# Bounds on Numbers of Vectors of Multiplicities for Polynomials which are Easy to Compute

Dima Grigoriev
IRMAR, Université de Rennes,
Campus de Beaulieu,
35042 Rennes, cedex France

Nicolai Vorobjov
Department of Mathematical Sciences,
University of Bath,
Bath, BA2 7AY, England

## ABSTRACT

Let $\mathbf{F}$ be an algebraically closed field of zero characteristic, a polynomial $\varphi \in \mathbf{F}[X_1, \dots, X_n]$ have a multiplicative complexity $r$ and $f_1, \dots, f_k \in \mathbf{F}[X_1, \dots, X_n]$ be some polynomials of degrees not exceeding $d$, such that $\varphi = f_1 = \cdots = f_k = 0$ has a finite number of roots. We show that the number of possible distinct vectors of multiplicities of these roots is small when $r, d$ and $k$ are small. As technical tools we design algorithms which produce Gröbner bases and vectors of multiplicities of the roots for a parametric zero-dimensional system. The complexities of these algorithms are singly exponential. We also describe an algorithm for parametric absolute factorization of multivariate polynomials. This algorithm has subexponential complexity in the case of a small (relative to the number of variables) degree of the polynomials.

## INTRODUCTION

The main aim of this paper is to prove some new features of polynomials which are easy to compute. Previously, the only known characterizations were the bounds on the sizes of polynomials vanishing on the variety of the coefficients of polynomials which are easy to compute (see [BCS 97]).

Let $\mathbf{F}$ be an algebraically closed field of characteristic zero, $\varphi \in \mathbf{F}[X_1, \dots X_n]$ be a polynomial which is easy to compute, i.e., having a multiplicative complexity $r$. Let $f_1, \dots, f_k \in \mathbf{F}[X_1, \dots, X_n]$ be some polynomials of degrees not exceeding $d$, such that the system $\varphi = f_1 = \cdots = f_k = 0$ has a finite number of roots. We show (see Corollary, Section 3) that the number of possible distinct vectors of multiplicities of these roots is less than

$$(2^r + d)^{O(n^2(r^2 + kn^d))}.$$

To prove this bound we design (Theorem 1) an algorithm having singly exponential complexity which produces a reduced Gröbner basis for a parametric zero-dimensional system of polynomial equations.

The Gröbner bases for zero-dimensional systems were intensively studied, see [B 85, CGH 89, DGFS 89, FGLM 93, Gi 89, GM 89, GH 93, K 89, KMH 89, Lak 91, Laz 81, T 78] and others. The Gröbner bases for parametric systems were considered in [W 89], without addressing the complexity issues.

In Theorem 2 an algorithm is described which, invoking Theorem 1, partitions the space of the parameters of a system of equations into constructive sets, such that under a specialization by any point from a given set, the vector of multiplicities of the roots of the system is the same (provided the system has a finite number of roots). The algorithm also finds vectors of multiplicities. The running time of the algorithm is singly exponential. We mention that in the univariate case ($n = 1$), an algorithm for parametric solving of equations (i.e., parametric computing of the $GCD$ of a family of univariate polynomials) was suggested in [G 87]. In Theorem 3 (Section 4) we describe an algorithm for parametric absolute factorization of multivariate polynomials. This algorithm has a subexponential complexity in the case of a small (relative to the number of variables) degree of the polynomials.

## 1. PARAMETRIC GRÖBNER BASIS OF A ZERO-DIMENSIONAL IDEAL

Let $F_1, \dots, F_k$ be polynomials in variables $X_1, \dots, X_n$ of degrees at most $d$ with variable pair-wise distinct coefficients $T_1, \dots, T_s$, which are considered as parameters. Thus,

$$F_i \in \mathbf{Z}[T_1, \dots, T_s][X_1, \dots, X_n],$$

where $s \le k\binom{n+d}{d} \le kn^d$. Let for a specialization of all parameters $T_1, \dots, T_s$ in algebraically closed field $\mathbf{F}$ of characteristic zero the corresponding system of equations $f_1 = \cdots = f_k = 0$ have a finite number of roots in $\mathbf{F}^n$. In [CGH 89, Lak 91] a Gröbner basis $(g_1, \dots, g_r)$ for $(f_1, \dots, f_k)$ was constructed such that $\deg(g_i) < d^{O(n)}$ (here and throughout the paper we fix a certain computable monomial ordering, for example *deglex* [BW 93]).

The aim of this section is to describe an algorithm for constructing a *parametric* Gröbner basis for $(F_1, \dots, F_k)$ and to estimate the algorithm's complexity, in particular to bound the sizes of coefficients of the Gröbner basis (which are ratio-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage, and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

*ISSAC 2000*, St. Andrews, Scotland
©2000 ACM 1-58113-218-2/ 00/ 0008 $5.00

nal functions of $T_1, \dots, T_s$). In is known (see, e.g., [W 89]) that the existing algorithms for Gröbnes basis construction (for arbitrary dimension) can be parametrized. Complexity bounds were not considered, but it is clear that straightforward bounds are doubly exponential in $n$ even in zero-dimensional case. Now we proceed to the description of the algorithm.

Fix for a time being a specialization of the parameters $T_1, \dots, T_s$ and introduce the algebra

$$\mathcal{A} = \mathbf{F}[X_1, \dots, X_n]/(f_1, \dots, f_k).$$

The dimension $\dim_{\mathbf{F}}(\mathcal{A})$ coincides with the sum of multiplicities of all roots of $f_1 = \dots = f_k = 0$ (see, e.g., [ABRW 96, Ro 99]), therefore, due to the Bézout's inequality, $\dim_{\mathbf{F}}(\mathcal{A}) \le d^n$ (see, e.g., [H 83]). Observe that for any $i$, $1 \le i \le n$ there exists a polynomial $q_i \in \mathbf{F}[X_i]$ such that $\deg(q_i) \le \dim_{\mathbf{F}}(\mathcal{A})$ and $q_i \in \sqrt{(f_1, \dots, f_k)}$. If we require $q_i$ to be monic and of the minimal possible degree, then such $q_i$ is unique. According to the Effective Nullstellensatz [FG 90] for any $i$, $1 \le i \le n$ there exist polynomials $h_j$, $1 \le j \le k$ of degrees $\deg(h_j) \le d^{O(n)}$ and $l \le d^{O(n)}$ such that

$$q_i^l = \sum_{1 \le j \le k} h_j f_j. \qquad (1)$$

Consider the following polynomials with indeterminate coefficients: monic $Q_i$, $1 \le i \le n$ in variables $X_i$ respectively; and $H_j$, $1 \le j \le k$, all in variables $X_1, \dots, X_n$, such that $\deg(Q_i) = \delta_i \le d^{O(n)}$, $\deg(H_j) = \beta \le d^{O(n)}$, where $\delta_i \ge l \deg(q_i)$, $\beta \ge \deg(h_j)$. Consider

$$Q_i = \sum_{1 \le j \le k} H_j F_j \qquad (2)$$

as a system of linear equations of the size not exceeding $d^{O(n^2)}$ in the indeterminate coefficients of $Q_i, H_j$. Observe that for any specialization of the parameters $T_1, \dots, T_s$ with $\dim((f_1, \dots, f_k)) = 0$, the linear system (2) has a root over $\mathbf{F}$. Conversely, if (2) has a root over $\mathbf{F}$ then the ideal $(f_1, \dots, f_k)$ is zero-dimensional. Applying the procedure from [H 83] (see also [CG 84, G 88, G 90]), for solving parametric systems of linear equations by Gaussian elimination, to the linear system (2), we get the constructive subset $V \subset \mathbf{F}^s$ of all parameters from $\mathbf{F}^s$ such that for any $v \in V$ the specialization of (2) by $v$ has a root in $\mathbf{F}^n$. We also get a partition of $V$ into constructive sets

$$V = \bigcup_{1 \le \alpha \le N} V_\alpha.$$

The algorithm describes each set $V_\alpha$ by a system of polynomial equations and inequations (relations with $\neq$)

$$B_1^{(\alpha)} = \dots = B_{M_\alpha}^{(\alpha)} = 0, B_{M_\alpha + 1}^{(\alpha)} \neq 0, \qquad (3)$$

where $B_j^{(\alpha)} \in \mathbf{Z}[T_1, \dots T_s]$. For each $V_\alpha$ the algorithm produces the (uniform) solution of the linear system (2) in the following form. Firstly, a *particular* solution of (2) as a vector of rational functions $\{R_{0\beta}^{(\alpha)}\}_\beta$ from $\mathbf{Q}(T_1, \dots, T_s)$; secondly a basis of solutions of the homogeneous linear system corresponding to (2), as a vector of rational functions $\{R_{\gamma,\beta}^{(\alpha)}\}_\beta$ from $\mathbf{Q}(T_1, \dots, T_s)$, where $\gamma$ ranges from 1 to the dimension of the space of the solutions of this homogeneous system.

