DOI 10.1007/s10958-017-3422-4
Journal of Mathematical Sciences, Vol. 224, No. 2, July, 2017

EFFICIENT ABSOLUTE FACTORIZATION OF POLYNOMIALS WITH PARAMETRIC COEFFICIENTS

A. L. Chistov* UDC 513.6, 518.5

Consider a polynomial with parametric coefficients. We show that the variety of parameters can be represented as a union of strata. For values of the parameters from each stratum, the decomposition of this polynomial into absolutely irreducible factors is given by algebraic formulas depending only on the stratum. Each stratum is a quasiprojective algebraic variety. This variety and the corresponding output are given by polynomials of degrees at most D with $D = d'd^{O(1)}$ where d', d are bounds on the degrees of the input polynomials. The number of strata is polynomial in the size of the input data. Thus, here we avoid double exponential upper bounds for the degrees and solve a long-standing problem. Bibliography: 4 titles.

Introduction

Let k be an arbitrary field containing at least $2d^2+1$ pairwise distinct elements (d is specified below, see (1)). Let p be the characteristic exponent of the field k, i.e., $p = 1$ if $\mathrm{char}(k) = 0$ and $p = \mathrm{char}(k)$ if $\mathrm{char}(k) > 0$. Let $a_1, \dots, a_\nu$ 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 $a_1, \dots, a_\nu$ (in a more general situation, one may consider an algebraic variety of parameters $\mathcal{V} \subset \mathbb{A}^\nu(\overline{k})$, but this case is easily reduced to the particular one when $\mathcal{V} = \mathbb{A}^\nu(\overline{k})$).

Let $f \in k[a_1, \dots, a_\nu, X_1, \dots, X_n]$ be a polynomial and

$$\deg_{X_1,\dots,X_n} f \le d, \quad \deg_{a_1,\dots,a_\nu} f \le d' \tag{1}$$

for some integers $d \ge 2$ and $d' \ge 2$. In the present paper, we consider the problem of representing the space of parameters

$$\mathbb{A}^\nu(\overline{k}) = \bigcup_{\alpha\in A} \mathcal{W}_\alpha \tag{2}$$

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 $a^* = (a_1^*, \dots, a_\nu^*) \in \mathcal{W}_\alpha$ there is a decomposition

$$f(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n) = \lambda_{a^*} \prod_{\gamma\in\Gamma_\alpha} F_{\gamma,a^*}^{e_\gamma}(X_1^{p^{i_\gamma}}, \dots, X_n^{p^{i_\gamma}}), \tag{3}$$

where $F_{\gamma,a^*} \in \overline{k}[X_1, \dots, X_n]$ are polynomials irreducible over the field $\overline{k}$, $\lambda_{a^*} \in k$, $1 \le e_\gamma \in \mathbb{Z}$, $0 \le i_\gamma \in \mathbb{Z}$, $\#\Gamma_\alpha < +\infty$. The decomposition (3) is given uniformly, i.e., by some algebraic formulas (see below for details) defined everywhere on $\mathcal{W}_\alpha$ and depending on $a_1^*, \dots, a_\nu^*$ as parameters. Note that all the integers e_γ, i_γ and the set of indices Γ_α do not depend on $a^* \in \mathcal{W}_\alpha$.

Now we are going to give a precise meaning to this uniformity. Namely, the decomposition (2) satisfies the following properties.

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

*St.Petersburg Department of Steklov Institute of Mathematics, St.Petersburg, Russia, e-mail: alch@pdmi.ras.ru.

Translated from *Zapiski Nauchnykh Seminarov POMI*, Vol. 448, 2016, pp. 286–325. Original article submitted October 3, 2016.

(ii) One can represent $\mathcal{W}_\alpha$ in the form

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

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

For every $\alpha \in A$, denote by $\overline{\mathcal{W}}_\alpha$ the closure with respect to the Zariski topology of the algebraic variety $\mathcal{W}_\alpha$ in $\mathbb{A}^\nu(\overline{k})$. Denote by $\mathcal{I}_\alpha$ the ideal of the affine algebraic variety $\overline{\mathcal{W}}_\alpha$.

(iii) There are a set of indices J_α, polynomials $\lambda_{\alpha,0}, \lambda_{\alpha,1} \in k[a_1, \ldots, a_\nu]$, polynomials $f_j \in k[a_1, \ldots, a_\nu, X_1, \ldots, X_n]$, integers e_j relatively prime to p, integers $i_j \ge 0$ for all $j \in J_\alpha$ such that each of the polynomials $\lambda_{\alpha,0}, \lambda_{\alpha,1}$ does not vanish at any point of the algebraic variety $\mathcal{W}_\alpha$,

$$f = \frac{\lambda_{\alpha,1}}{\lambda_{\alpha,0}} \prod_{j \in J_\alpha} f_j^{e_j}(a_1, \ldots, a_\nu, X_1^{p^{i_j}}, \ldots, X_n^{p^{i_j}}) \tag{4}$$

on the algebraic variety $\overline{\mathcal{W}}_\alpha$ (this means that

$$\lambda_{\alpha,0} f - \lambda_{\alpha,1} \prod_{j \in J_\alpha} f_j^{e_j}(a_1, \ldots, a_\nu, X_1^{p^{i_j}}, \ldots, X_n^{p^{i_j}}) \in \mathcal{I}_\alpha \otimes_{\overline{k}} \overline{k}[X_1, \ldots, X_n])$$

and $J_{\alpha_1} \cap J_{\alpha_2} = \varnothing$ for $\alpha_1 \ne \alpha_2$. Besides, if $p = 1$ then $i_j = 0$ for every $j \in J_\alpha$.

(iv) For every $i = -1, 0$ there is at most one $\alpha \in A$ such that $\deg f_j = i$ for some $j \in J_\alpha$. In this case, $\# J_\alpha = 1$, $e_j = 1$, and $\lambda_{\alpha,0} = \lambda_{\alpha,1} = 1$, and if $i = -1$ then $f_j = 0$, if $i = 0$ then $0 \ne f_j = f(a_1, \ldots, a_\nu, 0, \ldots, 0) \in k[a_1, \ldots, a_\nu]$.

(v) For every $\alpha \in A$, for every $j \in J_\alpha$, for every $a^* \in \mathcal{W}_\alpha$,

$$\deg_{X_1, \ldots, X_n} f_j(a_1^*, \ldots, a_\nu^*, X_1, \ldots, X_n) = \deg_{X_1, \ldots, X_n} f_j.$$

If $\deg_{X_1, \ldots, X_n} f_j \ge 0$, then the polynomial $f_j(a_1^*, \ldots, a_\nu^*, X_1, \ldots, X_n)$ is separable (i.e., does not have multiple factors in $\overline{k}[X_1, \ldots, X_n]$). For all pairwise distinct $j_1, j_2 \in J_\alpha$, the polynomials $f_{j_1}(a_1^*, \ldots, a_\nu^*, X_1, \ldots, X_n)$ and $f_{j_2}(a_1^*, \ldots, a_\nu^*, X_1, \ldots, X_n)$ are relatively prime in the ring $\overline{k}[X_1, \ldots, X_n]$.

Denote by A' the subset of $\alpha \in A$ such that $\deg f_j \ge 1$ for all $j \in J_\alpha$. For all $\alpha \in A'$, $j \in J_\alpha$ there is a polynomial $H_j \in k[a_1, \ldots, a_\nu][Z]$ satisfying the following properties.

(vi) Let $\alpha \in A'$, $j \in J_\alpha$. Denote by $\Delta_j \in k[a_1, \ldots, a_\nu]$ the discriminant of the polynomial H_j with respect to Z. Then Δ_j does not vanish at any point of the algebraic variety $\mathcal{W}_\alpha$.

Under the conditions of (vi), for every $a^* \in \mathcal{W}_\alpha$ denote by Ξ_{j,a^*} the set of all roots of the polynomial $H_{\alpha,j}(a_1^*, \ldots, a_\nu^*, Z) \in \overline{k}[Z]$. Then by (vi) for every $a^* \in \mathcal{W}_\alpha$ the number of roots $\#\Xi_{j,a^*}$ is equal to $\deg_Z H_j$ and the leading coefficient $\mathrm{lc}_Z H_j$ does not vanish at any such point a^*.

(vii) Let $\alpha \in A'$, $j \in J_\alpha$. Then there is a polynomial $F_j \in k[a_1, \ldots, a_\nu, Z, X_1, \ldots, X_n]$ such that for every $a^* \in \mathcal{W}_\alpha$, for every root $\xi \in \Xi_{j,a^*}$, the polynomial

$$F_j(a_1^*, \ldots, a_\nu^*, \xi, X_1, \ldots, X_n)$$

is irreducible in $\overline{k}[X_1, \ldots, X_n]$ (i.e., absolutely irreducible) and $0 \le \deg_Z F_j < \deg_Z H_j$,

$$\deg_{X_1, \ldots, X_n} F_j(a_1^*, \ldots, a_\nu^*, \xi, X_1, \ldots, X_n) = \deg_{X_1, \ldots, X_n} F_j.$$

(viii) Let $\alpha \in A'$, $j \in J_\alpha$. Then

$$f_j(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n) = \prod_{\xi \in \Xi_{j,a^*}} F_j(a_1^*, \dots, a_\nu^*, \xi, X_1, \dots, X_n) \tag{5}$$

and hence (5) is a decomposition of the separable polynomial $f_j(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n)$ into a product of pairwise distinct absolutely irreducible factors. Hence the degree $\deg_Z H_j = \#\Xi_{j,a^*}$ is bounded from above by d.

Now we are able to formulate our main result.

Theorem 1. *Let $f \in k[a_1, \dots, a_\nu, X_1, \dots, X_n]$ be as above. Then there is a stratification $\{\mathcal{W}_\alpha\}_{\alpha \in A}$ of the space of parameters $\mathbb{A}^\nu(\overline{k})$ satisfying properties* (i)–(viii) *and such that*

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

(b) *the degrees with respect to $a_1, \dots, a_\nu$ of all the polynomials $\psi_{\alpha,1}^{(\beta)}, \dots, \psi_{\alpha,m_{\alpha,\beta}}^{(\beta)}$, $\lambda_{\alpha,0}, \lambda_{\alpha,1}$, H_j, F_j, f_j are bounded from above by $d' d^{O(1)}$ with an absolute constant in $O(1)$.*

The proof of this theorem is based on [1, 2]. One can also consider the case of a covering (rather than a stratification) of the space of parameters (i.e., in this case (i) does not necessarily hold). *If in the statement of Theorem* 1 *one replaces* "(i)–(viii)" *by* "(ii)–(viii)," *then one can claim additionally that $\mu_\alpha = 2$ for every $\alpha \in A$.*

Remark 1. Let $d \geq -1$ be an integer. According to [1], we identify the set of polynomials from $\overline{k}[X_1, \dots, X_n]$ of degree at most d with $\overline{k}^{N(n,d)}$ where $N(n,d) = \binom{n+d}{n}$. Denote by $P_{n,d} \subset \overline{k}^{N(n,d)}$ the subset of polynomials from $\overline{k}[X_1, \dots, X_n]$ of degree d. In [1], we introduced the function $\mathrm{RDP}_{X_1,\dots,X_n} : \bigcup\limits_{d \geq 0} \overline{k}^{N(n,d)} \to \bigcup\limits_{d \geq 0} P_{n,d}$ corresponding to some computation forest. Namely, if $g \in \overline{k}^{N(n,d)}$, then $\mathrm{RDP}_{X_1,\dots,X_n}(g) \in P_{n,d'}$ where $d' = \deg_{X_1,\dots,X_n} g$ is the degree of g and $g = \mathrm{RDP}_{X_1,\dots,X_n}(g)$ in $\overline{k}[X_1, \dots, X_n]$. Throughout this paper, we sometimes apply the function $\mathrm{RDP}_{X_1,\dots,X_n}$ (or a similar function with other variables in place of $X_1, \dots, X_n$) without mentioning it. This will not lead to an ambiguity. The function $\mathrm{RDP}_{X_1,\dots,X_n}$ is used when one needs to know the exact degrees of the polynomials under consideration.

1. The noether normalization of a polynomial

Let k be a field. Let $f \in k[X_1, \dots, X_n]$ be a nonzero polynomial and $\deg_{X_1,\dots,X_n} f = d$ for an integer $d \geq 0$. Then one can represent f in the form

$$f = \sum_{\substack{i_1,\dots,i_n \geq 0 \\ i_1+\dots+i_n \leq d}} f_{i_1,\dots,i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n},$$

where all the coefficients $f_{i_1,\dots,i_n}$ are in k.

Put $K_0 = k_0 = \mathbb{Z}$ if the characteristic $\mathrm{char}(k)$ is zero. If $\mathrm{char}(k) = p > 0$, then put $k_0 = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ to be the primitive field. Further, let us define K_0 to be some ring such that $k_0 \subset K_0 \subset k$ and K_0 contains at least $2d^2 + 1$ elements. The ring K_0 exists since $\#k \geq 2d^2 + 1$, see the introduction. In what follows, we will need to choose finite sets with sufficiently many elements from the field k. We will choose them from the ring K_0.

Let $\mathcal{J}_d \subset K_0$ be a subset containing exactly $d + 1$ elements. We choose and fix this subset $\mathcal{J}_d$. In the case $\mathrm{char}(k) = 0$, put $\mathcal{J}_d = \{0, 1, \dots, d\} \subset \mathbb{Z}$. Additionally, we will assume without loss of generality that $\mathcal{J}_d$ is well-ordered.

Let $j_2, \dots, j_n \in \mathcal{J}_d$. Put

$$f^{(j_2,\dots,j_n)} = f(X_1, X_2 + j_2X_1 \dots, X_n + j_nX_1) \in k[X_1, \dots, X_n].$$

Let us order the set of multiindices $(j_2, \dots, j_n) \in \mathcal{J}_d^{n-1}$ lexicographically: $(j_2, \dots, j_n) < (j_2', \dots, j_n')$ if and only if there is an integer α with $2 \le \alpha \le n$ such that $j_v = j_v'$ for $2 \le v < \alpha$ but $j_\alpha < j_\alpha'$. Denote by $\mathcal{J}_{n,d}$ the set of all multiindices $(j_2, \dots, j_n) \in \mathcal{J}_d^{n-1}$ such that $j_\alpha \in \mathcal{J}_d$ for $2 \le \alpha \le n$. Then $\mathcal{J}_{n,d}$ is linearly ordered and $\#\mathcal{J}_{n,d} = (d+1)^{n-1}$.

Let $f = \varphi_0 + \varphi_1 + \dots + \varphi_d$ where $\varphi_i \in k[X_1, \dots, X_n]$ is a homogeneous polynomial of degree i.

Put $\mathrm{NN}_{X_1}(f; X_1, \dots, X_n) = f^{(\iota_2,\dots,\iota_n)}$ where $(\iota_2, \dots, \iota_n)$ is the least multiindex from $\mathcal{J}_{n,d}$ such that

$$0 \ne \varphi_d(1, \iota_2, \dots, \iota_n) \in k$$

(here NN is an abbreviation for "Noether normalization"). Set

$$\mathrm{inn}_{X_1}(f; X_1, \dots, X_n) = (\iota_2, \dots, \iota_n).$$

Thus $f \mapsto \mathrm{inn}_{X_1}(f; X_1, \dots, X_n)$ is a function $P_{n,d} \to \mathcal{J}_{n-1,d}$.

In other words,

$$\mathrm{NN}_{X_1}(f; X_1, \dots, X_n) = f^{(\iota_2,\dots,\iota_n)} \quad \text{and} \quad \mathrm{inn}_{X_1}(f; X_1, \dots, X_n) = (\iota_2, \dots, \iota_n)$$

if and only if $\varphi_d(1, \iota_2, \dots, \iota_n) \ne 0$ and $\varphi_d(1, j_2, \dots, j_n) = 0$ for all $(j_2, \dots, j_n) \in J_{n,d}$ such that $(j_2, \dots, j_n) < (\iota_2, \dots, \iota_n)$.

