Новые результаты в задачах Р. Беллмана и Д. Кнута

В. В. Кочергин*

В работе рассматриваются задача Беллмана о сложности (минимально возможном числе операций умножения, достаточном для вычисления) одночлена от m переменных и задача Кнута о сложности вычисления набора из m степеней одной переменной. Для любого фиксированного действительного числа $a \geq 2$ и любой положительной функции $\varphi(m)$, удовлетворяющей условию $|\log \varphi(m)| = o(\log m)$, установлены асимптотически точные оценки соответствующих функций Шеннона, характеризующих максимально возможную сложность при ограничении показателей величиной $A = \varphi(m)m^a$. Эти функции при $m \to \infty$ асимптотически равны am и $(a-1)m$ соответственно.

Ключевые слова: аддитивные цепочки, векторные аддитивные цепочки, задача Беллмана, задача Кнута, схемная сложность.

1. Постановка задачи, известные результаты, формулировка основной теоремы

В работе рассматриваются два обобщения классической задачи об эффективном возведении в степень, которая заключается в нахождении по натуральному n сложности $l(x^n)$ вычисления степени x^n, т. е. минимального числа умножений, достаточного для возведения переменной x произвольной природы в степень n. При вычислениях предполагается, что результаты промежуточных вычислений могут использоваться многократно, а от операции, названной «умножением», требуется лишь ассоциативность. В аддитивной постановке эта задача известна как задача об аддитивных цепочках — см., например, [3].

В 1939 году А. Брауэр [18] установил для величины $l(x^n)$ при $n \to \infty$ асимптотическую формулу[1]

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

* *Кочергин Вадим Васильевич* — зав. каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: vvkoch@yandex.ru, ORCID: 0000-0002-7798-9502.

Kochergin Vadim Vasil'evich — Head of Chair of Discrete Mathematics, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics.

[1] Здесь и далее запись $\log x$ без указания основания логарифма означает $\log_2 x$.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

дополнив очевидную нижнюю оценку через двоичный логарифм следующей верхней оценкой:

$$l(x^n) \le \log n + \frac{\log n}{\log\log n}\,(1 + o(1))\,.$$

В 1960 г. П. Эрдёш показал [21], что для почти всех n эта верхняя оценка, записанная в таком виде, в некотором смысле неулучшаема, а именно, для почти всех n справедливо асимптотическое равенство

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

В 1963 г. Р. Беллман [17] (для случая $m = 2$), а затем в 1964 г. Е. Штраус [28] (для произвольного m) сформулировали задачу[2] о сложности вычисления одночлена от m переменных, т. е. нахождения величины $l(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m})$. Эту задачу, следуя [26,29], 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 возможное число r добавленных векторов в последовательности m-мерных векторов (наборов)

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

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

В 1969 г. Д. Кнут [2, разд. 4.6.3., упр. 32] поставил задачу о сложности вычисления m степеней одной переменной, т. е. нахождения величины $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$. Эту задачу обычно называют (см., например, [9,24]) *задачей Кнута*. Очевидно, что величина $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$ численно равна минимально возможной длине аддитивной цепочки для числа $\max_i n_i$, 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 в 1980 г. Н. Пиппенджером [26] задачи о сложности вычисления системы из p одночленов от q переменных.

[2] В задаче о сложности вычисления одночлена дополнительно предполагается коммутативность умножения.

В 1964 г. Е. Штраус [28] показал, что для любого фиксированного m при условии $\sum n_i \to \infty$ 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 [30] для любого фиксированного m при условии $\sum n_i \to \infty$ установил аналогичную формулу для сложности вычисления набора из m степеней:

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

В 1981 г. независимо А. Ф. Сидоренко [15], Дж. Оливосом [23], а также Д. Кнутом и К. Пападимитриу [22] 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*. В силу этой связи большинство оценок будет выписываться для одной из двух задач. Заметим, что добавление в вычисляемый набор степени с уже имеющимся показателем не меняет значения сложности в задаче Кнута, а добавление переменной с тем же положительным показателем увеличивает сложность задачи Беллмана на единицу, и при переходе к набору различных показателей следует учитывать изменение числа его компонент.

Также в 1981 г. в работе [20] установлено, что задача распознавания по набору натуральных чисел $(n_1, n_2, \dots, n_m, l)$ существования аддитивной цепочки, имеющей длину l и содержащей числа $n_1, n_2, \dots, n_m$, является NP-полной. Поэтому под решением задач Беллмана и Кнута естественно подразумевать не нахождение точного значения сложности, а получение асимптотически точных оценок, как, например, для исходной задачи возведения в степень.

Асимптотическая постановка задачи естественным образом также приводит к задаче исследования поведения соответствующих функций Шеннона, которые для задач Беллмана и Кнута определяются соответственно равенствами

$$L_B(n_1, n_2, \dots, n_m) = \max l(x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}),$$
$$L_K(n_1, n_2, \dots, n_m) = \max l(x^{k_1}, x^{k_2}, \dots, x^{k_m}),$$

где максимумы берутся по всем ненулевым наборам $(k_1, k_2, \ldots, k_m)$ целых неотрицательных чисел, удовлетворяющих неравенствам $k_i \le n_i$, $i = 1, 2, \ldots, m$.

Нулевые показатели в задаче Кнута не требуют вычислений; единичный элемент считается доступным бесплатно. В задаче Беллмана переменные с нулевыми показателями исключаются из одночлена. Для действительных значений $n_i \ge 1$ те же определения означают максимум по целым неотрицательным k_i, не превосходящим $\lfloor n_i \rfloor$.

