 2(\log s)^2 \rceil$, можно выписать такие оценки:

$$M_{\text{ср}}(n_s) \lesssim \frac{\log n_s}{\log\log n_s} + \log\left(2^{t/(\log t)^2} p_1 p_2 \dots p_{d-1} p'_d\right) + \left(\frac{t}{(\log t)^2} + d\right) +$$
$$+ \frac{\log(2^t) a(t) + t b(t)}{\varrho(t)} \sim$$

$$\sim \frac{\log n_s}{\log\log n_s} + \log(p_1 p_2 \dots p_{d-1} p'_d) + \frac{ta(t)+tb(t)}{\varrho(t)};$$

$$m_{\mathrm{cp}}(n_s) \lesssim \frac{\log n_s}{\log\log n_s} + \log\left(2^{t/(\log t)^2} p_1\right) + \left(\frac{t}{(\log t)^2} + d\right) +$$

$$+ \frac{\log(2^t)a(t)+tb(t)}{\varrho(t)} \sim$$

$$\sim \frac{\log n_s}{\log\log n_s} + \log p_1 + \frac{ta(t)+tb(t)}{\varrho(t)}.$$

Отметим, что величина $a(t)$ равна числу неупорядоченных разбиений числа t на натуральные слагаемые, наибольшее из которых не менее чем $t/(\log t)^2$, а величина $b(t)$ равна числу неупорядоченных разбиений числа t на не менее чем $t/(\log t)^2$ натуральных слагаемых. Известно (см., например, теорему 4.1.1 из [107]), что число разбиений натурального числа t на u частей равно числу разбиений t на части, наибольшая из которых есть u. Поэтому $a(t) = b(t)$.

Далее, для $i = 1, 2, \dots, t$, обозначив через $\varrho_i(t)$ число неупорядоченных разбиений числа t на i частей, имеем:

$$b(t) = \sum_{i=\lceil t/(\log t)^2\rceil}^{t} \varrho_i(t) \leqslant \sum_{i=\lceil t/(\log t)^2\rceil}^{t} \varrho(t-i) < t\varrho\left(t - \lceil t/(\log t)^2\rceil\right).$$

Теперь, используя асимптотическую формулу (при $n \to \infty$)

$$\varrho(n) \sim \frac{1}{4\sqrt{3}n} e^{\pi\sqrt{\frac{2n}{3}}},$$

которая следует из более сильной теоремы Харди — Рамануджана (см., например, [107, 113]), получаем:

$$\frac{b(t)t}{\varrho(t)} \leqslant \frac{\varrho\left(t - \lceil t/(\log t)^2\rceil\right)}{\varrho(t)} t^2 \sim$$

$$\sim \frac{e^{\pi\sqrt{\frac{2\left(t-\lceil t/(\log t)^2\rceil\right)}{3}}}}{e^{\pi\sqrt{\frac{2t}{3}}}} t^2.$$

Покажем, что последнее выражение стремится к 0 при $t \to \infty$. Действительно, логарифм этой величины стремится к $-\infty$ при $t \to \infty$:

$$\ln\left(\frac{e^{\pi\sqrt{\frac{2\left(t-\lceil t/(\log t)^2\rceil\right)}{3}}}}{e^{\pi\sqrt{\frac{2t}{3}}}} t^2\right) =$$

$$= \pi\sqrt{\frac{2t}{3}}\left(\left(1 - \left(\frac{1}{(\log t)^2}\right) + O\left(\frac{1}{t}\right)\right)^{1/2} - 1\right) + 2\ln t =$$

$$= \pi\sqrt{\frac{2t}{3}}\left(-\left(\frac{1}{2(\log t)^2}\right) + O\left(\frac{1}{(\log t)^4}\right)\right) + 2\ln t =$$

$$= -\pi\sqrt{\frac{2}{12}}\,\frac{\sqrt{t}}{(\log t)^2} + O\left(\frac{\sqrt{t}}{(\log t)^4}\right).$$

Таким образом,

$$\frac{ta(t)+tb(t)}{\varrho(t)}=o(1)$$

и, следовательно, в случае 2 также справедливы верхние оценки

$$m_{\mathrm{cp}}(n_s)\lesssim\frac{\log n_s}{\log\log n_s}+\log p_1;\quad M_{\mathrm{cp}}(n_s)\lesssim\frac{\log n_s}{\log\log n_s}+\log\left(p_1p_2\ldots p_{d-1}p'_d\right).$$

Объединяя верхние оценки с нижними оценками, доказанными ранее, и учитывая допустимость функций h_1 и h_2, получаем:

$$m_{\mathrm{cp}}(n_s)\sim\frac{\log n_s}{\log\log n_s}+\log p_1\sim$$
$$\sim\frac{s}{\log s}+\max\left\{h_1(2^s)-\frac{s}{\log s},\ \frac{s}{(\log s)^2}\right\}\sim h_1(2^s)\sim h_1(n_s);$$

$$M_{\mathrm{cp}}(n_s)\sim\frac{\log n_s}{\log\log n_s}+\log\left(p_1p_2\ldots p_{d-1}p'_d\right)\sim$$
$$\sim\frac{s}{\log s}+\max\left\{h_2(2^s)-\frac{s}{\log s},\ \frac{s}{(\log s)^2}\right\}\sim h_2(2^s)\sim h_2(n_s).$$

Теорема 22 доказана.

4.4. Сравнение оценок сложности в задачах Беллмана и Лупанова. Как уже отмечалось, для произвольного элемента $a_1^{n_1}a_2^{n_2}\ldots a_m^{n_m}$ абелевой группы $\langle a_1\rangle\times\langle a_2\rangle\times\ldots\times\langle a_m\rangle$ справедливо неравенство

$$L\left(a_1^{n_1}a_2^{n_2}\ldots a_m^{n_m};\{a_1,a_2,\ldots,a_m\}\right)\leqslant l\left(x_1^{n_1}x_2^{n_2}\ldots x_m^{n_m}\right).$$

Поэтому верхняя оценка сложности в задаче Беллмана автоматически дает верхнюю оценку в задаче Лупанова. С другой стороны, нижние оценки, полученные при исследовании задачи Беллмана — Кнута, не могут быть напрямую применены для получения нижних оценок сложности вычислений элементов конечных абелевых групп — об этом говорят примеры 2 и 3 на с. 163. Однако многие методы получения нижних оценок работают и при нахождении нижних границ сложности реализации элементов конечных абелевых групп — в первую очередь это касается неконструктивных мощностных оценок, позволяющих оценивать снизу сложность почти всех объектов из заданного класса. Дополнительные трудности в получении нижних оценок сложности вычисления элементов конечных абелевых групп, по сравнению с нахождением нижних границ сложности в задаче Беллмана, не помешали получить удовлетворительные ответы на поставленные О. Б. Лупановым задачи путем прямого применения верхних и адаптации нижних оценок сложности, полученных при исследовании задачи Беллмана — Кнута (см. теоремы 17–22). При этом вопрос о возможной степени различия значений сложности в задачах Лупанова и Беллмана пока оставался практически незатронутым. Теперь перейдем именно к этому вопросу. Для его формализации сначала дадим некоторые определения.

Пусть g — произвольный элемент конечной абелевой группы G, заданной своим базисом $B=\{a_1,\ldots,a_q\}$. Представление элемента g в базисе B, имеющее вид

$$g=a_1^{n_1}a_2^{n_2}\ldots a_q^{n_q},$$

будем называть *каноническим*, если для всех значений i, $1 \leqslant i \leqslant q$, выполняются неравенства $0 \leqslant n_i \leqslant u_1 - 1$, где u_i — порядок базисного элемента a_i.

Будем говорить, что представлению элемента g в базисе $B = \{a_1, \ldots, a_q\}$ конечной абелевой группы G *соответствует* одночлен $x_1^{n_1} x_2^{n_2} \ldots x_q^{n_q}$, если набор показателей степеней переменных в одночлене совпадает с набором показателей степеней базисных элементов в каноническом представлении элемента g в базисе B. Одночлен, соответствующий представлению элемента g в базисе B, будем обозначать через $P[g; B]$.

Для произвольного натурального n, $n \geqslant 2$, положим

$$\sigma(n) = \max \{l(P[g; B]) - L(g; B)\}, \qquad \pi(n) = \max \frac{l(P[g; B])}{L(g; B)},$$

где максимумы берутся по всем элементам и всем базисам всех абелевых групп, имеющих порядок, не превосходящий n.

Функции $\sigma(n)$ и $\pi(n)$ показывают на сколько и, соответственно, во сколько раз вычисление элемента конечной абелевой группы порядка не более n в каком-либо базисе этой группы может быть экономнее по сравнению с вычислением одночлена, соответствующего представлению этого элемента в выбранном базисе. Постановки задач об исследовании поведения функций $\sigma(n)$ и $\pi(n)$ идейно сильно перекликаются с некоторыми задачами, обсуждаемыми в обзоре [152], при этом стоит отметить, что в решении этих задач общего уже существенно меньше.

Т е о р е м а 23. *При $n \to \infty$ справедливо асимптотическое равенство*

$$\sigma(n) \sim \frac{\log n}{\log \log n}.$$

Д о к а з а т е л ь с т в о. *Верхняя оценка.* Пусть $G = \langle a_1 \rangle_{u_1} \times \ldots \times \langle a_q \rangle_{u_q}$, $|G| \leqslant n$. Для произвольного элемента g этой группы, заданного каноническим представлением $g = a_1^{n_1} a_2^{n_2} \ldots a_q^{n_q}$, обозначим через q_g число ненулевых показателей степеней в этом каноническом представлении. Тогда, с одной стороны, для сложности реализации элемента g в базисе $B = \{a_1, \ldots, a_q\}$ справедливо неравенство

$$L(g; B) \geqslant \lceil \log \max n_i \rceil + q_g - 1,$$

а с другой — из теоремы 10 вытекают соотношения

$$l\left(x_1^{n_1} x_2^{n_2} \ldots x_q^{n_q}\right) \leqslant \log \max_i n_i + \frac{\log\left(\prod (n_i + 1)\right)}{\log \log \left(\prod (n_i + 1)\right)}(1 + o(1)) + q_g \leqslant$$
$$\leqslant \log \max_i n_i + \frac{\log |G|}{\log \log |G|}(1 + o(1)) + q_g.$$

Поэтому

$$\sigma(n) \leqslant \frac{\log |G|}{\log \log |G|}(1 + o(1)) \leqslant \frac{\log n}{\log \log n}(1 + o(1)).$$

Нижняя оценка. Обозначим через $m = m(n)$ натуральное число, не превосходящее $2^{\lfloor \log n \rfloor - 1}$ и удовлетворяющее условию $l(x^m) = \max l\left(x^t\right)$, где максимум берется по всем значениям t, не превосходящим $2^{\lfloor \log n \rfloor - 1}$. Тогда в силу нижней оценки сложности возведения в степень (теорема 2) при $n \to \infty$ верно асимптотическое неравенство

$$l(x^n) - \log n \gtrsim \frac{\log n}{\log \log n}.$$

Теперь рассмотрим циклическую группу порядка $2^{\lfloor \log n \rfloor} - m$ с порождающим элементом a. В этой группе справедливы равенства $a^m = a^{2^{\lfloor \log n \rfloor} - m + m} = a^{2^{\lfloor \log n \rfloor}}$. Поэтому $L(a^m; \{a\}) \leqslant \lfloor \log n \rfloor$. Следовательно,

$$\sigma(n) \gtrsim \frac{\log n}{\log \log n}.$$

Нижняя оценка, а с ней и вся теорема 23, доказана.

Т е о р е м а 24. *При $n \to \infty$ справедливо асимптотическое равенство*

$$\pi(n) \sim \frac{\sqrt{\log n}}{2 \log \log n}.$$

Д о к а з а т е л ь с т в о.

Верхняя оценка. Используя обозначения и соотношения из доказательства верхней оценки теоремы 23, получаем:

$$\frac{l(P[g;B])}{L(g;B)} \leqslant \frac{\log \max\limits_i n_i + \frac{\log\left(\prod(n_i+1)\right)}{\log\log\left(\prod(n_i+1)\right)}(1+o(1)) + q_g}{\lceil \log \max n_i \rceil + q_g - 1}.$$

Далее, из соотношения

$$\log(n_1+1) + \log(n_2+1) + \ldots + \log(n_q+1) \leqslant q \log \max(n_i+1),$$

используя неравенство между средним арифметическим и средним геометрическим, получаем, что

$$q + \log \max(n_i+1) \geqslant 2\sqrt{\log\left(\prod(n_i+1)\right)}.$$

Поэтому

$$\frac{l(P[g;B])}{L(g;B)} \leqslant \frac{\sqrt{\log\left(\prod(n_i+1)\right)}}{2\log\log\left(\prod(n_i+1)\right)}(1+o(1)) \leqslant \frac{\sqrt{\log|G|}}{2\log\log|G|}(1+o(1)) \leqslant \frac{\sqrt{\log n}}{2\log\log n}(1+o(1)).$$

Следовательно,

$$\pi(n) \leqslant \frac{\sqrt{\log n}}{2\log\log n}(1+o(1)).$$

Нижняя оценка. Положим

$$q = q(n) = \left\lfloor \sqrt{\log n} \right\rfloor, \quad m = m(n) = \left\lfloor 2^{\sqrt{\log n} - 1} \right\rfloor.$$

Обозначим через $\widetilde{k} = \widetilde{k}(n) = (k_1, k_2, \ldots, k_q)$ набор натуральных чисел, не превосходящих m, удовлетворяющий условию

$$l\left(x_1^{k_1} x_2^{k_2} \ldots x_q^{k_q}\right) = \max_{(t_1,\ldots,t_q)\,:\,t_i \leqslant m} l\left(x_1^{t_1} x_2^{t_2} \ldots x_q^{t_q}\right).$$

При $n \to \infty$ мощностная нижняя оценка (см., например, теорему 7) устанавливает асимптотическое соотношение

$$l\left(x_1^{k_1} x_2^{k_2} \ldots x_q^{k_q}\right) \gtrsim \frac{\log(m+1)^q}{\log\log(m+1)^q} = \frac{q\log(m+1)}{\log q + \log\log(m+1)} \sim \frac{\log n}{\log\log n}.$$

Рассмотрим абелеву группу G, имеющую вид $G = \langle a_1\rangle_{u_1} \times \ldots \times \langle a_q\rangle_{u_q}$, где $u_i = 2m - k_i$, для $i = 1, 2, \ldots, q$. Оценим порядок этой группы: $|G| = u_1 u_2 \ldots u_q \leqslant (2m)^q \leqslant 2^{q(\log m+1)} \leqslant n$.

Для сложности реализации в базисе $B = \{a_1, \ldots, a_q\}$ элемента $g = a_1^{k_1} a_2^{k_2} \ldots a_q^{k_q}$ группы G в силу равенств

$$a_i^{k_i} = a_i^{2m-k_i+k_i} = a_i^{2m} = a_i^{2^{\left\lfloor 2\sqrt{\log n}-1\right\rfloor}}, \quad i = 1, 2, \ldots, q,$$

верна оценка

$$L(g; B) \leqslant \log m + q \leqslant 2\sqrt{\log n}.$$

Таким образом,

$$\pi(n) \geqslant \frac{l\left(x_1^{k_1} x_2^{k_2} \ldots x_q^{k_q}\right)}{L(g; B)} \gtrsim \frac{\sqrt{\log n}}{2 \log\log n}.$$

Нижняя оценка, а с ней и вся теорема 24, доказаны.

Отметим, что доказанные в теоремах 23 и 24 нижние оценки величин $\sigma(n)$ и $\pi(n)$ ввиду использования мощностной нижней оценки для задачи Беллмана носят неконструктивный характер и не дают возможности предъявить элемент и базис конечной абелевой группы, для которых соотношение сложности для соответствующей задачи Беллмана и сложности этого элемента в выбранном базисе было достаточно велико. При сравнении сложности реализации системы элементов конечных абелевых групп и сложности соответствующей системы одночленов ситуация может быть иной, что подтверждается приведенным ниже примером.

Пример 4. Пусть выполняется условие $p = p(n) = o\left(\sqrt{\log n}\right)$ при $n \to \infty$. Положим

$$m = m(n) = \left\lfloor \frac{\sqrt[p]{n}}{2^{(p+1)/2}} \right\rfloor.$$

Отметим, что $\log m \sim (\log n)/p$ при $n \to \infty$.

Рассмотрим абелеву группу

$$G = \langle a_1\rangle_{2m} \times \langle a_2\rangle_{2^2 m} \times \ldots \times \langle a_{p-1}\rangle_{2^{p-1}m} \times \langle a_p\rangle_{2^{p-1}m+1}.$$

Оценим сверху порядок этой группы: $|G| < m^p 2^{p(p+1)/2} \leqslant n$.

Выберем в группе G систему элементов $\{g_1, \ldots, g_p\}$, задаваемых в базисе $B = \{a_1, a_2, \ldots, a_p\}$ следующими каноническими представлениями: $g_1 = a_1^m \ldots a_p^m$, $g_2 = a_2^{2m} \ldots a_p^{2m}, \ldots, g_p = a_p^{2^{p-1}m}$. С использованием равенств $g_{i+1} = g_i^2$, $i = 1, \ldots, p-1$ получаем соотношения

$$L(g_1, \ldots, g_p; B) \leqslant \log m(1 + o(1)) + 2(p-1) \sim \log m.$$

С другой стороны, применяя нижнюю оценку через логарифм определителя матрицы, задающей показатели степеней в одночленах системы (см. например, [43,170] или теорему 26 из следующего параграфа), имеем:

$$l\left(x_1^m \ldots x_p^m, x_2^{2m} \ldots x_p^{2m}, \ldots, x_p^{2^{p-1}m}\right) \geqslant \log\left(m^p 2^{(p-1)p/2}\right) + p - 1 \sim p \log m.$$

Таким образом,

$$l\left(x_1^m \dots x_p^m, x_2^{2m} \dots x_p^{2m}, \dots, x_p^{2^{p-1}m}\right) - L(g_1, \dots, g_p; B) \gtrsim \frac{p-1}{p} \log n.$$

Тем самым приведен конструктивный пример системы из p, $p \geqslant 2$, элементов конечной абелевой группы, для которой при реализации этой системы в некотором базисе экономия в количестве операций по сравнению с вычислением системы одночленов, соответствующих представлениям этих элементов, составляет по порядку логарифм от порядка группы.

§ 5. Задача Пиппенджера

Задача Пиппенджера является центральной для настоящей работы. Большинство обсуждаемых в ней задач либо представляют собой частные случаи задачи Пиппенджера, либо служат аналогами этой задачи для близких вычислительных моделей. Параграф про задачу Пиппенджера вполне может быть отправной точкой для читателя и поэтому представляется естественным кратко напомнить основные определения.

Пусть задана система из p нормированных одночленов от q переменных:

$$f_1 = x_1^{a_{11}} x_2^{a_{12}} \dots x_q^{a_{1q}},$$

$$f_2 = x_1^{a_{21}} x_2^{a_{22}} \dots x_q^{a_{2q}},$$

$$\dots$$

$$f_p = x_1^{a_{p1}} x_2^{a_{p2}} \dots x_q^{a_{pq}},$$

описываемая целочисленной неотрицательной (с неотрицательными элементами) матрицей $A = (a_{ij})$ размера $p \times q$. Обозначим через $l(f_1, f_2, \dots, f_p)$ (будем использовать также обозначение $l(A)$) 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. Назовем *векторной аддитивной цепочкой* (см., например, [119, 121, 173, 188]) для целочисленной неотрицательной матрицы $A = (a_{ij})$ размера $p \times q$ последовательность q-мерных векторов (наборов) вида

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

начинающуюся с q единичных векторов и удовлетворяющую следующим условиям:

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

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

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 [70, 97]), 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 изучения величины $l(f_1, f_2, \ldots, f_p)$ поставлена в 1980 г. Н. Пиппенджером [177] и, соответственно, называется *задачей Пиппенджера*.

Прежде чем перейти к достаточно подробному описанию известных результатов для этой задачи, напомним, что задача Пиппенджера обладает важнейшим свойством двойственности, которое в общем виде можно условно сформулировать так: по решению некоторой задачи, соответствующей матрице A, можно предложить решение с такой же (или почти такой же) трудоемкостью для аналогичной задачи, соответствующей матрице A^T, где A^T — матрица, получающаяся из матрицы A транспонированием. Применительно к задаче Пиппенджера это свойство описывается теоремой 4: для любой целочисленной матрицы A с неотрицательными элементами размера $p \times q$ без нулевых строк и столбцов выполняется равенство

$$l(A) + p = l\left(A^T\right) + q.$$

5.1. Функция Шеннона сложности вычисления систем одночленов. Следуя Н. Пиппенджеру [177], положим $L(p, q, K) = \max l(A)$ при $K \geqslant 2$, где максимум берется по всем целочисленным матрицам $A = (a_{ij})$ с неотрицательными элементами без нулевых строк размера $p \times q$, удовлетворяющим условиям $a_{ij} \leqslant K - 1,\ i = 1, \ldots, p,\ j = 1, \ldots, q$. Таким образом, $L(p, q, K)$ — максимально возможная сложность таких систем из p одночленов от q переменных, что все показатели степеней переменных в одночленах не превосходят $K - 1$. Функцию $L(p, q, K)$ будем называть *функцией Шеннона сложности вычисления систем одночленов*.

В 1980 г. Н. Пиппенджер [177], существенно опираясь на результат своей работы [175], в которой была завершена начатая О. Б. Лупановым и Э. И. Нечипоруком разработка методов построения асимптотически наилучших вентильных схем с кратными путями (подробнее см. § 8 настоящей работы), получил фундаментальный результат: при слабых ограничениях он установил асимптотику роста величины $L(p, q, K)$.

Теорема 25 (Н. Пиппенджер [177]). *При выполнении условия* $pq \log K \to \infty$ *имеет место равенство*

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

Доказательство этой важной теоремы здесь не приводится по следующим причинам. Технически непростое доказательство верхней оценки функции Шеннона, содержащееся в [177], является лишь заключительным этапом полного доказательства, основанного на асимптотически наилучшем методе [175] построения вентильных схем с кратными путями,

о котором будет сказано в § 8 и который, в свою очередь, базируется на методах построения классических вентильных схем из работ О. Б. Лупанова [66] и Э. И. Нечипорука [85, 89]. Тем самым полное доказательство верхней оценки заняло бы слишком много места. С нижней оценкой ситуация тоже нетривиальная. С одной стороны, справедливы оценка $L(p, q, K) \gtrsim \frac{pq \log K}{\log(pq \log K)}$, получающаяся из стандартных мощностных соображений, и почти очевидная оценка $L(p, q, K) \geqslant \min(p,\ q) \log(K - 1)$, которые вместе дают нижнюю оценку

$$L(p, q, K) \gtrsim \max\left(\min(p,\ q) \log K,\ \frac{pq \log K}{\log(pq \log K)}\right).$$

Тем самым в [177] эта нижняя оценка «всего лишь» усилена в случае, когда величины $\min(p,\ q) \log K$ и $\frac{pq \log K}{\log(pq \log K)}$ имеют при $pq \log K \to \infty$ одинаковый порядок роста, да и в этом случае получено повышение нижней оценки асимптотически не более чем вдвое. Однако на самом деле это формально незначительное усиление, во-первых, очень непросто, а во-вторых, позволяет завершить процесс нахождения асимптотики роста функции Шеннона.

Последнюю фразу стоит прокомментировать отдельно. В асимптотической теории сложности принято считать, что задача о сложности вычисления систем функций получает асимптотически точное решение (в данном случае на уровне оценивания функции Шеннона), если найдена асимптотика роста сложности при условии, что количество полюсов в задаче (суммарное число входов и выходов) растет существенно медленнее сложности. Поэтому в этом смысле можно говорить, что для задачи о сложности вычисления систем одночленов Н. Пиппенджером в [177] получено асимптотически точное решение задачи о поведении соответствующей функции Шеннона.

Некоторые дополнения и уточнения оценок из теоремы 25, а также более простое доказательство верхней оценки в случае, названном Пиппенджером «трудным», даны в работе [10].

Также стоит упомянуть работу [38], в которой исследовалась функция Шеннона (наверное, точнее — функция шенноновского типа), численно равная максимальной сложности реализации систем одночленов, задаваемых матрицами, элементы которых не превосходят некоторого значения, индивидуального для элементов каждого столбца (строки). Для этой функции установлен порядок роста, а при некоторых ограничениях найдена и асимптотика.

5.2. Универсальная нижняя оценка. В формуле из теоремы 25, оценивающей функцию Шеннона сложности вычисления систем одночленов, при ограниченных или слаборастущих значениях параметров p и q, численно равных количеству переменных и одночленов соответственно, основным слагаемым является выражение, получаемое не из мощностных соображений. Этот факт оставляет надежду на получение достаточно точных оценок сложности вычисления конкретных последовательностей систем одночленов, состоящих из фиксированного числа одночленов от фиксированного числа переменных.

Первый шаг в этом направлении — получение немощностной нижней оценки. В ее основе лежат известные соображения об оценке сложности

схемы через определитель матрицы, порождаемой вычисляемыми в вершинах схемы функциями. Впервые, по-видимому, рассуждения такого типа для нижних оценок сложности были использованы в работе [170].

Эта оценка носит в некотором смысле универсальный характер — помимо вычислительной модели, использующей только операцию вычитания, она справедлива еще для нескольких моделей, в том числе для двух моделей, которым посвящены следующие два параграфа. Доказывать универсальную нижнюю оценку через определитель будем сразу для трех моделей. Для этого введем еще две меры сложности целочисленных (уже не обязательно неотрицательных) матриц.

Пусть $A=(a_{ij})$ — целочисленная матрица размера $p\times q$, которой естественным образом сопоставлена система M_A, состоящая из функций $x_1^{a_{11}}x_2^{a_{12}}\ldots x_q^{a_{1q}}$, $x_1^{a_{21}}x_2^{a_{22}}\ldots x_q^{a_{2q}}$, $\ldots$, $x_1^{a_{p1}}x_2^{a_{p2}}\ldots x_q^{a_{pq}}$.

Обозначим через $l_2(A)$ минимально возможную сложность (число элементов) схемы из функциональных элементов со входами $x_1, x_2, \ldots, x_q$, на выходах которой вычисляются все функции системы M_A, а сама схема состоит из двухвходовых элементов, реализующих либо произведение, либо частное функций, подаваемых на входы элемента.

Далее, обозначим через $l_F(A)$ минимально возможную сложность (число элементов) 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 все функции системы M_A, а сама схема состоит из двухвходовых элементов, реализующих произведение функций, подаваемых на входы элемента.

Наконец, введем вспомогательную модель, сочетающую возможности всех трех моделей, и для нее обозначим через $\widetilde{l}(A)$ минимально возможную сложность (число элементов) 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 $x_1^{a_{11}}x_2^{a_{12}}\ldots x_q^{a_{1q}}$, $x_1^{a_{21}}x_2^{a_{22}}\ldots x_q^{a_{2q}}$, $\ldots$, $x_1^{a_{p1}}x_2^{a_{p2}}\ldots x_q^{a_{pq}}$, а сама схема состоит из двухвходовых элементов, реализующих либо произведение, либо частное функций, подаваемых на входы элемента.

В силу данных определений имеют место неравенства

$$l_2(A)\geqslant\widetilde{l}(A),\quad l_F(A)\geqslant\widetilde{l}(A),$$

а если в матрице A все элементы неотрицательные и в ней нет нулевых строк, то справедливо и неравенство

$$l(A)\geqslant\widetilde{l}(A).$$

Сформулируем утверждение, являющееся основой для доказательства нужных нижних оценок. Как уже отмечалось, аналогичный результат был получен в работе [170]. В более общем виде он содержится в [43, 46].

Лемма 10 [43, 46, 48]. *Пусть в k вершинах схемы S, состоящей из элементов умножения и деления, со входами x_1, x_1^{-1}, x_2, x_2^{-1}, $\ldots$, x_k, x_k^{-1} реализуется система функций*

$$\{x_1^{a_{11}}x_2^{a_{12}}\ldots x_k^{a_{1k}},\ x_1^{a_{21}}x_2^{a_{22}}\ldots x_k^{a_{2k}},\ \ldots,\ x_1^{a_{k1}}x_2^{a_{k2}}\ldots x_k^{a_{kk}}\},$$

задаваемая целочисленной матрицей $A=(a_{ij})$ размера $k\times k$. Тогда

$$2^{\widetilde{l}(S)}\geqslant|\det A|.$$

Доказательство. Зафиксируем множество

$$\{x_1, x_1^{-1}, x_2, x_2^{-1}, \ldots, x_k, x_k^{-1}\}$$

символов, приписываемых входам схем. Утверждение леммы будем доказывать индукцией по сложности схемы S, т. е. по величине $\widetilde{l}(S)$.

Если $\widetilde{l}(S) = 0$, то в вершинах схемы S (а в схеме есть только входные вершины) вычисляются функции $x_1, x_1^{-1}, x_2, x_2^{-1}, \ldots, x_k, x_k^{-1}$ и, следовательно, в каждой строке матрицы A, задающей такую систему функций, по одному ненулевому элементу и по $k-1$ нулей, причем ненулевые элементы по абсолютной величине равны 1. Поэтому $|\det A| \leqslant 1$ и доказываемое неравенство выполняется.

Докажем утверждение леммы для произвольной схемы S сложности $\widetilde{l}(S)$, $\widetilde{l}(S) \geqslant 1$, в предположении, что для любой схемы сложности менее $\widetilde{l}(S)$ лемма справедлива. Пусть v_1 — невходовая вершина (элемент) схемы S, в которой реализуется функция, не использующаяся для дальнейших вычислений в схеме S, т. е. эта функция не подается на вход никакого элемента схемы.

Схему, получающуюся из схемы S удалением вершины v_1 и ребер, входящих в эту вершину, обозначим через S'. Очевидно, что $\widetilde{l}(S') = \widetilde{l}(S) - 1$.

Пусть в схеме S произвольным образом выбраны k вершин. Если среди выбранных вершин нет вершины v_1, то утверждение леммы для этих k вершин следует из предположения индукции, так как $2^{\widetilde{l}(S)} > 2^{\widetilde{l}(S')} \geqslant |\det A|$. Если вершина v_1 выбрана более одного раза, то утверждение леммы также выполняется, так как в этом случае в соответствующей матрице будут две одинаковые строки и определитель этой матрицы будет равен 0. Поэтому можно считать, что среди выбранных вершин вершина v_1 содержится ровно один раз. Пусть в вершине v_1 вычисляется функция $x_1^{a_{11}} x_2^{a_{12}} \ldots x_k^{a_{1k}}$, а в остальных выбранных вершинах $v_2, v_3, \ldots, v_k$ — соответственно функции $x_1^{a_{21}} x_2^{a_{22}} \ldots x_k^{a_{2k}}$, $x_1^{a_{31}} x_2^{a_{32}} \ldots x_k^{a_{3k}}, \ldots, x_1^{a_{k1}} x_2^{a_{k2}} \ldots x_k^{a_{kk}}$.

Пусть на входы элемента, соответствующего вершине v_1, подаются функции $x_1^{a'_{11}} x_2^{a'_{12}} \ldots x_k^{a'_{1k}}$ и $x_1^{a''_{11}} x_2^{a''_{12}} \ldots x_k^{a''_{1k}}$, вычисляемые в вершинах v' и v'' соответственно. Тогда в зависимости от того, какая операция приписана вершине v_1 — умножение или деление — имеет место либо равенство

$$x_1^{a_{11}} x_2^{a_{12}} \ldots x_k^{a_{1k}} = x_1^{a'_{11}+a''_{11}} x_2^{a'_{12}+a''_{12}} \ldots x_k^{a'_{1k}+a''_{1k}},$$

либо равенство

$$x_1^{a_{11}} x_2^{a_{12}} \ldots x_k^{a_{1k}} = x_1^{a'_{11}-a''_{11}} x_2^{a'_{12}-a''_{12}} \ldots x_k^{a'_{1k}-a''_{1k}}.$$

Обозначим через A' и A'' матрицы, получающиеся из матрицы A заменой первой строки на строки $(a'_{11}, a'_{12}, \ldots, a'_{1k})$ и $(a''_{11}, a''_{12}, \ldots, a''_{1k})$ соответственно. Обозначив через $\pi(\sigma)$ число инверсий в подстановке σ, получаем:

$$\begin{aligned}
|\det A| &= \left| \sum_{\sigma \in S_k} (-1)^{\pi(\sigma)} (a'_{1,\sigma(1)} \pm a''_{1,\sigma(1)}) a_{2,\sigma(2)} \ldots a_{k,\sigma(k)} \right| = \\
&= \left| \sum_{\sigma \in S_k} (-1)^{\pi(\sigma)} a'_{1,\sigma(1)} a_{2,\sigma(2)} \ldots a_{k,\sigma(k)} \pm \right. \\
&\qquad \left. \pm \sum_{\sigma \in S_k} (-1)^{\pi(\sigma)} a''_{1,\sigma(1)} a_{2,\sigma(2)} \ldots a_{k,\sigma(k)} \right| = \\
&= |\det A' \pm \det A''| \leqslant |\det A'| + |\det A''| .
\end{aligned}$$

Для наборов вершин $(v', v_2, \ldots, v_k)$ и $(v'', v_2, \ldots, v_k)$ схемы S' по предположению индукции справедливо утверждение леммы. Поэтому

$$|\det A| \leqslant |\det A'| + |\det A''| \leqslant 2^{\widetilde{l}(S')} + 2^{\widetilde{l}(S')} = 2^{\widetilde{l}(S)}.$$

Лемма 10 доказана.

Для вычислительной модели, допускающей операции умножения и деления, немного усилим утверждение леммы 10.

Лемма 11 [43]. *Пусть в k вершинах состоящей из элементов умножения и деления схемы S со входами $x_1, x_2, \ldots, x_k$ реализуется система функций*

$$\{x_1^{a_{11}} x_2^{a_{12}} \ldots x_k^{a_{1k}},\ x_1^{a_{21}} x_2^{a_{22}} \ldots x_k^{a_{2k}},\ \ldots,\ x_1^{a_{k1}} x_2^{a_{k2}} \ldots x_k^{a_{kk}}\},$$

задаваемая целочисленной матрицей $A=(a_{ij})$ размера $k\times k$. Тогда

$$2^{l_2(S)-\delta(S)} \geqslant |\det A|,$$

где величина $\delta(S)$ равна 0, если в схеме S нет ни одного элемента деления и в вершинах схемы S реализуются только функции, являющиеся степенями входных переменных, и равна 1 в остальных случаях.

Доказательство. Пусть множество входных переменных $x_1, x_2, \ldots, x_k$ фиксировано. Утверждение леммы будем доказывать индукцией по сложности схемы S, т. е. по величине $l_2(S)$.

