

XIV Международный научный семинар «ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЁ ПРИЛОЖЕНИЯ»

Доклад
«Сравнение оценок сложности
для задач Р. Беллмана и О. Б. Лупанова»

В. В. Кочергин

21 июня 2022 г.

Задача об эффективном возведении в степень

Задача Беллмана является обобщением классической задачи об эффективном возведении в степень, т. е. нахождении величины $I(x^n)$ — минимального числа операций умножения, достаточного для вычисления по переменной x величины x^n .

В аддитивной постановке исходная классическая задача известна как задача об аддитивных цепочках.

Задача об аддитивных цепочках

Аддитивной цепочкой для натурального числа n называется последовательность натуральных чисел

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

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

Число r называется *длиной цепочки*.

Очевидно, что минимальная длина аддитивной цепочки для n равна $l(x_n)$.

Оценки сложности возведения в степень

А. Брауэр, 1939:

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

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

П. Эрдёш, 1960: для любого $\varepsilon > 0$ для почти всех n

$$l(x^n) \geq \log n + (1 - \varepsilon) \frac{\log n}{\log \log n}.$$

В. В. Кочергин, Д. В. Кочергин, 2017: для любого $\varepsilon > 0$ для почти всех n

$$\left| \max_{k: k \leq n} l(x^k) - \left(\log n + \frac{\log n}{\log \log n} \right) \right| \leq (2 + \varepsilon) \frac{\log n \log \log \log n}{(\log \log^2 n)}.$$

А. Шенхаге, 1975:

$$l(x^n) \geq \log n + \log s(n) - 2,13,$$

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

Задача Беллмана

Р. Беллман, 1963 (для случая $m = 2$), Е. Страус, 1964 (для произвольного m):

задача о сложности вычисления одночлена от m переменных т. е. нахождение величины $l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m})$.

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)

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

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

Задача Беллмана. Некоторые результаты

Е. Страус, 1964:

для любого фиксированного m

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

П. Доуни, Б. Леонг, Р. Сети, 1981:

задача распознавания по набору натуральных чисел

$(n_1, n_2, \dots, n_p, l)$ существования аддитивной цепочки, имеющей длину l и содержащей числа $n_1, n_2, \dots, n_p$, является NP -полной.

Связь задачи Беллмана с задачей Кнута

Д. Кнут, 1969:

поставил задачу о сложности вычисления набора из m степеней одной переменной т. е. нахождения величины $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$.

Двойственность задач Беллмана и Кнута

1981, независимо

А. Ф. Сидоренко (в наиболее общем виде)

Д. Кнут и К. Пападимитриу

Дж. Оливос:

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

Поэтому можно говорить об одной задаче Беллмана — Кнута.

Задача Лупанова

Пусть G — конечная мультипликативная абелева группа.

Множество $B = \{a_1, \dots, a_q\}$ элементов группы — *базис* в группе G , если G раскладывается в прямое произведение циклических подгрупп, порожденных элементами множества B :

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

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

Сложность $L(g; B)$ элемента g группы G над базисом B — минимальное число операций умножения, достаточное для вычисления элемента g с использованием элементов множества B , при этом все уже вычисленные элементы могут быть использованы многократно.

Записи О. Б. Лупанова с постановкой задач

G_2, G_4

*	0	0
	0	1
	0	2
	0	3
	1	0
	1	1
	1	2
	1	3

$a(1,0)$
 $b(0,1)$

$G = \bigcup G_i$

B

$\angle(G, B)$

$$\angle M(G) = \max_B \angle(G, B)$$

$$\angle m(G) = \min_B \angle(G, B)$$

$$\rightarrow M(v) \\ m(v)$$

$v = (2, 2, 3, 3, 4, 4, 4)$

$(2, 2, 2, \dots, 2)$

$(P, P, \dots, P)$

$M(P, n)$

$m(P, n)$

числовое $f(v)$ (функция)
Найти Φ функцию, определенную на
векторах v , описывающих характеристики
порядка прикратных численных групп,
с помощью которой выражались бы
 $M(v)$ и $m(v)$
(хотя бы асимптотически
или с точностью до порядка).

наименее, при условии
что порядок всех групп $\rightarrow \infty$

$f(p, n)$

$m(p, n)$

$$M(n) = \max_{v \text{ порядка } \leq n} M(v)$$

$$m(n) = \max_{v \text{ порядка } \leq n} m(v)$$

$$M_1(n) = \sum_{v \text{ порядка } n} M(v)$$

число групп
порядка n

Задача Лупанова. Обозначения

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

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

Положим

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

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

Положим

$$M(n) = \max_{\mathbf{v}: \|\mathbf{v}\| \leq n} M(\mathbf{v}), \quad m(n) = \max_{\mathbf{v}: \|\mathbf{v}\| \leq n} m(\mathbf{v}),$$

где $\|\mathbf{v}\| = v_1 v_2 \dots v_q$.

