Polynomial Complexity of Solving Systems of Few Algebraic Equations with Small Degrees

Dima Grigoriev

CNRS, Mathématiques, Université de Lille, Villeneuve d'Ascq, 59655, France
Dmitry.Grigoryev@math.univ-lille1.fr
http://logic.pdmi.ras.ru/~grigorev

Abstract. An algorithm is designed which tests solvability of a system of k polynomial equations in n variables with degrees d within complexity polynomial in $n^{d^{3k}}$. If the system is solvable then the algorithm yields one of its solutions. Thus, for fixed d, k the complexity of the algorithm is polynomial.

Keywords: polynomial complexity, solving systems of few equations, small degrees.

Introduction

Consider a system of polynomial equations

$$f_1 = \cdots = f_k = 0, \tag{1}$$

where $f_1, \dots, f_k \in \mathbb{Z}[X_1, \dots, X_n]$, $\deg f_i \le d$, $1 \le i \le k$. The algorithm from [1], [2] (see also [3]) solves (1) within complexity polynomial in M, k, d^{n^2}, where M denotes the bound on bit-sizes of (integer) coefficients of polynomials $f_1, \dots, f_k$. Moreover, this algorithm finds the irreducible components of the variety in $\mathbb{C}^n$ determined by (1). We mention also that in [4] an algorithm is designed which tests solvability of (1) reducing it to a system of equations over $\mathbb{R}$, within a better complexity polynomial in M, $(k \cdot d)^n$. We note that the algorithm from [4] tests solvability of (1) and outputs a solution, provided that (1) is solvable, rather than finds the irreducible components as the algorithms from [1], [2].

In the present paper we design an algorithm which tests solvability of (1) within complexity polynomial in $M \cdot \binom{n+d^{3k}}{n} \le M \cdot n^{d^{3k}}$, which provides polynomial (in the size $M \cdot k \cdot \binom{n+d}{n}$ of the input system (1)) complexity when d, k being fixed. If (1) is solvable then the algorithm yields one of its solutions. Note that the algorithm from [4] has a polynomial complexity when, say $d > n^2$ and k being polynomial in n; when d is close to n the complexity is subexponential, while for small d the complexity is exponential.

We mention that in [5] an algorithm was designed testing solvability of (1) over $\mathbb{R}$ (and finding a real solution, provided that it does exist) within the complexity polynomial in M, n^{2k} for quadratic equations ($d = 2$), and moreover, one can replace equations by inequalities.

V.P. Gerdt et al. (Eds.): CASC 2013, LNCS 8136, pp. 136–139, 2013.

It would be interesting to clarify, for which relations between n, k, and d the complexity of solvability of (1) is polynomial. In particular, when $d = 2$ and k is close to n the problem of solvability is NP-hard.

1 Testing Points for Sparse Polynomials

Recall (see [6]) a construction of testing points for sparse polynomials in n variables. Let p_i denote the ith prime and $s_j = (p_1^j, \dots, p_n^j) \in \mathbb{Z}^n, j \geq 0$ be a point. A polynomial $f \in \mathbb{C}[X_1, \dots, X_n]$ is called t-sparse if it contains at most t monomials.

Lemma 1. *For a t-sparse polynomial f there exists $0 \leq j < t$ such that $f(s_j) \neq 0$.*

The proof follows from the observation that writing $f = \sum_{1 \leq l \leq t} a_l \cdot X^{I_l}$ where coefficients $a_l \in \mathbb{C}$ and X^{I_l} are monomials, the equations $f(s_j) = 0$, $0 \leq j < t$ lead to a $t \times t$ linear system with Vandermonde matrix and its solution $(a_1, \dots, a_t)$. Since Vandermonde matrix is nonsingular, the obtained contradiction proves the lemma.

The substitution of points s_j was first introduced in the proof of theorem 1 [6].

Corollary 1. *Let* $\deg f \leq D$. *There exists* $0 \leq j < \binom{n+D}{n}$ *such that* $f(s_j) \neq 0$.

2 Reduction of Solvability to Systems in Few Variables

The goal of this section is to reduce testing solvability of (1) to testing solvability of several systems in k variables.

Let $V \subset \mathbb{C}^n$ be an irreducible (over $\mathbb{Q}$) component of the variety determined by (1). Observe that the algorithm described in the next Section does not need to produce V. Then $\dim V =: m \geq n - k$ and $\deg V \leq d^{n-m} \leq d^k$ due to Bezout inequality [7].

