Записки научных
семинаров ПОМИ
Том 277, 2001 г.

Д. Ю. Григорьев

ДВАЖДЫ ЭКСПОНЕНЦИАЛЬНЫЙ РОСТ КОЛИЧЕСТВА ВЕКТОРОВ КРАТНОСТЕЙ РЕШЕНИЙ СИСТЕМ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ

Мы рассматриваем системы полиномиальных уравнений вида $g_1 = \ldots = g_n = 0$, где $g_i \in F[X_1, \ldots, X_n]$, $\deg g_i \leqslant d$, $1 \leqslant i \leqslant n$, и поле F алгебраически замкнуто. Для всякой 0-мерной (неприводимой) компоненты $a = (a_1, \ldots, a_n) \in F^n$ многообразия решений $V = \{g_1 = \ldots = g_n = 0\} \subset F^n$ ее (конечная) кратность [2] определяется как $m_a = \dim_F((F[X_1, \ldots, X_n]/(g_1, \ldots, g_n))_{(X_1-a_1, \ldots, X_n-a_n)})$. Системе $g_1, \ldots, g_n$ припишем (упорядоченный) вектор $\{m_a\}_a$, где a пробегает все 0-мерные компоненты многообразия V. Можно также рассматривать $\{m_a\}_a$ как разбиение числа $\sum_a m_a \leqslant d^n$ (последнее неравенство вытекает из неравенства Безу [2]). Обозначим через $M_{n,d}$ количество всевозможных векторов $\{m_a\}_a$.

В [4] было показано, что для полей F нулевой характеристики в случае, когда $\dim V = 0$, выполнена оценка

$$M_{n,d} \leqslant d^{O\left(\binom{n+d}{n}\right)}. \tag{1}$$

В [4] можно также найти мотивировку оценки $M_{n,d}$ из теории сложности вычислений. Упомянем также, что эту верхнюю оценку можно установить и без ограничения $\dim = 0$, используя технику "шевеления" систем полиномиальных уравнений, развитую в [3]. Заметим, что показатель $\binom{n+d}{n}$ в оценке равен числу коэффициентов многочленов степени не превосходящей d, иными словами, числу параметров рассматриваемых систем. Можно сравнить верхнюю оценку из [4] с очевидной верхней оценкой $M_{n,d} \leqslant \exp(O(d^n))$ количества разбиений числа Безу d^n (см. выше). При d меньшем n оценка из [4] сильнее этой очевидной верхней оценки.

В настоящей заметке мы изучаем вопрос, насколько точна верхняя оценка (1). Основным результатом является следующая теорема, из которой, в частности при $d = n$, вытекает дважды экспоненциальная (от n) нижняя оценка $M_{n,n} \geqslant n^{n^{\Omega(n^{1/(3+\varepsilon)})}}$ для произвольного $\varepsilon > 0$ (напомним, что асимптотическая нижняя оценка $f_1 \geqslant \Omega(f_2)$ обозначает, что $f_1 \geqslant cf_2$ для подходящей константы $c > 0$).

Теорема. a). $M_{n,d} \geqslant d^{d^{\Omega(\min\{d^{1/(3+\varepsilon)}, n\})}}$ *для произвольного* $\varepsilon > 0$*;*
b). $M_{n,d} \geqslant d^{\Omega(n)}$.

Отметим, что оценка a) сильнее оценки b), когда $d > (\Omega(\log n / \log\log n))^{(3+\varepsilon)}$. Когда $d > \Omega(n^{3+\varepsilon})$, то нижняя оценка a) $d^{d^{\Omega(n)}}$ имеет тот же порядок роста, что и верхняя оценка $2^{O(d^n)}$.

Рассмотрим в открытом в топологии Зарисского (см. [2]) множестве всех систем $g_1 = \ldots = g_n = 0$ с конечным числом решений (дискриминантное) подмногообразие систем, имеющих хотя бы одно кратное решение. Интересный вопрос, верно ли, что вектор кратностей постоянен на всякой страте стратификации Уитни дискриминантного подмногообразия? Если бы это было так, то из теоремы следовала бы нижняя оценка на количество страт. Упомянем, что до сих пор неизвестно, как растет количество страт: экспоненциально или дважды экспоненциально?