Далее, говоря об асимптотических оценках, будем полагать, что рассматриваются последовательности наборов натуральных чисел $\tilde{n}(s) = \big(n_1(s), n_2(s), \ldots, n_{m(s)}(s)\big)$, $s = 1, 2, \ldots$, удовлетворяющие условию

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

При этом параметр s будем обычно опускать. Условие попарной различности показателей, когда оно необходимо, будет оговариваться отдельно. К аргументам функций Шеннона это условие не относится.

При фиксированном m (числе переменных в одночлене или числе вычисляемых степеней соответственно) для задач Беллмана и Кнута асимптотически точное решение было найдено Е. Штраусом и А. Яо. 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 из них заключается в установленном в работах [19, 27] асимптотически точном решении для одного частного случая, упоминавшегося Д. Кнутом при постановке общей задачи, — когда набор показателей степеней является последовательностью квадратов натуральных чисел от 1 до m:

$$l\left(x^1, x^4, x^9, \ldots, x^{m^2}\right) = m + O\left(\frac{m}{\sqrt{\log m}}\right)$$

при $m \to \infty$.

Второй результат, полученный в 1976 г. Н. Пиппенджером [24], состоит в следующем асимптотическом равенстве при $n \ge 2$, $m \log n \to \infty$:

$$L_K(\underbrace{n, n, \ldots, n}_{m \text{ раз}}) = \log n + (1 + o(1))\frac{m \log n}{\log(m \log n)} + O(m).$$

Продвижения в вопросе получения асимптотики сложности для задачи Беллмана — Кнута при растущем числе переменных или степеней были получены в начале 90-х годов прошлого века.

Сначала в работе автора [7] на основе собственной вентильной конструкции из [4, 5], использующей результаты Пиппенджера [24, 25], которые, в свою очередь, существенно опираются на работы [10, 13, 14], было установлено соотношение

$$L_B(n_1, n_2, \ldots, n_m) = \frac{\log N}{\log\log N}\left(1 + O\left(\left(\frac{\log\log\log N}{\log\log N}\right)^{1/2}\right)\right) + \\ + O(m + \log\max n_i),$$

где $N = n_1 n_2 \ldots n_m$. Здесь и далее в этом разделе предполагается, что выполняется условие $N \to \infty$.

В 1992 г. С. Б. Гашковым и автором [1] верхняя оценка из предыдущего асимптотического равенства была усилена следующим образом:

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

где $N = n_1 n_2 \ldots n_m$.

Эта верхняя оценка вместе с простыми нижними оценками

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

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

справедливыми для всех наборов $(n_1, n_2, \ldots, n_m)$, а также с «мощностной» нижней оценкой (см., например, [12]), дает 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 [6] удалось восполнить этот пробел, в некотором смысле объединив в одну нижнюю оценку «мощностную» оценку и оценку через $\log(\max n_i)$. Было доказано, что найдутся такие положительная константа c и функция $f(x)$, стремящаяся к 0 при $x \to \infty$, что доля наборов $(k_1, k_2, \ldots, k_m)$, где $k_1 \le n_1$, $k_2 \le n_2, \ldots, k_m \le n_m$, для которых выполняются соотношения

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

стремится к единице при $N \to \infty$, где $N = n_1 n_2 \dots n_m$.

В качестве функции $f(x)$ в этой нижней оценке можно взять функцию $2(\log\log x)^{-1/2}$.

Последний результат дает асимптотически точное решение задач Беллмана и Кнута при стандартном условии — «сложность (число операций) существенно больше числа полюсов (суммы «входов» и «выходов», в данном случае $m+1$)» — действительно, при таком условии для почти всех исследуемых объектов (наборов) верхняя оценка асимптотически совпадает с нижней.

Однако в случае, когда условие «число переменных или степеней существенно меньше суммы логарифма максимальной степени и мощностного слагаемого» не выполняется, эти задачи остались нерешенными. Значительным продвижением в этом направлении стал в 2014 г. один из результатов работы [8]. К сожалению, в формулировку этой теоремы в [8] вкралась опечатка. Дадим здесь правильную формулировку того утверждения, которое доказано в [8].

Ниже эта оценка приводится в необходимом нам частном случае: число попарно различных показателей стремится к бесконечности. Тогда $N \geq m!$, а основание $m/(f(m))^2$ при достаточно больших m превосходит единицу; все логарифмы в формулах определены.

Теорема 1 ([8]). *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 попарно различных натуральных чисел*

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

удовлетворяющей условию

$$m(s) \to \infty,$$

выполняются неравенства

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

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

где $N = n_1 n_2 \dots n_m$.

Отметим, что в этой теореме отличие оценок сложности для задач Беллмана и Кнута на величину $m-1$ становится существенным.

Применим теорему 1 к задаче Кнута в случае, когда попарно различные натуральные показатели $n_1,\dots,n_m$ не превосходят m^a, где $a>1$ — фиксированное число. Тогда

$$m!\le N\le m^{am},\qquad \log\log N=\log m+O(\log\log m).$$

Из условия $\log f(m)=o(\log m)$ следует

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

При достаточно больших m имеем

$$\log_{m/(f(m))^2} n_i\le\frac{a\log m}{\log m-2\log f(m)}<\lfloor a\rfloor+1,$$

поскольку $a<\lfloor a\rfloor+1$. Учитывая также $\log(\max n_i)=O(\log m)=o(m)$, из теоремы 1 получаем

$$l(x^{n_1},\dots,x^{n_m})\le\sum_{i=1}^{m}\left\lceil\log_{m/(f(m))^2} n_i\right\rceil-m+o(m)\le(\lfloor a\rfloor)m+o(m).$$

Эту оценку можно получить и непосредственно, без предположения о различности показателей и использования теоремы 1 (на самом деле излагаемый ниже способ — иллюстрация метода доказательства теоремы 1). Заметим, что при всех достаточно больших значениях m любое число, не превосходящее m^a, будет не более чем $(\lfloor a\rfloor+1)$-разрядным в системе счисления по основанию $d=\lceil m/\log m\rceil$. Поэтому с использованием $O(m/\log m)$ операций умножения можно вычислить степени

$$x^2,x^3,\dots,x^d;\ x^{2d},x^{3d},\dots,x^{d^2};\dots;x^{2d^{\lfloor a\rfloor}},x^{3d^{\lfloor a\rfloor}},\dots,x^{d^{\lfloor a\rfloor+1}},$$

а затем из них получить все степени x^{n_i}, затратив не более чем $\lfloor a\rfloor$ операций умножения на каждую степень.

