Некоторые многочлены, имеющие высокую сложность вычисления [1]

И. фон цур Гатен, Ф. Штрассен [2]

Используя результат Хайнца и Зивекинга [1], мы показываем, что многочлены $\sum_{1 \leqslant j \leqslant d} b^{1/j} X^j$, где b — положительное действительное число, отличное от единицы, и $\sum_{1 \leqslant j \leqslant d} j^r X^j$, где r — рациональное число, не являющееся целым, имеют высокую сложность вычисления.

Мы используем следующий вариант основного результата Хайнца и Зивекинга [1]. Пусть $f = \sum_{1 \leqslant j \leqslant d} b_j X^j \in \mathbb{C}[X]$ — многочлен, K_0 — подполе поля $\mathbb{C}$ комплексных чисел, такое, что все коэффициенты b_j многочлена f алгебраичны над K_0, и пусть N — число точек, сопряженных с точкой $(b_1, \ldots, b_d)$ над полем K_0 (т. е. число элементов орбиты точки $(b_1, \ldots, b_d)$ пространства $\mathbb{C}^d$ под действием группы Галуа поля $\mathbb{C}$ над K_0).

Пусть, далее, $g_1, \ldots, g_n \in K_0[T_1, \ldots, T_d]$ — многочлены степеней, не превосходящих M, такие, что множество их общих нулей $\{x \in \mathbb{C}^d \colon g_1(x) = \ldots = g_n(x) = 0\}$ конечно и содержит точку $(b_1, \ldots, b_d)$. Тогда

$$L(f) \geqslant (\log N/(24 \log (dM)))^{1/2}.$$

Здесь $L(f)$ — наименьшее число нескалярных умножений и делений, достаточное для вычисления многочлена f схемой над $\mathbb{C} \cup \{X\}$. (Таким образом, допускается произвольная обработка.)

Применение 1. *Пусть b — положительное действительное число, отличное от единицы. Тогда*

$$L\Big(\sum_{1 \leqslant j \leqslant d} b^{1/j} X^j\Big) \succcurlyeq (d/\log d)^{1/2}.$$

(Соотношение $u(d) \succcurlyeq v(d)$ означает, что существует положительная постоянная c, такая, что $u(d) \geqslant c \cdot v(d)$ при больших d.

---

[1]) von zur Gathen J., Strassen V. Some polynomials that are hard to compute. — Theoret. Computer Sci., 1980, v. 11, No. 3, p. 331—335.

[2]) Seminar für die angewandte Mathematik, Universität Zürich, Switzerland.

Корни из положительных действительных чисел считаются положительными действительными числами, если не оговорено противное.)

Доказательство. Пусть

$$K_0 = \mathbb{Q}(b, \exp(2\pi i/3, \ldots, \exp(2\pi i/d)) = \mathbb{Q}(b, \exp(2\pi i/l)),$$

где $l =$ н. о. к. $(1, \ldots, d)$, и пусть $g_j = T_j^j - b$ для $j = 1, \ldots, d$. Тогда $\deg g_j \leqslant d$, и мы положим $M = d$. Кроме того, поле $K = K_0(b^{1/2}, \ldots, b^{1/d})$ является расширением Галуа поля K_0, и орбиты точки $(b, b^{1/2}, \ldots, b^{1/d})$ под действием групп $\mathrm{Gal}(\mathbb{C}/K_0)$ и $\mathrm{Gal}(K/K_0)$ совпадают. Поскольку лишь единичный элемент группы $\mathrm{Gal}(K/K_0)$ оставляет точку $(b, \ldots, b^{1/d})$ на месте, число N элементов орбиты точки $(b, b^{1/2}, \ldots, b^{1/d})$ под действием группы $\mathrm{Gal}(K/K_0)$ совпадает с числом элементов группы $\mathrm{Gal}(K/K_0)$. Таким образом,

$$N = \# \mathrm{Gal}(K/K_0) = [K : K_0],$$

и поэтому

$$L\Big(\sum_{1 \leqslant j \leqslant d} b^{1/j} X^j\Big) \geqslant (\log [K : K_0]/\log d)^{1/2}.$$