The following bounds hold [CG 84, C 84, G 84]. The number of the constructive sets $N$ and the number of polynomials $M_\alpha$ do not exceed $d^{O(n^2 s)}$, the degrees

$$\deg(B_j^{(\alpha)}),\ \deg(R_{0\beta}^{(\alpha)}),\ \deg(R_{\gamma\beta}^{(\alpha)}) \le d^{O(n^2)}.$$

The running time of the algorithm for solving parametric system (2) does not exceed $d^{O(n^2 s)}$.

Fix $\alpha$. Abusing the notation, we denote by

$$Q_i, H_j \in \mathbf{Q}(T_1, \dots, T_s)[X_1, \dots, X_n]$$

the polynomials from (2) corresponding to the particular solution $\{R_{0\beta}^{(\alpha)}\}_\beta$. Fix for a time being a point from $V_\alpha$, denote by

$$\overline{Q}_i, \overline{H}_j, f_1, \dots, f_k \in \mathbf{F}[X_1, \dots X_n]$$

the specialization of $Q_i, H_j, F_1, \dots, F_k$ respectively, at this point. The following argument is a slight modification of the one from [CGH 89].

Take an arbitrary $f \in (f_1, \dots, f_k)$ with $\deg_{X_i}(f) \le \deg(q_i)$ for any $i$, $1 \le i \le n$; note that any polynomial from the *reduced Gröbner basis* of $(f_1, \dots, f_k)$ (see [CLO 92, BW 93]) satisfies the latter bound. Then

$$f = \sum_{1 \le j \le k} A_j f_j,$$

where $A_j \in \mathbf{F}[X_1, \dots, X_n]$. Divide each $A_j$ by the family $\overline{Q}_1, \dots, \overline{Q}_n$ with the remainder. We get

$$A_j = \sum_{1 \le i \le n} \overline{Q}_i S_{ji} + P_j,$$

where $S_{ji}, P_j \in \mathbf{F}[X_1, \dots, X_n]$, and the degrees $\deg_{X_l}(P_j) \le \delta_l$, $\deg_{X_l}(\overline{Q}_i S_{ji}) \le \deg_{X_l} A_j$, $(1 \le l \le n)$. Plugging the expression for $A_j$ in the expression for $f$ we get

$$f = \sum_{1 \le j \le k} P_j f_j + S,$$

where $S \in (\overline{Q}_1, \dots, \overline{Q}_n)$. Hence, $\deg_{X_l}(S) \le \delta_l + d \le d^{O(n)}$, $1 \le l \le n$. Dividing $S$ by the family $\overline{Q}_1, \dots, \overline{Q}_n$ with the remainder, we get $S = \sum_{1 \le i \le n} S_i \overline{Q}_i$ for some $S_i \in \mathbf{F}[X_1, \dots, X_n]$, where $\deg_{X_l}(S_i \overline{Q}_i) \le \deg_{X_l}(S) \le d^{O(n)}$, $1 \le l \le n$. Plugging this expression for $S$ in $f$, we obtain

$$f = \sum_{1 \le j \le k} P_j f_j + \sum_{1 \le i \le n} S_i \overline{Q}_i. \qquad (4)$$

For a given fixed $\alpha$ consider the following matrix $\mathcal{M}_\alpha$ of the size at most $d^{O(n)}$ with entries in $\mathbf{F}(T_1, \dots, T_s)$. The columns of $\mathcal{M}_\alpha$ correspond to all the monomials (in the descending order with respect to the chosen monomial ordering) $X_1^{m_1} \cdots X_n^{m_n}$, where $m_l \le \delta_l + d$, $1 \le l \le n$; each row of $\mathcal{M}_\alpha$ corresponds to the expansion in the basis of these monomials of either $X_1^{m_1} \cdots X_n^{m_n} F_j$ or $X_1^{m_1} \cdots X_n^{m_n} Q_i$ for all possible $i, j, m_1, \dots, m_n$ such that $m_l + \deg_{X_l}(F_j)$, $m_l + \deg_{X_l}(Q_i) \le \delta_l + d$ (cf. (4)).

Fix again a point from $V_\alpha$ and denote the corresponding specialization of $\mathcal{M}_\alpha$ by $\overline{\mathcal{M}}_\alpha$. Using elementary transformations of rows one can reduce $\overline{\mathcal{M}}_\alpha$ to a following "stairs" form $(w_{ij})_{i,j}$. Let $w_{1\mu_1} = \dots = w_{r\mu_r} = 1$ be the first non-zero elements in the rows $1, \dots, r$ respectively, where $r = \mathrm{rank}(\overline{\mathcal{M}}_\alpha)$, and $\mu_1 < \cdots < \mu_r$. We also require that $w_{i\mu_j} = 0$ for any $i < j$ $(1 \le i, j \le r)$. Let $X^{(\mu_1)}, \dots, X^{(\mu_r)}$ be the monomials corresponding to columns $\mu_1, \dots, \mu_r$ of $\overline{\mathcal{M}}_\alpha$. Choose among them all the monomials $X^{(\mu_{j_0})}$ such that $X^{(\mu_j)}$ does not divide $X^{(\mu_{j_0})}$ for all $1 \le j \le r$, $j \ne j_0$ and in addition $\deg_{X_i}(X^{(\mu_{j_0})}) \le \deg(q_i)$ for all $1 \le i \le n$. Then the set of all polynomials corresponding to rows $j$ such that $X^{(\mu_j)}$ was chosen above, constitutes the reduced Gröbner basis of $(f_1, \dots, f_k)$, taking into the account that any element of the reduced Gröbner basis is contained in the linear hull of the rows of $\overline{\mathcal{M}}_\alpha$ (see (4)).

The algorithm applies the procedure for solving parametric systems of linear equations by means of the Gaussian elimination from [H83, CG 84, G 88, G 90] to the matrix $\mathcal{M}_\alpha$ under the condition that the parameters $T_1, \dots, T_s$ satisfy (3). In the process of Gaussian elimination, a current pivot is chosen in the left-most possible column. As a result, the algorithm obtains a "stairs" form of $\mathcal{M}_\alpha$. More precisely, the algorithm outputs a partition of $V_\alpha$ into constructive sets

$$V_\alpha = \bigcup_{1 \le \nu \le N_\alpha} V_{\alpha,\nu}.$$

Each $V_{\alpha,\nu}$ is defined by a system of polynomial equations and inequations

$$B_1^{(\alpha,\nu)} = \cdots = B_{M_{\alpha,\nu}}^{(\alpha,\nu)} = 0, B_{M_{\alpha,\nu}+1}^{(\alpha,\nu)} \ne 0, \qquad (5)$$

where $B_i^{(\alpha,\nu)} \in \mathbf{Z}[T_1, \dots, T_s]$. For every $\nu$ the algorithm outputs the sequence $\mu_1^{(\nu)} < \cdots < \mu_{r_\nu}^{(\nu)}$ of the columns, such that in $\mathcal{M}_\alpha^{(\nu)} = (w_{ij}^{(\nu)})_{i,j}$ the entries $w_{i\mu_i}^{(\nu)} = 1$ $(1 \le i \le r_\nu)$ are the first non-zero elements in the rows $1, \dots, r_\nu$, where $r_\nu = \mathrm{rank}(\mathcal{M}_\alpha^{(\nu)})$. Each entry $w_{ij}^{(\nu)}$, where $j > \mu_i$ and $j \ne \mu_l$ for all $l \ne i$, is given by the algorithm as rational function from $\mathbf{Q}(T_1, \dots, T_s)$. Observe that all the rest of the entries $w_{ij}^{(\nu)}$ vanish on $V_{\alpha,\nu}$.

The following bounds hold (see [CG 84, C 84 G 84]). The number of sets $N_\alpha$ and the number of polynomials $M_{\alpha,\nu}$ do not exceed $d^{O(n^2 s)}$, the degrees $\deg(B_j^{(\alpha,\nu)})$, $\deg(w_{ij}^{(\nu)}) < d^{O(n^2)}$. The running time of reducing $\mathcal{M}_\alpha^{(\nu)}$ to "stairs" form does not exceed $d^{O(n^2 s)}$.

We summarize the results of this section in the following theorem, which uses the notations introduced previously in this Section.