Доказательство теоремы

Обратимся сначала к доказательству a). Зафиксируем некоторые попарно различные точки $y_1, \ldots, y_k \in F$ и натуральные числа $m_1, \ldots, m_k > 0$. Обозначим $L = m_1 + \ldots + m_k$ и рассмотрим $L \times L$ матрицу H интерполяции Эрмита [1]. Элемент матрицы H в строке (i, j), где $1 \leqslant i \leqslant k$, $0 \leqslant j < m_i$, и столбце $0 \leqslant l < L$, равен $\binom{l}{j} y_i^{l-j}$, и является коэффициентом в разложении X^l по степеням $\{(X - y_i)^s\}_s$ при степени $(X - y_i)^j$. Хорошо известно, что матрица H неособая [1], более того $\det H = \prod_{1 \leqslant p < q \leqslant k} (y_p - y_q)^{m_p m_q}$. Иными словами, можно произвольно назначить значения разложения (единственного) многочлена степени не превосходящей L, в точках y_i, $1 \leqslant i \leqslant k$ вплоть до степеней $m_i - 1$, соответственно.

Для упрощения обозначений, положим $m_1 = \ldots = m_k = m$ и обозначим $mk \times mk$ матрицу $H_{m,k} = H$. Рассмотрим $(mk)^n \times (mk)^n$ матрицу $H^{(n)}$, являющуюся n-ой тензорной степенью матрицы

$H_{m,k}$. Тогда $H^{(n)}$ неособая, и ее элементы являются коэффициентами в разложении многочлена степеней меньших mk относительно каждой из n переменных $X_1, \dots, X_n$ в k^n точках $(x_1, \dots, x_n)$ решетки $R = \{y_1, \dots, y_k\}^n \subset F^n$ вплоть до степеней $m-1$ относительно каждой из n переменных $X_1 - x_1, \dots, X_n - x_n$. Таким образом, назначая произвольно эти коэффициенты, можно построить единственный многочлен из $F[X_1, \dots, X_n]$ степеней меньших mk относительно каждой из переменных $X_1, \dots, X_n$, с данными коэффициентами в разложениях в точках решетки.

Выберем для каждой точки $x = (x_1, \dots, x_n)$ решетки R n натуральных чисел $1 \leqslant l_1, \dots, l_n \leqslant m-1$ и построим (единственное) семейство многочленов $f_1, \dots, f_n \in F[X_1, \dots, X_n]$ степеней меньших mk относительно каждой из переменных $X_1, \dots, X_n$, таких, что разложение многочлена f_j, $1 \leqslant j \leqslant n$ в точке x имеет единственный ненулевой терм среди всех термов степеней меньших m относительно каждой из переменных $X_1 - x_1, \dots, X_n - x_n$, а именно, терм равный $(X_j - x_j)^{l_j}$.

Следующая лемма известна в фольклоре, но мы приводим ее доказательство в целях полноты изложения.

Лемма. *Кратность (0-мерной компоненты) x многообразия решений системы $f_1 = \ldots = f_n = 0$ равна $l_1 \ldots l_n$.*

Доказательство. Рассмотрим локальную алгебру

$$A = (F[X_1, \dots, X_n]/(f_1, \dots, f_n))_{(X_1 - x_1, \dots, X_n - x_n)}.$$

Очевидно, что мономы $(X_1 - x_1)^{l_1'} \ldots (X_n - x_n)^{l_n'}$ при $0 \leqslant l_1' < l_1, \dots, 0 \leqslant l_n' < l_n$ линейно независимы в A. Поэтому достаточно показать, что эти мономы составляют базис алгебры A.

