Efficient solving systems of polynomial equations with parametric coefficients

Alexander L. Chistov

St. Petersburg Department of Steklov Mathematical Institute
of the Academy of Sciences of Russia
Fontanka 27, St. Petersburg 191023, Russia,
e-mail: alch@pdmi.ras.ru

2017

Abstract

Consider a system of polynomial equations with parametric coefficients over an arbitrary ground field. We show that the variety of parameters can be represented as union of strata. Each stratum is a quasiprojective algebraic variety with the degree bounded from above by a subexponential function in the size of the input data. Also the number of strata is subexponential in the size of the input data. This solves a long standing problem to avoid double exponential growth of coefficients for this problem.

Let k be an arbitrary field containing sufficiently many elements with the characteristic exponent p. Let $\nu \geqslant 0$ be an integer. Let $a_1, \ldots, a_\nu$ be a family of independent variables (or parameters) over k. Denote by $\mathbb{A}^\nu(\overline{k})$ the affine space of parameters with the coordinate functions $a_1, \ldots, a_\nu$ (in a more general situation one can consider an algebraic variety of parameters $\mathcal{V} \subset \mathbb{A}^\nu(\overline{k})$ but this case is easily reduced to the particular one: $\mathcal{V} = \mathbb{A}^\nu(\overline{k})$).

Let $m, n \geqslant 1$ be integers. Let $f_0, \ldots f_{m-1} \in k[a_1, \ldots, a_\nu, X_0, \ldots, X_n]$ be homogeneous with respect to $X_0, \ldots, X_n$ polynomials. Assume that the degrees

$$\deg_{X_1,\ldots,X_n} f_i = d_i \leqslant d, \quad \deg_{a_1,\ldots,a_\nu} f \leqslant d' \tag{1}$$

for some integers $d_0, \ldots, d_{m-1} \geqslant 0$ and $d, d' \geqslant 2$. Let $a^* = (a_1^*, \ldots, a_\nu^*) \in \mathbb{A}^\nu(\overline{k})$ Denote by $V_{a^*} \subset \mathbb{P}^n(\overline{k})$ the variety of all the solutions of the system of polynomial equations

$$f_0(a_1^*, \ldots, a_\nu^*, X_0, \ldots, X_n) = \ldots = f_{m-1}(a_1^*, \ldots, a_\nu^*, X_0, \ldots, X_n) = 0.$$

Let $-1 \leqslant c \leqslant n$ be an integer. Denote by $\mathcal{U}_c$ the subset of all $a^* \in \mathbb{A}^\nu(\overline{k})$ such that the dimension $\dim V_{a^*} \leqslant c$. One can prove that it is an open in the Zariski topology subset of $\mathbb{A}^\nu(\overline{k})$. For every point $a^* \in \mathcal{U}_c$ for every integer $0 \leqslant s \leqslant c$ denote by $V_{a^*,s}$ the union of all irreducible components W of the variety V_{a^*} such that the dimension $\dim W = s$.

Key words and phrases: parametric coefficients, stratifications, absolutely irreducible components, solving polynomial systems.

UDK 513.6+518.5; 2010 Mathematics Subject Classification: 14Q15.

Consider the problem to represent the set of parameters

$$\mathcal{U}_c = \bigcup_{\alpha\in A} \mathcal{W}_\alpha \tag{2}$$

as a union of a finite number, i.e., $\#A < +\infty$, of quasiprojective algebraic varieties $\mathcal{W}_\alpha$ satisfying the following properties. For every $\alpha \in A$ for all $a^* = (a_1^*, \dots, a_\nu^*) \in \mathcal{W}_\alpha$ the variety of solutions V_{a^*} is given uniformly, i.e., by some algebraic formulas (similarly to [2], see below for details) everywhere defined on $\mathcal{W}_\alpha$ and depending on $a_1^*, \dots, a_\nu^*$ as parameters.

For an arbitrary polynomial $f \in k[a_1, \dots, a_\nu, X_0, \dots, X_n]$ and a point $a^* = (a_1^*, \dots, a_\nu^*) \in \mathbb{A}^\nu(\overline{k})$ we shall write $f(a^*, X_0, \dots, X_n) = f(a_1^*, \dots, a_\nu^*, X_0, \dots, X_n)$ and use other similar notations. We shall write $V_{a^*} = \mathcal{Z}(f_i(a^*, X_0, \dots, X_n),\ 0 \leqslant i \leqslant m-1)$. Here $\mathcal{Z}(f_i(a^*, X_0, \dots, X_n),\ 0 \leqslant i \leqslant m-1)$ denotes the set of all common zeroes of the considered polynomials in $\mathbb{P}^n(\overline{k})$. We will use also other analogous notations. In what follows all the constants in $O(\dots)$ are absolute. All the linear forms $Y_i, Y_{i,v}$ from the described below construction can be chosen with coefficients of length, say, $O(n^2 \log_2 d)$ in any subring of k with sufficiently many elements.

