2. *Лукашенко Т.П.* О свойствах орторекурсивных разложений по неортогональным системам // Вестн. Моск. ун-та. Матем. Механ. 2001. № 1. 6–10.
3. *Галатенко В.В.* Об орторекурсивном разложении с ошибками в вычислении коэффициентов // Изв. РАН. Сер. матем. 2005. **69**, № 1. 3–16.
4. *Filippov V.I., Oswald P.* Representation in L_p by series of translates and dilates of one function // J. Approx. Theory. 1995. **82**, N 1. 15–29.
5. *Кудрявцев А.Ю.* Орторекурсивные разложения по системам сжатий и сдвигов фиксированной функции // Современные методы теории функций и смежные проблемы: Тез. докл. Воронеж. зимней матем. школы. Воронеж, 2001. 161–162.
6. *Политов А.В.* Орторекурсивные разложения в гильбертовых пространствах // Вестн. Моск. ун-та. Матем. Механ. 2010. № 3. 95–99.
7. *Кашин Б.С., Саакян А.А.* Ортогональные ряды. М.: Наука, Гл. ред. физ.-мат. лит-ры, 1984.
8. *Дьяченко М.И., Ульянов П.Л.* Мера и интеграл. М.: Факториал, 1998.
9. *Кусис П.* Введение в теорию пространств H^p. М.: Мир, 1984.

Поступила в редакцию
03.02.2023

УДК 519.71

О СЛОЖНОСТИ ВЫЧИСЛЕНИЯ СИСТЕМ ЭЛЕМЕНТОВ КОНЕЧНЫХ АБЕЛЕВЫХ ГРУПП

В. В. Кочергин[1]

Исследуется сложность реализации систем элементов конечных абелевых групп. Под сложностью реализации системы элементов над заданным базисом понимается минимальное число применений групповых операций для вычисления элементов системы по базисным элементам, при этом допускается многократное использование результатов промежуточных вычислений. Для функции Шеннона $L(n, m)$, характеризующей максимальную сложность системы из m элементов, где максимум берется по всем абелевым группам порядка не более n, по всем их базисам и по всем реализуемым системам, установлено, что в случае выполнения условия $m = o(\log\log n)$ при $n \to \infty$ справедливо асимптотичское равенство $L(n, m) \sim \log_2 n$. Кроме того, при тех же условиях установлена асимптотика максимально возможного отличия сложности вычисления системы элементов конечной абелевой группы и сложности реализации системы одночленов, соответствующих представлениям этих элементов через базисные элементы.

Ключевые слова: конечная абелева группа, сложность вычисления, аддитивные цепочки, векторные аддитивные цепочки, задача Беллмана, задача Пиппенджера.

The computation compelxity of the systems of the finite Abelian group elements is studied in the paper. The complexity of computation means the minimal number of group operations required to calculate elements of the system over the basis elements, all results of intermediate calculations may be used multiple times. We define the Shannon function $L(n, m)$ as the maximal complexity of m-elements system group, the maximum is taken over all Abelian groups of order less than n, over all their bases, over all computed systems. It is stated that if $m = o(\log\log n)$ for $n \to \infty$, than the asymptotic equality $L(n, m) \sim \log_2 n$ is valid. In addition, the asymptotic of the maximal possible difference of computation complexity of the systems of a finite Abelian group elements and the computation complexity of a monomial system corresponding to the representation of these elements over basis elements is obtained under the same conditions.

[1] *Кочергин Вадим Васильевич* — доктор физ.-мат. наук, проф., зав. каф. дискретной математики мех.-мат. ф-та МГУ; проф. общеуниверситетской каф. высшей математики НИУ ВШЭ, e-mail: vvkoch@yandex.ru.

Kochergin Vadim Vasil'evich — Doctor of Physical and Mathematical Sciences, Professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Head of Chair of Discrete Mathematics; Professor, National Research University — Higher School of Economics, Independent HSE Departments / Department of Higher Mathematics.