Если $l_2(S) = 0$, то в вершинах схемы S (а в схеме есть только входные вершины) вычисляются функции $x_1, x_2, \ldots, x_k$ и, следовательно, в каждой строке матрицы A, задающей такую систему функций, по одной единице и по $k-1$ нулей. Поэтому $\delta(S)=0$ и $|\det A| \leqslant 1$. Тогда

$$2^{l_2(S)-\delta(S)} = 1 \geqslant |\det A|.$$

Докажем утверждение леммы для произвольной схемы S сложности $l_2(S)$, $l_2(S) \geqslant 1$, в предположении, что для любой схемы сложности менее $l_2(S)$ лемма справедлива. Пусть v_1 — невходовая вершина (элемент) схемы S, в которой реализуется функция, не использующаяся для дальнейших вычислений в схеме S, т. е. эта функция не подается на вход никакого элемента схемы.

Схему, получающуюся из схемы S удалением вершины v_1 и ребер, входящих в эту вершину, обозначим через S'. Очевидно, что $l_2(S')=l_2(S)-1$.

Пусть в схеме S произвольным образом выбраны k вершин. Если среди выбранных вершин нет вершины v_1, то утверждение леммы для этих k вершин следует из предположения индукции, так как

$$2^{l_2(S)-\delta(S)} \geqslant 2^{l_2(S')} \geqslant 2^{l_2(S')-\delta(S')} \geqslant |\det A|.$$

Если вершина v_1 выбрана более одного раза, то утверждение леммы также выполняется, так как в этом случае в соответствующей матрице будут две одинаковые строки, и определитель этой матрицы будет равен 0. Далее будем считать, что среди выбранных вершин вершина v_1 содержится ровно один раз. Пусть в вершине v_1 вычисляется функция $x_1^{a_{11}} x_2^{a_{12}} \ldots x_k^{a_{1k}}$,

а в остальных выбранных вершинах $v_2, v_3, \ldots, v_k$ — соответственно функции $x_1^{a_{21}} x_2^{a_{22}} \ldots x_k^{a_{2k}}$, $x_1^{a_{31}} x_2^{a_{32}} \ldots x_k^{a_{3k}}, \ldots, x_1^{a_{k1}} x_2^{a_{k2}} \ldots x_k^{a_{kk}}$.

Пусть на входы элемента, соответствующего вершине v_1, подаются функции $x_1^{a'_{11}} x_2^{a'_{12}} \ldots x_k^{a'_{1k}}$ и $x_1^{a''_{11}} x_2^{a''_{12}} \ldots x_k^{a''_{1k}}$, вычисляемые в вершинах v' и v'' соответственно.

Если вершине v_1 соответствует операция умножения, то выполняется равенство

$$x_1^{a_{11}} x_2^{a_{12}} \ldots x_k^{a_{1k}} = x_1^{a'_{11}+a''_{11}} x_2^{a'_{12}+a''_{12}} \ldots x_k^{a'_{1k}+a''_{1k}},$$

а если соответствует операция деления — то равенство

$$x_1^{a_{11}} x_2^{a_{12}} \ldots x_k^{a_{1k}} = x_1^{a'_{11}-a''_{11}} x_2^{a'_{12}-a''_{12}} \ldots x_k^{a'_{1k}-a''_{1k}}.$$

Обозначим через A' и A'' матрицы, получающиеся из матрицы A заменой первой строки на строки $(a'_{11}, a'_{12}, \ldots, a'_{1k})$ и $(a''_{11}, a''_{12}, \ldots, a''_{1k})$ соответственно.

Случай 1. Условие $\delta(S) = \delta(S')$ выполняется.

В этом случае достаточно дословно повторить соответствующие выкладки из леммы 10.

Случай 2. Условие $\delta(S) = \delta(S')$ не выполняется.

Тогда справедливы равенства $\delta(S) = 1$ и $\delta(S') = 0$. Из условия $\delta(S') = 0$ следует, что в матрицах A' и A'' в каждой строке ровно по одному ненулевому элементу. Из условия $\delta(S) = 1$ следует, что либо ненулевые элементы первых строк матриц A' и A'' находятся в разных столбцах, либо ненулевые элементы первых строк матриц A' и A'' находятся в столбцах с одним номером, но вершине v_1 соответствует операция деления. Покажем, что и в том и в другом случае выполняется неравенство

$$|\det A| \leqslant \max\left(|\det A'|, |\det A''|\right).$$

Действительно, если ненулевые элементы первых строк матриц A' и A'' находятся в разных столбцах, то в одной из матриц A' и A'' (без ограничения общности будем считать, что в матрице A'') найдутся две пропорциональные строки. Тогда

$$|\det A| = |\det A' \pm \det A''| = |\det A'| = \max\left(|\det A'|, |\det A''|\right).$$

Если же ненулевые элементы первых строк матриц A' и A'' находятся в столбцах с одним номером, а вершине v_1 соответствует операция деления, то в матрице A ровно k ненулевых элементов, стоящих на тех же местах, что и в матрицах A' и A'', причем ненулевой элемент, стоящий в первой строке матрицы A, равен разности ненулевых (причем положительных) элементов, стоящих в первых строках в матрицах A' и A'', а остальные ненулевые элементы матрицы A совпадают с соответствующими ненулевыми элементами матриц A' и A''. Поэтому

$$|\det A| = |\det A' - \det A''| \leqslant \max\left(|\det A'|, |\det A''|\right).$$

Теперь, используя предположение индукции, получаем:

$$|\det A| \leqslant \max\left(|\det A'|, |\det A''|\right) \leqslant 2^{l_2(S')-\delta(S')} = 2^{l_2(S)-1} = 2^{l_2(S)-\delta(S)}.$$

Лемма 11 доказана.

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

Положим

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

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

Т е о р е м а 26 [43, 46]. *Для любой ненулевой целочисленной матрицы A справедливы неравенства:*

$$l(A)\geqslant\log D(A),\quad l_2(A)\geqslant\log D(A),\quad l_F(A)\geqslant\log D(A)$$

(*в первом неравенстве подразумевается, что в матрице A нет нулевых строк и все ее элементы неотрицательны*).

Д о к а з а т е л ь с т в о. Пусть S — минимальная схема, реализующая в соответствующей модели систему функций

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

Пусть число k и наборы индексов $i_1,i_2,\ldots,i_k$ и $j_1,j_2,\ldots,j_k$, удовлетворяющие условиям $1\leqslant k\leqslant\min(p,q)$, $1\leqslant i_1<i_2<\ldots<i_k\leqslant p$, $1\leqslant j_1<j_2<\ldots<j_k\leqslant q$, выбраны таким образом, чтобы выполнялось равенство

$$|\det A(i_1,i_2,\ldots,i_k;\ j_1,j_2,\ldots,j_k)|=D(A).$$

Отметим, что тогда, в силу отличия матрицы A от нулевой, справедливо неравенство $|\det A(i_1,i_2,\ldots,i_k;\ j_1,j_2,\ldots,j_k)|\geqslant 1$.

Преобразуем схему S в схему S_1 следующим образом.

В случае второй вычислительной модели добавим новую вершину, в которой вычисляется функция, тождественно равная единице как результат деления x_{i_1} на x_{i_1}, и затем подадим функцию 1 на все входы исходной схемы, кроме входов, которым приписаны переменные $x_{j_1},x_{j_2},\ldots,x_{j_k}$.

В случае первой или третьей вычислительной модели припишем функцию 1 всем входам исходной схемы, кроме входов, которым приписаны переменные $x_{j_1},x_{j_2},\ldots,x_{j_k}$, и, в случае третьей вычислительной модели, обратные к этим переменным величины, а затем последовательно удалим все элементы умножения, хотя бы на один вход которых подается функция 1 (при этом далее вместо вычисляемой этим элементом функции будет использоваться функция, подаваемая на другой вход этого элемента умножения).

Тогда в вершинах схемы S_1, соответствующих вершинам исходной схемы, в которых вычислялись функции

$$x_1^{a_{i_1,1}}x_2^{a_{i_1,2}}\ldots x_q^{a_{i_1,q}},\ x_1^{a_{i_2,1}}x_2^{a_{i_2,2}}\ldots x_q^{a_{i_2,q}},\ \ldots,\ x_1^{a_{i_k,1}}x_2^{a_{i_k,2}}\ldots x_q^{a_{i_k,q}},$$

будут вычисляться функции

$$x_{j_1}^{a_{i_1,j_1}} x_{j_2}^{a_{i_1,j_2}} \dots x_{j_k}^{a_{i_1,j_k}},\ x_{j_1}^{a_{i_2,j_1}} x_{j_2}^{a_{i_2,j_2}} \dots x_{j_k}^{a_{i_2,j_k}},\ \dots,\ x_{j_1}^{a_{i_k,j_1}} x_{j_2}^{a_{i_k,j_2}} \dots x_{j_k}^{a_{i_k,j_k}}.$$

Для вычислительных моделей, не использующих операцию деления, далее достаточно применить лемму 10.

В случае вычислительной модели, использующей, наряду с умножением, и деление, справедливо неравенство $l_2(S_1) \leqslant l_2(S) + 1$. Применяя лемму 11, с учетом того, что в схеме S_1 есть элемент деления, получаем:

$$l_2(S_1) - 1 \geqslant \log |\det A(i_1, i_2, \dots, i_k;\ j_1, j_2, \dots, j_k)| = \log D(A).$$

Поэтому

$$l_2\left(x_1^{a_{11}} x_2^{a_{12}} \dots x_q^{a_{1q}},\ x_1^{a_{21}} x_2^{a_{22}} \dots x_q^{a_{2q}},\ \dots,\ x_1^{a_{p1}} x_2^{a_{p2}} \dots x_q^{a_{pq}}\right) = l_2(S) \geqslant \log D(A).$$

Теорема 26 доказана.

Забегая вперед, скажем, что большинство обсуждаемых в данной работе нижних оценок сложности для индивидуальных последовательностей матриц либо так или иначе непосредственно следуют из теоремы 26, либо существенно на нее опираются.

5.3. Вычисление систем одночленов от двух переменных. В оценке функции Шеннона сложности вычисления систем одночленов из теоремы 25 при выполнении условия $\max(p, q) = o(\log \log K)$ главным слагаемым является не слагаемое, определяемое мощностными соображениями, а слагаемое, определяемое «размерами» системы. Этот факт дает надежду на получение для задачи Пиппенджера достаточно точных, например асимптотически точных оценок сложности индивидуальных последовательностей матриц в наиболее важном с точки зрения различных приложений случае константных или слаборастущих размеров матриц.

Частные случаи задачи Пиппенджера, когда вычисляемая система состоит из одного одночлена или все вычисляемые одночлены являются степенями одной переменной, уже рассмотрены — это, соответственно, задачи Беллмана и Кнута.

В 2005 г. в [42] получено асимптотически точное решение задачи Пиппенджера в случае вычисления двух одночленов от двух переменных.

Т е о р е м а 27 [42]. *Пусть* $a_n = \max\{a_n, b_n, c_n, d_n\}$, $n = 1, 2, \dots$, *и* $a_n \to \infty$ *при* $n \to \infty$. *Тогда*

$$l(x^{a_n} y^{b_n}, x^{c_n} y^{d_n}) \sim \log\left(|a_n d_n - b_n c_n| + a_n\right).$$

На доказательстве теоремы 27 останавливаться не будем, так как доказанная в ней нижняя оценка лишь чуть-чуть сильнее универсальной нижней оценки, а верхняя оценка будет обобщена в следующей теореме, дающей асимптотически не улучшаемую верхнюю оценку сложности вычисления системы из двух одночленов или системы одночленов от двух переменных. В силу теоремы 4 о двойственности задачи Пиппенджера из этих двух случаев достаточно рассмотреть только один. Будем рассматривать случай вычисления системы одночленов от двух переменных.

Т е о р е м а 28 [44]. *Пусть*

$$a_m(n) = \max\{a_1(n), b_1(n), a_2(n), b_2(n), \dots, a_m(n), b_m(n)\}$$

и при $n\to\infty$ *выполняется условие* $a_m(n)\to\infty$. *Тогда*

$$l\left(x^{a_1}y^{b_1}, x^{a_2}y^{b_2}, \ldots, x^{a_m}y^{b_m}\right) \leqslant \log\left(a_m + \max_{i:\,1\leqslant i\leqslant m-1}|a_m b_i - a_i b_m|\right) + \\ + O\left(\frac{m\log a_m}{\log\log a_m}\right).$$

Доказательство. Положим

$$d_0 = \max_{i:\,1\leqslant i\leqslant m-1}\left|b_i - \frac{b_m}{a_m}a_i\right|, \quad d = \max(d_0, 1).$$

Тогда утверждение теоремы можно записать так:

$$l\left(x^{a_1}y^{b_1}, x^{a_2}y^{b_2}, \ldots, x^{a_m}y^{b_m}\right) \leqslant \log a_m + \log d + O\left(\frac{m\log a_m}{\log\log a_m}\right).$$

В таком виде и будем устанавливать оценку.

Без ограничения общности будем считать, что одночлены $x^{a_1}y^{b_1}$, $x^{a_2}y^{b_2}, \ldots, x^{a_m}y^{b_m}$ упорядочены в порядке возрастания показателей степеней переменной x (т. е. по возрастанию значений a_i), а при одинаковых показателях степеней переменной x — в порядке возрастания показателей степеней переменной y (т. е. по возрастанию значений b_i).

Если выполняется условие $b_m = 0$, то справедливо равенство $d = \max\{b_1, b_2, \ldots, b_m\}$ и для получения нужной верхней оценки достаточно отдельно вычислить ненулевые степени систем $\{x^{a_1}, x^{a_2}, \ldots, x^{a_m}\}$ и $\{y^{b_1}, y^{b_2}, \ldots, y^{b_m}\}$. Используя теорему 6 и учитывая условия доказываемой теоремы, получаем:

$$\begin{aligned} l\left(x^{a_1}y^{b_1}, x^{a_2}y^{b_2}, \ldots, x^{a_m}y^{b_m}\right) &\leqslant \\ &\leqslant l\left(x^{a_1}, x^{a_2}, \ldots, x^{a_m}\right) + l\left(y^{b_1}, y^{b_2}, \ldots, y^{b_{m-1}}\right) + m - 1 \leqslant \\ &\leqslant \left(\log a_m + \frac{\log\left(\prod\limits_{i=1}^{m}(a_i+1)\right)}{\log\log\left(\prod\limits_{i=1}^{m}(a_i+1)\right)}(1+o(1))\right) + \\ &+ \left(\log d + \frac{\log\left(\prod\limits_{i=1}^{m}(b_i+1)\right)}{\log\log\left(\prod\limits_{i=1}^{m}(b_i+1)\right)}(1+o(1))\right) + O(m) \leqslant \\ &\leqslant \log a_m + \log d + \frac{2\log(a_m+1)^m}{\log\log(a_m+1)^m}(1+o(1)) + O(m) = \\ &= \log a_m + \log d + O\left(\frac{m\log a_m}{\log\log a_m}\right). \end{aligned}$$

Таким образом, в случае $b_m = 0$ утверждение теоремы доказано. Далее будем считать, что $b_m \neq 0$.

Сопоставим каждому одночлену $x^{a_i}y^{b_i}$, $i = 1, 2, \ldots, m$, параметр φ_i следующим образом:

$$\varphi_i = \begin{cases} \dfrac{b_m}{a_m}, & \text{если } a_i = 0 \text{ или } \dfrac{b_i}{a_i} \geqslant \dfrac{b_m}{a_m}; \\ \dfrac{b_i}{a_i}, & \text{если } \dfrac{b_i}{a_i} < \dfrac{b_m}{a_m}. \end{cases}$$

Далее положим

$$\Phi(i) = \min_{j:\, i \leqslant j \leqslant m} \varphi_j, \quad i = 1, 2, \ldots, m.$$

Очевидно, что функция $\Phi(i)$, заданная на множестве $M = \{1, 2, \ldots, m\}$, является неубывающей. Разобьем область определения M функции $\Phi(i)$ на участки «постоянства» $M_1, M_2, \ldots, M_v$ так, чтобы выполнялись условия:

1) $M = M_1 \cup M_2 \cup \ldots \cup M_v$;

2) $M_s \cap M_t = \varnothing$ при $s \neq t$;

3) $\Phi(i) = \Phi(j)$ для любых i и j из одного множества M_s, $s = 1, 2, \ldots, v$;

4) для любых s и t, $1 \leqslant s < t \leqslant v$, и для любых i и j, $i \in M_s$, $j \in M_t$, справедливо неравенство $\Phi(i) < \Phi(j)$.

Положим $k_i = |M_1 \cup M_2 \cup \ldots \cup M_i|$, $i = 1, 2, \ldots, v$. Отметим, что $k_v = m$.

Пусть u — натуральный параметр, значение которого определим позже.

Для $r = 1, \ldots, v$ представим число a_{k_r} в системе счисления по основанию 2^u. Пусть значность полученного представления равна t_r. Тогда

$$a_{k_r} = \alpha_{k_r,0} + \alpha_{k_r,1} 2^u + \ldots + \alpha_{k_r,t_r-1} 2^{(t_r-1)u},$$

где $0 \leqslant \alpha_{k_r,j} < 2^u$, $j = 0, 1, \ldots, t_r - 1$; $\alpha_{t_r-1} \geqslant 1$. Отметим, что при этом справедливы соотношения

$$(t_r - 1)u \leqslant \log a_{k_r} \leqslant t_r u.$$

Для всех номеров i, удовлетворяющих неравенству $i \leqslant k_r$, в силу соотношения $a_i \leqslant a_{k_r}$, число a_i можно представить в виде

$$a_i = \alpha_{i0} + \alpha_{i,1} 2^u + \ldots + \alpha_{i,t_r-1} 2^{(t_r-1)u},$$

где $0 \leqslant \alpha_{ij} < 2^u$, $j = 0, 1, \ldots, t_r - 1$.

Далее положим

$$p_{rj} = \left\lfloor \varphi_{k_r} 2^{ju} \right\rfloor, \quad j = 0, 1, \ldots, t_r - 1.$$

Покажем, что $2^u p_{rj} \leqslant p_{r,j+1} \leqslant 2^u p_{rj} + 2^u - 1$, $j = 0, 1, \ldots, t_r - 2$. Действительно, с одной стороны,

$$\frac{p_{r,j+1}}{p_{rj}} = \frac{\left\lfloor \varphi_{k_r} 2^{(j+1)u} \right\rfloor}{\left\lfloor \varphi_{k_r} 2^{ju} \right\rfloor} \geqslant \frac{\left\lfloor \left\lfloor \varphi_{k_r} 2^{ju} \right\rfloor 2^u \right\rfloor}{\left\lfloor \varphi_{k_r} 2^{ju} \right\rfloor} = 2^u,$$

а с другой —

$$p_{r,j+1} - 2^u p_{rj} = \left\lfloor \varphi_{k_r} 2^{ju} 2^u \right\rfloor - \left\lfloor \varphi_{k_r} 2^{ju} \right\rfloor 2^u < \varphi_{k_r} 2^{ju} 2^u - \left(\varphi_{k_r} 2^{ju} - 1 \right) 2^u = 2^u,$$

и, следовательно, учитывая целочисленность величины $p_{r,j+1} - 2^u p_{rj}$, имеем: $p_{r,j+1} - 2^u p_{rj} \leqslant 2^u - 1$.

Теперь будем считать, что индекс i удовлетворяет неравенствам $k_{r-1} < i \leqslant k_r$ (здесь дополнительно подразумеваем, что $k_0 = 0$). Тогда положим

$$\widetilde{b_i} = \alpha_{i0} p_{10} + \alpha_{i1} p_{11} + \ldots + \alpha_{i,t_1-1} p_{1,t_1-1} + \alpha_{i,t_1} p_{2,t_1} + \alpha_{i,t_1+1} p_{2,t_1+1} + \ldots$$

$$+ \alpha_{i,t_1-1} p_{2,t_2-1} + \ldots + \alpha_{i,t_{r-1}} p_{r,t_{r-1}} + \alpha_{i,t_{r-1}+1} p_{r,t_{r-1}+1} + \ldots + \alpha_{i,t_r-1} p_{r,t_r-1}.$$

Считая, что $t_0 = 0$, это равенство можно переписать так:

$$\widetilde{b_i} = \sum_{s=1}^{r} \sum_{j=t_{s-1}}^{t_s-1} \alpha_{ij} p_{sj}.$$

Тогда

$$\widetilde{b_i} = \sum_{s=1}^{r} \sum_{j=t_{s-1}}^{t_s-1} \alpha_{ij} \left\lfloor \varphi_{k_s} 2^{ju} \right\rfloor \leqslant \varphi_{k_r} \sum_{s=1}^{r} \sum_{j=t_{s-1}}^{t_s-1} \alpha_{ij} 2^{ju} = \varphi_{k_r} \sum_{j=0}^{t_r-1} \alpha_{ij} 2^{ju} = \varphi_{k_r} a_i.$$

Учитывая, что $i > k_{r-1}$, справедливо неравенство $\varphi_i \geqslant \varphi_{k_r}$. Поэтому

$$\widetilde{b_i} \leqslant \varphi_{k_r} a_i < \varphi_i a_i \leqslant b_i.$$

С другой стороны, если $a_i \neq 0$, то выполняются соотношения

$$\widetilde{b_i} = \sum_{s=1}^{r} \sum_{j=t_{s-1}}^{t_s-1} \alpha_{ij} \left\lfloor \varphi_{k_s} 2^{ju} \right\rfloor \geqslant \sum_{s=1}^{r} \sum_{j=t_{s-1}}^{t_s-1} \alpha_{ij} \left(\frac{b_{k_s}}{a_{k_s}} 2^{ju} - 1 \right) =$$

$$= \sum_{s=1}^{r} \sum_{j=t_{s-1}}^{t_s-1} \alpha_{ij} \left(\frac{b_i}{a_i} + \frac{b_{k_s}}{a_{k_s}} - \frac{b_i}{a_i} \right) 2^{ju} - \sum_{j=0}^{t_r-1} \alpha_{ij} =$$

$$= \sum_{s=1}^{r} \sum_{j=t_{s-1}}^{t_s-1} \alpha_{ij} \frac{b_i}{a_i} 2^{ju} - \sum_{s=1}^{r} \sum_{j=t_{s-1}}^{t_s-1} \alpha_{ij} \left(\frac{b_i}{a_i} - \frac{b_{k_s}}{a_{k_s}} \right) 2^{ju} - \sum_{j=0}^{t_r-1} \alpha_{ij} \geqslant$$

$$\geqslant b_i - \sum_{s=1}^{r} \sum_{j=t_{s-1}}^{t_s-1} \alpha_{ij} \left(\frac{b_i}{a_i} - \frac{b_{k_s}}{a_{k_s}} \right) 2^{ju} - \left(t_r 2^u - 1 \right).$$

Оценим сверху входящую в последнее выражение двойную сумму:

$$\sum_{s=1}^{r} \sum_{j=t_{s-1}}^{t_s-1} \alpha_{ij} \left(\frac{b_i}{a_i} - \frac{b_{k_s}}{a_{k_s}} \right) 2^{ju} =$$

$$= \sum_{s=1}^{r-1} \left(\frac{b_i}{a_i} - \frac{b_{k_s}}{a_{k_s}} \right) \sum_{j=t_{s-1}}^{t_s-1} \alpha_{ij} 2^{ju} + \left(b_i - \frac{b_{k_r}}{a_{k_r}} a_i \right) \frac{1}{a_i} \sum_{j=t_{r-1}}^{t_r-1} \alpha_{ij} 2^{ju} \leqslant$$

$$\leqslant \sum_{s=1}^{r-1} \left(\frac{b_i}{a_i} - \frac{b_{k_s}}{a_{k_s}} \right) 2^{t_s u} + \left(b_i - \frac{b_{k_r}}{a_{k_r}} a_i \right) \leqslant$$

$$\leqslant \sum_{s=1}^{r-1} \left(\frac{b_i}{a_i} - \frac{b_{k_s}}{a_{k_s}} \right) a_{k_s} 2^u + \left(b_i - \frac{b_{k_r}}{a_{k_r}} a_i \right) = 2^u \sum_{s=1}^{r-1} \left| \frac{b_i}{a_i} a_{k_s} - b_{k_s} \right| + \left| b_i - \frac{b_{k_r}}{a_{k_r}} a_i \right| =$$

$$= 2^u \sum_{s=1}^{r-1} \left| \frac{b_i}{a_i} a_{k_s} - \frac{b_m}{a_m} a_{k_s} + \frac{b_m}{a_m} a_{k_s} - b_{k_s} \right| + \left| b_i - \frac{b_m}{a_m} a_i + \frac{b_m}{a_m} a_i - \frac{b_{k_r}}{a_{k_r}} a_i \right| \leqslant$$

$$\leqslant 2^u \sum_{s=1}^{r-1} \left(\frac{a_{k_s}}{a_i} \left| b_i - \frac{b_m}{a_m} a_i \right| + \left| \frac{b_m}{a_m} a_{k_s} - b_{k_s} \right| \right) + \left| b_i - \frac{b_m}{a_m} a_i \right| + \frac{a_i}{a_{k_r}} \left| \frac{b_m}{a_m} a_{k_r} - b_{k_r} \right| \leqslant$$

$$\leqslant 2^{u+1} r d \leqslant 2^{u+1} m d.$$

Следовательно, если $a_i \neq 0$, то

$$\widetilde{b_i} \geqslant b_i - 2^{u+1} m d - (t_v 2^u - 1).$$

Это же неравенство справедливо и при $a_i = 0$, так как тогда

$$\widetilde{b_i} \geqslant 0 = b_i - |b_i| = b_i - \left| b_i - \frac{b_m}{a_m} a_i \right| \geqslant b_i - d.$$

Таким образом,

$$0 \leqslant b_i - \widetilde{b_i} \leqslant 2^{u+1} md + (t_v 2^u - 1), \quad i = 1, 2, \ldots, m.$$

Теперь для $r = 1, \ldots, v-1$ оценим сверху величины $p_{r+1,t_{r-1}} - p_{r,t_r-1}$:

$$p_{r+1,t_{r-1}} - p_{r,t_r-1} = \left\lfloor \frac{b_{k_{r+1}}}{a_{k_{r+1}}} 2^{(t_r-1)u} \right\rfloor - \left\lfloor \frac{b_{k_r}}{a_{k_r}} 2^{(t_r-1)u} \right\rfloor \leqslant$$

$$\leqslant 2^{(t_r-1)u} \left(\frac{b_{k_{r+1}}}{a_{k_{r+1}}} - \frac{b_{k_r}}{a_{k_r}} \right) + 1 \leqslant \frac{2^{(t_r-1)u}}{a_{k_r}} \left(\frac{b_{k_{r+1}}}{a_{k_{r+1}}} a_{k_r} - b_{k_r} \right) + 1 \leqslant$$

$$\leqslant \left(\frac{b_{k_{r+1}}}{a_{k_{r+1}}} a_{k_r} - b_{k_r} \right) + 1 \leqslant \left(\frac{b_m}{a_m} a_{k_r} - b_{k_r} \right) + 1 = \left| \frac{b_m}{a_m} a_{k_r} - b_{k_r} \right| + 1 \leqslant d + 1.$$

Эти соотношения вместе с очевидными неравенствами $p_{r,t_r-1} \leqslant p_{r+1,t_r-1}$, $r = 1, \ldots, v-1$, дают такие оценки:

$$p_{r+1,t_r-1} - (d+1) \leqslant p_{r,t_r-1} \leqslant p_{r+1,t_r-1}, \quad r = 1, \ldots, v-1.$$

Перейдем непосредственно к описанию процесса совместного вычисления одночленов $x^{a_1} y^{b_1}$, $x^{a_2} y^{b_2}, \ldots, x^{a_m} y^{b_m}$. Это вычисление будет состоять из пяти этапов. Обозначим через l_i $(i = 1, 2, 3, 4, 5)$ число операций умножения, используемых на i-м этапе.

Этап 1. Вычисление системы степеней

$$y, y^2, y^3, \ldots, y^{2^u - 1}.$$

Очевидно, что $l_1 = 2^u - 2$.

Этап 2. Совместное вычисление системы степеней

$$y^{b_i - \widetilde{b_i}}, \quad i = 1, 2, \ldots, m; \qquad y^{p_{r+1,t_r-1} - p_{r,t_r-1}}, \quad r = 1, \ldots, v-1.$$

Представим величину $b_i - \widetilde{b_i}$, $i = 1, 2, \ldots, m$, в виде суммы целых чисел b_{i1} и b_{i2}, где

$$b_{i1} = \min \left(\left\lfloor 2^{u+1} md \right\rfloor, \; b_i - \widetilde{b_i} \right), \quad b_{i2} = b_i - \widetilde{b_i} - b_{i1}.$$

Тогда, учитывая неравенства $0 \leqslant b_i - \widetilde{b_i} \leqslant 2^{u+1} md + t_v 2^u - 1$, имеем:

$$0 \leqslant b_{i1} \leqslant 2^{u+1} md, \quad 0 \leqslant b_{i2} \leqslant t_v 2^u, \quad y^{b_i - \widetilde{b_i}} = y^{b_{i1}} y^{b_{i2}}; \qquad i = 1, 2, \ldots, m.$$

Далее положим

$$q_r = p_{r+1,t_r-1} - p_{r,t_r-1}, \quad r = 1, \ldots, v-1.$$

Тогда, учитывая неравенства $0 \leqslant p_{r+1,t_r-1} - p_{r,t_r-1} \leqslant d+1$, имеем:

$$0 \leqslant q_r \leqslant 2^{u+1} md.$$

Отметим также очевидные неравенства $b_{i1} \leqslant a_m$, $i = 1, 2, \ldots, m$; $q_r \leqslant a_m$, $r = 1, \ldots, v-1$.

Очевидно, что для вычисления нужной системы степеней переменной y достаточно для ненулевых значений b_{i1}, b_{i2}, $i = 1, 2, \ldots, m$, и q_r, $r = 1, \ldots, v-1$, вычислить степени $y^{b_{i1}}, y^{b_{i2}}, y^{q_r}$, — после этого достаточно выполнить не более m операций умножения. Поэтому, используя теорему 6 и учитывая условия доказываемой теоремы, получаем:

$$l_2 \leqslant \log\left(\max\{b_{11}, b_{12}, \ldots, b_{1m}, q_1, q_2, \ldots, q_v\}\right) + \\ + \frac{\log\left(\prod\limits_{i=1}^{m}(b_{i1}+1)\prod\limits_{r=1}^{v}(q_r+1)\right)}{\log\log\left(\prod\limits_{i=1}^{m}(b_{i1}+1)\prod\limits_{r=1}^{v}(q_r+1)\right)}(1+o(1)) + O(m+v) + mO\left(\log\left(t_v 2^u\right)\right) \leqslant$$

$$\leqslant (\log d + u + 1 + \log m) + \frac{\log\left((a_m+1)^{2m}\right)}{\log\log\left((a_m+1)^{2m}\right)}(1+o(1)) + O(m\log t_v) + O(mu) \leqslant$$

$$\leqslant \log d + \frac{2m\log a_m + 2m}{\log\log a_m}(1+o(1)) + O(m\log t_v) + O(mu) =$$

$$= \log d + O\left(\frac{m\log a_m}{\log\log a_m}\right) + O(m\log t_v) + O(mu).$$

Этап 3. Вычисление одночленов

$$xy^{p_{10}}, x^{2^u}y^{p_{11}}, x^{2^{2u}}y^{p_{12}}, \ldots, x^{2^{(t_1-1)u}}y^{p_{1,t_1-1}};$$

$$x^{2^{(t_1-1)u}}y^{p_{2,t_1-1}}, x^{2^{t_1 u}}y^{p_{2,t_1}}, x^{2^{(t_1+1)u}}y^{p_{2,t_1+1}}, \ldots, x^{2^{(t_2-1)u}}y^{p_{2,t_2-1}};$$

$$\ldots \qquad \ldots \qquad \ldots$$

$$x^{2^{(t_{v-1}-1)u}}y^{p_{v,t_{v-1}-1}}, x^{2^{t_{v-1}u}}y^{p_{v,t_{v-1}}}, x^{2^{(t_{v-1}+1)u}}y^{p_{v,t_{v-1}+1}}, \ldots, x^{2^{(t_v-1)u}}y^{p_{v,t_v-1}}.$$

Сначала, учитывая, что p_{10} равно либо 0, либо 1, последовательно вычисляем

$$xy^{p_{10}}, \left(xy^{p_{10}}\right)^2, \left(xy^{p_{10}}\right)^4, \ldots, \left(xy^{p_{10}}\right)^{2^u}.$$

Теперь, учитывая справедливость неравенств $p_{10}2^u \leqslant p_{11} \leqslant p_{10}2^u + 2^u - 1$, а также тот факт, что все степени y, не превышающие величины $2^u - 1$, уже вычислены на первом этапе, с использованием одной операции умножения можем получить одночлен

$$x^{2^u}y^{p_{11}} = x^{2^u}y^{p_{10}2^u}y^{p_{11}-p_{10}2^u} = \left(xy^{p_{10}}\right)^{2^u}y^{p_{11}-p_{10}2^u}.$$

Далее аналогично последовательно вычисляем такие одночлены:

$$\left(x^{2^u}y^{p_{11}}\right)^2, \left(x^{2^u}y^{p_{11}}\right)^4, \ldots, \left(x^{2^u}y^{p_{11}}\right)^{2^u}, x^{2^{2u}}y^{p_{12}};$$

$$\left(x^{2^{2u}}y^{p_{12}}\right)^2, \left(x^{2^{2u}}y^{p_{12}}\right)^4, \ldots, \left(x^{2^{2u}}y^{p_{12}}\right)^{2^u}, x^{2^{3u}}y^{p_{13}};$$

$$\ldots \qquad \ldots \qquad \ldots$$

$$\left(x^{2^{(t_1-2)u}}y^{p_{1,t_1-2}}\right)^2, \left(x^{2^{(t_1-2)u}}y^{p_{1,t_1-2}}\right)^4, \ldots, \left(x^{2^{(t_1-2)u}}y^{p_{1,t_1-2}}\right)^{2^u}, x^{2^{(t_1-1)u}}y^{p_{1,t_1-1}}.$$

Умножив последний одночлен на степень $y^{p_{2,t_1-1}-p_{1,t_1-1}}$, вычисленную на втором этапе, получаем одночлен $x^{2^{(t_1-1)u}}y^{p_{2,t_1-1}}$. Теперь аналогично последовательно вычисляем:

$$\left(x^{2^{(t_1-1)u}}y^{p_{2,t_1-1}}\right)^2, \left(x^{2^{(t_1-1)u}}y^{p_{2,t_1-1}}\right)^4, \ldots, \left(x^{2^{(t_1-1)u}}y^{p_{2,t_1-1}}\right)^{2^u}, x^{2^{t_1 u}}y^{p_{2,t_1}},$$

$$\left(x^{2^{t_1u}}y^{p_{2,t_1}}\right)^2, \left(x^{2^{t_1u}}y^{p_{2,t_1}}\right)^4, \ldots, \left(x^{2^{t_1u}}y^{p_{2,t_1}}\right)^{2^u}, x^{2^{(t_1+1)u}}y^{p_{2,t_1+1}},$$

$$\ldots \quad \ldots \quad \ldots$$

$$\left(x^{2^{(t_2-2)u}}y^{p_{2,t_2-2}}\right)^2, \left(x^{2^{(t_2-2)u}}y^{p_{2,t_2-2}}\right)^4, \ldots, \left(x^{2^{(t_2-2)u}}y^{p_{2,t_2-2}}\right)^{2^u}, x^{2^{(t_2-1)u}}y^{p_{2,t_2-1}},$$

$$x^{2^{(t_2-1)u}}y^{p_{3,t_2-1}};$$

$$\ldots \quad \ldots \quad \ldots$$

$$\ldots \quad \ldots \quad \ldots$$

$$\ldots \quad \ldots \quad \ldots$$

$$\left(x^{2^{(t_{v-1}-1)u}}y^{p_{v,t_{v-1}-1}}\right)^2, \left(x^{2^{(t_{v-1}-1)u}}y^{p_{v,t_{v-1}-1}}\right)^4, \ldots, \left(x^{2^{(t_{v-1}-1)u}}y^{p_{v,t_{v-1}-1}}\right)^{2^u}, x^{2^{t_{v-1}u}}y^{p_{v,t_{v-1}}},$$

$$\left(x^{2^{t_{v-1}u}}y^{p_{v,t_{v-1}}}\right)^2, \left(x^{2^{t_{v-1}u}}y^{p_{v,t_{v-1}}}\right)^4, \ldots, \left(x^{2^{t_{v-1}u}}y^{p_{v,t_{v-1}}}\right)^{2^u}, x^{2^{(t_{v-1}+1)u}}y^{p_{v,t_{v-1}+1}},$$

$$\ldots \quad \ldots \quad \ldots$$

$$\left(x^{2^{(t_v-2)u}}y^{p_{v,t_v-2}}\right)^2, \left(x^{2^{(t_v-2)u}}y^{p_{v,t_v-2}}\right)^4, \ldots, \left(x^{2^{(t_v-2)u}}y^{p_{v,t_v-2}}\right)^{2^u}, x^{2^{(t_v-1)u}}y^{p_{v,t_v-1}}.$$

Для каждого нового одночлена, получаемого на третьем этапе, использовалась одна операция умножения. Поэтому $l_3 \leqslant (t_v-1)(u+1)+v$. Учитывая соотношения $(t_v-1)u \leqslant \log a_{k_v} = \log a_m$ и $v \leqslant m$, получаем:

$$l_3 \leqslant \log a_m + t_v + m.$$

Этап 4. Вычисление одночленов $x^{a_i}\widetilde{y^{b_i}}$, $i = 1, 2, \ldots, m$.