Запишем $[K : K_0] = [K : \mathbb{Q}(b)] / [K_0 : \mathbb{Q}(b)]$. Если b трансцендентно, то $[K_0 : \mathbb{Q}(b)] = [\mathbb{Q}(\exp(2\pi i/l)) : \mathbb{Q}] = \varphi(l)$. Если b алгебраично, то $[K_0 : \mathbb{Q}(b)]$ делит

$$[K_0 : \mathbb{Q}] = \varphi(l) \cdot [K_0 : \mathbb{Q}(\exp(2\pi i/l))].$$

Поскольку все простые делители числа $\varphi(l)$ меньше $d/2$, а $[K_0 : \mathbb{Q}(\exp(2\pi i/l))]$ не превосходит величины $[\mathbb{Q}(b) : \mathbb{Q}]$, не зависящей от d, то в обоих случаях число $[K_0 : \mathbb{Q}(b)]$ не делится ни на одно простое число p из интервала $d/2 \leqslant p \leqslant d$ при условии, что d достаточно велико.

С другой стороны, мы утверждаем, что для достаточно больших d число $[K : \mathbb{Q}(b)]$ делится на каждое простое число p из интервала $d/2 \leqslant p \leqslant d$. Из этого вспомогательного утверждения с использованием теоремы о распределении простых чисел вытекает, что

$$\log [K : K_0] \geqslant \log \Big(\prod_{d/2 \leqslant p \leqslant d} p\Big) \geqslant d.$$

откуда в свою очередь вытекает справедливость применения 1.

Для доказательства указанного вспомогательного утверждения достаточно показать, что

$$[\mathbb{Q}(b^{1/p}) : \mathbb{Q}(b)] = p$$

для достаточно больших простых p.

Пусть p — простое; допустим, что $[\mathbb{Q}(b^{1/p}) : \mathbb{Q}(b)] < p$. Тогда многочлен $T^p - b$ имеет нетривиальный делитель $h \in \mathbb{Q}(b)[T]$.

Поскольку над полем $\mathbb{C}$ $T^p - b = (T - \zeta^0 a) \ldots (T - \zeta^{p-1} a)$, где $a = b^{1/p} \in \mathbb{R}$ и $\zeta = \exp(2\pi i/p)$, свободный член многочлена h имеет вид $\zeta^t a^m$, причем $1 \leqslant m < p$. Таким образом, $\zeta^t a^m \in \mathbb{Q}(b)$. Взяв u и v такими, что $um + vp = 1$, получаем $\zeta^{tu} a \in \mathbb{Q}(b)$. Отсюда, поскольку a и b — действительные числа, $a \in \mathbb{Q}(b)$. Если b трансцендентно, такого быть не может. Если b алгебраично, рассмотрим разложение $(b) = q_1^{e_1} \ldots q_r^{e_r}$ дробного идеала (b), где q_i — простые идеалы кольца $\mathcal{O}$ целых элементов поля $\mathbb{Q}(b)$, а $e_i \in \mathbb{Z} \setminus \{0\}$. Соответствующее разложение идеала (a) показывает, что число p делит каждое e_i. Если p велико, этого быть не может, разве что $r = 0$. В последнем случае a и b — единицы (обратимые элементы) кольца $\mathcal{O}$. В силу теоремы Дирихле о единицах существует однозначное представление $b = u \cdot v_1^{f_1} \ldots v_s^{f_s}$, где u — корень из единицы в поле $\mathbb{Q}(b)$, $\{v_1, \ldots, v_s\}$ — множество основных единиц поля $\mathbb{Q}(b)$ и $f_1, \ldots, f_s \in \mathbb{Z}$. Соответствующее представление a показывает, что число p делит каждое f_i. Если p велико, этого быть не может, разве что все f_i — нули. Но тогда $b = 1$, а это исключено. Тем самым требуемое утверждение доказано.