Theorem 1. *There is an algorithm which for a system of parametric polynomials* $F_1, \dots, F_k \in \mathbf{Z}[T_1, \dots, T_s][X_1, \dots, X_n]$ *produces the constructive subset* $V \subset \mathbf{F}^s$ *of all points* $v$ *for which the specializations* $f_1, \dots, f_k$ *of* $F_1, \dots, F_k$ *generate zero-dimensional ideals. The algorithm produces the partition*

$$V = \bigcup_{1 \le \alpha \le N} \bigcup_{1 \le \nu \le N_\alpha} V_{\alpha,\nu}$$

*into constructive sets defined by systems (5), and for each* $V_{\alpha,\nu}$ *the algorithm outputs a family of polynomials* $G_1, \dots, G_\rho \in \mathbf{Q}(T_1, \dots, T_s)[X_1, \dots, X_n]$ *(being monic with respect to the fixed monomial ordering of* $X_1, \dots, X_n$*) such that for any point* $v \in V_{\alpha,\nu}$ *the specialization* $g_1, \dots, g_\rho \in \mathbf{F}[X_1, \dots, X_n]$ *of* $G_1, \dots, G_\rho$ *at* $v$ *is the reduced Gröbner basis for* $f_1, \dots, f_k$*. The degrees with respect to* $T_1, \dots, T_s$ *of all produced rational functions do not exceed* $d^{O(n^2)}$*, and* $\deg_{X_1, \dots, X_n}(G_i) \le d^{O(n)}$ *for* $1 \le i \le \rho < d^{O(n^2)}$*. The running time of the algorithm is less than* $d^{O(n^2 s)}$*.*

Remark 1. *Obviously the theorem remains true if* $\mathbf{F}$ *is a field with a positive characteristic, and*
$F_i \in \mathrm{GF}(p)[T_1, \dots, T_s][X_1, \dots, X_n]$ *for a prime number* $p$*.*

## 2. VECTORS OF MULTIPLICITIES FOR A PARAMETRIC SYSTEM

In what follows we adopt the notations from Theorem 1. Fix some values of indices $\alpha, \nu$. For any value of the parameters from $V_{\alpha,\nu}$ we construct in a usual way [BW 93] the monomial basis and the multiplication tables for the algebra $\mathcal{A} = \mathbf{F}[X_1, \dots, X_n]/(f_1, \dots, f_k)$, involving the Gröbner basis produced in Theorem 1. More precisely, the table represents the product of some two monomials from the basis as a linear combination of elements of the basis with the coefficients being rational functions from $\mathbf{Q}(T_1, \dots, T_s)$ of degrees not exceeding $d^{O(n^2)}$. The running time of this construction is less than $d^{O(n^2 s)}$.

Fix for a time being a specialization of the parameters $T_1, \dots, T_s$. Introduce indeterminates $U_1, \dots, U_n$. Following [ABRW 96] (see also [Ro 99]), consider the map

$$\mathcal{U}: \quad \mathcal{A} \otimes \mathbf{Q}(U_1, \dots, U_n) \longrightarrow \mathcal{A} \otimes \mathbf{Q}(U_1, \dots, U_n),$$

which is the multiplication by the linear form

$$U_1 X_1 + \cdots + U_n X_n.$$

It follows from [ABRW 96] that all the roots of the characteristic polynomial $\chi(Z)$ of $\mathcal{U}$ are of the form $\xi_1 U_1 + \cdots + \xi_n U_n$ where $(\xi_1, \dots, \xi_n)$ is a root of $f_1 = \cdots = f_k = 0$ and the multiplicities of the respective roots $\xi_1 U_1 + \cdots + \xi_n U_n$ and $(\xi_1, \dots, \xi_n)$ coincide. Note that $\deg_Z(\chi(Z)) = \dim(\mathcal{A})$. Let $\eta_i$ be the vector $(1, i, i^2, \dots, i^{n-1}) \in \mathbf{Q}^n$ for any $1 \le i \le (n-1)d^{2n}$. Consider the multiplication map $\mathcal{U}_i: \quad \mathcal{A} \longrightarrow \mathcal{A}$ by the linear form $X_1 + iX_2 + i^2 X_3 + \cdots + i^{n-1} X_n$, and the characteristic polynomial ($U$-Chow polynomial) $\chi_{\eta_i}(Z)$ of $\mathcal{U}_i$ (see [ABRW 96, Ca 89]). Then there exists the integer $i_0$, $1 \le i_0 \le (n-1)d^{2n}$, such that the inner products $\eta_{i_0} \cdot (\xi_1, \dots, \xi_n)$ are distinct for distinct roots $(\xi_1 \dots, \xi_n)$ of $f_1 = \cdots = f_k = 0$ (cf. [CG 84]).

For each $i$, $1 \le i \le (n-1)d^{2n}$ the algorithm constructs the polynomial $\chi_{\eta_i} \in \mathbf{Q}[T_1, \dots, T_s][Z]$, and computes the vector of multiplicities of its roots, as described below. The degree $\deg_{T_1, \dots, T_s}(\chi_{\eta_i})$ does not exceed $d^{O(n^2)}$ and $\chi_{\eta_i}$ can be found in time not exceeding $d^{O(n^2 s)}$. For any $j$, $1 \le j \le \deg_Z(\chi_{\eta_i})$ the algorithm, using [G 90], computes the $\mathrm{GCD}(\chi_{\eta_i}, \chi'_{\eta_i}, \dots, \chi_{\eta_i}^{(j)})$ representing it in the form

$$\Delta_l^{(i,j)} Z^l + \Delta_{l-1}^{(i,j)} Z^{l-1} + \cdots + \Delta_0^{(i,j)},$$

where $\Delta_l^{(i,j)}, \dots, \Delta_0^{(i,j)} \in \mathbf{Q}[T_1, \dots, T_s]$ are some minors of a relevant matrix, whose entries are coefficients of the polynomials $\chi_{\eta_i}, \chi'_{\eta_i}, \dots, \chi_{\eta_i}^{(j)}$ of the sizes not exceeding $d^{O(n)}$, with $\deg_{T_1,\dots,T_s}(\Delta_m^{(i,j)}) \le d^{O(n^2)}$ and $l \le \deg(\mathcal{A}) - j$. Note that the polynomials $\Delta_l^{(i,j)}, \dots, \Delta_0^{(i,j)}$ are generalizations of subresultants for the case of GCD of many polynomials (rather than just two). Observe that the degrees of $\mathrm{GCD}(\chi_{\eta_i}, \chi'_{\eta_i}, \dots, \chi_{\eta_i}^{(j)})$ for all $j$ determine the multiplicities of $\chi_{\eta_i}$.

The algorithm lists all the non-empty constructive sets $W$ of the form

$$\{\Delta_m^{(i,j)} *_{i,j,m} 0\} \subset V_{\alpha,\nu} \subset \mathbf{F}^s, \tag{6}$$

where $*_{i,j,m} \in \{=, \neq\}$, using [H 83]. The number of the sets does not exceed $d^{O(n^2 s)}$ [H 83], the running time of the listing is less than $d^{O(n^2 s)}$ [CG 83].

Each of the constructive sets $W$ determines the degrees with respect to $Z$ of $\mathrm{GCD}(\chi_{\eta_i}, \chi'_{\eta_i}, \dots, \chi_{\eta_i}^{(j)})$, and thereby the vectors of multiplicities of all $\chi_{\eta_i}$. The algorithm finds among vectors of multiplicities the one with the maximal number of components, which is the vector of multiplicities of the roots of $f_1 = \dots = f_k = 0$ for any specialization from $W$. We summarize the results of this section, using Theorem 1, in the following theorem.

