Math-Net.Ru

Общероссийский математический портал

В. В. Кочергин, О сложности вычисления систем одночленов с ограничениями на степени переменных, *Дискрет. матем.*, 1998, том 10, выпуск 3, 27–34

DOI: <https://doi.org/10.4213/dm434>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.81.137.203

26 апреля 2023 г., 12:49:55

УДК 519.7

О сложности вычисления систем одночленов с ограничениями на степени переменных

© 1998 г. В. В. Кочергин

Рассматривается задача о сложности вычисления систем одночленов от многих переменных, получено обобщение известного результата Пиппенджера на случай различных верхних границ степеней переменных в одночленах.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 96-01-01068, и ФЦП «Интеграция», проект 473.

Рассматривается задача о сложности вычисления систем одночленов от многих переменных (см., например, [1]).

Пусть $\mathcal{K} = (k_1, k_2, \dots, k_q)$ — набор из q натуральных чисел, больших единицы.

Обозначим через $L(\mathcal{K}, p)$ наименьшее число операций умножения, достаточное для вычисления по переменным $x_1, x_2, \dots, x_q$ любой системы $y_1, y_2, \dots, y_p$, где

$$y_1 = x_1^{r_{11}} x_2^{r_{12}} \dots x_q^{r_{1q}},$$

$$y_2 = x_1^{r_{21}} x_2^{r_{22}} \dots x_q^{r_{2q}},$$

...

$$y_p = x_1^{r_{p1}} x_2^{r_{p2}} \dots x_q^{r_{pq}},$$

удовлетворяющей условиям $r_{ij} \leq k_j - 1$, $i = 1, \dots, p$, $j = 1, \dots, q$.

Через $L^*(\mathcal{K}, p)$ обозначим наименьшее число операций умножения, достаточное для вычисления по переменным $x_1, x_2, \dots, x_p$ любой системы $y_1, y_2, \dots, y_q$, где

$$y_1 = x_1^{r_{11}} x_2^{r_{12}} \dots x_p^{r_{1p}},$$

$$y_2 = x_1^{r_{21}} x_2^{r_{22}} \dots x_p^{r_{2p}},$$

...

$$y_q = x_1^{r_{1q}} x_2^{r_{2q}} \dots x_p^{r_{pq}},$$

удовлетворяющей условиям $r_{ij} \leq k_j - 1$, $i = 1, \dots, p$, $j = 1, \dots, q$.

Положим $K = k_1 k_2 \dots k_q$.

В дальнейшем при изучении поведения функционала $L(\mathcal{K}, p)$ будем считать, что выполнено естественное условие $p \leq K$, а при изучении поведения функционала $L^*(\mathcal{K}, p)$ условие $q \leq K$ (то есть число вычисляемых одночленов не превосходит общего числа одночленов соответствующего вида).

Сформулируем на языке введенных обозначений известные результаты из данной области. Заметим, что в данной работе логарифмы берутся по основанию 2.

Пусть $\mathcal{K} = (k)$, $p = 1$. Тогда при $k \rightarrow \infty$

$$L((k), 1) = \log k + \frac{\log k}{\log \log k} \left(1 + o \left(\frac{\log \log \log k}{\log \log k} \right) \right).$$

Верхняя оценка была установлена А. Брауэром [2], а нижняя П. Эрдёшем [3] (см. также [4]).

Пусть $p = 1$. Тогда задача изучения поведения функционала $L(\mathcal{K}, 1)$ есть, по существу, задача Д. Кнута (см. [4], разд. 4.6.3., упр. 32), а функционала $L^*(\mathcal{K}, 1)$ задача Р. Беллмана [5].

В работах [6, 7] было показано, что при $K \rightarrow \infty$

$$\begin{aligned} L(\mathcal{K}, 1) &= \log(\max k_i) + \frac{\log K}{\log \log K} (1 + o(1)) + O(q), \\ L^*(\mathcal{K}, 1) &= \log(\max k_i) + \frac{\log K}{\log \log K} (1 + o(1)) + O(q). \end{aligned}$$

Пусть $k_1 = \dots = k_q = k$. Тогда справедливо установленное Н. Пиппенджером [8] равенство: при $k \rightarrow \infty$

$$L(\mathcal{K}, p) = \min(p, q) \log k + \frac{pq \log k}{\log(pq \log k)} (1 + o(1)) + O(p + q).$$

Без ограничения общности будем считать, что $k_1 \geq k_2 \geq \dots \geq k_q$. Всюду запись $f \asymp g$ означает, что одновременно выполняются соотношения $f = O(g)$ и $g = O(f)$, а запись $f \sim g$ означает, что при стремлении некоторого параметра к бесконечности $f = g(1 + o(1))$.