Замечание. Мы сформулировали применение 1 для случая положительных корней из положительного действительного b. На самом деле данное доказательство проходит для любого ненулевого комплексного b, не являющегося корнем из единицы, и любых значений корней $b^{1/i}$. Если же b является корнем из единицы — скажем, для простоты, $b = \exp(2\pi i/t)$, — многочлен будет иметь высокую сложность (см. [1], следствие 1), если брать $b^{1/j} = \exp(2\pi i/tj)$. Однако для любого указанного b можно выбрать значения корней $b^{1/i}$ и таким образом, чтобы многочлен имел невысокую сложность.

А именно, свяжем с каждым натуральным числом j пару натуральных чисел f, g, определяемых следующим образом: f — наибольший общий делитель чисел j и t^l для больших l, а g таково, что $1 \leqslant g < t$ и $g \cdot (j/f) \equiv 1 \pmod t$; число j однозначно определяет значения f и g. Положим $b_j = \exp(2\pi i g/ft)$, тогда $b_j^j = \exp(2\pi i/t) = b$. Если t имеет s различных простых делителей, то для чисел f, g, связанных с числами $j \in \{1, \ldots, d\}$, имеется не более $(\log d)^s \cdot t$ возможностей. Разобьем сумму $\sum_{1 \leqslant j \leqslant d} b_j X^j$ на части в соответствии со значениями f, g. Каждая из частных сумм этого разбиения представляет собой сумму некоторой геометрической прогрессии и может быть вычислена со сложностью $O(\log d)$. Таким образом, $L\left(\sum_{1 \leqslant j \leqslant d} b_j X^j\right) = O((\log d)^{s+1})$.

Применение 2. *Пусть $r \in \mathbb{Q} \setminus \mathbb{Z}$. Тогда*

$$L\Big(\sum_{1 \leqslant j \leqslant d} j^r X^j\Big) \geqslant d^{1/2}/\log d.$$

Доказательство. Пусть $r = s/t$, причем числа $s \in \mathbb{Z}$ и $t \in \mathbb{N}$ взаимно просты, p — простой делитель числа t, $\zeta = \exp(2\pi i/p)$, $K_0 = \mathbb{Q}(\zeta)$ и $g_j = T_j^t - j^s$ для $j = 1, \ldots, d$. Пусть, далее, $q_1, \ldots, q_m$ — простые числа, не превосходящие d. Тогда число N точек, сопряженных с точкой $(1^r, 2^r, \ldots, d^r)$ над полем K_0, равно числу точек, сопряженных над K_0 с точкой $(g_1^r, \ldots, g_m^r)$, которое в свою очередь не меньше числа точек, сопряженных над K_0 с точкой $((q_1^s)^{1/p}, \ldots, (q_m^s)^{1/p})$. Последнее равно степени расширения $[K_0((q_1^s)^{1/p}, \ldots, (q_m^s)^{1/p}) : K_0]$, поскольку, как и в предыдущем доказательстве, указанное расширение есть расширение Галуа. Мы утверждаем, что для каждого $l < m$

$$(q_{l+1}^s)^{1/p} \notin K_0((q_1^s)^{1/p}, \ldots, (q_l^s)^{1/p}).$$

Тогда имеем $N \geqslant 2^m$, откуда с использованием теоремы о распределении простых чисел получаем

$$L\Big(\sum_{1 \leqslant j \leqslant d} j^r X^j\Big) \geqslant \big(m/(24 \log(dt))\big)^{1/2} \geqslant d^{1/2}/\log d.$$

Указанное вспомогательное утверждение вытекает из следующего общего факта.