Now we are going to give the precise meaning to the uniformity of algebraic formulas related to (2). Namely the following properties hold true.

(i) For every $\alpha \in A$ the variety $\mathcal{W}_\alpha \neq \varnothing$. For all $\alpha_1, \alpha_2 \in A$ if $\alpha_1 \neq \alpha_2$ then $\mathcal{W}_{\alpha_1} \cap \mathcal{W}_{\alpha_2} = \varnothing$, i.e., these varieties $\mathcal{W}_\alpha$ are pairwise disjoint; so we shall call them strata and union (2) is a stratification.

(ii) One can represent

$$\mathcal{W}_\alpha = \mathcal{W}_\alpha^{(1)} \setminus \bigcup_{2\leqslant\beta\leqslant\mu_\alpha} \mathcal{W}_\alpha^{(\beta)}$$

where each $\mathcal{W}_\alpha^{(\beta)} = \mathcal{Z}(\psi_{\alpha,1}^{(\beta)}, \dots, \psi_{\alpha,m_{\alpha,\beta}}^{(\beta)})$, $1 \leqslant \beta \leqslant \mu_\alpha$, is the set of all common zeroes of the polynomials $\psi_{\alpha,1}^{(\beta)}, \dots, \psi_{\alpha,m_{\alpha,\beta}}^{(\beta)} \in k[a_1, \dots, a_\nu]$ in the affine space $\mathbb{A}^\nu(\overline{k})$, $m_{\alpha,\beta} \geqslant 1$ is an integer.

For every $\alpha \in A$ for every integer $0 \leqslant s \leqslant c$ there are linear forms $Y_0, \dots, Y_{s+1} \in k[X_0, \dots, X_n]$ (depending on α and s) satisfying the following properties.

(iii) For every $a^* \in \mathcal{W}_\alpha$ the intersection $V_{a^*,s} \cap \mathcal{Z}(Y_0, \dots, Y_s) = \varnothing$ in $\mathbb{P}^n(\overline{k})$.

(iv) Let $\rho = 0$ if $p = 1$ and otherwise $\rho = \log_p d^{n-s}$. For every integer $0 \leqslant r \leqslant \rho$ there is a nonzero polynomial $\Phi_{\alpha,s,r} \in k[a_1, \dots, a_\nu, Y_0, \dots, Y_{s+1}]$ homogeneous with respect to $Y_0, \dots, Y_{s+1}$ such that for every $a^* \in \mathcal{W}_\alpha$ the degree

$$0 \leqslant \deg_{Y_0,\dots,Y_{s+1}} \Phi_{\alpha,s,r} = \deg_{Y_{s+1}} \Phi_{\alpha,s,r}(a^*, Y_0, \dots, Y_{s+1}) \leqslant d^{n-s}/p^r,$$

the leading coefficient $\operatorname{lc}_{Y_{s+1}} \Phi_{\alpha,s,r} \in k[a_1, \dots, a_\nu]$, and the polynomial $\prod_{0\leqslant r\leqslant\rho} \Phi_{\alpha,s,r}(a^*, Y_0^{p^r}, \dots, Y_{s+1}^{p^r})$ vanishes on the projective algebraic variety $V_{a^*,s}$. Finally denote by $\Delta_{\alpha,s,r}$ the discriminant of the polynomial $\Phi_{\alpha,s,r}$ with respect to Y_{s+1} (by definition $\Delta_{\alpha,s,r} = 1$ if $\deg_{Y_{s+1}} \Phi_{\alpha,s,r} = 0$). Then for every $a^* \in \mathcal{W}_\alpha$ the polynomial $\Delta_{\alpha,s,r}(a^*, Y_0, \dots, Y_s) \neq 0$.

(v) Let Z be a new variable. There is a finite (or empty) family of polynomials $H_j \in k[a_1, \ldots, a_\nu, Z]$, $j \in J_{\alpha,s,r}$, satisfying the following properties. The degree $1 \leqslant \deg_Z H_j \leqslant d^{n-s}$. Denote by Δ_j the discriminant of the polynomial Δ_j with respect to Z. Then $\Delta_j(a^*) \neq 0$ for every $a^* \in \mathcal{W}_\alpha$. Denote by Ξ_{j,a^*} the family of roots from $\overline{k}$ of the separable polynomial $H_j(a^*, Z)$. We assume that the sets of indices $J_{\alpha,s,r}$ are pairwise disjoint.