If $k = \overline{k}$ (i.e., the field k is algebraically closed), then the function

$$\bigcup_{d \ge 0} P_{n,d} \to \bigcup_{d \ge 0} P_{n,d}, \quad f \mapsto \mathrm{NN}_{X_1}(f; X_1, \dots, X_n),$$

is an algorithm corresponding to a computation forest. Denote this forest by $\{T_d\}_{d \ge 0}$. Each tree T_d is of level $l(T_d) = 1$ and has $(d+1)^{n-1}$ leaves.

Note that the composition $\mathrm{LC}_{X_1} \circ \mathrm{NN}_{X_1}$ is defined, see Example 3 from Sec. 3 in [1], and $\mathrm{LC}_{X_1}(\mathrm{NN}_{X_1}(f)) = f(1, \iota_2, \dots, \iota_n)$.

2. The square-free factorization of a polynomial

First, we recall the main result of [3] in the form required for our purposes. Unless otherwise stated, in this section Λ is an integral algebra over the ground field k with field of fractions L (of course, the reader will see that some assertions are valid in the case where Λ is an arbitrary integral ring). Let $f, g \in \Lambda[X]$ be two polynomials in one variable X. Let $\deg_X f = n \ge 0$, $\deg_X g = m \ge 0$. Let r be an integer, $0 \le r \le \min\{n, m\} - 1$. Let $A, B \in L[X]$ be polynomials such that $0 \le \deg_X A \le m - r - 1$, $0 \le \deg_X B \le n - r - 1$. Put $h = Af + Bg$.

Let

$$f = \sum_{0 \le i \le n} f_i X^i, \quad g = \sum_{0 \le i \le m} g_i X^i, \quad h = \sum_{0 \le i \le m+n-r-1} h_i X^i,$$
$$A = \sum_{0 \le i \le m-r-1} A_i X^i, \quad B = \sum_{0 \le i \le n-r-1} B_i X^i,$$

where $f_i, g_i \in \Lambda$, $h_i, A_i, B_i \in L$. Assume that f, g, h are given. Then the equality $Af + Bg = h$ is equivalent to the following linear system $\mathcal{S}_r$:

$$\sum_{\max\{\nu-n,0\} \le i \le \nu} A_i f_{\nu-i} + \sum_{\max\{\nu-m,0\} \le j \le \nu} B_j g_{\nu-j} = h_\nu, \quad 0 \le \nu \le n + m - r - 1, \qquad (6)$$

with respect to the unknowns A_i, $0 \le i \le m-r-1$, and B_j, $0 \le j \le n-r-1$. Denote by S_r the coefficient matrix of this system. It has $m+n-r$ rows and $m+n-2r$ columns. Note that S_r is a submatrix of the Sylvester matrix $\mathrm{Syl}(f,g)$ of the polynomials f and g.

For each i, $0 \le i \le r$, denote by $\mathcal{S}_{r,i}$ the subsystem of $\mathcal{S}_r$ consisting of the equations from (6) with $\nu = i$ and $r+1 \le \nu \le n+m-r-1$ (so the number of equations in $\mathcal{S}_{r,i}$ is $m+n-2r$). Denote by $S_{r,i}$ the coefficient matrix of the system $\mathcal{S}_{r,i}$. Then $S_{r,i}$ has $m+n-2r$ rows and $m+n-2r$ columns. Let $\delta_{r,i} = \det(S_{r,i})$ be the determinant of the matrix $S_{r,i}$, $0 \le i \le r$.

Now if $h = \gcd(f,g) \in L[X]$ is the greatest common divisor of the polynomials f, g in the ring of polynomials $L[X]$ (it is uniquely defined up to a factor from $L \setminus \{0\}$) and $\deg_X h = r$, $0 \le r \le \min\{m,n\} - 1$ (so $h_i = 0$ for $r+1 \le i \le n+m-r-1$), then there are unique polynomials $A, B \in L[X]$ such that $\deg_X A \le m-r-1$, $\deg_X B \le n-r-1$, and $h = Af + Bg$.

Next, consider the case where $r = \min\{n,m\}$ (so the system $\mathcal{S}_r$ is not defined). Then, by definition, if $n = r$ put $\delta_{r,i} = f_i$ for $0 \le i \le r$, and if $n \ne r$ put $\delta_{r,i} = g_i$ for $0 \le i \le r$.

Lemma 1. *Under the above conditions, the following assertions hold.*

(i) *Assume that $h = \gcd(f,g) \in L[X]$ is the greatest common divisor of the polynomials f, g in the ring of polynomials $L[X]$ and $\deg_X h = r \le \min\{m,n\}$.*

If $r \le \min\{m,n\} - 1$, then the system $\mathcal{S}_r$ is equivalent to the system $\mathcal{S}_{r,r}$ and the latter has a unique solution.

Therefore, for an arbitrary r with $0 \le r \le \min\{m,n\}$, the element $\delta_{r,r}$ is not zero, and for all i with $0 \le i \le r$, we have $h_i/h_r = \delta_{r,i}/\delta_{r,r}$.

(ii) *Assume that $0 \le r \le \min\{m,n\}-1$, the elements h_i are zero for $r+1 \le i \le n+m-r-1$, $h_r \ne 0$, and the system $\mathcal{S}_{r,r}$ has no solution. Then $\delta_{r,r} = 0$ and $\deg_X \gcd(f,g) > r$.*

Proof. These assertions follow straightforwardly from the given definitions, and we leave to the reader to prove them, cf. also [3]. □

Corollary 1. *For given polynomials $f, g \in \Lambda[X]$ such as above, the degree of their greatest common divisor satisfies the inequality $\deg_X \gcd(f,g) = r \le \min\{m,n\}$ if and only if $\delta_{j,j} = 0$ for $0 \le j \le r-1$ and $\delta_{r,r} \ne 0$. Moreover, in this case*

$$\gcd(f,g) = \sum_{0 \le i \le r} \delta_{r,i} X^i \in \Lambda[X]. \tag{7}$$

Proof. This follows immediately from Lemma 1. □

Obviously, there are unique polynomials $\Delta_{r,i} \in k_0[Y_0, \ldots, Y_n, Z_0, \ldots, Z_m]$ (here Y_i, Z_j are new variables) such that $\delta_{r,i} = \Delta_{r,i}(f_0, \ldots, f_n, g_0, \ldots, g_m)$ for $0 \le i \le r$ and all polynomials f, g and rings Λ such as above. For $0 \le r \le \min\{m,n\}$, $0 \le i \le r$, we have the following bounds on the degrees with respect to all the variables $Y_0, \ldots, Y_n$, and $Z_0, \ldots, Z_m$:

$$\deg_{Y_0,\ldots,Y_n} \Delta_{r,i} \le m-r, \quad \deg_{Z_0,\ldots,Z_m} \Delta_{r,i} \le n-r. \tag{8}$$

Recall that $f, g \in \Lambda[X]$, $\deg_X f = n \ge 0$, $\deg_X g = m \ge 0$. We will use the following definition.

(**) Let r be an arbitrary integer, $0 \le r \le \min\{m,n\}$. If $\Delta_{j,j}(f_0, \ldots, f_n, g_0, \ldots, g_m) = 0$ for $0 \le j < r$ and $\Delta_{r,r}(f_0, \ldots, f_n, g_0, \ldots, g_m) \ne 0$, then

$$\mathrm{GCD}_{\Lambda,X}(f,g) = \sum_{0 \le i \le r} \Delta_{r,i}(f_0, \ldots, f_n, g_0, \ldots, g_m) X^i.$$

In the particular case where $k = \overline{k}$ is an algebraically closed field, the function $\mathrm{GCD}_{\overline{k},X} : \bigcup_{n,m \ge 0} (P_n \times P_m) \to \bigcup_{r \ge 0} P_r$ is an algorithm corresponding to a computation forest. Denote this forest by $\{T_{n,m}\}_{n,m \ge 0}$. Each tree $T_{n,m}$ is of level 1 and has $1 + \min\{m,n\}$ leaves.

Lemma 2. *Let n, m be integers, $n \geq m \geq 0$. There are polynomials*

$$Q_i \in k_0[Y_0, \ldots, Y_n, Z_0, \ldots, Z_m], \quad 0 \leq i \leq n-m,$$
$$R_i \in k_0[Y_0, \ldots, Y_n, Z_0, \ldots, Z_m], \quad 0 \leq i \leq m-1,$$

satisfying the following properties. Let Λ be an arbitrary commutative algebra with unity over k_0. Let $f, g \in \Lambda[X]$ be two polynomials such that $\deg_X f = n$, $\deg_X g = m$ and $f = \sum\limits_{0 \leq i \leq n} f_i X^i$, $g = \sum\limits_{0 \leq j \leq m} g_j X^j$ where $f_i, g_j \in \Lambda$. Then

$$g_m^{n-m+1} f = g \sum_{0 \leq i \leq m-n} Q_i(f_0, \ldots, f_n, g_0, \ldots, g_m) X^i + \sum_{0 \leq i \leq m-1} R_i(f_0, \ldots, f_n, g_0, \ldots, g_m) X^i$$

in the ring $\Lambda[X]$. Besides,

$$\deg_{Y_0,\ldots,Y_n} Q_i \leq 1, \quad \deg_{Z_0,\ldots,Z_m} Q_i \leq n-m, \quad 0 \leq i \leq n-m, \tag{9}$$

$$\deg_{Y_0,\ldots,Y_n} R_i \leq 1, \quad \deg_{Z_0,\ldots,Z_m} R_i \leq n-m+1, \quad 0 \leq i \leq m-1. \tag{10}$$

Further, let L be the total quotient ring of Λ. Assume additionally that the leading coefficient $g_m = \mathrm{lc}_X g$ is not a zero divisor in Λ and g divides f in the ring $L[X]$. Then $R_i(f_0, \ldots, f_n, g_0, \ldots, g_m) = 0$ for all i.

Proof. This is straightforward. □

For any f, g satisfying the conditions of Lemma 2, by definition put

$$Q_{\Lambda,X}(f,g) = \sum_{0 \leq i \leq m-n} Q_i(f_0, \ldots, f_n, g_0, \ldots, g_m) X^i,$$

$$R_{\Lambda,X}(f,g) = \sum_{0 \leq i \leq m-1} R_i(f_0, \ldots, f_n, g_0, \ldots, g_m) X^i.$$

Consider the multivariate case. Assume that $n \geq 2$.

Let $f, g \in k[X_1, \ldots, X_n]$, $\deg_{X_1,\ldots,X_n} f = d_1 \geq 0$, $\deg_{X_1,\ldots,X_n} g = d_2 \geq 0$. Put

$$f_1 = \mathrm{NN}_{X_1}(f; X_1, \ldots, X_n), \quad \mathrm{inn}_{X_1}(f; X_1, \ldots, X_n) = (i_2, \ldots, i_n),$$

$g_1 = g(X_1, X_2 + i_2 X_1, \ldots, X_1 + i_n X_n)$. Set $\Lambda = k[X_2, \ldots, X_n]$ and $h = \mathrm{GCD}_{\Lambda,X_1}(f_1, g_1)$, $a = \mathrm{LC}_{X_1}(h_1)$,

$$a_1 = \mathrm{NN}_{X_2}(a; X_2, \ldots, X_n), \quad (\iota_3, \ldots, \iota_n) = \mathrm{inn}_{X_2}(a; X_2, \ldots, X_n),$$

$h_1 = h(X_1, X_2, X_3 + \iota_3 X_2, \ldots, X_n + \iota_n X_2)$, $\Lambda_1 = k[X_1, X_3, \ldots, X_n]$, $q_1 = Q_{\Lambda_1,X_2}(h_1, a_1)$ and $q_2 = q_1(X_1, X_2, X_3 - \iota_3 X_2, \ldots, X_n - \iota_n X_2)$, $q = q_2(X_1, X_2 - i_2 X_1, \ldots, X_1 - i_n X_n)$. Then, obviously, $q = \gcd(f, g)$ is the greatest common divisor of the polynomials f, g in the ring $k[X_1, \ldots, X_n]$. If $k = \overline{k}$, then the function

$$\mathrm{GCD}_{X_1,\ldots,X_n} : \bigcup_{d_1,d_2 \geq 0} (P_{n,d_1} \times P_{n,d_2}) \to \bigcup_{d \geq 0} P_{n,d}, \quad (f,g) \mapsto q,$$

is defined. This function $\mathrm{GCD}_{X_1,\ldots,X_n}$ corresponds to a computation forest $\{T_{d_1,d_2}\}_{d_1,d_2 \geq 0}$, see the definitions in [1].

Now we proceed to the square-free factorization of polynomials. Let $f \in k[X_1, \ldots, X_n]$ be a polynomial with $\deg_{X_1,\ldots,X_n} f \geq 1$. Denote by k_{pf} the perfect closure of the field k. Then one can represent f in the form

$$f = \lambda_0 F_1 F_2^2 \cdot \ldots \cdot F_d^d \tag{11}$$

where $0 \neq \lambda_0 \in k$, all polynomials $F_i \in k_{\mathrm{pf}}[X_1, \dots, X_n]$ are separable (or, which is the same, square-free), $\gcd(F_{i_1}, F_{i_2}) = 1$ for $1 \leq i_1 \neq i_2 \leq d$, and $\deg_{X_1,\dots,X_n} F_i \geq 0$. We will see that one can choose F_i such that $F_i^i \in k[X_1, \dots, X_n]$, $1 \leq i \leq d$.

First, assume that $\mathrm{char}(k) = 0$. Then $k = k_{\mathrm{pf}}$. Set

$$f_1 = \mathrm{NN}_{X_1}(f; X_1, \dots, X_n),$$

$(\iota_2, \dots, \iota_n) = \mathrm{inn}_{X_1}(f; X_1, \dots, X_n)$. Let $\Lambda = k[X_2, \dots, X_n]$. Let $f_1' = \frac{df_1}{dX}$ be the derivative of the polynomial f_1. Then put

$$q_1 = Q_{\Lambda, X_1}(f_1, \mathrm{G\,C\,D}_{X_1,\dots,X_n}(f_1, f_1')) \in k[X_1, \dots, X_n]$$

and $G = q_1(X_1, X_2 - \iota_2 X_1, \dots, X_n - \iota_n X_1)$. Obviously, $G = \lambda_1 F_1 F_2 \cdot \ldots \cdot F_d$ where $0 \neq \lambda_1 \in k$. So G is the square-free part of the polynomial f in the ring $k[X_1, \dots, X_n]$.

Assume that $\mathrm{char}(k) = p > 0$. Let $i \geq 0$ be an integer. Set $B_i = \{jp^i : 1 \leq jp^i \leq d \ \&\ j \in \mathbb{Z}\}$ (hence $B_i = \varnothing$ if $p^i > d$) and $\Phi_i = \prod\limits_{j \in B_i} F_j^j$. Put

$$\Psi_i = \Phi_i(X_1^{p^{-i}}, \dots, X_n^{p^{-i}}) / \Phi_{i+1}(X_1^{p^{-i}}, \dots, X_n^{p^{-i}}).$$

Now $f = \lambda_0 \prod\limits_{0 \leq i \leq \log_p d} \Psi_i(X_1^{p^i}, \dots, X_n^{p^i})$ and $\Psi_i = \prod\limits_{j \in B_i \setminus B_{i+1}} F_j(X_1^{p^{-i}}, \dots, X_n^{p^{-i}})^j$. Note that if $j \in B_i \setminus B_{i+1}$, then j/p^i is an integer and p does not divide j/p^i.

Let i be fixed. One can represent f in the form $f = \sum\limits_{0 \leq r_1, \dots, r_n < p^i} X_1^{r_1} \cdot \ldots \cdot X_n^{r_n} f_{i, r_1, \dots, r_n}$ where $f_{i, r_1, \dots, r_n} \in k[X_1^{p^i}, \dots, X_n^{p^i}]$. We have $\gcd\{f_{i, r_1, \dots, r_n} : 0 \leq r_1, \dots, r_n < p^i\} = \Phi_i$ in the ring $k[X_1, \dots, X_n]$ (we leave the details to the reader).