Нижнюю оценку для функции Шеннона $L_K(n_1,n_2,\dots,n_m)$ установим через оценку для функции Шеннона $L_B(n_1,n_2,\dots,n_m)$, для которой можно использовать стандартные мощностные рассуждения (см., например, [12]), которые дают оценку

$$L_B(\underbrace{m^a,m^a,\dots,m^a}_{m\text{ раз}})\ge am-o(m).$$

Учитывая двойственность задач Беллмана и Кнута, имеем:

$$(a-1)m - o(m) \le L_K(\underbrace{m^a, m^a, \ldots, m^a}_{m \text{ раз}}) \le (\lfloor a \rfloor)m + o(m).$$

В предположении, что все показатели степени n_i различны, при $a < 1$ задачи вырождаются. При $a = 1$ имеем точное равенство

$$L_K(\underbrace{m, \ldots, m}_{m \text{ раз}}) = m - 1.$$

Для значений a, удовлетворяющих неравенствам $1 < a < 2$, тривиальный факт о том, что на вычисление m различных степеней требуется не менее $m - 1$ операции умножения, дает нижнюю оценку, асимптотически совпадающую с установленной верхней оценкой. При $a \ge 2$ нижняя и верхняя оценки близки, но, вообще говоря, имеют разную асимптотику (разные коэффициенты в линейных оценках). Основным результатом данной работы, устраняющим этот разрыв, является

Теорема 2. *Пусть* $\varphi(m) > 0$, $|\log \varphi(m)| = o(\log m)$ *при* $m \to \infty$, $a \ge 2$ — *фиксированное действительное число,* $A = A(m) = \varphi(m)m^a$. *Тогда*

$$L_K(\underbrace{A, A, \ldots, A}_{m \text{ раз}}) \sim (a-1)m, \quad L_B(\underbrace{A, A, \ldots, A}_{m \text{ раз}}) \sim am.$$

В следующих трех разделах дано сжатое, но полное доказательство этой теоремы.

2. Нижняя оценка

Нижняя оценка доказывается стандартными мощностными рассуждениями. При ее доказательстве будем использовать язык схем из функциональных элементов (см., например, [9, 11]), т. е. в качестве вычислительной модели будем рассматривать схемы из двухвходовых элементов умножения. При таком подходе сложность вычисления одночлена или системы степеней — это минимально возможное число элементов в реализующей их схеме.

Хорошо известно (см., например, [12]), что количество схем с m входами, одним выходом, сложности не более l, состоящих из двухвходовых элементов, среди которых нет дублирующих и висящих, при $l \ge m$ не превосходит величины $(c(l+m))^l$ для некоторой абсолютной положительной константы c.

Зафиксируем произвольное значение ε, $0 < \varepsilon < 1$. Положим $l_\varepsilon = (a-\varepsilon)m$. В силу неравенства $a \geq 2$ выполняется соотношение $l_\varepsilon \geq m$. Покажем, что при всех достаточно больших значениях m количество описанных схем сложности не более l_ε меньше числа одночленов от m переменных с положительными показателями степени не более A. Действительно,

$$\log \frac{(c(l_\varepsilon + m))^{l_\varepsilon}}{\lfloor A \rfloor^m} \leq (a-\varepsilon)m \log m + O(m) - m \log \left(\lfloor \varphi(m) m^a \rfloor\right) =$$
$$= -\varepsilon m \log m + O(m) - m \log \varphi(m) = -\varepsilon m \log m + o(m \log m),$$

где последнее выражение стремится к $-\infty$ при $m \to \infty$. Следовательно, при всех достаточно больших значениях m выполняется неравенство

$$L_B(\underbrace{A, A, \ldots, A}_{m \text{ раз}}) > (a-\varepsilon)m,$$

которое в силу произвольности ε устанавливает нижнюю оценку теоремы 2 для задачи Беллмана. Необходимая оценка для задачи Кнута следует из соображений двойственности.

3. Комбинаторная лемма

В этом разделе будет установлена техническая комбинаторная лемма, на основе которой будет доказана верхняя оценка теоремы 2. Базовая идея была почерпнута из работы [16].

Лемма 1. *Пусть M, k, t, B — натуральные числа, для которых выполняются соотношения*

$$1 \leq B < M, \qquad M \geq 4t, \qquad \left\lfloor \frac{M}{4t} \right\rfloor \left(\frac{B}{2M(k+t)} \right)^{1+\frac{k}{t}} \geq 4.$$

Тогда существует подмножество U множества $\{1, 2, \ldots, 2M\}$, удовлетворяющее условиям:

1) $|U| \leq 8B(k+t)\lceil \log_3(4(2M)^k) \rceil$;

2) *для каждого набора $w = (w_1, w_2, \ldots, w_k)$, $w_i \in \{M, M+1, \ldots, 2M-1\}$, $i = 1, 2, \ldots, k$, найдутся такие целые числа $\xi_1, \xi_2, \ldots, \xi_t$, что выполняются условия:*

$$0 = \xi_0 < \xi_1 < \xi_2 < \ldots < \xi_t \leq M/4,$$
$$\xi_i - \xi_{i-1} \in U \quad (1 \leq i \leq t),$$
$$w_j - \xi_{\sigma(j)} \in U \quad (1 \leq j \leq k),$$

где $\sigma(j)$ — наименьшее i, такое что $j \leq \lfloor \frac{ik}{t} \rfloor$.

