Constructing double-exponential number of vectors of multipilicities of solutions of polynomial systems

Dima Grigoriev*

Abstract

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

Introduction

We consider systems $g_1 = \cdots = g_n = 0, g_i \in F[X_1, \ldots, X_n]$ where $\deg(g_i) \leq d, 1 \leq i \leq n$ and F is an algebraically closed field. To each 0-dimensional component $a = (a_1, \ldots, a_n) \in F^n$ of the variety of solutions $V = \{g_1 = \cdots = g_n = 0\} \subset F^n$ one attaches its (finite) multiplicity

$m_a = \dim_F(F[X_1, \ldots, X_n]/(g_1, \ldots, g_n))_{(X_1-a_1, \ldots, X_n-a_n)}$ [S].

One attributes to the system $g_1 = \cdots = g_n = 0$ the (ordered) vector $\{m_a\}_a$ over all 0-dimensional components a of the variety V. Denote by $M_{n,d}$ the number of all possible vectors of the form $\{m_a\}_a$.

It was proved in [GV] that for fields F of zero characteristics in case when $\dim(V) = 0$, we have an upper bound $M_{n,d} \leq d^{O(\binom{n+d}{n})}$ (majorating $M_{n,d}$ was

*IRMAR, Université de Rennes, Campus de Beaulieu, 35042 Rennes, cedex France

motivated by the complexity issues, see [GV]). We mention that making use of the machinery of algorithmic perturbations of systems of polynomial equations developped in [CG], one could establish a similar upper bound on $M_{n,d}$ getting rid of the restriction $\dim(V) = 0$. We note that the exponent $\binom{n+d}{n}$ in the bound is the number of the coefficients of polynomials of degree d, in other words, the number of parameters of systems under considerations. One could compare the upper bound from [GV] with the obvious upper bound $2^{O(d^n)}$, taking into account that $\{m_a\}_a$ is in fact, a partition of an integer less or equal to d^n due to the Bezout inequality [S]. For $d < n$ the bound from [GV] is better than this obvious upper bound.

In the present paper we study a question, how sharp is the upper bound on $M_{n,d}$ from [GV]? We prove the following theorem, from which particularly, in case $d = n$ one gets a doubly-exponential (in n) lower bound $M_{n,n} \geq n^{n^{\Omega(n^{1/(3+\varepsilon)})}}$ for any $\varepsilon > 0$ (we remind that an asymptotical lower bound $f_1 \geq \Omega(f_2)$ means that $f_1 \geq cf_2$ for a suitable constant $c > 0$).

Theorem 1 *a)* $M_{n,d} \geq d^{d^{\Omega(\min\{d^{1/(3+\varepsilon)}, n\})}}$ *for any* $\varepsilon > 0$*;*
b) $M_{n,d} \geq d^{\Omega(n)}$.

The bound from a) is stronger than the one from b) when $d > \left(\Omega\left(\frac{\log n}{\log\log n}\right)\right)^{3+\varepsilon}$. When $d > \Omega(n^{3+\varepsilon})$ for a certain $\varepsilon > 0$ then the lower bound in a) $d^{d^{\Omega(n)}}$ grows with a similar order as the upper bound $2^{O(d^n)}$ (cf. above).

Consider in the Zariski open set of all the systems $f_1 = \cdots = f_n = 0$ with a finite number of solutions the (discriminantal) subvariety of systems with at least one multiple solution. The question is whether on every stratum of a Whitney stratification of the discriminantal variety the vector of multiplicities is constant? If this would be true the above theorem would provide a lower bound on the number of strata. We mention that this is a challenging problem to clarify whether the number of strata (say, of a hypersurface) could be double-exponential or just a single-exponential?

Constructing vectors of multiplicities

Now we proceed to the proof of a).

Fix some pairwise distinct points $y_1, \ldots, y_k \in F$ and integers $m_1, \ldots, m_k > 0$. Denote $L = m_1 + \cdots + m_k$ and consider $L \times L$ matrix H of the Hermite interpolation as follows. The entry of H in a row (i, j) where $1 \leq i \leq k$, $0 \leq j < m_i$ and a column l, $0 \leq l < L$, equals to $\binom{l}{j} y_i^{l-j}$ being the coefficient of the expansion of X^l in the powers $\{(X - y_i)^s\}_s$ at the power $(X - y_i)^j$. It is well known that H is non-singular, moreover $\det(H) = \prod_{1 \leq p < q \leq k} (y_p - y_q)^{m_p m_q}$. In other words, one can assign in an arbitrary way the values of the expansions of a (unique) polynomial of the degree L at the points $y_i, 1 \leq i \leq k$ up to the powers $m_i - 1$, respectively.

