СЛОЖНОСТЬ ВЫЧИСЛЕНИЯ МНОГОЧЛЕНОВ

С. Б. ГАШКОВ, И. С. СЕРГЕЕВ
МГУ им. М.В. Ломоносова

I. КЛАССИЧЕСКИЕ РЕЗУЛЬТАТЫ

i.1 Вычисление вещественных многочленов в полном арифметическом базисе $A = \{+,\times,\boldsymbol{R}\}$

Для вычисления многочлена степени n достаточно:

n аддитивных операций

$n/2+O(1)$ умножений

$\Omega(n^{1/2})$ нескалярных операций

Эти оценки неулучшаемы (Motzkin, Пан, Белага 1950-е гг. Paterson, Stockmeyer 1973)

I. КЛАССИЧЕСКИЕ РЕЗУЛЬТАТЫ

i.2 Способ вычисления многочлена за $n/2+O(\log n)$ умножений (метод Винограда)

Идея: пусть $f(x)$ – нормированный многочлен степени $2^{k+1}-1$

Тогда $$f(x) = (x^{2^k} + a)\, f_0(x) + f_1(x), \qquad (1)$$

где $f_0(x), f_1(x)$ – нормированные многочлены степени $2^k - 1$

Разложение (1) применим к $f_0(x), f_1(x)$ и т.д.

Проверить: (а) необходимые степени $x^{2^k}, x^{2^{k-1}}, \ldots, x^2$ вычисляются за k умножений (аддитивной цепочкой);

(б) если они вычислены, то любой промежуточный многочлен степени $2^m - 1$ вычисляется за $2^{m-1} - 1$ умножений (очевидно из (1))

I. КЛАССИЧЕСКИЕ РЕЗУЛЬТАТЫ

i.3 Способ вычисления многочлена за $2n^{1/2}$ нескалярных умножений

Идея: многочлен $f(x)$ степени $rs - 1$ представляется в виде

$$f(x) = (\dots((f_0(x)\, x^r + f_1(x))\, x^r + \dots)\, x^r + f_{s-1}(x), \qquad (2)$$

(схема Горнера) где $f_k(x)$ – многочлены степени $r - 1$

(а) степени $x^2, x^3, \dots, x^r$ вычисляются за $r - 1$ нескалярных умножений; многочлены $f_k(x)$ получаются как линейные комбинации этих степеней;

(б) для завершения вычислений по формуле (2) достаточно выполнить еще $s - 1$ умножений на x^r

I. КЛАССИЧЕСКИЕ РЕЗУЛЬТАТЫ

i.4 Эффективные нижние оценки

В 70-90-х гг. Straßen и его ученики (von zur Gathen, Heintz, Schnorr, Stoß, Baur, Halupczok, а также Sieveking, van de Wiele) построили примеры конкретных многочленов, имеющих сложность, близкую к максимально возможной. Коэффициенты таких многочленов, как правило, алгебраически независимые вещественные или быстро растущие рациональные числа. Примеры сложных многочленов:

$$\sum p_i^{1/2} x^i \qquad \sum 2^{2^i} x^i \qquad \sum i^r x^i$$

Здесь: $p_i \in \boldsymbol{P}$, $r \in \boldsymbol{Q} / \boldsymbol{Z}$

I. КЛАССИЧЕСКИЕ РЕЗУЛЬТАТЫ

i.5 *Подстановка Кронекера*

$$x_i = x^{2^i}$$

устанавливает взаимно однозначное соответствие между многочленами одной переменной степени 2^n-1 и *мультилинейными* (линейными по каждой переменной) многочленами n переменных

Поэтому если $f(x)$ соответствует $g(x_0, \dots, x_{n-1})$, то

$$L(f) \le L(g) + n - 1$$

II. МОНОТОННАЯ СЛОЖНОСТЬ

ii.1 Рассматриваются монотонные многочлены, т.е. с неотрицательными вещественными коэффициентами, и сложность их реализации над монотонным арифметическим базисом $A_+ = \{+,\times,\boldsymbol{R}_+\}$. Содержательной является задача построения сложных многочленов с коэффициентами 0 и 1

ii.2 Субкспоненциальные нижние оценки

Первая сверхполиномиальная нижняя оценка получена для характеристического многочлена наличия k-клики в графе:

$$CL_{n,k} = \sum_{1 \le i_1 < \ldots < i_k \le n} \prod_{1 \le s < t \le k} x_{i_s, i_t}$$