Задача Лупанова. Обозначения (2)

Положим

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

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 .

Функции $M_{\text{ср}}(n)$ и $m_{\text{ср}}(n)$ характеризуют средние значения соответствующих мер сложности абелевых групп порядка n .

Задача заключается в том, чтобы

- во-первых, найти числовые функции $f_1(\mathbf{v})$ и $f_2(\mathbf{v})$, определенные на векторах $\mathbf{v}$, характеризующих порядки примарных циклических групп, с помощью которых выражались бы величины $M(\mathbf{v})$ и $m(\mathbf{v})$ (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 $n \rightarrow \infty$.

Задача Лупанова через призму задачи Беллмана

В основе исследований задачи Лупанова лежат оценки величины

$$L(a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}; \{a_1, a_2, \dots, a_m\}).$$

Эта задача связана с задачей Беллмана не только очевидным неравенством

$$L(a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}; \{a_1, a_2, \dots, a_m\}) \leq l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}),$$

но и общностью методов получения и верхних, и нижних оценок.

Направления исследований по задаче Лупанова

Можно выделить следующие составляющие исследований, связанных с задачей Лупанова:

- I. Разработка достаточно универсальных (относительно задач Беллмана и Лупанова) методов нахождения верхних и нижних оценок сложности реализации одночленов и сложности элементов конечных абелевых групп.
- II. Получение ответов на остальные вопросы из задачи Лупанова.
- III. Изучение вопроса о степени различия значений сложности реализации одночленов и сложности элементов конечных абелевых групп.

По этому направлению все результаты формулируются только для задачи Беллмана.

Е. Страус, 1964:
для любого фиксированного m

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

Следствие из более общего результата Н. Пиппенджера, 1980:

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

Напр. I.: Общие методы и оценки (2)

С. Б. Гашков, В. В. Кочергин, 1992:

$$\begin{aligned} I(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}) &\leq \\ &\leq \log \max_{1 \leq i \leq m} n_i + \frac{\log N}{\log \log N} \left(1 + O \left(\left(\frac{\log \log \log N}{\log \log N} \right)^{1/2} \right) \right) + O(m), \end{aligned}$$

где $N = n_1 n_2 \dots n_m$.

В. В. Кочергин, 1994:

для почти всех наборов $\tilde{n} = (n_1, n_2, \dots, n_m)$, справедливо асимптотическое равенство

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

В. В. Кочергин, 2014:

$$I(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}) \leq \log(\max n_i)(1 + o(1)) + \frac{\log N}{\log \log N}(1 + o(1)) + m.$$

В. В. Кочергин, 2021:

$$I(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}) \leq \log(\max n_i) + \frac{\log N}{\log \log N}(1 + o(1)) + m.$$

Положим

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

где $N = n_1 n_2 \dots n_m$.

Тогда для любого $\varepsilon > 0$ почти все наборы $(k_1, k_2, \dots, k_m)$, не превышающие набора $(n_1, n_2, \dots, n_m)$, удовлетворяют неравенствам

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

В. В. Кочергин, 1991–1992, 2015:

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

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

Напр. II.: Функции $m(\mathbf{v})$ и $M(\mathbf{v})$

При $\|\mathbf{v}\| \rightarrow \infty$ выполняются соотношения

$$\frac{\log \|\mathbf{v}\|}{\log \log \|\mathbf{v}\|} \lesssim m(\mathbf{v}) \leq M(\mathbf{v}) \lesssim \log \|\mathbf{v}\|,$$

причем для любых медленно изменяющихся (по Карамате) функций $h_1(n)$ и $h_2(n)$, удовлетворяющих при $n \rightarrow \infty$ условиям

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

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

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

Напр. II.: Функция $M(\mathbf{v})$

Обозначим:

$q(\mathbf{v})$ — размерность (число координат) вектора $\mathbf{v}$;

$P(\mathbf{v})$ — максимальное значение порядка среди всех элементов группы G , задаваемой вектором $\mathbf{v}$ порядков примарных циклических подгрупп.

При $\|\mathbf{v}\| \rightarrow \infty$ выполняются соотношения

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

Напр. II.: Функция $m(\mathbf{v})$

Пусть B — базис конечной абелевой группы G . Введем обозначения:

$k(B)$ — максимальный порядок среди базисных элементов;

$r(B) = \lfloor \log(k(B) - 1) \rfloor + |B|$;

$r(\mathbf{v}) = \min r(B)$, где минимум берется по всем базисам абелевой группы, у которой порядки примарных циклических подгрупп задаются вектором $(\mathbf{v})$.