For the sake of simplicity of notations we set $m_1 = \dots m_k = m$ and denote $mk \times mk$ matrix $H_{m,k} = H$. Denote by $H^{(n)}$ the matrix of the size $(mk)^n \times (mk)^n$ being the n-th tensor power of $H_{m,k}$. Then $H^{(n)}$ is non-singular and its entries correspond to the coefficients in the expansion of a polynomial of a degree at most $mk - 1$ with respect to each of n variables $X_1, \dots, X_n$ at k^n points of the form $(x_1, \dots, x_n)$ from the grid $R = \{y_1, \dots, y_k\}^n \subset F^n$ up to the powers $m - 1$ with respect to each of n variables $X_1 - x_1, \dots, X_n - x_n$. Thus, after assigning in an arbitrary way these coefficients one could find a unique polynomial in n variables $X_1, \dots, X_n$ of the degrees at most $mk - 1$ with respect to each of the variables $X_1, \dots, X_n$ just with these assigned coefficients in the expansions.

Choose for each point $x = (x_1, \dots, x_n)$ from the grid R n integers $1 \leq l_1, \dots, l_n \leq m - 1$ and take the (unique) family of polynomials $f_1, \dots, f_n \in F[X_1, \dots, X_n]$ of the degrees at most $mk - 1$ with respect to each of the variables $X_1, \dots, X_n$ such that the polynomial $f_j, 1 \leq j \leq n$ in the expansion at the point x has the unique non-zero term among all the terms of the degrees at most $m - 1$ with respect to each of the variables $X_1 - x_1, \dots, X_n - x_n$, namely, equal to $(X_j - x_j)^{l_j}$.

The following lemma belongs to the folklore, but we still give its proof for the sake of self-containdness.

Lemma 1 *The multiplicity of (the 0-dimensional component) x of the variety of solutions of the system $f_1 = \dots = f_n = 0$ equals to $l_1 \cdots l_n$.*

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

Clearly, the monomials $(X_1 - x_1)^{l_1'} \cdots (X_n - x_n)^{l_n'}$ for $0 \leq l_1' < l_1, \dots, 0 \leq l_n' < l_n$ are linearly independent in A. Therefore, it suffices to show that these monomials constitute a basis in A.

Take any monomial $G = (X_1 - x_1)^{s_1} \cdots (X_n - x_n)^{s_n}$ out of this set. Then $s_j \geq l_j$ for a certain $1 \leq j \leq n$. In the algebra A the element

$$G = G - f_j \frac{G}{(X_j - x_j)^{l_j}} \in (X_1 - x_1, \ldots, X_n - x_n)^m \tag{1}$$

After that take any monomial $G' = (X_1 - x_1)^{s_1'} \cdots (X_n - x_n)^{s_n'}$ occurring in the latter element of A, then $s_{j'}' \geq m$ for a suitable $1 \leq j' \leq n$. Since $m > l_{j'}$ we have in the algebra A

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

Acting in a similar way with each monomial occurring in (1), we obtain as a result that G equals to a sum of monomials from the ideal $A \cap (X_1 - x_1, \ldots, X_n - x_n)^{m+1}$, moreover for any of these monomials $(X_1 - x_1)^{s_1''} \cdots (X_n - x_n)^{s_n''}$ from the sum there exists $1 \leq j'' \leq n$ such that $s_{j''}'' \geq m$.

Continuing further we conclude that $G \in \cap_{1 \leq s < \infty} (X_1 - x_1, \ldots, X_n - x_n)^s$, hence $G = 0$ due to Nakayama's lemma (see e.g. [S]). This completes the proof of lemma. $\Box$

Thus, for every family of k^n integers of the form $l_1 \cdots l_n$ where $1 \leq l_1, \ldots, l_n \leq m - 1$, one can construct a system of polynomials $f_1, \ldots, f_n \in F[X_1, \ldots, X_n]$ with the multiplicities of the system $f_1 = \ldots = f_n = 0$ at k^n points of the grid R being equal to $l_1 \cdots l_n$, respectively. Let us bound from below, how many *diverse* vectors of multiplicities we have constructed totally.