THEOREM 2. *There is an algorithm, which for a system of parametric polynomials*

$$F_1, \dots, F_k \in \mathbf{Z}[T_1, \dots, T_s][X_1, \dots, X_n]$$

*produces a constructive subset $V \subset \mathbf{F}^s$ of all points $v$ for which the specializations $f_1, \dots, f_k$ of $F_1, \dots, F_k$ respectively, generate zero-dimensional ideals. The algorithm produces a partition*

$$V = \bigcup_{1 \le \alpha \le \overline{N}} W_\alpha$$

*into constructive subsets of the form (6). For every $\alpha$, $1 \le \alpha \le \overline{N}$ the vector of multiplicities of the roots is the same for a specialization $f_1 = \dots = f_k = 0$ by any point $w \in W_\alpha$. The algorithm finds such vector of multiplicities for every $W_\alpha$. The number $\overline{N}$ of sets does not exceed $d^{O(n^2 s)}$, the degrees of the polynomials defining $W_\alpha$ is less than $d^{O(n^2)}$, and the running time of the algorithm is bounded by $d^{O(n^2 s)}$*

REMARK 2. *The algorithm from the theorem can be modified to express the solutions of a parametric polynomial system via primitive element using the "Shape Lemma" (see, e.g., [KP 94, GH 93]). More precisely, the algorithm produces a partition of $W_\alpha$ into constructive sets $W_{\alpha,\nu}$. Each set $W_{\alpha,\nu}$ is equipped with a linear combination $\gamma_1 X_1 + \dots + \gamma_n X_n$ where $1 \le \gamma_i \le d^{O(n)}$ and rational functions $p_1, \dots, p_n \in \mathbf{Q}(T_1, \dots, T_s)[Z]$. Herewith, for any $v \in W_{\alpha,\nu}$ the set of all roots of the specialization $f_1 = \dots = f_k = 0$ of $F_1 = \dots = F_k = 0$ by $v$ coincides with the set of points $(p_1(v)(\theta), \dots, p_n(v)(\theta))$ where $\theta$ runs over all distinct roots of the characteristic polynomial $\chi(v)[Z]$ of the linear multiplication map by the element $\gamma_1 X_1 + \dots + \gamma_n X_n$ in the algebra $\mathcal{A}$. The number of sets $W_{\alpha,\nu}$ does not exceed $d^{O(n^2 s)}$, the degrees $\deg_Z(p_i), \deg_Z(\chi) \le d^{2n}, \deg_{T_1,\dots,T_s}(p_i)$, $\deg_{T_1,\dots,T_s}(\chi) \le d^{O(n^2)}$. The running time of the algorithm is less than $d^{O(n^2 s)}$.*

REMARK 3. *In the case when the polynomials $F_1, \dots F_k$ are homogeneous in $X_0, X_1, \dots, X_n$ one can prove a projective version of Theorem 1. Namely, the algorithm produces a partition*

$$\overline{V} = \bigcup_\alpha \overline{V}_\alpha \subset \mathbf{F}^s$$

*of the constructive set $\overline{V}$ of points in $\mathbf{F}^s$ for which the specializations $f_1 = \dots = f_k = 0$ of $F_1 = \dots = F_s = 0$ have finite numbers of roots in the projective space $\mathbf{P}^s(\mathbf{F})$. For each $\overline{V}_\alpha$ the algorithm, using [Laz 81], constructs a polynomial $R_\beta \in \mathbf{Q}[T_1, \dots, T_s, U_0, U_1, \dots, U_n]$ such that for any specialization by a point from $\overline{V}_\alpha$, the polynomial $R_\alpha$ converts to $U$-resultant of the system $f_1 = \dots = f_k = 0$. Both, the degrees of polynomials defining $\overline{V}_\alpha$ and $\deg(R_\alpha)$ do not exceed $d^{O(n)}$. The running time of the algorithm is less than $d^{O(ns)}$.*

REMARK 4. *One can also prove a projective analogue of Theorem 2. Namely, the algorithm partitions $\overline{V}$ into at most $d^{O(ns)}$ constructive sets $\overline{V}_\alpha$ such that the specializations $f_1 = \dots = f_k = 0$ of $F_1 = \dots = F_k = 0$ by all points from $\overline{V}_\alpha$ have the same vector of multiplicities of their roots. The degrees of polynomials defining $\overline{V}_\alpha$ do not exceed $d^{O(n)}$ and the running time of the algorithm is bounded by $d^{O(ns)}$.*

## 3. APPLICATION TO POLYNOMIALS WHICH ARE EASY TO COMPUTE

In this section we consider a multivariate analogue of the construction of Strassen and Schnorr (see [BCS 97]).

Fix a point $\zeta = (\zeta_1, \dots, \zeta_n) \in \mathbf{F}^n$ and introduce the algebra

$$\mathcal{B} = \mathbf{F}[X_1, \dots, X_n]/(X_1 - \zeta_1, \dots, X_n - \zeta_n)^{D+1}.$$

Consider the class $\mathcal{C}_{r,D,n}^{(\zeta)} \subset \mathcal{B}$ of the elements with multiplicative complexity not exceeding $r$. According to (a natural generalization of) the Representation Theorem of Strassen and Schnorr [BCS 97], the class $\mathcal{C}_{r,D,n}^{(\zeta)}$ can be represented as a union of $2^r$ subsets each of which is an image of a polynomial map defined by the formula

$$\Phi = \sum_{|I| \le D} \Psi_I(\Lambda)(X - \zeta)^I, \tag{7}$$

where $I$ is a multi-index, polynomials $\Psi_I \in \mathbf{F}[\Lambda_1, \dots, \Lambda_{(r+1)^2+1}]$, and the degrees $\deg(\Psi_I) \le (2r-1)|I| + 2$.

Consider the grid $\Xi = \{0, 1, \dots, 2^{2r+2}\}^n \subset \mathbf{F}^n$. Obviously, any polynomial of the degree at most $2^{2r+2}$ can't vanish at all the points from $\Xi$. Consider now the class $\mathcal{C}_{r,D,n} \subset \mathbf{F}[X_1, \dots, X_n]$ of polynomials $\phi$ such that $\deg(\phi) \le D$, and the multiplicative complexity not exceeding $r$. For an arbitrary $\phi \in \mathcal{C}_{r,D,n}$ consider a straight-line program with multiplicative complexity at most $r$ which computes $\phi$. There exists a point from $\Xi$ at which all intermediate rational functions in the program are defined (and are different from zero). Therefore,

$$\mathcal{C}_{r,D,n} \subset \bigcup_{\zeta \in \Xi} \mathcal{C}_{r,D,n}^{(\zeta)}.$$

Our aim is to estimate the number of possible distinct multiplicities vectors for the intersections of hypersurfaces $\phi = 0$, $\phi \in \mathcal{C}_{r,D,n}$ with several hypersurfaces of small degrees.

Fix a point $\zeta \in \mathbf{F}^n$. Consider a specialization $\phi \in \mathbf{F}[X_1, \dots, X_n]$ of $\Phi$ from (7) with respect to a point from $\mathbf{F}^{(r+1)^2+1}$.

In what follows we use the notations from Sections 1 and 2. One can apply the algorithms from Sections 1 and 2 to polynomials $\Phi, F_1, \dots, F_k$. We apply Theorem 2 to elements of the set $\mathcal{C}^{(\zeta)}_{r,D,n} \subset \mathcal{B}$ which are treated as the polynomials in $X_1 - \zeta_1, \dots, X_n - \zeta_n$ of degrees at most $D$.

Corollary 1. *The number of possible distinct vectors of multiplicities of the roots of any system $\phi = f_1 = \cdots = f_k = 0$, where $\phi, f_1, \dots, f_k \in \mathbf{F}[X_1, \dots, X_n]$ with $\deg(\phi) \leq D$, $\deg(f_i) \leq d$, $(1 \leq i \leq k)$, multiplicative complexity of $\phi$ at most $r$, does not exceed*

$$(D+d)^{O(n^2(r^2+k\binom{d+n}{d}))} \leq (D+d)^{O(n^2(r^2+kn^d))},$$

*provided that $\phi = f_1 = \cdots = f_k = 0$ has a finite number of roots.*

Remark 5. *Note that the number of roots of $\phi = f_1 = \cdots = f_k = 0$ does not exceed $(D+nd)^n$ according to the Bézout inequality (see [H 83]), thus the a priori number of the partitions of this number is exponential in $(D+nd)^n$, which considerably exceeds the bound from the Corollary 1 for small values of $r$ and $d$.*

Remark 6. *Obviously, $D \leq 2^r$.*

Remark 7. *In case $n = 1$ we conclude, in particular, that for each $D$ there exists a vector of multiplicities $m_1, \dots, m_l$ with $m_1 + \cdots + m_l = D$ such that the multiplicative complexity of any polynomial $(X-a_1)^{m_1} \cdots (X-a_l)^{m_l}$ for arbitrary roots $a_1, \dots, a_l$ is greater than $\Omega(\sqrt{D/\log D})$ (in fact almost all vectors of multiplicities satisfy this bound).*

Remark 8. *The bound from Corollary becomes meaningful, for example, for $d = 2$ and $r$ being polynomial in $n \log D$.*

## 4. PARAMETRIC ABSOLUTE FACTORING OF POLYNOMIALS OF SMALL DEGREE

Let $G \in \mathbf{Z}[T_1, \dots, T_s][X_1, \dots, X_n]$ be a polynomial with degrees

$$\deg_{X_1,\dots,X_n}(G) \leq d, \deg_{T_1,\dots,T_s}(G) \leq \delta,$$

and bit-sizes of integer coefficients not exceeding $L$. Here variables $T_1, \dots, T_s$ are considered as parameters. In this section we describe an algorithm for parametric factoring of $G$ over $\mathbf{F}$.