Key words: finite Abelian group, computational complexity, addition chains, vectorial addition chains, Bellman's problem, Pippenger's problem.

DOI: 10.55959/MSU0579-9368-1-64-4-4

В работе исследуется задача о сложности реализации систем элементов конечных абелевых групп.

Пусть G — конечная абелева группа (по умножению), а подмножество $B = \{a_1, \ldots, a_q\}$ элементов группы — *базис* в группе G, т.е. 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 элемента g группы G под *сложностью реализации над базисом* B (формальные определения, в том числе на языке схем из функциональных элементов [1] и аддитивных цепочек [2], см., например, в [3–5]), обозначаемой через $L(g; B)$, понимается минимальное число операций умножения, достаточное для вычисления элемента g с использованием элементов множества B, причем все уже вычисленные элементы могут быть использованы многократно — в этом принципиальное отличие этой, "схемной", меры сложности от другой, "формульной" (см., например, [6]), меры сложности вычислений элементов в группах. 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, [7]).

Следуя [3], определим функцию Шеннона $L(n)$ сложности реализации элементов абелевых групп равенством $L(n) = \max L(g, B)$, где максимум берется по всем элементам g и по всем базисам B всех абелевых групп порядка не более n.

Рост функции Шеннона $L(n)$ установлен с большой точностью: в [3] доказано, что при $n \to \infty$ справедливо равенство[2]

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

В работах [3–5, 8–11] изучались различные аспекты задачи о сложности вычисления элементов конечных абелевых групп. В настоящей работе исследуется сложность вычисления не одного элемента, а системы элементов конечной абелевой группы.

Для произвольного подмножества $M = \{g_1, g_2, \ldots, g_m\}$ элементов группы G определим его *сложность реализации над базисом* B, обозначаемую через $L(M; B)$, как минимальное число операций умножения, достаточное для вычисления элементов множества M с использованием элементов множества B.

Введем функцию Шеннона $L(n, m)$ сложности реализации систем элементов абелевых групп, положив

$$L(n, m) = \max L(M; B),$$

где максимум берется по всем абелевым группам порядка не более n, по всем их базисам B и по всем m-элементным подмножествам M этих групп.

Теорема 1. *Пусть при* $n \to \infty$ *выполняется условие* $m = m(n) = o(\log \log n)$. *Тогда*

$$L(n, m) \sim \log n.$$

Утверждение теоремы 1 базируется на двух леммах.

Лемма 1. *Пусть*

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

причем выполнены следующие условия:

1) $\log \min(u_1, \ldots, u_q) \geqslant (\log |G|)^{\frac{1}{2}}$;

2) $m = o(\log \log |G|)$ *при* $|G| \to \infty$.

Тогда для произвольной системы $M = \{g_1, g_2, \ldots, g_m\}$ *элементов группы* G *справедливо соотношение*

$$L(M; \{a_1, \ldots, a_q\}) \leqslant \log |G| + o(\log |G|).$$

[2]Здесь и далее все логарифмы берутся по основанию 2.

Доказательство. Будем использовать обозначения $n = |G|$, $B = \{a_1, \ldots, a_q\}$.

Пусть в разложение элемента g_i базисный элемент a_j входит в степени k_{ij}, где $k_{ij} \leqslant u_j - 1$, $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, q$,