$L_+(CL_{n,k}) \ge C_n^k - 1$, в частности, $L_+(CL_{n,n/2}) \ge 2^{n/2-o(n)}$

Schnorr 1976

II. МОНОТОННАЯ СЛОЖНОСТЬ

Помимо Шнорра нижние оценки вида $2^{\Omega(n)}$ для мультилинейных многочленов n переменных в начале 80-х гг. получали Valiant, Jerrum, Snir

ii.3 Экспоненциальные нижние оценки

$2^{n/2} - 1$	Касим-Заде 1983
$\Omega(2^{2n/3})$	Гашков 1987
$2^{n-o(n)}$	Гашков, Сергеев 2010

(далее подробно)

III. МЕТОД РЕДКИХ МНОЖЕСТВ

iii.1 *ОПР*. Подмножество M коммутативной полугруппы $(G, +)$ называется (k, l)-редким, где $k \le l$, если для любых подмножеств $A, B \subset G$, таких, что $|A|=k$ и $|B|=l$ выполнено

$$A \times B = \{ a+b \mid a \in A, b \in B \} \not\subset M$$

При $k=l$ используем термин k-редкое подмножество.

Пример: Подмножество $\{0, 1, 3\} \subset (\boldsymbol{Z}_7, +)$ является 2-редким

ОПР. Пусть f – многочлен n переменных. Тогда

$\mathrm{mon}\, f \subset (\boldsymbol{N} \cup \{0\})^n$ – множество вектор-степеней его мономов.

III. МЕТОД РЕДКИХ МНОЖЕСТВ

iii.2 ОСНОВНАЯ ТЕОРЕМА

Пусть $k \geq 1$ и $\mathrm{mon}\, f$ – (k, l)-редкое подмножество $(\boldsymbol{N} \cup \{0\})^n$,

$L_+(f)$ – аддитивная монотонная сложность многочлена f,

$L_\times(f)$ – мультипликативная монотонная сложность f,

$\alpha(k)$ – наибольшее число булевых векторов длины $k - 1$, ни один из которых не равен дизъюнкции нескольких других.

Пусть $h = \min \{ (k-1)^3, (l-1)^2 \}$.

Тогда: (i) $L_+(f) \geq h^{-1} \,|\, \mathrm{mon}\, f \,| - 1$

(ii) $L_\times(f) \geq C_{k,l} \,|\, \mathrm{mon}\, f \,|^{\alpha(k)/(2\alpha(k)-1)} - n - 2$

В частности, $L_\times(f) = \Omega(|\, \mathrm{mon}\, f \,|^{2/3})$ при $k=l=2$

и $L_\times(f) = \Omega(|\, \mathrm{mon}\, f \,|^{3/5})$ при $k=l=3$.

Эти оценки по порядку неулучшаемы Гашков 1987

III. МЕТОД РЕДКИХ МНОЖЕСТВ

iii.3 Примеры 2- и 3-редких множеств большой мощности

1. 2-редкие подмножества $\boldsymbol{Z}_n$ мощности $\sim n^{1/2}$:

Множество В.Е. Алексеева 1979:

Пусть $n=p(p-1)$, $p \in \boldsymbol{P}$, ζ – порождающий элемент мультипликативной группы поля $\boldsymbol{Z}_p$. Тогда

$$M = \{ s_i \mid i = 0, \dots, p-2 \}, \text{ где } \quad s_i \equiv i \bmod (p-1), \quad s_i \equiv \zeta^i \bmod p$$

Множество Зингера 1938:

Пусть $n=q^2+q+1$, q – степень простого числа, θ – примитивный элемент поля $GF(q^3)$. Пусть $GF(q) = \{ \zeta_1, \dots, \zeta_q \}$. Тогда

$$M = \{0\} \cup \{ s_i \mid \theta^{s_i} / (\theta + \zeta_i) \in GF(q), \ i=1, \dots, q \}$$

III. МЕТОД РЕДКИХ МНОЖЕСТВ

ОПР. $E_m = \{ 0, \ldots, m\text{-}1 \}$.