Доказательство. Положим

$$h = \left\lfloor \frac{M}{4t} \right\rfloor .$$

По условию леммы h — натуральное число.

Для $i = 1, 2, \ldots, t$ зададим интервал целых чисел равенством

$$I_i = \{(i-1)h + 1, \ldots, ih\}.$$

Положим

$$\mathcal{X} = I_1 \times \cdots \times I_t, \qquad |\mathcal{X}| = h^t.$$

Докажем, что требуемый леммой набор $\xi = (\xi_1, \ldots, \xi_t)$ можно выбрать в множестве $\mathcal{X}$, т. е. для $i = 1, 2, \ldots, t$ будут выполняться неравенства $(i-1)h < \xi_i \leq ih$ и как следствие соотношения $0 < \xi_1 < \xi_2 < \ldots < \xi_t \leq M/4$. Для любого набора $\xi \in \mathcal{X}$ дополнительно положим $\xi_0 = 0$.

Зафиксируем один набор $w = (w_1, w_2, \ldots, w_k)$ с компонентами из множества $\{M, M+1, \ldots, 2M-1\}$.

Паре (w, ξ), где $w \in \{M, M+1, \ldots, 2M-1\}^k$, $\xi \in \mathcal{X}$, сопоставим помеченный ориентированный граф, в котором $t+1+k$ вершин и $t+k$ дуг (ориентированных ребер). Вершины помечаются числами $\xi_0, \xi_1, \ldots, \xi_t, w_1, w_2, \ldots, w_k$, причем если в наборе w есть равные компоненты, то в графе будут вершины с одинаковыми метками. Вершины, помеченные числами $\xi_1, \xi_2, \ldots, \xi_t$, так же как и сами эти числа, будем называть *анкерами*, а вершины, помеченные числами $w_1, w_2, \ldots, w_k$, — концевыми вершинами или *листьями*.

Вершину с меткой $\xi_0 = 0$ будем называть корнем. При изменении набора w или размещения ξ вершины и дуги сохраняют свои номера, меняются только их числовые метки.

В графе будут дуги двух типов: t дуг *первого типа* — для $i = 1, 2, \ldots, t$ дуга первого типа с номером i выходит из вершины с меткой ξ_{i-1} и входит в анкер ξ_i; k дуг *второго типа* — для $j = 1, 2, \ldots, k$ дуга второго типа с номером j ведет из анкера $\xi_{\sigma(j)}$ в лист, помеченный числом w_j. Множество всех дуг обозначим через $\mathcal{E}$. Каждой дуге $e \in \mathcal{E}$ сопоставим число $\varphi_e(\xi)$, равное разности меток конца дуги и начала дуги.

Отметим, что метки всех дуг положительны, метки дуг первого типа не превосходят $\xi_t \leq M/4$, для меток дуг второго типа выполняются неравенства

$$M - M/4 \leq w_j - \xi_{\sigma(j)} \leq 2M - 2, \qquad j = 1, 2, \ldots, k.$$

В частности, все метки принадлежат множеству $\{1, 2, \ldots, 2M\}$.

Рассмотрим множество Ω всех таблиц, строки которых помечены дугами из $\mathcal{E}$, столбцы пронумерованы первыми $2M$ натуральными числами, а в каждой клетке записано натуральное число, не превосходящее M. Таким образом, таблица — это отображение

$$\omega : \mathcal{E} \times \{1, 2, \ldots, 2M\} \longrightarrow \{1, 2, \ldots, M\}.$$

Отметим, что

$$|\Omega| = M^{2M|\mathcal{E}|} = M^{2M(k+t)}.$$

Для фиксированной таблицы $\omega \in \Omega$ каждой дуге $e \in \mathcal{E}$ сопоставим множество

$$U_e(\omega) = \big\{z \in \{1, 2, \ldots, 2M\} \mid \omega(e, z) \leq B\big\}.$$

Тем самым каждой таблице будет сопоставлено семейство множеств

$$\{U_e(\omega) \mid e \in \mathcal{E}\}.$$

Набор (размещение) $\xi \in \mathcal{X}$ назовём допустимым для таблицы ω, если $\varphi_e(\xi) \in U_e(\omega)$ для всех дуг $e \in \mathcal{E}$. Обозначим число таких наборов через $Z(\omega)$. Для фиксированного размещения ξ в каждой строке таблицы ограничена ровно одна клетка: в ней допустимы B значений, в остальных — M. Подсчитывая пары из таблицы и допустимого для неё размещения, получаем

$$\sum_{\omega \in \Omega} Z(\omega) = |\Omega| h^t \left(\frac{B}{M}\right)^{k+t}.$$

Для оценки суммы квадратов рассмотрим множество $S \subseteq \mathcal{E}$ и пары размещений ξ, η, для которых $\varphi_e(\xi) = \varphi_e(\eta)$ для всех дуг $e \in S$. Дуги первого типа из множества S разбивают цепочку от корня до последнего анкера на компоненты связности; направления дуг здесь не учитываются, изолированные вершины также считаются компонентами. Компоненту назовём закреплённой, если она содержит корень или начало дуги второго типа из множества S, и свободной в противном случае. В каждой компоненте разности $\xi_i - \eta_i$ постоянны, а в закреплённой компоненте равны нулю. Обозначим через $r(S)$ разность между числом t и числом свободных компонент. При фиксированном наборе ξ для каждой свободной компоненты достаточно выбрать одну координату η_i, имеющую не более h значений. Поэтому число рассматриваемых пар не превосходит $h^{2t-r(S)}$. Для пустого множества S имеем равенство $r(S) = 0$, а для непустого множества S выполняются неравенства $1 \leq r(S) \leq t$.