При $\|\mathbf{v}\| \rightarrow \infty$ выполняется верхняя оценка

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

при всех достаточно больших значениях $\|\mathbf{v}\|$ справедлива нижняя оценка

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

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

причем для любых медленно меняющихся (по Карамате) функций $h_1(n)$ и $h_2(n)$, удовлетворяющих при $n \rightarrow \infty$ условиям

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

найдется подпоследовательность $\{n_s\}$, для которой справедливы соотношения

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

Напр. III.: Формальное сопоставление элементу конечной абелевой группы одночлена

Пусть g — произвольный элемент конечной абелевой группы G , заданной своим базисом $B = \{a_1, \dots, a_q\}$. Представление

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

элемента g в базисе B *каноническое*, если $0 \leq n_i \leq u_i - 1$ для всех i , где u_i — порядок базисного элемента a_i .

Представлению элемента g в базисе B *соответствует* одночлен $x_1^{n_1} x_2^{n_2} \dots x_q^{n_q}$, если набор показателей степеней переменных в одночлене совпадает с набором показателей степеней в каноническом представлении элемента g в базисе B .

Обозначение для этого многочлена: $P[g; B]$.

Каноническому представлению $g = a_1^{n_1} a_2^{n_2} \dots a_q^{n_q}$, элемента g конечной абелевой группы G в базисе B сопоставлен одночлен:

$$g = a_1^{n_1} a_2^{n_2} \dots a_q^{n_q} \longrightarrow P[g; B] = x_1^{n_1} x_2^{n_2} \dots x_q^{n_q}.$$

Очевидно, что

$$L(g; B_G) \leq I(P[g; B_G]).$$

Как сильно могут отличаться величины $L(g; B_G)$ и $I(P[g; B_G])$?

Положим

$$\sigma(n) = \max \{I(P[g; B_G]) - L(g; B_G)\},$$

$$\pi(n) = \max \frac{I(P[g; B_G])}{L(g; B_G)},$$

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

Напр. III.: Асимптотическое поведение величины $\sigma(n)$

При $n \rightarrow \infty$ верно асимптотическое равенство

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

Верхняя оценка после внешне незначительного усиления в 2021 г. верхней оценки задачи Беллмана становится почти очевидной.

Идея нижней оценки. Пусть $m = m(n)$ удовлетворяет условиям $m \leq 2^{\lfloor \log n \rfloor - 1}$ и $l(x^m) = \max l(x^t)$, где максимум берется по всем значениям t , не превосходящим $2^{\lfloor \log n \rfloor - 1}$. Тогда $l(x^m) - \log n \gtrsim \frac{\log n}{\log \log n}$.

С другой стороны, в циклической группе порядка $2^{\lfloor \log n \rfloor} - m$ с порождающим элементом a справедливы равенства $a^m = a^{2^{\lfloor \log n \rfloor} - m + m} = a^{2^{\lfloor \log n \rfloor}}$. Поэтому $L(a^m; \{a\}) \leq \lfloor \log n \rfloor$.

Напр. III.: Асимптотическое поведение величины $\pi(n)$

При $n \rightarrow \infty$ верно асимптотическое равенство

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

Верхняя оценка основана на том факте, что для элемента $g = a_1^{n_1} a_2^{n_2} \dots a_q^{n_q}$, выполняется неравенство

$$q + \log \max(n_i + 1) \geq 2\sqrt{\log \Pi(n_i + 1)}.$$

Нижняя оценка устанавливается подбором для трудновычислимого одночлена, который существует ввиду мощностной нижней оценки, абелевой группы и ее такого базиса, что соответствующий элемент вычисляется достаточно просто.

Напр. III.: Сравнение сложности вычисления системы элементов абелевой группы и системы одночленов

Пусть $p = p(n) = o(\sqrt{\log n})$ при $n \rightarrow \infty$. Положим

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

Тогда $\log m \sim (\log n)/p$ при $n \rightarrow \infty$.

Рассмотрим абелеву группу

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

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

В базисе $B = \{a_1, a_2, \dots, a_p\}$ рассмотрим систему элементов

$$g_1 = a_1^m \dots a_p^m, \quad g_2 = a_2^{2m} \dots a_p^{2m}, \quad \dots, \quad g_p = a_p^{2^{p-1}m}.$$

С использованием равенств $g_{i+1} = g_i^2$, $i = 1, \dots, p-1$, получаем соотношения

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

Напр. III.: Сравнение сложности вычисления системы элементов абелевой группы и системы одночленов (2)

С другой стороны, применяя нижнюю оценку через логарифм определителя матрицы, задающей показатели степеней в одночленах системы, имеем:

$$\begin{aligned} I \left(x_1^m \dots x_p^m, x_2^{2m} \dots x_p^{2m}, \dots, x_p^{2^{p-1}m} \right) &\geq \\ &\geq \log \left(m^p 2^{(p-1)p/2} \right) + p - 1 \sim p \log m. \end{aligned}$$

Таким образом,

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

| Спасибо за внимание!