О сложности монотонных вычислений действительных многочленов

С. Б. Гашков, И. С. Сергеев

sbgashkov@gmail.com, isserg@gmail.com

МГУ им. М. В. Ломоносова, Москва

[1]

Рассматриваются многочлены из полукольца $\mathbb{R}_+[x_1, \ldots, x_n]$ и вычисление их схемами, состоящими из элементов сложения, умножения и положительных действительных констант. Для любого такого многочлена $f(x_1, \ldots, x_n)$ обозначим через $L_+(f)$ наименьшее число сложений (аддитивная монотонная сложность многочлена f), а через $L_\times(f)$ — наименьшее число нескалярных умножений (мультипликативная монотонная сложность), необходимое для его вычисления. Изучается задача эффективного построения многочленов, имеющих высокую монотонную сложность.

Обозначим через $P(N^n)$ полукольцо конечных подмножеств множества N^n (где $N = \mathbb{N} \cup \{0\}$) относительно операции дизъюнкции $\vee$ и умножения $\times$: если $A, B \in P(N^n)$, то $A, B \subset N^n$, $A \vee B = A \cup B$, $A \times B = \{a + b \mid a \in A,\ b \in B\}$.

Через mon обозначим гомоморфизм полукольца $\mathbb{R}_+[x_1, \ldots, x_n]$ в полукольцо $P(N^n)$, определяемый условием: $a = (a_1, \ldots, a_n) \in \operatorname{mon} f$ тогда и только тогда, когда многочлен f содержит моном $c_a x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$.

Пусть $k \leqslant l$. Подмножество H коммутативной полугруппы $(G, +)$ назовем (k, l)-*редким*, если оно не содержит подмножеств вида $A + B = \{a + b \mid a \in A,\ b \in B\}$, где $|A| = k$ и $|B| = l$ (здесь и далее мощность конечного множества M обозначается через $|M|$).

Обозначим через $\alpha(k)$ наибольшее количество различных булевых $(k-1)$-мерных векторов, ни один из которых не равен дизъюнкции двух других. Известно, что $\alpha(2) = 2$, $\alpha(3) = 3$, $\alpha(4) = 5$, $\alpha(k) \sim C_{k-1}^{\lfloor \frac{k-1}{2} \rfloor}$.

Метод [1] основан на наблюдении: если для многочлена f множество $\operatorname{mon} f$ является (k, l)-редким в $(P(N^n), \vee)$ (при не очень больших k и l), то f имеет высокую монотонную сложность. Эта связь между редкостью и сложностью описывается следующей теоремой, доказанной в [1] в случае $k = l$.

Теорема 1. *Пусть $k > 1$ и $\operatorname{mon} f$ — (k, l)-редкое подмножество множества $(N^n, +)$. Положим $h = \max\{(k-1)^3, (l-1)^2\}$ и $H = h^{-1}|\operatorname{mon} f|$. Тогда справедливы неравенства:*

(i) $L_+(f) \geqslant H - 1$;

(ii) $L_\times(f) \geqslant 2\sqrt{H} - n - 2$;

[1] Материалы XVI Международной конференции «Проблемы теоретической кибернетики» (Нижний Новгород, 20-25 июня 2011 г.). Н.Н.: Изд-во Нижегородского госуниверситета, 2011, 114-117.

(iii) Если $H > (2\alpha(k)-3)^{2\alpha(k)-1}(\alpha(l)-\alpha(k)+1)^{\frac{2}{\alpha(k)}-2}$, *то*

$$L_\times(f) \geqslant$$
$$2C\left(H - C^{2-\frac{2}{\alpha(k)}}(\alpha(k)-1)H^{\frac{2\alpha(k)-2}{2\alpha(k)-1}} - C(\alpha(k)-2)H^{\frac{\alpha(k)}{2\alpha(k)-1}}\right)^{\frac{\alpha(k)}{2\alpha(k)-1}} - n - 2,$$

где $C = (\alpha(l)-\alpha(k)+1)^{\frac{-1}{2\alpha(k)-1}}$.

Заметим, что оценки теоремы 1 существенно улучшить, вообще говоря, нельзя. Действительно, для любого многочлена f справедливо $L_+(f) \leqslant |\operatorname{mon} f| - 1$, поэтому при небольших k и l оценка (i) является точной по порядку, а в случае $k = l = 2$ — просто точной. Оценки (ii) и (iii) также близки к наилучшим возможным, что вытекает из следующей теоремы из работы [1].