Из определения функции σ следует, что из q последовательных анкеров выходит не более $qk/t + 1$ дуг второго типа, а из первых q анкеров —

ровно $\lfloor qk/t \rfloor \le qk/t$. Действительно, для интервала анкеров с номерами от u до $u+q-1$ число этих дуг равно

$$\left\lfloor \frac{(u+q-1)k}{t} \right\rfloor - \left\lfloor \frac{(u-1)k}{t} \right\rfloor.$$

Свободная компонента из q анкеров вносит вклад, равный $q-1$, как в величину $r(S)$, так и в число $|S|$ дуг множества S. Закреплённая компонента из q анкеров без корня вносит вклад q в величину $r(S)$ и не более $(q-1)+(qk/t+1) = (1+k/t)q$ в число $|S|$ дуг множества S. Компонента с корнем и q анкерами вносит вклад соответственно q и не более $q+qk/t$; здесь допускается $q=0$. Суммируя по компонентам, получаем

$$|S| \le (1+k/t)r(S).$$

Подсчитаем тройки из таблицы и двух допустимых размещений. В каждой строке требуется ограничить две клетки, кроме случая совпадения меток, когда ограничена одна клетка. Поэтому каждое совпадение умножает число таблиц на M/B. Представляя этот множитель в виде $1+(M/B-1)$ и раскрывая произведение по строкам, имеем

$$\frac{\sum_{\omega\in\Omega} Z(\omega)^2}{|\Omega|(B/M)^{2(k+t)}} = \\ = \sum_{S\subseteq\mathcal{E}} \left(\frac{M}{B}-1\right)^{|S|} \left|\{(\xi,\eta)\in\mathcal{X}^2 : \varphi_e(\xi)=\varphi_e(\eta)\ (e\in S)\}\right| \le \\ \le h^{2t}\left(1+\sum_{\varnothing\ne S\subseteq\mathcal{E}} h^{-r(S)}\left(\frac{M}{B}\right)^{|S|}\right).$$

При заданном значении $r=r(S)\ge 1$ число множеств S, в силу полученного неравенства, не превосходит

$$\sum_{j=1}^{\min\{k+t,\lfloor(1+k/t)r\rfloor\}} \binom{k+t}{j} \le [2(k+t)]^{(1+k/t)r}$$

(здесь использованы неравенство $\binom{k+t}{j} \le (k+t)^j$ и оценка суммы геометрической прогрессии). Следовательно, по условию леммы

$$\frac{\sum_{\omega\in\Omega} Z(\omega)^2}{|\Omega|h^{2t}(B/M)^{2(k+t)}} \le 1+\sum_{r=1}^{t}\left[\frac{1}{h}\left(\frac{2M(k+t)}{B}\right)^{1+k/t}\right]^r \le \frac{4}{3}.$$

По неравенству Коши

$$\bigl|\{\omega : Z(\omega) > 0\}\bigr| \geq \frac{\bigl(\sum_\omega Z(\omega)\bigr)^2}{\sum_\omega Z(\omega)^2} \geq \frac{3}{4}|\Omega|.$$

Таким образом, для каждого набора w не менее трёх четвертей таблиц имеют допустимое размещение.

Назовём таблицу малой, если выполняется условие

$$\sum_{e\in\mathcal{E}} |U_e(\omega)| \leq 8B(k+t).$$

Обозначим множество малых таблиц через Ω_0. Подсчёт по клеткам даёт

$$\sum_{\omega\in\Omega}\sum_{e\in\mathcal{E}} |U_e(\omega)| = 2B(k+t)|\Omega|,$$

откуда следует неравенство $|\Omega_0| \geq 3|\Omega|/4$. Для каждого набора w число неподходящих малых таблиц не больше $|\Omega|/4 \leq |\Omega_0|/3$. Значит, число элементов любого непустого семейства ещё не покрытых наборов w можно сократить по крайней мере втрое, выбрав одну малую таблицу: это следует из подсчёта пар «набор w — подходящая малая таблица». Первоначально имеется M^k наборов, поэтому после не более чем $\lceil \log_3(4(2M)^k)\rceil$ таких шагов число непокрытых наборов меньше единицы и, следовательно, равно нулю. Объединение множеств $U_e(\omega)$ по всем дугам и выбранным таблицам даёт требуемое множество U и оценку его мощности. □

4. Доказательство верхней оценки теоремы 2

Верхнюю оценку будем доказывать для задачи Кнута. Достаточно рассмотреть произвольный набор из m положительных показателей, не превосходящих величины $A = \varphi(m)m^a = m^{a+o(1)}$. Нулевые показатели не требуют вычислений и могут быть заменены единицами.