We call a vector $\beta = (\beta_1, \dots, \beta_n) \in \mathbf{Z}^n_+$ *$(d,n)$-separating* if for all vectors $j = (j_1, \dots, j_n) \in \mathbf{Z}^n_+$ such that $j_1 + \cdots + j_n \leq d$ the inner products $\beta j$ are pair-wise distinct.

Let $N = \binom{n+d}{n}^2(n-1)+1$. Then there exists a prime number $p$ such that $N < p \leq 2N$. Consider an $(N \times n)$-matrix $\mathcal{D}$ whose $(i,j)$-entry is the residue $r$, $0 \leq r \leq p-1$ of $i^j$ modulo $p$, where $1 \leq i \leq N$, $0 \leq j \leq n-1$.

Lemma 1. *At least one of the rows of the matrix $\mathcal{D}$ is $(d,n)$-separating.*

Proof. Suppose, contrary to the claim of the lemma, that for any row $\beta$ of $\mathcal{D}$ there exist two distinct vectors $j = (j_1, \dots, j_n)$, $j' = (j'_1, \dots, j'_n) \in \mathbf{Z}^n_+$ such that $j_1 + \cdots + j_n \leq d$, $j'_1 + \cdots + j'_n \leq d$ and $\beta j = \beta j'$. Observe that each $(n \times n)$-minor of $\mathcal{D}$ is non-zero being a Vandermonde determinant modulo $p$ (cf. [GKS 90]). It follows that for each pair of distinct vectors $j, j'$ as above, there exist at most $n-1$ rows $\beta$ such that $\beta j = \beta j'$. The obtained contradiction proves the lemma. □

Fix the row $\beta$ of $\mathcal{D}$ satisfying Lemma 1. Consider the $\binom{n+d}{n} \times n$-matrix $\mathcal{E}$ whose $(i,k)$-entry is $i^{\beta_k}$, where $1 \leq i \leq \binom{n+d}{n}$, $1 \leq k \leq n$.

Lemma 2. *For any polynomial $0 \not\equiv g \in \mathbf{F}[X_1, \dots, X_n]$ of the degree not exceeding $d$, there exists a row $\xi$ of $\mathcal{E}$ such that $g(\xi) \neq 0$.*

Proof. Consider the $\binom{n+d}{n} \times \binom{n+d}{n}$-matrix $\mathcal{F}$ whose $(i,j)$-entry is $i^{\beta j}$, where $1 \leq i \leq \binom{n+d}{n}$ and $j = (j_1, \dots, j_n) \in \mathbf{Z}^n_+$, $j_1 + \cdots + j_n \leq d$. Lemma now follows from the non-singularity of $\mathcal{F}$ (see [PS 64]). □

Let the polynomial $g \in \mathbf{F}[X_1, \dots, X_n]$ have the degree $d_1 \leq d$. Let $\hat{g} \in \mathbf{F}[X_1, \dots, X_n]$ be the leading homogeneous form of degree $d_1$ of $g$. For any row $\xi = (\xi_1, \dots, \xi_n)$ of $\mathcal{E}$ consider the non-singular linear transformation of the coordinates

$$X_1 \longrightarrow \xi_1 X_1, \quad X_i \longrightarrow X_i + \xi_i X_1, \qquad (7)$$

where $2 \leq i \leq n$. Applying this transformation to $g$ we obtain the polynomial $g_\xi$. Note that the coefficient at the monomial $X_1^{d_1}$ of $g_\xi$ equals to $\hat{g}(\xi_1, \dots, \xi_n)$. Then, according to Lemma 2, there exists a row $\xi$ of $\mathcal{E}$ such that the corresponding polynomial $g_\xi$ contains the monomial $X_1^{d_1}$.

We call a polynomial from $\mathbf{F}[X_1, \dots, X_n]$ *monic* (in $X_1$), if the coefficient at the highest power of $X_1$ belongs to $\mathbf{F}$. Note that $g_\xi$ is monic.

The algorithm performs the transformation (7) of $G$ for the various rows $\beta$ of the matrix $\mathcal{D}$ and the various rows $\xi$ of the matrix $\mathcal{E}$. For a fixed $\xi$ denote the result of the transformation by $G_\xi$. The algorithm partitions the space $\mathbf{F}^s$ of the parameters into the constructive sets $V$ such that all specializations $g$ of $G_\xi$ by the points from $V$ are of the same degree $d_1$ and are monic. W.l.o.g. we assume that the coefficient at $X_1^{d_2}$ of $G_\xi$ is 1 (dividing $G_\xi$ by this coefficient).

The number of sets $V$ does not exceed $\binom{n+d}{n}^{O(1)}$. Each set $V$ is defined by a system of polynomial equations and inequations of degrees at most $\delta$ in variables $T_1, \dots, T_s$. For deciding the non-emptiness of these sets, the algorithm uses the procedure from [C 84, G 84], whence the running time of the algorithm at this stage is bounded by $\left(L\delta^s\binom{n+d}{n}\right)^{O(1)}$, taking into the account that the bit-size of $\xi_j$ is bounded by $\binom{n+d}{n}^{O(1)}$.

Fix for a time being a set $V$. The algorithm reduces the absolute factorization of $G_\xi$ to the absolute factorization of a separable polynomial. Namely, note that for any specialization $g$ of $G_\xi$ (by the points from $V$), the polynomial

$g/\mathrm{GCD}(g, \partial g/\partial X_1)$ is separable. The algorithm computes the $\mathrm{GCD}(g, \partial g/\partial X_1)$ (treating $g$ as a polynomial in $X_1$) parametrically, using the subresultant algorithm [Co 67]. Namely, the algorithm constructs the minors of the Sylvester matrix for $G_\xi$ and $\partial G_\xi/\partial X_1$, and partitions the set $V$ into constructive subsets $V_{d_2}$. For each set $V_{d_2}$ the algorithm produces a polynomial $\Delta_{d_2}X_1^{d_2}+\Delta_{d_2-1}X_1^{d_2-1}+\cdots+\Delta_0$, where $\Delta_j \in \mathbf{Z}[T_1,\dots,T_s][X_2,\dots,X_n]$, $0 \le j \le d_2$. Each specialization $\Delta_{d_2}(v)$ of $\Delta_{d_2}$ by the points $v \in V_{d_2}$ is a non-zero element of $\mathbf{F}[X_1,\dots,X_n]$. The specialization $\Delta_{d_2}(v)X_1^{d_2} + \cdots + \Delta_0(v)$ coincides with the $\mathrm{GCD}(g, \partial g/\partial X_1)$ in the ring $\mathbf{F}(X_2,\dots,X_n)[X_1]$. Since $g$ is monic, the polynomial $\Delta_{d_2}(v)$ divides $\Delta_j(v)$ for all $0 \le j \le d_2 - 1$ in $\mathbf{F}[X_2,\dots X_n]$, due to the Gauss Lemma.

The algorithm computes the quotients $\Delta_j/\Delta_{d_2}$ parametrically. Namely, the coefficients of the quotients are the unique solutions of the suitable systems of linear equations with coefficients in $\mathbf{Z}[T_1,\dots,T_s]$ (provided that $v \in V_{d_2}$). As a result, the algorithm produces a monic polynomial $X_1^{d_2} + \hat{\Delta}_{d_2-1}X_1^{d_2-1} + \cdots + \hat{\Delta}_0$, where $\hat{\Delta}_j \in \mathbf{Q}(T_1,\dots,T_s)[X_2,\dots,X_n]$, $0 \le j \le d_2 - 1$. For any point $v \in V_{d_2}$ the specialization $X_1^{d_2} + \hat{\Delta}_{d_2-1}(v)X_1^{d_2-1} + \cdots + \hat{\Delta}_0(v)$ coincides with the $\mathrm{GCD}(g, \partial g/\partial X_1)$ in the ring $\mathbf{F}[X_1,\dots,X_n]$.

The algorithm computes the quotient $g/\mathrm{GCD}(g, \partial g/\partial X_1)$ parametrically (cf. computing of $\Delta_j/\Delta_{d_2}$ above). Namely, the coefficients of the quotient are unique solutions of suitable systems of linear equations with coefficients in $\mathbf{Z}[T_1,\dots,T_s]$ (provided that $v \in V_{d_2}$). Thus, the algorithm provides a polynomial

$$H = X_1^{d_1-d_2} + \Lambda_{d_1-d_2-1}X_1^{d_1-d_2-1} + \cdots + \Lambda_0,$$

where $\Lambda_j \in \mathbf{Q}(T_1,\dots,T_s)[X_2,\dots,X_n]$, $0 \le j \le d_1 - d_2 - 1$. For any point $v \in V_{d_2}$ the specialization

$$H(v) = X_1^{d_1-d_2} + \cdots + \Delta_0(v)$$

coincides with $g/\mathrm{GCD}(g, \partial g/\partial X_1)$ in the ring $\mathbf{F}[X_1,\dots,X_n]$.