Let variables $X_{i_1}, \dots, X_{i_m}$ constitute a transcendental basis over $\mathbb{C}$ of the field $\mathbb{C}(V)$ of rational functions on V, clearly such $i_1, \dots, i_m$ do exist. Then the degree of fields extension $e := [\mathbb{C}(V) : \mathbb{C}(X_{i_1}, \dots, X_{i_m})] \leq \deg V$ equals the typical (and at the same time, the maximal) number of points in the intersections $V \cap \{X_{i_1} = c_1, \dots, X_{i_m} = c_m\}$ for different $c_1, \dots, c_m \in \mathbb{C}$, provided that this intersection being finite. Observe that for almost all vectors $(c_1, \dots, c_m) \in \mathbb{C}^n$ the intersection is finite and consists of e points.

There exists a primitive element $Y = \sum_{i \neq i_1, \dots, i_m} b_i \cdot X_i$ of the extension $\mathbb{C}(V)$ of the field $\mathbb{C}(X_{i_1}, \dots, X_{i_m})$ for appropriate integers b_i [8] (moreover, one can take integers $0 \leq b_i \leq e$ for all i, see e. g. [1], [2], but we do not need here these bounds). Moreover, there exist $n - m$ linearly over $\mathbb{C}$ independent primitive elements $Y_1, \dots, Y_{n-m}$ of this form. One can view $Y_1, \dots, Y_{n-m}, X_{i_1}, \dots, X_{i_m}$ as new coordinates.

Consider a linear projection $\pi_l : \mathbb{C}^n \to \mathbb{C}^{m+1}$ onto the coordinates $Y_l, X_{i_1}, \dots, X_{i_m}$, $1 \leq l \leq n-m$. Then the closure $\overline{\pi_l(V)} \subset \mathbb{C}^{m+1}$ is an irreducible hypersurface, so $\dim \overline{\pi_l(V)} = m$. Denote by $g_l \in \mathbb{Q}[Y_l, X_{i_1}, \dots, X_{i_m}]$ the minimal polynomial providing the equation of $\overline{\pi_l(V)}$. Then $\deg g_l = \deg \overline{\pi_l(V)} \le \deg V$ [7] and $\deg_{Y_l} g_l = e$, taking into account that Y_l is a primitive element.

Rewriting $g_l = \sum_{q \le e} Y_l^q \cdot h_q$, $h_q \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$ as a polynomial in a distinguished variable Y_l, we denote $H_l := h_e \cdot \mathrm{Disc}_{Y_l}(g_l) \in \mathbb{Q}[X_{i_1}, \dots, X_{i_m}]$, where Disc_{Y_l} denotes the discriminant with respect to the variable Y_l (the discriminant does not vanish identically since Y_l is a primitive element). We have $\deg H_l \le d^k + d^{2k}$. Consider the product $H := \prod_{1 \le l \le n-m} H_l$, then $D := \deg H \le (n-m) \cdot (d^k + d^{2k}) \le d^{3k}$.

Due to Corollary 1 there exists $0 \le j < \binom{D+m}{D} \le m^{d^{3k}}$ such that $H(s_j) = H(p_1^j, \dots, p_m^j) \neq 0$. Observe that the projective intersection $\overline{V} \cap \{X_{i_1} = p_1^j \cdot X_0, \cdots, X_{i_m} = p_m^j \cdot X_0\}$ in the projective space $\mathbb{PC}^n \supset \mathbb{C}^n$ with the coordinates $[X_0 : X_1 : \cdots : X_n]$ consists of e points, where $\overline{V}$ denotes the projective closure of V. On the other hand, coordinate Y_l of the points of the affine intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ attains e different values, taking into account that $H_l(s_j) \neq 0$, $1 \le l \le n-m$. Therefore, all e points from the projective intersection lie in the affine chart $\mathbb{C}^n$. Consequently, the intersection $V \cap \{X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j\}$ is not empty.