Then one can compute each polynomial Φ_i, for example, as follows. Let $Y_1, \dots, Y_n$ be new variables. Put

$$q_i = \sum_{0 \leq r_1, \dots, r_n < p^i} Y_1^{r_1} \dots Y_n^{r_n} f_{i, r_1, \dots, r_n} \in k[Y_1 \dots, Y_n, X_1, \dots, X_n].$$

Then $\Phi_i = \mathrm{G\,C\,D}_{Y_1 \dots, Y_n, X_1, \dots, X_n}(q_i, \mathrm{LC}_Y(q_i))$ up to a nonzero factor from k, and we will assume without loss of generality that this factor is equal to 1.

Put $\Lambda = k[X_2, \dots, X_n]$,

$$\begin{aligned}
&\varphi_1 = \mathrm{NN}_{X_1}(\Phi_{i+1}; X_1, \dots, X_n), \quad (\iota_1, \dots, \iota_n) = \mathrm{inn}_{X_1}(\Phi_{i+1}; X_1, \dots, X_n),\\
&\varphi_2 = \Phi_i(X_1, X_2 + \iota_2 X_1, \dots, X_n + \iota_n X_1),\\
&\psi_1 = Q_{\Lambda, X_1}(\varphi_2, \varphi_1),\\
&\psi_2 = \psi_1(X_1, X_2 - \iota_2 X_1, \dots, X_n - \iota_n X_1),\\
&\psi_3 = \psi_2(X_1^{p^{-i}}, \dots, X_n^{p^{-i}}).
\end{aligned}$$

Now the polynomial ψ_3 coincides with Ψ_i up to a nonzero factor from k.

Further, similarly to the case of characteristic zero,

$$\begin{aligned}
&\psi = \mathrm{NN}_{X_1}(\psi_3; X_1, \dots, X_n), \quad (\iota_2', \dots, \iota_n') = \mathrm{inn}_{X_1}(\psi_3; X_1, \dots, X_n),\\
&q_1 = Q_{\Lambda, X_1}\Big(\psi, \mathrm{G\,C\,D}_{Y_1 \dots, Y_n, X_1, \dots, X_n}\Big(\psi, \sum_{1 \leq i \leq n} Y_i \frac{\partial \psi}{\partial X_i}\Big)\Big) \in k[X_1, \dots, X_n],
\end{aligned}$$

and $G_i = q_1(X_1, X_2 - \iota_2' X_1, \ldots, X_n - \iota_n' X_1)$. Obviously, G_i is the square-free part of the polynomial Ψ_i in the ring $k[X_1, \ldots, X_n]$. We have

$$G_i(X_1^{p^i}, \ldots, X_n^{p^i}) = \mu_i \prod_{j \in B_i \setminus B_{i+1}} F_j^{p^i},$$

$$\prod_{0 \le i \le \log_p d} G_i(X_1^{p^i}, \ldots, X_n^{p^i})^{p^{-i}} = \mu\, F_1 \cdot \ldots \cdot F_d,$$

where $0 \ne \mu_i \in k$, $0 \ne \mu \in k_{\mathrm{pf}}$. So, the family of separable polynomials G_i, $0 \le i \le \log_p d$, determines the square-free part of the polynomial f.

Let us return to the case of an arbitrary characteristic of the ground field. Let j be an arbitrary integer, $1 \le j \le d$.

If $\mathrm{char}(k) = 0$, put $G_0 = G$, $B_0 = \{1, 2, \ldots, d\}$, $B_1 = \varnothing$, $i = 0$, $p = 1$. If $\mathrm{char}(k) = p > 0$, assume that p^i divides j and p^{i+1} does not divide j for an integer i, $0 \le i \le \log_p d$.

Now we are going to find the polynomial $F_j^{p^i}(X_1^{p^{-i}}, \ldots, X_n^{p^{-i}})$ up to a nonzero factor from k. Put $G_{i,\alpha} = \mathrm{G\,C\,D}_{X_1,\ldots,X_n}(G_i(X_1^{p^i}, \ldots, X_n^{p^i}), F^\alpha)$, $1 \le \alpha \in \mathbb{Z}$. Then $G_{i,\alpha}$ coincides with

$$\prod_{j \in B_i \setminus B_{i+1}\,\&\, j < \alpha p^i} F_j^j \;\times \prod_{j \in B_i \setminus B_{i+1}\,\&\, j \ge \alpha p^i} F_j^{\alpha p^i}$$

up to a nonzero factor from k. The ratio $G_{i,\alpha}/G_{i,\alpha-1}$ coincides with

$$\prod_{j \in B_i \setminus B_{i+1}\,\&\, j \ge \alpha p^i} F_j^{p^i}$$

up to a nonzero factor from k.

Let $B_i \setminus B_{i+1} = \{\alpha_1 p^i, \ldots, \alpha_r p^i\}$ where $\alpha_1, \ldots, \alpha_r$ are integers and $1 \le \alpha_1 < \alpha_2 < \ldots < \alpha_r \le d/p^i$. Then for every s, $1 \le s < r$, the ratio

$$Q_s = (G_{i,\alpha_s}/G_{i,\alpha_s - 1})/(G_{i,\alpha_{s+1}}/G_{i,\alpha_{s+1}-1})$$

coincides with $F_{\alpha_s p^i}^{p^i}$ up to a nonzero factor from k. The ratio $G_{i,\alpha_r}/G_{i,\alpha_r - 1}$ coincides with $F_{\alpha_r p^i}^{p^i}$ up to a nonzero factor from k.

Applying the Noether normalization and Lemma 2 (cf. the computation of G_i), for each s, $1 \le s \le r-1$, we find a polynomial $\widetilde{F}_{\alpha_s p^i}$ coinciding with Q_s up to a nonzero factor from k. Then $\widetilde{F}_{\alpha_s p^i}$ coincides with $F_{\alpha_s p^i}^{p^i}$ up to a nonzero factor from k. In a similar way we compute a polynomial $\widetilde{F}_{\alpha_r p^i}$ coinciding with $F_{\alpha_r p^i}^{p^i}$ up to a nonzero factor from k.

Thus, for every $j \in B_i \setminus B_{i+1}$, the polynomial $\widetilde{F}_j(X_1^{p^{-i}}, \ldots, X_n^{p^{-i}}) \in k[X_1, \ldots, X_n]$ coincides with $F_j^{p^i}(X_1^{p^{-i}}, \ldots, X_n^{p^{-i}})$ up to a nonzero factor from k. In particular, we have proved that one can choose each F_j so that F_j^j has coefficients from k.

Let $1 \le j \le d$. If $\mathrm{char}(k) = 0$, then set $\mathrm{SQF}_{j,X_1,\ldots,X_n}(f) = \widetilde{F}_j$. If $\mathrm{char}(k) = p > 0$, then set $\mathrm{SQF}_{j,X_1,\ldots,X_n}(f) = \widetilde{F}_j(X_1^{p^{-i}}, \ldots, X_n^{p^{-i}})$ if and only if $j \in B_i \setminus B_{i+1}$, $0 \le i \le \log_p d$. Let $k = \overline{k}$. Then we introduce the function

$$\mathrm{SQF}_{X_1,\ldots,X_n} : \bigcup_{d \ge 1} P_{n,d} \to \bigcup_{d \ge 1} \Big(\bigcup_{m \ge 1} P_{n,m} \Big)^d, \quad f \mapsto \{\mathrm{SQF}_{j,X_1,\ldots,X_n}(f)\}_{1 \le j \le d}. \tag{1}$$

According to the described construction, the function $\mathrm{SQF}_{X_1,\ldots,X_n}$ is an algorithm corresponding to a computation forest. Denote this forest by $\{T_d'\}_{d \ge 1}$ (now n is fixed).

3. The absolute factorization of polynomials

Let $F \in k[X_1, \dots, X_n]$ be a polynomial, $\deg_{X_1,\dots,X_n} F = d \geq 2$. In this section, we will assume that F is separable, i.e., $\deg F_i = 0$ for $2 \leq i \leq d$ in (11), see Sec. 2. Denote by $P_{\mathrm{spr},n,d}$ the set of all separable polynomials from $\overline{k}[X_1, \dots, X_n]$ of degree d.

Let $u_2, \dots, u_n, w_2, \dots, w_n$ be elements algebraically independent over the field k. For brevity, denote by $k[u, w]$ the ring $k[u_2, \dots, u_n, w_2, \dots, w_n]$ and by $k_{u,w}$ the field of fractions of $k[u, w]$. If $a \in k[u, w]$, then put $\deg_{u,w} a = \deg_{u_2,\dots,u_n,w_2,\dots,w_n} a$.

Set $F_{u,w} = F(X_1, u_2X_1 + w_2, \dots, u_nX_1 + w_n)$. By the Bézout theorem, the polynomial $F_{u,w} \in k_{u,w}[X_1]$ has d pairwise distinct roots in the algebraic closure $\overline{k_{u,w}}$ of the field $k_{u,w}$. Hence the discriminant of the polynomial $F_{u,w}$ with respect to X_1 does not vanish:

$$\Delta = \mathrm{Res}_{X_1}\left(F_{u,w}, \frac{\partial F_{u,w}}{\partial X_1}\right) \neq 0.$$

Note that $\Delta \in k[u, w]$ and $\deg_{u,w} \Delta \leq (2d-1)d$. Let us choose and fix a set $\mathcal{J}_{2d^2} \subset K_0$ (recall that the notation $\mathcal{J}_d$ and $\mathcal{J}_{n,d}$ is introduced in Sec. 1). As in Sec. 1, we will assume that the set $\mathcal{J}_{2d^2}$ is well-ordered and $\mathcal{J}_{2n-1,2d^2}$ is ordered lexicographically.

Put

$$\begin{aligned} &\mathrm{NND}_{X_1}(F; X_1, \dots, X_n) = F(X_1, X_2 + \alpha_2X_1 + \beta_2, \dots, X_n + \alpha_nX_1 + \beta_n), \\ &\mathrm{innd}_{X_1}(F; X_1, \dots, X_n) = (\alpha_2, \dots, \alpha_n, \beta_2, \dots, \beta_n), \end{aligned} \tag{12}$$

where $(\alpha_2, \dots, \alpha_n, \beta_2, \dots, \beta_n) \in \mathcal{J}_{2n-1,2d^2}$ is the least multiindex such that

$$\Delta(\alpha_2, \dots, \alpha_n, \beta_2, \dots, \beta_n) \neq 0$$

and $\Phi_d(1, \alpha_2, \dots, \alpha_n) \neq 0$ where Φ_d is the form of degree d such that $\deg_{X_1,\dots,X_n}(F - \Phi_d) < d$.

Set $f = \mathrm{NND}_{X_1}(F; X_1, \dots, X_n)$. Then, obviously, $\deg_{X_1} f(X_1, 0, \dots, 0) = d$ and the polynomial $f(X_1, 0, \dots, 0) \in k[X_1]$ is separable, i.e., has d pairwise distinct roots in $\overline{k}$. Put $c = \mathrm{LC}_{X_1} f = \mathrm{lc}_{X_1} f(X_1, 0)$. Thus c is the leading coefficient of the polynomial f with respect to X_1.

If $k = \overline{k}$, then the function

$$\bigcup_{d\geq 2} P_{\mathrm{spr},n,d} \to \bigcup_{d\geq 0} P_{\mathrm{spr},n,d}, \quad F \mapsto \mathrm{NND}_{X_1}(F; X_1, \dots, X_n),$$

is an algorithm corresponding to a computation forest. Denote this forest by $\{T''_d\}_{d\geq 0}$.

Now we are going to apply the results of [2]. Let $v_3, \dots, v_n$ be elements algebraically independent over the field k. For brevity, denote by $k[v]$ the ring $k[v_3, \dots, v_n]$ and by k_v the field of fractions of $k[v]$ (in what follows, we will use other similar notations). If $a \in k[v]$, then put $\deg_v a = \deg_{v_3,\dots,v_n} a$.

Put $X = X_1$, $T = X_2$, $f_v = f(X, T, v_3T, \dots, v_nT) \in k[v][X, T]$. Set $\rho = \deg_T f_v$.

Set $f_0 = f(X, 0, \dots, 0)$. Let us write $f_0 = f_0(Z) + (X - Z)g_0$ for a polynomial $g_0 \in k[Z, X]$. Note that $g_0(Z, Z) = f'_0(Z) = \frac{df_0}{dZ}$. Put $\delta = f'_0(Z)$.

Set $f_v = \sum_{i\geq 0} f_{v,i} T^i$ where $f_{v,i} \in k[v][X]$ (hence if $i > \rho$, then $f_{v,i} = 0$). Set $\overline{f}_{v,i} = \delta^{2i-2} f_{v,i}$ for $i \geq 1$. Put $\overline{z}_0 = Z$.

For $i \geq 1$, let us define recursively polynomials $\overline{g}_{i,j} \in k_v[Z]$, $0 \leq j \leq m-2$, and $\overline{z}_i \in k_v[Z]$. Put $\overline{g}_i = \sum\limits_{0\leq j\leq m-2} \overline{g}_{i,j} X^j \in k_v[Z, X]$.

Assume that $\overline{g}_j$ and $\overline{z}_j$ are defined for $0 \leq j < i$ for some $i \geq 1$. Then

$$(X - Z)\overline{g}_i - g_0\overline{z}_i = \delta\Big(\overline{f}_{v,i} + \sum_{1\leq w\leq i-1} \overline{g}_w \overline{z}_{i-w}\Big). \tag{13}$$

Now, to find all $\overline{g}_{i,j} \in k(Z)$, $0 \le j \le m-2$, and $-\overline{z}_i \in k(Z)$, one should solve a linear system with coefficients from $k(Z)$ by Cramer's rule. It corresponds to (13). The coefficient matrix of this system is the Sylvester matrix of the polynomials $X - Z$ and g_0. Its determinant is $\pm\delta$. All free terms of this system are divisible by δ. Hence, actually, $\overline{g}_{i,j} \in k[v][Z]$ and $\overline{z}_i \in k[v][Z]$. The recursive step for the definition of $\overline{g}_i$ and $\overline{z}_i$ is described.

Consider the separable k-algebra $k' = k[Z]/(f_0(Z))$. Put $z = Z \bmod f_0(Z) \in k'$. In a similar way we define the separable k_v-algebra $k'_v = k_v[Z]/(f_0(Z))$. Thus $k'_u \supset k'$.

Then $f_0 = (X - z)g_0(z, X)$ where $g_0(z, X) \in k'_v[X]$. Note that $\delta(z) = g_0(z, z)$ is an invertible element of k', since the polynomial f_0 is separable. Let $k'_v[[\,T\,]]$ be the ring of formal power series in T over the algebra k'_v. One can apply Hensel's lifting to the decomposition $f(X, 0) = (X - z)g_0(z, X)$ and get

$$f = \Big(X - \sum_{i\ge 0} z_i\,T^i\Big)\Big(g_0(z, X) + \sum_{i\ge 1} g_i\,T^i\Big) \tag{14}$$

in the ring $k'_v[[\,T\,]][X]$. Here $z_0 = z$, $z_i \in k'_v$, $g_i \in k'_v[X]$, $\deg_X g_i \le m-2$ for $i \ge 1$.

For all $i \ge 1$,

$$z_i = \frac{\overline{z}_i(z)}{\delta(z)^{2i-1}}, \quad g_i = \frac{\overline{g}_i(z, X)}{\delta(z)^{2i-1}}. \tag{15}$$

This follows from Lemma 4 of [2].