Отдельно для каждого j, $j = 1, 2, \ldots, q$, вычислим элементы $a_j^{k_{1j}}, a_j^{k_{2j}}, \ldots, a_j^{k_{mj}}$. Для этого все показатели степени k_{ij} элемента a_j представим в системе счисления по основанию 2^{d_j}, где

$$d_j = \lfloor \log\log u_j - \log\log\log n \rfloor.$$

Вычислить все элементы $a_j^{k_{1j}}, a_j^{k_{2j}}, \ldots, a_j^{k_{mj}}$ можно в два этапа. На первом вычисляются все степени вида $a_j^{2^{d_j t}}$, где $2^{d_j t}$ не превосходит $u_j - 1$, на это будет потрачено не более $\log u_j$ операций. На втором этапе методом Яо (см. [12] или, например, [5]) из этих степеней "собираются" элементы $a_j^{k_{1j}}, a_j^{k_{2j}}, \ldots, a_j^{k_{mj}}$, на получение каждой из этих m степеней дополнительно потребуется не более

$$\frac{\log u_j}{d_j} + 2^{d_j}$$

операций (на самом деле слагаемое 2^{d_j} можно добавить только один раз для всех m степеней).

Таким образом, суммируя эти верхние оценки числа операций для всех базисных элементов a_j, заключаем, что

$$L\left(M; \{a_1, \ldots, a_q\}\right) \leqslant \sum_{j=1}^{q} \log u_j + m \sum_{j=1}^{q} \frac{\log u_j}{d_j} + m \sum_{j=1}^{q} 2^{d_j} + m(q-1).$$

Следующим образом оценивая отдельно каждое слагаемое

$$\sum_{j=1}^{q} \log u_j = \log n, \qquad m \sum_{j=1}^{q} \frac{\log u_j}{d_j} \leqslant 4m \sum_{j=1}^{q} \frac{\log u_j}{\log\log n} = \frac{4m \log n}{\log\log n} = o(\log n),$$

$$m \sum_{j=1}^{q} 2^{d_j} \leqslant m \sum_{j=1}^{q} \frac{\log u_j}{\log\log n} = \frac{m \log n}{\log\log n} = o(\log n), \qquad m(q-1) \leqslant m \frac{\log n}{\sqrt{\log n}} = o(\log n),$$

получаем требуемое соотношение. Лемма 1 доказана.

Лемма 2. *Пусть*

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

причем выполнены следующие условия:

1) $\log \max(u_1, \ldots, u_q) \leqslant (\log |G|)^{\frac{3}{4}}$;

2) $m = o\left(\log\log |G|\right)$ *при* $|G| \to \infty$.

Тогда для произвольной системы $M = \{g_1, g_2, \ldots, g_m\}$ *элементов группы* G *справедливо соотношение*

$$L\left(M; \{a_1, \ldots, a_q\}\right) \leqslant \log |G| + o(\log |G|).$$

Доказательство. Обозначим $n = |G|$. Введем натуральный параметр d, значение которого выберем позже.

Пусть для $j = 1, 2, \ldots, q$ представление величины $u_j - 1$ в системе счисления по основанию 2^d имеет $s_j + 1$ разряд, т.е. $s_j + 1 = \lceil \log_{2^d} u_j \rceil$. Положим $s = \max s_j$. Без ограничения общности будем считать, что выполняются неравенства $u_1 \geqslant u_2 \geqslant \ldots \geqslant u_q$. Тогда $s = s_1$.

В записи чисел в системе счисления по основанию 2^d будем называть младший разряд нулевым, следующий разряд — первым и т. д. В представлении всех q величин $u_j - 1$, естественно, будет нулевой разряд. Для $i = 1, 2, \ldots, s$ обозначим через q_i количество базисных элементов a_j, для которых в представлении величины $u_j - 1$ в системе счисления по основанию 2^d присутствует i-й разряд. Для единообразия положим $q_0 = q$. Тогда

$$\sum_{i=0}^{s} q_i = \sum_{j=1}^{q} (s_j + 1) = \sum_{j=1}^{q} \lceil \log_{2^d} u_j \rceil = \sum_{j=1}^{q} \left\lceil \frac{\log u_j}{d} \right\rceil < \frac{\log n}{d} + q.$$