Для каждого индекса i, $i = 1, 2, \ldots, m$, определим число $r = r(i)$ из следующих соотношений:

$$k_{r-1} < i \leqslant k_r.$$

Введем множества индексов

$$I_1^{ij}, I_2^{ij}, \ldots, I_{2^u-1}^{ij}, i = 1, 2, \ldots, m, j = 1, \ldots, r(i),$$

следующим образом:

$$I_s^{ij} = \{n \mid (t_{j-1} \leqslant n \leqslant t_j - 1)\&(\alpha_{in} = s)\}, i = 1, 2, \ldots, m, j = 1, \ldots, r(i),$$

$$s = 1, 2, \ldots, 2^u - 1.$$

Отметим справедливость неравенств

$$\sum_{s=1}^{2^u-1} \sum_{j=1}^{r(i)} |I_i^{ij}| \leqslant t_r, \quad i = 1, 2, \ldots, m.$$

Последовательно определим одночлены

$$f_{2^u-1}^i(x, y), f_{2^u-2}^i(x, y), \ldots, f_1^i(x, y), \quad i = 1, 2, \ldots, m.$$

Сначала положим

$$f_{2^u-1}^i(x, y) = \prod_{j=1}^{r(i)} \prod_{n \in I_{2^u-1}^{ij}} \left(x^{2^{nu}}y^{p_{jn}}\right), \quad i = 1, 2, \ldots, m.$$

Далее, для $s=2^u-2, 2^u-3, \ldots, 1$, положим

$$f_s^i(x,y)=f_{s+1}^i(x,y)\prod_{j=1}^{r(i)}\prod_{n\in I_s^{ij}}\left(x^{2^{nu}}y^{p_{jn}}\right),\quad i=1,2,\ldots,m.$$

Теперь, считая, что произведение пустого множества сомножителей по определению равно единице, для $i=1,2,\ldots,m$ вычислим последовательно все отличные от единицы одночлены

$$\prod_{j=1}^{r(i)}\prod_{n\in I_{2^u-1}^{ij}}\left(x^{2^{nu}}y^{p_{jn}}\right),\ \prod_{j=1}^{r(i)}\prod_{n\in I_{2^u-2}^{ij}}\left(x^{2^{nu}}y^{p_{jn}}\right),\ \ldots,\ \prod_{j=1}^{r(i)}\prod_{n\in I_1^{ij}}\left(x^{2^{nu}}y^{p_{jn}}\right).$$

На вычисление этих одночленов потребуется не более mt_v операций умножения.

Далее, используя по одной операции на каждый новый одночлен, для $i=1,2,\ldots,m$ вычислим:

$$f_{2^u-1}^i(x,y),\ f_{2^u-2}^i(x,y),\ \ldots,\ f_1^i(x,y),$$
$$f_{2^u-1}^i(x,y)f_{2^u-2}^i(x,y),\ f_{2^u-1}^i(x,y)f_{2^u-2}^i(x,y)f_{2^u-3}^i(x,y),\ \ldots,$$
$$f_{2^u-1}^i(x,y)f_{2^u-2}^i(x,y)\ldots f_1^i(x,y),$$

потратив на это не более $m2^{u+1}$ операций умножения. Тем самым будут вычислены все одночлены $x^{a_i}y^{\widetilde{b_i}}$, $i=1,2,\ldots,m$. Действительно,

$$f_{2^u-1}^i(x,y)f_{2^u-2}^i(x,y)\ldots f_1^i(x,y)=$$
$$=\left(\prod_{j=1}^{r(i)}\prod_{n\in I_{2^u-1}^{ij}}\left(x^{2^{nu}}y^{p_{jn}}\right)\right)^{2^u-1}\left(\prod_{j=1}^{r(i)}\prod_{n\in I_{2^u-2}^{ij}}\left(x^{2^{nu}}y^{p_{jn}}\right)\right)^{2^u-2}\ldots\left(\prod_{j=1}^{r(i)}\prod_{n\in I_1^{ij}}\left(x^{2^{nu}}y^{p_{jn}}\right)\right)^{1}=$$
$$=\left(\prod_{j=1}^{r(i)}\prod_{n\in I_{2^u-1}^{ij}}\left(x^{2^{nu}}y^{p_{jn}}\right)^{\alpha_{in}}\right)\left(\prod_{j=1}^{r(i)}\prod_{n\in I_{2^u-2}^{ij}}\left(x^{2^{nu}}y^{p_{jn}}\right)^{\alpha_{in}}\right)\ldots\left(\prod_{j=1}^{r(i)}\prod_{n\in I_1^{ij}}\left(x^{2^{nu}}y^{p_{jn}}\right)^{\alpha_{in}}\right)=$$
$$=\left(\prod_{n=0}^{t_r-1}x^{\alpha_{in}2^{nu}}\right)\left(\prod_{j=0}^{r(i)}\prod_{n=t_{j-1}}^{t_j-1}y^{\alpha_{in}p_{jn}}\right)=$$
$$=\exp\left(\ln x\left(\sum_{n=0}^{t_r-1}\alpha_{in}2^{nu}\right)\right)\exp\left(\ln y\left(\sum_{j=0}^{r(i)}\sum_{n=t_{j-1}}^{t_j-1}\alpha_{in}p_{jn}\right)\right)=x^{a_i}y^{\widetilde{b_i}}.$$

Очевидно, что $l_4\leqslant mt_v+2m2^u$.

Этап 5. Вычисление одночленов $x^{a_i}y^{b_i}$, $i=1,2,\ldots,m$.

На втором этапе вычислены степени $y^{b_i-\widetilde{b_i}}$, $i=1,2,\ldots,m$, а на четвертом — одночлены $x^{a_i}y^{\widetilde{b_i}}$, $i=1,2,\ldots,m$. Поэтому систему одночленов $\{x^{a_1}y^{b_1},x^{a_2}y^{b_2},\ldots,x^{a_m}y^{b_m}\}$, можно получить, использовав не более m операций умножения, т. е. $l_5\leqslant m$.

Таким образом, окончательно величину $l\left(x^{a_1}y^{b_1},x^{a_2}y^{b_2},\ldots,x^{a_m}y^{b_m}\right)$ можно сверху оценить следующим образом:

$$l\left(x^{a_1}y^{b_1},x^{a_2}y^{b_2},\ldots,x^{a_m}y^{b_m}\right)\leqslant l_1+l_2+l_3+l_4+l_5\leqslant$$
$$\leqslant\left(2^u-2\right)+\left(\log d+O\left(\frac{m\log a_m}{\log\log a_m}\right)+O(mt_v)+O(m2^u)\right)+$$
$$+\left(\log a_m+t_v+m\right)+\left(mt_v+2m2^u\right)+m\leqslant$$
$$\leqslant\log a_m+\log d+O\left(\frac{m\log a_m}{\log\log a_m}\right)+O(mt_v)+O(m2^u).$$

Положим $u = \lfloor \log\log a_m - 2\log\log\log a_m \rfloor$. Тогда, учитывая неравенство $(t_v - 1)u \leqslant \log a_m$, имеем:

$$t_v \leqslant \frac{\log a_m}{\lfloor \log\log a_m - 2\log\log\log a_m \rfloor} + 1, \quad 2^u \leqslant \frac{\log a_m}{(\log\log a_m)^2},$$

и, следовательно,

$$mt_v = O\left(\frac{m\log a_m}{\log\log a_m}\right), \quad m2^u = o\left(\frac{m\log a_m}{\log\log a_m}\right).$$

Окончательно имеем такую оценку:

$$l\left(x^{a_1}y^{b_1}, x^{a_2}y^{b_2}, \ldots, x^{a_m}y^{b_m}\right) \leqslant \log a_m + \log d + O\left(\frac{m\log a_m}{\log\log a_m}\right).$$

Теорема 28 доказана.

Из теоремы 28 и универсальной нижней оценки сразу получаем асимптотику сложности матриц из двух строк или двух столбцов.

Следствие 3. *Пусть $A_n = (a_{ij})$ — последовательность целочисленных матриц либо из двух строк и $m(n)$ столбцов, либо из $m(n)$ строк и двух столбцов. Тогда при условии*

$$m(n) = o\left(\log\log \max_{i,j} a_{i,j}(n)\right)$$

справедливо соотношение

$$l(A_n) \sim \log D(A_n).$$

Отметим, что в условиях следствия 3 асимптотика роста сложности и в случае системы из двух одночленов, и в случае системы одночленов от двух переменных определяется сложностью самой сложной подсистемы из двух одночленов от двух переменных.

5.4. Вспомогательная вычислительная модель. Доказательства верхних оценок теорем 27 и 28 выглядят технически очень непростыми, хотя на идейном уровне объяснить, как доказательство теоремы Брауэра можно обобщить на случай вычисления системы из двух одночленов от двух переменных и на еще более общий случай вычисления системы из m одночленов от двух переменных, уже не так трудно. Однако совмещение содержательной идеи и технических выкладок делает эти доказательства трудновоспринимаемыми. Для того, чтобы разделить описание процесса вычисления систем одночленов (матриц) на две составляющие — «содержательную» и «техническую» — и тем самым значительно упростить процесс доказательства асимптотических верхних оценок, введем вспомогательную вычислительную модель. Разрешим в схемах из умножения использование еще и одновходовых элементов, реализующих по подаваемой на вход элемента функции f ее степень f^r, где r — рациональное число, удовлетворяющее условию $0 \leqslant r \leqslant 2$ (значение r, вообще говоря, свое для каждого такого элемента). Будем называть такие схемы *обобщенными* или *λ-схемами*, а схемы, не использующие такие одновходовые элементы, иногда будем называть *обычными*.

Заметим, что при таком усилении вычислительных возможностей также расширяется и класс вычисляемых матриц: обобщенными схемами можно вычислить любую неотрицательную матрицу с рациональными элементами.

Пусть $A=(a_{ij})$ — матрица размера $p\times q$ с неотрицательными рациональными элементами. Обозначим через $\lambda(A)$ минимально возможную сложность обобщенной схемы из функциональных элементов, на входы которой подаются переменные $x_1, x_2, \ldots, x_q$, на выходах схемы вычисляются функции $x_1^{a_{11}}x_2^{a_{12}}\ldots x_q^{a_{1q}}$, $x_1^{a_{21}}x_2^{a_{22}}\ldots x_q^{a_{2q}}$, $\ldots$, $x_1^{a_{p1}}x_2^{a_{p2}}\ldots x_q^{a_{pq}}$, а сама схема состоит из одновходовых элементов описанного выше вида и двухвходовых элементов, реализующих произведение функций, подаваемых на входы элемента. Меру сложности λ будем называть *λ-сложностью*.

Очевидно, что имеет место неравенство $\lambda(A)\leqslant l(A)$. Отметим также, что величина $\lambda(A)$, как и величины $l(A)$, $l_2(A)$ и $l_F(A)$, ограничена снизу значением $\log D(A)$ — в случае вычисления обобщенными схемами этот факт устанавливается так же, как и в теореме 26 для случая реализации обычными схемами.

Ключевым свойством обобщенных схем является полная определенность со сложностью возведения в степень: при $0\leqslant\alpha<1$ выполняется равенство $\lambda(x^\alpha)=1$, а при $\alpha\geqslant 1$ — равенство $\lambda(x^\alpha)=\lceil\log\alpha\rceil$.

Поясним на примере как обобщенные схемы помогают разделить описание процесса вычисления одночленов (матриц) на две составляющие — «содержательную» и «техническую».

Пример 5. Пусть построена схема S_1, вычисляющая степень x^m; надо построить схему S, вычисляющую x^n, где $n>m$.

Если речь идет о построении обобщенной схемы, то достаточно построить обобщенную схему $\widehat{S}_2$, вычисляющую функцию $x^{n/m}$ (это можно сделать с λ-сложностью $\lceil\log(n/m)\rceil$), и на вход схемы $\widehat{S}_2$ подать выход схемы S_1, т.е. степень x^m. Полученная таким образом обобщенная схема $\widehat{S}$ будет вычислять степень x^n, причем $\lambda(\widehat{S})=l(S_1)+\lambda(\widehat{S}_2)=l(S_1)+\lceil\log(n/m)\rceil$.

Можно ли построить обычную схему S, вычисляющую с использованием схемы S_1 степень x^n со сложностью $l(S_1)+\log(n/m)+o(\log n)$, т.е. без асимптотического увеличения сложности по сравнению со случаем обобщенных схем? Если при этом использовать только выход схемы S_1 и переменную x, то это сделать, вообще говоря, нельзя: в случае когда $n=2m-1$, при построении схемы S потребуется дополнительно к схеме S_1 не менее $\log(m-1)$ элементов умножения, при этом $\log(n/m)=O(1)$, а $\log(m-1)\sim\log n$. Однако если использовать не только степень, реализованную на выходе схемы S_1, но и некоторые степени, вычисленные элементами схемы S_1, то можно добиться желаемого эффекта. Покажем, как это можно сделать.

Запишем число n в таком виде:

$$n=\left\lfloor\frac{n}{m}\right\rfloor m+\left(\frac{n}{m}-\left\lfloor\frac{n}{m}\right\rfloor\right)m.$$

Положим $u=\lfloor\log\log n-2\log\log\log n\rfloor$. Представим число $\lfloor n/m\rfloor$ в системе

счисления по основанию 2^u:

$$\left\lfloor \frac{n}{m} \right\rfloor = \mu_0 + \mu_1 2^u + \mu_2 2^{2u} + \ldots + \mu_{t-1} 2^{(t-1)u},$$

где $0 \leqslant \mu_i < 2^u$, $i = 0, 1, \ldots, t-1$; $\mu_{t-1} \neq 0$. Тогда справедливы неравенства $2^{(t-1)u} \leqslant \lfloor n/m \rfloor < 2^{tu}$.

Положим $s = \lfloor (\log m)/u \rfloor + 1$. Тогда выполняются соотношения $2^{(s-1)u} \leqslant m < 2^{su}$. Для каждого i, $i = 1, 2, \ldots, s-1$, через m_i обозначим наименьшее из чисел r, удовлетворяющих условиям: 1) $2^{iu} \leqslant r < 2^{iu+1}$; 2) в схеме S_1 есть элемент, вычисляющий степень x^r. Очевидно, что такое число существует. Тогда число $\big((n/m) - \lfloor n/m \rfloor\big)\, m$ можно представить следующим образом:

$$\left(\frac{n}{m} - \left\lfloor \frac{n}{m} \right\rfloor \right) m = \nu_0 + \nu_1 m_1 + \nu_2 m_2 + \ldots + \nu_{s-1} m_{s-1},$$

где $0 \leqslant \nu_i < 2^{u+1}$, $i = 0, 1, \ldots, s-1$.

Таким образом,

$$n = \sum_{i=0}^{t-1} \mu_i m 2^{iu} + \sum_{i=0}^{s-1} \nu_i m_i.$$

Построим схему S_2, которая по степеням $x^{m_1}, x^{m_2}, \ldots, x^{m_{s-1}}, x^m$ и переменной x вычисляет степень x^n. Сначала, потратив $(t-1)u$ элементов умножения, последовательно возводим в квадрат степень x^m, реализуя тем самым степени $x^{m2^u}, x^{m2^{2u}}, \ldots, x^{m2^{(t-1)u}}$. После этого для вычисления степени x^n в силу представления

$$x^n = \prod_{i=0}^{t-1} \left(x^{m2^{iu}}\right)^{\mu_i} \times \prod_{i=0}^{s-1} \left(x^{m_i}\right)^{\nu_i}$$

достаточно $s + t + 2^{u+1}$ операций умножения. Действительно, вычислить одночлен $z_1^{\beta_1} z_2^{\beta_2} \ldots z_{s+t}^{\beta_{s+t}}$, где $0 \leqslant \beta_i \leqslant 2^{u+1} - 1$, $i = 1, 2, \ldots, s+t$, от заданных выражений $z_1, z_2, \ldots, z_{s+t}$ можно следующим образом.

Положим

$$I_k = \{i : 1 \leqslant i \leqslant s+t,\ \beta_i = k\}, \quad k = 1, 2, \ldots, 2^{u+1} - 1.$$

Очевидно, что $|I_1| + |I_2| + \ldots + |I_{2^{u+1}-1}| \leqslant s+t$.

Последовательно определим одночлены $f_{2^{u+1}-1}, f_{2^{u+1}-2}, \ldots, f_1$ от переменных $z_1, z_2, \ldots, z_{s+t}$:

$$f_{2^{u+1}-1} = \prod_{i \in I_{2^{u+1}-1}} z_i; \qquad f_k = f_{k+1} \prod_{i \in I_k} z_i, \quad k = 2^{u+1} - 2, 2^u - 3, \ldots, 1.$$

Теперь, считая, что произведение пустого множества сомножителей по определению равно единице, вычислим последовательно все отличные от единицы одночлены

$$\prod_{i \in I_{2^{u+1}-1}} z_i, \ \prod_{i \in I_{2^{u+1}-2}} z_i, \ \ldots, \ \prod_{i \in I_1} z_i,$$

потратив на это не более $s + t - |\{I_k : |I_k| \neq 0\}|$ операций умножения. Далее с использованием не более $|\{I_k : |I_k| \neq 0\}|$ операций умножения можно вычислить все одночлены $f_{2^{u+1}-1}, f_{2^{u+1}-2}, \ldots, f_1$.

Окончательно, потратив еще не более $2^{u+1}-1$ операций умножения, получаем одночлен

$$f_{2^{u+1}-1}f_{2^{u+1}-2}\dots f_1 = \\ = \left(\prod_{i\in I_{2^{u+1}-1}} z_i\right)^{2^{u+1}-1}\left(\prod_{i\in I_{2^{u+1}-2}} z_i\right)^{2^{u+1}-2}\dots\left(\prod_{i\in I_1} z_i\right)^{1} = \\ = \left(\prod_{i\in I_{2^{u+1}-1}} z_i^{\beta_i}\right)\left(\prod_{i\in I_{2^{u+1}-2}} z_i^{\beta_i}\right)\dots\left(\prod_{i\in I_1} z_i^{\beta_i}\right) = z_1^{\beta_1}z_2^{\beta_2}\dots z_{s+t}^{\beta_{s+t}}.$$

Итак, для вычисления одночлена $z_1^{\beta_1}z_2^{\beta_2}\dots z_{s+t}^{\beta_{s+t}}$ было потрачено не более $s+t+2^{u+1}$ операций умножения.

Таким образом,

$$l(S) = l(S_1)+l(S_2) \leqslant l(S_1)+(t-1)u+s+t+2^{u+1}.$$

Учитывая соотношения

$$(t-1)u \leqslant \log\left(\frac{n}{m}\right), \quad s \leqslant \frac{\log m}{u}, \quad t \leqslant \frac{\log\left(\frac{n}{m}\right)}{u}$$

и подставляя значение параметра u, получаем:

$$l(S) = l(S_1)+\log\left(\frac{n}{m}\right)+\frac{\log n}{u}+2^{u+1} \leqslant l(S_1)+\log\left(\frac{n}{m}\right)+O\left(\frac{\log n}{\log\log n}\right),$$

следовательно,

$$l(S) = \lambda(\widehat{S})+O\left(\frac{\log n}{\log\log n}\right).$$

Приведенный пример иллюстрирует способ перехода от вычисления обобщенными схемами к вычислению обычными схемами без асимптотического увеличения сложности.

Отметим также, что при построении схемы S_1 информация о том, что выходы некоторых элементов схемы S_1 будут использованы при дальнейших вычислениях, может давать дополнительные преимущества (если не по сложности, то, по крайней мере, в удобстве использования) при переходе от обобщенных схем к обычным.

Итак, доказательства верхних оценок сложности матрицы A в классической модели, допускающей только операции умножения, можно разбить на две составляющие.

Первая — содержательная — заключается в построении для матрицы A обобщенной схемы нужной сложности (скажем, если получится, сложности $\log D(A)+O(1)$), причем эта обобщенная схема, помимо ограничения на сложность, должна обладать еще одним важным свойством — допускать разбиение на ограниченное (напомним, что речь идет о вычислении последовательности матриц) или слаборастущее число подсхем, каждая из которых либо состоит из одного двухвходового функционального элемента, либо имеет один вход, один выход и, соответственно, вычисляет некоторую степень подаваемой на вход подсхемы функции. Подсхемы этих двух типов будем называть *простейшими*. Отметим, что тип простейшей обобщенной схемы полностью определяется числом входов.

Вторая — техническая — заключается в перестроении без асимптотического увеличения сложности уже имеющейся обобщенной схемы, состоящей из небольшого числа простейших подсхем, в обычную схему, вычисляющую ту же матрицу, что и исходная обобщенная схема. При этом следующая теорема дает возможность проделать такую технически тяжелую работу всего один раз.

Т е о р е м а 29 [46, 48, 53]. *Пусть последовательность целочисленных матриц* $A(n) = \big(a_{ij}(n)\big)$ *размера* $p(n) \times q(n)$, $n = 1, 2, \ldots$, *удовлетворяющая при* $n \to \infty$ *условию*

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

вычисляется обобщенными схемами $\widehat{S}(n)$, *состоящими из* $k(n)$ *простейших подсхем, причем выполняются неравенства*

$$k(n) \leqslant \left(\log\log\log \max_{a_{ij} \in A(n)} |a_{ij}(n)| \right)^{1/2},$$

$$q(n) \leqslant \frac{1}{8} \left(\log\log\log \max_{a_{ij} \in A(n)} |a_{ij}(n)| \right)^{1/2}.$$

Тогда справедливо соотношение

$$l\left(A(n)\right) \leqslant \lambda\left(\widehat{S}(n)\right) + o\left(\frac{\log \max\limits_{a_{ij} \in A(n)} |a_{ij}(n)|}{\log\log\log \max\limits_{a_{ij} \in A(n)} |a_{ij}(n)|} \right).$$

Надо сказать, что при перестроении обобщенных схем в обычные, при всей прозрачности общей идеи, приходится преодолевать значительные трудности. И поэтому доказательство теоремы 29 достаточно громоздкое и здесь не приводится. Основные идеи содержатся в работах [46, 48], а в сформулированном здесь виде теорема содержится в [53]. Кроме того, стоит отметить, что в теореме 29 можно значительно ослабить условия и несколько понизить порядок остаточного члена, однако добиться того, чтобы остаточный член имел порядок $\log D(A)/\log\log D(A)$ (именно такой порядок остаточного члена получается при непосредственном доказательстве верхних оценок в наиболее простых случаях, в частности, это имеет место в теоремах 27 и 28), при таком подходе невозможно.

Завершая обсуждение технической составляющей доказательства верхних оценок, сформулируем важную гипотезу, доказательство которой стало бы значительным продвижением в исследовании задачи Пиппенджера.

Г и п о т е з а. *Существует такое* m (*зависящее только от* p *и* q), *что для любой последовательности неотрицательных матриц* $\{A_n\}$, *имеющих фиксированный размер* $p \times q$ *и удовлетворяющих условию* $D(A_n) \to \infty$, *найдется последовательность реализующих их* λ*-схем* $\{S_n\}$, *удовлетворяющая условиям:*

1) $\dfrac{\lambda(S_n)}{\lambda(A_n)} \to 1$;

2) *каждая схема* S_n *состоит не более чем из* m *простейших подсхем.*

Если гипотеза верна, то автоматически для любой последовательности целочисленных неотрицательных матриц A_n произвольного фиксированного размера при условии $D(A_n) \to \infty$ выполняется асимптотическое равенство $l(A_n) \sim \lambda(A_n)$.

5.5. Вычисление системы их трех одночленов от трех переменных. В 2005 г. в [46] с использованием аппарата перехода без асимптотического увеличения сложности от обобщенных схем, описанных выше, к обычным схемам умножения установлена верхняя оценка сложности вычисления систем из трех одночленов от трех переменных, асимптотически совпадающая с универсальной нижней оценкой. К сожалению, это доказательство имеет длину более 60 журнальных страниц. В 2019 г. в работе [62] предложено существенно более простое доказательство, которое лежит в основе приводимого здесь.

Т е о р е м а 30 [46, 62]. *Пусть последовательность* $\{A_n\}$ *целочисленных неотрицательных матриц размера* 3×3 *удовлетворяет условию* $D(A_n)\to\infty$ *при* $n\to\infty$. *Тогда*

$$l(A_n) = (1+o(1))\log D(A_n).$$

Нижняя оценка следует из универсальной нижней оценки, т. е. из теоремы 26. Для того, чтобы установить требуемую верхнюю оценку, в силу теоремы 29 достаточно показать, что $\lambda(A_n)\leqslant(1+o(1))\log D(A_n)$. Для доказательства этой верхней оценки покажем, что можно с заданной сложностью построить обобщенные схемы частного вида — в них, помимо элементов умножения, допускается использование элементов, реализующих для некоторого рационального r (вообще говоря, своего для каждого элемента), $1<r\leqslant 2$, r-ю степень подаваемой на вход элемента функции. Реализуемые такими обобщенными схемами системы функций задаются матрицами показателей степеней с рациональными неотрицательными элементами, при этом все ненулевые элементы должны быть не менее единицы. Такие матрицы будем называть *допустимыми*. Реализуемые такими обобщенными схемами функции в работе [46] назывались «обобщенными одночленами», здесь же слово «обобщенный» опускается.

Доказательство оценки $\lambda(A_n)\leqslant(1+o(1))\log D(A_n)$ будет опираться на несколько вспомогательных утверждений.

Для произвольной матрицы A обозначим через $D_{ij}(A)$ максимум абсолютных величин тех миноров матрицы A, при вычислении которых берутся квадратные подматрицы, содержащие i-ю строку и j-й столбец.

Л е м м а 12 [46]. *Пусть в допустимой матрице* A *размера* 3×3 *максимальным элементом является элемент* a_{11}. *Тогда* $D(A)\leqslant 4D_{11}(A)$.

Далее во всех вспомогательных утверждениях предполагается, что рассматривается не одна матрица, а последовательность матриц, удовлетворяющая следующему условию: последовательность максимальных элементов матриц стремится к бесконечности. Будем говорить, что такая последовательность матриц $\{A_n\}$ *правильно реализуется* последовательностью обобщенных схем $\{S_n\}$, если для каждого n схема S_n вычисляет систему одночленов, задаваемую матрицей показателей степеней A_n, причем любую обобщенную схему S_n можно разбить на ограниченное абсолютной константой число простейших подсхем, т. е. подсхем двух типов: подсхемы первого типа имеют один вход и один выход и, следовательно, вычисляют на своем выходе некоторую степень функции, подаваемой на вход, а подсхемы второго типа состоят из одного элемента умножения. В этом случае про схему S_n будем говорить, что она *правильно реализует* матрицу A_n.

Из доказательства теоремы 28 и принципа двойственности извлекается следующее утверждение.

Лемма 13. *Пусть A — допустимая матрица размера 3×2 или размера 2×3. Тогда можно построить обобщенную схему S, которая правильно реализует матрицу A и для которой справедливо соотношение $\lambda(S)\leqslant \log D(A)+O(1)$.*

Лемма 14. *Пусть максимальный элемент допустимой матрице $A=(a_{ij})$ размера 3×3 находится в первой строке и $a_{23}=a_{33}=0$. Тогда можно построить обобщенную схему S, которая правильно реализует матрицу A и для которой справедливо соотношение $\lambda(S)\leqslant \log D(A)+O(1)$.*

Доказательство. Если максимальным элементом матрицы A является элемент a_{13}, то отдельно вычисляем одночлен $x^{a_{11}}y^{a_{12}}z^{a_{13}}$ и систему $x^{a_{21}}y^{a_{22}}, x^{a_{31}}y^{a_{32}}$. Тогда в силу леммы 13 можно построить такую обобщенную схему S, правильно реализующую матрицу A, что

$$\lambda(S)\leqslant \log a_{13}+\log\max\left(a_{21},a_{22},a_{31},a_{32}|a_{21}a_{32}-a_{22}a_{31}|\right)+O(1)\leqslant \\ \leqslant \log D(A)+O(1).$$

Далее без ограничения общности будем считать, что максимальным элементом матрицы A является элемент a_{11}.

Случай 1. Пусть выполняется неравенство $a_{12}\geqslant a_{13}$.

Сначала вычислим систему $x^{a_{11}/a_{13}}y^{a_{12}/a_{13}}, x^{a_{21}}y^{a_{22}}, x^{a_{31}}y^{a_{32}}$, затем, умножив одночлен $x^{a_{11}/a_{13}}y^{a_{12}/a_{13}}$ на z и возведя полученный одночлен в степень a_{13}, получим одночлен $x^{a_{11}}y^{a_{12}}z^{a_{13}}$.

Положим

$$A_1=\begin{pmatrix} a_{11}/a_{13} & a_{12}/a_{13}\\ a_{21} & a_{22}\\ a_{31} & a_{32}\end{pmatrix}.$$

Тогда в условиях случая 1 в силу леммы 13 можно построить обобщенную схему S, которая правильно реализует матрицу A и для которой справедливы соотношения

$$\lambda(S)\leqslant \log D(A_1)+\log a_{13}+O(1)\leqslant \\ \leqslant \log\max\left(\frac{a_{11}}{a_{13}},a_{21},a_{22},a_{31},a_{32},\frac{1}{a_{13}}|a_{11}a_{22}-a_{12}a_{21}|,\right. \\ \left.\frac{1}{a_{13}}|a_{11}a_{32}-a_{12}a_{31}|,|a_{21}a_{32}-a_{22}a_{31}|\right)+\log a_{13}+O(1)\leqslant \\ \leqslant \log D(A)+O(1).$$

Случай 2. Пусть выполняется неравенство $a_{12}<a_{13}$.

Сначала вычислим систему $x^{a_{11}/a_{13}}, x^{a_{21}}y^{a_{22}}, x^{a_{31}}y^{a_{32}}$, затем одночлен $x^{a_{11}/a_{13}}z$, возведя который в степень a_{13}/a_{12}, получим одночлен $x^{a_{11}/a_{12}}z^{a_{13}/a_{12}}$, из которого, в свою очередь, получим одночлен $x^{a_{11}/a_{12}}yz^{a_{13}/a_{12}}$ и, наконец, посредством возведения в степень a_{12} — одночлен $x^{a_{11}}y^{a_{12}}z^{a_{13}}$.

Положим

$$A_2=\begin{pmatrix} a_{11}/a_{13} & 0\\ a_{21} & a_{22}\\ a_{31} & a_{32}\end{pmatrix}.$$

Тогда в условиях случая 2 в силу леммы 13 можно построить обобщенную схему S, которая правильно реализует матрицу A и для которой справедливы соотношения

$$\lambda(S) \leqslant \log D(A_2) + \log \frac{a_{13}}{a_{12}} + \log a_{12} + O(1) \leqslant$$
$$\leqslant \log \max \left(a_{11}, a_{13}a_{21}, a_{13}a_{22}, a_{13}a_{31}, a_{13}a_{32}, a_{11}a_{22}, a_{11}a_{32}, a_{13}|a_{21}a_{32} - a_{22}a_{31}|\right) + O(1).$$

Оценим сверху величины $a_{11}a_{22}$ и $a_{11}a_{32}$.

Если выполняется неравенство $a_{11}a_{22} \leqslant 2a_{12}a_{21}$, то выполняется и неравенство $a_{11}a_{22} \leqslant 2a_{13}a_{21}$. Если же выполняется неравенство $a_{11}a_{22} > 2a_{12}a_{21}$, то

$$a_{11}a_{22} = 2a_{11}a_{22} - a_{11}a_{22} < 2a_{11}a_{22} - 2a_{12}a_{21} = 2|a_{11}a_{22} - a_{12}a_{21}|.$$

Таким образом, $a_{11}a_{22} \leqslant 2\max\{a_{13}a_{21}, |a_{11}a_{22} - a_{12}a_{21}|\}$.

Аналогично устанавливается, что $a_{11}a_{32} \leqslant 2\max\{a_{13}a_{31}, |a_{11}a_{32} - a_{12}a_{31}|\}$.

Поэтому в условиях случая 2 справедливо соотношение

$$\lambda(S) \leqslant \log D(A) + O(1).$$

Лемма 14 доказана.

Далее для допустимой матрицы $A = (a_{ij})$ размера 3×3 определим *операцию приведения* относительно строки, содержащей максимальный элемент матрицы.