Теорема 1. Пусть $p \log K \rightarrow \infty$. Тогда

$$\begin{aligned} L(\mathcal{K}, p) &\asymp \sum_{i=1}^{\min(p, q)} \log k_i + \frac{p \log K}{\log(p \log K)} + p + q, \\ L^*(\mathcal{K}, p) &\asymp \sum_{i=1}^{\min(p, q)} \log k_i + \frac{p \log K}{\log(p \log K)} + p + q, \end{aligned}$$

причем, если выполняются условия

$$\sum_{i=1}^{\min(p, q)} \log k_i + p + q = o \left(\frac{p \log K}{\log(p \log K)} \right), \quad q = o(\log K),$$

то справедливы соотношения

$$\begin{aligned} L(\mathcal{K}, p) &\sim \frac{p \log K}{\log(p \log K)}, \\ L^*(\mathcal{K}, p) &\sim \frac{p \log K}{\log(p \log K)}. \end{aligned}$$

Доказательство. В силу леммы 2 из [6] наименьшее число операций умножения, достаточное для вычисления по переменным $x_1, x_2, \dots, x_q$ системы из p одночленов от этих переменных

$$\begin{aligned} & x_1^{r_{11}} x_2^{r_{12}} \dots x_q^{r_{1q}}, \\ & x_1^{r_{21}} x_2^{r_{22}} \dots x_q^{r_{2q}}, \\ & \dots \\ & x_1^{r_{p1}} x_2^{r_{p2}} \dots x_q^{r_{pq}}, \end{aligned}$$

и наименьшее число операций умножения, достаточное для вычисления по переменным $x_1, x_2, \dots, x_p$ системы из q одночленов от этих переменных

$$\begin{aligned} & x_1^{r_{11}} x_2^{r_{21}} \dots x_p^{r_{p1}}, \\ & x_1^{r_{12}} x_2^{r_{22}} \dots x_p^{r_{p2}}, \\ & \dots \\ & x_1^{r_{1q}} x_2^{r_{2q}} \dots x_p^{r_{pq}}, \end{aligned}$$

отличаются, в случае, когда в матрице (r_{ij}) нет нулевых строк и нулевых столбцов, на величину $q - p$. Поэтому справедливо равенство

$$L^*(\mathcal{X}, p) + q = L(\mathcal{X}, p) + p.$$

Следовательно, достаточно доказать утверждения теоремы только для величины $L(\mathcal{X}, p)$ (с последующим небольшим уточнением нижней оценки для величины $L^*(\mathcal{X}, p)$).

Найдем верхнюю оценку. Отдельно рассмотрим случаи $p \geq q$ и $p < q$.

Пусть выполняется неравенство $p \geq q$. Обозначим последовательно через

$$u_1, u_2, \dots, u_s, \quad s = \lceil \log k_1 \rceil + \lceil \log k_2 \rceil + \dots + \lceil \log k_q \rceil,$$

следующие степени исходных переменных

$$x_1, x_1^2, x_1^4, \dots, x_1^{2^{\lceil \log k_1 \rceil - 1}}, x_2, x_2^2, x_2^4, \dots, x_2^{2^{\lceil \log k_2 \rceil - 1}}, \dots, x_q, x_q^2, x_q^4, \dots, x_q^{2^{\lceil \log k_q \rceil - 1}}.$$

Тогда систему одночленов $y_1, y_2, \dots, y_p$ можно представить в виде

$$\begin{aligned} y_1 &= u_1^{a_{11}} u_2^{a_{12}} \dots u_s^{a_{1s}}, \\ y_2 &= u_1^{a_{21}} u_2^{a_{22}} \dots u_s^{a_{2s}}, \\ &\dots \\ y_p &= u_1^{a_{p1}} u_2^{a_{p2}} \dots u_s^{a_{ps}}, \end{aligned}$$

где $a_{ij} \in \{0, 1\}$, $i = 1, \dots, p$, $j = 1, \dots, s$.