Возьмем произвольный моном $G = (X_1 - x_1)^{s_1} \ldots (X_n - x_n)^{s_n}$ вне этого множества мономов. Тогда $s_j \geqslant l_j$ для некоторого $1 \leqslant j \leqslant n$. В алгебре A справедливо равенство

$$G = G - f_j \frac{G}{(X_j - x_j)^{l_j}} \in (X_1 - x_1, \dots, X_n - x_n)^m. \qquad (2)$$

Затем возьмем любой моном $G' = (X_1 - x_1)^{s_1'} \ldots (X_n - x_n)^{s_n'}$, входящий в элемент $G - f_j \frac{G}{(X_j - x_j)^{l_j}} \in A$, тогда $s_{j'}' \geqslant m$ для подходящего $1 \leqslant j' \leqslant n$. Поскольку $m > l_{j'}$, в алгебре A выполнено равенство

$$G' = G' - f_{j'} \frac{G'}{(X_{j'} - x_{j'})^{l_{j'}}} \in (X_1 - x_1, \dots, X_n - x_n)^{m+1}.$$

Поступая подобным образом с каждым из мономов, входящих в (2), мы получим в результате, что G равен сумме мономов из идеала $A \cap (X_1 - x_1, \dots, X_n - x_n)^{m+1}$, кроме того для каждого монома $(X_1 - x_1)^{s_1''} \dots (X_n - x_n)^{s_n''}$ из этой суммы существует $1 \leqslant j'' \leqslant n$, такой что $s_{j''} \geqslant m$.

Продолжая далее, мы заключаем, что $G \in \bigcap_{1 \leqslant s < \infty} (X_1 - x_1, \dots, X_n - x_n)^s$, отсюда $G = 0$ ввиду леммы Накаямы [2]. Лемма доказана.

Итак, для любого набора из k^n натуральных чисел вида $l_1 \cdots l_n$, где $1 \leqslant l_1, \dots, l_n \leqslant m - 1$, можно построить семейство многочленов $f_1, \dots, f_n \in F[X_1, \dots, X_n]$ с кратностями системы $f_1 = \dots = f_n = 0$ в k^n точках решетки R равными $l_1 \cdots l_n$, соответственно. Оценим теперь снизу, сколько мы построили всего различных векторов кратностей.

Так как $\deg f_j \leqslant (km - 1)n$, сумма кратностей 0-мерных компонент многообразия решений системы $f_1 = \dots = f_n = 0$ меньше $(kmn)^n$ в силу неравенства Безу. Если в качестве чисел $l_1, \dots, l_n$ мы выберем попарно различные простые числа между $\frac{m}{2}$ и $m-1$, то $l_1 \cdots l_n \geqslant \left(\frac{m}{2}\right)^n$. Имеется $\Omega\left(\frac{m}{\log m}\right)$ таких простых чисел (согласно закону о распределении простых чисел), поэтому различных произведений вида $l_1 \cdots l_n$ больше $P = \binom{\Omega\left(\frac{m}{\log m}\right)}{n}$, и количество построенных систем уравнений по крайней мере $\binom{P}{k^n}$. Среди кратностей 0-мерных компонент многообразия решений системы $f_1 = \dots = f_n = 0$ имеется не более $\frac{(kmn)^n}{(m/2)^n} = (2kn)^n$ кратностей больших $(m/2)^n$. Следовательно, самое большее $\binom{(2kn)^n}{k^n}$ среди векторов кратностей построенных систем вида $f_1 = \dots = f_n = 0$ могут совпадать с данным вектором.

Таким образом, при условии $P \geqslant (2kn)^{n(1+\varepsilon_1)}$ для некоторого $\varepsilon_1 > 0$, количество различных векторов кратностей для построенных систем больше, чем $\binom{P^{\Omega(1)}}{k^n}$. Это условие выполнено при $m > n^{2+\varepsilon}$ для некоторого $\varepsilon > 0$, и если положить $k = \left\lceil \left(\frac{m}{\log m}\right)^{3/(3+\varepsilon)} \frac{1}{n^2} \right\rceil$, то количество различных векторов кратностей будет больше $\binom{P^{\Omega(1)}}{k^n} > m^{m^{\Omega(n)}}$. Степени построенных многочленов $\deg f_i \leqslant kmn$, $1 \leqslant i \leqslant n$. Это доказывает теорему

a) в случае, когда $d > \Omega(n^{3+\varepsilon_2})$ для некоторого $\varepsilon_2 > 0$.