Пусть максимальный элемент содержится в первой строке матрицы A (в ином случае предварительно соответствующим образом переставим строки). Тогда результатом приведения матрицы A относительно первой строки будет квадратная матрица B порядка 3, которая получается из матрицы A путем вычитания из второй и третьей строк первой строки, умноженной соответственно на t_2 и t_3, где

$$t_2 = \min\left\{\frac{a_{21}}{a_{11}}, \frac{a_{22}}{a_{12}}, \frac{a_{23}}{a_{13}}\right\}, \qquad t_3 = \min\left\{\frac{a_{31}}{a_{11}}, \frac{a_{32}}{a_{12}}, \frac{a_{33}}{a_{13}}\right\}$$

(при этом если $a_{1j} = 0$, то полагаем $a_{ij}/a_{1j} = \infty$), с последующей заменой всех положительных элементов, которые меньше единицы, на нули. Таким образом,

$$B = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix},$$

где

$$b_{ij} = \max_{s\in\{1,2,3\}} \left(a_{ij} - a_{1j}\frac{a_{is}}{a_{1s}}\right) \times \operatorname{sign}\left[\max_{s\in\{1,2,3\}} \left(a_{ij} - a_{1j}\frac{a_{is}}{a_{1s}}\right)\right], i = 2,3, j = 1,2,3.$$

Отметим, что при построении матрицы B по матрице A в первой строке матрицы B будет содержаться максимальный элемент матрицы, а во второй и третьей строках будет по крайней мере по одному нулевому элементу.

Лемма 15. *Пусть матрица B получена из допустимой матрицы A применением операции приведения. Тогда* $|\log D(A) - \log D(B)| \leqslant 2$.

Кроме того, если обобщенная схема S_B правильно реализует матрицу B, то можно построить обобщенную схему S_A, которая правильно реализует матрицу A и для которой справедливо соотношение $\lambda(S_A) \leqslant \lambda(S_B) + O(1)$.

Доказательство. Пусть a_{ij} — максимальный элемент в матрице A, а матрица B получена из матрицы A применением операции приведения относительно i-й строки. Тогда, используя лемму 12, имеем

$$D(A) \leqslant 4D_{ij}(A) = 4D_{1j}(B) \leqslant 4D(B) \leqslant 16D_{1j}(B) = 16D_{ij}(A) \leqslant 16D(A),$$

откуда непосредственно следует первое утверждение леммы.

Существование обобщенной схемы S_A с указанным свойством в случае, когда в процессе применения операции приведения не пришлось обнулять элементы, меньшие единицы, практически очевидно. В общем случае это утверждение формально следует из лемм 11–15 работы [46].

Лемма 15 доказана.

Лемма 16. *Пусть в допустимой матрице $A = (a_{ij})$ максимальный элемент находится в первой строке и $a_{13} = a_{23} = 0$. Тогда можно построить обобщенную схему S, которая правильно реализует матрицу A и для которой справедливо соотношение* $\lambda(S) \leqslant \log D(A) + O(1)$.

Доказательство. К матрице A применим операцию приведения относительно первой строки. Полученную матрицу обозначим B. В силу леммы 15 справедливо равенство $\log D(B) = \log D(A) + O(1)$.

В матрице B в двух первых столбцах на пересечении со второй и третьей строками содержится по крайней мере по одному нулевому элементу. Если эти элементы находятся в одном столбце, то доказываемое неравенство получается применением леммы 14. В ином случае с точностью до перестановки первого и второго столбца матрица B имеет вид

$$B = \begin{pmatrix} b_{11} & b_{12} & 0 \\ b_{21} & 0 & 0 \\ 0 & b_{32} & b_{33} \end{pmatrix}.$$

Случай 1. Пусть выполняется неравенство $b_{32} \leqslant b_{33}$. Тогда вычислим систему из двух одночленов, задаваемых первыми двумя строкам матрицы B, и отдельно одночлен, задаваемый третьей строкой матрицы B. В силу леммы 13 (случай матриц размера 2×3) можно построить обобщенную схему S_B, которая правильно реализует матрицу B и для которой справедливы соотношения

$$\lambda(S_B) \leqslant \log \max(b_{11}, b_{12}, b_{12}b_{21}) + \log b_{33} + O(1) \leqslant$$
$$\leqslant \log D(B) + O(1) = \log D(A) + O(1).$$

Случай 2. Пусть выполняется неравенство $b_{32} > b_{33}$. Сначала вычислим систему $x^{b_{11}}y^{b_{12}}, x^{b_{21}}, y^{\frac{b_{32}}{b_{33}}}$, затем домножим последний одночлен на z и полученный результат возведем в степень b_{33}. В силу леммы 13 можно построить обобщенную схему S_B, которая правильно реализует матрицу B и для которой справедливы соотношения

$$\lambda(S_B) \leqslant \log \max\left(b_{11}\frac{b_{32}}{b_{33}}, b_{12}, b_{12}b_{21}\right) + \log b_{33} + O(1) \leqslant$$
$$\leqslant \log D(B) + O(1) = \log D(A) + O(1).$$

Таким образом, в обоих случаях, учитывая лемму 15, можно построить обобщенную схему S, которая правильно реализует матрицу A и для которой справедливы соотношения $\lambda(S) \leqslant \lambda(S_B) + O(1) \leqslant \log D(A) + O(1)$. Лемма 16 доказана.

Лемма 17. *Пусть матрица B' получается из матрицы B заменой некоторого единичного элемента на нулевой. Тогда $D(B') \leqslant 2D(B)$.*

Доказательство. Без ограничения общности полагаем, что $b_{11} = 1$, $b'_{11} = 0$. Если минор матрицы B', модуль которого равен $D(B')$, не содержит элемента b'_{11}, то, очевидно, выполняется неравенство $D(B') \leqslant D(B)$. Далее также без ограничения общности будем считать, что этот минор M' состоит из первых t строк и первых t столбцов матрицы B'. Обозначив соответствующий минор матрицы B через M, а алгебраическое дополнение элемента b_{1j} в матрицах M и M' через A_{1j}, получаем

$$D(B') = |\det M'| = \left|\sum_{j=2}^{t} b_{1j}A_{1j}\right| = \left|\sum_{j=1}^{t} b_{1j}B_{1j} - A_{11}\right| =$$
$$= |\det M - A_{11}| \leqslant |\det M| + |A_{11}| \leqslant 2D(B).$$

Лемма 17 доказана.

Лемма 18. *Пусть в каждом столбце и каждой строке допустимой матрицы A размера 3×3 ровно по одному нулевому элементу. Тогда можно построить обобщенную схему S, которая правильно реализует матрицу A и для которой справедливо соотношение $\lambda(S) \leqslant \log D(A) + O(1)$.*

Доказательство. Обозначим через m величину минимального ненулевого элемента матрицы A, через A/m матрицу, которая получается из матрицы A путем деления каждого элемента на m, а через B матрицу, получающуюся из матрицы A/m посредством замены одного единичного элемента (а такой в матрице A/m точно есть) на нулевой.

Отметим, что в условиях леммы 18 будут справедливы равенства $D(A) = |\det A|$ и $D(A/m) = |\det A/m|$. В матрице B найдется столбец, в котором есть два нулевых элемента. Из леммы 14 или леммы 16, а также леммы 17 следует, что можно построить обобщенную схему S, которая правильно реализует матрицу A и для которой справедливы соотношения

$$\lambda(S) \leqslant 3\log m + \log D(B) + O(1) \leqslant 3\log m + \log D(A/m) + O(1) =$$
$$= 3\log m + \log|\det(A/m)| + O(1) = \log|\det A| + O(1) = \log D(A) + O(1).$$

Лемма 18 доказана.

Лемма 19. *Пусть последовательность $\{A_n\}$ допустимых матриц размера 3×3 удовлетворяет условию $D(A_n) \to \infty$ при $n \to \infty$. Тогда можно построить такую последовательность S_n обобщенных схем, правильно реализующих последовательность матриц A_n, что выполняется соотношение $\lambda(S_n) \leqslant \log D(A_n) + O(1)$.*

Доказательство. К матрице A, являющейся элементом исходной последовательности, применим операцию приведения относительно строки, содержащей максимальный элемент. Полученную матрицу обозначим $B = (b_{ij})$. В силу леммы 15 выполняется неравенство $D(B) \leqslant 4D(A)$.

По построению матрицы B среди элементов первой строки находится максимальный элемент, а во второй и третьей строках есть по крайней мере один нулевой элемент.

Если в матрице B есть два нулевых элемента в одном столбце, то, используя либо лемму 14, либо лемму 16, а затем лемму 15, получаем, что можно построить обобщенную схему S, которая правильно реализует матрицу A и для которой справедливо соотношение $\lambda(S)\leqslant\log D(A)+O(1)$.

Далее считаем, что нулевые элементы матрицы B находятся в разных столбцах.

Пусть максимальным элементом матрицы B является элемент b_{11}. В силу леммы 12 верно неравенство $D(B)\leqslant 4D_{11}(B)$. Обозначим через $B'(x)$ матрицу, получающуюся из матрицы B путем деления всех элементов первой строки матрицы B на x. Очевидно, что

$$D_{11}(B'(1))=D_{11}(B)\geqslant D(B)/4,\quad \lim_{x\to\infty}D_{11}(B'(x))=0,$$
$$D(B'(x))\geqslant\max\{b_{21},b_{22},b_{23},b_{31},b_{32},b_{33}\}.$$

Обозначим через x_0 наименьшее значение x, удовлетворяющее равенству $D_{11}(B'(x))=D(B'(x))/5$.

Далее положим $k=\min\{x_0,b_{12},b_{13}\}$, $C=B'(k)$. Тогда

$$D(C)\leqslant 5D_{11}(C)=5D_{11}(B)/k\leqslant 5D(B)/k\leqslant 20D(A)/k.$$

Если $k=x_0$, то любая обобщенная схема S_C, правильно реализующая матрицу C, легко достраивается до обобщенной схемы S_B, правильно реализующей матрицу B и удовлетворяющей неравенству

$$\lambda(S_B)\leqslant\lceil\log k\rceil+\lambda(S_C).$$

В силу леммы 12 и равенства $D(C)=5D_{11}(C)$ элемент матрицы C, стоящий в первой строке и первом столбце, не может быть максимальным элементом матрицы C. Остальные элементы первой строки матрицы C не превосходят этого элемента, следовательно, максимальный элемент матрицы C находится во второй или третьей строках.

Применяя к матрице C операцию приведения относительно строки, содержащей максимальный элемент, получаем матрицу F, содержащую хотя бы по одному нулевому элементу в каждой строке. В силу леммы 15 верно неравенство $D(F)\leqslant 4D(C)$ и, следовательно, $D(F)\leqslant 80D(A)/k$.

Рассмотрим теперь случай равенства $k=\min(b_{12},b_{13})$. Без ограничения общности будем считать, что $k=b_{13}$. В матрице $C=(c_{ij})$ элементы первой строки определяются равенствами $c_{11}=b_{11}/k$, $c_{12}=b_{12}/k$, $c_{13}=1$, а остальные элементы совпадают с соответствующими элементами матрицы B.

В этом случае через F обозначим матрицу, получающуюся из матрицы C заменой элемента c_{13}, равного единице, на нулевой элемент. В силу леммы 17 верно неравенство $D(F)\leqslant 2D(C)$ и, следовательно, $D(F)\leqslant 40D(A)/k$.

Таким образом, в обоих случаях матрица F удовлетворяет условию $D(F)\leqslant 80D(A)/k$ и в каждой строке матрицы F есть хотя бы один нулевой элемент.

В силу лемм 14, 16 и 18 можно построить обобщенную схему S_F, которая правильно реализует матрицу F и для которой справедливо соотношение $\lambda(S_F) \leqslant \log D(F) + O(1)$. Теперь по схеме S_F можно построить обобщенную схему S_C, правильно реализующую матрицу C и удовлетворяющую условию $\lambda(S_C) \leqslant \lambda(S_F) + O(1)$. Во втором случае этот факт очевиден, а в первом следует из леммы 15.

Далее, из леммы 15 следует возможность построения обобщенной схемы S, правильно реализующей матрицу A и удовлетворяющей соотношению $\lambda(S) \leqslant \lambda(S_B) + O(1) \leqslant \lambda(S_C) + \log k + O(1)$. Поэтому

$$\lambda(S) \leqslant \lambda(S_F) + \log k + O(1) \leqslant \log D(F) + \log k + O(1) \leqslant \log D(A) + O(1).$$

Лемма 19 доказана.

Из леммы 19 непосредственно следует оценка

$$\lambda(A_n) \leqslant (1 + o(1)) \log D(A_n),$$

которая завершает доказательство теоремы 30.

5.6. Сложность одной системы из $2t$ одночленов от $2t$ переменных. Итак, исследование задачи Пиппенджера в направлении нахождения асимптотики роста величины $l(A_n)$ для произвольной (индивидуальной) последовательности матриц $A_n = (a_{ij}(n))$ фиксированного размера $p \times q$, удовлетворяющей при $n \to \infty$ условию $\max\limits_{i,j}\{a_{ij}(n)\} \to \infty$, в случаях, когда матрицы имеют размер $1 \times q$ (задача Р. Беллмана), $p \times 1$ (задача Д. Кнута), $2 \times q$, $p \times 2$ или 3×3, дало результаты, которые могут быть сформулированы единообразно: все упомянутые асимптотики имеют вид $\log D(A_n)$, где $D(A_n)$ — максимум абсолютных величин всех миноров матрицы A_n. Эти результаты, а также тот факт, что для вычислительной модели, в которой, помимо операции умножения, доступна операция деления и о которой подробно пойдет речь в следующем параграфе, асимптотика роста сложности имеет вид $\log D(A_n)$ (см. основной результат работы [43] или теорему 34 из следующего параграфа) уже для произвольной последовательности матриц A_n фиксированного размера $p \times q$, естественным образом могут привести к предположению о том, что для матриц любого фиксированного размера $p \times q$ в рамках асимптотической постановки задачи справедливо соотношение $l(A) \sim \log D(A)$.

Однако в 2008 г. установлено [50], что 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 — приведен пример последовательности матриц размера $2t \times 2t$, для которой можно усилить универсальную нижнюю оценку из теоремы 26 асимптотически 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

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

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

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 записью a_{ij} при $j>2t$ и $1\leqslant i\leqslant 2t$ понимать элемент a_{ir}, где r определяется из условий $1\leqslant r\leqslant 2t$, $r\equiv j \pmod{2t}$.

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 записью x_j при $j>2t$ понимать переменную x_r, где r определяется из условий $1\leqslant r\leqslant 2t$, $r\equiv j \pmod{2t}$, 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 так: $f_i=x_i^n x_{i+1}^n\ldots x_{i+t-1}^n$.

Т е о р е м а 31 [50]. *При условии $t=o(\log n)$ справедливо асимптотическое равенство*

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

Д о к а з а т е л ь с т в о. *Нижняя оценка.* Пусть S — минимальная схема из элементов умножения с $2t$ входами, на которые подаются переменные $x_1,x_2,\ldots,x_{2t}$, и $2t$ выходами, которые вычисляют одночлены $f_i=x_i^n x_{i+1}^n\ldots x_{i+t-1}^n$, т. е. на выходах схемы S вычисляется система одночленов, задаваемая матрицей $A(t,n)$. Будем считать, что на i-м выходе схемы S реализуется одночлен f_i.

Среди всех элементов схемы S выделим подмножества S_i, $i=1,2,\ldots,2t$, следующим образом. Элемент схемы S отнесем к множеству S_i, если вычисляемый этим элементом одночлен имеет вид

$$x_i^{\alpha_i}x_{i+1}^{\alpha_{i+1}}\ldots x_{i+t-1}^{\alpha_{i+t-1}},$$

где $\alpha_i\geqslant 1$, $\alpha_j\geqslant 0$ при $i+1\leqslant j\leqslant i+t-1$.

При $i\neq j$ выполняется соотношение $S_i\cap S_j=\varnothing$. Действительно, пусть это не так, т. е. некоторый элемент e схемы S содержится и в множестве S_i, и в множестве S_j. Тогда он вычисляет одночлен, содержащий в качестве множителя и ненулевую степень переменной x_i, и ненулевую степень переменной x_j. Далее, если $x_i\in\{x_j,x_{j+1},\ldots,x_{j+t-1}\}$, то $x_j\notin\{x_i,x_{i+1},\ldots,x_{i+t-1}\}$ и, следовательно, хотя бы одно из двух включений

$$x_i\in\{x_j,x_{j+1},\ldots,x_{j+t-1}\},\quad x_j\in\{x_i,x_{i+1},\ldots,x_{i+t-1}\}$$

не выполняется, что противоречит тому, что вычисляемый элементом e одночлен содержит в качестве множителя и ненулевую степень переменной x_i, и ненулевую степень переменной x_j.

С другой стороны, для любого i, $1\leqslant i\leqslant 2t$, справедливо неравенство $|S_i|\geqslant\log n$ и поэтому окончательно имеем:

$$l(A(t,n))=l(S)\geqslant 2t\log n.$$

Верхняя оценка. Для вычисления системы одночленов $\{f_1, f_2, \ldots, f_{2t}\}$, задаваемой матрицей $A(t,n)$, достаточно каждую переменную возвести в степень n, а затем для каждого из одночленов $f_1, f_2, \ldots, f_{2t}$ перемножить соответствующие t степеней. Поэтому, применяя теорему Брауэра, при $t = o(\log n)$ имеем:

$$l(A(t,n)) \leqslant 2t\left(\log n + O\left(\frac{\log n}{\log\log n}\right)\right) + 2t(t-1) = 2t(\log n + o(\log n)).$$

Теорема 31 доказана.

Л е м м а 20. *При* $t \leqslant \log n/(\log\log n)$ *справедливо равенство*

$$D(A(t,n)) = n^{t+1}.$$

Д о к а з а т е л ь с т в о. Разобьем строки матрицы $A(t,n)$ на t пар, отнеся для $i = 1, 2, \ldots, t$ к i-й паре строки с номерами i и $i+t$. Аналогичным образом разобьем столбцы матрицы $A(t,n)$ на t пар, отнеся для $j = 1, 2, \ldots, t$ к j-й паре столбцы с номерами j и $j+t$. Покомпонентная сумма строк (столбцов) любой пары дает строку $(n, n, \ldots, n)$ (столбец $(n, n, \ldots, n)^T$). Следовательно, любое множество строк (столбцов), включающее в себя для двух некоторых пар обе строки (оба столбца) этих пар, является линейно зависимым, и поэтому любой минор порядка r, где $r \geqslant t+2$, равен 0.

Рассмотрим миноры порядка $t+1$. Для того, чтобы определитель подматрицы, состоящей из $t+1$ строки и $t+1$ столбца матрицы $A(t,n)$, был отличен от 0, необходимо выполнение двух условий: ровно для одной пары обе строки включены в подматрицу (следовательно, среди выбранных строк должен быть представитель каждой пары) и ровно для одной пары оба столбца включены в подматрицу (среди выбранных столбцов должен быть представитель каждой пары).

В случае выполнения этих условий из такой подматрицы с помощью элементарных преобразований, не изменяющих абсолютную величину определителя — перестановки строк, умножения строки на -1, сложения строки со строкой $(n, n, \ldots, n)$, перестановки столбцов, умножения столбца на -1, сложения столбца со столбцом $(n, n, \ldots, n)^T$, — можно получить матрицу, совпадающую с подматрицей матрицы $A(t,n)$, состоящей из ее первых $t+1$ строк и первых $t+1$ столбцов. Определитель такой матрицы равен n^{t+1}. Таким образом, миноры порядка $t+1$ по абсолютной величине равны либо 0, либо n^{t+1}.

Миноры порядка не более t не превосходят по абсолютному значению величины $t!n^t$.

Следовательно, при выполнении условия $t \leqslant \log n/(\log\log n)$ имеем:

$$n^{t+1} \leqslant D(A(t,n)) \leqslant \max\left(n^{t+1},\ t!n^t\right) = n^{t+1}.$$

Лемма 20 доказана.

С помощью леммы 20 из теоремы 31 легко получить

С л е д с т в и е 4. *При условии* $t \leqslant \log n/(\log\log n)$ *справедливо асимптотическое равенство*

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

Тем самым уже для матриц размера 4×4 нижняя оценка из теоремы 26 в случае классической вычислительной модели может быть усилена в $4/3$ раз. Таким образом, гипотеза о том, что в задаче Пиппенджера для произвольной последовательности матриц A_n фиксированного размера $p \times q$, справедливо соотношение $l(A_n) \sim \log D(A_n)$, опровергнута уже на примере матриц размера 4×4. Задача об асимптотике роста сложности даже в случае фиксированного размера матриц представляется очень тяжелой. К настоящему моменту не выработана приемлемая гипотеза об асимптотике роста сложности даже для матриц размера 4×4. Более того, начиная с 2009 г. в этом направлении не было никакого принципиального продвижения. Только в 2020 г. С. А. Корнееву удалось [26, 29] перенести один свой результат относительно сложности вычисления систем одночленов схемами композиции на случай вычисления классическими схемами умножения. Об этом подробнее будет сказано в последнем параграфе — см. теорему 77.

§ 6. Аддитивные вычисления целочисленных линейных форм

Если в задаче Пиппенджера помимо операции умножения дополнительно разрешить использование операции деления, то получится другая задача, которая и рассматривается в настоящем параграфе.

В мультипликативной постановке — это задача об исследовании величины $l_2(z_1, z_2, \ldots, z_p)$, численно равной минимальному количеству операций умножения и деления, достаточному для вычисления системы функций

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

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

Однако для этой задачи чаще используется следующая аддитивная постановка. Пусть задана система из p линейных форм от q переменных:

$$y_1 = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1q}x_q,$$

$$y_2 = a_{21}x_1 + a_{22}x_2 + \ldots + a_{2q}x_q,$$

$$\ldots$$

$$y_p = a_{p1}x_1 + a_{p2}x_2 + \ldots + a_{pq}x_q,$$

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).

Очевидно, что мультипликативная и аддитивная постановки задачи эквивалентны, т. е. при введенных обозначениях справедливо равенство

$$l_2(z_1, z_2, \ldots, z_p) = l_2(y_1, y_2, \ldots, y_p).$$

Величину $l_2(A)$ можно определить также на языке аддитивных цепочек (см., например, [161, 169, 172, 195, 198]). *Цепочкой из сложений и вычитаний (векторов)* для матрицы $A=(a_{ij})$ размера $p\times q$ назовем последовательность q-мерных векторов (наборов) вида

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

начинающуюся с q единичных векторов и удовлетворяющую следующим условиям:

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

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

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 $p\times q$, а сама схема состоит из двухвходовых элементов, реализующих сумму или разность функций, подаваемых на входы элемента.

Задача исследования величины $l_2(y_1,y_2,\ldots,y_p)$ поставлена, например, в [101].

Так же, как и в предыдущем параграфе, прежде чем переходить к описанию известных результатов для задачи о сложности вычисления линейных форм, сформулируем доказанное в 1981 г. А. Ф. Сидоренко [101] следующее свойство двойственности.

Т е о р е м а 32 [101]. *Для любой целочисленной матрицы A размера $p\times q$ выполняются неравенства*

$$-q\leqslant l_2\left(A^T\right)-l_2(A)\leqslant p.$$

Исходное доказательство теоремы 32 из [101] довольно тяжелое. Однако утверждение теоремы 32 нетрудно установить, несколько модифицировав доказательство теоремы 4, как это сделано, например, в [99]. Отметим также, что если в обсуждаемой вычислительной модели в аддитивной постановке помимо операций $x+y$ и $x-y$ разрешить использование еще и операции $-x-y$, то для естественным образом определяемой (см., например, [163, 169]) меры сложности l_2' справедливо утверждение, аналогичное теореме 4: для любой целочисленной матрицы A размера $p\times q$ без нулевых строк и столбцов справедливо равенство

$$l_2'\left(A^T\right)-l_2'(A)=p-q.$$

6.1. Функция Шеннона сложности вычисления систем целочисленных линейных форм. Определим *функцию Шеннона* $L_2(p,q,K)$ *сложности вычисления систем целочисленных линейных форм*, положив $L(p,q,K)=\max l(A)$, где максимум берется по всем целочисленным матрицам $A=(a_{ij})$ размера $p\times q$, удовлетворяющим условиям $|a_{ij}|\leqslant K-1$, $i=1,\ldots,p$, $j=1,\ldots,q$. 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 $\{0,\pm1,\ldots,\pm(K-1)\}$.

Т е о р е м а 33 [33]. *При условии* $pq\log K\to\infty$ *справедливо равенство*

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

Д о к а з а т е л ь с т в о. В силу теоремы 32 справедливы неравенства

$$-q\leqslant L_2(q,p,K)-L_2(p,q,K)\leqslant p.$$

Поэтому без ограничения общности можно далее считать, что выполняется условие $p\leqslant q$.

Верхняя оценка. Опишем метод вычисления системы, состоящей из p линейных форм от q переменных, заданной целочисленной матрицей $A=(a_{ij})$ размера $p\times q$, элементы которой удовлетворяют условию $a_{ij}\in\{0,\pm1,\pm2,\ldots,\pm(K-1)\}$.

С л у ч а й 1. Пусть выполняется неравенство $\log\log(2K-1)\leqslant(pq)^{1/2}$.

Отметим, что в условиях этого случая, если $pq\log K\to\infty$, то $pq\to\infty$. Сначала вычислим линейную форму $-(K-1)(x_1+x_2+\ldots+x_q)$. Это можно сделать, используя одну операцию вычитания и не более $q+2\log K$ операций сложения. После этого вычислим систему из p линейных форм от q переменных, заданную матрицей $B=(b_{ij})$ размера $p\times q$, определяемую для всех $i=1,2,\ldots,p$, $j=1,2,\ldots,q$, равенством $b_{ij}=a_{ij}+K-1$. В силу соотношений $0\leqslant b_{ij}\leqslant 2K-2$ и теоремы 25 для этого достаточно

$$p\log(2K-1)+\frac{pq\log(2K-1)}{\log(pq\log(2K-1))}\left(1+O\left(\left(\frac{\log\log(pq\log K)}{\log(pq\log K)}\right)^{1/2}\right)\right)+O(q)$$

операций сложения. После этого получить систему линейных форм, заданную матрицей A, можно, используя p операций сложения.

Таким образом,

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

Отсюда вытекает требуемая верхняя оценка в случае 1, так как

$$\frac{\log K}{\frac{pq\log K}{(\log(pq\log K))^{3/2}}}=\left(\frac{\log(pq)+\log\log K}{(pq)^{2/3}}\right)^{3/2}=o(1),$$

т. е. $\log K=o\left(\dfrac{pq\log K}{(\log(pq\log K))^{3/2}}\right)$.

С л у ч а й 2. Пусть выполняется неравенство $\log\log(2K-1) > (pq)^{1/2}$.

Сначала последовательно вычислим линейные формы

$$\begin{gathered} x_1+x_2,\ x_1+x_2+x_3,\ \ldots,\ x_1+x_2+\ldots+x_q; \\ 2(x_1+x_2+\ldots+x_q),\ -(x_1+x_2+\ldots+x_q); \\ -x_q,\ -(x_1+x_2+\ldots+x_{q-1}); \\ -x_{q-1},\ -(x_1+x_2+\ldots+x_{q-2}); \\ \ldots\ldots \\ -x_3,\ -(x_1+x_2);\quad -x_2,\ -x_1. \end{gathered}$$

Для этого достаточно использовать $q+2(q-1)$ операций сложения и одну операцию вычитания.

Реализуемые линейные формы

$$s_i = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{iq}x_q, \quad i = 1, 2, \ldots, p,$$

где $-K < a_{ij} < K$, представим (при некотором фиксированном параметре t, значение которого будет выбрано позже) в виде

$$s_i = \left(s_{i1}2^{t-1} + s_{i2}\right)2^{t-2} + \ldots + s_{ir},$$

где $r = \left\lceil \frac{\lceil \log K \rceil}{t} \right\rceil$, а s_{ij}, $j = 1, 2, \ldots, r$, — линейные формы от q переменных с коэффициентами из множества $\{0, \pm 1, \pm 2, \ldots, \pm(2^t-1)\}$ (аналог схемы Горнера).

Теперь, используя $2q(2^t-2)$ операций сложения, вычислим все формы kx_j, $-(2^t-1) \leqslant k \leqslant 2^t-1$, $j = 1, 2, \ldots, q$, а затем с помощью не более чем $rp(q-1)$ операций сложения — все формы s_{ij}, и, наконец, используя $p(t+1)(r-1)$ сложений, вычислим все формы s_i.

Таким образом, в случае 2 получаем

$$\begin{aligned} L_2(p,q,K) &\leqslant 3q + 2q(2^t-2) + rp(q-1) + p(t+1)(r-1) \leqslant \\ &\leqslant p\log K + \frac{pq\log K}{t} + 2pq + 2^{t+1}q. \end{aligned}$$

Положим $t = \lceil \log\log K - 2\log\log\log K \rceil$. Тогда

$$\begin{aligned} L_2(p,q,K) &\leqslant p\log K + \frac{pq\log K}{\log\log K - 2\log\log\log K} + 2pq + \frac{4q\log K}{(\log\log K)^2} \leqslant \\ &\leqslant p\log K + \frac{pq\log K}{\log\log K}\left(1 + O\left(\frac{\log\log\log K}{\log\log K}\right)\right) + 2(\log\log K)^2 = \\ &= p\log K + \frac{pq\log K}{\log(pq\log K)}\left(1 + O\left(\frac{\log\log(pq\log K)}{\log(pq\log K)}\right)\right) \leqslant \\ &\leqslant p\log K + \frac{pq\log(2K-1)}{\log(pq\log K)}\left(1 + O\left(\frac{\log\log(pq\log K)}{\log(pq\log K)}\right)\right). \end{aligned}$$

Нижняя оценка доказывается аналогично нижней оценке теоремы 25. Незначительные изменения связаны с тем, что вместо одной операции можно использовать две.

Теорема 33 доказана.

Отметим, что при доказательстве верхней оценки предложен подход к вычислению системы целочисленных линейных форм, дающий требуемую оценку числа операций и использующий в случае $p \leqslant q$ ровно одну операцию вычитания. Промоделировав доказательство леммы 2 из [99], нетрудно установить, что и в двойственном случае $p > q$ для получения требуемой верхней оценки достаточно использовать ровно одну операцию вычитания.

6.2. Случай слаборастущих значений числа линейных форм и количества переменных. Для этой задачи для любых фиксированных (и даже слаборастущих) значениях размеров матрицы, задающей систему целочисленных линейных форм, получено асимптотически точное решение — в 2006 г. установлена верхняя оценка сложности, асимптотически совпадающая с нижней.

Теорема 34 [43]. *Пусть последовательность целочисленных матриц* $A(n) = \big(a_{ij}(n)\big)$ *размера* $p(n) \times q(n)$ *при* $n \to \infty$ *удовлетворяет условию*

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

Тогда

$$\log D(A(n)) \leqslant l_2\left(A(n)\right) \leqslant \log D(A(n)) + o\big(\log D(A(n))\big).$$

Нижняя оценка теоремы 34 следует непосредственно из теоремы 26.

Доказательство верхней оценки из [43] приводиться не будет, здесь ограничимся значительно более простым доказательством этой верхней оценки при выполнении несколько более сильного условия

$$\frac{p(n) + q(n)}{\left(\log\log\log \max\limits_{a_{ij} \in A(n)} |a_{ij}|\right)^{1/4}} \to 0,$$

которое, однако, сохраняет на качественном уровне основной результат, заключающийся в том, что для любых фиксированных (и даже слаборастущих) значениях размеров матрицы, задающей систему функций, верхняя оценка сложности вычисления этой системы асимптотически совпадает с нижней.

Упрощение доказательства, так же, как и в случае исследования задачи Пиппенджера в предыдущем параграфе, связано с переходом к рассмотрению вспомогательной вычислительной модели — *обобщенных* λ_2*-схем*, отличающихся от введенных при изучении задачи Пиппенджера обобщенных схем только наличием дополнительной операции деления (здесь для единообразия с задачей Пиппенджера переходим к мультипликативной постановке задачи). Меру сложности обобщенных λ_2-схем, связанную с общим числом элементов в схеме, будем называть λ_2-сложностью.

Для меры сложности l_2 в условиях теоремы 29 справедлива оценка через величину λ_2-сложности, аналогичная оценке из теоремы 29:

$$l_2\left(A\right) \leqslant \lambda_2\left(\widehat{S}\right) + o\left(\frac{\log \max |a_{ij}|}{\log\log\log \max |a_{ij}|}\right).$$

Это неравенство и позволяет свести доказательство верхней оценки теоремы 34 (в ослабленной формулировке) к доказательству следующего утверждения.

Лемма 21. *Для произвольной матрицы A размера $p\times q$ с рациональными элементами можно построить вычисляющую ее обобщенную λ_2-схему S, удовлетворяющую условию*

$$\lambda_2(S)\leqslant \log D(A)+3(p+q)^2$$

и состоящую не более чем из $2(p+q)^2$ простейших подсхем.

Доказательство. Будем вести индукцию по величине $\min\{p,q\}$.

База индукции. Пусть выполняется условие $\min\{p,q\}=1$.

Рассмотрим случай $p=1$, т.е. случай вычисления функции $x_1^{a_1}x_2^{a_2}\ldots x_q^{a_q}$. Без ограничения общности будем считать, что $|a_1|\geqslant|a_2|\geqslant\ldots\geqslant|a_q|>0$. Предварительно для всех j, $j=1,2,\ldots,q$, для которых выполняется условие $a_j<0$, построим подсхему (состоящую из двух элементов деления), возводящую переменную x_j в степень -1. Положим $y_j=x_j^{\operatorname{sgn} a_j}$, $j=1,2,\ldots,q$. Теперь построим обобщенную схему, вычисляющую по функциям $y_1,y_2,\ldots,y_q$ функцию $y_1^{|a_1|}y_2^{|a_2|}\ldots y_q^{|a_q|}=x_1^{a_1}x_2^{a_2}\ldots x_q^{a_q}$. Сначала переменную y_1 возведем в степень $|a_1/a_2|$, а полученную функцию домножим на переменную y_2, тем самым вычисляя функцию $y_1^{|a_1/a_2|}y_2$, затем эту функцию возведем в степень $|a_2/a_3|$, а полученную функцию домножим на переменную y_3, тем самым вычисляя функцию $y_1^{|a_1/a_3|}y_2^{|a_2/a_3|}y_3$, и т.д. На предпоследнем шаге вычислим функцию $y_1^{|a_1/a_q|}y_2^{|a_2/a_q|}\ldots y_{q-1}^{|a_{q-1}/a_q|}y_q$, а на последнем, возведя эту функцию в степень $|a_q|$, получим функцию $y_1^{|a_1|}y_2^{|a_2|}\ldots y_q^{|a_q|}$.

Таким образом, построенная обобщенная λ_2-схема S вычисляет функцию $x_1^{a_1}x_2^{a_2}\ldots x_q^{a_q}$, состоит не более чем из $3q-1$ простейших подсхем и удовлетворяет соотношению (здесь предполагаем, что все подсхемы возведения в степень минимальны)

$$\lambda_2(S)\leqslant 2q+\left\lceil\log\left|\frac{a_1}{a_2}\right|\right\rceil+\left\lceil\log\left|\frac{a_2}{a_3}\right|\right\rceil+\ldots+\left\lceil\log\left|\frac{a_{q-1}}{a_q}\right|\right\rceil+\lceil\log|a_q|\rceil+q+1,$$

из которого следует, что $\lambda_2(S)\leqslant\log|a_1|+4q$.