В соответствии с результатом работы [8], для вычисления системы $y_1, y_2, \dots, y_p$ по переменным $u_1, u_2, \dots, u_s$ требуется не более

$$s + \frac{ps}{\log(ps)}(1 + o(1)) + O(p + s)$$

операций умножения. Поэтому в условиях первого случая

$$\begin{aligned} L(\mathcal{K}, p) &\leq s + \frac{ps}{\log(ps)}(1 + o(1)) + O(p + s) \\ &= \frac{p \log K}{\log(p \log K)}(1 + o(1)) + O\left(\sum_{i=1}^q \log k_i + p\right) \\ &= \frac{p \log K}{\log(p \log K)}(1 + o(1)) + O\left(\sum_{i=1}^{\min(p, q)} \log k_i + p + q\right). \end{aligned}$$

Пусть теперь выполняется неравенство $p < q$. Представим каждый одночлен y_i , $i = 1, \dots, p$, в виде $y_i = y'_i y''_i$, где

$$y'_i = x_1^{r_{i1}} x_2^{r_{i2}} \dots x_p^{r_{ip}}, \quad y''_i = x_{p+1}^{r_{i,p+1}} x_{p+2}^{r_{i,p+2}} \dots x_q^{r_{iq}}.$$

Положим

$$K' = k_1 k_2 \dots k_p, \quad K'' = k_{p+1} k_{p+2} \dots k_q.$$

Как показано в предыдущем случае, для вычисления системы одночленов $y'_1, y'_2, \dots, y'_p$ достаточно

$$\frac{p \log K'}{\log(p \log K')}(1 + o(1)) + O\left(\sum_{i=1}^p \log k_i\right)$$

операций умножения.

Для вычисления системы одночленов $y''_1, y''_2, \dots, y''_p$ представим эти одночлены следующим образом:

$$\begin{aligned} y''_1 &= v_1(v_2(v_3(\dots(v_{\lfloor \log k_{p+1} \rfloor - 1}(v_{\lfloor \log k_{p+1} \rfloor})^2 \dots)^2)^2)^2, \\ y''_2 &= v_{1+\lfloor \log k_{p+1} \rfloor}(v_{2+\lfloor \log k_{p+1} \rfloor}(v_{3+\lfloor \log k_{p+1} \rfloor}(\dots(v_{2\lfloor \log k_{p+1} \rfloor - 1}(v_{2\lfloor \log k_{p+1} \rfloor})^2 \dots)^2)^2)^2, \\ &\dots \\ y''_p &= v_{1+(p-1)\lfloor \log k_{p+1} \rfloor}(v_{2+(p-1)\lfloor \log k_{p+1} \rfloor}(v_{3+(p-1)\lfloor \log k_{p+1} \rfloor}(\dots(v_{p\lfloor \log k_{p+1} \rfloor - 1}(v_{p\lfloor \log k_{p+1} \rfloor})^2 \dots)^2)^2)^2, \end{aligned}$$

где одночлены v_i имеют вид

$$v_i = x_{p+1}^{b_{i,p+1}} x_{p+2}^{b_{i,p+2}} \dots x_q^{b_{iq}}, \quad b_{ij} \in \{0, 1\}, \quad j = p+1, \dots, q, \quad i = 1, \dots, p\lfloor \log k_{p+1} \rfloor.$$

Натуральное число i , удовлетворяющее неравенствам $1 \leq i \leq p\lfloor \log k_{p+1} \rfloor$, можно единственным образом представить в виде

$$i = \alpha(i) + \beta(i)p\lfloor \log k_{p+1} \rfloor,$$

где $0 \leq \alpha(i) < \lfloor \log k_{p+1} \rfloor$, $0 \leq \beta(i) \leq p$.