We now estimate the complexity of the just described stage of the algorithm. The number of distinct sets $V_{d_2}$ does not exceed $d_1 \le d$. Each $V_{d_2}$ is defined by a system of polynomial equations and inequations of degrees not exceeding $O(\delta d)$ since the size of the Sylvester matrix involved is $O(d)$. For the same reason the degrees of $\Delta_j, \hat{\Delta}_j$ and $\Lambda_j$ with respect to $T_1,\dots,T_s$ also are bounded by $O(\delta d)$. The degrees with respect to $X_2,\dots,X_n$ of the minors of the Sylvester matrix do not exceed $O(d^2)$, and therefore, the degrees of $\Delta_j, \hat{\Delta}_j$ and $\Lambda_j$ also do not exceed $O(d^2)$. The running time of the algorithm on this stage is less than

$$\left( L(\delta d)^s \binom{n+d^2}{n} \right)^{O(1)},$$

since the non-emptiness of $V_{d_2}$ is decided using [C 84, G 84] in time $(L(\delta d)^s)^{O(1)}$. Denote by $D \in \mathbf{Q}(T_1,\dots,T_s)[X_2,\dots,X_n]$ the discriminant of the polynomial $H$ with respect to $X_1$. Recall that for any $v \in V_{d_2}$ the specialization $D(v) \in \mathbf{F}[X_2,\dots,X_n]$ of $D$ is non-zero. Observe that $\deg_{X_2,\dots,X_n}(D) \le O(n^3)$, $\deg_{T_1,\dots,T_n}(D) \le O(\delta d^2)$.

Fix for a time being a point $v \in V_{d_2}$. The algorithm computes the matrix $\mathcal{D}$, and for each row of $\mathcal{D}$ it produces the matrix $\mathcal{E}$ (as described above, see Lemmas 1, 2), replacing $d$ by $O(d^3)$ and $n$ by $n-1$ respectively. Due to Lemmas 1, 2, there exists a row $(\xi_2,\dots,\xi_n)$ in one of these matrices $\mathcal{E}$ such that $0 \ne D(v)(\xi_2,\dots,\xi_n) \in \mathbf{F}$. Denote by $\hat{H} \in \mathbf{Q}(T_1,\dots,T_s)[X_1,\dots,X_n]$ the result of the linear change of variables

$$X_2 \longrightarrow X_2 - \xi_2, \dots, X_n \longrightarrow X_n - \xi_n$$

in $H$, and by $h \in \mathbf{F}[X_1,\dots,X_n]$ the specialization $\hat{H}(v)$. Note that $h$ is monic. The discriminant of the univariate polynomial $h(X_1,0,\dots,0) \in F[X_1]$ coincides with $D(v)(\xi_2,\dots,\xi_n)$, which does not vanish.
Hence $h(X_1,0,\dots,0)$ is separable.

The algorithm partitions the set $V_{d_2}$ into constructive subsets. Each such constructive subset $W$ stems from a certain vector $(\xi_2,\dots,\xi_n)$ considered above such that for any $v \in W$ we have $D(v)(\xi_2,\dots,\xi_n) \ne 0$. As before, the algorithm makes these sets $W$ to be disjoint. The number of the sets $W$ in $V_{d_2}$ is less than $\binom{n+d}{n}^{O(1)}$. Each $W$ is defined by a system of equations and inequations of degrees $O(\delta d^2)$ with respect to $T_1,\dots,T_s$, since $D$ is the determinant of a matrix of a size of $O(d)$. The bounds on the degrees of $\hat{H}$ with respect to $T_1,\dots,T_s$ and $X_1,\dots,X_n$ are similar to the ones for $H$. The running time of the algorithm at this stage is

$$\left( L(\delta d)^s \binom{n+d^3}{n} \right)^{O(1)}.$$

Fix for a time being the set $W$ and the corresponding polynomial $\hat{H}$. Our next goal is to describe a parametric version of a quadratic Hensel lifting which we will apply below to $\hat{H}$ (see [Ga 84, GK 85, Kal 85]).

For any point $v \in W$ consider the absolute factorization $h = h_1 \cdots h_m$. The algorithm retrieves this factorization from the corresponding univariate factorization

$$h_1(X_1,0,\dots,0) \cdots h_m(X_1,0,\dots,0)$$

using the parametric Hensel lifting described below. The algorithm considers one by one all the partitions $(r_1,\dots,r_m)$ of the difference $d_1 - d_2$ for diverse $m$ i.e., $r_1 \le r_2 \le \cdots \le r_m$ and $r_1 + \cdots + r_m = d_1 - d_2$. Fix one such partition $(r_1,\dots,r_m)$.

Introduce new variables $Y_{i,j}$, where $1 \le i \le m$, $0 \le j \le r_i - 1$. The algorithm will perform the Hensel lifting of the factorization of the product

$$\hat{H}(X_1,0\dots,0) = \prod_{1 \le i \le m} \hat{H}_i(X_1), \tag{8}$$

where $\hat{H}_i(X_1) = X_1^{r_i} + Y_{i,r_i-1}X_1^{r_i-1} + \cdots + Y_{i,0}$. The result of the Hensel lifting of (8) is a product of power series

$$\hat{H} = \prod_{1 \le i \le m} \mathcal{H}_i, \tag{9}$$

where

$$\mathcal{H}_i = \sum_{|J| \ge 0} a_J^{(i)} X^J,$$

$$a_J^{(i)} \in \mathbf{Q}(T_1, \dots, T_s)(Y_{1,1}, \dots, Y_{m,r_m-1})[X_1],$$

herewith $\deg_{X_1}(a_J^{(i)}) \le r_i - 1$ for $|J| \ge 1$, $a_0^{(i)} = \hat{H}_i$, and $X^J = X_2^{j_2} \cdots X_n^{j_n}$.

We view (8) as a base of the recursion in the Hensel lifting. As a recursion hypothesis for the recursion step $l$ we assume that the algorithm had already constructed all the coefficients $a_J^{(i)}$ for $|J| \le 2^l - 1$. In particular, all $\mathcal{H}_i$ are monic.

Consider a multi-index $I$ with $2^l \le |I| \le 2^{l+1} - 1$. Then (9) yields a equation for $a_J^{(i)}$, $1 \le i \le m$ of the following form:

$$a_J^{(1)} \hat{H}_2 \cdots \hat{H}_m + a_I^{(2)} \hat{H}_1 \hat{H}_3 \cdots \hat{H}_m + a_I^{(m)} \hat{H}_1 \cdots \hat{H}_{m-1} + A = B. \tag{10}$$

Here $A = \sum a_K^{(k)} A_K^{(k)}$, $1 \le k \le m$, $K \prec I$ ($\prec$ denotes a natural partial order on the set of multi-indices), $|K| \ge 2^l$; $A_K^{(k)}$ is a polynomial of a degree at most $m-1$ in $a_J^{(i)}$ with $|J| \le 2^l - 1$; $B$ is a polynomial of a degree not exceeding $m$ in $a_J^{(i)}$ with $|J| \le 2^l - 1$, and $B$ is linear in the coefficient at $X^J$ of $\hat{H}$.

Arguing by induction, one shows that each system of the form (10) for all multi-indices $K \prec I$ has the unique solution in $a_K^{(k)}$, $1 \le k \le m$ under the condition $\deg_{X_1}(a_K^{(k)}) \le r_i - 1$. Therefore, the degrees of $A$ and $B$ with respect to $X_1$ do not exceed $d_1 - d_2 - 1$. It follows that there exist unique $a_I^{(1)}, \dots, a_I^{(m)}$ satisfying (10) such that $\deg_{X_1}(a_I^{(i)}) \le r_i - 1$, $1 \le i \le m$.

The algorithm solves recursively systems of the form (10) according to increasing multi-indices with respect to the partial order $\prec$ and finds the solutions $a_I^{(i)}$, $1 \le i \le m$. The Hensel lifting terminates when $2^{l+1}$ exceeds $\deg_{X_2, \dots, X_n}(\hat{H}) \le O(d^2)$ (see above).

