ПЛЕНАРНЫЕ ДОКЛАДЫ

СРАВНЕНИЕ ОЦЕНОК СЛОЖНОСТИ ДЛЯ ЗАДАЧ Р. БЕЛЛМАНА И О. Б. ЛУПАНОВА

В. В. Кочергин (Москва)

Задача об эффективном возведении в степень. Задача Беллмана является обобщением классической задачи об эффективном возведении в степень, т. е. задачи о нахождении величины $l(x^n)$ — минимального числа операций умножения, достаточного для вычисления по переменной x величины x^n, при этом вычислительная модель допускает возможность многократного использования результатов промежуточных вычислений.

В аддитивной постановке исходная классическая задача известна как задача об аддитивных цепочках [1].

Аддитивной цепочкой для натурального числа n называется последовательность натуральных чисел

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

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

Число r называется *длиной цепочки*.

Минимальная длина аддитивной цепочки для n равна *сложности $l(x^n)$ возведения в n-ю степень*.

Оценки сложности возведения в степень. Различным аспектам классической задачи об эффективном вычислении степеней (задачи о длине аддитивных цепочек) посвящено большое число публикаций — см., например, работы [1–4], являющиеся обзорами или содержащие обзорную часть. Кроме того, в связи с активным применением аппарата аддитивных цепочек в криптографических алгоритмах и других приложениях, 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 следующих оценок величины $l(x^n)$, доказанных в середине прошлого века, практически не получено.

А. Брауэром [5] в 1939 г. установлена верхняя оценка

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

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

В 1960 г. П. Эрдёш [6], установил принципиальную неулучшаемость этой оценки в общем случае, показав, что для любого $\varepsilon > 0$ для почти всех n

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

Последний результат можно усилить, используя решение более общей задачи из [7]; дальнейшее продвижение в направлении уточнения нижней оценки содержится в [8]: для любого $\varepsilon > 0$ для почти всех n

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

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 $l(x^n) - \log n$ достаточно велика, предъявить явным образом бесконечную последовательность таких значений не удается. Конструктивных нижних оценок, качественно сильнее неравенства

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

(здесь $\nu(n)$ — число единиц в двоичной записи числа n), установленного в 1975 г А. Шёнхаге [9], до сих пор, по-видимому, не получено.

Задача Беллмана. В 1963 г. Р. Беллман [10] (для случая $m = 2$), а затем в 1964 г. Е. Штраус [11] (для произвольного m) сформулировали задачу о *сложности вычисления одночлена от m переменных*, т. е. нахождения величины $l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m})$. Эту задачу,

следуя [2, 7], будем называть *задачей Беллмана*. 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)

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

начинающейся с m единичных векторов и удовлетворяющей условию: для каждого k, $m+1 \le k \le m+r$, найдется 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 1964 г. Е. Штраус [11] установил, что для любого фиксированного m

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

В 1969 г. Д. Кнут [1] поставил задачу о сложности вычисления набора из m степеней одной переменной т. е. нахождения величины $l(x^{n_1}, x^{n_2}, \dots x^{n_m})$.

В 1980–1981 гг. независимо А. Ф. Сидоренко [12] (в наиболее общем виде), Д. Кнут и К. Пападимитриу [13], а также Дж. Оливос [14] установили взаимодвойственную природу задач Беллмана и Кнута, доказав что

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

Таким образом, можно говорить об одной задаче Беллмана — Кнута.

П. Доуни, Б. Леонг, Р. Сети в 1981 г. показали [15], что задача распознавания по набору натуральных чисел $(n_1, n_2, \dots, n_p, l)$ возможности вычислить систему степеней $x^{n_1}, x^{n_2}, \dots, x^{n_p}$ с использованием l операций умножения является NP-полной. Поэтому в задаче Беллмана — Кнута и других обсуждаемых здесь задачах речь идет не о вычислении точного значения сложности, а об ее асимптотическом поведении.

Задача Лупанова. Пусть G — конечная мультипликативная абелева группа. Множество $B = \{a_1, \dots, a_q\}$ элементов группы будем называть *базисом* в группе G, если G раскладывается в прямое произведение циклических подгрупп, порожденных элементами множества B:

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

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

Сложность $L(g;B)$ элемента g группы G над базисом B определим 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.

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

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

Далее введем две меры сложности абелевых групп:

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

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

Теперь определим функции Шеннона равенствами

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

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

Наконец, 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 Лупанова о сложности вычислений в конечных абелевых группах, помимо исследования исходных величин $L(g;B)$ и $L(G;B)$ 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 $n \to \infty$.