Set $D = (2d-1)\rho + 1$ and

$$\begin{aligned}\eta &= \delta^{2D-3}X - \delta^{2D-3}\Big(Z + \sum_{1\le i\le D-1} \frac{\overline{z}_i\,T^i}{\delta^{2i-1}}\Big) \\ &= \delta^{2D-3}X - \Big(\delta^{2D-3}Z + \sum_{1\le i\le D-1} \overline{z}_i\delta^{2(D-1-i)}T^i\Big) \in K[\,Z, X, T].\end{aligned} \tag{16}$$

Let $x \in \overline{k}$. We will regard x as a parameter. If $f(x, 0) \ne 0$, then, by definition, the output of the described construction is $(\varnothing, 1, 1, 1, 1, 1)$, see Sec. 5 below for details. In what follows, unless otherwise stated, we will assume that $f(x, 0) = 0$. Hence every element of $k[x]$ can be represented in the form $\sum\limits_{0\le i<d} a_i x^i$ with $a_i \in k$. Nonetheless, performing the algebraic operations $\times, +, -$ with elements of $k[x]$, we will not use the relation $f(x, 0) = 0$ unless otherwise stated. Hence we will represent elements of $k[x]$ in the form $\sum\limits_{0\le i\le N} a_i x^i$ where $a_i \in k$ and N is arbitrary, i.e., in these computations x is analogous to a transcendental element over k (of course, such a representation with an arbitrary N is not unique, but it will arise in a natural way from the context).

Put

$$\begin{aligned} a_i &= \eta(x, X, T)X^{i-1}, && 1 \le i \le d-1, \\ a_i &= T^D X^{i-m}, && d \le i \le 2d-1. \end{aligned} \tag{17}$$

Set $B_1 = \overline{k_v}[T]$. We will identify the set of polynomials $g \in \overline{k_v}[X, T]$ such that $\deg_X g < d$ with B_1^d. Under this identification,

$$g = g_0 + g_1 X + \ldots + g_{d-1}X^{d-1} \mapsto (g_0, g_1, \ldots, g_{d-1}); \tag{18}$$

here $g_i \in B_1$ for all i.

Hence, under the identification (18), all a_i are in B_1^d.

Put $n_1 = d$, $n_2 = 2d-1$. Let A be the $n_1 \times n_2$ matrix with the rows $a_1, \ldots, a_{2m-1}$. Then the entries of A are in B_1. Denote by M the lattice in B_1^d generated by the rows of the matrix A.

Let $g = (g_0, \ldots, g_{d-1}) \in M$. Then put $|g| = \sup\{\deg_T g_i \,:\, 0 \le i \le d-1\}$ and $\deg_X g = \sup(\{i \,:\, g_i \ne 0 \,\&\, 0 \le i \le d-1\} \cup \{-1\})$.

For any two elements $g, h \in M$, put $g < h$ if and only if $|g| < |h|$ or $|g| = |h|$ but $\deg_X g < \deg_X h$. A minimal element of M is an arbitrary nonzero element $q \in M$ such that for every nonzero $g \in M$ it is not true that $g < q$, i.e., either $q < g$, or $|q| = |g|$ and $\deg_X q = \deg_X g$.

Lemma 3. *Assume that $f(x,0) = 0$ and q is a minimal element of M. Then q is an irreducible factor of the polynomial f_v in the ring $\overline{k_v}[X,T]$ such that $X - x$ divides $q(X,0)$ in the ring $\overline{k_v}[X]$. Further, $\mathrm{lc}_X q \in \overline{k_v}$, since $\mathrm{lc}_X f_v \in k$. Hence $q/\mathrm{lc}_X q \in \overline{k_v}[X,T]$.*

Proof. This follows immediately from the proof of Lemma 6 in [1] (we leave the details to the reader). □

Let $q^{(1)} \in M$ be an arbitrary nonzero element such that $|q^{(1)}| \le D$. By Lemma 1 of [1], one can represent $q^{(1)}$ in the form

$$q^{(1)} = \sum_{1 \le i \le 2d-1} \lambda_i a_i, \tag{19}$$

where $\lambda_i \in \overline{k_v}[T]$ and $\deg_T \lambda_i \le (2d+1)D$ for $1 \le i \le 2d-1$. Hence $\lambda_i = \sum_{0 \le j \le (2d+1)D} \lambda_{i,j} T^j$ where $\lambda_{i,j} \in \overline{k_v}$.

For an integer α, $0 \le \alpha \le D$, denote by $\mathcal{E}_\alpha$ the following assertion: "There is a nonzero element $q^{(1)} \in M$ with $|q| \le \alpha$." Then a homogeneous linear system $\mathcal{S}_\alpha$ over the field $k_v[x]$ corresponds to $\mathcal{E}_\alpha$ and satisfies the following properties. It is a system in the unknowns $\lambda_{i,j}$, $1 \le i \le 2d-1$, $0 \le j \le (2d+1)D$. The entries of its coefficient matrix are from $k[x][v]$. This system has a nonzero solution if and only if the assertion $\mathcal{E}_\alpha$ is true. Actually, a nonzero solution of the system $\mathcal{S}_\alpha$ determines an element $q^{(1)}$ such that $|q^{(1)}| \le \alpha$ according to (19). One can easily construct the system $\mathcal{S}_\alpha$ (we leave the details to the reader).

For integers α_1, α_2 with $0 \le \alpha_1 \le D$, $0 \le \alpha_2 \le d$, denote by $\mathcal{E}_{\alpha_1,\alpha_2}$ the following assertion: "There is a nonzero element $q^{(1)} \in M$ such that $|q^{(1)}| \le \alpha_1$ and $\deg_X q^{(1)} \le \alpha_2$." Then a homogeneous linear system $\mathcal{S}_{\alpha_1,\alpha_2}$ over the field $k_v[x]$ corresponds to $\mathcal{E}_{\alpha_1,\alpha_2}$ and satisfies the following properties. It is a system in the unknowns $\lambda_{i,j}$, $1 \le i \le 2d-1$, $0 \le j \le (2d+1)D$. The entries of its coefficient matrix are from $k[x][v]$. This system has a nonzero solution if and only if the assertion $\mathcal{E}_{\alpha_1,\alpha_2}$ is true. Actually, a nonzero solution of the system $\mathcal{S}_{\alpha_1,\alpha_2}$ determines an element $q^{(1)}$ such that $|q^{(1)}| \le \alpha_1$ and $\deg_X q^{(1)} \le \alpha_2$ according to (19). One can easily construct the system $\mathcal{S}_{\alpha_1,\alpha_2}$ (we leave the details to the reader).

Let $0 \le \alpha_1 \le D$, $1 \le \alpha_2 \le d$. Now an element q with $|q| = \alpha_1$, $\deg_X q = \alpha_2$ is minimal if and only if the following conditions are satisfied:

(a) the system $\mathcal{S}_{\alpha_1,\alpha_2}$ has a nonzero solution,
(b) if $\alpha_1 \ge 1$, then the system $\mathcal{S}_{\alpha_1-1}$ has only the zero solution,
(c) the system $\mathcal{S}_{\alpha_1,\alpha_2-1}$ has only the zero solution.

In this case, a nonzero solution of the system $\mathcal{S}_{\alpha_1,\alpha_2}$ determines an element q according to (19) (with q in place of $q^{(1)}$). Therefore, there is a minimal element $q \in M$ such that $q \in k[x][v][X,T]$.

The factor q irreducible over $\overline{k_v}$ of the polynomial f is uniquely defined up to a nonzero factor from $\overline{k_v}$. Hence if (a), (b), and (c) are satisfied, then the system $\mathcal{S}_{\alpha_1,\alpha_2}$ has only one solution linearly independent over $k_v[x]$.

The number of unknowns of the homogeneous linear systems from (a), (b), and (c) is equal to $r' = (2d-1)((2d+1)D+1)$. Denote by S_{α_1,α_2}, S_{α_1-1} (if $\alpha_1 \ge 1$), S_{α_1,α_2-1} the matrices of the homogeneous linear systems from (a), (b), and (c), respectively.

Condition (a) is fulfilled if and only if all minors of size r' of the matrix S_{α_1,α_2} are equal to 0.

Condition (b) is fulfilled if and only if $\alpha_1 = 0$ or not all minors of size r' of the matrix S_{α_1-1} are equal to 0.

Condition (c) is fulfilled if and only if not all minors of size r' of the matrix S_{α_1,α_2-1} are equal to 0.

Denote by $\Delta_1, \ldots, \Delta_{m_1}$ all minors of size r' of the matrix S_{α_1,α_2}. Denote by $\Delta_{m_1+1}, \ldots, \Delta_{m_2}$ all minors of size r' of the matrix S_{α_1-1} (if $\alpha_1 = 0$, then $m_1 = m_2$). Denote by $\Delta_{m_2+1}, \ldots, \Delta_{m_3}$ all minors of size r' of the matrix S_{α_1,α_2-1}.

Let $\wedge$, $\vee$ denote the logical conjunction and disjunction. Now (a) $\wedge$ (b) $\wedge$ (c) is equivalent to the condition

$$\begin{aligned}&(\Delta_1 = \ldots = \Delta_{m_1} = 0) \wedge ((\Delta_{m_1+1} \neq 0) \vee \ldots \vee (\Delta_{m_2} \neq 0))\\ &\wedge((\Delta_{m_2+1} \neq 0) \vee \ldots \vee (\Delta_{m_3} \neq 0)).\end{aligned} \tag{20}$$

Applying a result of [4], one can replace the minors Δ_i by some linear combinations of these minors and assume that $m_3 = d^{O(1)}$, but in fact it is not necessary.

Denote by J_{m_1,m_2,m_3} the set of all pairs (i_2, i_3) such that $m_1 < i \leq m_2$, $m_2 < j \leq m_3$. Let us order the pairs from J_{m_1,m_2,m_3} lexicographically, i.e., put $(i', j') < (i, j)$ if and only if $i' < i$ or $i' = i$ but $j' < j$. Let $(i, j) \in J_{m_1,m_2,m_3}$. Denote by $\mathcal{E}_{\alpha_1,\alpha_2,i,j}$ the following condition:

$$(\Delta_1 = \ldots = \Delta_{m_1} = 0) \wedge \bigwedge_{\substack{(i',j')\in J_{m_1,m_2,m_3},\\ (i',j')<(i,j)}} (\Delta_{i'}\Delta_{j'} = 0) \wedge (\Delta_i\Delta_j \neq 0). \tag{21}$$

Then condition (20) is equivalent to the disjunction $\bigvee_{(i,j)\in J_{m_1,m_2,m_3}} \mathcal{E}_{\alpha_1,\alpha_2,i,j}$.

Besides, if condition (20) is fulfilled, then one can choose a solution of the system $\mathcal{S}_{\alpha_1,\alpha_2}$ in the form $\lambda_{i,j} = \Delta'_{i,j}$ where each $\Delta'_{i,j}$ is equal, up to a sign, to some minor of size $r'-1$ of the matrix S_{α_1,α_2}. A minimal element q is computed by the formula $q = \sum\limits_{1\leq i\leq 2d-1} \sum\limits_{0\leq j\leq (2d+1)D} \Delta'_{i,j} T^j a_i$, see (19).

Note that $\Delta_i \in k[x][v]$ for $1 \leq i \leq m_3$. More precisely, one can represent Δ_i in the form $\Delta_i = \sum\limits_{0\leq j\leq N} \Delta_{i,j} x^j$ where $\Delta_{i,j} \in k[v]$ and N is bounded from above by $d^{O(1)}$ with an absolute constant in $O(1)$ (we leave to the reader to compute such a constant $O(1)$). Put $\widetilde{\Delta}_i = \sum\limits_{0\leq j\leq N} \Delta_{i,j} X^j \in k[v][X]$, $1 \leq i \leq m_3$.

If all polynomials $\widetilde{\Delta}_i$, $1 \leq i \leq m_3$, are zero, then put $\psi^{(1)} = f(X, 0)$. Assume that not all polynomials $\widetilde{\Delta}_i$, $1 \leq i \leq m_3$, are zero. There is an injective function $\varkappa : \{1, 2, \ldots, m_3 + m_3^2\} \to \mathbb{Z}^n$ such that if $\varkappa(i) = (j_1, \ldots, j_n)$ then $j_\alpha \geq 0$ for all α and $j_1 + \ldots + j_n \leq N$ where $N = d^{O(1)}$. Put

$$\psi^{(1)} = \mathrm{GCD}_{Y_1,\ldots,Y_n,X,v_3,\ldots,v_n}\Big(\sum_{1\leq i\leq m_1} Y_1^{j_1} \ldots Y_n^{j_n}\widetilde{\Delta}_i, f(X, 0)\Big) \in k[v][X],$$

where $(j_1, \ldots, j_n) = \varkappa(i)$ for every summand $Y_1^{j_1} \ldots Y_n^{j_n}\widetilde{\Delta}_i$. Further, set

$$\psi^{(2)} = \mathrm{GCD}_{Y_1,\ldots,Y_n,X,v_3,\ldots,v_n}\Big(\psi^{(1)}, \sum_{\substack{m_1<i_2\leq m_2,\\ m_2<i_3\leq m_3}} Y_1^{j_1} \ldots Y_n^{j_n}\widetilde{\Delta}_{i_2}\widetilde{\Delta}_{i_3}\Big) \in k[v][X],$$

where $(j_1, \ldots, j_n) = \varkappa(i_2 + m_3 i_3)$ for every summand $Y_1^{j_1} \ldots Y_n^{j_n}\widetilde{\Delta}_{i_2}\widetilde{\Delta}_{i_3}$. Now $\psi^{(2)} \neq 0$ and $\psi^{(2)}$ divides $\psi^{(1)}$ in the ring $k[v][X]$. Applying the Noether normalization and Lemma 2 (cf. Sec. 2), we compute a polynomial $\psi^{(3)} \in k[v][X]$ coinciding with $\psi^{(1)}/\psi^{(2)}$ up to a nonzero factor from k.

Note that $\mathrm{lc}_X \psi^{(3)} \in k[v]$. Further,

$$\psi^{(4)} = \psi^{(3)} / \mathrm{lc}_X \psi^{(3)} \in k[X],$$

since $\psi^{(4)}$ divides the polynomial $f(X,0)$ in the ring $k_v[X]$ and $f(X,0) \in k[X]$. Again applying Lemma 2, we compute a polynomial $\psi \in k[X]$ coinciding with $\psi^{(4)}$ up to a nonzero factor from k. We have $\psi(x) = 0$, since otherwise condition (20) does not hold. Hence $\deg_X \psi = \alpha_3 \geq 1$ and $\deg_X \psi^{(1)} > \deg_X \psi^{(2)} \geq 0$. We write ψ in the form $\psi = \sum\limits_{0 \leq i \leq \alpha_3} \psi_i X^i$ where $\psi_i \in k$. According to the described construction, all ψ_i are polynomials of degree $d^{O(1)}$ in the coefficients of f. These polynomials have coefficients in the ring K_0.

Under the identification (18), we have $q = \sum\limits_{0 \leq i \leq \alpha_2} q_i X^i$ where $q_i \in k[x][v][T]$. Note that $q_{\alpha_2} = \mathrm{lc}_X q \in k[x][v]$, since q divides f_v in the ring $k_v[x][X,T]$ and $\mathrm{lc}_X f_v = \mathrm{lc}_X f(X,0) \in k$. Further, $q / \mathrm{lc}_X q \in k[x][v][X,T]$, since this polynomial divides f_v in the ring $k_v[x][X,T]$ and $\mathrm{lc}_X f_v \in k$.

Applying the Noether normalization and Lemma 2 (here we leave the details to the reader), we compute a polynomial q' coinciding with $q / \mathrm{lc}_X q$ up to a nonzero factor from $k[x]$. So, replacing q by q', in what follows we will asume without loss of generality that $\mathrm{lc}_X q \in k[x]$.

According to the described construction, one can represent q in the form

$$q = \sum_{0 \leq s \leq \deg_T q} \sum_{0 \leq i \leq \alpha_2} \sum_{0 \leq j \leq N} q_{s,i,j} X^i x^j T^s,$$

where $q_{s,i,j} \in k[v]$, the integer N is bounded from above by $d^{O(1)}$, and all $q_{i,j,s}$ are polynomials in the coefficients from $k[v]$ of f_v. These polynomials have coefficients in the ring K_0. Put $q_{i,j} = \sum\limits_{0 \leq s \leq \deg_T q} q_{s,i,j} T^s$ for all i, j. Now $q_i = \sum\limits_{0 \leq j \leq N} q_{i,j} x^j$ for all i.