Теперь перейдем к случаю $q=1$, т.е. к случаю вычисления системы степеней $x^{a_1},x^{a_2},\ldots,x^{a_p}$. Снова без ограничения общности будем считать, что $|a_1|\geqslant|a_2|\geqslant\ldots\geqslant|a_p|>0$. Построим обобщенную λ_2-схему, вычисляющую систему степеней $x^{|a_1|},x^{|a_2|},\ldots,x^{|a_p|}$. Эта схема будет состоять из цепочки подсхем, каждая из которых возводит подаваемую на вход подсхемы функцию, соответственно, в степени $|a_q|$, $|a_{q-1}/a_q|$, …, $|a_2/a_1|$, а на вход первой из них подается переменная x.

Далее для всех i, $i=1,2,\ldots,p$, для которых выполняется условие $a_i<0$, построим подсхему (состоящую из двух элементов деления), возводящую функцию $x^{|a_i|}$ в степень -1.

Таким образом построенная обобщенная λ_2-схема S вычисляет систему степеней $x^{a_1},x^{a_2},\ldots,x^{a_p}$, состоит не более чем из $2p$ простейших подсхем и удовлетворяет соотношению (здесь снова предполагаем, что все подсхемы возведения в степень минимальны)

$$\lambda_2(S)\leqslant\lceil\log|a_p|\rceil+\left\lceil\log\left|\frac{a_{p-1}}{a_p}\right|\right\rceil+\ldots+\left\lceil\log\left|\frac{a_1}{a_2}\right|\right\rceil+2p,$$

из которого следует, что $\lambda_2(S)\leqslant\log|a_1|+3p$.

Для завершения доказательства базы индукции осталось учесть равенство $D(A) = a_1$.

Шаг индукции. Без ограничения общности будем считать, что имеет место равенство

$$|a_{11}| = \max |a_{ij}|.$$

При $|a_{11}| < 1$ утверждение очевидно. Далее будем считать, что $|a_{11}| \geqslant 1$.

Не изменяя абсолютных значений элементов исходной матрицы A, определим еще одну матрицу размера $p \times q$ с рациональными элементами — матрицу $B = (b_{ij})$ — следующим образом:

$$b_{i1} = a_{i1} \operatorname{sgn} a_{i1}, \quad i = 1, 2, \ldots, p;$$
$$b_{ij} = a_{ij} \operatorname{sgn}(a_{i1} a_{11} a_{1j}), \quad i = 2, 3, \ldots, p, \ j = 1, 2, \ldots, q.$$

Отметим, что в матрице B все элементы первого столбца и все элементы первой строки неотрицательны. Кроме того, имеет место равенство $b_{11} = \max |b_{ij}|$.

Матрицу A по матрице B можно восстановить таким образом. Сначала i-ю строку матрицы B, $i = 1, 2, \ldots, p$, домножим на $\operatorname{sgn} a_{i1}$ (это соответствует переходу от функции $x_1^{b_{i1}} x_2^{b_{i2}} \ldots x_q^{b_{iq}}$ к функции $x_1^{-b_{i1}} x_2^{-b_{i2}} \ldots x_q^{-b_{iq}} = \left(x_1^{b_{i1}} x_2^{b_{i2}} \ldots x_q^{b_{iq}}\right)^{-1}$ в случае, когда выполняется неравенство $a_{i1} < 0$), а затем j-й столбец полученной матрицы, $j = 1, 2, \ldots, q$, домножим на величину $\operatorname{sgn}(a_{1j} a_{11})$ (это соответствует замене переменной x_j на x_j^{-1} во всех функциях в случае, когда выполняется неравенство $a_{1j} a_{11} < 0$). Поэтому, в частности, имеет место равенство

$$D(A) = D(B).$$

Таким образом, если построена обобщенная λ_2-схема S, реализующая матрицу B, то на ее основе построить обобщенную λ_2-схему S', вычисляющую матрицу A, можно следующим образом. Сначала к i-му выходу схемы S, $i = 2, 3, \ldots, p$, в случае, если выполняется неравенство $a_{i1} < 0$, присоединим подсхему (состоящую из двух элементов деления), возводящую подаваемую на вход функцию в степень -1, а затем на j-й вход полученной схемы, $j = 1, 2, \ldots, q$, в случае, если выполняется неравенство $a_{1j} a_{11} < 0$, вместо переменной x_j подадим выход подсхемы (состоящей из двух элементов деления), возводящей переменную x_j в степень -1. Следовательно, для построения по обобщенной λ_2-схеме, вычисляющей матрицу B, обобщенной λ_2-схемы, вычисляющей матрицу A, достаточно к входам и выходам схемы присоединить не более $p+q$ одновходовых обобщенных схем с общим числом элементов не более $2(p+q)$.

Докажем требуемую оценку для матрицы B.

Положим

$$b'_{ij} = b_{i1} \frac{b_{1j}}{b_{11}}, \qquad i = 2, 3, \ldots, p, \quad j = 2, 3, \ldots, q.$$

Заметим, что справедливы неравенства

$$0 \leqslant b'_{ij} \leqslant \min(b_{i1}, b_{1j}), \quad i = 2, 3, \ldots, p, \quad j = 2, 3, \ldots, q.$$

В силу равенств

$$x_1^{b_{i1}}x_2^{b_{i2}}\dots x_q^{b_{iq}} = x_1^{b_{i1}}x_2^{b'_{i2}}\dots x_q^{b'_{iq}}x_2^{b_{i2}-b'_{i2}}x_3^{b_{i3}-b'_{i3}}\dots x_q^{b_{iq}-b'_{iq}}, \quad i=2,3,\dots,p,$$

для построения обобщенной λ_2-схемы S, вычисляющей матрицу B, достаточно построить обобщенную λ_2-схему S_1, вычисляющую систему функций

$$\left\{x_1^{b_{11}}x_2^{b_{12}}\dots x_q^{b_{1q}}, x_1^{b_{21}}x_2^{b'_{22}}\dots x_q^{b'_{2q}}, \dots, x_1^{b_{p1}}x_2^{b'_{p2}}\dots x_q^{b'_{pq}}\right\},$$

и обобщенную λ_2-схему S_2, вычисляющую систему функций

$$\left\{x_2^{b_{22}-b'_{22}}x_3^{b_{23}-b'_{23}}\dots x_q^{b_{2q}-b'_{2q}}, x_2^{b_{32}-b'_{32}}x_3^{b_{33}-b'_{33}}\dots x_q^{b_{3q}-b'_{3q}}, \dots \right.$$
$$\left. \dots, x_2^{b_{p2}-b'_{p2}}x_3^{b_{p3}-b'_{p3}}\dots x_q^{b_{pq}-b'_{pq}}\right\},$$

а затем с помощью $p-1$ одноэлементной подсхемы для $i=2,3,\dots,p$ перемножить i-й выход схемы S_1 и $(i-1)$-й выход подсхемы S_2.

Схема S_1, в свою очередь, при наличии среди неотрицательных чисел b_{i1}, $i=2,3,\dots,p$, хотя бы одного отличного от 0 числа будет состоять из двух подсхем S'_1 и S''_1.

Подсхема S'_1 по переменным $x_1, x_2, \dots, x_q$ для некоторого i_0, $1 \leqslant i_0 \leqslant p$, удовлетворяющего условию $b_{i_0 1} \neq 0$, вычисляет функцию $x_1^{b_{i_0 1}}x_2^{b'_{i_0 2}}\dots x_q^{b'_{i_0 q}}$. В силу базы индукции (случай $p=1$) можно считать, что схема S'_1 состоит не более чем из $3q-1$ простейших подсхем и удовлетворяет в силу очевидных неравенств $b_{i_0 1} \geqslant b'_{i_0 j}$, $j=2,3,\dots,q$, соотношению $\lambda_2(S'_1) \leqslant \log b_{i_0 1} + 4q$.

Подсхема S'_2 возводит функцию $x_1^{b_{i_0 1}}x_2^{b'_{i_0 2}}\dots x_q^{b'_{i_0 q}}$ в степени $b_{i1}/b_{i_0 1}$, $i=1,2,\dots,p$, тем самым вычисляя систему всех отличных от единичной функций из множества

$$\left\{x_1^{b_{11}}x_2^{b_{12}}\dots x_q^{b_{1q}}, x_1^{b_{21}}x_2^{b'_{22}}\dots x_q^{b'_{2q}}, \dots, x_1^{b_{p1}}x_2^{b'_{p2}}\dots x_q^{b'_{pq}}\right\}.$$

В силу базы индукции (случай $q=1$) можно считать, что схема S'_2 состоит не более чем из $2p$ простейших подсхем и удовлетворяет соотношению $\lambda_2(S'_1) \leqslant \log\left(b_{11}/b_{i_0 1}\right) + 3p$.

Таким образом, можно считать, что обобщенная λ_2-схема S_1 состоит не более чем из $2p+3q$ простейших подсхем и удовлетворяет условию $\lambda_2(S_1) \leqslant \log b_{11} + 3p + 4q$.

Переходя к описанию подсхемы S_2, обозначим матрицу

$$\begin{pmatrix} b_{22}-b'_{22} & b_{23}-b'_{23} & \dots & b_{2q}-b'_{2q} \\ b_{32}-b'_{32} & b_{33}-b'_{33} & \dots & b_{3q}-b'_{3q} \\ \dots & \dots & \dots & \dots \\ b_{p2}-b'_{p2} & b_{p3}-b'_{p3} & \dots & b_{pq}-b'_{pq} \end{pmatrix}$$

размера $(p-1)\times(q-1)$ через $\widetilde{B}$. По предположению индукции для системы функций, заданной матрицей B, можно построить вычисляющую эту систему обобщенную λ_2-схему S_2, состоящую не более чем из $2(p+q-2)^2$ простейших подсхем и удовлетворяющую соотношению

$$\lambda(S_2) \leqslant \log D\left(\widetilde{B}\right) + 3(p+q)^2.$$

Пусть число s и наборы индексов $i_1, i_2, \ldots, i_s$ и $j_1, j_2, \ldots, j_s$, удовлетворяющие условиям $1 \leqslant s \leqslant \min(p, q) - 1$, $2 \leqslant i_1 < i_2 < \ldots < i_s \leqslant p$, $2 \leqslant j_1 < j_2 < \ldots < j_s \leqslant q$, выбраны таким образом, чтобы выполнялось равенство

$$D\left(\widetilde{B}\right) = \left|\det \begin{pmatrix} b_{i_1,j_1} - b'_{i_1,j_1} & b_{i_1,j_2} - b'_{i_1,j_2} & \ldots & b_{i_1,j_s} - b'_{i_1,j_s} \\ b_{i_2,j_1} - b'_{i_2,j_1} & b_{i_2,j_2} - b'_{i_2,j_2} & \ldots & b_{i_2,j_s} - b'_{i_2,j_s} \\ \ldots & \ldots & \ldots & \ldots \\ b_{i_s,j_1} - b'_{i_s,j_1} & b_{i_s,j_2} - b'_{i_s,j_2} & \ldots & b_{i_s,j_s} - b'_{i_s,j_s} \end{pmatrix}\right|.$$

Обозначим через B_j, $j = 1, j_1, j_2, \ldots, j_s$, вектор-столбец

$$\left(b_{i_1,j}, b_{i_2,j}, \ldots, b_{i_s,j}\right)^T$$

высоты s. Тогда

$$\det \widetilde{B} = \det \begin{pmatrix} b_{i_1,j_1} - b_{i_1,1}\frac{b_{1,j_1}}{b_{11}} & b_{i_1,j_2} - b_{i_1,1}\frac{b_{1,j_2}}{b_{11}} & \ldots & b_{i_1,j_s} - b_{i_1,1}\frac{b_{1,j_s}}{b_{11}} \\ b_{i_2,j_1} - b_{i_2,1}\frac{b_{1,j_1}}{b_{11}} & b_{i_2,j_2} - b_{i_2,1}\frac{b_{1,j_2}}{b_{11}} & \ldots & b_{i_2,j_s} - b_{i_2,1}\frac{b_{1,j_s}}{b_{11}} \\ \ldots & \ldots & \ldots & \ldots \\ b_{i_s,j_1} - b_{i_s,1}\frac{b_{1,j_1}}{b_{11}} & b_{i_s,j_2} - b_{i_s,1}\frac{b_{1,j_2}}{b_{11}} & \ldots & b_{i_s,j_s} - b_{i_s,1}\frac{b_{1,j_s}}{b_{11}} \end{pmatrix} =$$

$$= \det\left(B_{j_1} - \frac{b_{1,j_1}}{b_{11}}B_1, B_{j_2} - \frac{b_{1,j_2}}{b_{11}}B_1, \ldots, B_{j_s} - \frac{b_{1,j_s}}{b_{11}}B_1\right) =$$

$$= \det\left(B_{j_1}, B_{j_2}, \ldots, B_{j_s}\right) - \det\left(\frac{b_{1,j_1}}{b_{11}}B_1, B_{j_2}, \ldots, B_{j_s}\right) -$$

$$- \det\left(B_{j_1}, \frac{b_{1,j_2}}{b_{11}}B_1, B_{j_3}, \ldots, B_{j_s}\right) - \ldots - \det\left(B_{j_1}, B_{j_2}, \ldots, B_{j_{s-1}}, \frac{b_{1,j_s}}{b_{11}}B_1\right) =$$

$$= \frac{1}{b_{11}}\Big(b_{11}\det\left(B_{j_1}, B_{j_2}, \ldots, B_{j_s}\right) - b_{1,j_1}\det\left(B_1, B_{j_2}, \ldots, B_{j_s}\right) +$$

$$+ b_{1,j_2}\det\left(B_1, B_{j_1}, B_{j_3}, \ldots, B_{j_s}\right) - \ldots (-1)^s b_{1,j_s}\det\left(B_1, B_{j_1}, \ldots, B_{j_{s-1}}\right)\Big).$$

С другой стороны, используя формулу разложения определителя по первой строке, получаем:

$$\det \begin{pmatrix} b_{1,1} & b_{1,j_1} & b_{1,j_2} & \ldots & b_{1,j_s} \\ b_{i_1,1} & b_{i_1,j_1} & b_{i_1,j_2} & \ldots & b_{i_1,j_s} \\ b_{i_2,1} & b_{i_2,j_1} & b_{i_2,j_2} & \ldots & b_{i_2,j_s} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ b_{i_s,1} & b_{i_s,j_1} & b_{i_s,j_2} & \ldots & b_{i_s,j_s} \end{pmatrix} = b_{11}\det\left(B_{j_1}, B_{j_2}, \ldots, B_{j_s}\right) -$$

$$- b_{1,j_1}\det\left(B_1, B_{j_2}, \ldots, B_{j_s}\right) + b_{1,j_2}\det\left(B_1, B_{j_1}, B_{j_3}, \ldots, B_{j_s}\right) - \ldots$$

$$\ldots + (-1)^s b_{1,j_s}\det\left(B_1, B_{j_1}, \ldots, B_{j_{s-1}}\right).$$

Следовательно,

$$D\left(\widetilde{B}\right) = \frac{1}{b_{11}}\left|\det \begin{pmatrix} b_{1,1} & b_{1,j_1} & b_{1,j_2} & \ldots & b_{1,j_s} \\ b_{i_1,1} & b_{i_1,j_1} & b_{i_1,j_2} & \ldots & b_{i_1,j_s} \\ b_{i_2,1} & b_{i_2,j_1} & b_{i_2,j_2} & \ldots & b_{i_2,j_s} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ b_{i_s,1} & b_{i_s,j_1} & b_{i_s,j_2} & \ldots & b_{i_s,j_s} \end{pmatrix}\right| \leqslant \frac{D(B)}{b_{11}} = \frac{D(A)}{b_{11}}.$$

Окончательно имеем: схема S состоит не более чем из

$$(2p+3q)+2(p+q-2)^2+(p-1)+(p+q)\leqslant 2(p+q)^2$$

простейших схем, причем справедливы соотношения

$$\lambda_2(S)\leqslant(\log b_{11}+3p+4q)+\left(\log\left(\frac{D(A)}{b_{11}}\right)+3(p+q-2)^2\right)+$$
$$+(p-1)+2(p+q)\leqslant\log D(A)+3(p+q)^2.$$

Лемма 21 доказана.

Таким образом завершено и доказательство верхней оценки (в ослабленной форме) теоремы 34.

6.3. Схемы из делений. В этом параграфе пока исследовалась задача, получающаяся из задачи Пиппенджера посредством увеличения возможностей построения схем: помимо операции умножения (сложения), стала доступна для использования и операция деления (вычитания). А что будет, если разрешить использование только операции деления (вычитания)?

Пусть $A=(a_{ij})$ — целочисленная матрица размера $p\times q$. Обозначим через $l_{\{-\}}(z_1,z_2,\ldots,z_p)$ или $l_{\{-\}}(A)$ минимальное количество операций деления, достаточное для вычисления системы функций

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

В первом параграфе при обсуждении обобщений задачи об эффективном возведении в степень (п. 1.2) уже упоминалось, что при $n\to\infty$ справедливо асимптотическое равенство

$$l_{\{-\}}(n)\sim\log_\varphi n,$$

где $\varphi=\dfrac{\sqrt{5}+1}{2}$, т. е. возведение в степень с использованием только операции деления асимптотически в $\log_\varphi 2$ раз менее эффективно, чем возведение в степень с использованием операции умножения или с использованием двух операций — умножения и деления.

В 2009 г. в работе [51] установлено, что соотношение сложности систем функций, задаваемых целочисленными матрицами размера $p\times q$, при вычислениях с использованием только операции деления и при вычислениях с использованием операций и умножения, и деления остается асимптотически равным $\log_\varphi 2$ для любых фиксированных и даже слаборастущих значениях параметров p и q.

Т е о р е м а 35 [51]. *Пусть последовательность целочисленных матриц $A(n)=\big(a_{ij}(n)\big)_{p(n)\times q(n)}$ при $n\to\infty$ удовлетворяет условию*

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

Тогда

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

Нижняя оценка теоремы 35 устанавливается аналогично универсальной нижней оценке из теоремы 26. Изменение, по существу, только одно —

доказательство опирается не на лемму 10, а на тот факт, что любая схема, состоящая из l элементов деления и вычисляющая матрицу A, удовлетворяет неравенству $|\det A| \geqslant F_l$, где F_l — l-й элемент последовательности Фибоначчи, определяемой начальными условиями $F_1 = F_2 = 1$ и рекуррентным соотношением $F_n = F_{n-1} + F_{n-2}$. Впрочем, сам этот факт устанавливается так же, как и лемма 10.

Верхнюю оценку, асимптотически совпадающую с нижней, можно получить из доказательства верхней оценки теоремы 34, заменив в доказательстве леммы 21 все обобщенные λ_2-подсхемы, возводящие подаваемую на вход функцию в степень, и имеющую λ_2-сложность $\lceil \log k \rceil$, где k — показатель степени, на обобщенные λ_2-подсхемы, не содержащие элементов умножения и имеющие сложность $\log_\varphi k + O(1)$.

Итак, вычисления с использованием двух операций, умножения и деления, асимптотически в $\log_\varphi 2$ раз эффективнее вычислений с использованием только операции деления. А вот при сравнении эффективности вычислений с использованием одной операции — только умножения и только деления — был обнаружен удивительный эффект: в отдельных случаях операция деления оказывается более эффективной.

Пусть показатели степеней переменных системы $\Sigma(t, n)$ из $2t$ одночленов от $2t$ переменных задаются матрицей $A(t, n)$ (подробнее см. п. 5.6) размера $2t \times 2t$: 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.

В силу теоремы 35 минимальное число делений, достаточное для вычисления системы $\Sigma(t, n)$, при фиксированном t асимптотически равно $\log_\varphi D(A(t, n)) = (t + 1) \log_\varphi n$, а теорема 31 утверждает, что минимальное число операций умножения, достаточное для вычисления этой же системы одночленов, асимптотически равно $2t \log_2 n$. Учитывая, что $\log_2 \left(\frac{\sqrt{5}+1}{2} \right) \approx 0,694242\ldots$, при $t \geqslant 3$ и достаточно больших n для вычисления системы $\Sigma(t, n)$ более эффективной операцией является деление, а не умножение.

§ 7. Вычисление элементов свободной абелевой группы

В предшествующем параграфе рассматривалась задача, получающаяся из задачи Пиппенджера путем расширения вычислительных возможностей за счет добавления к операции умножения операции деления. При этом вычислительная сила модели увеличилась: в отличие от классической модели схем умножения для схем умножения-деления для любых фиксированных размеров матрицы показателей степеней, задающих систему одночленов, справедлива верхняя оценка сложности вычисления этой системы, асимптотически совпадающая с универсальной нижней оценкой из теоремы 26. В этом параграфе рассмотрим промежуточную вычислительную модель, в которой операция деления недоступна, но в которой, помимо переменных $x_1, \ldots, x_q$, можно использовать величины $x_1^{-1}, \ldots, x_q^{-1}$, обратные к переменным. О вычислениях в этой модели будем говорить как о вычислениях 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

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

определяется целочисленной матрицей $A = (a_{ij})$ размера $p \times q$. Обозначим через $l_F(f_1, f_2, \ldots, f_p)$ (будем также использовать обозначение $l_F(A)$) 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 $l_F(A)$ может быть определена также на языке аддитивных цепочек. *Аддитивной F-цепочкой* (см., например, [47, 49]) для целочисленной матрицы $A = (a_{ij})$ размера $p \times q$ назовем последовательность q-мерных векторов (наборов) вида

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

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

1) для каждого k, $2q + 1 \leqslant k \leqslant 2q + r$, найдется два натуральных числа (не обязательно различных) i и j, $1 \leqslant i \leqslant k - 1$, $1 \leqslant j \leqslant k - 1$, таких, что $\boldsymbol{v}_k = \boldsymbol{v}_i + \boldsymbol{v}_j$ (сложение векторов покомпонентное);

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

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

Величину $l_F(g_1, g_2, \ldots, g_p)$ (или $l_F(A)$) 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 $p \times q$; а 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 [47].

Отметим, что соображения двойственности для l_F-сложности не работают, по крайней мере, в той степени, в какой они работают для классической модели схем умножения и для модели, допускающей использование и операции умножения, и операции деления. Действительно,

$$l_F\left(\left(2^k, -2^k\right)\right) = k + 1, \quad l_F\left(\left(2^k, -2^k\right)^T\right) = 2k.$$

7.1. Функция Шеннона сложности систем элементов свободной абелевой группы. Определим *функцию Шеннона* $L_F(p,q,K)$ *сложности вычисления систем элементов свободной абелевой группы*, положив

$$L_F(p,q,K)=\max l_F(A),$$

где максимум берется по всем целочисленным матрицам $A=(a_{ij})$ размера $p\times q$, удовлетворяющим условиям $|a_{ij}|\leqslant K-1$, $i=1,\ldots,p$, $j=1,\ldots,q$. 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 все показатели степени не превосходят по абсолютной величине значения $K-1$.

Т е о р е м а 36. *Пусть* $pq\log K\to\infty$. *Тогда*

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

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

Верхняя оценка теоремы 36 установлена в [47].

Нижняя оценка

$$L_F(p,q,K)\geqslant \min(p,\ q+1)\log(K-1)$$

при $p\leqslant q$ (и, следовательно, при $\min(p,\ q+1)=p$) следует из неравенства $l_F(x_1^n,x_2^n,\ldots,x_p^n)\geqslant p\log n$, а при $p>q$ справедливо равенство $\min(p,\ q+1)=q+1$, и нужная оценка вытекает из соотношения

$$l_F\left(x_1^n,\ldots,x_{q-1}^n,x_q^n,x_q^{-n}\right)\geqslant (q+1)\log n.$$

Из стандартных мощностных рассуждений (см., например, теорему Д.1 из [71]) несложно выводится неравенство

$$L_F(p,q,K)+p+q-\frac{pq\log(2K-1)}{\log(pq\log(2K-1))}\geqslant \frac{\log\log(pq\log(2K-1))}{\left(\log(pq\log(2K-1))\right)^2}(1+o(1)).$$

С учетом соотношения

$$\frac{pq\log(2K-1)}{\log(pq\log K)}-\frac{pq\log(2K-1)}{\log(pq\log(2K-1))}=O\left(\frac{pq\log(2K-1)}{\log(pq\log K)}\right),$$

объединяя оба неравенства в одно, получаем нижнюю оценку

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

которая в случае разных порядков роста величин $\min(p,\ q+1)\log K$ и $\frac{pq\log(2K-1)}{\log(pq\log K)}$ приносит требуемый результат.

Объединение двух нижних оценок в одну, равную сумме оценок, проводится аналогично нижней оценке теоремы 25.

7.2. Сложность систем элементов свободной абелевой группы в случае малых размеров матрицы. Сначала сформулируем результаты о сложности вычисления систем элементов свободных абелевых групп в самых простых случаях — когда матрицы, задающие показатели степеней, имеют размеры $1\times q$, $p\times 1$, $2\times q$. При этом для последних двух типов матриц при получении асимптотики роста их F-сложности возникает новый эффект.

Еще более нетривиальная ситуация возникает в случае матриц размера 3×2, для которого также установлен асимптотический рост F-сложности.

В случае вычисления одного элемента свободной абелевой группы все достаточно просто: для произвольной последовательности целочисленных наборов $\bigl(a_1(n), a_2(n), \ldots, a_{q(n)}(n)\bigr)$, удовлетворяющей условию

$$\frac{q(n)}{\log\log \max\limits_i |a_i(n)|}\to 0$$

при $n\to\infty$, справедливо асимптотическое равенство

$$l_F(x_1^{a_1}x_2^{a_2}\ldots x_q^{a_q})\sim \log\max|a_i|.$$

Для того, чтобы оценить сверху величину $l_F(x^{a_1}, x^{a_2}, \ldots, x^{a_p})$ в силу неравенства

$$l_F(x^{a_1}, x^{a_2}, \ldots, x^{a_p})\leqslant l\left(\{x^{a_i}\mid a_i>0\}\right)+l\left(\{x^{|a_i|}\mid a_i<0\}\right)+1,$$

достаточно воспользоваться теоремой 6 — при выполнении условия $p=o\bigl(\log\log\bigl(\max|a_i|\bigr)\bigr)$ имеет место асимптотическое неравенство

$$l_F(x^{a_1}, x^{a_2}, \ldots, x^{a_p})\leqslant \log\max\{1, a_1, a_2, \ldots, a_p\}+ \\ +\log\max\{1, -a_1, -a_2, \ldots, -a_p\}+o(\log\max|a_i|).$$

Чтобы оценить снизу $l_F(x^{a_1}, x^{a_2}, \ldots, x^{a_p})$, введем одну величину, а также докажем вспомогательную лемму.

Для произвольной матрицы A размера $p\times q$ определим величину $T(A)$ равенством

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

Таким образом, $T(A)$ — это максимум абсолютных величин попарных произведений элементов матрицы A, где максимум берется по всем парам элементов, удовлетворяющих двум условиям: эти элементы должны находиться в одном столбце и иметь разные знаки (если таких пар нет, то $T(A)=0$).

Лемма 22. *Для любой целочисленной матрицы A справедливо неравенство*

$$l_F(A)\geqslant \log\max\{T(A), 1\}.$$

Доказательство. Без ограничения общности будем считать, что $T(A)=|a_{11}a_{21}|$, причем $a_{11}\geqslant 1$, $a_{21}\leqslant -1$. Рассмотрим схему S со входами $x_1, x_1^{-1}, x_2, x_2^{-1}\ldots, x_q, x_q^{-1}$, вычисляющую матрицу A и удовлетворяющую

условию $l_F(S)=l_F(A)$. Преобразуем схему S в схему S' следующим образом. Входу, которому был приписан символ x_1, припишем символ новой переменной u, а входу которому был приписан символ x_1^{-1}, — символ новой переменной v. Тогда в вершинах, соответствующих в исходной схеме первым двум строкам матрицы A, будут вычисляться функции вида $u^{a_{11}+\alpha_1}v^{\alpha_1}x_2^{a_1 2}\dots x_q^{a_1 q}$ и $u^{\alpha_2}v^{|a_{21}|+\alpha_2}x_2^{a_2 2}\dots x_q^{a_2 q}$, где α_1 и α_2 — некоторые неотрицательные целые числа. Поэтому, применяя лемму 10, имеем:

$$l_F(A)=l_F(S)=l_F(S')\geqslant\log\left|\det\begin{pmatrix}a_{11}+\alpha_1 & \alpha_1\\ \alpha_2 & |a_{21}|+\alpha_2\end{pmatrix}\right|\geqslant$$
$$\geqslant\log|a_{11}a_{21}|=\log T(A).$$

Лемма 22 доказана.

Суммируя вышесказанное, с использованием леммы 22 получаем следующее утверждение

Т е о р е м а 37. *Для произвольной последовательности целочисленных наборов* $\left(a_1(n),a_2(n),\dots,a_{p(n)}(n)\right)$, *удовлетворяющей условию*

$$\frac{p(n)}{\log\log\max\limits_i|a_i(n)|}\to 0$$

при $n\to\infty$, *справедливо асимптотическое равенство*

$$l_F(x^{a_1},x^{a_2},\dots,x^{a_p})\sim\log\max\left\{|a_1|,|a_2|,\dots,|a_p|,T\left((a_1,a_2,\dots,a_p)^T\right)\right\}.$$

Перейдем теперь к случаю матриц размера $2\times q$.

Л е м м а 23. *Пусть в целочисленной матрице* $A=(a_{ij})$ *размера* $p\times q$ *для элемента* a_{ij} *найдется индекс* s, $1\leqslant s\leqslant p$, *такой, что выполняется условие* $a_{ij}a_{sj}\leqslant 0$. *Тогда для любого* t, $1\leqslant t\leqslant q$, *справедливо неравенство*

$$\max\{|a_{ij}a_{st}|,|a_{it}a_{sj}|\}\leqslant 2\max\{D(A),T(A)\}.$$

Д о к а з а т е л ь с т в о. При выполнении условия $a_{ij}a_{st}a_{it}a_{sj}\leqslant 0$ справедливы соотношения

$$\max\{|a_{ij}a_{st}|,|a_{it}a_{sj}|\}\leqslant|a_{ij}a_{st}|+|a_{it}a_{sj}|=|a_{ij}a_{st}-a_{it}a_{sj}|\leqslant D(A).$$

Пусть теперь выполняется неравенство $a_{ij}a_{st}a_{it}a_{sj}>0$. Без ограничения общности будем считать, что

$$|a_{ij}a_{st}|\geqslant|a_{it}a_{sj}|.$$

Тогда при $|a_{ij}a_{st}|\geqslant 2|a_{it}a_{sj}|$ верны соотношения

$$|a_{it}a_{sj}|\leqslant|a_{ij}a_{st}|\leqslant 2|a_{it}a_{sj}-a_{ij}a_{st}|\leqslant 2D(A).$$

Если же выполняется условие $|a_{ij}a_{st}|<2|a_{it}a_{sj}|$, то справедливо хотя бы одно из неравенств: $|a_{ij}|\leqslant 2|a_{it}|$ или $|a_{st}|\leqslant 2|a_{sj}|$. Тогда при выполнении первого неравенства имеем:

$$|a_{it}a_{sj}|\leqslant|a_{ij}a_{st}|\leqslant 2|a_{it}a_{st}|\leqslant 2T(A),$$

а при выполнении второго получаем:

$$|a_{it}a_{sj}| \leqslant |a_{ij}a_{st}| \leqslant 2|a_{ij}a_{sj}| \leqslant 2T(A).$$

Лемма 23 доказана.

Л е м м а 24. *Пусть последовательность* $A(n) = \big(a_{ij}(n)\big)$ *ненулевых целочисленных матриц размера* $q(n)\times 2$ *удовлетворяет условию*

$$\max_{a_{ij}\in A(n)} |a_{ij}| \to \infty \quad \textit{при} \quad n \to \infty.$$

Тогда справедлива следующая верхняя оценка:

$$l_F(A(n)) \leqslant \log \max\{D(A(n)), T(A(n))\} + O\left(\frac{q(n)\log \max\{|a_{ij}| \mid a_{ij}\in A(n)\}}{\log\log \max\{|a_{ij}| \mid a_{ij}\in A(n)\}}\right).$$

Д о к а з а т е л ь с т в о. По целочисленной матрице $A = A(n)$ размера $2\times q$ определим целочисленную матрицу B с неотрицательными элементами, последовательно преобразуя столбцы исходной матрицы следующим образом.

1. Если в столбце $\begin{pmatrix} a_{1i} \\ a_{2i} \end{pmatrix}$ элементы имеют один знак, т. е. $a_{1i}a_{2i} \geqslant 0$, то включаем в матрицу B вместо этого столбца столбец $\begin{pmatrix} |a_{1i}| \\ |a_{2i}| \end{pmatrix}$.

2. Если в столбце $\begin{pmatrix} a_{1i} \\ a_{2i} \end{pmatrix}$ элементы имеют разные знаки, т. е. $a_{1i}a_{2i} < 0$, то включаем в матрицу B вместо этого столбца матрицу $\begin{pmatrix} |a_{1i}| & 0 \\ 0 & |a_{2i}| \end{pmatrix}$.

Таким образом, B — целочисленная матрица с неотрицательными элементами размера $2\times r$, где r удовлетворяет условию $q \leqslant r \leqslant 2q$.

В силу определения матрицы B имеем:

$$l_F(A) = l_F(x_1^{a_{11}}x_2^{a_{12}}\dots x_q^{a_{1q}},\ x_1^{a_{21}}x_2^{a_{22}}\dots x_q^{a_{2q}}) \leqslant \\ \leqslant l(z_1^{b_{11}}z_2^{b_{12}}\dots z_r^{b_{1r}},\ z_1^{b_{21}}z_2^{b_{22}}\dots z_r^{b_{2r}}).$$

Далее, применяя теоремы 28 и 4, получаем:

$$l(z_1^{b_{11}}z_2^{b_{12}}\dots z_r^{b_{1r}},\ z_1^{b_{21}}z_2^{b_{22}}\dots z_r^{b_{2r}}) \leqslant \log D(B) + O\left(r\frac{\log \max b_{ij}}{\log\log \max b_{ij}}\right) = \\ = \log D(B) + O\left(q\frac{\log \max |a_{ij}|}{\log\log \max |a_{ij}|}\right).$$

Покажем, что $D(B) \leqslant 2\max\{D(A), T(A)\}$. Действительно, если $D(B) = b_{ij}$, для некоторых i и j, $1 \leqslant i \leqslant 2$, $1 \leqslant j \leqslant r$, то справедливо неравенство $D(B) \leqslant D(A)$.

Пусть теперь для некоторых j и t, $1 \leqslant j < t \leqslant r$ выполняется условие

$$D(B) = |b_{1j}b_{2t} - b_{1t}b_{2j}|.$$

Тогда в случае $b_{1j}b_{2t}b_{1t}b_{2j} \neq 0$ для некоторых j' и t', $1 \leqslant j', t' \leqslant q$, справедливо равенство

$$a_{1j'}a_{2t'} - a_{1t'}a_{2j'} = b_{1j}b_{2t} - b_{1t}b_{2j}$$

и, следовательно, $D(B) \leqslant D(A)$.