Сохранились (см., например, [16]) листочки с записями Олега Борисовича Лупанова, датированные, по-видимому 1988 г., в которых он ставил эту задачу автору, тогда еще пятикурснику.

В основе исследований задачи Лупанова лежат оценки величины

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

а эта задача тесно связана с задачей Беллмана не только очевидным неравенством

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

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

Направления исследований по задаче Лупанова. Можно выделить следующие составляющие исследований, связанных с задачей Лупанова:

I. Разработка достаточно универсальных (применимых как к задаче Беллмана, так и к задача 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.

Приоритетной целью настоящей работы является третье направление, но сначала вкратце остановимся на первых двух.

Направление I: общие методы и оценки для задач Беллмана и Лупанова. По этому направлению все результаты будут сформулированы только для задачи Беллмана.

Первым стоит назвать уже упоминавшийся результат Е. Штрауса [11]. Далее, следствием из более общего результата Н. Пиппенджера [7] 1980 г. является оценка

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

В 1992 г. автором совместно с С. Б. Гашковым установлено [17],

что

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

где $N = n_1 n_2 \dots n_m$.

В 1994 в работе [18] доказано, что для почти всех наборов $\tilde{n} = (n_1, n_2, \dots, n_m)$ эта нижняя оценка неулучшаема, т. е. справедливо асимптотическое равенство

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

В 2014 году получено [19] следующее усиление верхней оценки для задачи Беллмана:

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

Однако, этого оказалось недостаточно для получения асимптотически точного результата о сравнении оценок сложности в задачах Беллмана и Кнута, о котором будет сказано ниже. Последнюю верхнюю оценку удалось уточнить нужным образом, «отбросив» множитель $1 + o(1)$ в первом слагаемом:

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

Также стоит отметить следующий полученный в [19] результат. Пусть

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

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

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

Направление II: получение ответов на остальные вопросы из задачи Лупанова. Работы [20–24] дают ответ на вопрос об асимптотическом поведении соответствующих функций Шеннона:

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

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

Далее, в [22, 23] получены следующие результаты, касающиеся поведения функционалов сложности $m(\mathbf{v})$ и $M(\mathbf{v})$.

1. При $\|\mathbf{v}\| \to \infty$ выполняются соотношения

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

причем для любых медленно изменяющихся (по Карамате) функций $h_1(n)$ и $h_2(n)$, удовлетворяющих при $n \to \infty$ 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 $\|\mathbf{v}_s\| \to \infty$, для которой справедливы соотношения

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

2. При $\|\mathbf{v}\| \to \infty$ выполняются соотношения

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

где $q(\mathbf{v})$ — 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.

3. Для описания асимптотического поведения функционала $m(\mathbf{v})$ введем дополнительные обозначения. Пусть B — базис конечной абелевой группы G. Обозначим через $k(B)$ максимальный порядок среди базисных элементов, а также положим $r(B) = \lfloor\log(k(B)-1)\rfloor + |B|$ и $r(\mathbf{v}) = \min r(B)$, где минимум берется по всем базисам абелевой

группы, у которой порядки примарных циклических подгрупп задаются вектором $\mathbf{v}$.

При $\|\mathbf{v}\| \to \infty$ 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

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

Наконец, в [22] для величин $m_{\mathrm{cp}}(n)$ и $M_{\mathrm{cp}}(n)$ при $n \to \infty$ получены следующие асимптотические соотношения

$$\frac{\log n}{\log\log n} \lesssim m_{\mathrm{cp}}(n) \leq M_{\mathrm{cp}}(n) \lesssim \log n.$$

При этом установлено, что для любых медленно меняющихся (по Карамате) 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 подпоследовательность $\{n_s\}$, для которой справедливы соотношения

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

Направление III: степень различия значений сложности реализации одночленов и сложности элементов конечных абелевых групп. Задача о сложности вычисления одночлена $x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}$ и задача нахождения величины $L\left(a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}; \{a_1, a_2, \dots, a_m\}\right)$, безусловно, очень похожи, но все же это разные задачи. Действительно, с одной стороны, справедливо равенство $l(x^{31}) = 7$ (см., например, [1]), а с другой стороны, в группе $\langle a\rangle_{33}$, очевидно, выполняется соотношение $L(a^{31}, \{a\}) = 6$. 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 (подробнее см. [24]).