Put $q(X,0) = q|_{T=0}$. Then $q(X,0) \in k[x][X]$, since $q(X,0)$ divides $f(X,0)$ in the ring $k_v[x][X]$ and $\mathrm{lc}_X q(X,0) \in k[X]$.

Let $A = k[Z]/(\psi(Z))$ be a separable algebra and $z_1 = Z \bmod \psi \in A$. Thus $1, z_1, \ldots, z_1^{\deg \psi - 1}$ is a basis of A over k. Put $\nu_0 = \mathrm{lc}_X \psi$. Let $N \geq \alpha_3$, and let all $a_i \in k$, $0 \leq i \leq N$, be arbitrary. Note that the element $\sum\limits_{0 \leq i \leq N} a_i z_1^i$ can be represented in the form $\sum\limits_{0 \leq i < \alpha_3} b_i z_1^i$ with $b_i \in k$ using Lemma 2. Namely, every $\nu_0^{N - \alpha_3 + 1} b_i$ is a polynomial in $\psi_0, \ldots, \psi_{\alpha_3}$ and $a_0, \ldots, a_N$ with coefficients from the ring K_0.

The element q_{α_2} is invertible in $k[x]$ for every root x of ψ, since $\deg_X q(X,0) = \alpha_2$ for every root x of ψ. We are going to find $q_{\alpha_2}^{-1}$. Put $\widetilde{q}_{\alpha_2} = \sum\limits_{0 \leq j \leq N} q_{0,\alpha_2,j} z_1^j$ where $q_{0,\alpha_2,j} \in k[x]$. Then $\widetilde{q}_{\alpha_2}$ is invertible in A. Let $\widetilde{q}_{\alpha_2}^{-1} = \sum\limits_{0 \leq i < \alpha_3} b_i z_1^i$ where $b_i \in k$. Then

$$\left(\sum_{0 \leq i \leq N} q_{0,\alpha_2,j} z_1^j \right) \left(\sum_{0 \leq i < \alpha_3} b_i z_1^i \right) = 1.$$

From here, applying Lemma 2, we get the relation

$$\sum_{0 \leq i < \alpha_3} \sum_{0 \leq j < \alpha_3} L_{i,j} b_j z_1^i = \nu_0^{N+1},$$

where all $L_{i,j}$ are polynomials in $\psi_0, \ldots, \psi_{\alpha_3}$, $q_{\alpha_2,0}, \ldots, q_{\alpha_2,N}$ with coefficients from the ring K_0. Hence we obtain a linear system for finding $b_0, \ldots, b_{\alpha_3 - 1}$. We solve it by Cramer's rule.

Put $\nu_1 = \det(\{L_{i,j}\}_{0\le i,j<\alpha_3})$. Thus, one can write

$$q_{\alpha_2}^{-1} = \sum_{0\le i<\alpha_3} a_i \nu_0^{N+1} x^i/\nu_1, \tag{22}$$

where all a_i, ν_1 are polynomials in $\psi_0,\dots,\psi_{\alpha_3}$, $q_{\alpha_2,0},\dots,q_{\alpha_2,N}$ with coefficients from the ring K_0.

Put $q'' = (\nu_1/q_{\alpha_2})q$. Let

$$q'' = \sum_{0\le s\le \deg_T q''} \sum_{0\le i\le\alpha_2} \sum_{0\le j<\alpha_3} q''_{s,i,j} X^i x^j T^s,$$

where $q''_{s,i,j} \in k$. Then, by (22) and Lemma 2, we have $\mathrm{lc}_X q'' \in k$ and all $q_{s,i,j}$ are polynomials in $\psi_0,\dots,\psi_{\alpha_3}$, $q_{i,0},\dots,q_{i,N}$ with coefficients from the ring K_0. One can compute all $q''_{i,j}$ using (22) and Lemma 2. Now, replacing $(N, q, \{q_{s,i,j}\}_{\forall i,j})$ by $(\alpha_3-1, q'', \{q''_{s,i,j}\}_{\forall i,j})$, in what follows we will assume without loss of generality that $\mathrm{lc}_X q \in k$ and $N = \alpha_3 - 1$.

4. Completing the construction of the absolute factorization of polynomials

In this section, we will construct primitive elements of the fields generated by the coefficients of the absolute irreducible factors of a polynomial f. Here, as in the previous section, we need a detailed description, in order to obtain an algorithm corresponding to a computation forest in the next section.

Let $q(X,0) = \sum_{0\le i\le\alpha_2} Q_{0,i}X^i$ where $Q_{0,i} \in k[x]$. Then $Q_{0,\alpha_2} = q_{\alpha_2} \in k$. Further, for every i, $0 \le i < \alpha_3$, a representation $Q_{0,i} = \sum_{0\le j<\alpha_3} q_{0,i,j}x^j$ is computed with $q_{0,i,j} \in k$. Let Y be a new variable. Put

$$\theta_i = \sum_{0\le j<\alpha_3} q_{0,i,j} z_1^j \in A, \quad 0 \le i \le \alpha_2,$$
$$\theta = \sum_{0\le i\le\alpha_2} \theta_i Y^i \in A[Y].$$

Hence for every root x of the polynomial ψ, we have $\theta_i|_{z_1=x} = q_{0,i}$, $0 \le i \le \alpha_2$, and $\theta|_{z_1=x} = \sum_{0\le i\le\alpha_2} Q_{0,i}Y^i = q(Y,0)$.

For an integer α_4 with $0 \le \alpha_4 \le \alpha_3$, denote by $\mathcal{E}'_\delta$ the following assertion: "The elements $1,\theta,\dots,\theta^{\alpha_4} \in A \otimes_k k(Y)$ are linearly dependent over the field $k(Y)$." Let us write $\nu_0^{(\alpha_3-1)^2+1}\theta^i = \sum_{0\le j<\alpha_3} \theta_{i,j} z_1^j$ where $\theta_{i,j} \in k[Y]$ and, by Lemma 2, they are polynomials in Y, $\psi_0,\dots,\psi_{\alpha_3}$ and all $q_{0,i,j}$ with coefficients from the ring K_0. Denote by $\mathcal{S}'_{\alpha_4}$ the following homogeneous linear system over the field $k(Y)$ in the unknowns Z_i, $0 \le i \le \alpha_4$:

$$\sum_{0\le i\le\alpha_4} Z_i\theta_{i,j} = 0, \quad 0 \le j < \alpha_3. \tag{23}$$

Then the condition $\mathcal{E}'_{\alpha_4}$ is fulfilled if and only if the system $\mathcal{S}'_{\alpha_4}$ has a nonzero solution. Denote by S'_{α_4} the matrix of this system; its entries are in $k[Y]$.

Denote by $H \in k(Y)[Z]$ the minimal polynomial of the element $\theta \in A\otimes_k k(Y)$ over the field $k(Y)$ such that $H \in k[Y,Z]$. Let $\deg_Z H = \alpha_4$, and hence $H = \sum_{0\le i\le\alpha_4} H_i Z^i \in k[Y,Z]$ where $H_i \in k[Y]$. Then $H(Y,\theta) = 0$.

The degree $\deg_Z H$ is equal to α_4 if and only if the following two conditions are satisfied:

(c) the homogeneous linear system $\mathcal{S}'_{\alpha_4}$ has a nonzero solution,

(d) the homogeneous linear system $\mathcal{S}'_{\alpha_4-1}$ has only the zero solution.

If (c) and (d) are fulfilled, then any nonzero solution from $k[Y]^{\alpha_4+1}$ of the system $\mathcal{S}'_{\alpha_4}$ gives the coefficients $(H_0,\dots,H_{\alpha_4})$ of a minimal polynomial H (such a polynomial is uniquely defined up to a nonzero factor from $k[Y]$).

Condition (c) is fulfilled if and only if all minors of size α_4+1 of the matrix S'_{α_4} are equal to 0. Condition (d) is fulfilled if and only if not all minors of size α_4 of the matrix S'_{α_4-1} are equal to 0.

Denote by $\Delta_{m_3+1},\dots,\Delta_{m_4}$ all minors of size α_4+1 of S'_{α_4}. Denote by $\Delta_{m_4+1},\dots,\Delta_{m_5}$ all minors of size α_4 of S'_{α_4-1}. Note that $\Delta_i\in k[Y]$ for $m_3<i\le m_5$.

Now the conjunction (c) $\wedge$ (d) is equivalent to the condition

$$(\Delta_{m_3+1}=\ldots=\Delta_{m_4}=0)\wedge((\Delta_{m_4+1}\ne 0)\vee\ldots\vee(\Delta_{m_5}\ne 0)). \tag{24}$$

Besides, if condition (24) is fulfilled, then one can choose a solution of the system $\mathcal{S}'_{\alpha_4}$ in the form $Z_i=\Delta'_i$ where each Δ'_i is equal, up to a sign, to some minor of size α_4-1 of the matrix S'_{α_4} and Δ'_{α_4} is a nonzero minor of the matrix S'_{α_4-1}. The minors Δ'_i, $0\le i\le\alpha_4$, are taken from the same rows with indices $0\le i_0<\ldots<i_{\alpha_4-1}<\alpha_3$ of the matrix S'_{α_4}.

Put $H_i=\Delta'_i$, $0\le i\le\alpha_4$, $\nu_2=\Delta'_{\alpha_4}$. Note that $\deg_Y\Delta'_{\alpha_4}<\alpha_2\alpha_4\le d^2$.

For every root x of the polynomial ψ, the element $q(Y,0)$ is integral over $k[Y]$. Hence there is a minimal polynomial $\widetilde{H}_x\in k(Y)[Z]$ of the element $q(Y,0)$ over the field $k(Y)$ such that $\widetilde{H}_x\in k[Y,Z]$ and $\mathrm{lc}_Z\widetilde{H}_x\in k$. Note that each polynomial $\widetilde{H}_x$ is separable with respect to Z.

Denote by $\widetilde{H}$ the product of all pairwise distinct polynomials $\widetilde{H}_x$ where x runs over all roots of the polynomial ψ, i.e., $\widetilde{H}$ is the square-free part of the polynomial $\prod\limits_{\{x\,:\,\psi(x)=0\}}\widetilde{H}_x$. Then $\widetilde{H}$ coincides with H/H_{α_4} up to a nonzero factor from k. Therefore, $H/H_{\alpha_4}\in k[Y,Z]$. Applying Lemma 2, we compute a polynomial $H'\in k[Y,Z]$ such that H/H_{α_4} and H' coincide up to a nonzero factor from k. Replacing H by H', in what follows we will assume without loss of generality that $\mathrm{lc}_Z H\in k$.

Further, for every root x of the polynomial ψ, the field $k(Y)[q_{0,0},\dots,q_{0,\alpha_2}]$ contains the primitive element $q(Y,0)$. Hence, by the Chinese remainder theorem, the separable algebra $k(Y)[\theta_0,\dots,\theta_{\alpha_2}]$ (it is a subalgebra of $A\otimes_k k(Y)$) contains the primitive element θ. Therefore, there is a unique representation

$$\theta_i=\sum_{0\le j<\alpha_4}c_{i,j}\theta^j,\quad 0\le i\le\alpha_2,$$

where $c_{i,j}\in k(Y)$.

To find the coefficients $c_{i,j}$, note that

$$\theta_i=\sum_{0\le j<\alpha_4}c_{i,j}\theta^j=\sum_{0\le s<\alpha_3}\sum_{0\le j<\alpha_4}c_{i,j}\theta_{j,s}z_1^s\nu_0^{-(\alpha_3-1)^2-1}$$

and $\theta_i=\sum\limits_{0\le s<\alpha_3}q_{0,i,s}z_1^s$. Hence $\sum\limits_{0\le j<\alpha_4}c_{i,j}\theta_{j,s}=q_{0,i,s}\nu_0^{(\alpha_3-1)^2+1}$ for all i,s.

Now consider the linear system

$$\sum_{0\le j<\alpha_4}Z_j\theta_{j,s}=q_{0,i,s}\nu_0^{(\alpha_3-1)^2+1},\quad s=i_0,\dots,i_{\alpha_4-1}, \tag{25}$$

for $0\le i<\alpha_2$. Then $Z_j=c_{i,j}$, $0\le j<\alpha_4$, is the unique solution of the system (25). It can be found by Cramer's rule. Hence one can write $c_{i,j}=a_{i,j}/\nu_2$ where $a_{i,j}\in k[Y]$ and compute all $a_{i,j}$.

Enumerating the elements from the set $\mathcal{J}_{d^2-1}$, we find $y^* \in \mathcal{J}_{d^2-1}$ such that $\nu_2(y^*) \neq 0$. Put $\xi = \theta|_{Y=y^*}$.

Let us show that ξ is a primitive element of the separable algebra $k[\theta_0, \dots, \theta_{\alpha_2}]$ (it is a subalgebra of A) over the field k. Indeed, the elements $1, \xi, \dots, \xi^{\alpha_4-1}$ are linearly independent over k, since $\nu_2(y^*) \neq 0$. The polynomial $H(y^*, Z)$ is a minimal polynomial of the element ξ, since $H(y^*, \xi) = 0$, $0 \neq \mathrm{lc}_Z H \in k$, and $\deg_Z H(y^*, Z) = \alpha_4$. Finally, $\theta_i = \sum\limits_{0 \leq j < \alpha_4} \theta^*_{i,j} \cdot \xi^j$ where $\theta^*_{i,j} = a_{i,j}(y^*)/\nu_2(y^*)$ for all i, j. The required assertion is proved.

Every element of $k[\xi]$ can be represented in the form $\sum\limits_{0 \leq i < \alpha_4} a_i \xi^i$ where $a_i \in k$. Nonetheless, performing the algebraic operations $\times, +, -$ with elements of $k[\xi]$, we will not use the relation $H(y^*, \xi) = 0$ unless otherwise stated. Hence we will represent elements of $k[\xi]$ in the form $\sum\limits_{0 \leq i \leq N} a_i \xi^i$ where $a_i \in k$ and N is arbitrary, i.e., in these computations ξ is analogous to a transcendental element over k (of course, such a representation with an arbitrary N is not unique, but it will arise in a natural way from the context).

Put $Q_0 = q(X, 0)\nu_2(y^*)$. So $Q_0 \in k[\xi][X]$ and $\mathrm{lc}_X Q_0 \in k$. Applying Lemma 2, we find a polynomial $U_0 \in k[\xi][X]$ such that $Q_0 U_0$ coincides with $f(X, 0)$ up to a nonzero factor from k. More precisely, $Q_0 U_0 = \lambda_0 f(X, 0)$ where $0 \neq \lambda_0 = (\mathrm{lc}_X Q_0)^{d-\alpha_2+1} \in k$.

Let $\lambda_0 f_v = \sum\limits_{i \geq 0} \Phi_i T^i$ where $\Phi_i \in k[v][X]$ for all i and $\Phi_0 = \lambda_0 f(X, 0)$ (here $\Phi_i = 0$ if $i \geq \deg_T f_v$). Now we are going to use Hensel's lifting. Namely, we will construct the decomposition

$$\Big(Q_0 + \sum_{i \geq 1} Q_i T^i \Big) \Big(U_0 + \sum_{j \geq 1} U_j T^j \Big) = \Phi_0 + \sum_{i \geq 1} \Phi_i T^i, \tag{26}$$

where $Q_i, U_j \in k[\xi][v][X]$. More precisely, let $R_0 = \mathrm{Res}_X(Q_0, U_0) \in k$ be the resultant of the polynomials Q_0 and U_0. Let R_1 (respectively, R_2, R_3) be the discriminant of the polynomial $\lambda_0 f(X, 0)$ (respectively, Q_0, U_0). Therefore,

$$R_1 = R_2 R_3 R_0^2. \tag{27}$$

The elements R_0, R_2, R_3 are not zero divisors in $k[\xi]$, since $0 \neq R_1 \in k$.