Произвольный элемент h группы G можно представить в следующем виде:

$$h = \left(a_1^{k_{01}} \dots a_{q_0}^{k_{0q_0}}\right)\left(a_1^{k_{11}} \dots a_{q_1}^{k_{1q_1}}\right)^{2^d} \dots \left(a_1^{k_{s-1,1}} \dots a_{q_{s-1}}^{k_{s-1,q_{s-1}}}\right)^{2^{d(s-1)}} \left(a_1^{k_{s1}} \dots a_{q_s}^{k_{sq_s}}\right)^{2^{ds}} =$$

$$= \left(\dots\left(\left(a_1^{k_{s1}} \dots a_{q_s}^{k_{sq_s}}\right)^{2^d}\left(a_1^{k_{s-1,1}} \dots a_{q_{s-1}}^{k_{s-1,q_{s-1}}}\right)\right)^{2^d} \dots \left(a_1^{k_{11}} \dots a_{q_1}^{k_{1q_1}}\right)\right)^{2^d} \left(a_1^{k_{01}} \dots a_{q_0}^{k_{0q_0}}\right) =$$

$$= \left(\dots\left(h_s^{2^d} h_{s-1}\right)^{2^d} \dots h_1\right)^{2^d} h_0,$$

где все показатели степени k_{ij} не превосходят $2^d - 1$, а каждый элемент h_i является произведением степеней первых q_i базисных элементов, в котором показатели степеней не превосходят $2^d - 1$.

С использованием этого "послойного" представления сам элемент h можно вычислить по элементам $h_0, h_1, \dots, h_s$, затратив не более $(d+1)s$ операций умножения.

На основе таких "послойных" представлений для реализуемых элементов $g_1, g_2, \dots, g_m$ задача вычисления системы M сводится к задаче вычисления систем $M_0, M_1, \dots, M_s$, где M_i — система из m элементов, являющихся i-ми слоями элементов из системы M и порожденных первыми q_i базисными элементами.

Покажем, как можно вычислить систему элементов

$$a_1^{l_{11}} a_2^{l_{12}} \dots a_r^{l_{1r}}, \quad a_1^{l_{21}} a_2^{l_{22}} \dots a_r^{l_{2r}}, \ \dots, \ a_1^{l_{m1}} a_2^{l_{m2}} \dots a_r^{l_{mr}},$$

где все показатели степени l_{ij} не превосходят $2^d - 1$.

Множество базисных элементов a_j, $j = 1, 2, \dots, a_r$, разобьем на группы с одинаковыми наборами $(l_{1j}, l_{2j}, \dots, l_{mj})$ показателей степеней этих элементов в вычисляемой системе. Количество таких групп не превосходит величины 2^{dm}. Для каждой из этих групп можно реализовать произведение входящих в данную группу базисных элементов, используя не более r операций умножения для получения сразу всех групп.

Далее, для каждой группы вычислим нужные степени реализованных произведений. Скажем, для группы, включающей в себя базисный элемент a_j, возведем соответствующее произведение в степени $l_{1j}, l_{2j}, \dots, l_{mj}$. На это потребуется не более $2dm$ операций на каждую группу. После этого вычислить элементы $a_1^{l_{i1}} a_2^{l_{i2}} \dots a_r^{l_{ir}}$, $i = 1, 2, \dots, m$, можно, истратив не более $m2^{dm}$ операций.

Итого, для получения системы элементов $a_1^{l_{11}} a_2^{l_{12}} \dots a_r^{l_{1r}}$, $a_1^{l_{21}} a_2^{l_{22}} \dots a_r^{l_{2r}}$, $\dots$, $a_1^{l_{m1}} a_2^{l_{m2}} \dots a_r^{l_{mr}}$ достаточно

$$r + 2dm2^{dm} + m2^{dm}$$

операций.