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

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

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

Будем говорить, что представлению элемента g в базисе B *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 в каноническом представлении элемента g в базисе B. Обозначим этот многочлен через $P[g; B]$.

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

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

Очевидно, что $L(g; B_G) \leq l(P[g; B_G])$. Как сильно могут отличаться величины $L(g; B_G)$ и $l(P[g; B_G])$?

Положим

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

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

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

В [24] доказано, что при $n \to \infty$ верно асимптотическое равенство

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

Верхняя оценка после описанного внешне незначительного последнего усиления верхней оценки задачи Беллмана становится почти очевидной.

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

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 $L(a^m; \{a\}) \le \lfloor \log n \rfloor$.

Далее, установлено, асимптотическое поведение величины $\pi(n)$ при $n \to \infty$ задается формулой

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

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

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

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.

Отметим, что 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 в соответствующей задаче Беллмана и сложности этого элемента в выбранном базисе было бы 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.

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

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

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

Рассмотрим абелеву группу

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

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

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

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

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

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

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

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

Таким образом,

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

Работа выполнена при частичной финансовой поддержке Минобрнауки России в рамках реализации программы Московского центра фундаментальной и прикладной математики по соглашению № 075-15-2022-284.

Список литературы

1. Кнут Д. Е. Искусство программирования для ЭВМ, т. 2. 1-е издание. — М.: Мир, 1977.

2. 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.

3. Gordon D. M. A survey of fast exponentiation methods // Journal of Algorithms. — 1998. — V. 27. — P. 129–146.

4. Thurber E. G., Clift N. M. Addition chains, vector chains, and efficient computation // Discrete Mathematics. — 2021. — V. 344, iss. 2. — 112200.

5. Brauer A. On addition chains // Bull. Amer. Math. Soc. — 1939. — V. 45. — P. 736–739.

6. Erdos P. Remarks on number theory, III: On addition chains // Acta Arith. — 1960. — V. 6. — P. 77–81.

7. Pippenger N. On evaluation of powers and monomials // SIAM J. Comput. — 1980. — V. 9, N 2. — P. 230–250.

8. Кочергин В. В., Кочергин Д. В. Уточнение нижней оценки сложности возведения в степень // Прикладная дискретная математика. — 2017. — № 38. — С. 119–132.

9. Schönhage A. A lower bound for the lenght of addition chains // Theoretical Computer Science. — 1975. — V. 1. — P. 1–12.

10. Bellman R. E. Addition chains of vectors (Advanced problem 5125) // Amer. Math. Monthly. — 1963. — V. 70. — P. 765.

11. Straus E. G. Addition chains of vectors // Amer. Math. Monthly. — 1964. — V. 71. — P. 806–808.

12. Сидоренко А. Ф. Сложность аддитивных вычислений семейств целочисленных линейных форм // Записки научных семинаров ЛОМИ. — Л.: Наука, 1981. — Т. 105. — С. 53–61.

13. 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.

14. Olivos J. On vectorial addition chains // J. Algorithms. — 1981. — V. 2, N 1. — P. 13–21.

15. Downey P., Leong B., Sethi R. Computing sequences with addition chains // SIAM Journal on Computing. — V. 10. — 1981. — P. 638–646.

16. URL: `http://new.math.msu.su/department/dm/data/uploads/zapisi_ob.pdf`

17. Гашков С. Б., Кочергин В. В. Об аддитивных цепочках векторов, вентильных схемах и сложности вычисления степеней // Методы дискретного анализа в теории графов и сложности. — Новосибирск, 1992. — Вып. 52. — С. 22–40.

18. Кочергин В. В. О сложности вычислений одночленов и наборов степеней // Дискретный анализ. — Новосибирск: Издательство Института математики СО РАН, 1994. — (Тр./РАН. Сиб. отделение. Ин-т математики; Т. 27) — С. 94–107.

19. 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.

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

21. Кочергин В. В. О сложности вычислений в конечных абелевых группах // Математические вопросы кибернетики, вып. 4. — М.: Наука, 1992. — С. 178–217.

22. Кочергин В. В. О некоторых мерах сложности конечных абелевых групп // Дискретн. мат. — 2015. — Т. 27, вып. 3. — С. 25–43.

23. 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.

24. Кочергин В. В. Сравнение сложности вычисления одночленов и элементов конечных абелевых групп // Вестник Московского университета. Сер. 1. Математика. Механика. — 2022, № 3. — С. 6–11.

DOI: 10.20948/dms-2022-1