Put $\overline{Q}_i = R_0^{2i-1} Q_i$, $\overline{U}_j = R_0^{2i-1} U_i$, $\overline{\Phi}_i = R_0^{2i-2} \Phi_i$ for $i, j \geq 1$. We will prove that one can represent these elements in the form $\overline{Q}_i = \sum\limits_{0 \leq j \leq \alpha_2 - 1} \overline{Q}_{i,j} X^j$, $\overline{U}_i = \sum\limits_{0 \leq j \leq d - \alpha_2 - 1} \overline{U}_{i,j} X^j$ where all $\overline{Q}_{i,j}, \overline{U}_{i,j}$ are in $k[\xi][v]$.

Assume that for some $i \geq 1$, the elements $\overline{Q}_j$ and $\overline{U}_j$ are already defined for $0 \leq j < i$ and $\overline{Q}_j, \overline{U}_j \in k[\xi][v][X]$. Then

$$U_0 \overline{Q}_i + Q_0 \overline{U}_i = R_0 \Big(\overline{\Phi}_i + \sum_{1 \leq w \leq i-1} \overline{Q}_w \overline{U}_{i-w} \Big). \tag{28}$$

Now, to find all $\overline{Q}_{i,j}$, $0 \leq j \leq \alpha_2 - 1$, and $\overline{U}_{i,j}$, $0 \leq j \leq d - \alpha_2 - 1$, one should solve the linear system with coefficients from $k[\xi][v]$ corresponding to (28). It has the unique solution, which can be obtained by Cramer's rule. The coefficient matrix of this system is the Sylvester matrix of the polynomials Q_0 and U_0. Its determinant $\pm R_0$ is not a zero divisor in $k[\xi][v]$. All free terms of this system are divisible by R_0. Hence $\overline{Q}_{i,j} \in k[\xi][v]$, $\overline{U}_{i,j} \in k[\xi][v]$ for all i, j, and, actually, they are polynomials in the coefficients from $k[\xi][v]$ of $Q_0, U_0, \lambda_0 f_v$. The recursive step for the definition and construction of $\overline{Q}_i$ and $\overline{U}_i$ is described.

Recall that $\deg_T q = \alpha_1$. Put $q''' = q\nu_2(y^*) R_1^{\alpha_1} \in k[\xi][v][T, X]$. Now (27) implies that $q''' \in k[\xi][v][T, X]$. We have $\mathrm{lc}_X q''' \in k$, and, according to the described construction of Hensel's lifting, all coefficients from $k[\xi]$ of q''' are polynomials in the coefficients from $k[\xi][v]$

of q_0 and $\lambda_0 f_v$. The degrees of these polynomials are bounded from above by $d^{O(1)}$ with an absolute constant in $O(\ldots)$.

We have $q''' = q'''(v_3, \ldots, v_n, T, X) \in k[\xi][v_3, \ldots, v_n, T, X]$. Put

$$Q''' = q'''(X_3/X_2, \ldots, X_n/X_2, X_2, X_1).$$

Then $Q''' \in k[\xi][X_1, \ldots, X_n]$ by the Gauss lemma (we leave the details to the reader). Put

$$Q^{(4)} = Q'''(X_1, X_2 - \alpha_2 X_1 - \beta_2, \ldots, X_n - \alpha_n X_1 - \beta_n),$$

see (12) at the beginning of Sec. 3.

According to the described construction, one can write

$$Q^{(4)} = \sum_{0 \le i \le N_1} \sum_{i_1, \ldots, i_n} Q^{(4)}_{i, i_1, \ldots, i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n} \xi^i,$$

where $Q^{(4)}_{i,i_1,\ldots,i_n} \in k$ and N_1 is the minimum possible such that $N_1 \ge \alpha_4 - 1$. The integer N_1 is bounded from above by $d^{O(1)}$ with an absolute constant in $O(\ldots)$. Moreover, all $Q^{(4)}_{i,i_1,\ldots,i_n}$ are polynomials in the coefficients of f. These polynomials have coefficients from the ring K_0.

Put $Q = H_{\alpha_4}^{N_1 - \alpha_4 + 1} Q^{(4)}$. Then, by Lemma 2, one can find a representation

$$Q = \sum_{0 \le i < \alpha_4} \sum_{i_1, \ldots, i_n} Q_{i, i_1, \ldots, i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n} \xi^i$$

where $Q_{i,i_1,\ldots,i_n} \in k$. Moreover, all $Q_{i,i_1,\ldots,i_n}$ are polynomials in the coefficients of f. These polynomials have coefficients from the ring K_0.

Set

$$\varepsilon = q_{\alpha_2} \nu_2(y^*) R_1^{\alpha_1} H_{\alpha_4}^{N_1 - \alpha_4 + 1}. \tag{29}$$

Then $\varepsilon = H_{\alpha_4}^{N_1 - \alpha_4 + 1} \mathrm{lc}_X q'''(X, 0)$.

For every root $Z = \xi^*$ of the polynomial $H(y^*, Z)$, put $Q^* = Q|_{\xi = \xi^*}$. Then the polynomial Q^* is irreducible in the ring $\overline{k}[X_1, \ldots, X_n]$ and Q^* divides F in the ring $k[\xi^*][X_1, \ldots, X_n]$ (we leave the details to the reader). Thus Q^* is an absolutely irreducible factor of the polynomial F.

5. Computation trees, coverings, and stratifications

In this section, we will obtain the required decomposition of the polynomial f into absolutely irreducible factors.

In what follows, we will not assume that necessarily $f(x, 0) = 0$. Let $k = \overline{k}$. Set $\widetilde{P}_{n,d} = \bigcup_{-1 \le d' \le d} P_{n,d}$, $d \ge 0$ (we assume here that $\deg_{X_1,\ldots,X_n} 0 = -1$). By definition, put $\widetilde{P}^0_{n,d} = \{\varnothing\}$ (it is a one-element set). Denote by P_{2,d_2,d_3} the set of all polynomials Φ from $\overline{k}[Y, Z]$ such that $\deg_Z \Phi = d_2$, $\deg_Y \Phi = d_3$.

The construction described in the previous sections defines the function

$$\mathfrak{t} : \bigcup_{d \ge 2} (P_{\mathrm{spr},n,d} \times \overline{k}) \to \bigcup_{d_1 \ge 0,\ d_2 \ge 0,\ d_3 \ge 0} (\widetilde{P}^{d_2}_{n,d_1} \times P_{2,d_2,d_3} \times \overline{k}^4)$$

given by the formula

$$\mathfrak{t}(F, x) = \begin{cases} ((Q_0, \ldots, Q_{\alpha_4 - 1}), H(Y, Z), \varepsilon, q_{\alpha_2}, c, y^*) & \text{if} \quad f(x, 0) = 0, \\ (\varnothing, 1, 1, 1, 1, 1) & \text{if} \quad f(x, 0) \ne 0, \end{cases}$$

where $Q = \sum_{0 \le i < \alpha_4} Q_i \xi^i$ and $Q_i \in k[X_1, \ldots, X_n]$ for all i. Recall that $c = \mathrm{lc}_X f(X, 0)$, $q_{\alpha_2} = \mathrm{lc}_X q(X, 0)$, $y^* \in \mathcal{J}_{d^2 - 1}$ and ε is defined by (29), see Secs. 3, 4. We leave to the reader to prove that this function is an algorithm corresponding to a computation forest (this follows

straightforwardly from the construction described in two preceding sections). Denote this forest by $\{T'''_d\}_{d\geq 2}$ (now we assume that n is fixed).

Remark 2. One can omit $\overline{k}^4$ in the definition of $\mathfrak{t}$. Indeed, assume that

$$((Q_0,\dots,Q_{\alpha_4-1}),H(Y,Z))$$

are computed at the output corresponding to a leaf w of a computation tree. This computation tree is obtained from the construction described in the two preceding sections. Then all elements $\varepsilon, q_{\alpha_2}, c, y^*$ are also computed at some vertices v_1, v_2, v_3, v_4 which are ancestors of w in this computation tree. So, we introduce $\overline{k}^4$ in the definition of $\mathfrak{t}$ only for convenience.

Denote by $b_1,\dots,b_\mu, Z$ the coordinate functions of the space of parameters $P_{\mathrm{spr},n,d}\times\overline{k}$. Here $\mu=\binom{n+d}{n}$ and Z is the coordinate function of $\overline{k}$.

Recall that in the notation of [1], a condition $\mathcal{A}_w$ corresponds to each vertex w of the tree T'''_d. For the reader's convenience and better understanding, here we observe that, for example, for all possible α_1,α_2, $(i,j)\in J_{m_1,m_3,m_3}$, there is a vertex w of the tree T'''_d such that $\mathcal{A}_w=\mathcal{E}_{\alpha_1,\alpha_2,i,j}$ (now all Δ_i in (21) are polynomials with coefficients in $k[b_1,\dots,b_\mu]$).

Let $L(T'''_d)$ be the set of leaves of the tree T'''_d. In the notation of [1], a condition $\overline{\mathcal{A}}_w$ corresponds to each leaf $w\in L(T'''_d)$ (one should not confuse this w with that from the preceding sections). It follows from the construction described in Secs. 3, 4 that each $\overline{\mathcal{A}}_w$ is equivalent to

$$(\varphi_{w,1}=\ldots=\varphi_{w,\mu_{w,1}}=0)\wedge((\varphi_{w,\mu_{w,1}+1}\neq 0)\vee\ldots\vee(\varphi_{w,\mu_{w,2}}\neq 0),$$

where there is exactly one index j_0 with $1\leq j_0\leq\mu_{w,2}$ such that

$$\varphi_{w,j_0}\in k[b_1,\dots,b_\mu,Z]\setminus k[b_1,\dots,b_\mu].$$

Moreover, $j_0=1$ or $j_0=\mu_{w,1}+1$. All other polynomials $\varphi_{w,j}$, $1\leq j\leq\mu_{w,2}$, $j\neq j_0$, are in $k[b_1,\dots,b_\mu]$. Actually, if $j_0=1$ then the polynomial φ_{w,j_0} corresponds to $\psi(Z)$, and if $j_0=\mu_{w,1}+1$ then φ_{w,j_0} corresponds to $f(Z,0)$, see Sec. 3.

If $j_0\neq\mu_{w,1}+1$, then, by definition, w is a leaf of the first kind, otherwise w is a leaf of the second kind.

In the notation of [1], we have the quasiprojective algebraic variety

$$\mathcal{W}_w=\mathcal{Z}(\varphi_{w,1},\dots,\varphi_{w,\mu_{w,1}})\setminus\mathcal{Z}(\varphi_{w,\mu_{w,1}+1},\dots,\varphi_{w,\mu_{w,2}})\subset P_{\mathrm{spr},n,d}\times\overline{k}.$$

Let w be a leaf of the first kind. Then, by definition, we have the quasiprojective algebraic variety

$$\mathcal{W}'_w=\mathcal{Z}(\varphi_{w,2},\dots,\varphi_{w,\mu_{w,1}})\setminus\mathcal{Z}(\varphi_{w,\mu_{w,1}+1},\dots,\varphi_{w,\mu_{w,2}})\subset P_{\mathrm{spr},n,d}.$$

The degrees of all polynomials $\varphi_{w,j}$ with respect to $b_1,\dots,b_\mu,Z$ are bounded from above by $d^{O(1)}$ with an absolute constant in $O(\dots)$ (the reader may compute such a constant). Further, the tree $L(T'''_d)$ has level $l(T'''_d)$ bounded from above by $d^{O(1)}$, again with an absolute constant in $O(\dots)$.

The output corresponding to a leaf $w\in L(T'''_d)$ of the first kind has the form

$$((Q_{w,0},\dots,Q_{w,d_2-1}),H_w,\varepsilon_w,e_w,c_w,y_w)$$

where

$$\begin{aligned}
&H_w\in k[b_1,\dots,b_\nu][Y,Z],\quad \deg_Y H=d_3\geq 1,\quad \deg_Z H_w=d_2\geq 1,\\
&Q_{w,i}\in k[b_1,\dots,b_\mu][X_1,\dots,X_n],\quad \max_{0\leq i\leq d_2-1}\deg_{X_1,\dots,X_n}Q_{w,i}=d_1\geq 1,\\
&0\neq\varepsilon_w,e_w,c_w\in k[b_1,\dots,b_\mu],\quad y_w\in k.
\end{aligned}$$

Here $1 \le d_1 \le d$, $1 \le d_2 \le d$, $1 \le d_3 \le d^2$. The degrees $\deg_{b_1,\dots,b_\mu} Q_{w,i}$ for all i, $\deg_{b_1,\dots,b_\mu} H_w$, $\deg_{b_1,\dots,b_\mu} e_w$, $\deg_{b_1,\dots,b_\mu} \varepsilon_w$, $\deg_{b_1,\dots,b_\mu} c_w$ are bounded from above by $d^{O(1)}$ with an absolute constant in $O(\dots)$.

Besides, e_w, c_w, $\mathrm{lc}_Z H_w$ do not have zeros on $\mathcal{W}_w$ and $\mathcal{W}'_w$, i.e., $\mathcal{W}_w \cap \mathcal{Z}(\varepsilon_w e_w c_w \mathrm{lc}_Z H_w)=\varnothing$ and $\mathcal{W}'_w \cap \mathcal{Z}(\varepsilon_w e_w c_w \mathrm{lc}_Z H_w) = \varnothing$. This follows immediately from the construction described in Secs. 3, 4.

The output corresponding to a leaf $w \in L(T'''_d)$ of the second kind has the form

$$(\varnothing, 1, 1, 1, 1, 1).$$

Put $\mathcal{P}_{i,d_{i,1},d_{i,2},d_{i,3}} = \widetilde{P}^{d_{i,2}}_{n,d_{i,1}} \times P_{2,d_{i,2},d_{i,3}} \times \overline{k}^4$, $1 \le i \le d$. Now consider the function

$$\mathfrak{T} : \bigcup_{d\ge 2} (P_{\mathrm{spr},n,d} \times \overline{k}^d) \to \bigcup_{d\ge 1} \bigcup_{\substack{d_{i,1}\ge 0,\ d_{i,2}\ge 0,\\ d_{i,3}\ge 0\ \forall\, 1\le i\le d}} \prod_{1\le i\le d} \mathcal{P}_{i,d_{i,1},d_{i,2},d_{i,3}}$$

given by the formula

$$\mathfrak{T}(F, (x_1, \dots, x_d)) = (\mathfrak{t}(F, x_1), \dots, \mathfrak{t}(F, x_d)).$$

The function $\mathfrak{T}$ is an algorithm corresponding to a computation forest $\{T^{(4)}_d\}_{d\ge 2}$. For every d, the tree $T^{(4)}_d$ is obtained from the trees T'''_d similarly to the construction of a d-tuple of computation trees, see [1, Sec. 2] (here we leave the details to the reader). We will assume that the coordinate functions on $P_{\mathrm{spr},n,d} \times \overline{k}^d$ are $b_1, \dots, b_\mu, Z_1, \dots, Z_d$.