Суммируя оценки для реализации отдельных слоев и добавляя оценку на число операций для окончательной "сборки" элементов $g_1, g_2, \dots, g_m$, получаем

$$L(M; \{a_1, \dots, a_q\}) \leqslant \sum_{i=0}^{s} \left(q_i + 2dm2^{dm} + m2^{dm}\right) + m(d+1)s \leqslant$$

$$\leqslant q + \frac{\log n}{d} + \left(\frac{\log u_1}{d} + 1\right)(2dm2^{dm} + m2^{dm}) + m(\log u_1)^{1+\frac{1}{d}} \leqslant$$

$$\leqslant q + \frac{\log n}{d} + \left((\log n)^{\frac{3}{4}} + 1\right)(2dm2^{dm} + m2^{dm}) + m\,(\log n)^{\frac{3}{4}+\frac{3}{4d}}.$$

Положим

$$d = \left\lfloor \sqrt{\frac{\log\log n}{m}} \right\rfloor.$$

Тогда $d \to \infty$ при $n \to \infty$ и $dm \leqslant \sqrt{m \log\log n} = o(\log\log n)$. Поэтому при всех достаточно больших значениях n выполняется неравенство $dm \leqslant \frac{1}{5}\log\log n$, а следовательно, и оценка $2^{dm} \leqslant (\log n)^{1/5}$. Учитывая эти соотношения, окончательно получаем

$$L(M; \{a_1, \dots, a_q\}) \leqslant q + o(\log n) \leqslant \log n + o(\log n).$$

Лемма 2 доказана.

Доказательство теоремы 1. Пусть группа G порядка не более n, ее базис B и система M из m элементов группы G удовлетворяют условию $L(M;B) = L(n,m)$. Элементы базиса B разобьем на два подмножества в зависимости от значения порядка этих элементов. Элемент $a \in B$ порядка u отнесем к множеству B_1 в случае, если выполняется неравенство

$$\log u \geqslant (\log |G|)^{\frac{1}{2}},$$

в противном случае отнесем элемент a к множеству B_2. Если множество B_i, $i = 1, 2$, непусто, то обозначим через G_i подгруппу группы G (возможно, совпадающую со всей группой), порожденную множеством B_i, при этом множество B_i будет базисом в группе G_i.

Каждый элемент g реализуемого множества M однозначно представляется в виде $g = g_1 g_2$, где $g_1 \in G_1$, $g_2 \in G_2$. Таким образом, множество M индуцирует множества M_1 и M_2 мощности m, состоящие из элементов групп G_1 и G_2 соответственно. Очевидно, что

$$L(M;B) \leqslant L(M_1;B_1) + L(M_2;B_2) + m.$$

Если для одной из групп G_i, $i = 1$ или $i = 2$, выполняется условие

$$\log |G_i| < (\log |G|)/(\log\log |G|)^3,$$

то, применяя для вычисления произвольного элемента h из группы G_i теорему 4 из [3] или теорему 1 из [13] (см. также [14, 15]), получаем

$$L(h;B_i) = O\left(\log |G_i|\right).$$

Следовательно, в этом случае

$$L(M_i;B_i) \leqslant mO\left(\log |G_i|\right) = o\left(\log\log n \frac{\log |G|}{(\log\log |G|)^3}\right) = o(\log n).$$

Далее будем предполагать, что выполняются условия

$$\log |G_i| \geqslant (\log |G|)/(\log\log |G|)^3, \quad i = 1, 2.$$

Тогда для группы G_1 выполнены все условия леммы 1. Поэтому

$$L(M_1;B_1) \leqslant \log |G_1| + o(\log |G_1|) = \log |G_1| + o(\log n).$$

Теперь оценим сверху величину $L(M_2;B_2)$. В силу предположения при всех достаточно больших значениях величины $|G|$ выполняются неравенства

$$\log\log |G_2| \geqslant \log\log |G| - 3\log\log\log |G| \geqslant \frac{1}{2}\log\log |G|.$$