Рассмотрим случай выполнения условия $b_{1j}b_{2t}b_{1t}b_{2j} = 0$. Без ограничения общности будем считать, что $b_{1j} = 0$. Тогда, с одной стороны, справедливо равенство $D(B) = |b_{1t}b_{2j}|$, а с другой — найдутся j' и t', $1 \leqslant j', t' \leqslant q$, для которых выполняются условия:

$$|a_{2j'}| = b_{2j}, \quad a_{1j'}a_{2j'} \leqslant 0; \quad |a_{1t'}| = b_{1t}.$$

Поэтому, применяя лемму 23, получаем:

$$D(B) = |b_{1t}b_{2j}| = |a_{1t'}a_{2j'}| \leqslant 2\max\{D(A), T(A)\}.$$

Таким образом окончательно имеем:

$$l_F(A) \leqslant \log\max\{D(A), T(A)\} + O\left(q\frac{\log\max|a_{ij}|}{\log\log\max|a_{ij}|}\right).$$

Лемма 24 доказана.

В силу теоремы 26 и лемм 22 и 24 справедлива

Т е о р е м а 38 [45]. *Для произвольной последовательности целочисленных матриц $A(n) = \big(a_{ij}(n)\big)$ размера $2 \times q(n)$, удовлетворяющей условию*

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

при $n \to \infty$, справедливо асимптотическое равенство

$$l_F(A(n)) \sim \log\max\{D(A(n)), T(A(n))\}.$$

Еще одним подтверждением отсутствия двойственности в задаче вычисления элементов свободной абелевой группы является сравнение оценок сложности вычисления двух элементов в группе с тремя порождающими и трех элементов в группе с двумя порождающими. Во втором случае для формулировки результата об асимптотике роста сложности требуется введение дополнительного параметра.

Пусть матрица A имеет размеры 3×2. Для удобства под записью 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 назовем *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

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

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

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

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

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

Т е о р е м а 39 [49]. *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

$$l_F(A(n)) \sim \log \max\{D(A(n)), T(A(n)), R(A(n))\}.$$

Доказательство этой теоремы технически очень тяжелое и достаточно длинное, в работе [49] оно занимает более 30 страниц. Здесь это доказательство не приводится, однако представляется естественным отметить одно соображение, на которое во многом опирается доказательство как верхней, так и нижней оценки теоремы 39 и которое уже в некотором виде использовалось при доказательстве леммы 22. Несколько подробнее опишем это соображение.

Пусть схема S из элементов умножения со входами, которым приписаны величины $x_1, x_1^{-1}, \ldots, x_q, x_q^{-1}$, реализует матрицу A, причем выполняется равенство $l_F(S) = l_F(A)$. На выходах этой схемы будут реализованы функции $g_i = x_1^{a_{i1}} \ldots x_q^{a_{iq}}$, $i = 1, \ldots, p$. Преобразуем схему S в схему S' следующим образом. Выберем параметр k, $1 \leqslant k \leqslant q$. Для каждого $j = k, \ldots, q$ входу, которому был приписан символ x_j, припишем символ новой переменной u_j, а входу которому был приписан символ x_j^{-1} — символ новой переменной v_j. Полученная схема S' будет реализовывать функции h_i, $i = 1, \ldots, p$, которые будут получаться из функций g_i заменой каждой из величин $x_j^{a_{ij}}$,

$j = k, \ldots, q$, на произведение $u_j^{a_{ij}+b_{ij}} v_j^{b_{ij}}$ при $a_{ij} \geqslant 0$ или на произведение $u_j^{b_{ij}} v_j^{a_{ij}+b_{ij}}$ при $a_{ij} \leqslant 0$ для некоторого неотрицательного целого b_{ij}. Так как число элементов в схеме S' такое же, как и в схеме S, то оценки количества элементов в схеме S' (в частности, универсальная нижняя оценка) являются и оценками величины $l_F(A)$.

В заключение остановимся на сравнении величин $l(A)$, $l_2(A)$ и $l_F(A)$ при ограниченных размерах $p \times q$ матрицы A.

Если матрица A — произвольная целочисленная, то сравнивать можно только величины $l_2(A)$ и $l_F(A)$. Очевидно, что

$$l_2(A) \leqslant l_F(A) + q + 1.$$

При этом из теорем 34, 38 и 39 следует, что величина $l_F(A)$ может быть значительно больше величины $l_2(A)$, асимптотически равной $\log D(A)$ при любых фиксированных p и q.

Для целочисленных неотрицательных матриц, помимо неравенства $l_2(A) \leqslant l_F(A) + q + 1$, выполняются очевидные неравенства

$$l_2(A) \leqslant l(A), \quad l_F(A) \leqslant l(A).$$

Теорема 34 и следствие 4 дают пример последовательности матриц, для которых сложность в классической модели схем умножения асимптотически вдвое превышает их сложность в модели схем умножения и деления. При этом асимптотика роста l_F-сложности матриц этой последовательности совпадает с асимптотикой роста их l_2-сложности. Более того, представляется правдоподобным следующее утверждение.

Гипотеза. *Для любой последовательности A_n целочисленных неотрицательных матриц ограниченного размера, удовлетворяющей при $n \to \infty$ условию $D(A_n) \to \infty$, справедливо соотношение*

$$l_F(A_n) \sim \log D(A_n).$$

§ 8. Вентильные схемы

Рассматриваемые в работе вычислительные схемы относятся к одному из важнейших модельных классов управляющих систем — классу схем из функциональных элементов. При этом изучаемые схемы обладают также многими свойствами, присущими вентильным схемам — классу наиболее простых управляющих систем, несущему большую топологическую нагрузку и удобному для разработки общих методов синтеза, которые, как правило, в той или иной степени могут быть промоделированы в других классах управляющих систем. Кроме того, уже в самом начале настоящей работы, а именно при обсуждении двойственности задачи Пиппенджера в § 1 (теорема 4) и в доказательстве верхней оценки для задачи Беллмана — Кнута в § 2 (лемма 2) если не центральную, то уж, по крайней мере, очень важную роль сыграли вентильные схемы. Вообще, связь между различными вариантами задачи Пиппенджера и вентильными схемами, конечно, не вызывает сомнений. Но на самом деле эта связь даже намного теснее и глубже, чем кажется на первый взгляд, и до конца, по-видимому, еще не изучена.

В этом параграфе дается основанный на работе [55] краткий обзор известных результатов по теории вентильных схем.

Теорию схем можно подразделить по мощности применяемых средств на несколько уровней: теория вентильных схем, теория контактных схем, теория схем из функциональных элементов, теория автоматов с памятью. При этом конструкции одного уровня могут (в той или иной степени) быть промоделированы во всех высших уровнях. Поэтому результаты вентильного уровня, несущего наибольшую топологическую нагрузку, имеют принципиальную — общекибернетическую — значимость.

В литературе по синтезу и сложности управляющих систем под вентильными схемами в зависимости от исследуемых задач могут пониматься несколько разные объекты, которые условно можно разделить на классические вентильные схемы [66, 74, 174], реализующие булевы матрицы, а также на вентильные схемы с кратными путями (или графы с предписанным числом путей) [175] (см. также [52]), реализующие целочисленные неотрицательные матрицы. В последнее время более активно изучается второй вариант вентильных схем, имеющий тесную связь с задачами экономного вычисления систем одночленов (см., например, [177]). Однако результаты из теории классических вентильных схем занимают особое место в теории сложности. Кроме того, они и сейчас находят применение при решении различных задач (см., например, [12, 110, 152]). В частности, в основе асимптотически точной верхней оценки сложности для задачи Беллмана — Кнута лежит как раз технически тяжелый результат из леммы 1 относительно сложности реализации булевых матриц ступенчатого вида классическими вентильными схемами специального типа. Кроме того, методы исследований для случая реализации булевых матриц и случая реализации целочисленных неотрицательных матриц достаточно близки. Поэтому в этом параграфе, кроме описания последних достижений в задаче о сложности реализации целочисленных неотрицательных матриц вентильными схемами, дается обзор результатов по теории классических вентильных схем. Этот обзор касательно результатов, полученных до середины 70-х годов прошлого века, опирается на обзор О. Б. Лупанова [74]. Обозначения, используемые в данном параграфе, также в целом соответствуют [74] и формально (но не по сути) отличаются от используемых в первых двух параграфах. В определениях также есть несколько мелких непринципиальных отличий.

Прежде чем переходить к формулировкам известных результатов в этой области, нужно отметить работу [152], в которой также содержится обзор результатов по теории вентильных схем, но с несколько других позиций.

8.1. Классические вентильные схемы. Напомним определение классической вентильной схемы [66] или, более точно, классическое определение вентильной схемы.

В наиболее общем (для классического случая) виде *вентильная схема* определяется [74] как ориентированный граф, в котором выделено некоторое множество вершин — множество полюсов, — и эти вершины занумерованы. С каждой вентильной схемой S связывается матрица из нулей и единиц $A=(a_{ij})$ — *матрица проводимостей* ($a_{ij}=1$ тогда и только тогда, когда в схеме S имеется ориентированный путь из полюса с номером i в полюс с номером j). Очевидно, что матрица проводимостей любой вентильной схемы является транзитивной.

Важным классом вентильных схем [66, 85, 89] являются такие, в которых полюса разбиты на два подмножества: «входные» — с номерами $P=\{1,2,\ldots,p\}$ и «выходные» — с номерами $Q=\{p+1,p+2,\ldots,p+q\}$, и на матрицу проводимостей наложено дополнительное ограничение: $a_{ij}=0$, если $i\neq j$ и либо $i\in P$, $j\in P$, либо $i\in Q$, $j\in Q$, либо $i\in Q$, $j\in P$. В этом случае система проводимостей полностью определяется подматрицей данной матрицы, имеющей p строк и q столбцов; ее обычно и называют матрицей проводимостей.

Заметим, что без ограничения общности можно считать, что в вентильной схеме нет ориентированных циклов (без изменения матрицы проводимостей этот ориентированный цикл можно заменить на одну вершину).

Теперь дадим эквивалентное определение вентильной схемы, которое и будем, как правило, использовать в дальнейшем.

Пусть $A=(a_{ij})$ — булева (двоичная) матрица размера $p\times q$. *Вентильной схемой, реализующей матрицу* A, называется ориентированный граф S без ориентированных циклов, в котором:

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

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

3) для любой пары (i,j), $1\leqslant i\leqslant p$, $1\leqslant j\leqslant q$, ориентированный путь от i-го входа к j-му выходу существует тогда и только тогда, когда $a_{ij}=1$.

Через $L_{BC}(S)$ будем обозначать *сложность вентильной схемы* S, т. е. число ребер (вентилей) схемы S (в литературе по вентильным схемам сложность также иногда обозначается буквами B и C). *Сложность* $L_{BC}(A)$ *реализации булевой матрицы* A *вентильными схемами* определяется следующим образом: $L_{BC}(A)=\min L_{BC}(S)$, где минимум берется по всем вентильным схемам, реализующим матрицу A. Функция Шеннона $L_{BC}(p,q)$ сложности реализации булевых матриц вентильными схемами вводится стандартным образом как минимальное число вентилей, достаточное для реализации любой булевой матрицы с p строками и q столбцами, т. е. $L_{BC}(p,q)=\max L_{BC}(A)$, где максимум берется по всем булевым матрицам размера $p\times q$.

Аналогичным образом определяется и функция Шеннона $L^{(r)}_{BC}(p,q)$ сложности реализации булевых матриц вентильными схемами глубины r (*глубина схемы* — максимальное число вентилей в цепях от входа к выходу).

Во множестве всех вентильных схем выделим важный для приложений специальный класс — вентильные схемы, в которых число путей от произвольного входа до произвольного выхода равно либо 0, либо 1 (см., например, [174]).

Пусть $A=(a_{ij})$ — булева (двоичная) матрица размера $p\times q$. Ориентированный граф (без петель и кратных ребер) S будем называть 0-1-*вентильной схемой, реализующей матрицу* A, если:

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

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

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

Обозначим через $L_{01}(S)$ *сложность* 0-1-*вентильной схемы* S, т. е. число ребер (вентилей) схемы S. Определим *сложность* $L_{01}(A)$ *реализации булевой матрицы* A 0-1-*вентильными схемами* следующим образом: $L_{01}(A) = \min L_{01}(S)$, где минимум берется по всем 0-1-вентильным схемам, реализующим матрицу A.

Таким образом, определение 0-1-вентильной схемы несколько отличается от классического определения вентильной схемы — в п. 3 определения в случае, когда $a_{ij} = 1$, накладывается более сильное условие: вместо существования пути от i-го входа к j-му выходу требуется существование и единственность такого пути.

Стоит отметить, что в литературе встречается еще один очень важный вариант вентильных схем, реализующих булевы матрицы, в рамках которого предполагается, что число ориентированных путей от i-го входа к j-му выходу должно быть четным, если $a_{ij} = 0$, и нечетным, если $a_{ij} = 1$. Этот вариант соответствует линейным булевым операторам (см., например, [19, 145] и в настоящем обзоре практически не затрагивается, но подробно изучается в монографии [152]. В [152] также подведен предварительный итог исследованиям экстремальных значений соотношений сложности для различных вариантов вентильных схем как без ограничений, так и с ограничениями на глубину.

Возвращаясь к классическим и 0-1-вентильным схемам, заметим, что все введенные меры сложности булевых матриц обладают свойством двойственности, т. е. сложность исходной матрицы и транспонированной к ней совпадают — для построения схемы, реализующей транспонированную матрицу, достаточно в исходной схеме поменять направления всех вентилей.

Помимо только что поясненных равенств

$$L_{BC}(A) = L_{BC}(A^T), \quad L^{(r)}_{BC}(A) = L^{(r)}_{BC}(A^T), \quad L_{01}(A) = L_{01}(A^T),$$

отметим следующие простые соотношения:

$$L_{BC}(A) \leqslant L_{01}(A), \quad L_{BC}(p, q) \leqslant L_{01}(p, q).$$

Кроме того, для вентильных схем глубины 1 выполняются равенства

$$L^{(1)}_{BC}(A) = \|A\|, \quad L^{(1)}_{BC}(p, q) = pq,$$

где $\|A\|$ означает число единиц в матрице A. Тем самым задача о сложности реализации матриц вентильными схемами глубины 1 является тривиальной. Однако уже для схем глубины 2 задача оказалась значительно более содержательной.

В 1956 г. О. Б. Лупановым [66] предложен асимптотически наилучший (будем считать, что значения p и q являются функциями некоторого натурального параметра n и имеются в виду асимптотические соотношения при $n \to \infty$) метод построения вентильных схем глубины 2, который в дальнейшем лег в основу асимптотически оптимальных методов синтеза «более сильных» классов управляющих систем (контактных схем, схем из функциональных элементов, автоматов и т. д.; см., например, [70, 75]):

Т е о р е м а 40 [66]. *Пусть выполнены условия*

а) $p \to \infty$;

б) $p \leqslant q$;

в) $\frac{\log q}{p} \to 0$.

Тогда

$$L_{BC}^{(2)}(p,q) \sim \frac{pq}{\log q}.$$

С л е д с т в и е 5. *В условиях теоремы* 40

$$\frac{pq}{\log(pq)} \lesssim L_{BC}(p,q) \lesssim \frac{pq}{\log q}.$$

С л е д с т в и е 6. *В условиях теоремы* 40

$$\frac{pq}{\log(pq)} \lesssim L_{01}(p,q) \lesssim \frac{pq}{\log q}.$$

С л е д с т в и е 7. *В условиях теоремы* 40 *при дополнительном условии*

$г_0$) $\frac{\log p}{\log q} \to 0$

выполняются соотношения

$$L_{BC}(p,q) \sim L_{01}(p,q) \sim L_{BC}^{(2)}(p,q) \sim \frac{pq}{\log q}.$$

Уточнение оценок для величины $L_{BC}(p,q)$ было получено в 1963 г. Э. И. Нечипоруком [85, 89].

Т е о р е м а 41 [85, 89]. *Пусть выполнены условия а) и б) теоремы* 40, *а также условие*

$г_c$) $\lim \frac{\log p}{\log q} = \frac{\mu}{\mu(\varrho-1)+\varrho}$, *где* μ *и* ϱ *— целые числа, большие нуля.*

Тогда

$$L_{BC}(p,q) \sim L_{01}(p,q) \sim L_{BC}^{(3)}(p,q) \sim \frac{pq}{\log(pq)}.$$

З а м е ч а н и е. Условие $г_c$) включает важный для приложений случай, когда величины p и q имеют одинаковый порядок роста.

Окончательное асимптотически точное решение (при естественном условии, что число полюсов существенно меньше сложности) было получено Н. Пиппенджером [174, 175] в 1976 г.

Т е о р е м а 42 [174, 175]. *Пусть выполнены условия теоремы* 40. *Тогда*

$$L_{BC}(p,q) \sim L_{01}(p,q) \sim \frac{pq}{\log(pq)}.$$

Отметим, что конструкция из верхней оценки теоремы 42 требует растущей глубины вентильной схемы. Вопрос о том, достаточно ли вентильных схем ограниченной глубины для получения асимптотической верхней оценки вида $\frac{pq}{\log(pq)}$, долгое время оставался формально открытым. На эту задачу неоднократно обращал внимание своих учеников О. Б. Лупанов. В 2018 г. И. С. Сергеев, ученик С. Б. Гашкова, являющегося, в свою очередь, учеником О. Б. Лупанова, дал утвердительный ответ на этот вопрос. На самом деле И. С. Сергеев решил [100] более общую задачу и об этом будет сказано ниже.

Т е о р е м а 43 [100]. *Пусть выполнены условия*

а) $p \to \infty$;

б) $p \leqslant q$;

в) $\dfrac{(\log q)^{3/2}}{p} \to 0$.

Тогда

$$L_{BC}(p,q) \sim L_{01}(p,q) \sim L_{BC}^{(3)}(p,q) \sim L_{01}^{(3)}(p,q) \sim \frac{pq}{\log(pq)}.$$

Случай, когда не выполняется условие *в*) из теоремы 40 (т. е. число полюсов сравнимо со сложностью) был исследован В. А. Орловым [94].

Т е о р е м а 44 [94]. *Пусть k — произвольное фиксированное целое число. Тогда*

$$L_{BC}^{(2)}(\lfloor k \log q \rfloor, q) \sim (k+1)q.$$

Т е о р е м а 45 [94]. *Пусть выполнены условия*

а') $q \to \infty$,

в$_\alpha$) $\lim \dfrac{p}{\log q} = \alpha$, *причем* $\alpha > 1$, α *— не целое число.*

Тогда

$$L_{BC}^{(2)}(p,q) \sim \lfloor \alpha + 1 \rfloor q.$$

Т е о р е м а 46 [94]. *Пусть* $q \geqslant p2^{p-1} - p$. *Тогда*

$$L_{BC}^{(2)}(p,q) = p2^{p-1} - p + q.$$

Т е о р е м а 47 [94]. *Пусть выполнено условие а), а также условия*

в$_1$) $\lim \dfrac{p}{\log q} = 1$,

д) $q \geqslant p2^{p-1} - p$.

Тогда

$$L_{BC}^{(2)}(p,q) \sim 2q.$$

Т е о р е м а 48 [94]. *Пусть выполнены условия а) и в$_1$), а также условие*

д$^-$) $q \leqslant 2(2^p - p - 1)$.

Тогда

$$L_{BC}(p,q) \sim L_{BC}^{(2)}(p,q) \sim 2q.$$

Т е о р е м а 49 [94]. *Пусть выполнено условие а), а также условие*

д$^+$) $q \geqslant 2(2^p - p - 1)$.

Тогда

$$L_{BC}(p,q) \sim L_{BC}^{(2)}(p,q) \sim 2 \cdot 2^p + q.$$

Наряду с задачей о реализации произвольных булевых матриц (заданных размеров), исследовались вопросы о сложности реализации матриц из специальных классов.

Положим $L_{BC}^{(r)}(p,q,\alpha) = \max L_{BC}^{(r)}(A)$, где максимум берется по всем булевым матрицам из p строк и q столбцов, имеющих αpq единичных элементов. Введем обозначения

$$\alpha^* = \min(\alpha, 1-\alpha), \quad H(\alpha) = \alpha \log \frac{1}{\alpha} + (1-\alpha) \log \frac{1}{(1-\alpha)}.$$

Э. И. Нечипорук доказал следующие утверждения.

Т е о р е м а 50 [85, 89]. *Пусть выполнено условие б), а также условия*

a_α) $\alpha p \to \infty$;

$e_{\alpha,\varrho}$) $\dfrac{\log q}{\log \frac{1}{\alpha}} \to \varrho$, ϱ — *целое*, $\varrho > 0$;

$ж_{\alpha,\varrho}$) $q\alpha^\varrho \to \infty$.

Тогда

$$L_{BC}^{(2)}(p, q, \alpha) \sim \frac{\alpha pq}{\varrho}.$$

Т е о р е м а 51 [86, 89]. *Пусть выполнены условия а) и б), а также условия*

$в_\alpha$) $H(\alpha)\dfrac{p}{\log q} \to \infty$;

e_∞) $\dfrac{\log q}{\log \frac{1}{\alpha^*}} \to \infty$.

Тогда

$$L_{BC}^{(2)}(p, q, \alpha) \sim H(\alpha)\frac{pq}{\log q}.$$

Т е о р е м а 52 [89]. *Пусть выполнены условия а), $в_\alpha$) и e_∞), а также условие*

$г_1$) $\log p \sim \log q$.

Тогда

$$L_{BC}^{(3)}(p, q, \alpha) \sim H(\alpha)\frac{pq}{\log(pq)}.$$

Важное место в теории вентильных схем занимает тесно связанная, например, с построением самокорректирующихся схем задача о сложности реализации не всюду определенных (недоопределенных) матриц — матриц, элементами которых могут быть не только нули и единицы, но и символы $*$ (символ $*$ соответствует неопределенному элементу). Доопределением не всюду определенной матрицы является полностью определенная матрица, все элементы которой совпадают с соответствующими определенными элементами исходной матрицы. Под сложностью не всюду определенной матрицы понимается минимальная сложность ее доопределений.

Положим $L_{BC}^{(r)}(\gamma; p, q) = \max L_{BC}^{(r)}(A)$, где максимум берется по всем не всюду определенным матрицам из p строк и q столбцов, имеющих γpq определенных элементов и $(1-\gamma)pq$ символов $*$.

Э. И. Нечипорук получил следующий результат.

Т е о р е м а 53 [87, 89]. *Пусть выполнены условия а) и б), а также условия*

$в^\gamma$) $\dfrac{\gamma p}{\log q} \to \infty$;

e^γ) $\dfrac{\log q}{\log \frac{1}{\gamma}} \to \infty$.

Тогда

$$L_{BC}^{(2)}(\gamma; p, q) \sim \gamma\frac{pq}{\log q}.$$

В некотором смысле окончательное (при естественном ограничении, что число полюсов существенно меньше сложности) асимптотически точное решение задачи о сложности реализации не всюду определенных матриц вентильными схемами глубины 2 было предложено А. Е. Андреевым в 1987 г.

Т е о р е м а 54 [3]. *Пусть выполнено условие б), а также условия*

a^γ) $\gamma q \to \infty$;

$в_a^\gamma$) $\frac{\gamma p}{\log(\gamma q)} \to \infty$.

Тогда

$$L_{BC}^{(2)}(\gamma; p, q) \sim \frac{\gamma pq}{\log(\gamma q)}.$$

Вместе с задачами о сложности реализации произвольных матриц и матриц из специальных классов значительное внимание привлекает задача о сложности реализации конкретных матриц. Во многом это связано с тем, что для вентильных схем, в отличие от большинства модельных объектов управляющих систем, удается получать нетривиальные (существенно превышающие линейные относительно числа полюсов и даже сравнимые с мощностными) нижние оценки для «индивидуальных последовательностей» матриц.

Э. И. Нечипоруком исследовалась [90] сложность реализации следующей последовательности булевых матриц. Пусть r — простое число и $n = r^2$. Обозначим через $F_{a,b}$ квадратную булеву матрицу порядка r, получающуюся из диагональной матрицы циклическим сдвигом ее столбцов на $ab \pmod r$ позиций. Из этих блоков образуем квадратную матрицу F_n порядка n:

$$F_n = \{F_{a,b}\}_{a,b=0,1,\ldots,r-1}.$$

Т е о р е м а 55 [90]. *Всякая минимальная вентильная схема, реализующая матрицу F_n, состоит из $n^{3/2}$ вентилей, т. е. $L_{BC}(F_n) = n^{3/2}$.*

Несколько позже аналогичные результаты были получены Е. Ламаньей и Дж. Севиджем [164], а также Р. Тарьяном [189, 190] (для матриц Адамара).

В обзоре по вентильным схемам О. Б. Лупанова [74] (в котором отражены все перечисленные выше результаты, за исключением теорем 42, 43 и 54) были поставлены три задачи.

1. Получить асимптотическое выражение для роста функции Шеннона $L_{BC}(p, q)$ в случае, когда величины $\log p$ и $\log q$ имеют одинаковый порядок роста.

2. Получить асимптотическую формулу для функции Шеннона $L_{BC}(n)$ в случае вентильных схем, реализующих произвольные транзитивные квадратные булевы матрицы порядка n (в которых не выделены специально входы и выходы).

3. Построить «эффективно» последовательность квадратных булевых матриц порядка n, которые реализуются лишь со сложностью, существенно большей, чем $n^{3/2}$.

Первая из этих задач, как уже говорилось, решена Н. Пиппенджером [174, 175] — см. теорему 42.

Вторую задачу решил в 1985 г. А. Е. Андреев [1].

Т е о р е м а 56 [1]. *При $n \to \infty$ имеет место соотношение*

$$L_{BC}(n) \sim \frac{n^2}{8 \log n}.$$

Продвижения в решении третьей задачи оказались связаны с построением семейств (k, l)-редких матриц (у которых никакие k строк не имеют

l общих единиц, т. е. без единичных подматриц размера $k \times l$) — подробнее см., например, [12, 17]. Построение $(2,2)$-редких матриц с числом единиц порядка $n^{3/2}$ привело [90, 164, 189] к получению нижней оценки сложности реализации этих матриц вентильными схемами, равной по порядку $n^{3/2}$, построение $(3,3)$-редких матриц с числом единиц порядка $n^{5/3}$ — к получению [77, 176] нижней оценки сложности реализации этих матриц вентильными схемами, равной по порядку $n^{5/3}$. В 1985 г. А. Е. Андреев [2] для любого t построил пример $(O_t(1), O_t(1))$-редкой $n \times n$-матрицы с числом единиц порядка $n^{2-1/t}$ и получил для этой матрицы нижние оценки порядка $n^{2-1/t}$ для сложности ее реализации вентильными схемами. Последний результат несколько усилен в работах [116, 159]. Тем самым для конкретных последовательностей матриц удается доказать нижние оценки, рост которых несильно отличается от роста функции Шеннона сложности реализации булевых матриц вентильными схемами.

Возвращаясь к задаче о сложности реализации вентильными схемами матриц из специальных классов, отметим, что сам факт существования достаточно плотных (с достаточно большим общим числом единиц) редких матриц может давать высокие нижние оценки, но, конечно, неконструктивные. В этом направлении для класса циклических (циркулянтных) булевых матриц, являющегося значительно более узким, нежели класс всех булевых матриц (так как циклическая матрица полностью определяется первой строкой — остальные строки получаются из нее соответствующими сдвигами), М. И. Гринчуком [16] получены нижние оценки сложности реализации вентильными схемами, близкие к значениям для класса всех булевых матриц.

Т е о р е м а 57 [16]. *Существует последовательность $\{C_n\}$ циклических булевых матриц порядка n такая, что для некоторых положительных c_1 и c_2 при всех достаточно больших n выполняются неравенства*

$$L_{BC}(\Omega_n) \geqslant c_1 \frac{n^2}{\log^{12} n}, \quad L^{(2)}_{BC}(\Omega_n) \geqslant c_2 \frac{n^2}{\log^{10} n}.$$

В работе [17] этот результат несколько усилен — доказано существование циклических матриц сложности по порядку не менее $\frac{n^2}{\log^5 n}$ при реализации произвольными вентильными схемами и по порядку не менее $\frac{n^2}{\log^4 n}$ при реализации вентильными схемами глубины 2.

Теперь остановимся на задаче о сложности реализации вентильными схемами матриц с заданной площадью информационной части.

Пусть по-прежнему $A = (a_{ij})$ — булева матрица размера $p \times q$. Для $j = 1, 2, \ldots, q$ обозначим через p_j наибольший номер среди ненулевых элементов j-го столбца матрицы A. Таким образом,

$$p_j = \max \{i \mid a_{ij} \neq 0\}, \quad j = 1, 2, \ldots, q.$$

Положим

$$\mathscr{S}(A) = \sum_{j=1}^{q} p_j.$$

Величину $\mathscr{S}(\mathscr{A})$ будем называть *информационной площадью матрицы A*.

Отметим, что, вообще говоря, величина информационной площади матрицы не инвариантна относительно операции транспонирования матрицы. Кроме того, очевидно, что в матрице A среди pq элементов не менее $pq - \mathscr{S}(\mathscr{A})$ элементов нулевые.

Введем функцию Шеннона сложности реализации булевых матриц размера $p \times q$ с информационной площадью $\mathscr{S}$:

$$L_{BC}(p, q; \mathscr{S}) = \max L_{BC}(A),$$

где максимум берется по всем матрицам размера $p \times q$ с информационной площадью $\mathscr{S}$.

Аналогично определяется и функция Шеннона $L_{01}(p, q; \mathscr{S})$.

С использованием теоремы 42 установлен следующий факт.

Т е о р е м а 58 [30,31]. *Пусть выполнено условие*

в$_{\mathscr{S}}$) $\dfrac{(p+q)\log \mathscr{S}}{\mathscr{S}} \to 0$.

Тогда

$$L_{01}(p, q; \mathscr{S}) \sim L_{BC}(p, q; \mathscr{S}) \sim \frac{\mathscr{S}}{\log \mathscr{S}}.$$

Верхняя оценка из теоремы 58, сформулированная в немного другом виде в лемме 1, стала важнейшим элементом нахождения асимптотически точного решения задачи Беллмана — Кнута (см. § 2).

8.2. Вентильные схемы с кратными путями. Н. Пиппенджер, завершивший исследования О. Б. Лупанова и Э. И. Нечипорука по нахождению асимптотики роста функции Шеннона сложности реализации булевых матриц вентильными схемами, обобщил этот результат на естественным образом возникающую, например в задаче, которую мы называем задачей Пиппенджера, следующую модификацию классических вентильных схем.

Пусть $A = (a_{ij})$ — целочисленная матрица размера $p \times q$ с неотрицательными элементами. Ориентированный граф S без ориентированных циклов будем называть *вентильной схемой с кратными путями* (или *вентильной схемой с предписанным числом путей*), *реализующей матрицу* A, если: в S выделено p вершин — входных полюсов и q вершин — выходных полюсов; в S нет ориентированных путей от одного входа к другому, от одного выхода к другому, от выхода к входу; для любой пары (i, j), $1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant q$, число ориентированных путей от i-го входа к j-му выходу равно в точности a_{ij}. Аналогично случаю классических вентильных схем, через $L^m_{BC}(S)$ обозначим число ребер (вентилей) схемы S и положим $L^m_{BC}(A) = \min L^m_{BC}(S)$, где минимум берется по всем схемам, реализующим матрицу A.

Для функции Шеннона, определяемой равенством

$$L^m_{BC}(p, q, K) = \max L^m_{BC}(A),$$

где максимум берется по всем матрицам размера $p \times q$ с неотрицательными целыми элементами, не превосходящими $K - 1$, в 1979 г. Н. Пиппенджером при условии $pq \log K \to \infty$ и слабых ограничениях на соотношения параметров установлена асимптотика роста.

Т е о р е м а 59 (Н. П и п п е н д ж е р). *Пусть выполняется условие* $pq \log K \to \infty$. *Тогда*

$$L^m_{BC}(p, q, K) = 3 \min(p,\ q) \log_3 K + \frac{pq \log K}{\log(pq \log K)}(1 + o(1)) + O(\max(p,\ q)).$$

Этот результат сформулирован в [175], а его доказательство можно восстановить, объединив доказательства из [175] и [177].

Конструкция Пиппенжера из верхней оценки теоремы 59 имеет растущую глубину. Растущей глубины, очевидно, нельзя избежать при сохранении асимптотически оптимальной сложности и достаточно быстром росте параметра K. В 2018 г. И. С. Сергеевым установлено [100], что при некоторых довольно естественных ограничениях асимптотически точные верхние оценки функции Шеннона $L^m_{BC}(p,q,K)$ можно получать, используя, в зависимости от ограничений, схемы глубины 3 или 4. Естественным образом определив для любого натурального r функцию Шеннона $L^{m\,(r)}_{BC}(p,q,K)$ сложности реализации целочисленных матриц вентильными схемами глубины r с кратными путями, результаты И. С. Сергеева могут быть сформулированы следующим образом.

Т е о р е м а 60 [100]. *Пусть выполнены условия*

а) $p \to \infty$;

б) $p \leqslant q$;

в) $\dfrac{(\log q)^{3/2}}{p} \to 0$;

г) $\dfrac{\log K}{\log q} \to 0$.

Тогда

$$L^{m\,(3)}_{BC}(p,q,K) \sim L^m_{BC}(p,q,K) \sim \frac{pq\log K}{\log(pq\log K)} \sim \frac{pq\log K}{\log(pq)}.$$

Т е о р е м а 61 [100]. *Пусть выполнены условия*

а) $p \to \infty$;

б) $p \leqslant q$;

в) $\dfrac{(\log q)^{3/2}}{p} \to 0$;

г) $\dfrac{K\log^2 q}{q} \to 0$.

Тогда

$$L^{m\,(4)}_{BC}(p,q,K) \sim L^m_{BC}(p,q,K) \sim \frac{pq\log K}{\log(pq\log K)} \sim \frac{pq\log K}{\log(pq)}.$$

Возвращаясь к оценкам функций Шеннона из теорем 42 и 59, отметим, что для обеих модификаций вентильных схем при слабых ограничениях на число полюсов (входов и выходов) установлена асимптотика роста функций Шеннона и предложен метод синтеза вентильных схем, дающий для почти всех матриц асимптотически минимальную верхнюю оценку. Однако при попытках получения асимптотически точных оценок сложности индивидуальных последовательностей матриц при реализации классическими схемами возникают стандартные трудности с доказательством нижних оценок, в той или иной степени близких к «мощностной», которые удается так или иначе преодолеть лишь отчасти (см., например, [2, 77, 90, 164, 189]). При реализации матриц вентильными схемами с кратным числом путей ситуация, вообще говоря, не такая — в наиболее естественном и интересном случае, когда размеры матриц ограничены (или очень слабо растут), слагаемое, соответствующее мощностным соображениям, вносит не основной по порядку вклад в рост функции Шеннона. Это дает надежду получать асимптотически точные нижние оценки для индивидуальных последовательностей (матриц). И в этом направлении получены значительные продвиже-

ния, которые на самом деле на качественном уровне полностью соответствуют результатам, установленным в этом направлении для задачи Пиппенджера. Переходя к их формулировке, условимся далее под вентильными схемами понимать вентильные схемы с кратным числом путей.