Чтобы завершить доказательство теоремы а) в случае, когда $d < O(n^{3+\varepsilon})$ для любого $\varepsilon > 0$, мы сперва применим изложенную выше конструкцию для числа переменных $n_0 = \lceil d^{1/(3+\varepsilon_0)} \rceil$ для произвольного $\varepsilon_0 > 0$, что даст нижнюю оценку на количество различных векторов кратностей $d^{d^{\Omega(d^{1/(3+\varepsilon_0)})}}$, а на оставшиеся $n - n_0$ переменных наложим в системе $f_1 = \ldots = f_n = 0$ уравнения, что они равны нулю.

Перейдем теперь к доказательству теоремы b). Зафиксируем некоторые константы $c_1, c_2 > 0$, положим $s = \lceil c_1 n \rceil$ и рассмотрим многочлены вида $f = (X-1)^{m_1} \ldots (X-s)^{m_s}$ в предположении, что $m_1 \ldots m_s \leqslant d^{c_2 n}$. Можно выразить f как модифицированную "схему вычисления", содержащую "элементарные операции" трех типов: сложение, умножение и взятие степени d_1 для всякого $d_1 \leqslant d$. Легко построить такую "схему", содержащую не более $N = O(\log_d m_1 + \ldots + \log_d m_s + s)$ "элементарных операций". Введем N новых переменных $Z_1, \ldots, Z_N$, примем также соглашение, что $Z_0 = X$, и представим такую модифицированную "схему" как последовательность из N уравнений вида либо

$$\begin{gathered} Z_j = Z_{j_1} + Z_{j_2}, \quad \text{либо} \quad Z_j = Z_{j_1} Z_{j_2}, \quad \text{либо} \\ Z_j = c Z_{j_1}, \quad \text{либо} \quad Z_j = Z_{j_1}^{d_1} \end{gathered} \tag{3}$$

в зависимости от текущей (j-ой) "элементарной операции", где $1 \leqslant j \leqslant N$, $j_1, j_2 < j$, $c \in F$, $d_1 \leqslant d$. Тогда Z_N "вычисляет" f.

Присоединяя к (3) еще уравнение $Z_N = 0$, получаем в результате систему в F^{N+1}, имеющую s решений кратностей $m_1, \ldots, m_s$, соответственно. Отметим, что $N \leqslant O(n)$. В итоге мы построим по крайней мере $d^{c_2 n}$ различных векторов кратностей $(m_1, \ldots, m_s)$, поскольку всякому значению произведения $m_1 \ldots m_s$ соответствует хотя бы один вектор $(m_1, \ldots, m_s)$. Теорема доказана.

Автор выражает признательность Вите Васильеву за полезные обсуждения.

Литература

1. И. С. Березин, Н. П. Жидков, *Методы вычислений.* Москва (1966).
2. И. Р. Шафаревич, *Основы алгебраической геометрии.* Москва (1974).
3. A. L. Chistov, D. Yu. Grigoriev, *Subexponential time solving systems of algebraic equations I, II.* Preprints LOMI E-9-83, E-10-83, Leningrad, 1983.

4. D. Yu. Grigoriev, N. N. Vorobjov, *Bounds on numbers of vectors of multiplicaties for polynomials which are easy to compute.* Proc. Intern. ACM Symp. on Symbol Algebr. Comput., Scotland, 2000, p. 138–146.

Grigor'ev D. Yu. Double-exponential growth of the number of vectors of solutions of polynomial systems.

In [4] it was proved an upper bound $d^{\left(\binom{n+d}{n}\right)}$ on the number of vectors of multiplicities of the solutions of systems of the form $g_1 = \ldots = g_n = 0$ (provided, it has a finite number of solutions) of polynomials $g_1, \ldots, g_n \in F[X_1, \ldots, X_n]$ with degrees $\deg g_i \leqslant d$ (the field F is algebraically closed). In the present paper it is shown that this bound is close in order to the exact one. In particular, in case $d = n$ the construction provides a double-exponential (in n) number of vectors of multiplicities.

IMR, Université de Rennes,
Beaulien 35042 Rennes, France,
Санкт-Петербургское отделение
Математического института
им. В. А. Стеклова РАН
dima@maths.univ-rennes1.fr

Поступило 3 августа 2000 г.