Следовательно, обозначив через u максимальный порядок среди элементов множества B_2, будем иметь

$$\log u < (\log |G|)^{\frac{1}{2}} \leqslant \left(\log |G_2| \left(\log\log |G|\right)^3\right)^{\frac{1}{2}} \leqslant \left(8\log |G_2| \left(\log\log |G_2|\right)^3\right)^{\frac{1}{2}}.$$

Тем самым выполнены условия леммы 2. Применяя ее, получаем

$$L(M_2;B_2) \leqslant \log |G_2| + o(\log |G_2|) = \log |G_2| + o(\log n).$$

Суммируя соответствующие оценки, окончательно имеем

$$L(M;B) \leqslant \log |G| + o(\log n) \leqslant \log n + o(\log n).$$

Верхняя оценка теоремы доказана.

Для установления нижней оценки достаточно воспользоваться следующим простым фактом: для сложности вычисления элемента g^{n-1} циклической группы $\langle g \rangle$ порядка n справедливо неравенство

$$L\left(g;\{g\}\right) \geqslant \log(n-1).$$

Теорема 1 доказана.

Теперь перейдем к одной задаче, решение которой существенно опирается на теорему 1.

В работе [10] исследовался вопрос о возможной степени различия соответствующих величин в задаче Лупанова о сложности вычисления элементов конечной абелевой группы и в задаче Беллмана о сложности вычисления нормированного одночлена от многих переменных (о задаче Беллмана подробнее см., например, [5, 14–16]), который формализуется следующим образом.

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

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

является *каноническим*, если для всех значений j, $1 \leqslant j \leqslant q$, выполняются неравенства $0 \leqslant n_j \leqslant u_j - 1$, где u_j — порядок базисного элемента a_j.

Представлению элемента g в базисе $B = \{a_1, \ldots, a_q\}$ конечной абелевой группы G *соответствует* одночлен $x_1^{n_1} x_2^{n_2} \ldots x_q^{n_q}$, у которого 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, обозначается через $P[g; B]$.

В [10] исследовалась функция $\sigma(n)$, определяемая равенством $\sigma(n) = \max\{l(P[g; B]) - L(g; B)\}$, где максимум берется по всем элементам и всем базисам всех абелевых групп, имеющих порядок, не превосходящий n. Величина $\sigma(n)$ показывает, на сколько вычисление элемента конечной абелевой группы порядка не более n в каком-либо базисе этой группы может быть экономнее, чем вычисление одночлена, соответствующего представлению этого элемента в выбранном базисе. В [10] установлено, что при $n \to \infty$ справедливо асимптотическое равенство

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

Важно отметить, что доказанная в теореме 2 работы [10] нижняя оценка величины $\sigma(n)$ ввиду использования мощностной нижней оценки для задачи Беллмана носит неконструктивный характер и не дает возможности предъявить элемент и базис конечной абелевой группы, для которых разность сложности для соответствующей задачи Беллмана и сложности этого элемента в выбранном базисе была бы достаточно велика. В то же время, как показано в примере из [10], при сравнении сложности реализации системы элементов конечных абелевых групп и сложности соответствующей системы одночленов ситуация может быть иной.

Формализуем эту задачу сравнения сложности реализации системы элементов конечной абелевой группы и сложности реализации соответствующей системы одночленов.

Пусть $M = \{g_1, g_2, \ldots, g_m\}$ — система элементов конечной абелевой группы, заданной своим базисом B. Положим

$$\hat{M} = \{P[g_1; B], P[g_2; B], \ldots, P[g_m; B]\}.$$

Обозначим через $l\left(\hat{M}\right)$ сложность реализации системы одночленов $\hat{M}$, т.е. минимально возможное число операций умножения, достаточное для получения системы $\hat{M}$ (подробнее об исследовании задачи о сложности вычисления систем одночленов, известной как задача Пиппенджера, см., например, [5, 15, 17]).