2. 2-редкие подмножества $E_m^{\,n}$ мощности $\sim m^{n/2}$:

Пусть $q = p^k$, $p \in \boldsymbol{P} \setminus \{2\}$. Тогда

$$M = \{ (x, x^2) \mid x \in GF(q) \} \subset GF(q^2) \to E_p^{\,2k}$$

Пусть $q = 2^k$. Тогда

$$M = \{ (x, x^3) \mid x \in GF(q) \} \subset GF(q^2) \to E_2^{\,2k}$$

3. 3-редкие подмножества $E_m^{\,n}$ мощности $\sim m^{2n/3}$:

Множество Брауна 1966:

Пусть $q = p^k$, $p \in \boldsymbol{P} \setminus \{2\}$ и γ – квадратичный невычет в $GF(q)$. Тогда

$$M = \{ (x, y, z) \mid x^2 + y^2 + z^2 = -\gamma,\ x, y, z \in GF(q) \} \subset GF(q^3) \to E_p^{\,3k}$$

III. МЕТОД РЕДКИХ МНОЖЕСТВ

iii.4 Следствия для сложности многочленов

Можно эффективно указать многочлен f от n переменных степени не выше $m - 1$ по каждой переменной, такой, что (при определенных ограничениях на m и n)

$$L_+(f) \geq (1 - o(1))m^{n/2} \qquad L_\times(f) \geq (2 - o(1))m^{n/3}$$

(если в качестве $\mathrm{mon}\, f$ выбирается подходящее 2-редкое множество) или

$$L_+(f) \geq (1/8 - o(1))m^{2n/3} \qquad L_\times(f) \geq (2^{-4/5} - o(1))m^{2n/5}$$

(если в качестве $\mathrm{mon}\, f$ выбирается подходящее 3-редкое множество)

(в примерах Шнорра и Касим-Заде: 2-редкие множества)

III. МЕТОД РЕДКИХ МНОЖЕСТВ

Факт (Erdös, Spencer 1974): любое (k, l)-редкое подмножество $M \subset {E_m}^n$ имеет мощность $O_{k,l}(m^{n(1-1/k)})$

iii.5 Редкие множества экстремальной мощности

Множество Коллара-Роньяи-Жабо 1996:

В группе $(GF(q^t), +)$ множество элементов единичной нормы

$$M = \{ x \mid x^{(q^t-1)/(q-1)} = 1,\ x \in GF(q^t) \}$$

является $(t, t!+1)$-редким подмножеством и имеет мощность $(q^t - 1)/(q - 1)$.

III. МЕТОД РЕДКИХ МНОЖЕСТВ

iii.6 ЛЕММА 1

Пусть $\psi_{s,t,m}: {E_m}^{st} \to {E}^{s}_{(2m-1)^t}$ –

взаимно однозначное отображение:

$$\psi_{s,t,m}(\dots, a_{it}, \dots, a_{it+t-1}, \dots) = (\dots, [a_{it}, \dots, a_{it+t-1}]_{2m-1}, \dots) \quad *$$

Тогда если $M \subset {E_m}^{st}$ является (k, l)-редким подмножеством, то $\psi_{s,t,m}(M) \subset {E}^{s}_{(2m-1)^t}$ также является (k, l)-редким подмножеством.

* $[a_k, \dots, a_0]_m = (\dots(a_k\, m + a_{k-1})m + \dots)m + a_0$ (запись числа в системе счисления с основанием m)

III. МЕТОД РЕДКИХ МНОЖЕСТВ

iii.7 ОСНОВНОЕ СЛЕДСТВИЕ (из основной теоремы и технической теоремы 1)

Пусть $m \geq 2$ и $n \geq 1$. Можно эффективно указать многочлен f от n переменных степени не выше $m - 1$ по каждой переменной, такой, что при $m^n \to \infty$

$$L_+(f) \geq m^{\,n\,(1 - o(1))} \qquad L_\times(f) \geq m^{\,n\,(1/2 - o(1))}$$

Обе оценки в таком виде уже неулучшаемы.