Лемма 25 [52]. *Пусть k вершинам вентильной схемы S приписаны наборы $(a_{11}, a_{12}, \ldots, a_{1k})$, $(a_{21}, a_{22}, \ldots, a_{2k})$, $\ldots$ $(a_{k1}, a_{k2}, \ldots, a_{kk})$, задаваемые матрицей $A=(a_{ij})$ размера $k\times k$. Тогда*

$$3^{L^m_{BC}(S)} \geqslant |\det A|^3.$$

Доказательство. Будем вести доказательство индукцией по числу вершин схемы, в которые входит хотя бы один вентиль. Для схемы, не содержащей ни одного вентиля, утверждение леммы очевидно.

В схеме S среди k выбранных вершин обозначим через v_k ту вершину, от которой к другим выделенным вершинам не ведут пути (хотя бы одна такая вершина всегда найдется в силу ацикличности вентильной схемы). Пусть в вершину v_k ведут r вентилей. Вершины, из которых выходят эти вентили, обозначим соответственно через $v_k^{(1)}, v_k^{(2)}, \ldots, v_k^{(r)}$. Пусть этим вершинам приписаны наборы $(a_{k1}^{(i)}, a_{k2}^{(i)}, \ldots, a_{kk}^{(i)})$, $i = 1, 2, \ldots, r$. Тогда набор $(a_{k1}, a_{k2}, \ldots, a_{kk})$ есть покомпонентная сумма наборов $(a_{k1}^{(i)}, a_{k2}^{(i)}, \ldots, a_{kk}^{(i)})$, $i = 1, 2, \ldots, r$. Матрицу, получающуюся из матрицы A путем замены строки $(a_{k1}, a_{k2}, \ldots, a_{kk})$ на строку $(a_{k1}^{(i)}, a_{k2}^{(i)}, \ldots, a_{kk}^{(i)})$, обозначим через $A^{(i)}$. Схему, получающуюся из схемы S путем удаления вершины v_k и всех вентилей, входящих в v_k, обозначим через S'. Применяя предположение индукции, имеем:

$$|\det A| = \left|\sum_{i=1}^{r} \det A^{(i)}\right| \leqslant \sum_{i=1}^{r} \left|\det A^{(i)}\right| \leqslant$$

$$\leqslant r\left(3^{L^m_{BC}(S')}\right)^{1/3} = r\left(3^{L^m_{BC}(S)-r}\right)^{1/3} \leqslant \left(3^{L^m_{BC}(S)}\frac{r^3}{3^r}\right)^{1/3} \leqslant \left(3^{L^m_{BC}(S)}\right)^{1/3}.$$

Лемма 25 доказана.

Лемма 25 является для вентильных схем аналогом леммы 10, доказанной для задачи Пиппенджера и ее вариаций в близких вычислительных моделях. Так же, как из леммы 25 вытекает теорема 26, из леммы 10 следует нижняя оценка сложности реализации вентильными схемами матрицы A через величину $D(A)$, где $D(A)$ — это максимум абсолютных величин миноров матрицы A, где максимум берется по всем минорам.

Теорема 62 [52]. *Для любой ненулевой целочисленной матрицы A с неотрицательными элементами справедливо неравенство*

$$L^m_{BC}(A) \geqslant 3\log_3 D(A).$$

Нижняя оценка из теоремы 62 является хорошей базой для исследования асимптотического поведения сложности индивидуальных последовательностей матриц фиксированного размера, что подтверждает следующая

Теорема 63 [52]. *Для произвольного натурального m и произвольной последовательности матриц $\{A_n\}$ с неотрицательными элементами, каждая из которых имеет размер либо $2\times q_n$, где $q_n \leqslant m$,*

либо $p_n \times 2$, *где* $p_n \leqslant m$, *либо* 3×3, *при условии* $D(A_n) \to \infty$ *выполняется соотношение*

$$L^m_{BC}(A_n) \sim 3 \log_3 D(A_n).$$

Доказательства верхних оценок этой теоремы в идейном плане не сильно отличаются от доказательств верхних оценок сложности вычисления систем одночленов схемами из умножений в теоремах 27, 28 и 30. Все эти доказательства технически тяжелые. При этом, с одной стороны, оценки сложности реализации матриц вентильными схемами формально никак не следуют из соответствующих оценок для задачи Пиппенджера, а с другой — все содержательное отличие упирается в тот факт, что минимальное число операций умножения для возведения в n-ю степень асимптотически равно $\log n$, а минимальное число дуг, достаточное для организации n различных путей от одной вершины к другой, асимптотически равно $3 \log_3 n$. Такое же соотношение сложностей сохраняется и для последовательности матриц из теоремы 31 (см. следствие 4 из этой теоремы), для которой универсальная нижняя оценка теоремы 26 не является асимптотически точной.

Т е о р е м а 64. *При условии* $t = o\left(\log n\right)$ *справедливо асимптотическое равенство*

$$L^m_{BC}(A(t,n)) \sim 6t \log_3 n.$$

Доказательство этой теоремы нетрудно получить из доказательства теоремы 31.

Следствием теоремы 64 является такое утверждение: при условии $t \leqslant \frac{\log n}{\log \log n}$ выполняется соотношение $L^m_{BC}(A(t,n)) \sim \frac{6t}{t+1} \log_3 D(A(t,n))$. Таким образом, для последовательности матриц $A(t,n)$ размера $2t \times 2t$ устанавливаемую теоремой 62 нижнюю оценку можно усилить асимптотически в $2t/(t+1)$ раз. При этом, как уже отмечалось, и в этом случае при переходе от меры сложности, соответствующей классическим схемам из умножений, к сложности реализации вентильными схемами сложность увеличивается асимптотически в $3 \log_3 2$ раза. Более того, представляется очень правдоподобным следующее предположение о том, что с асимптотической точки зрения оценки сложности в задаче Пиппенджера и в задаче реализации матриц вентильными схемами различаются только коэффициентом или относительным масштабом.

Г и п о т е з а. *Для любой последовательности целочисленных неотрицательных матриц* $\{A_n\}$, *имеющих фиксированный размер* $p \times q$ *и удовлетворяющих условию* $D(A_n) \to \infty$, *выполняется соотношение*

$$\frac{L^m_{BC}(A_n)}{l(A_n)} \sim 3 \log_3 2.$$

Отметим, что справедливость гипотезы, сформулированной в п. 5.4, автоматически приведет к истинности соотношения

$$\frac{L^m_{BC}(A_n)}{l(A_n)} \lesssim 3 \log_3 2.$$

Теперь перейдем к задаче о сложности реализации недоопределенных матриц вентильными схемами с кратными путями. Пусть $A = (a_{ij})$ — матрица, элементами которой являются целые неотрицательные числа и элементы $*$ (символ $*$ соответствует неопределенному элементу).

Такую матрицу так же, как и в булевом случае, будем называть *не всюду определенной* или *недоопределенной* (отметим, что формально полностью определенные матрицы являются частным случаем недоопределенных).

Матрица $B=(b_{ij})$ называется *доопределением* матрицы $A=(a_{ij})$ такого же размера, если в матрице B все элементы определены (нет символов $*$) и для любого определенного элемента a_{ij} матрицы A справедливо равенство $a_{ij}=b_{ij}$.

Пусть A — недоопределенная матрица, в которой все определенные элементы целочислены и неотрицательны. Положим

$$L^m_{BC}(A)=\inf L^m_{BC}(B),$$

где инфинум берется по всем доопределениям B матрицы A до целочисленной матрицы с неотрицательными элементами.

Очевидно, что инфинум достигается.

Без ограничения общности можно считать, что в матрицах нет ни строк, ни столбцов, полностью состоящих из нулей и символов $*$.

Теперь рассмотрим случай, когда матрица состоит либо из двух строк, либо из двух столбцов. Без ограничения общности будем считать, что $A=(a_{ij})$ — недоопределенная матрица размера $p\times 2$.

Обозначим через $A_o=A_o(A)$ полностью определенную (возможно, пустую) матрицу, получающуюся из матрицы A путем вычеркивания не полностью определенных строк. Положим $d_0(A)=D(A_o)$, если матрица A_o непустая, и $d_0(A)=1$ в случае отсутствия полностью определенных строк в матрице A.

Выделим три подмножества множества $\{1,2,\ldots,p\}$ номеров строк матрицы A. Через I_1 обозначим множество номеров таких строк, в которых первый элемент является определенным, а второй элемент — символ $*$; через I_2 — множество номеров таких строк, в которых первый элемент является символом $*$, а второй элемент — определенный; и, наконец, через J — множество номеров строк, оба элемента которых являются определенными.

Положим

$$d_1(A)=\frac{\max\left(\max\limits_{i\in I_1}\{a_{i1}\},1\right)}{\max\left(\max\limits_{j\in J}\{a_{j1}\},1\right)},\qquad d_2(A)=\frac{\max\left(\max\limits_{i\in I_2}\{a_{i2}\},1\right)}{\max\left(\max\limits_{j\in J}\{a_{j2}\},1\right)}.$$

Здесь максимумы в числителях (по i) берутся по всем определенным элементам, стоящим в неполностью определенных строках (т. е. в строках, в которых второй элемент — символ $*$), а максимумы в знаменателях (по j) берутся по всем определенным элементам, стоящим в полностью определенных строках.

Теперь положим

$$D^*(A)=d_0(A)\max\{d_1(A),d_2(A),1\}.$$

Т е о р е м а 65 [54]. *Для произвольной последовательности недоопределенных матриц $A_n=\big(a_{ij}(n)\big)$, $n=1,2,\ldots$, фиксированного размера $p\times 2$, все определенные элементы которых неотрицательны, при условии $\sum a_{ij}(n)\to\infty$ (сумма берется по всем определенным элементам матрицы A_n) выполняется соотношение*

$$L^m_{BC}(A_n)\sim 3\log_3 D^*(A_n).$$

§ 9. Схемы композиции

В настоящем параграфе рассматривается сложность реализации систем одночленов в рамках еще одной вычислительной модели, как представляющей самостоятельный интерес, так и позволяющей иначе взглянуть на задачу Пиппенджера и на подходы к разработке новых методов для ее решения. Эта модель — схемы композиции [25, 26, 81, 105, 106] — основана на одном из обобщений операции умножения, естественным образом возникающем в алгебре (см., например, [111]), — операции композиции.

Следуя А. И. Ширшову [111], определим понятие композиции одночленов следующим образом. Пусть $U = x_1^{u_1} \dots x_q^{u_q}$, $V = x_1^{v_1} \dots x_q^{v_q}$ — произвольные одночлены, и задан одночлен $R = x_1^{r_1} \dots x_q^{r_q}$, где $0 \leqslant r_i \leqslant \min(u_i, v_i)$, $1 \leqslant i \leqslant q$ (отметим, что для выражения R может быть выполнено условие $\sum\limits_{i=1}^{q} r_i = 0$, но все равно будем в дальнейшем называть его одночленом). *Композицией* одночленов U и V относительно одночлена R называется одночлен $x_1^{u_1+v_1-r_1} \dots x_q^{u_q+v_q-r_q}$, который будем обозначать через $(U, V)_R$.

Последовательность S, состоящая из одночленов

$$X_1, \dots, X_q, X_{q+1}, \dots, X_{q+n},$$

называется *схемой композиции* [81] *для одночлена* X_{q+n}, если эта последовательность удовлетворяет условиям:

1) для $i = 1, \dots, q$ выполняется равенство $X_i = x_i$;

2) для $i = q+1, \dots, q+n$ найдутся s и t, не превосходящие $i-1$, а также одночлен R_i, такие что $X_i = (X_s, X_t)_{R_i}$.

Под *сложностью* $l_{sh}(S)$ схемы композиции S указанного вида будем понимать число n (количество в схеме одночленов, отличных от переменных).

Теперь определим сложность вычисления систем одночленов схемами композиции (подробнее см. [25, 106]).

Схемой композиции для системы одночленов

$$M = \{x_1^{a_{11}} \dots x_q^{a_{1q}}, \dots, x_1^{a_{p1}} \dots x_q^{a_{pq}}\}$$

будем называть схему композиции S для некоторого одночлена из системы M, которая содержит в качестве элементов остальные одночлены из множества M.

Положим $l_{sh}(M) = \min l_{sh}(S)$, где минимум берется по всем схемам композиции для системы M. Величину $l_{sh}(M)$ назовем *сложностью системы одночленов* M (*при реализации схемами композиции*). Система одночленов M полностью определяется матрицей $A = (a_{ij})_{p \times q}$ показателей степеней. Поэтому, как и при вычислениях в других моделях, можно говорить не только о сложности $l_{sh}(M)$ вычисления системы M, но и о *сложности* $l_{sh}(A)$ *матрицы* A, задающей эту систему. Далее не будем различать эти понятия и будем считать, что $l_{sh}(A) = l_{sh}(M)$.

Так же, как и для большинства исследуемых модельных классов вычислений, понятие схемы композиции можно проинтерпретировать на языке схем из функциональных элементов. Принципиальным отличием в данном случае является то обстоятельство, что функциональному элементу,

соответствующему операции $(U,V)_R$, помимо собственно операции композиции, приписывается в качестве параметра одночлен R. Тем самым количество типов функциональных элементов становится бесконечным. Отметим, что схемная сложность в бесконечных базисах исследовалась многими авторами — в случае реализации булевых функций см., например, [21, 22, 73, 76, 84, 88]. В данной модели, во-первых, вычисляются не булевы функции, а системы одночленов, а во-вторых, и это существенно, не любая схема из двухвходовых функциональных элементов после приписывания каждому элементу E_i одночлена R_i и сопоставления этому элементу операции композиции относительно одночлена R_i будет работать корректно. Тем не менее проверить корректность работы схемы (т. е. корректность работы всех элементов схемы) нетрудно. Очевидно, что по заданной схеме композиции можно построить соответствующую корректно работающую схему из функциональных элементов той же сложности. Верно и обратное утверждение. Таким образом, и для данного модельного объекта язык схем из функциональных элементов вполне естествен.

Схемы композиции были введены в 2003 году Ю. В. Мерекиным [81]. Им установлено точное значение сложности реализации одного одночлена схемами композиции.

Т е о р е м а 66 [81]. *Справедливо равенство*

$$l_{sh}(x_1^{a_1}\dots x_q^{a_q}) = \lceil \log a \rceil + q - 1, \ \textit{где}\ a = \max(a_1 \dots a_q).$$

На самом деле в [81] установлен более сильный факт, заключающейся в том, что требуемая теоремой 66 верхняя оценка справедлива и при дополнительном условии: степени всех одночленов, относительно которых выполняются операции композиции в схеме, не превосходят единицы.

Дальнейшие продвижения в задаче о сложности вычисления систем одночленов схемами композиции связаны в основном с именами Е. Н. Трусевич и С. А. Корнеева, учениками автора.

Прежде всего отметим некоторые результаты, показывающие, что мера сложности l_{sh} существенно отличается от обсуждавшихся выше мер сложности целочисленных матриц.

Одним из отличий является тот факт, что для данной меры сложности не работают (или не работают в достаточной мере) соображения двойственности.

Определим две матрицы размера $m \times 1$:

$$B_1(m) = \begin{pmatrix} 1 \\ 2 \\ 3 \\ \vdots \\ m \end{pmatrix}, \qquad B_2(m) = \begin{pmatrix} 1 \\ 2 \\ 4 \\ \vdots \\ 2^{m-1} \end{pmatrix}.$$

Сложность реализации этих матриц схемами композиции одинаковая:

$$l_{sh}(B_1(m)) = l_{sh}(B_2(m)) = m - 1.$$

А вот сложность транспонированных к ним матриц отличается асимптотически в два раза:

$$l_{sh}(B_1^T(m)) = m - 1 + \lceil \log m \rceil \sim m, \quad l_{sh}(B_2^T(m)) = 2m - 2 \sim 2m.$$

Заметим, что этот пример, в отличие от примера из предисловия к параграфу о вычислениях элементов свободной абелевой группы, опровергающего соображения двойственности для меры сложности l_F, не основан на наличии в матрице элементов разных знаков.

Вторым важнейшим отличием меры сложности l_{sh} является то обстоятельство, что для этой меры сложности не выполняется универсальная нижняя оценка, т. е. оценка, аналогичная оценке из теоремы 26, ни для какого «масштабирования» (кстати, масштабирования для этой задачи и не предполагается, так как сложность вычисления одночлена x^n схемами композиции равна $\lceil \log n \rceil$).

Действительно, следуя [106], обозначим через $B(p, n)$ квадратную матрицу порядка p, в которой на главной диагонали стоит число $2n$, а остальные элементы равны n. Для примера выпишем матрицу $B(3, n)$:

$$B(3,n) = \begin{pmatrix} 2n & n & n \\ n & 2n & n \\ n & n & 2n \end{pmatrix}.$$

Используя введенную последовательность матриц, в 2014 г. Е. Н. Трусевич для модели схем композиции установила возможность получения верхних оценок сложности, существенно меньших универсальной нижней оценки из теоремы 26, справедливой для других вычислительных моделей.

Т е о р е м а 67 [106]. *Пусть* $B_n = B(\lceil \log n \rceil / 2, n)$. *Тогда при* $n \to \infty$ *справедливы соотношения*

$$l_{sh}(B_n) \sim 2\sqrt{2 \log D(B_n)} \sim 2\sqrt{2l(B_n)} \sim 2\sqrt{2l_2(B_n)}.$$

Д о к а з а т е л ь с т в о. Учитывая результат из [81], получаем:

$$l_{sh}(B(p,n)) = \lceil \log n \rceil + 2p - 1.$$

С другой стороны, для определителя матрицы $B(p, n)$ справедливо равенство:

$$\det B(p,n) = (p+1)n^p.$$

Поэтому при $p + n \to \infty$ имеем:

$$\log D(B(p,n)) = \log(\det B(p,n)) = p \log n + \log(p+1) \sim p \log n.$$

Кроме того, учитывая теорему 26 и простые верхние оценки, при $p + n \to \infty$ получаем соотношения

$$l(B(p,n)) \sim l_2(B(p,n)) \sim \log D(B(p,n)) \sim p \log n.$$

Таким образом, с одной стороны,

$$l_{sh}(B_n) \sim 2 \log n,$$

а с другой —

$$\log D(B_n) \sim (\log n)^2/2$$

и, следовательно,

$$l(B_n) \sim l_2(B_n) \sim (\log n)^2/2.$$

Поэтому окончательно имеем:

$$l_{sh}(B_n) \sim 2\sqrt{2\log D(B_n)} \sim 2\sqrt{2l(B_n)} \sim 2\sqrt{2l_2(B_n)}.$$

Теорема 67 доказана.

Таким образом, для сложности (относительно меры l_{sh}) последовательности матриц B_n не выполняется универсальная нижняя оценка, аналогичная оценкам из теоремы 26 ни при каком «масштабировании». Более того, величина $l_{sh}(B_n)$ растет по порядку как квадратный корень из величины $\log D(B_n)$, а следовательно, и как квадратный корень из величины $l_2(B_n)$.

Этот факт говорит о значительной вычислительной силе схем, использующих операции композиции. Возникает естественный вопрос — всегда ли рост сложности для меры l_{sh} асимптотически не превосходит роста сложности для меры l_2? Оказывается, что ответ на этот вопрос отрицательный. Для того, чтобы убедиться в этом, достаточно рассмотреть введенное в п. 5.6 множество матриц $A(t,n)$ размера $2t \times 2t$: 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.

Т е о р е м а 68 [106]. *Пусть* $t \leqslant \frac{\log n}{\log\log n}$. *Тогда при* $n \to \infty$ *справедливы соотношения*

$$l_{sh}(A(t,n)) \sim \frac{2t}{t+1}\log D(A(t,n)) \sim \frac{2t}{t+1} l_2(A(t,n)).$$

Таким образом, возможностей операции композиции оказывается недостаточно даже для того, чтобы асимптотику роста сложности с величины $\frac{2t}{t+1}\log D(A(t,n))$, характерной для «слабой» вычислительной модели, использующей только операцию умножения, понизить хотя бы до величины универсальной нижней оценки $\log D(A(t,n))$. И, таким образом, сила операции композиции носит далеко не универсальный характер.

Более того, при вычислении системы одночленов, задаваемой матрицей $A(t,n)$, при $t \geqslant 2$ и всех достаточно больших n даже операция деления является более эффективной, чем операция композиции (см. теорему 35 и обсуждения после нее).

Теперь вернемся к уже затронутому вопросу о том, насколько сильно могут отличаться величины $l_{sh}(A)$ и $l_{sh}(A^T)$. Значительное продвижение в этом направлении получила в 2014 г. Е. Н. Трусевич.

Для произвольных s и t определим матрицу размера $st\times t$ равенством

$$C(s,t,n)=\begin{pmatrix} n^s & n^s & \cdots & n^s \\ n^{s-1} & n^s & \cdots & n^s \\ \vdots & \vdots & \ddots & \vdots \\ n^{s-1} & n^{s-1} & \cdots & n^s \\ n^{s-1} & n^{s-1} & \cdots & n^{s-1} \\ n^{s-2} & n^{s-1} & \cdots & n^{s-1} \\ \vdots & \vdots & \ddots & \vdots \\ n^{s-2} & n^{s-2} & \cdots & n^{s-1} \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ n & n & \cdots & n \\ 1 & n & \cdots & n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & n \end{pmatrix}.$$

Далее, положим $C_n=C(\lceil\log n\rceil,\lceil\log n\rceil,n)$.

Т е о р е м а 69 [106]. *При $n\to\infty$ справедливо соотношение*

$$l_{Sh}(C_n)\gtrsim\left(\frac{l_{Sh}(C_n^T)}{3}\right)^{\frac{3}{2}}.$$

Особенности модельного класса схем композиции будут еще неоднократно отмечаться. Своеобразие схем композиции нашло отражение и при исследовании *функции Шеннона сложности реализации систем одночленов схемами композиции*, задаваемой формулой

$$L_{sh}(p,q,K)=\max l_{sh}(A),$$

где максимум берется по всем целочисленным неотрицательным матрицам $A=(a_{ij})$ размера $p\times q$, удовлетворяющим условиям $0\leqslant a_{ij}\leqslant K-1$, $i=1,\ldots,p$, $j=1,\ldots,q$.

В 2021 г. С. А. Корнеевым при некоторых ограничениях установлена асимптотика роста функции Шеннона.

Т е о р е м а 70 [28]. *Пусть $pq\log K\to\infty$ и дополнительно выполнено хотя бы одно из условий:*

а) $p\leqslant q$;

б) $p=o(\log K)$;

в) $\log K=o(q/\log p)$.

Тогда

$$L_{sh}(p,q,K)=\left(\min(p,q)\log K+\frac{pq}{\log(pq)}\right)(1+o(1))+O(p+q).$$

Наличие указанных ограничений обусловливается некоторыми свойствами рассматриваемой вычислительной модели, затрудняющими получение оценок сложности: в частности, обсуждавшейся неэффективностью соображений двойственности для схем композиции, а также дополнительными трудностями получения нижних оценок в силу бесконечности базиса.

Таким образом, вопрос о возможности избавиться от выполнения хотя бы одного из условий а)–в) из теоремы 70 с сохранением асимптотики роста функции Шеннона $L_{sh}(p, q, K)$ остается открытым.

Переходя, как и при обсуждении других моделей, к исследованию поведения сложности реализации схемами композиции небольшого числа одночленов от фиксированного числа переменных, стоит отметить два обстоятельства. В силу некоторых особенностей модели при изучении вопросов сложности, с одной стороны, естественно ожидать дополнительных трудностей, а с другой — остается надежда получать точные значения сложности или в том или ином смысле близкие к точным оценки. И оба этих соображения на самом деле получили подтверждения.

Как уже отмечалось, Ю. В. Мерекин нашел [81] точное значение сложности реализации одного одночлена схемами композиции — см. теорему 66.

В случае реализации схемами композиции набора степеней также известно точное значение сложности: если $0 < a_1 < \ldots < a_p$, то

$$l_{sh}(x^{a_1}, x^{a_2}, \ldots, x^{a_p}) = \lceil \log a_1 \rceil + \sum_{k=2}^{p} \left\lceil \log \left(\frac{a_k}{a_{k-1}} \right) \right\rceil .$$

Эта формула легко доказывается и, по-видимому, является фольклорной.

Для случая вычисления схемами композиции системы из двух одночленов от двух переменных в 2011 г. Е. Н. Трусевич [105, 106] установлено точное значение сложности, которое впоследствии было чуть подкорректировано С. А. Корнеевым [29].

Т е о р е м а 71 [105, 106]. *Пусть в целочисленной матрице* $A = (a_{ij})_{2\times 2}$ *с неотрицательными элементами нет нулевых строк и столбцов, а минимальным элементом матрицы* A *является элемент* a_{21}. *Тогда*

$$l_{sh}(A) = \lceil \log a_{22} \rceil + \left\lceil \log \max \left(\frac{a_{11}}{\max(a_{21}, 1)}, \frac{a_{12}}{a_{22}} \right) \right\rceil + \operatorname{sgn} a_{12} + \gamma(A),$$

где $\gamma(A) \in \{0, 1\}$, *причем* $\gamma(A) = 0$ *при* $a_{12} = 0$ *или* $a_{12} \geqslant a_{22}$.

Приведем сформулированный в теореме 71 результат к стандартному симметричному относительно элементов матрицы виду (выражаемому через величину $D(A)$).

Л е м м а 26 [105]. *Пусть* $1 \leqslant a_{21} = \min(a_{11}, a_{12}, a_{21}, a_{22})$. *Тогда выполнены неравенства*

$$0 \leqslant \log a_{22} + \max \log \left(\frac{a_{11}}{a_{21}}, \frac{a_{12}}{a_{22}} \right) - \left(\log a_{21} + \log D\left(A/a_{21}\right) \right) \leqslant 1.$$

В силу леммы 26 теорему 71 можно переформулировать следующим образом.

Т е о р е м а 72 [105, 106]. *Пусть в целочисленной матрице* $A = (a_{ij})_{2\times 2}$ *с неотрицательными элементами нет нулевых строк и столбцов и* $m = \max\left(\min\left(a_{11}, a_{12}, a_{21}, a_{22}\right), 1\right)$. *Тогда при* $D(A) \to \infty$ *справедливо соотношение*

$$l_{sh}(A) = \log m + \log D\left(A/m\right) + O(1).$$

Задача о сложности реализации систем из двух одночленов схемами композиции исследовалась С. А. Корневым. Им для этой задачи найдено [25] точное значение сложности.

Для произвольной матрицы $A=\left(a_{ij}\right)$ положим

$$a_{ij}^{+}=\max\left(a_{ij},1\right),\quad \delta(A)=\begin{cases}1, \text{ если в матрице } A \text{ нет столбцов без нулей;}\\ 0, \text{ иначе.}\end{cases}$$

Т е о р е м а 73 [25]. *Пусть в целочисленной матрице* $A=\left(a_{ij}\right)_{2\times q}$ *с неотрицательными элементами нет нулевых строк и столбцов. Тогда*

$$l_{sh}(A)=\max\left(\left\lceil\log\max_{k:1\leqslant k\leqslant q}a_{1k}^{+}\right\rceil+\left\lceil\log\max_{k:1\leqslant k\leqslant q}\frac{a_{2k}^{+}}{a_{1k}^{+}}\right\rceil,\right.$$
$$\left.\left\lceil\log\max_{k:1\leqslant k\leqslant q}a_{2k}^{+}\right\rceil+\left\lceil\log\max_{k:1\leqslant k\leqslant q}\frac{a_{1k}^{+}}{a_{2k}^{+}}\right\rceil\right)+q-1-\delta(A).$$

Теорема 73 позволяет дать следующую формулировку.

Т е о р е м а 74 [25]. *Пусть в целочисленной матрице* $A=\left(a_{ij}\right)_{2\times q}$ *с неотрицательными элементами нет нулевых строк и столбцов. Тогда*

$$l_{sh}(A)=\max_{(k,l):1\leqslant k<l\leqslant q}l_{sh}\left(A_{kl}^{+}\right)+q-2-\delta(A),$$

где

$$A_{kl}^{+}=\begin{pmatrix}a_{1k}^{+} & a_{1l}^{+}\\ a_{2k}^{+} & a_{2l}^{+}\end{pmatrix}.$$

В случае реализации схемами композиции матриц размера $2\times q$ асимптотика роста сложности отличается от асимптотики роста сложности из задачи Пиппенджера и других обсуждаемых задач. Однако, как видно из теоремы 74, свойство, состоящее в том, что асимптотика роста сложности матриц размера $2\times q$ определяется асимптотикой роста сложности самой сложнореализуемой подматрицы размера 2×2, сохраняется и для вычислений схемами композиции.

Для двойственного случая реализации системы одночленов от двух переменных С. А. Корнеевым [27] был обнаружен принципиально новый эффект: асимптотика роста сложности реализации схемами композиции матриц размера $p\times 2$ не только не определяется никакими квадратными подматрицами порядка 2, но и, вообще говоря, не определяется никакими подматрицами размера $(p-1)\times 2$. Приведем пример, демонстрирующий этот эффект. Для произвольного четного p (для нечетного p пример строится аналогично) и всех натуральных n, следуя [27], положим

$$H_n=\begin{pmatrix}2^{2n} & 1\\ 2^{2n} & 2^{3n}\\ 2^{4n} & 2^{3n}\\ 2^{4n} & 2^{5n}\\ \vdots & \vdots\\ 2^{pn} & 2^{(p-1)n}\\ 2^{pn} & 2^{(p+1)n}\end{pmatrix}.$$

Обозначим через $H_n^{(k)}$ матрицу, полученную из матрицы H_n удалением k-й строки. Для сложности реализации матриц H_n и $H_n^{(k)}$ справедливы равенства

$$l_{sh}(H_n) = (2p+1)n + 1, \qquad l_{sh}(H_n^{(k)}) = (2p-1)n + 1.$$

Для произвольной последовательности k_n элементов из множества $\{1, 2, \ldots, p\}$ для соотношения сложностей реализации схемами композиции матриц H_n и $H_n^{(k_n)}$ выполняется условие

$$\lim_{n\to\infty} \frac{l_{sh}(H_n)}{l_{sh}\left(H_n^{(k_n)}\right)} = 1 + \frac{1}{p - 1/2}.$$

Таким образом, асимптотика роста сложности последовательности матриц H_n отличается от асимптотики роста сложности последовательности матриц, получающейся из матриц последовательности H_n путем вычеркивания одной (произвольной) строки в каждой матрице.

Этот пример показывает принципиальное отличие в поведении сложности реализации схемами композиции двух классов матриц — матриц, состоящих из двух строк, и матриц, состоящих из двух столбцов: сложность в первом случае определяется некоторой самой сложной квадратной подматрицей порядка 2, а во втором, вообще говоря, не определяется никакой собственной подматрицей. Кроме того, приведенный пример говорит о том, что не стоит ожидать простой и компактной формулы, определяющей сложность реализации матриц размера $p \times 2$ схемами композиции. С. А. Корнееву [27] удалось найти это значение с точностью до слагаемого порядка p, и соответствующие оценки имеют довольно громоздкий вид.

Т е о р е м а 75 [27]. *Пусть в целочисленной матрице $A = \left(a_{ij}\right)_{p\times 2}$ с неотрицательными элементами нет нулевых строк и столбцов. Тогда*

$$g(A) \leqslant l_{sh}(A) \leqslant g(A) + 2p - 3,$$

где

$$g(A) = \max_{(i_1,\ldots,i_p)\in S_p} \sum_{k=1}^{p} \left\lceil \log \max\left(\frac{a^+_{i_k 1}}{\max\limits_{l:l<k} a^+_{i_l 1}}, \frac{a^+_{i_k 2}}{\max\limits_{l:l<k} a^+_{i_l 2}}, 1 \right) \right\rceil,$$

а S_p обозначает группу перестановок множества из p элементов.

В заключение остановимся на еще одном результате С. А. Корнеева о сложности реализации систем одночленов схемами композиции, который при некоторых слабых ограничениях удалось перенести на классическую модель схем из умножений и тем самым получить заметное продвижение в исследовании задачи Пиппенджера, в которой до этого более 10 лет не было принципиальных сдвигов.

Следуя [26], введем необходимые обозначения. Для произвольных матриц A и B одинакового размера $p\times q$ будем использовать запись $B \leqslant A$, если выполняются неравенства $b_{ij} \leqslant a_{ij}$, $i = 1, \ldots, p$, $j = 1, \ldots, q$. Положим

$$L_{sh}(A) = \max_{B:\, B\leqslant A} l_{sh}(B).$$

Функция шенноновского типа $L_{sh}(A)$ характеризует сложность реализации схемами композиции самой сложной матрицы, «не превосходящей» данной матрицы A.

Для произвольной квадратной матрицы $B=(b_{ij})$ порядка n положим

$$d_{mt}(B)=\max_{\sigma\in S_n}\left(b_{1\sigma(1)},b_{2\sigma(2)},\ldots,b_{n\sigma(n)}\right).$$

Таким образом, величина $d_{mt}(B)$ равна значению максимального слагаемого (без учета знака) определителя матрицы B. Для произвольной матрицы A положим $D_{MT}(A)=\max d_{mt}(B)$, где максимум берется по всем квадратным подматрицам B матрицы A.

Т е о р е м а 76 [26]. *Пусть $A_n=\left(a_{ij}^{(n)}\right)$ — последовательность матриц размера $p_n\times q_n$ из целых неотрицательных чисел и при $n\to\infty$ выполнено условие*

$$\max_{i,j}a_{ij}^{(n)}\to\infty.$$

Тогда

$$L_{sh}(A_n)=\log D_{MT}(A_n)+\alpha(A_n),$$

где $\alpha(A_n)\geqslant 0$, $\alpha(A_n)=O(p_nq_n)$.

Оказалось, что предложенный для доказательства верхней оценки теоремы 76 метод построения схем композиции при некоторой доработке эффективно «работает» и в случае построения обобщенных схем (λ-схем). Этот факт в совокупности с выполнением условий теоремы 29 позволил при некоторых условиях верхнюю оценку сложности схем композиции перенести на случай схем умножения.