Because $\deg(f_j) \leq (km - 1)n$ the sum of the multiplicities of the 0-dimensional solutions of the system $f_1 = \ldots = f_n = 0$ is less than $(kmn)^n$ due to the Bezout inequality. As the integers $l_1, \ldots, l_n$ we choose the pairwise distinct prime numbers between $m/2$ and $m - 1$, so $l_1 \cdots l_n \geq (m/2)^n$. Since there are $\Omega(m/\log m)$ such prime numbers (according to the law of distribution of prime numbers) we conclude that the number of diverse products of the form $l_1 \cdots l_n$ is greater than $P = \binom{\Omega(m/\log m)}{n}$, and the number of the constructed systems is at least $\binom{P}{k^n}$. Among the multiplicities of 0-dimensional solutions of a system $f_1 = \ldots = f_n = 0$ there are at most $\frac{(kmn)^n}{(m/2)^n}$ multiplicities which are greater or equal to $(m/2)^n$. Therefore, at most $\binom{(2kn)^n}{k^n}$ of the vectors of multiplicities of the constructed systems of the form $f_1 = \ldots = f_n = 0$ could coincide with a given one.

Thus, under the condition $P \geq (2kn)^{n(1+\varepsilon_1)}$ for a certain $\varepsilon_1 > 0$, the number of diverse vectors of multiplicities of the constructed systems is greater than $\binom{P^{\Omega(1)}}{k^n}$. The latter condition would be fulfilled when $m > n^{2+\varepsilon}$ for a certain $\varepsilon > 0$ and if one takes $k = \lceil (\frac{m}{\log m})^{3/(3+\varepsilon)} \frac{1}{n^2} \rceil$ then the number of diverse vectors of multiplicities would be greater than $\binom{P^{\Omega(1)}}{k^n} > m^{m^{\Omega(n)}}$. The degrees of the constructed polynomials $\deg(f_i) \leq kmn$. This proves the theorem a) when $d > \Omega(n^{3+\varepsilon_2})$ for an appropriate $\varepsilon_2 > 0$.

To complete the proof of the theorem a) when $d < O(n^{3+\varepsilon})$ for any $\varepsilon > 0$ we first apply the above construction for the number of variables $n_0 = \lceil d^{1/(3+\varepsilon_0)} \rceil$ for an arbitrary $\varepsilon_0 > 0$, that provides the number of diverse vectors of multiplicities greater than $d^{d^{\Omega(d^{1/(3+\varepsilon_0)})}}$, and the remaining $n - n_0$ variables we take as dum and imposing them to vanish. $\Box$

Now we proceed to the proof of the theorem b). Fix some constants $c_1, c_2 > 0$, set $s = \lceil c_1 n \rceil$ and consider univariate polynomials of the form $f = (X-1)^{m_1} \cdots (X-s)^{m_s}$ with the condition $m_1 \cdots m_s \leq d^{c_2 n}$. One can realize f as a "modified straight-line program" with three types of elementary operations: addition, multiplication and taking d_1-power with $d_1 \leq d$. To realize f at most $N = O(\log_d m_1 + \cdots + \log_d m_s + s)$ operations of described types are sufficient. One can introduce N new variables $Z_1, \ldots, Z_N$, we also agree that $Z_0 = X$ and represent such a "modified straight-line program" as a sequence of N equations of the form either

$$Z_j = Z_{j_1} + Z_{j_2}, \text{ either } Z_j = Z_{j_1} Z_{j_2}, \text{ either } Z_j = cZ_{j_1} \text{ or } Z_j = Z_{j_1}^{d_1} \qquad (2)$$

where $1 \leq j \leq N, j_1, j_2 < j, c \in F, d_1 \leq d$. Then Z_N "calculates" f.

Adjoining to (2) an equation $Z_N = 0$ we obtain as a result a system in F^{N+1} having s solutions with the multiplicities $m_1, \ldots, m_s$, respectively. Note that $N \leq O(n)$. We get greater or equal to $d^{c_2 n}$ distinct vectors of multiplicities $m_1, \ldots, m_s$ because to every value of the product $m_1 \cdots m_s$ corresponds at least one vector $m_1, \ldots, m_s$. This completes the proof of the theorem. $\Box$

Acknowledgement. The author would like to thank Vitya Vassiliev for useful discussions.

References

[CG] A.Chistov, D.Grigoriev. Subexponential time solving systems of algebraic equations I, II. Preprints LOMI E-9-83, E-10-83, Leningrad, 1983.

[GV] D.Grigoriev, N.Vorobjov. Bounds on the number of vectors of multiplicities for polynomials which are easy to compute. Proc. ACM Intern. Conf. Symbol. and Algebr. Comput., Scotland, 2000, p. 137–145.

[S] I.Shavarevich. Basic algebraic geometry, Springer, 1982.