Наконец, положим

$$\sigma(n, m) = \max\left\{l\left(\hat{M}\right) - L(M; B)\right\},$$

где максимум берется по всем m-элементным системам M и всем базисам B всех абелевых групп, имеющих порядок, не превосходящий n. Отметим, что задача об изучении величины $\sigma(n, m)$ перекликается с некоторыми задачами, о которых идет речь в обзоре [18].

Прежде чем перейти к исследованию асимптотического роста величины $\sigma(n, m)$, отметим, что при доказательстве теоремы 1 все верхние оценки сложности систем элементов конечных абелевых групп остаются справедливыми и для соответствующих им систем одночленов. Сформулируем этот факт в виде леммы.

Лемма 3. *Для произвольной системы $M = \{g_1, \ldots, g_m\}$ элементов абелевой группы порядка не более n и любого базиса этой группы в случае выполнения условия $m = o(\log \log n)$ при $n \to \infty$ справедливо соотношение*

$$l\left(\hat{M}\right) \leqslant (1 + o(1)) \log n.$$

Теорема 2. *Пусть при* $n \to \infty$ *выполняются условия* $m \geqslant 2$ *и* $m(n) = o(\log\log n)$. *Тогда*

$$\sigma(n, m) \sim \frac{m-1}{m} \log n.$$

Доказательство. *Нижняя оценка* по существу содержится в примере из [10]. В соответствии с введенными обозначениями кратко опишем эту конструкцию. Отметим, что для доказательства нижней оценки достаточно, чтобы выполнялось более слабое условие, а именно, чтобы при $n \to \infty$ выполнялось соотношение $m = m(n) = o\left(\sqrt{\log n}\right)$.

Положим

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

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

Рассмотрим абелеву группу

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

Для порядка этой группы выполняются неравенства $|G| < k^m 2^{m(m+1)/2} \leqslant n$.

В группе G выберем систему элементов $\{g_1, \ldots, g_m\}$, задаваемых в базисе $B = \{a_1, a_2, \ldots, a_m\}$ следующими каноническими представлениями:

$$g_1 = a_1^k \ldots a_m^k, \quad g_2 = a_2^{2k} \ldots a_m^{2k}, \ldots, g_m = a_m^{2^{m-1}k}.$$

В силу равенств $g_{i+1} = g_i^2$, $i = 1, \ \ldots, \ m-1$, верны соотношения

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

С другой стороны, применяя нижнюю оценку через логарифм определителя матрицы, задающей показатели степеней в одночленах системы (см., например, [5, 15, 19]), имеем

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

Таким образом, для системы $M = \{g_1, \ldots, g_m\}$ элементов группы G выполняется соотношение

$$l\left(\hat{M}\right) - L(M; B) \gtrsim \frac{m-1}{m} \log n,$$

тем самым нижняя оценка доказана.

Верхняя оценка. Пусть группа G порядка не более n, базис B и система элементов $M = \{g_1, \ldots, g_m\}$ этой группы выбраны так, что выполняется равенство

$$l\left(\hat{M}\right) - L(M; B) = \sigma(n, m).$$

Кроме того, без ограничения общности будем считать, что среди одночленов $P[g_i; B]$, $i = 1, \ldots, m$, наибольшую сложность имеет одночлен $P[g_1; B]$, т.е. имеет место равенство

$$l\left(P[g_1; B]\right) = \max\left(l\left(P[g_1; B]\right), \ldots, l\left(P[g_m; B]\right)\right).$$

Тогда

$$l\left(P[g_1; B]\right) \geqslant \frac{1}{m} \sum_{i=1}^{m} l\left(P[g_i; B]\right) \geqslant \frac{1}{m} l\left(\hat{M}\right).$$

Далее, в силу уже упоминавшегося соотношения $\sigma(n) \sim (\log n)/\log\log n$, верного при $n \to \infty$ (теорема 2 из [10]), справедливо неравенство

$$l\left(P[g_1; B]\right) - L(g_1; B) \leqslant \frac{\log n}{\log\log n}(1 + o(1)).$$