Т е о р е м а 77 [26]. *Пусть $A_n=\left(a_{ij}^{(n)}\right)$ — последовательность матриц размера $p_n\times q_n$ из целых неотрицательных чисел, причем последовательность $\{p_n+q_n\}$ ограничена и при $n\to\infty$ выполнено условие*

$$\max_{i,j}a_{ij}^{(n)}\to\infty.$$

Тогда

$$L(A_n)=(1+o(1))\log D_{MT}(A_n).$$

СПИСОК ЛИТЕРАТУРЫ

1. А н д р е е в А. Е. О сложности реализации транзитивных отношений вентильными схемами // Физическое и математическое моделирование дискретных систем. Научные труды. Вып 56.— М.: МЭИ, 1985. — С. 11–21.
2. А н д р е е в А. Е. Об одном семействе булевых матриц // Вестник МГУ. Серия 1. Математика. Механика. — 1986. — № 2. — С. 97–100.
3. А н д р е е в А. Е. О сложности реализации вентильными схемами недоопределенных матриц // Математические заметки. — 1987. — Т. 41, № 1. — С. 77–86.
4. А н д р е е в А. Е. О сложности градиентных вентильных схем // Дискретная математика. — 1995. — Т. 7, № 1. — С. 66–76.
5. Б е л а г а Э. Г. Аддитивная сложность натурального числа // Доклады АН СССР. — 1976. — Т. 226, № 1. — С. 15–18.
6. В а й н ц в а й г М. Н. О мощности схем из функциональных элементов // Доклады АН СССР. — 1961. — Т. 139, № 2. — С. 320–323.
7. В а л ь с к и й Р. Э. О наименьшем числе умножений для возведения в данную степень // Проблемы кибернетики. Вып. 2. — М.: Физматгиз, 1959. — С. 73–74.
8. Г а ш к о в С. Б. Замечание о минимизации глубины булевых схем // Вестник МГУ. Серия 1. Математика. Механика. — 2007. — № 6. — С. 7–9.

9. Гашков С. Б., Гашков И. Б. О сложности вычисления дифференциалов и градиентов // Дискретная математика. — 2005. — Т. 17, № 3. — С. 45–67.
10. Гашков С. Б., Кочергин В. В. Об аддитивных цепочках векторов, вентильных схемах и сложности вычисления степеней // Методы дискретного анализа в теории графов и сложности. Сборник научных трудов. Вып. 52.— Новосибирск, 1992. — С. 22–40.
11. Гашков С. Б., Сергеев И. С. О применении метода аддитивных цепочек к инвертированию в конечных полях // Дискретная математика. — 2006. — Т. 18, № 4. — С. 56–72.
12. Гашков С. Б., Сергеев И. С. О сложности линейных булевых операторов с редкими матрицами // Дискретный анализ и исследование операций. — 2010. — Т. 17, № 3. — С. 3–18.
13. Гашков С. Б. Задача об аддитивных цепочках и ее обобщения // Математическое просвещение. Третья серия. Вып. 15. — М.: МЦНМО, 2011. — С. 138–153.
14. Глухов М. М., Зубов А. Ю. О длинах симметрических и знакопеременных групп подстановок в различных системах образующих // Математические вопросы кибернетики. Вып. 8. — М.: Наука, 1999. — С. 5–32.
15. Григорьев Д. Ю. Нижние оценки в алгебраической сложности вычислений // Теория сложности вычислений. I. Записки научного семинара ЛОМИ. Т. 118. — Л.: Наука, 1982. — С. 25-82.
16. Гринчук М. И. О сложности реализации циклических булевых матриц вентильными схемами // Известия ВУЗов. Математика. — 1988. — № 7. — 39–43.
17. Гринчук М. И., Сергеев И. С. Редкие циркулянтные матрицы и нижние оценки сложности некоторых булевых операторов // Дискретный анализ и исследование операций. — 2011. — Т. 18, № 5. — С.38–53.
18. Евдокимов А. А. Полные множества слов и их числовые характеристики // Методы дискретного анализа. — Новосибирск, 1983. — Вып. 39. — С. 7–19.
19. Зыков К. А. О сложности реализации линейных булевых преобразований схемами глубины три // Вестник МГУ. Серия 1. Математика. Механика. — 1998. — № 2. — С. 68–70.
20. Ильин А. М. Об аддитивных цепочках чисел // Проблемы кибернетики. Вып. 13. — М.: Физматлит, 1965. — С. 245–248.
21. Касим-Заде О. М. Об одном методе получения оценок сложности схем над произвольным бесконечным базисом // Дискретный анализ и исследование операций. Серия 1. — 2004. — Т. 11, № 2. — С. 41–65.
22. Касим-Заде О. М. О порядках роста функций Шеннона сложности схем над бесконечными базисами // Вестник МГУ. Серия 1. Математика. Механика. — 2013. — № 3. — С. 55–57.
23. Кнут Д. Е. Искусство программирования для ЭВМ, т. 2, 1-е издание. — М.: Мир, 1977.
24. Кнут Д. Е. Искусство программирования, т. 2, 3-е издание. — М.: Издательский дом «Вильямс», 2000.
25. Корнеев С. А. О сложности реализации системы из двух одночленов схемами композиции // Дискретная математика. — 2020. — Т. 32, № 2. — С. 15–31.
26. Корнеев С. А. Об асимптотическом поведении функций шенноновского типа, характеризующих сложность вычисления систем одночленов // Ученые записки Казанского университета. Серия «Физико- математические науки». — 2020. — Т. 162, № 3. — С. 300–310.
27. Корнеев С. А. О сложности реализации системы одночленов от двух переменных схемами композиции // Прикладная дискретная математика. — 2021. — № 53. — С. 103–119.
28. Корнеев С. А. О поведении функции Шеннона сложности реализации систем одночленов схемами композиции // Интеллектуальные системы. Теория и приложения. — 2021. — Т. 25, № 3. — С. 173–188.
29. Корнеев С. А. О сложности реализации систем одночленов схемами композиции: Дисс. . . . канд. физ.-мат. наук: 01.01.09. — М.: МГУ, 2021.
30. Кочергин В. В. О сложности вычислений в конечных абелевых группах // ДАН СССР. — 1991. — Т. 317, № 2. — С. 291–294.
31. Кочергин В. В. О сложности вычислений в конечных абелевых группах // Математические вопросы кибернетики. Вып. 4. — М.: Наука, 1992. — С. 178–217.
32. Кочергин В. В. О сложности вычислений одночленов и наборов степеней // Труды Ин-та математики СО РАН — 1994. — Т. 27. — С. 94–107.
33. Кочергин В. В. Об аддитивных вычислениях систем целочисленных линейных форм // Вестник МГУ. Серия 1. Математика. Механика. — 1993. — № 6. — С. 97–101.

34. Кочергин В. В. О сложности вычислений в конечных абелевых, нильпотентных и разрешимых группах // Дискретная математика. — 1993. — Т. 5, № 1. — С. 91–111.
35. Кочергин В. В. О вычислении наборов степеней // Дискретная математика. — 1994. — Т. 6, № 2. — С. 129–137.
36. Кочергин В. В. Об одном классе аддитивных цепочек // Теоретические и прикладные аспекты математических исследований (сборник трудов конференции молодых ученых механико-математического факультета МГУ). — Москва: Изд-во МГУ, 1994. — С. 9–13.
37. Кочергин В. В. О сложности вычислений в конечных нильпотентных группах // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 1. — С. 43–51.
38. Кочергин В. В. О сложности вычисления систем одночленов с ограничениями на степени переменных // Дискретная математика. — 1998. — Т. 10, № 3. — С. 27–34.
39. Кочергин В. В. О мультипликативной сложности двоичных слов с заданным числом единиц // Математические вопросы кибернетики. Вып. 8. — М.: Наука, 1999. — С. 63–76.
40. Кочергин В. В. О двух обобщениях задачи об аддитивных цепочках // Труды IV Международной конференции «Дискретные модели в теории управляющих систем» (19–25 июня 2000 г.). — М., МАКС Пресс, 2000. — С. 55–59.
41. Кочергин В. В. О некоторых обобщениях задачи об аддитивных цепочках // Дискретная математика и ее приложения. Сборник лекций. — М.: Изд-во Центра прикладных исследований при механико-математическом факультете МГУ, 2001. — С. 59–83.
42. Кочергин В. В. О сложности вычисления пары одночленов от двух переменных // Дискретная математика. — 2005. — Т. 17, № 4. — С. 116–142.
43. Кочергин В. В. Об асимптотике сложности аддитивных вычислений систем целочисленных линейных форм // Дискретный анализ и исследование операций. Серия 1. — 2006. — Т. 13, № 2. — С. 38–58.
44. Кочергин В. В. О сложности вычисления систем одночленов от двух переменных // Труды VII Международной конференции «Дискретные модели в теории управляющих систем» (Покровское, 4–6 марта 2006 г.). — М.: МАКС Пресс, 2006. — С. 185–190.
45. Кочергин В. В. О сложности совместного вычисления двух элементов свободной абелевой группы // Материалы XVI Международной школы-семинара «Синтез и сложность управляющих систем» (Санкт-Петербург, 26–30 июня 2006 г.). — М.: Изд-во механико-математического факультета МГУ, 2006. — С. 54–59.
46. Кочергин В. В. О сложности вычисления системы из трех одночленов от трех переменных // Математические вопросы кибернетики. Вып. 15. — М.: ФИЗМАТЛИТ, 2006. — С. 79–155.
47. Кочергин В. В. О максимальной сложности совместного вычисления систем элементов свободной абелевой группы // Вестник МГУ. Серия 1. Математика. Механика. — 2007. — № 3. — С. 14–19.
48. Кочергин В. В. О сложности вычисления систем одночленов и систем целочисленных линейных форм // Дискретная математика и ее приложения. Сборник лекций молодежных научных школ по дискретной математике и ее приложениям. Выпуск III. — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 3–63.
49. Кочергин В. В. О сложности совместного вычисления трех элементов свободной абелевой группы с двумя образующими // Дискретный анализ и исследование операций. Серия 1. — 2008. — Т. 15, № 2. — С. 23–64.
50. Кочергин В. В. Об одном соотношении двух мер сложности вычисления систем одночленов // Вестник МГУ. Серия 1. Математика. Механика. — 2009. — № 4. — С. 8–13.
51. Кочергин В. В. О сложности аддитивных вычислений, использующих только операции вычитания // Труды VIII Международной конференции «Дискретные модели в теории управляющих систем» (Москва, 6–9 апреля 2009 г.). — М.: Издательский отдел факультета ВМиК МГУ имени М. В. Ломоносова; МАКС Пресс, 2009. — С. 174–179.
52. Кочергин В. В. О сложности вентильных схем с кратным числом путей // Материалы XVIII Международной школы-семинара «Синтез и сложность управляющих систем» имени академика О. Б. Лупанова (Пенза, 28 сентября – 03 октября 2009 г.). — М.: Изд-во механико-математического факультета МГУ, 2009. — С. 51–56.
53. Кочергин В. В. Задачи Р. Беллмана и Д. Кнута и их обобщения (Сложность аддитивных вычислений). — Saarbrücken: Palmarium academic publishing, 2012. — 396 с.
54. Кочергин В. В. О реализации недоопределенных матриц из двух столбцов вентильными схемами с кратными путями // Вестник Нижегородского университета им. Н. И. Лобачевского. — 2012. — № 5–2. — С. 111–116.

55. Кочергин В. В. Теория вентильных схем (современное состояние) // Дискретная математика и ее приложения. Сборник лекций молодежных научных школ по дискретной математике и ее приложениям. Выпуск VII. — М.: ИПМ им. М. В. Келдыша РАН, 2013. — С. 23–40.
56. Кочергин В. В. Уточнение оценок сложности вычисления одночленов и наборов степеней в задачах Беллмана и Кнута // Дискретный анализ и исследование операций. — 2014. — Т. 21, № 6. — С. 51–72.
57. Кочергин В. В. О некоторых мерах сложности конечных абелевых групп // Дискретная математика. — 2015. — Т. 27, № 3. — С. 25–43.
58. Кочергин В. В. О задачах Беллмана и Кнута и их обобщениях // Фундаментальная и прикладная математика. — 2015. — Т. 20, № 6. — С. 159–189.
59. Кочергин В. В., Кочергин Д. В. Уточнение асимптотического поведения сложности сборки слов схемами конкатенации // Вестник МГУ. Серия 1. Математика. Механика. — 2016. — № 2. — С. 12–18.
60. Кочергин В. В. Об одной задаче О. Б. Лупанова // Материалы XII Международного семинара «Дискретная математика и ее приложения» имени академика О. Б. Лупанова (Москва, МГУ, 20–25 июня 2016 г.) — М.: Изд-во механико-математического факультета МГУ, 2016. — С. 4–17.
61. Кочергин В. В., Кочергин Д. В. Уточнение нижней оценки сложности возведения в степень // Прикладная дискретная математика. — 2017. — № 38. — С. 119–132.
62. Кочергин В. В. Простое доказательство верхней оценки сложности вычисления трех одночленов трех переменных // Вестник МГУ. Серия 1. Математика. Механика. — 2019. — № 2. — С. 3–8.
63. Кочергин В. В. Сравнение сложности вычисления одночленов и элементов конечных абелевых групп // Вестник МГУ. Серия 1. Математика. Механика. — 2022. — № 3. — С. 6–11.
64. Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. Вып. 6. — М.: Наука, 1996. — С. 189–214.
65. Ложкин С. А. Асимптотические оценки высокой степени точности для сложности реализации булевских функций схемами из функциональных элементов // Труды II Международной конференции «Дискретные модели в теории управляющих систем» (23–28 июня 1997 г.). — Москва: Диалог-МГУ, 1997. — С. 37–39.
66. Лупанов О. Б. О вентильных и контактно-вентильных схемах // Доклады АН СССР. — 1956. — Т. 111, № 6. — С. 1171–1174.
67. Лупанов О. Б. Об одном методе синтеза схем // Известия вузов. Сер. Радиофизика. — 1958. — Т. 1, № 1. — С. 120–140.
68. Лупанов О. Б. О синтезе контактных схем // ДАН СССР. — 1958. — Т 119, № 1. — С. 23–26.
69. Лупанов О. Б. О сложности реализации функций алгебры логики формулами // Проблемы кибернетики. Вып. 3. — М.: Физматлит, 1960. — С. 61–80.
70. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып. 10. — М.: Физматгиз, 1963. — С. 63–97.
71. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. Вып. 14. — М.: Наука, 1965. — С. 31–110.
72. Лупанов О. Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. Вып. 23. — М.: Наука, 1970. — С. 43–81.
73. Лупанов О. Б. О синтезе схем из пороговых элементов // Проблемы кибернетики. Вып. 26. — М.: Наука, 1973. — С. 109–140.
74. Лупанов О. Б. О вентильных схемах // Acta Cybernetica. — 1980. — V. 4, № 4. — P. 311–315.
75. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.
76. Марков А. А. Об инверсионной сложности систем функций // Доклады АН СССР. — 1957. — Т. 116, № 6. — С. 917–919.
77. Мельхорн К. Некоторые замечания, касающиеся булевых сумм // Кибернетический сборник. Вып. 18. — М.: Мир, 1981. — С. 39–45.
78. Мерекин Ю. В. Нижняя оценка сложности для схем конкатенации слов // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 1. — С. 52–56.

79. Мерекин Ю. В. Нижние оценки мультипликативной сложности символьных последовательностей, определяемых монотонными симметрическими булевыми функциями // Дискретный анализ и исследование операций. Серия 1. — 1999. — Т. 6, № 3. — С. 3–9.
80. Мерекин Ю. В. Оценки мультипликативной сложности двоичных слов, определяемых поясковыми булевыми функциями // Дискретный анализ и исследование операций. Серия 1. — 2002. — Т. 9, № 2. — С. 36–47.
81. Мерекин Ю. В. О порождении слов с использованием операции композиции // Дискретный анализ и исследование операций. — 2003. — Т. 10, № 4. — С. 70–78.
82. Мерекин Ю. В. Об аддитивной сложности частично коммутативных слов // Дискретный анализ и исследование операций. Серия 1. — 2005. — Т. 12, № 4. — С. 40–50.
83. Митягин Б. С., Садовский Б. Н. О линейных булевских операторах // Доклады АН СССР. — 1965. — Т. 165, № 4. — С. 773–776.
84. Нечипорук Э. И. О сложности схем в некоторых базисах, содержащих нетривиальные элементы с нулевыми весами // Проблемы кибернетики. Вып. 8. — М.: Физматгиз, 1962. — С. 123–160.
85. Нечипорук Э. И. О вентильных схемах // Доклады АН СССР. — 1963. — Т. 148, № 1. — С. 50–53.
86. Нечипорук Э. И. О синтезе вентильных схем // Проблемы кибернетики. Вып. 9. — М.: Физматгиз, 1963. — С. 37–44.
87. Нечипорук Э. И. О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // Доклады АН СССР. — 1965. — Т. 163, №1. — С. 40–42.
88. Нечипорук Э. И. О синтезе логических сетей в неполных и вырожденных базисах // Проблемы кибернетики. Вып. 14. — М.: Наука, 1968. — С. 111–160.
89. Нечипорук Э. И. О топологических принципах самокорректирования // Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 5–102.
90. Нечипорук Э. И. Об одной булевской матрице // Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 237–240.
91. Нигматуллин Р. Г. Сложность булевых функций. — М.: Наука, 1991.
92. Олег Борисович Лупанов (к шестидесятилетию со дня рождения) // Методы дискретного анализа в теории графов и сложности. Сборник научных трудов. Вып. 52.— Новосибирск, 1992. — С. 3–14.
93. Ольшанский А. Ю. О сложности вычислений в группах // Соросовский образовательный журнал. — 2000. — Т. 6, №3. — С. 118–123.
94. Орлов В. А. Реализация «узких» матриц вентильными схемами // Проблемы кибернетики. Вып. 22. — М.: Наука, 1970. — С 45–52.
95. Потапов В. Н. Аддитивная сложность слов с ограничениями на состав подслов // Дискретный анализ и исследование операций. Серия 1. — 2004. — Т. 11, № 1. — С. 52–78.
96. Потапов В. Н. О максимальной длине двоичных слов с ограниченной частотой единиц и без одинаковых подслов заданной длины // Дискретный анализ и исследование операций. Серия 1. — 2004. — Т. 11, № 3. — С. 48–58.
97. Сэвидж Д. Е. Сложность вычислений. — М.: Изд-во «Факториал», 1998.
98. Сенета Е. Правильно меняющиеся функции. — М.: Наука, 1985.
99. Сергеев И. С. О сложности градиента рациональной функции // Дискретный анализ и исследование операций. Серия 1. — 2007. — Т. 14, № 4. — С. 57–75.
100. Сергеев И. С. Вентильные схемы ограниченной глубины // Дискретный анализ и исследование операций. — 2018. — Т. 25, № 1. — С. 120–141.
101. Сидоренко А. Ф. Сложность аддитивных вычислений семейств целочисленных линейных форм // Записки научных семинаров ЛОМИ. Т. 105.— Л.: Наука, 1981. — С. 53–61.
102. Слисенко А. О. Сложностные задачи теории вычислений // Успехи математических наук. — 1981. — Т. 36, №6. — С. 21–103.
103. Смарт Н. Криптография. — М.: Техносфера, 2005.
104. Страница кафедры дискретной математики механико-математического факультета МГУ имени М. В. Ломоносова. Рукопись О. Б. Лупанова из личного архива В. В. Кочергина. URL: http://new.math.msu.su/department/dm/data/uploads/zapisi_ob.pdf (дата обращения 22.07.2022).
105. Трусевич Е. Н. О сложности реализации схемами композиции систем из двух мономов от двух переменных // Материалы VIII молодежной научной школы по дискретной

математике и ее приложениям. (Москва, 24–29 октября 2011 г.). Часть 2. — М., 2011. — С. 40–44.
106. Трусевич Е. Н. О сложности вычисления некоторых систем одночленов схемами композиции // Вестник МГУ. Серия 1. Математика. Механика. — 2014. — № 5. — С. 18–22.
107. Холл М. Комбинаторика. — М.: Мир, 1970.
108. Храпченко В. М. Нижние оценки сложности схем из функциональных элементов // Кибернетический сборник. Новая серия. Вып. 21. — М.: Мир, 1984. — С. 3–54.
109. Чандрасекхаран К. Введение в аналитическую теорию чисел. — М.: Мир, 1974.
110. Чашкин А. В. О сложности булевых матриц, графов и соответствующих им булевых функций // Дискретная математика. — 1994. — Т. 6, № 2. — С. 44–73.
111. Ширшов А. И. Некоторые алгоритмические проблемы для алгебр Ли // Сибирский математический журнал. — 1962. — Т. 3, № 2. — С. 292–296.
112. Шоломов Л. А. О функционалах сложности, характеризующих сложность систем недоопределенных булевых функций // Проблемы кибернетики. Вып. 19. — М.: Наука, 1967. — С. 123–140.
113. Эндрюс Г. Теория разбиений. — М.: Наука, 1982.
114. Яблонский С. В. Об алгоритмических трудностях синтеза минимальных контактных схем // Проблемы кибернетики. Вып. 2. — М.: Физматгиз, 1959. — С. 75–121.
115. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.
116. Alon N., Rónyai L., Szabó T. Norm-graphs: variations and applications // J. Combinat. Theory. Ser. B. — 1999. — V. 76, No 3. — P. 280–290.
117. Althöfer I. Tight lower bounds on the length of word chains // Inform. Process. Lett. — 1990. — V. 34, № 5. — P. 275–276.
118. Arnold A., Brlek S. Optimal word chains for the Thue-Morse word // Inform. and Comput. — 1989. — V. 83, No 2. — P. 140–151.
119. Bellman R. E. Addition chains of vectors (Advanced problem 5125) // Amer. Math. Monthly. — 1963. — V. 70. — P. 765.
120. Bergeron F., Berstel J., Brlek S., Duboc C. Addition chains using continued fractions // Journal of Algorithms. — 1989. — V. 10, No 3. — P. 403–412.
121. Bernstein D. J. Pippenger's exponentiation algorithm // Персональная страница Д. Ж. Бернштейна, 2002. URL: http://cr.yp.to/papers/pippenger.pdf (дата обращения 22.07.2022).
122. Bernstein D. J. The transposition principle // Персональная страница Д. Ж. Бернштейна, 2004. URL: http://cr.yp.to/transposition.html (дата обращения 22.07.2022).
123. Berstel J., Brlek S. On the lenght of word chains // Inform. Process. Lett. — 1987. — V. 26, No 1. — P. 23–28.
124. Bosma W. Signed bits and fast exponentiation // Journal de Théorie des Nombres de Bordeaux. — 2001. — V. 13. — P. 27–41.
125. Bostan A., Lecerf G., Schost E. Tellegen's principle into practice // ISSAC Conf. — Philadelphia: ACM Press, 2003. — P. 37–44.
126. Bos J., Coster M. Addition chain heuristics // Proceedings of Crypto'89. — Springer-Verlag, 1990. — V. 435. — P. 400–407.
127. Bordewijk J. L. Inter-reciprocity applied to electrical networks // Applied Scientific Research B: Electrophysics, Acoustics, Optics, Mathematical Methods. — 1956. — V. 6. — P. 1–74.
128. Bousquet-Mélou M. The number of minimal word chains computing the Thue-Morse word // Inform. Process. Lett. — 1992. — V. 44, No 2. — P. 57–64.
129. Brauer A. On addition chains // Bull. Amer. Math. Soc. — 1939. — V. 45. — P. 736–739.
130. Brickell E. F., Gordon D. M., McCurley K. S., Wilson D. B. Fast exponentiation with precomputation: algorithms and lower bounds. — Preprint, 1995.
131. Brickell E. F., Gordon D. M., McCurley K. S., Wilson D. B. Fast exponentiation with precomputation. // Proceedings of Eurocrypt'92. — Springer-Verlag, 1992. — V. 658. — P. 200–207.
132. de Bruijn N. G. A combitorial problem // Nederl. Akad. Wetensch. Proc. — 1946. — V. 49. — P. 758–764.
133. Byrne A., Meloni N., Crowe F., Marnane W. P., Tisserand A., Popovici E. M. SPA resistant elliptic curve cryptosystem using addition chains // International Conference on Information Technology-ITNG'07. — 2007. — P. 995–1000.
134. Clift N. M. Calculating optimal addition chains // Computing. — 2011. — V. 91. — P. 265–284.

135. Coster M. J. Some algorithms on addition chains and their complexity. — CWI Report CS-R9024, 1990.
136. Datta B., Singh A. N. History of Hindi Mathematics. — Bombay, 1935.
137. Diwan A. A. A new combinatorial complexity measure for languages. — Tata Institute. Bombay, India, 1986.
138. Dobkin D., Lipton R. J. Addition chain methods for the evaluation of specific polynomials // SIAM J. Comput. — 1980. — V. 9. — P. 121–125.
139. Downey P., Leong B., Sethi R. Computing sequences with addition chains // SIAM Journal on Computing. — V. 10. — 1981. — P. 638–646.
140. de Rooij P. Efficient exponentiation using precomputation and vector addition chains // Proceedings of Eurocrypt'94. — Springer-Verlag, 1994. — V. 950. — P. 389–399.
141. Eisentrager K., Lauter K., Montgomery P. L. Fast elliptic curve arithmetic and improved Weil Pairings evaluation // Proceedings of RSA-CT 2003.
142. Elias M., Neri F. A note on addition chains and some related conjectures // Sequences. Editor R. M. Capocelli. — Springer-Verlag, 1990. — P. 166–181.
143. Erdos P. Remarks on number theory, III: On addition chains // Acta Arith. — 1960. — V. 6. — P. 77–81.
144. Fiduccia C. M. On the algebraic complexity of matrix multiplication. — Brown university, Providence, 1973.
145. Find M., Göös M., Järvisalo M. et al. Separating OR, SUM, and XOR circuits // J. Computer System Sci. — 2016. — V. 82, No 5. — P. 793–801.
146. Von zur Gathen J., Nocker M. Exponentiation in finite fields: theory and practice // Lecture Notes Computer Sci. — 1997. — V. 1255. — P. 88–113.
147. Gordon D. M. A survey of fast exponentiation methods // Journal of Algorithms. — 1998. — V. 27. — P. 129–146.
148. Goundar R. R., Shiota K., Toyonaga M. New strategy for doubling-free short addition-subtraction chain // International Journal of Applied Mathematics. — 2007. — V. 2, No 3.
149. Graham R. L., Yao A. C.-C., Yao F.-F. Addition chains with multiplicative cost // Discrete Math. — 1978. — V. 23. — P. 115–119.
150. Hebb K. R. Some results on addition chains // Notices of the American Mathematical Society. — 1974. — V. 21. — P. A-294.
151. Järvinen K., Dimitrov V. and Azarderakhsh R. A generalization of addition chains and fast inversions in binary fields // IEEE Transactions on Computers. — 2015. — V. 64(9). — P. 2421–2432.
152. Jukna S., Sergeev I. Complexity of linear Boolean operators // Found. and Trends in Theor. Comput. Sci. — 2013. — V. 9, No 1. — P. 1–123.
153. Kaltofen E., Shoup V. Subquadratic-time factoring of polynomials over finite fields // Math. Comput. — 1998. — V. 67, No 223. — P. 1179–1197.
154. Kaminski M., Kirkpatrick D., Bshouty N. Addition requirements for matrix and transposed matrix products // Journal of Algorithms. — 1988. — T. 9, No 3. — C. 354–364.
155. Knuth D. E., Papadimitriou C. H. Duality in addition chains // Bulletin of the European association for Theoretical Computer Science. — 1981. — V. 13. — P. 2–4.
156. Kobayashi K., Morita H., Hakuta M. Multi scalar-multiplication algorithm over elliptic curve // IEICE Transactions on Information and Systems. — 2001. — V. E84-D, No 2. — P. 271–276.
157. Koblitz N. Elliptic curve cryptosystems // Mathematics of Computation. — 1987. — V. 48(177). — P. 203–209.
158. Kochergin V. V. Some generalizations of addition chains problem // Proceedings of two joint French-Russian seminars on combinatorial and algorithmical properties of discrete structures (April 1998, Moscow — February 1999, Nansy, France). Project No 8/97. — French-Russian A. M. Liapunov Institute, 2001. — P. 33–41.
159. Kóllar J., Rónyai L., Szabó T. Norm-graphs and bipartite Turán numbers // Combinatorica. — 1996. — V. 16, No 3. — P. 399–406.
160. Koyama K., Tsuruoka Y. A signed binary window method for fast computing over elliptic curves // IEICE Trans. Fundamentals. — 1993. — V. E76-A. — P. 55–62.
161. Kunihiro N., Yamamoto H. Window and extended window methods for addition chain and addition-subtraction chain // IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. — 1998. — V. E81-A, No 1. — P. 72–81.

162. Kunihiro N., Yamamoto H. New method for generating short addition chains // IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. — 2000. — V. E83-A, No 1. — P. 60–66.
163. Kweon K., Hong S.-M., Oh S.-Y., Yoon H. Finding shorter addition/subtraction-chains // CCCT'05 (International Conference on Computing, Communications and Control Technologies). URL: http://hdl.handle.net/10203/447 (дата обращения 22.07.2022).
164. Lamagna E. A., Savage J. E. Computational complexity of some monotone functions // Proc. 15th SWAT Conference. — Long Beach: IEEE Comput. Soc. Press, 1974. — P. 140–144.
165. McCarthy D. P. Effect of improved multiplication efficiency on exponentiation algorithms derived from addition chains // Math. Comp. — 1976. — V. 46. — P. 603–608.
166. McCarthy D. P. The optimal algorithm to evaluate x^n using elementary multiplication methods // Math. Comp. — 1977. — V. 31 (137). — P. 251–256.
167. McColl W. F., Paterson M. S. The depth of all Boolean functions // SIAM J. Comput. — 1977. — V. 6, No 2. — P. 373–380.
168. Merekin Yu. V. Some bounds on the complexity of words // Southeast Asian Bulletin of Mathematics. — 2006. — V. 30. — P. 1081–1121.
169. Morain F., Olivos J. Speeding up the computation on an eliptic curve using addition-subsraction chains // Informatique Théorique et Applications. — 1990. — V. 24. — P. 531–544.
170. Morgenstern J. Note on a lower bound of the linear complexity of the fast Fourier transform // J. Assoc. Comput. Mach. — 1973. — V. 20. — P. 305–306.
171. Morgenstern J. On linear algorithms // Theory of machines and computations. — New York, 1971. — P. 59–66.
172. Nedjah N., Mourelle L. Minimal addition-subtraction chains using genetic algorithm // Advances in Information Systems. Lecture Notes in Computer Science. — 2002. — V. 2457. — P. 303–313.
173. Olivos J. On vectorial addition chains // J. Algorithms. — 1981. — V. 2, No 1. — P. 13–21.
174. Pippenger N. On evaluation of powers and related problems // Proc. 17^{th} Ann. IEEE Symp. on Found. of Computer Sci. (Houston, TX, 25–27 Oct. 1976.) — P. 258–263.
175. Pippenger N. The mimimum number of edges in graphs with prescribed paths // Math. Systems Theory. — 1979. — V. 12, No. 4. — P. 325–346.
176. Pippenger N. On another Boolean matrix // Theoretical Computer Science. — 1980. — V. 11, I 1. — P. 49–56.
177. Pippenger N. On evaluation of powers and monomials // SIAM J. Comput. — 1980. — V. 9, No 2. — P. 230–250.
178. Red'kin N. P. Complexity of concatenation schemes for words from some classes // Proceedings of two joint French-Russian seminars on combinatorial and algorithmical properties of discrete structures (April 1998, Moscow — February 1999, Nansy, France). Project No 8/97. — French-Russian A. M. Liapunov Institute, 2001. — P. 107–114.
179. Riordan J., Shannon C. E. The number of two-terminal series-parallel networks // J. Math. Phys. Mass. Inst. Tech. — 1942. — V. 21. No 2. — P. 83–93. Рус. пер.: Риодан Дж., Шеннон К. Число двухполюсных параллельно-последовательных сетей // В сборнике: Шеннон К. Работы по теории информации и кибернетике. — М.: ИЛ, 1963. — С. 46–58.
180. Savage J. E. An algorithm for the computation of linear forms // SIAM J. Comput. — 1974. — V. 3, No 2. — P. 150–158.
181. Scholz A. Jahresbericht // Deutsche Mathematiker-Vereinigung. — 1937. — V. 47. — P. 41–42.
182. Schönhage A. A lower bound for the lenght of addition chains // Theoretical Computer Science. — 1975. — V. 1. — P. 1–12.
183. Shannon C. E. The synthesis of two-terminal switching circuits // Bell Syst. Techn. J. — 1949. — V. 28, No 1. — P. 59–98. (Русский перевод: Шеннон К. Работы по теории информации и кибернетике. — М.: ИЛ, 1963. — С. 59–101.)
184. Southard T. H. Addition chains for the first N squares // Tech. Rep. CNA-84, Univ. of Texas at Austin, 1974.
185. Stam M. Speeding up subgroup cryptosystems. — Eindhoven: Technische Universiteit Eindhoven, 2003.
186. Strassen V. Berechnungen in partiellen Algebren endlichen Typs // Computing. — 1973. — V. 11. — P. 181–196.

187. Straus E. G. Addition chains of vectors // Amer. Math. Monthly. — 1964. — V. 71. — P. 806–808.
188. Subbarao M. V. Addition chains — some results and problems // Number Theory and Applications. Editor R. A. Mollin. NATO Advanced Science Institutes Series: Series C. — Kluwer Academic Publisher Group, 1989. — V. 265. — P. 555–574.
189. Tarjan T. G. Complexity of lattice-configurations // Studia Sci. Math. Hungar. — 1975. — V. 10. — P. 203–211.
190. Tarjan T. G. Complexity of monotone networks for computing conjunctionns // Ann. Discrete Math. — 1978. — No 2. — P. 121–133.
191. Thurber E. G. The Scholz — Brauer problem on addition chains // Pacific Journal of Mathematics. — 1973. — V. 40. — P. 229–242.
192. Thurber E. G. Addition chains — an erratic sequence // Discrete Mathematics. — 1993. — V. 122. — P. 287–305.
193. Thurber E. G. Efficient generation of minimal length addition chains // SIAM Journal of Computing. — 1999. — V. 28. — P. 1247–1263.
194. Thurber E. G., Clift N. M. Addition chains, vector chains, and efficient computation // Discrete Mathematics. — 2021. — V. 344. — 112200.
195. Toundar R. R., Shiota K., Toyonaga M. New strategy for doubling-free short addition-substruction chain // International Journal of Applied Mathematics. — 2007. — V. 2, No 3.
196. Tsai Y., Chin Y. A study of some addition chain problems // Intern. J. Computer Math. — 1987. — V. 22. — P. 117–134.
197. Vassiliev N. N. Complexity of monomial evaluations and duality // Computer algebra in scientific computing — CASC'99 (Munich). — Berlin: Springer, 1999. — P. 479–484.
198. Volger H. Some results on addition/subtraction chains // Information Processing Letters. — 1985. — V. 20. — P. 155–160.
199. Walter C. D. Exponentiation using division chains // IEEE Transactions on Computers. — 1998. — V. 47 (7). — P. 757–765.
200. Yacobi Y. Exponentiating faster with addition chains // Eurocrypt'90. — 1991. — P. 222–229.
201. Yao A. C.-C. On the evaluation of powers // SIAM J. Comput. — 1976. — V. 5. — P. 100–103.

Поступило в редакцию 22 IV 2022,
окончательный вариант 21 VII 2022.