Теорема 2. *Пусть* $E_m = \{0, 1, \ldots, m-1\}$. *Для любого* n *при* $k = 2$ *и любого* $n > 1$ *при* $k > 2$ *существует* (k,k)*-редкое множество* $\operatorname{mon} f \subset E_m^n$ *такое, что* $|\operatorname{mon} f| \geqslant m^{c_k n^{\log_2 3-1}}$ *и*

$$L_\times(\operatorname{mon} f) \lesssim \begin{cases} \Theta\left(|\operatorname{mon} f|^{\frac{k+1}{2k}}\right), & k > 3 \\ 3|\operatorname{mon} f|^{3/5}, & k = 3 \\ 3|\operatorname{mon} f|^{2/3}, & k = 2 \end{cases}.$$

Используя теорему 1 и конструкцию редкого множества из работы [2], можно установить следующий результат:

Теорема 3.

(i) Пусть p *— простое число. Тогда можно эффективно указать монотонный многочлен* f *от* n *переменных степени не выше* $p-1$ *по каждой из переменных, такой, что при* $n \to \infty$*:*

$$L_+(f) = \Omega\left(p^{n-o(n)}\right), \qquad L_\times(f) = \Omega\left(p^{0{,}5n-o(n)}\right).$$

(ii) При любом $\varepsilon > 0$ *существует* m_ε*, такое, что для любого* $m > m_\varepsilon$ *можно эффективно указать монотонный многочлен* f *от* n *переменных степени не выше* $m-1$ *по каждой из переменных, такой, что при* $n \to \infty$*:*

$$L_+(f) = \Omega_\varepsilon\left(m^{n(1-\varepsilon)}\right), \qquad L_\times(f) = \Omega_\varepsilon\left(m^{0{,}5n(1-\varepsilon)}\right).$$

Известно, что если степень многочлена f по каждой из переменных не превосходит $m-1$, то $L_+(f) < m^n$ и $L_\times(f) \leqslant \Theta\left(m^{n/2}\right)$ при $n \to \infty$. Таким образом, оценки теоремы 2 в том виде, в котором они приведены, являются неулучшаемыми.

В важном частном случае $p = 2$ теорема 3 дает пример мультилинейного (линейного по каждой переменной) многочлена n переменных с коэффициентами 0 и 1, имеющего аддитивную монотонную сложность $2^{(1-o(1))n}$ и мультипликативную монотонную сложность $2^{(0{,}5-o(1))n}$.

Ранее мультилинейный многочлен с коэффициентами 0 и 1, и имеющий монотонную аддитивную сложность $2^{\lceil n/2\rceil}-1$, был построен О. М. Касим-Заде [3]

(первая эффективная экспоненциальная нижняя оценка). В работе [1] был построен мультилинейный многочлен с коэффициентами 0 и 1 с аддитивной монотонной сложностью, по порядку не меньшей $2^{2n/3}$, и с мультипликативной монотонной сложностью по порядку не меньшей 2^{cn}, где $c > 1/3$.

Несколько модифицировав конструкцию из теоремы 3, можно получить пример многочлена с высоким отношением монотонной сложности и сложности вычисления в полном арифметическом базисе, включающем дополнительно отрицательные действительные константы.

Теорема 4. *Можно эффективно указать мультилинейный многочлен n переменных, для которого отношение сложности реализации в монотонном базисе $\{x+y,\, xy\} \cup \mathbb{R}_+$ к сложности реализации в полном базисе $\{x+y,\, xy\} \cup \mathbb{R}$ не меньше, чем $2^{(0{,}5-o(1))n}$.*

Ранее Вэльянт [4] для подобного отношения получил оценку $2^{\Omega(\sqrt{n})}$ (используя всего один элемент умножения на отрицательную константу).

Работа выполнена при поддержке РФФИ, проекты № 08-01-00863, 08-01-00632, и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Литература

[1] *Гашков С. Б.* Об одном методе получения нижних оценок сложности монотонных вычислений многочленов // Вестник МГУ. Математика. Механика. — 1987. — № 5. — С. 7–13.

[2] *Kóllar J., Rónyai L., Szabó T.* Norm-graphs and bipartite Turán numbers // Combinatorica. — 1996. — V. 16, № 3. — P. 399–406.

[3] *Касим-Заде О. М.* Об арифметической сложности монотонных многочленов // Тезисы Всесоюзной конференции 1983 г. «Теоретические проблемы кибернетики». Ч. 1. — Саратов: Изд-во Саратовского ун-та, 1986. — С. 68–69.

[4] *Valiant L. G.* Negation can be exponenially powerful // Th. Comput. Sci. — 1980. — V. 12. — P. 303–314.