(vi) There is a family of polynomials $\Phi_{\alpha,s,j} \in k[a_1, \ldots, a_\nu, Z, Y_0, \ldots, Y_{s+1}]$, $j \in J_{\alpha,s,r}$, and polynomials $\lambda_0, \lambda_1 \in k[a_1, \ldots, a_\nu]$ (they depend on α, s, r) satisfying the following properties. For every $a^* \in \mathcal{W}_\alpha$ the polynomials $\Phi_{\alpha,s,j}$ are homogeneous with respect to $Y_0, \ldots, Y_{s+1}$, the degree $\deg_Z \Phi_{\alpha,s,j} < \deg_Z H_j$, the leading coefficient $\mathrm{lc}_{Y_{s+1}} \Phi_{\alpha,s,j} \in k[a_1, \ldots, a_\nu]$, all the polynomials $\Phi_{\alpha,s,j}(a^*, \xi, Y_0, \ldots, Y_{s+1})$, $\xi \in \Xi_{j,a^*}$, $j \in J_{\alpha,s,r}$, are irreducible over $\overline{k}$ in the ring $\overline{k}[X_0, \ldots, X_n]$, $\lambda_0(a^*) \neq 0$, $\lambda_1(a^*) \neq 0$ and

$$\Phi_{\alpha,s,r}(a^*, Y_0, \ldots, Y_{s+1}) = \frac{\lambda_0(a^*)}{\lambda_1(a^*)} \prod_{j \in J_{\alpha,s,r},\, \xi \in \Xi_{j,a^*}} \Phi_{\alpha,s,j}(a^*, \xi, Y_0, \ldots, Y_{s+1}).$$

Hence $\deg_{Y_0,\ldots,Y_{s+1}} \Phi_{\alpha,s,j} \leqslant \deg_{Y_0,\ldots,Y_{s+1}} \Phi_{\alpha,s,r} \leqslant d^{n-s}/p^r$.

(vii) For every $a^* \in \mathcal{W}_\alpha$ the irreducible over $\overline{k}$ components of the projective algebraic variety $V_{a^*,s}$ are in the natural one–to–one correspondence with pairs (ξ, j) where $\xi \in \Xi_{j,a^*}$, $j \in J_{\alpha,s,r}$, $0 \leqslant r \leqslant \rho$. Denote by $W_{j,a^*,\xi}$ the irreducible over $\overline{k}$ component of the algebraic variety $V_{a^*,s}$ corresponding to the pair (ξ, j). We have $\deg W_{j,a^*,\xi} = \deg_{Y_{s+1}} \Phi_{\alpha,s,j}$.

(viii) Let Y and Z be variables, $t_1, \ldots, t_s$ be a family of algebraically independent elements over $\overline{k}$, the element $j \in J_{\alpha,s,r}$ and $\Phi_{\alpha,s,j}(a^*, \xi, 1, t_1^{p^r}, \ldots, t_s^{p^r}, \theta^{p^r}) = 0$. Then there are polynomials $D_j \in k[a_1, \ldots, a_\nu, t_1, \ldots, t_s]$, $D_{j,i} \in k[a_1, \ldots, a_\nu, Z, t_1, \ldots, t_s, Y]$, $0 \leqslant i \leqslant n$, satisfying the following properties. The polynomial $D_j(a^*, t_1, \ldots, t_s) \neq 0$ for every $a^* \in \mathcal{W}_\alpha$, the degrees $\deg_Z D_{j,i} < \deg_Z H_j$, $\deg_Y D_{j,i} < \deg_{Y_{s+1}} \Phi_{\alpha,s,j}$ and all $\deg_{t_1,\ldots,t_s} D_j$, $\deg_{t_1,\ldots,t_s} D_{j,i}$ are bounded from above by $d^{O(n-s)}$. Further there is a $\overline{k}$-isomorphism of fields $\overline{k}(W_{j,a^*,\xi}) \to \overline{k}(t_1, \ldots, t_s)[\theta]$ such that $Y_i/Y_0 \mapsto t_i$, $1 \leqslant i \leqslant s$, $Y_{s+1}/Y_0 \mapsto \theta$,

$$(X_i/Y_0)^{p^r} \mapsto D_{j,i}(a^*, \xi, t_1^{p^r}, \ldots, t_s^{p^r}, \theta^{p^r}) / D_j(a^*, t_1^{p^r}, \ldots, t_s^{p^r}), \quad 0 \leqslant i \leqslant n.$$

Hence this isomorphism gives a generic point of the algebraic variety $W_{j,a^*,\xi}$.