Actually, we will use only the following properties of the tree $T^{(4)}_d$. The set of leaves $L(T^{(4)}_d)$ can be identified with $L(T'''_d)^d$ where $L(T'''_d)$ is the set of leaves of the tree T'''_d. Let $w = (w_1, \dots, w_d) \in L(T^{(4)}_d)$ where $w_i \in L(T'''_d)$. Assume that the algebraic variety of parameters $\mathcal{W}_{w_i}$ corresponds to w_i, $1 \le i \le d$, see above and the definitions in [1]. So, $\mathcal{W}_{w_i} \subset P_{\mathrm{spr},n,d} \times \overline{k}$. Then the variety of parameters $\mathcal{W}_w$ corresponding to w is equal to

$$\{(z, (x_1, \dots, x_n)) : (z, x_i) \in \mathcal{W}_{w_i}, 1 \le i \le d\}.$$

Hence if all leaves $w_1, \dots, w_d \in L(T'''_d)$ are of the first kind, then

$$\mathcal{W}_w = \mathcal{Z}(\psi_{w,1}, \dots, \psi_{w,\mu_{w,1}}) \setminus \mathcal{Z}(\psi_{w,\mu_{w,1}+1}, \dots, \psi_{w,\mu_{w,2}}) \tag{30}$$

for some integers $\mu_{w,2}$, $\mu_{w,1}$, where $\mu_{w,2} \ge \mu_{w,1} \ge d$, and polynomials $\psi_{w,i}$ such that

$$\begin{aligned} &\psi_{w,i} \in k[b_1, \dots, b_\mu, Z_i] \setminus k[b_1, \dots, b_\mu], && 1 \le i \le d,\\ &\psi_{w,i} \in k[b_1, \dots, b_\mu], && d+1 \le i \le \mu_{w,2}. \end{aligned} \tag{31}$$

For all i, the degrees $\deg_{b_1,\dots,b_\mu,Z_1,\dots,Z_d} \psi_{w,i}$ are bounded from above by $d^{O(1)}$ with an absolute constant in $O(\dots)$. The level $l(T^{(4)}_d)$ is also bounded from above by $d^{O(1)}$.

Further, if all leaves $w_1, \dots, w_d \in L(T'''_d)$ are of the first kind, then $\bigcap_{1\le i\le d} \mathcal{W}'_{w_i}$ coincides with the set of z such that there is $(x_1, \dots, x_d)$ with $(z, (x_1, \dots, x_d)) \in \mathcal{W}_w$.

Let $\mathcal{U} \subset \prod\limits_{1\le i\le d} \mathcal{P}_{i,d_{i,1},d_{i,2},d_{i,3}}$ be a Zariski open subset of all elements

$$(Q^{(i)}, H^{(i)}, \varepsilon^{(i)}, e^{(i)}, c^{(i)}, y^{(i)})_{1\le i\le d}$$

such that $Q^{(i)} \in \widetilde{P}^{d_{i,2}}_{n,d_{i,1}}$, $H^{(i)} \in \overline{k}[Y, Z]$, $H^{(i)} \in P_{2,d_{i,2},d_{i,3}}$, $0 \ne \varepsilon^{(i)}, e^{(i)}, c^{(i)} \in \overline{k}$, $y^{(i)} \in \overline{k}$, and $\mathrm{lc}_Z H^{(i)} \in \overline{k}$ for $1 \le i \le d$. Then $\mathcal{U}$ depends on d and $d_{j,i}$ $1 \le j \le 3$, $1 \le i \le d$. So we will write $\mathcal{U} = \mathcal{U}(d, d_{j,i})$ for brevity. Put $\mathcal{P}_{i,d_{i,1},d_{i,2}} = \widetilde{P}^{d_{i,2}}_{n,d_{i,1}} \times P_{1,d_{i,2}} \times \overline{k}^2$.

Now we introduce the function

$$\mathfrak{S}:\bigcup_{d\geq 1}\bigcup_{\substack{d_{i,1}\geq 0,\,d_{i,2}\geq 0,\\ d_{i,3}\geq 0\ \forall\, 1\leq i\leq d}}\mathcal{U}(d,d_{j,i})\to\bigcup_{d\geq 1}\bigcup_{\substack{d_{i,1}\geq 0,\,d_{i,2}\geq 0,\\ d_{i,3}\geq 0\ \forall\, 1\leq i\leq d}}\prod_{1\leq i\leq d}\mathcal{P}_{i,d_{i,1},d_{i,2}}$$

given by the formula

$$\mathfrak{S}((Q^{(i)},H^{(i)},\varepsilon^{(i)},e^{(i)},y^{(i)})_{1\leq i\leq d})=(\widetilde{Q}^{(i)},\widetilde{G}^{(i)},\widetilde{\varepsilon}^{(i)},c^{(i)})_{1\leq i\leq d},$$

where $\widetilde{Q}^{(i)}\in\widetilde{P}^{\alpha_{i,2}}_{n,\alpha_{i,1}}$, $\widetilde{G}^{(i)}\in P_{1,\alpha_{i,2}}$, $\widetilde{\varepsilon}^{(i)}\in\overline{k}$, $\alpha_{i,1},\alpha_{i,2}\geq 0$, are computed in the following way.

If $\deg_Z H^{(i)}=0$ for at least one i, $1\leq i\leq d$, then put $\alpha_{i,1}=\alpha_{i,2}=0$, $\widetilde{Q}^{(i)}=\varnothing$ and $\widetilde{G}^{(i)}=1$, $\widetilde{\varepsilon}^{(i)}=\varepsilon^{(i)}$ for all i (actually, we are not intrested in this case).

Assume that $\deg_Z H^{(i)}\geq 1$ for $1\leq i\leq d$. Then we compute the polynomial

$$E^{(i)}=\mathrm{G\,C\,D}_{Y,Z}\Big(H^{(i)}(Y,e^{(i)}Z)),\ \prod_{1\leq j<i}H^{(j)}(Y,e^{(j)}Z)\Big)$$

and, using Lemma 2, a polynomial $\widetilde{H}^{(i)}$ coinciding with $H^{(i)}/E^{(i)}$ up to a nonzero factor from k.

Put $\alpha_{i,2}=\deg_Z\widetilde{H}^{(i)}$. If $\alpha_{i,2}=0$, then put $\alpha_{i,1}=0$ and $\widetilde{G}^{(i)}=\widetilde{H}^{(i)}$, $\widetilde{Q}^{(i)}=\varnothing\in\widetilde{P}^0_0$, $\widetilde{\varepsilon}^{(i)}=\varepsilon^{(i)}$.

Assume that $\alpha_{i,2}>0$. Let $\widetilde{H}^{(i)}(y^{(i)},Z)=\sum_{0\leq j\leq\alpha_{i,2}}\widetilde{H}^{(i)}_jZ^j$ where $\widetilde{H}^{(i)}_j\in\overline{k}$. Then put

$$\widetilde{G}^{(i)}=\sum_{0\leq j\leq\alpha_{i,2}}\widetilde{H}^{(i)}_j\cdot(e^{(i)})^{\alpha_{i,2}-j}Z^j.$$

Let $\nu_{i,2}=\mathrm{lc}_Z\widetilde{G}^{(i)}$ (note that $\mathrm{lc}_Z\widetilde{G}^{(i)}=\widetilde{H}^{(i)}_{\alpha_2}=\mathrm{lc}_Z\widetilde{H}^{(i)}\in\overline{k}$). Then, using Lemma 2, we write for every i, $0\leq i\leq d-1$, the representation

$$\nu_{i,2}^{d_{i,2}-\alpha_{i,2}+1}\sum_{0\leq j<d_{i,2}}Q^{(i)}_jZ^j=A^{(i)}\widetilde{G}^{(i)}+B^{(i)},$$

where $A^{(i)},B^{(i)}\in\overline{k}[X_1,\ldots,X_n][Z]$ and $\deg_Z B^{(i)}<\alpha_{i,2}$. Let

$$B^{(i)}=\sum_{0\leq j<\alpha_{i,2}}B^{(i)}_jZ^j,\quad B^{(i)}_j\in\overline{k}[X_1,\ldots,X_n]\quad\text{for all}\quad i,j.$$

Put $\widetilde{Q}^{(i)}=(B^{(i)}_0,\ldots,B^{(i)}_{\alpha_{i,2}-1})$ and $\alpha_{i,1}=\max_{1\leq j<\alpha_{i,2}}\deg_{X_1,\ldots,X_n}B^{(i)}_j$. Finally, set $\widetilde{\varepsilon}^{(i)}=\nu_{i,2}^{d_{i,2}-\alpha_{i,2}+1}\varepsilon^{(i)}$. Thus, the element $(\widetilde{Q}^{(i)},\widetilde{H}^{(i)},\widetilde{\varepsilon}^{(i)},c^{(i)})_{1\leq i\leq d}$ is defined.

According to the described construction, the function $\mathfrak{S}$ is an algorithm corresponding to a computation forest. Denote this forest by $T^{(5)}=\{T^{(5)}_{d,d_{i,j}}\}_{\forall d,d_{i,j}}$.

Now the composition $T^{(5)}\circ T^{(4)}$ of the computation forests $T^{(5)}$ and $T^{(4)}$ is defined, see [1]. Recall that $T^{(5)}\circ T^{(4)}$ corresponds to the function $\mathfrak{S}\circ\mathfrak{T}$. Put $T^{(6)}=T^{(5)}\circ T^{(4)}$. Thus $T^{(6)}=\{T^{(6)}_d\}_{d\geq 2}$ where each $T^{(6)}_d$ is a computation tree.

The output corresponding to any leaf $w\in L(T^{(6)}_d)$ of the tree $T^{(6)}_d$ has the form

$$(Q^{(i)}_w,G^{(i)}_w,\varepsilon^{(i)}_w,c_w)_{1\leq i\leq d}$$

where

$$G^{(i)}_w\in k[b_1,\ldots,b_\mu][Z],\quad\deg_Z G^{(i)}_w=\alpha_{w,i,2}\geq 0,$$

if $\alpha_{w,i,2}>0$ then $Q^{(i)}_w=(Q^{(i)}_{w,0},\ldots,Q^{(i)}_{w,\alpha_{w,i,2}-1})$ where $Q^{(i)}_{w,j}\in k[b_1,\ldots,b_\mu][X_1,\ldots,X_n]$ and

$$\alpha_{w,i,1}=\max_{1\leq j\leq\alpha_{w,i,2}-1}\deg_{X_1,\ldots,X_n}Q^{(i)}_{w,j},$$

if $\alpha_{w,i,2}=0$ then $\alpha_{w,i,1}=0$ and $Q_w^{(i)}=\varnothing$. We have $0\neq\varepsilon_w^{(i)}, c_w\in k[b_1,\dots,b_\mu]$ (here c_w does not depend on i).

The degrees with respect to $b_1,\dots,b_\mu$ of all polynomials $G_w^{(i)}, \varepsilon_w^{(i)}, c_w$ and $Q_{w,j}^{(i)}$ (if $\alpha_{w,i,2}>0$) are bounded from above by $d^{O(1)}$ with an absolute constant in $O(\dots)$.

The algebraic variety $\mathcal{W}_w$ corresponding to any leaf $w\in L(T_d^{(6)})$ has the form (30) where each $\psi_{w,i}$ is a polynomial from $k[b_1,\dots,b_\mu]$ or $k[b_1,\dots,b_\mu,Z_j]$ for some j, $1\leq j\leq d$. Actually, all polynomials $\psi_{w,i}$ have coefficients in K_0. For all i, the degrees $\deg_{b_1,\dots,b_\mu,Z_1,\dots,Z_d}\psi_{w,i}$ are bounded from above by $d^{O(1)}$ with an absolute constant in $O(\dots)$. The level $l(T_d^{(6)})$ is also bounded from above by $d^{O(1)}$.

Besides, all polynomials $\varepsilon_w^{(i)}$, c_w, $\mathrm{lc}_Z G_w^{(i)}$ do not have zeros on $\mathcal{W}_w$, i.e.,

$$\mathcal{W}_w\cap\mathcal{Z}\Big(c_w\prod_{1\leq i\leq d}(\varepsilon_w^{(i)}\mathrm{lc}_Z G_w^{(i)})\Big)=\varnothing.$$

This follows immediately from our construction.

Denote by $L'(T_d^{(6)})$ the set of leaves w of the tree $T_d^{(6)}$ satisfying the following properties:

- there are leaves $w_1,\dots,w_d\in L(T_d''')$ of the first kind such that w is a descendant of the leaf $(w_1,\dots,w_d)\in L(T^{(4)})$,
- $\sum_{1\leq i\leq d}\alpha_{w,i,1}\alpha_{w,i,2}=d$.

The algebraic variety $\mathcal{W}_w$ corresponding to any leaf $w\in L'(T_d^{(6)})$ has the form (30) for some integers $\mu_{w,1}$, $\mu_{w,1}$ with $\mu_{w,2}\geq\mu_{w,1}\geq d$ and polynomials $\psi_{w,i}$ satisfying (31). Put

$$\mathcal{W}'_w=\mathcal{Z}(\psi_{w,d+1},\dots,\psi_{w,\mu_{w,1}})\setminus\mathcal{Z}(\psi_{w,\mu_{w,1}+1},\dots,\psi_{w,\mu_{w,2}})\subset P_{\mathrm{spr},n,d}.$$

For every $w\in L'(T_d^{(6)})$, denote by I_w the set of all integers i such that $1\leq i\leq d$ and $\alpha_{w,i,1}\alpha_{w,i,2}\neq 0$. For every $i\in I_w$, put

$$F_{w,i}=\sum_{0\leq j<\alpha_{w,i,2}}Q_{w,j}^{(i)}Z^j\in k[b_1,\dots,b_\mu,Z,X_1,\dots,X_n].$$

For every point $(b_1^*,\dots,b_\mu^*)\in\mathcal{W}'_w$, denote by $\Xi_{w,i}$ the set of roots of the polynomial

$$G_w^{(i)}(b_1^*,\dots,b_\mu^*,Z)\in\overline{k}[Z].$$

Thus $\#\Xi_{w,i}=\alpha_{w,i,2}$.

Let $F\in\overline{k}[b_1,\dots,b_\mu,X_1,\dots,X_n]$ be a generic polynomial of degree $\deg_{X_1,\dots,X_n}F=d\geq 2$. As a polynomial in $X_1,\dots,X_n$, it has all coefficients in the family $b_1,\dots,b_\mu$.

Lemma 4. *The following assertions hold.*

(a) *The union* $\bigcup_{w\in L'(T_d^{(6)})}\mathcal{W}'_w$ *is* $P_{\mathrm{spr},n,d}$, *i.e.,* $\{\mathcal{W}'_w\}_{w\in L'(T_d^{(6)})}$ *is a covering of the space* $P_{\mathrm{spr},n,d}$.

(b) *For every* $w\in L'(T_d^{(6)})$, *for every point* $(b_1^*,\dots,b_\mu^*)\in\mathcal{W}'_w$, *for every root* $\xi\in\Xi_{w,i}$, *the polynomial*

$$F_{w,i}(b_1^*,\dots,b_\mu^*,\xi,X_1,\dots,X_n)\in\overline{k}[X_1,\dots,X_n]$$

is irreducible in the latter ring, i.e., it is absolutely irreducible.

(c) *The family* $\{F_{w,i}(b_1^*,\dots,b_\mu^*,\xi,X_1,\dots,X_n)\}_{\xi\in\Xi_{w,i}\ i\in I_w}$ *contains* $\sum_{i\in I_w}\alpha_{w,i,2}$ *polynomials pairwise relatively prime in the ring* $\overline{k}[X_1,\dots,X_n]$.

(d) *We have*

$$c_w(b_1^*,\dots,b_\mu^*)\prod_{i\in I_w}\prod_{\xi\in\Xi_{w,i}}F_{w,i}(b_1^*,\dots,b_\mu^*,\xi,X_1,\dots,X_n)$$

$$=\Big(\prod_{i\in I_w}(\varepsilon_w^{(i)}(b_1^*,\dots,b_\mu^*))^{\alpha_{w,i,2}}\Big)F(b_1^*,\dots,b_\mu^*,X_1,\dots,X_n). \tag{32}$$

Hence (32) *is a decomposition of the polynomial* $F(b_1^*,\dots,b_\mu^*,X_1,\dots,X_n)$ *into absolutely irreducible factors up to a nonzero factor from* $\overline{k}$.