Зафиксируем достаточно большое натуральное число k и положим

$$t = \lceil (a-2)k\rceil + 1, \qquad M = \left\lceil m^{a-1+1/(4(k+t))}\right\rceil, \qquad B = \left\lfloor m^{1-1/(4(k+t))}\right\rfloor.$$

Сначала будем считать число k фиксированным и устремим число m к бесконечности. Константы в оценках ниже могут зависеть от чисел a и k. Очевидно, при достаточно больших значениях m выполнены неравенства $1 \leq B < M$ и $M \geq 4t$. Кроме того,

$$\left\{\left\lfloor\frac{M}{4t}\right\rfloor\left(\frac{B}{2M(k+t)}\right)^{1+k/t}\right\}^t = m^{\,t-(a-2)k-\frac{2k+t}{4(k+t)}+o(1)} \longrightarrow \infty,$$

поскольку выполняются неравенства $t-(a-2)k \geq 1$ и $(2k+t)/(4(k+t)) < 1/2$. Таким образом, выполнены все условия леммы 1, в том числе при $a = 2$, когда $t = 1$.

Выберем множество U по этой лемме. При фиксированных числах k и t имеем оценку $|U| = O(B \log m)$. Все степени x^u, $u \in U$, можно подготовить бинарным методом за

$$O(B(\log m)^2) = o(m)$$

умножений в силу неравенства $u \leq 2M$ и соотношения $\log M = O(\log m)$.

Обозначим через m_0 число заданных показателей, меньших числа M. Остальные распределим по промежуткам $[jM, (j+1)M)$, $1 \leq j \leq \lfloor A/M \rfloor$, а внутри каждого промежутка — по группам не более чем из k показателей. В силу соотношения

$$\frac{A}{M} = m^{1-1/(4(k+t))+o(1)} = o(m),$$

число групп не превосходит $(m - m_0)/k + o(m)$. Все необходимые степени $x^{(j-1)M}$ с положительным показателем также подготовим бинарным методом. Это требует $O((A/M) \log m) = o(m)$ умножений.

В группе из j-го промежутка представим показатели в виде $c + w_1, \ldots, c + w_k$, где $c = (j-1)M$ и $M \leq w_i < 2M$; неполную группу дополним повторениями. По лемме для этой группы достаточно $t + k$ умножений:

$$x^{c+\xi_i} = x^{c+\xi_{i-1}} x^{\xi_i - \xi_{i-1}} \quad (1 \leq i \leq t), \qquad \xi_0 = 0,$$
$$x^{c+w_j} = x^{c+\xi_{\sigma(j)}} x^{w_j - \xi_{\sigma(j)}} \quad (1 \leq j \leq k).$$

При нулевом значении c первое умножение пропускается, поскольку число ξ_1 принадлежит множеству U. Значит, с учётом предварительных вычислений затраты на показатели, не меньшие числа M, не превосходят

$$\left(1 + \frac{t}{k}\right)(m - m_0) + o(m).$$

Для показателей, меньших числа M, положим $q = \lfloor a \rfloor$ и $d = \lfloor M^{1/q} \rfloor + 1$. В силу неравенства $q > a - 1$ при достаточно большом фиксированном числе k имеем неравенство $a - 1 + 1/(4(k+t)) < q$, откуда следует соотношение $d \log m = o(m)$. Подготовим бинарным методом степени с показателями sd^j, $1 \leq s < d$, $0 \leq j < q$; это требует $O(d \log m) = o(m)$ умножений. Разложение по основанию d представляет любое положительное число, меньшее числа $M < d^q$, в виде суммы не более q таких

показателей. Поэтому каждую из оставшихся степеней можно получить не более чем за $q-1 \le a-1$ умножений.

В итоге получаем для любого допустимого набора показателей следующую оценку, в которой остаточный член $o(m)$ не зависит от выбора набора:

$$l(x^{n_1},\dots,x^{n_m}) \le (q-1)m_0 + \left(1+\frac{t}{k}\right)(m-m_0) + o(m) \le \\ \le \left(a-1+\frac{2}{k}\right)m + o(m).$$

Эта оценка выполняется и для набора, на котором достигается максимум из определения функции Шеннона. Поэтому для функции Шеннона справедлива такая же оценка.

Далее в силу произвольности числа k получаем

$$L_K(\underbrace{A,\dots,A}_{m \text{ раз}}) \le (a-1)m + o(m).$$

При переходе к задаче Беллмана из соображений двойственности вытекает оценка $L_B(A,\dots,A) \le am + o(m)$, что вместе с нижними оценками доказывает теорему.

Список литературы

[1] С. Б. Гашков, В. В. Кочергин, “Об аддитивных цепочках векторов, вентильных схемах и сложности вычисления степеней”, *Методы дискретного анализа в теории графов и сложности*, Вып. 52, Новосибирск, 1992, 22–40.

[2] Д. Е. Кнут, *Искусство программирования для ЭВМ*, 1-е издание. Т. 2, Мир, М., 1977.

[3] Д. Е. Кнут, *Искусство программирования*, 3-е издание. Т. 2, Издательский дом «Вильямс», М., 2000.

[4] В. В. Кочергин, “О сложности вычислений в конечных абелевых группах”, *Доклады АН СССР*, **317**:2 (1991), 291–294.

[5] В. В. Кочергин, “О сложности вычислений в конечных абелевых группах”, *Математические вопросы кибернетики*, Вып. 4, Наука, М., 1992, 178–217.

[6] В. В. Кочергин, “О сложности вычислений одночленов и наборов степеней”, *Дискретный анализ*, Труды Института математики СО РАН, **27**, Издательство Института математики СО РАН, Новосибирск, 1994, 94–107.

[7] В. В. Кочергин, “О вычислении наборов степеней”, *Дискретная математика*, **6**:2 (1994), 129–137.

[8] В. В. Кочергин, “Уточнение оценок сложности вычисления одночленов и наборов степеней в задачах Беллмана и Кнута”, *Дискретный анализ и исследование операций*, **21**:6 (2014), 51–72.