Пусть $a_1, \ldots, a_l, a$ — положительные рациональные числа, причем

$$a^{1/p} \in K_0(a_1^{1/p}, \ldots, a_l^{1/p}).$$

Тогда существуют числа $w \in \mathbb{Q}$ и $e_1, \ldots, e_l \in \mathbb{N}$, такие, что

$$a = w^p a_1^{e_1} \ldots a_l^{e_l}.$$

Докажем это индукцией по l. Для $l = 0$ имеем

$$[\mathbb{Q}(a^{1/p}) : \mathbb{Q}] \leqslant [K_0 : \mathbb{Q}] = p - 1.$$

Отсюда, как в предыдущем доказательстве, вытекает, что $a^{1/p} \in \mathbb{Q}$, и мы принимаем $w = a^{1/p}$. Предположим по индукции, что

$$a^{1/p} \notin K = K_0(a_1^{1/p}, \ldots, a_{l-1}^{1/p}).$$

Положим $\theta = a_l^{1/p}$, $\eta = a^{1/p}$. Тогда поле $K(\theta)$ является расширением Галуа поля K и элементы $1, \theta, \ldots, \theta^z$ составляют K-базис поля $K(\theta)$ при некотором $z \leqslant p - 1$. (В действительности $z = p - 1$.) Пусть

$$\eta = b_0 + b_1\theta + \ldots + b_z\theta^z,$$

где $b_i \in K$, и пусть $\sigma \in \mathrm{Gal}(K(\theta)/K)$, причем $\sigma(\theta) \neq \theta$. Существуют натуральные u, v, такие, что $\sigma(\theta) = \zeta^u\theta$, причем $(u, p) = 1$, и $\sigma(\eta) = \zeta^v\eta$. Сравнивая коэффициенты в выражениях

$$\sigma(\eta) = b_0 + b_1\sigma(\theta) + \ldots + b_z\sigma(\theta)^z = \\ = b_0 + b_1\zeta^u\theta + \ldots + b_z\zeta^{uz}\theta^z$$

и

$$\sigma(\eta) = \zeta^v\eta = b_0\zeta^v + b_1\zeta^v\theta + \ldots + b_z\zeta^v\theta^z$$

и замечая, что все ζ^{ui} попарно различны, устанавливаем, что имеется в точности одно значение i, для которого $b_i \neq 0$. Стало быть,

$$(a/a_l^i)^{1/p} = \eta/\theta^i = b_i \in K.$$

Используя предположение индукции, заключаем, что

$$a/a_l^i = w^p a_1^{e_1} \ldots a_{l-1}^{e_{l-1}}.$$

Замечания. (1) Для любого $r \in \mathbb{N}$ имеем $L\left(\sum_{1 \leqslant j \leqslant d} j^r X^j\right) = O(\log d)$. Чтобы убедиться в этом, положим $f_r = \sum_{1 \leqslant j \leqslant d} j^r X^j$. Из соотношения $f_r = x \cdot (\mathrm{d}/\mathrm{d}x) f_{r-1}$ по индукции следует, что $f_r = (x^{d+1} \cdot g + h)/(x-1)^{r+1}$, где g и h — многочлены степеней не выше r. Отсюда $L(f_r) = O(\log d)$.

(2) Поскольку наибольшая сложность многочленов степени d (считая лишь нелинейные операции) имеет порядок роста $d^{1/2}$, нижние оценки данной статьи не могут быть значительно улучшены. Конечно, аналогичные результаты имеют место и в том случае, когда считаются все операции. Несколько более слабые оценки получаются также методом Штрассена [3] (с учетом улучшения, сделанного Шнорром [2]). Однако метод Хайнца — Зивекинга [1] гораздо элегантнее.

ЛИТЕРАТУРА

[1] Heintz J., Sieveking M. Lower bounds for polynomials with algebraic coefficients. — Theoret. Comput. Sci., 1980, v. 11, No. 3, p. 321—330. [Имеется перевод: настоящий сборник, с. 46—58.]

[2] Schnorr C. P. Improved lower bounds on the number of multiplications/divisions which are necessary to evaluate polynomials. — Theoret. Comput. Sci., 1978, v. 7, No. 3, p. 251—261. [Имеется перевод: настоящий сборник, с. 30—44.]

[3] Strassen V. Polynomials with rational coefficients which are hard to compute. — SIAM J. Comput., 1974, v. 3, No. 2, p. 128—149.