IV. МОНОТОННАЯ И НЕМОНОТОННАЯ СЛОЖНОСТЬ

iv.1 Примеры расхождения между сложностью $L(f)$ в полном базисе $A = \{+,\times,\boldsymbol{R}\}$ и сложностью $L_M(f)$ в монотонном базисе $A_+ = \{+,\times,\boldsymbol{R}_+\}$

f – мультилинейные многочлены n переменных:

$L(f) = n^{O(1)}$	$L_M(f) \geq c^{n^{1/2}}$	Valiant 1979
$L(f) = n^{O(1)}$	$L_M(f) \geq c^{n}$	Касим-Заде 1983
$L_M(f) \,/\, L(f) = n^{\Omega(1)}$	$\deg f = 3$	Schnorr 1976

$L_M(f) \,/\, L(f) \geq 2^{n(1/2-o(1))}$		Гашков, Сергеев 2010
$L_M(f) \,/\, L(f) = n^{1-o(1)}$	$\deg f = 2$	Гашков, Сергеев 2010

IV. МОНОТОННАЯ И НЕМОНОТОННАЯ СЛОЖНОСТЬ

iv.2 Еще один способ построения редких множеств

ОПР. Булева матрица называется (k, l)-редкой, если она не содержит подматриц размера $k \times l$, состоящих из всех единиц

ЛЕММА 2

Пусть $M_1 = \{ a_1, \ldots, a_r \}$ и $M_2 = \{ b_1, \ldots, b_r \}$ – k-редкие подмножества E_m^n и $(\mu_{i,j})$ – l-редкая матрица порядка r. Тогда

(i) $$M = \{ (a_i, b_j) \mid \mu_{i,j} = 1 \} \subset E_m^{2n}$$

(ii) $$M = \{ a_i + (2m - 1) b_j \mid \mu_{i,j} = 1 \} \subset E^n_{m2}$$

– $((k-1)(l-1)+1)$-редкие подмножества

Свойство: $L(f_M) \le L(f_{a_1}, \ldots, f_{a_r}, f_{b_1}, \ldots, f_{b_r}) + L(\mu_{i,j}) + O(\log m)$, где $M = \mathrm{mon}\, f_M$, $L(\mu_{i,j})$ – сложность линейного преобразования

IV. МОНОТОННАЯ И НЕМОНОТОННАЯ СЛОЖНОСТЬ

СЛЕДСТВИЕ (из леммы 1 и результата Kóllar, Rónyai, Szabó)

Можно явно указать $n^{o(1)}$-редкую циркулянтную матрицу порядка n и веса $n^{2-o(1)}$

СЛЕДСТВИЕ (из леммы 2)

Пусть f – многочлен с коэффициентами 0 и 1, такой, что $M = \mathrm{mon}\, f$. Пусть $(\mu_{i,j})$ – $r^{o(1)}$-редкая циркулянтная матрица и пусть $k = r^{o(1)}$ и либо $n \log m = r^{o(1)}$, либо $\deg f = r^{o(1)}$. Тогда

$$L_M(f) = \Omega(r^{2-o(1)}) \qquad L(f) \le r^{1+o(1)}$$

IV. МОНОТОННАЯ И НЕМОНОТОННАЯ СЛОЖНОСТЬ

iv.3 СЛЕДСТВИЕ (о расхождении между монотонной и немонотонной сложностью)

Пусть $m \geq 2$ и $n \geq 1$. Можно эффективно указать многочлен f от n переменных степени не выше $m - 1$ по каждой переменной, такой, что при $m^n \to \infty$

$$L_M(f) \,/\, L(f) \geq m^{\,n\,(1/2 \,-\, o(1))}$$

iv.4 Пример многочлена степени 2

Пусть $(\mu_{i,j})$ – $n^{o(1)}$-редкая циркулянтная матрица порядка n и веса $n^{2-o(1)}$. Определим

$$f = \sum_{1 \leq i < j \leq n} \mu_{i,j}\, x_i\, y_j$$

Тогда $L_M(f) \,/\, L(f) = n^{1-o(1)}$

СЛОЖНОСТЬ ВЫЧИСЛЕНИЯ МНОГОЧЛЕНОВ

С. Б. ГАШКОВ, И. С. СЕРГЕЕВ
МГУ им. М.В. Ломоносова