[9] В. В. Кочергин, “Задачи Беллмана, Кнута, Лупанова, Пиппенджера и их вариации как обобщения задачи об аддитивных цепочках”, *Математические вопросы кибернетики*, Вып. 20, ФИЗМАТЛИТ, М., 2022, 119–256. DOI: 10.20948/mvk-2022-119, https://library.keldysh.ru/mvk.asp?id=2022-119.

[10] О. Б. Лупанов, “О вентильных и контактно-вентильных схемах”, *Доклады АН СССР*, **111**:6 (1956), 1171–1174.

[11] О. Б. Лупанов, “О синтезе некоторых классов управляющих систем”, *Проблемы кибернетики*, Вып. 10, Физматгиз, М., 1963, 63–97.

[12] О. Б. Лупанов, “Об одном подходе к синтезу управляющих систем — принципе локального кодирования”, *Проблемы кибернетики*, Вып. 14, Наука, М., 1965, 31–110.

[13] Э. И. Нечипорук, “О вентильных схемах”, *Доклады АН СССР*, **148**:1 (1963), 50–53.

[14] Э. И. Нечипорук, “О топологических принципах самокорректирования”, *Проблемы кибернетики*, Вып. 21, Наука, М., 1969, 5–102.

[15] А. Ф. Сидоренко, “Сложность аддитивных вычислений семейств целочисленных линейных форм”, *Записки научных семинаров ЛОМИ*, **105** (1981), 53–61.

[16] N. Alon, B. Bukh, B. Sudakov, “Discrete Kakeya-type problems and small bases”, *Israel Journal of Mathematics*, **174** (2009), 285–301. DOI: 10.1007/s11856-009-0115-9.

[17] R. E. Bellman, “Addition chains of vectors (Advanced problem 5125)”, *The American Mathematical Monthly*, **70**:7 (1963), 765. DOI: 10.2307/2312273.

[18] A. Brauer, “On addition chains”, *Bulletin of the American Mathematical Society*, **45**:10 (1939), 736–739. DOI: 10.1090/S0002-9904-1939-07068-7.

[19] D. Dobkin, R. J. Lipton, “Addition chain methods for the evaluation of specific polynomials”, *SIAM Journal on Computing*, **9**:1 (1980), 121–125. DOI: 10.1137/0209011.

[20] P. Downey, B. Leong, R. Sethi, “Computing sequences with addition chains”, *SIAM Journal on Computing*, **10**:3 (1981), 638–646. DOI: 10.1137/0210047.

[21] P. Erdős, “Remarks on number theory, III: On addition chains”, *Acta Arith.*, **6**:1 (1960), 77–81. DOI: 10.4064/aa-6-1-77-81.

[22] D. E. Knuth, C. H. Papadimitriou, “Duality in addition chains”, *Bulletin of the European Association for Theoretical Computer Science*, 1981, №13, 2–4.

[23] J. Olivos, “On vectorial addition chains”, *Journal of Algorithms*, **2**:1 (1981), 13–21. DOI: 10.1016/0196-6774(81)90003-1.

[24] N. Pippenger, “On the evaluation of powers and related problems”, *Proceedings of the 17th Annual Symposium on Foundations of Computer Science* (Houston, TX, October 25–27, 1976), IEEE, 1976, 258–263. DOI: 10.1109/SFCS.1976.21.

[25] N. Pippenger, “The minimum number of edges in graphs with prescribed paths”, *Mathematical Systems Theory*, **12**:4 (1979), 325–346. DOI: 10.1007/BF01776581.

[26] N. Pippenger, “On the evaluation of powers and monomials”, *SIAM Journal on Computing*, **9**:2 (1980), 230–250. DOI: 10.1137/0209022.

[27] T. H. Southard, *Addition chains for the first N squares*, Technical Report CNA-84, University of Texas at Austin, Austin, TX, 1974.

[28] E. G. Straus, "Addition chains of vectors", *The American Mathematical Monthly*, **71**:7 (1964), 806–808. DOI: 10.2307/2310929.

[29] M. V. Subbarao, "Addition chains — some results and problems", *Number Theory and Applications*, NATO ASI Series. Series C: Mathematical and Physical Sciences, **265**, eds. R. A. Mollin, Kluwer Academic Publishers, Dordrecht, 1989, 555–574.

[30] A. C.-C. Yao, "On the evaluation of powers", *SIAM Journal on Computing*, **5**:1 (1976), 100–103. DOI: 10.1137/0205008.

Статья поступила 9 ноября 2026 г.

New Results on R. Bellman's and D. Knuth's Problems

V. V. Kochergin

We consider Bellman's problem on the complexity of computing a monomial in m variables, defined as the minimum number of multiplications required, and Knuth's problem on the complexity of computing a set of m powers of a single variable. For every fixed real number $a \geq 2$ and every positive function $\varphi(m)$ satisfying $|\log \varphi(m)| = o(\log m)$, we establish asymptotically tight bounds for the corresponding Shannon functions, which describe the maximum possible complexity when the exponents are bounded by $A = \varphi(m)m^a$. As $m \to \infty$, these functions are asymptotic to am and $(a-1)m$, respectively.

Keywords: addition chains, vector addition chains, Bellman's problem, Knuth's problem, circuit complexity.

References

[1] S. B. Gashkov, V. V. Kochergin, "On addition chains of vectors, rectifier networks, and the complexity of computing powers", *Metody Diskretnogo Analiza v Teorii Grafov i Slozhnosti*, Issue 52, Novosibirsk, 1992, 22–40 (In Russian).

[2] D. E. Knuth, *The Art of Computer Programming*, 1st edition. V. 2, Mir, Moscow, 1977 (In Russian).

[3] D. E. Knuth, *The Art of Computer Programming*, 3rd edition. V. 2, Williams, Moscow, 2000 (In Russian).