В матрице $B = (b_{ij})$ размера $p\lfloor \log k_{p+1} \rfloor \times (q - p)$ (см. рис. 1) элемент b_{ij} , $1 \leq i \leq p\lfloor \log k_{p+1} \rfloor$, $p+1 \leq j \leq q$, будем называть информационным, если выполняется условие $\alpha(i) \leq \lfloor \log k_j \rfloor$. В силу неравенств

$$r_{ij} \leq k_j - 1, \quad i = 1, \dots, p, \quad j = 1, \dots, q,$$

Рис. 1.

любой элемент матрицы B , не являющийся информационным, равен 0. Особо отметим, что если $b_{ij} = 0$, то нулевыми будут также элементы b_{sj} , удовлетворяющие условиям $\beta(s) = \beta(i)$ и $\alpha(s) > \alpha(i)$, а также, в силу неравенств $k_1 \geq k_2 \geq \dots \geq k_q$, и элементы b_{it} , удовлетворяющие условию $t > j$. Число информационных элементов в матрице B не превосходит величины $p(\log K'' + q - p)$. Тогда, применяя теорему 3 и идею доказательства леммы 1 из [9], получаем, что системе одночленов $v_1, v_2, \dots, v_{p\lceil \log k_{p+1} \rceil}$ можно вычислить с использованием не более

$$\frac{p(\log K'' + q - p)}{\log(p \log K'')} (1 + o(1)) + O(q - p) + O(p\lceil \log k_{p+1} \rceil)$$

элементов умножения.

Таким образом, учитывая, что для реализации системы одночленов $y_1, y_2, \dots, y_p$, исходя из $v_1, v_2, \dots, v_{p \lceil \log k_{p+1} \rceil}$, требуется не более $2p(\lceil \log k_{p+1} \rceil + 1)$ операций умножения, в случае $p < q$ находим, что

$$L(\mathcal{X}, p) \leq \frac{p \log K'}{\log(p \log K')} (1 + o(1)) + O\left(\sum_{i=1}^p \log k_i\right) + \frac{p(\log K'' + q - p)}{\log(p \log K'')} (1 + o(1)) + O(q) + O(p \lceil \log k_{p+1} \rceil).$$

Оценим сверху величину

$$\frac{p \log K'}{\log(p \log K')} (1 + o(1)) + \frac{p(\log K'' + q - p)}{\log(p \log K'')} (1 + o(1)).$$

Если выполняется неравенство $\log K' \leq (\log K) / \log \log K$, то

$$\frac{p \log K'}{\log(p \log K')} (1 + o(1)) = o\left(\frac{p \log K}{\log(p \log K)}\right),$$

если же выполняется неравенство $\log K' > (\log K) / \log \log K$, то

$$\frac{p \log K'}{\log(p \log K')} (1 + o(1)) \leq \frac{p \log K'}{\log(p \log K)} (1 + o(1)).$$

Если выполняется неравенство $\log K'' \leq (\log K) / \log \log K$, то учитывая неравенство $q - p \leq \log K''$, получаем, что

$$\frac{p(\log K'' + q - p)}{\log(p \log K'')} (1 + o(1)) = o\left(\frac{p \log K}{\log(p \log K)}\right),$$

если же выполняется неравенство $\log K'' > (\log K) / \log \log K$, то

$$\frac{p(\log K'' + q - p)}{\log(p \log K'')} (1 + o(1)) \leq \frac{p \log K''}{\log(p \log K)} (1 + o(1)) + \frac{pq}{\log(p \log K)}.$$

Таким образом,

$$\begin{aligned} \frac{p \log K'}{\log(p \log K')} (1 + o(1)) + \frac{p(\log K'' + q - p)}{\log(p \log K'')} (1 + o(1)) \\ \leq \frac{p(\log K' + \log K'')}{\log(p \log K)} (1 + o(1)) + \frac{pq}{\log(p \log K)}. \end{aligned}$$

Теперь, используя еще неравенство

$$p \lceil \log k_{p+1} \rceil \leq \sum_{i=1}^p \log k_i + p,$$

окончательно в случае $p < q$ получаем оценку

$$L(\mathcal{X}, p) \leq \frac{p(\log K)}{\log(p \log K)} (1 + o(1)) + \frac{pq}{\log(p \log K)} + O\left(\sum_{i=1}^{\min(p, q)} \log k_i\right) + O(q).$$

Отсюда и из оценки в случае $p \geq q$ в силу очевидного неравенства $q \leq \log K$ следует требуемая верхняя оценка величины $L(\mathcal{K}, p)$, причем если выполняются условия

$$\sum_{i=1}^{\min(p,q)} \log k_i + p + q = o\left(\frac{p \log K}{\log(p \log K)}\right), \quad q = o(\log K),$$

то справедливо соотношение

$$L(\mathcal{K}, p) \leq \frac{p \log K}{\log(p \log K)} (1 + o(1)).$$

Верхняя оценка доказана.