3 Test of Solvability and Its Complexity

Thus, to test solvability of (1) the algorithm chooses all possible subsets $\{i_1, \dots, i_m\} \subset \{1, \dots, n\}$ with $m \ge n-k$ treating $X_{i_1}, \dots, X_{i_m}$ as a candidate for a transcendental basis of some irreducible component V of the variety determined by (1). The number of these choices is bounded by $\binom{n}{m} < n^k$. After that for each $0 \le j < \binom{D+m}{D}$ where $D \le d^{3k}$, the algorithm substitutes $X_{i_1} = p_1^j, \dots, X_{i_m} = p_m^j$ into polynomials $f_1, \dots, f_k$ and solves the resulting system of polynomial equations in $n-m \le k$ variables applying the algorithm from [1], [2]. The complexity of each of these applications does not exceed a polynomial in $M \cdot \binom{D+m}{D} \cdot d^{(n-m)^2}$, i. e., a polynomial in $M \cdot n^{d^{3k}}$. Moreover, the algorithm from [1], [2] yields an algebraic numbers solution of a system, provided that it does exist, in the symbolic way as follows. The algorithm produces an irreducible over $\mathbb{Q}$ polynomial $\phi(Z) \in \mathbb{Q}[Z]$ with degree $\deg(\phi) \le d^{n-m}$ and polynomials $\phi_i(Z) \in \mathbb{Q}[Z]$, $1 \le i \le n$, $i \neq i_1, \dots, i_m$ such that for a root $\theta \in \overline{\mathbb{Q}}$ of $\phi(\theta) = 0$ the point $(x_1, \dots, x_n) \in \overline{\mathbb{Q}}^n$ with $x_{i_1} = p_1^j, \dots, x_{i_m} = p_m^j$ and $x_i = \phi_i(\theta)$, $1 \le i \le n$, $i \neq i_1, \dots, i_m$ is a solution of (1).

Summarizing, we obtain the following theorem.

Theorem 1. *One can test solvability over $\mathbb{C}$ of a system (1) of k polynomials $f_1, \dots, f_k \in \mathbb{Z}[X_1, \dots, X_n]$ with degrees d within complexity polynomial in $M \cdot \binom{n+d^{3k}}{n} \le M \cdot n^{d^{3k}}$, where M bounds the bit-sizes of (integer) coefficients of $f_1, \dots, f_k$. If (1) is solvable then the algorithm yields one of its solutions.*

Corollary 2. *For fixed d, k the complexity of the algorithm is polynomial.*

The construction and the Theorem extend literally to polynomials with coefficients from a field F of characteristic zero (for complexity bounds one needs that the elements of F are given in an efficient way). For F of a positive characteristic one can obtain similar results replacing the zero test from Section 1 by the zero test from [9].

Acknowledgements. The author is grateful to the Max-Planck Institut für Mathematik, Bonn for its hospitality during writing this paper and to Labex CEMPI (ANR-11-LABX-0007-01).

References

1. Chistov, A.: An algorithm of polynomial complexity for factoring polynomials, and determination of the components of a variety in a subexponential time. J. Soviet Math. 34, 1838–1882 (1986)
2. Grigoriev, D.: Polynomial factoring over a finite field and solving systems of algebraic equations. J. Soviet Math. 34, 1762–1803 (1986)
3. Chistov, A., Grigoriev, D.: Complexity of quantifier elimination in the theory of algebraically closed fields. In: Chytil, M.P., Koubek, V. (eds.) Mathematical Foundations of Computer Science 1984. LNCS, vol. 176, pp. 17–31. Springer, Heidelberg (1984)
4. Renegar, J.: On the computational complexity and geometry of the first-order theory of the reals. I. Introduction. Preliminaries. The geometry of semi-algebraic sets. The decision problem for the existential theory of the reals. J. Symbolic Comput. 13, 255–299 (1992)
5. Grigoriev, D., Pasechnik, D.: Polynomial-time computing over quadratic maps I. Sampling in real algebraic sets. Computational Complexity 14, 20–52 (2005)
6. Grigoriev, D., Karpinski, M.: The matching problem for bipartite graphs with polynomially bounded permanents is in NC. In: Proc. 28 Symp. Found. Comput. Sci., pp. 166–172. IEEE, New York (1987)
7. Shafarevich, I.: Foundations of algebraic geometry. MacMillan Journals (1969)
8. Lang, S.: Algebra. Springer (2002)
9. Grigoriev, D., Karpinski, M., Singer, M.: Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields. SIAM J. Comput. 19, 1059–1063 (1990)