(ix) There is a finite family of linear forms $Y_{i,v} \in k[X_0, \ldots, X_n]$, $i \in I_{\alpha,s}$, $0 \leqslant v \leqslant s+2$, depending only on α, s and satisfying the following properties. For every $i \in I_{\alpha,s}$ for every $0 \leqslant v \leqslant s$ the linear form $Y_{i,v} = Y_v$. Further for every $j \in J_{\alpha,s,r}$, $0 \leqslant r \leqslant \rho$, $i \in I_{\alpha,s}$ there is a family of polynomials $\Psi_{\alpha,s,j,i,w} \in k[a_1, \ldots, a_\nu, Z, Y_{i,0}, \ldots, Y_{i,s+2}]$, $w \in I_{\alpha,s,j,i}$, homogeneous with respect to $Y_{i,0}, \ldots, Y_{i,s+2}$ and satisfying the following conditions. The degrees $\deg_Z \Psi_{\alpha,s,j,i,w} < \deg_Z H_j$, $\deg_{Y_{i,0},\ldots,Y_{i,s+2}} \Psi_{\alpha,s,j,i,w} \leqslant \deg_{Y_{s+1}} \Phi_{\alpha,s,j}$, finally for every point $a^* \in \mathcal{W}_\alpha$ the projective algebraic variety

$$W_{j,a^*,\xi} = \mathcal{Z}(\Psi_{\alpha,s,j,i,w}(a^*, \xi, Y_{i,0}^{p^r}, \ldots, Y_{i,s+2}^{p^r}),\ w \in I_{\alpha,s,j,i},\ i \in I_{\alpha,s}) \quad (3)$$

in $\mathbb{P}^n(\overline{k})$ and the number of elements $\#I_{\alpha,s} = d^{O(n-s)}$, $\#I_{\alpha,s,j,i} \leqslant d^{n-s}/p^r$ for all α, s, j, i. So (3) gives a system of homogeneous polynomial equations determining the algebraic variety $W_{j,a^*,\xi}$.

Now we able to formulate our main result.

THEOREM 1 *Let $f_0, \dots, f_{m-1} \in k[a_1, \dots, a_\nu, X_1, \dots, X_n]$ and $\mathcal{U}_c$ be as above. Then there is a stratification (2) satisfying the properties (i)–(ix) and such that*

(a) the number of elements $\#A$ and all the integers μ_α, $m_{\alpha,\beta}$ are bounded from above by $(d')^\nu d^{O(n\nu)}$ with an absolute constant in $O(n\nu)$,

(b) the degrees with respect to $a_1, \dots, a_\nu$ of all the polynomials $\psi^{(\beta)}_{\alpha,1}, \dots, \psi^{(\beta)}_{\alpha,m_{\alpha,\beta}}$, $\Phi_{\alpha,s,r}$, H_j, $\Phi_{\alpha,s,j}$, λ_0, λ_1, D_j, $D_{j,i}$, $\Psi_{\alpha,s,j,i,w}$ are bounded from above by $d'd^{O(n)}$ with an absolute constant in $O(n)$.

The proof of this theorem is based on the algorithm from [2] with some modifications and the results of [5], [6], see also [3], [4]. For the considered problem previously known estimates for degrees were double-exponential, cf. [1], [7].

References

[1] **Ayad A.:** *"Complexity of solving parametric polynomial systems"*, Zap. Nauchn. Semin. POMI v.387 (2011), p. 5–52

[2] **Chistov A. L.:** *"Polynomial complexity algorithm for factoring polynomials and constructing components of a variety in subexponential time"*, Zap. Nauchn. Semin. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) 137 (1984), p. 124–188 (in Russian) [English transl.: J. Sov. Math. 34, (4), (1986) p. 1838–1882].

[3] **Chistov A. L.:** *"An improvement of the complexity bound for solving systems of polynomial equations"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) 390 (2011), p. 299–306.

[4] **Chistov A. L.:** *"A Bound for the Degree of a System of Equations Determining the Variety of Reducible Polynomials"*, Algebra i Analiz 24 #3 (2012) p. 199–222 (in Russian), and *"Correction..."*, Algebra i Analiz 25 #2 (2013) p. 279 (in Russian) [English transl.: St. Petersburg Math. J. 24 #3 (2013), p. 513–528]

[5] **Chistov A. L.:** *"Computations with parameters: a theoretical background"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) 436 (2015), p. 219–239 (in Russian) [English transl.: Journal of Mathematical Sciences 2016, Volume 215, Issue 6, p. 769–781].

[6] **Chistov A. L.:** *"Efficient absolute factoring polynomials with parametric coefficients"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) 448 (2016), p. 286–325 (in Russian) [English transl.: to appear in St. Petersburg Math. J.]

[7] **Lazard D., Rouillier F.:** *"Solving parametric polynomial systems"*, Journal of Symbolic Computation v.42 #6 (2007), p. 636–667.