Introduce the truncated power series

$$\hat{\mathcal{H}}_i = \sum_{0 \le |J| \le 2^{l+1}-1} a_J^{(i)} X^J \in$$

$$\mathbf{Q}(T_1, \dots T_s)(Y_{1,1}, \dots, Y_{m,r_m-1})[X_1, \dots, X_n].$$

The algorithm should verify the equality

$$\hat{H} = \prod_{1 \le i \le m} \hat{\mathcal{H}}_i. \tag{11}$$

More precisely, using quantifier elimination [CG 84], the algorithm finds the constructive subset $W_{r_1, \dots, r_m} \subset W$ of all the points $v \in W$ such that there exist $y_{1,1}, \dots, y_{m,r_m-1} \in \mathbf{F}$ with the specialization of (11) by $v$ and $y_{1,1}, \dots, y_{m,r_m-1}$ is true.

Order all the partitions $(r_1, \dots, r_m)$ in an arbitrary order consistent with the decrease of $m$. The algorithm follows this ordering and replaces each next $W_{r_1, \dots, r_m}$ by subtracting from it the union of $W_{r'_1, \dots, r'_m}$ for all previous partitions $(r'_1, \dots, r'_m)$ in the ordering. These new constructive sets constitute a partition of $W$, we keep for them the same notations $W_{r_1, \dots, r_m}$.

Fix for a time being a set $W_{r_1, \dots, r_m}$. Observe that for any $v \in W_{r_1, \dots, r_m}$ the specialization of the equations (11) by $v$ and every $y_{1,1}, \dots, y_{m,r_m-1}$ satisfying (11) is the absolute factorization of $\hat{H}(v) = h$.

Recall that for any point $v \in W_{r_1, \dots, r_m}$ there exist $\kappa_1, \dots, \kappa_m \in \mathbf{Z}_+$ such that

$$g(X_1, X_2 + \xi_2, \dots, X_n + \xi_n) = \prod_{1 \le i \le m} \left(\hat{\mathcal{H}}_i(v)\right)^{\kappa_i}. \tag{12}$$

The algorithm looks over all possible vectors $(\kappa_1, \dots, \kappa_m) \in \mathbf{Z}_+^m$ such that $\kappa_1 + \cdots + \kappa_m = d_1$. For each vector $(\kappa_1, \dots, \kappa_m)$ the algorithm produces and tests non-emptiness of the constructive set $W^{(\kappa_1, \dots, \kappa_m)} \subset W_{r_1, \dots, r_m}$ of points $v \in W_{r_1, \dots, r_m}$ for which there exist the elements $y_{1,1}, \dots, y_{m,r_m-1} \in \mathbf{F}$ such that (12) holds, and also represents these elements as described in the paragraph. Observe that the sets $W^{(\kappa_1, \dots, \kappa_m)}$ form a partition of $W_{r_1, \dots, r_m}$, and for each $v \in W^{(\kappa_1, \dots, \kappa_m)}$ there is a finite set of the solutions $y_{1,1}, \dots, y_{m,r_m-1}$, due to the Gauss Lemma. The algorithms applies to the system of equations (12) the procedure from Theorems 1, 2 and the Remark 2. As a result, a parametric Gröbner basis for (12) will be computed (see Theorem 1), as well as the vectors of multiplicities (see Theorem 2) of the roots of (12). The algorithm produces a partition of the set $W^{(\kappa_1, \dots, \kappa_m)}$. Fix for a time being an element $U$ of the partition. The algorithm produces a primitive element $\gamma_{1,1} Y_{1,1} + \cdots + \gamma_{m,r_m-1} Y_{m,r_m-1}$, rational functions $p_{1,1}, \dots, p_{m,r_m-1} \in \mathbf{Q}(T_1, \dots T_s)[Z]$, and the characteristic polynomial $\chi \in \mathbf{Q}(T_1, \dots, T_s)[Z]$ of the linear multiplication map by the primitive element in the algebra $\mathcal{A}$, such that for any $v \in U$ the specializations $p_{1,1}(v)(\theta), \dots, p_{m,r_m-1}(v)(\theta)$ run over all solutions $y_{1,1}, \dots, y_{m,r_m-1}$ of (12) when $\theta$ runs over all roots of the polynomial $\chi(v)(Z)$.

Now we estimate the complexity of the algorithm. The algorithm looks through all $2^{O(d)}$ partitions $(r_1, \dots, r_m)$ of the difference $d_1 - d_2$. Then the algorithm, recursively on $l$, for each multi-index $J$ such that $|J| = 2^{l+1} - 1$ solves the union of the linear systems of the form (10) for all $I \preceq J$ and $|I| \ge 2^l$. The sizes of the matrices of systems (10) do not exceed $\left(2^{2^l} d\right)^{O(1)}$. For $J$ such that $|J| \le 2^{l+1} - 1$ the degrees

$$\deg_{T_1, \dots, T_s}(a_J^{(i)}) \le \left(2^{2^l} d^l \delta\right)^{O(1)},$$

$$\deg_{Y_{1,1}, \dots, Y_{m,r_m-1}}(a_J^{(i)}) \le \left(2^{2^l} d^l\right)^{O(1)}.$$

Therefore,

$$\deg_{T_1, \dots, T_s}(\hat{\mathcal{H}}_i) \le (2^d \delta)^{O(1)},$$

$$\deg_{Y_{1,1}, \dots, Y_{m,r_m-1}}(\hat{\mathcal{H}}_i) \le 2^{O(d)},$$

where $1 \le i \le m$. The running time of the Hensel lifting of $\hat{\mathcal{H}}_i$ does not exceed $\left(L\delta^s 2^{ds} 2^{d^2} \binom{n+d^2}{n}\right)^{O(1)}$.

Then the algorithm applies quantifier elimination to (11) and produces constructive subsets $W_{r_1, \dots, r_m}$. The number of sets is less than $(2^{d^2}\delta)^{O(s)}$. Each subset is defined by a system of polynomial equations and inequations of degrees at most $(2^{d^2}\delta)^{O(1)}$. The running time of this application of quantifier elimination does not exceed $\left(L\delta^s 2^{d^2 s} \binom{n+d^2}{n}\right)^{O(1)}$.

After that the algorithm applies the machinery from Sections 1, 2 to the system (12), and produces the constructive sets $U$ and the representations of the solutions $y_{1,1}, \dots, y_{m,r_m-1}$ via $\gamma_{1,1}Y_{1,1} + \cdots + \gamma_{m,r_m-1}Y_{m,r_m-1}$, the characteristic polynomial $\chi$, and the rational functions $p_{1,1}, \dots, p_{m,r_m-1}$. The number of sets $U$ does not exceed $2^{O(d^3 s)}$. Each set $U$ is defined by a system of polynomial equations and inequations of degrees not exceeding $(\delta 2^{d^3})^{O(1)}$. The degrees of rational functions

$$\deg_{T_1,\dots,T_s}(p_{i,j}),\ \deg_{T_1,\dots,T_s}(\chi) \le (\delta 2^{d^3})^{O(1)},$$

$$\deg_Z(\chi),\ \deg_Z(p_{i,j}) \le 2^{O(d^3)},$$

where $1 \le i \le m$, $1 \le j \le r_m - 1$. The running time of this stage of the algorithm is less than $\left(L\delta^s 2^{d^3 s}\binom{n+d^2}{n}\right)^{O(1)}$.

We summarise the results of this section in the following theorem, using the notations from the beginning of this section.

Theorem 3. *There is an algorithm which for a parametric polynomial $G \in \mathbf{Z}[T_1, \dots, T_s][X_1, \dots, X_n]$ produces the partition of $\mathbf{F}^s$ into the constructive sets. For each of these sets $U$ the algorithm outputs a family of polynomials*

$$G_1, \dots, G_m \in \mathbf{Q}(T_1, \dots, T_s)[Z][X_1, \dots, X_n],$$

*the vector of exponents $(\kappa_1, \dots, \kappa_m) \in \mathbf{Z}_+^m$, and a polynomial $\chi \in \mathbf{Q}(T_1, \dots, T_s)[Z]$.*

*For any point $v \in U$ and each root $\theta$ of the specialization $\chi(v)$ of $\chi$ by $v$ the absolute factorization of the specialization $G(v)$ of $G$ by $v$ is given by the formula*

$$G(v) = \prod_{1 \le i \le m} (G_i(v)(\theta))^{\kappa_i},$$

*moreover, every polynomial $G_i(v)(\theta) \in \mathbf{F}[X_1, \dots, X_n]$ is separable, $1 \le i \le m$. Herewith, the number of elements $U$ of the partition is less than $\left(2^{d^3 s}\binom{n+d}{n}\right)^{O(1)}$, each $U$ is defined by a system of polynomial equations and inequations of degrees not exceeding $(\delta 2^{d^3})^{O(1)}$. The degrees*

$$\deg_Z(G_i),\ \deg_Z(\chi) \le 2^{O(d^3)},$$

$$\deg_{T_1,\dots,T_s}(G_i),\ \deg_{T_1,\dots,T_s}(\chi) \le (\delta 2^{d^3})^{O(1)},$$