Найдем теперь оценку снизу. Очевидно, что

$$L(\mathcal{K}, p) \geq q - 1.$$

В силу неравенства $p \leq K$ справедливо также соотношение

$$L(\mathcal{K}, p) \geq p - q.$$

Сразу отметим, что для функционала $L^*(\mathcal{K}, p)$ справедливы аналогичные неравенства

$$L^*(\mathcal{K}, p) \geq p - 1, \quad L^*(\mathcal{K}, p) \geq q - p,$$

вследствие которых отличие значений $L(\mathcal{K}, p)$ и $L^*(\mathcal{K}, p)$ на величину $q - p$ несущественно для доказательства нижней оценки теоремы.

Далее, так как для вычисления системы одночленов

$$x_1^{2^{\lfloor \log k_1 \rfloor}}, x_2^{2^{\lfloor \log k_2 \rfloor}}, \dots, x_{\min(p,q)}^{2^{\lfloor \log k_{\min(p,q)} \rfloor}}$$

требуется не менее

$$\lfloor \log k_1 \rfloor + \lfloor \log k_2 \rfloor + \dots + \lfloor \log k_{\min(p,q)} \rfloor - \min(p, q)$$

элементов умножения, следовательно,

$$L(\mathcal{K}, p) \geq \sum_{i=1}^{\min(p,q)} \log k_i - 2 \min(p, q).$$

Кроме того, из стандартных мощностных рассуждений (см., например, теорему Д2 из [10]), нетрудно получить оценку

$$L(\mathcal{K}, p) \geq \frac{p(\log K)}{\log(p \log K)} (1 + o(1)) + O(p + q).$$

Объединяя все нижние оценки в одну, получаем, что

$$\log(p \log K) + \sum_{i=1}^{\min(p,q)} \log k_i + p + q = O(L(\mathcal{K}, p)),$$

причем, если выполнено условие

$$\sum_{i=1}^{\min(p,q)} \log k_i + p + q = o\left(\frac{p \log K}{\log(p \log K)}\right),$$

то справедливо неравенство

$$\frac{p \log K}{\log(p \log K)} \leq L(\mathcal{K}, p)(1 + o(1)).$$

Теорема доказана.

Список литературы

1. Сидоренко А. Ф. Сложность аддитивных вычислений семейств целочисленных линейных форм. *Записки научных семинаров ЛОМИ* (1981) **105**, 53–61.
2. Brauer A. On addition chains. *Bull. Amer. Math. Soc.* (1939) **45**, 736–739.
3. Erdos P. Remarks on number theory, III: On addition chains. *Acta Arith.* (1960) **6**, 77–81.
4. Кнут Д. Е. *Искусство программирования для ЭВМ*, т. 2, Мир, Москва, 1977.
5. Bellman R. E. Addition chains of vectors. *Amer. Math. Monthly* (1963) **70**, 765.
6. Гашков С. Б., Кочергин В. В. Об аддитивных цепочках векторов, вентильных схемах и сложности вычисления степеней. *Методы дискретного анализа в теории графов и сложности* (1992) **52**, 22–40.
7. Кочергин В. В. О сложности вычислений одночленов и наборов степеней. *Дискретный анализ*. (1994) **27**, 94–107.
8. Pippenger N. On the evaluation of powers and monomials. *SIAM J. Comput.* (1980) **9**, №2, 230–250.
9. Кочергин В. В. О сложности вычислений в конечных абелевых группах. *Математические вопросы кибернетики* (1992) **4**, 178–217.
10. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования. *Проблемы кибернетики* (1965) **14**, 31–110.

Статья поступила 04.02.1998.