Таким образом,

$$\sigma(n,m) = l\left(\hat{M}\right) - L(M;B) \leqslant l\left(\hat{M}\right) - L(g_1;B) \leqslant l\left(\hat{M}\right) - l\left(P[g_1;B]\right) + \frac{\log n}{\log\log n}(1+o(1)) \leqslant$$

$$\leqslant \frac{m-1}{m} l\left(\hat{M}\right) + \frac{\log n}{\log\log n}(1+o(1)).$$

Применение леммы 3 завершает доказательство верхней оценки. Теорема 2 доказана.

Тем самым приведен конструктивный пример системы из m элементов конечной абелевой группы, для которой в случае слабого роста параметра m при реализации этой системы в некотором базисе экономия в количестве операций по сравнению с вычислением системы одночленов, соответствующих представлениям этих элементов, асимптотически равна логарифму от порядка группы.

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

СПИСОК ЛИТЕРАТУРЫ

1. *Лупанов О.Б.* О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып. 10. М.: Физматгиз, 1963. 63–97.
2. *Кнут Д.Е.* Искусство программирования. Т. 2. 3-е изд. М.: Издательский дом "Вильямс", 2000.
3. *Кочергин В.В.* О сложности вычислений в конечных абелевых группах // Математические вопросы кибернетики. Вып. 4. М.: Наука, 1992. 178–217.
4. *Кочергин В.В.* О некоторых мерах сложности конечных абелевых групп // Дискретн. матем. 2015. **27**, № 3. 25–43.
5. *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. 119–256.
6. *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. 5–32.
7. *Ольшанский А.Ю.* О сложности вычислений в группах // Соросовский образовательный журнал. 2000. **6**, N 3. 118–123.
8. *Кочергин В.В.* О сложности вычислений в конечных абелевых группах // Докл. АН СССР. 1991. **317**, № 2. 291–294.
9. *Кочергин В.В.* Об одной задаче О. Б. Лупанова // Мат-лы XII Междунар. семинара "Дискретная математика и ее приложения" им. академика О. Б. Лупанова. М., 2016. 4–17.
10. *Кочергин В.В.* Сравнение сложности вычисления одночленов и элементов конечных абелевых групп // Вестн. Моск. ун-та. Матем. Механ. 2022. № 3. 6–11.
11. *Кочергин В.В.* Сравнение оценок сложности для задач Р. Беллмана и О. Б. Лупанова // Мат-лы XIV Междунар. семинара "Дискретная математика и ее приложения" им. академика О. Б. Лупанова (Москва, МГУ, 20–25 июня 2022 г.). М.: ИПМ им. М. В. Келдыша, 2022. 4–16.
12. *Yao A. C.C.* On the evaluation of powers // SIAM J. Comput. 1976. **5**. 100–103.
13. *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. **52**. 22–40.
14. *Кочергин В.В.* Уточнение оценок сложности вычисления одночленов и наборов степеней в задачах Беллмана и Кнута // Дискретн. анализ и исслед. операций. 2014. **21**, № 6. 51–72.
15. *Кочергин В.В.* О задачах Беллмана и Кнута и их обобщениях // Фунд. и прикл. матем. 2015. **20**, № 6. 159–189.
16. *Straus E.G.* Addition chains of vectors // Amer. Math. Monthly. 1964. **71**. 806–808.
17. *Pippenger N.* On evaluation of powers and monomials // SIAM J. Comput. 1980. **9**, N 2. 230–250.
18. *Jukna S., Sergeev I.* Complexity of linear Boolean operators // Found. and Trends in Theor. Comput. Sci. 2013. **9**, N 1. 1–123.
19. *Morgenstern J.* Note on a lower bound of the linear complexity of the fast Fourier transform // J. Assoc. Comput. Mach. 1973. **20**. 305–306.

Поступила в редакцию
17.02.2023