*where $1 \le i \le m$.*

*The running time of the algorithm is less than*

$$\left(L\delta^s 2^{d^3 s}\binom{n+d^3}{n}\right)^{O(1)}.$$

Remark 9. *The diverse roots $\theta$ of $\chi(v)$ correspond to permutations of the factors $G_i(v)$ (with some values of the exponents $\kappa_i$) in the absolute factorization.*

Remark 10. *The complexity of the algorithm described in Theorem 3, for $\delta$, $s$ and $d$ considerably less than $n$, is of the magnitude $n^{d^3}$, being subexponential in the size of the input $n^d$.*

Remark 11. *Since the number of possible vectors of degrees $\deg_{X_1,\dots,X_n}(G_i)$ and the exponents $\kappa_i$ in the absolute factorization could be exponential in $d$, the complexity is necessarily exponential in $d$.*

## 5. FURTHER RESEARCH

1. Theorem 2 provides an algorithm for solving parametric systems of polynomial equations, having finite number of roots, which also computes the multiplicities of the roots. In [C 84, G 84] an algorithm was constructed for finding irreducible components of polynomial systems in singly exponential time. It would be interesting to design an algorithm with singly exponential complexity for finding absolutely irreducible components of parametric polynomial systems.

2. In the Corollary 1 the number of possible vectors of multiplicities of roots of a system of polynomials which are easy to compute was bounded. A difficult problem is to describe explicitly the set of all realisable vectors of multiplicities, or at least to indicate a concrete vector not contained in this set. This might shed a light on algebraic complexity lower bounds problem.

## ACKNOWLEDGEMENTS

Authors would like to acknowledge the support of EPSRC visiting fellowship grant GR/M12308. The first author thanks the Department of Mathematical Sciences of the University of Bath which he had been visiting during the work on the paper. The second author was also partly supported by EPSRC grant GR/L77928.

## REFERENCES

[ABRW 96] Alonso, M., Becker, E., Roy, M.-F., Wörmann, T., Zeros, multiplicities and idempotents for zero-dimensional systems, *Algorithms in Algebraic Geometry and Applications. Progress in Math.,* 143, 1996, 1–20.

[BW 93] Becker, T., Weispfenning, V., *Gröbner Bases,* Springer-Verlag, New-York, 1993.

[B 85] Buchberger, B., Gröbner bases: An algorithmic method in polynomial ideal theory. In: Bose, N.K. (Ed.), *Multidimensional Systems Theory,* Reidel, Dordrecht, 1985, 184–232.

[BCS 97] Bürgisser, P., Clausen, M., Shokrollahi, M.A., *Algebraic Complexity Theory,* Berlin: Springer-Verlag, 1997.

[CGH 89] Caniglia, L., Galligo, A., Heintz, J., Some new effectivity bounds in computational geometry, *Lecture Notes Comp. Sci.,* 357, 1989, 131–151.

[Ca 89] Canny, J., Generalized characteristic polynomials, *Lecture Notes Comp. Sci.,* 358, 1989, 293–299.

[C 84] Chistov, A., Algorithm of polynomial complexity for factoring polynomials and finding the components of the varieties in subexponential time, In: *Zapiski Nauchnyh Seminarov LOMI,* 137, 1984, 124–188. English translation in: *J. Soviet Math.,* 34, 1838–1882.

[CG 84] Chistov, A., Grigoriev, D., Complexity of quantifier elimination in the theory of algebraically closed fields, *Lecture Notes Comp. Sci.,* 176, 1984, 17–31.

[Co 67] Collins, G.E., Subresultants and reduced polynomial reminder sequences, *J. ACM,* 14, 1967, 128–142.

[DGFS 89] Dickenstein, A., Giusti, M., Fitchas, N., Sessa, C., The membership problem for unmixed polynomial ideals is solvable in single exponential time, Proceedings 7th Intern. Conf. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes AAECC-7, Discrete Appl. Math., 33, 1989, 73–94.

[FGLM 93] Faugère, J.C., Gianni, P., Lazard, D., Mora, T., Efficient computation of zero-dimensional Gröbner bases by change of ordering, *J. Symbolic Computation,* 16, 1993, 329–344.

[FG 90] Fitchas, N., Galligo, A., Nullstellensatz effectif et conjacture de Serre (théorème de Quillen-Suslin) pour le calcul formel, *Math. Nachrichten,* 149, 1990, 231–253.

[Ga 84] Gathen, von zur., Hensel and Newton methods in valuation rings, *Math. Comp.,* 42, 1984, 637–661.

[GK 85] Gathen, von zur J., Kaltofen, E., Factoring sparse multivariate polynomials, *J. Comput. System Sci.,* 31, 1985.

[Gi 89] Gianni, P., Properties of Gröbner bases under specializations, *Lecture Notes Comp. Sci.,* 378, 1989, 293–297.

[GM 89] Gianni, P., Mora, T., Algebraic solution of systems of polynomial equations using Groebner bases, *Lecture Notes Comp. Sci.,* 356, 1989, 247–257.

[GH 93] Giusti, M., Heintz, J., La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial, Computational Algebraic Geometry and Commutative Algebra. Symposia Mathematica, 34, 1993, 216–256.

[G 84] Grigoriev, D., Factorization of polynomials over finite field and the solution of systems of algebraic equations, In: *Zapiski Nauchnyh Seminarov LOMI,* 137, 1984, 20–79. English translation in: *J. Soviet Math.,* 34, 1762–1803..

[G 86] Grigoriev, D., Complexity of deciding the first–order theory of algebraically closed fields, *Izvestia of Academy of Sciences of the USSR,* 50, 1986, 1106–1120 (in Russian, English translation in *Math. USSR Izvestia,* 29, 1987, 459–475).

[G 87] Grigoriev, D., Complexity of quantifier elimination in the theory of ordinary differential equations, *Lecture Notes in Computer Sci.,* 378, 1987, 11–25.

[G 88] Grigoriev, D., Complexity of deciding Tarski algebra. *J. Symbolic Comput.,* 5, 1988, 65–108.

[G 90] Grigoriev, D., Complexity of factoring and GCD calculating of ordinary linear differential operators, *J. Symbolic Comput.,* 10, 1990, 7–37.

[GKS 90] Grigoriev, D., Karpinski, M., Singer, M., Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields, *SIAM J. Comput.,* 19, 1990, 1059–1063.

[H 83] Heintz, J., Definability and fast quantifier elimination in algebraically closed fields, *Theor. Comput. Sci.,* 24, 1983, 239–277.

[K 89] Kalkbrener, M., Solving systems of algebraic equations by using Gröbner bases, *Lecture Notes Comp. Sci.,* 378, 1989, 282–292.

[Kal 85] Kaltofen, E., Sparse Hensel lifting, *Lecture Notes Comp. Sci.,* 204, 1985, 4–17.

[KMH 89] Kobayashi, H., Moritsugu, S., Hogan, R.W., Solving systems of algebraic equations, *Lecture Notes Comp. Sci.,* 358, 1989, 139–149.

[KP 94] Krick,T., Pardo, L.M., Une approche informatique pour l'approximation diophantienne, *C.R. Acad. Sci. Paris, Série I,* 318, 1994, 407–412.

[Lak 91] Lakshman, Y.N., A single exponential bound on the complexity of computing Gröbner bases of zero dimensional ideals, *Effective methods in algebraic geometry,* Progress in Mathematics, 94, Birkhäuser Verlag, Basel, 1991, 227–234.

[Laz 81] Lazard, D., Resolution des systemes d'equations algebriques, *Theoretical Computer Science,* 15, 1981, 77–110.

[PS 64] Pólya, G., Szegö, G., Aufgaben und Lehrsätze aus der Analysis, Springer-Verlag, Berlin, 1964.

[Ro 99] Rouillier, F., Solving zero-dimensional systems through rational univariate representations, *Applic. Algebra in Eng. Commun. Computing*, 9, 1999, 433-461.

[T 78] Trinks, W., Über Buchbergers Verfahren, Systeme algebraisher Gleichungen zu lösen, *J. Number Th.,* 10, 1978, 475–488.

[W 89] Weispfenning, V., Constructing universal Groebner bases, *Lecture Notes Comp. Sci.,* 356, 1989, 408–417.