[4] V. V. Kochergin, "On the complexity of computations in finite Abelian groups", *Doklady AN SSSR*, **317**:2 (1991), 291–294 (In Russian).

[5] V. V. Kochergin, "On the complexity of computations in finite Abelian groups", *Matematicheskie Voprosy Kibernetiki*, Issue 4, Nauka, Moscow, 1992, 178–217 (In Russian).

[6] V. V. Kochergin, “On the complexity of computing monomials and sets of powers”, *Diskretnyi Analiz*, Trudy Instituta Matematiki SO RAN, **27**, Institute of Mathematics, Siberian Branch of the Russian Academy of Sciences, Novosibirsk, 1994, 94–107 (In Russian).

[7] V. V. Kochergin, “On the computation of sets of powers”, *Diskretnaya Matematika*, **6**:2 (1994), 129–137 (In Russian).

[8] V. V. Kochergin, “Improvement of complexity bounds for computing monomials and sets of powers in Bellman’s and Knuth’s problems”, *Diskretnyi Analiz i Issledovanie Operatsii*, **21**:6 (2014), 51–72 (In Russian).

[9] V. V. Kochergin, “Problems of Bellman, Knuth, Lupanov, and Pippenger and their variations as generalizations of the addition chain problem”, *Matematicheskie Voprosy Kibernetiki*, Issue 20, FIZMATLIT, Moscow, 2022, 119–256. DOI: 10.20948/mvk-2022-119 (In Russian), https://library.keldysh.ru/mvk.asp?id=2022-119.

[10] O. B. Lupanov, “On rectifier and contact-rectifier networks”, *Doklady AN SSSR*, **111**:6 (1956), 1171–1174 (In Russian).

[11] O. B. Lupanov, “On the synthesis of certain classes of control systems”, *Problemy Kibernetiki*, Issue 10, Fizmatgiz, Moscow, 1963, 63–97 (In Russian).

[12] O. B. Lupanov, “On an approach to the synthesis of control systems: the local coding principle”, *Problemy Kibernetiki*, Issue 14, Nauka, Moscow, 1965, 31–110 (In Russian).

[13] E. I. Nechiporuk, “On rectifier networks”, *Doklady AN SSSR*, **148**:1 (1963), 50–53 (In Russian).

[14] E. I. Nechiporuk, “On topological principles of self-correction”, *Problemy Kibernetiki*, Issue 21, Nauka, Moscow, 1969, 5–102 (In Russian).

[15] A. F. Sidorenko, “The complexity of additive computations of families of integer linear forms”, *Zapiski Nauchnykh Seminarov LOMI*, **105** (1981), 53–61 (In Russian).

[16] N. Alon, B. Bukh, B. Sudakov, “Discrete Kakeya-type problems and small bases”, *Israel Journal of Mathematics*, **174** (2009), 285–301. DOI: 10.1007/s11856-009-0115-9.

[17] R. E. Bellman, “Addition chains of vectors (Advanced problem 5125)”, *The American Mathematical Monthly*, **70**:7 (1963), 765. DOI: 10.2307/2312273.

[18] A. Brauer, “On addition chains”, *Bulletin of the American Mathematical Society*, **45**:10 (1939), 736–739. DOI: 10.1090/S0002-9904-1939-07068-7.

[19] D. Dobkin, R. J. Lipton, “Addition chain methods for the evaluation of specific polynomials”, *SIAM Journal on Computing*, **9**:1 (1980), 121–125. DOI: 10.1137/0209011.

[20] P. Downey, B. Leong, R. Sethi, “Computing sequences with addition chains”, *SIAM Journal on Computing*, **10**:3 (1981), 638–646. DOI: 10.1137/0210047.

[21] P. Erdős, “Remarks on number theory, III: On addition chains”, *Acta Arith.*, **6**:1 (1960), 77–81. DOI: 10.4064/aa-6-1-77-81.

[22] D. E. Knuth, C. H. Papadimitriou, “Duality in addition chains”, *Bulletin of the European Association for Theoretical Computer Science*, 1981, № 13, 2–4.

[23] J. Olivos, “On vectorial addition chains”, *Journal of Algorithms*, **2**:1 (1981), 13–21. DOI: 10.1016/0196-6774(81)90003-1.

[24] N. Pippenger, “On the evaluation of powers and related problems”, *Proceedings of the 17th Annual Symposium on Foundations of Computer Science* (Houston, TX, October 25–27, 1976), IEEE, 1976, 258–263. DOI: 10.1109/SFCS.1976.21.

[25] N. Pippenger, “The minimum number of edges in graphs with prescribed paths”, *Mathematical Systems Theory*, **12**:4 (1979), 325–346. DOI: 10.1007/BF01776581.

[26] N. Pippenger, “On the evaluation of powers and monomials”, *SIAM Journal on Computing*, **9**:2 (1980), 230–250. DOI: 10.1137/0209022.

[27] T. H. Southard, *Addition chains for the first N squares*, Technical Report CNA-84, University of Texas at Austin, Austin, TX, 1974.

[28] E. G. Straus, “Addition chains of vectors”, *The American Mathematical Monthly*, **71**:7 (1964), 806–808. DOI: 10.2307/2310929.

[29] M. V. Subbarao, “Addition chains — some results and problems”, *Number Theory and Applications*, NATO ASI Series. Series C: Mathematical and Physical Sciences, **265**, eds. R. A. Mollin, Kluwer Academic Publishers, Dordrecht, 1989, 555–574.

[30] A. C.-C. Yao, “On the evaluation of powers”, *SIAM Journal on Computing*, **5**:1 (1976), 100–103. DOI: 10.1137/0205008.

Received on November 9, 2026