Proof. Note that any root of the polynomial $H(Y,q_{\alpha_2}Z)\in\overline{k}(Y)[Z]$ has the form $q(Y,0)/q_{\alpha_2}\in k[x][Y]$ for some root x of the polynomial $f(X,0)$. Therefore,

$$\mathrm{lc}_Y q(Y,0)/q_{\alpha_2}=1.$$

On the other hand, there is a unique absolutely irreducible factor φ of the polynomial f such that $\mathrm{lc}_{X_1}\varphi=1$ and $\varphi(Y,0,\dots,0)=q(Y,0)/q_{\alpha_2}$. Conversely, according to the described construction, for every absolutely irreducible factor φ of the polynomial f such that $\mathrm{lc}_{X_1}\varphi=1$ there is a root x of the polynomial $f(X,0)$ such that $\varphi(Y,0,\dots,0)=q(Y,0)/q_{\alpha_2}$. From here one can easily deduce all the assertions of the lemma (we leave the details to the reader). □

6. Lemma on a covering and a stratification

In the next general lemma, we show how to obtain a stratification of some variety if a covering of this variety is known. But first we need some definitions, cf. [1].

Let $\mathbb{A}^\mu(\overline{k})$ have coordinate functions $b_1,\dots,b_\mu$. Let $V\subset\mathbb{A}^\mu(\overline{k})$ be a quasiprojective algebraic variety and $\overline{V}$ be the closure of V with respect to the Zariski topology in the affine space $\mathbb{A}^\mu(\overline{k})$. Assume that $\overline{V}=\bigcup\limits_{0\le a\le\mu}V_a$ is a decomposition of $\overline{V}$ into the union of equidimensional affine algebraic varieties V_a, i.e., for every integer a, $0\le a\le\mu$, the dimension of every irreducible component E of the algebraic variety V_a is equal to a and E is an irreducible component of $\overline{V}$. Let $\deg V_a=D_a$ (the degree of an affine algebraic variety is the degree of its closure with respect to the Zariski topology in the corresponding projective space). By definition, set $D_a(V)=D_a$. For every integer $D\ge 2$, put

$$\begin{aligned}
&\deg V=\sum_{0\le a\le\mu}D_a,\\
&\delta_0(V)=D_a(V)\quad\text{where}\quad a=\dim(V),\\
&\delta_1(V,D)=\sum_{0\le a\le\mu}D_a(V)D^a,\\
&\delta(V,D)=\sum_{0\le a\le\mu}D_a(V)(D^{a+1}-1)/(D-1).
\end{aligned}$$

Let us fix an integer $D\ge 2$. Let $V_1,V_2\subset\mathbb{A}^\mu(\overline{k})$ be two quasiprojective algebraic varieties. We will say that $V_1<V_2$ if and only if $V_1\subset V_2$ and $\dim V_1<\dim V_2$ or $V_1\subset V_2$ and $\dim V_1=\dim V_2$ but $\delta_0(V_1)<\delta_0(V_2)$. Hence $<$ is a partial order on the set of all quasiprojective algebraic varieties in $\mathbb{A}^\mu(\overline{k})$.

Lemma 5. *Let* V *be a quasiprojective algebraic variety in* $\mathbb{A}^\mu(\overline{k})$. *Let* $\{\mathcal{W}_\gamma\}_{\gamma\in\Gamma}$ *be a family of quasiprojective algebraic varieties in* $\mathbb{A}^\mu(\overline{k})$. *Assume that for every* $\gamma\in\Gamma$

$$\mathcal{W}_\gamma=\mathcal{Z}(\psi_{\gamma,1},\dots,\psi_{\gamma,\mu_{\gamma,1}})\setminus\mathcal{Z}(\psi_{\gamma,\mu_{\gamma,1}+1},\dots,\psi_{\gamma,\mu_{\gamma,2}})\subset\mathbb{A}^\mu(\overline{k})$$

for some polynomials $\psi_{\gamma,i} \in \overline{k}[b_1, \dots, b_\mu]$ *such that* $\deg_{b_1,\dots,b_\mu} \psi_{\gamma,i} \le D$ *for all* i *for an integer* $D \ge 2$. *Assume that* $\bigcup_{\gamma\in\Gamma} \mathcal{W}_\gamma \supset V$. *Then there is a family of quasiprojective algebraic varieties* $\{\mathcal{W}_\beta\}_{\beta\in B}$ *satisfying the following properties.*

(a) *For every* $\beta \in B$,

$$\mathcal{W}_\beta = \mathcal{Z}(\psi^{(1)}_{\beta,1}, \dots, \psi^{(1)}_{\beta,\mu_{\beta,1}}) \setminus \bigcup_{2\le j\le m_\beta} \mathcal{Z}(\psi^{(j)}_{\beta,1}, \dots, \psi^{(j)}_{\beta,\mu_{\beta,j}}) \subset \mathbb{A}^\mu(\overline{k})$$

for an integer $m_\beta \ge 2$ *and some polynomials* $\psi^{(j)}_{\beta,i} \in \overline{k}[b_1, \dots, b_\mu]$ *such that*

$$\deg_{b_1,\dots,b_\mu} \psi_{\beta,i} \le D$$

for all i, j.

(b) *For every* $\beta \in B$, *the integer* m_β *is bounded from above by* $\delta_1(V, D)$.

(c) $\{V \cap \mathcal{W}_\beta\}_{\beta\in B}$ *is a stratification of the algebraic variety* V, *i.e.,* $\bigcup_{\beta\in B}(V \cap \mathcal{W}_\beta) = V$ *and* $(V \cap \mathcal{W}_{\beta_1}) \cap (V \cap \mathcal{W}_{\beta_2}) = \varnothing$ *for all pairwise distinct* β_1, β_2.

(d) *For every* $\beta \in B$ *there is* $\gamma \in \Gamma$ *such that* $\mathcal{W}_\beta \subset \mathcal{W}_\gamma$.

(e) $\#B \le \delta(V, D)$.

Proof. The proof uses recursion on V. Namely, we will assume that the lemma is proved for all quasiprojective algebraic varieties V' such that $V' < V$. The base of the recursion $V = \varnothing$ is obvious, since in this case $\delta(V, D) = 0$ and one can take $B = \varnothing$.

For every $\gamma \in \Gamma$, put

$$\mathcal{W}^{(1)}_\gamma = \mathcal{Z}(\psi_{\gamma,1}, \dots, \psi_{\gamma,\mu_{\gamma,1}}), \quad \mathcal{W}^{(2)}_\gamma = \mathcal{Z}(\psi_{\gamma,\mu_{\gamma,1}+1}, \dots, \psi_{\gamma,\mu_{\gamma,2}}).$$

Denote by $V^{(1)}_\gamma$ the union of all irreducible components E of V such that $E \subset \mathcal{W}^{(1)}_\gamma$ and $E \not\subset \mathcal{W}^{(2)}_\gamma$.

Denote by $V^{(2)}_\gamma$ the union of all irreducible components E of V such that $E \subset \mathcal{W}^{(1)}_\gamma \cap \mathcal{W}^{(2)}_\gamma$.

Denote by V'_γ the union of all irreducible components E of V such that $E \not\subset \mathcal{W}^{(1)}_\gamma$.

Put $V''_\gamma = (V^{(1)}_\gamma \cap \mathcal{W}^{(2)}_\gamma) \cup V^{(2)}_\gamma$.

Let us describe the step of the recursion. There is $\gamma_0 \in \Gamma$ such that $\dim V^{(1)}_{\gamma_0} = \dim V$. Let us choose and fix such an index γ_0. Now $V'_{\gamma_0} < V$ and $V''_{\gamma_0} < V$. Let us apply the recursive assumption to the algebraic varieties V'_{γ_0} and V''_{γ_0}. We get a family $\{\mathcal{W}'_\beta\}_{\beta\in B'}$ (respectively, $\{\mathcal{W}''_\beta\}_{\beta\in B''}$) satisfying properties (a)–(d) with (V'_{γ_0}, B') (respectively, (V''_{γ_0}, B'')) in place of (W, B).

We may assume without loss of generality that $\gamma_0 \notin B' \cup B''$ and $B' \cap B'' = \varnothing$. Put $B = B' \cup B'' \cup \{\gamma_0\}$ and

$$\mathcal{W}_\beta = \begin{cases} \mathcal{W}_{\gamma_0} & \text{if} \quad \beta = \gamma_0, \\ \mathcal{W}_\beta \setminus \mathcal{W}^{(1)}_{\gamma_0} & \text{if} \quad \beta \in B', \\ \mathcal{W}_\beta \cap \mathcal{W}^{(1)}_{\gamma_0} \cap \mathcal{W}^{(2)}_{\gamma_0} & \text{if} \quad \beta \in B''. \end{cases}$$

Obviously, now properties (a), (c), and (d) are satisfied. We have $\delta_1(V''_{\gamma_0}, D) \le \delta_1(V, D)$ by the Bézout theorem and, obviously, $\delta_1(V'_{\gamma_0}, D) < \delta_1(V, D)$. From here, using the recursive assumption, we get (b).

Let $E \subset \mathbb{A}^\mu(\overline{k})$ be a quasiprojective algebraic variety irreducible over k and

$$g \in \overline{k}[X_1, \dots, X_n]$$

be a polynomial of degree at most D. Then, by the Bézout theorem, $\delta(E \cap \mathcal{Z}(g), D) \le \delta(E, D)$, and if $E \cap \mathcal{Z}(g) \ne E$ then $\deg E + \delta(E \cap \mathcal{Z}(g), D) \le \delta(E, D)$.

Hence, repeatedly applying the latter assertion, we deduce that

$$1 + \delta(V^{(1)}_{\gamma_0} \cap \mathcal{W}^{(2)}_{\gamma_0}, D) \le \deg V^{(1)}_{\gamma_0} + \delta(V^{(1)}_{\gamma_0} \cap \mathcal{W}^{(2)}_{\gamma_0}, D) \le \delta(V^{(1)}_{\gamma_0}, D),$$

cf. the proof of Lemma 1 in [1] (here we leave the details to the reader).

Therefore, using the recursive assumption, we deduce that

$$\begin{aligned}
&\#B \le 1 + \#B' + \#B'' \le 1 + \delta(V', D) + \delta(V'', D)\\
&\le 1 + \delta(V^{(1)}_{\gamma_0} \cap \mathcal{W}^{(2)}_{\gamma_0}, D) + \delta(V^{(2)}_{\gamma_0}, D) + \delta(V'_{\gamma_0}, D)\\
&\le \delta(V^{(1)}_{\gamma_0}, D) + \delta(V^{(2)}_{\gamma_0}, D) + \delta(V'_{\gamma_0}, D) = \delta(V, D).
\end{aligned}$$

This proves (e). The lemma is proved. □

For example, applying Lemma 5 to the covering $\{\mathcal{W}'_w\}_{w \in L'(T^{(6)}_d)}$ of the space $P_{\mathrm{spr},n,d}$ from Lemma 4 (i), one can obtain a stratification $\{\mathcal{W}_\beta\}_{w \in B}$ of the space $P_{\mathrm{spr},n,d}$.

7. The general case

Recall that in Sec. 2, the function $\mathrm{SQF}_{X_1,\dots,X_n}$ corresponding to the computation forest $\{T'_d\}_{d \ge 0}$ is defined. We have $\mathrm{SQF}_{X_1,\dots,X_n} = \{\mathrm{SQF}_{i,X_1,\dots,X_n}\}_{1 \le i \le d}$, see the end of Sec. 2.

Let d be an integer, $d \ge 2$, let $F \in \overline{k}[X_1, \dots, X_n]$ be an arbitrary polynomial of degree $\deg_{X_1,\dots,X_n} F \le d$, and let $x_i = (x_{i,1}, \dots, x_{i,d}) \in \overline{k}^d$, $1 \le i \le d$. Then put $F' = \mathrm{RDP}_{X_1,\dots,X_n}(F)$, see Remark 1. Let $\deg_{X_1,\dots,X_n} F' = d_1$. If $d_1 \le 0$, put $\mathfrak{D}(F, (x_1, \dots, x_d)) = F'$.

Assume that $d_1 \ge 1$. Then put $F''_i = \mathrm{SQF}_{i,X_1,\dots,X_n}(F')$, $1 \le i \le d_1$. Let $d_{i,1} = \deg_{X_1,\dots,X_n} F''_i$. If $d_{i,1} \le 1$, put $G_i = F''_i$ for every i, $1 \le i \le d_{i,1}$. If $d_{i,1} \ge 2$, put $G_i = (\mathfrak{S} \circ \mathfrak{T})(F''_i, (x_{i,1}, \dots, x_{i,d_{i,1}}))$ for every i, $1 \le i \le d_{i,1}$. Set $\mathfrak{D}(F, (x_1, \dots, x_d)) = (G_1, \dots, G_{d_1})$.

Now $\mathfrak{D}$ is a function with the domain of definition $\bigcup_{d \ge 2}(\overline{k}^{N(n,d)} \times \overline{k}^{d^2})$. We leave to the reader to define the range of values of the function $\mathfrak{D}$. The function $\mathfrak{D}$ corresponds to a computation forest $T^{(7)} = \{T^{(7)}_d\}_{d \ge 2}$.

The following assertions on the computation trees $T^{(7)}_d$ are similar to those from Sec. 5 related to $T^{(6)}_d$. Their poofs are only sligtly more complicated than the proofs of the analogous assertions from Sec. 5. So we leave the details to the reader.

The level $l(T^{(7)}_d)$ of the tree $T^{(7)}_d$ is bounded from above by $d^{O(1)}$. For every leaf $w \in L(T^{(7)}_d)$, the degrees with respect to $b_1, \dots, b_\mu$ of all polynomials from the output corresponding to w are bounded from above by $d^{O(1)}$. The quasiprojective algebraic variety $\mathcal{W}_w$ can be represented in the form (30) where $\psi_{w,r} \in k[b_1, \dots, b_\mu, \{Z_{i,j}\}_{1 \le i,j \le d}]$ and for every (i,j) there is at most one polynomial $\psi_{w,r}$ such that $\deg_{Z_{i,j}} \psi_{w,r} > 0$. We will write $r = r_{i,j}$ in this case. Besides, if $\deg_{Z_{i,j}} \psi_{w,r} > 0$, then $\psi_{w,r} \in k[b_1, \dots, b_\mu, Z_{i,j}]$. The degrees of all polynomials $\psi_{w,r}$ are bounded from above by $d^{O(1)}$.

Let $w \in L(T^{(7)}_d)$. Assume that for all (i,j) we have $1 \le r_{i,j} \le \mu_{w,1}$ if $r_{i,j}$ is defined. In this case, by definition, w is a leaf of the first kind. For every leaf of the first kind, by definition, the quasiprojective algebraic variety $\mathcal{W}'_w$ is the projection of $\mathcal{W}_w$ to $\mathbb{A}^\mu(\overline{k})$ (this affine space has the coordinate functions $b_1, \dots, b_\mu$).

Proof of Theorem 1. First, consider the case where $((a_1, \dots, a_\nu), f) = ((b_1, \dots, b_\mu), F)$ with F a generic polynomial of degree d (i.e., the family of its coefficients is $\{b_j\}_{1 \le j \le \mu}$). Now the analog of Lemma 4 is exactly Theorem 1 (note only that a slightly different notation is used in the statement of the theorem). The tree $T^{(7)}_d$ now is similar to $T^{(6)}_d$.

One can define the subset $L'(T_d^{(7)}) \subset L(T_d^{(7)})$ of leaves w of the first kind such that for every point $(b_1^*, \ldots, b_\mu^*) \in \mathcal{W}'_w$ the output corresponding to w determines a decomposition of the polynomial $F(b_1^*, \ldots, b_\mu^*, X_1, \ldots, X_n)$ into absolutely irreducible factors. The family $\{\mathcal{W}'_w\}_{w \in L'(T_d^{(7)})}$ is a covering of the space $\overline{k}^{N(n,d)}$ for every $d \geq 2$. One can obtain a stratification $\{\mathcal{W}_\beta\}_{\beta \in B_1}$ of this space applying Lemma 5 to the covering under consideration.

Further, as in the proof of Lemma 4, combining the results of the preceding sections one can easily establish all the required assertions in the case of a generic polynomial F. In particular, one can compute the exact values of $\lambda_{\alpha,0}$ and $\lambda_{\alpha,1}$ in the terms from the constructions described in Secs. 2–4, cf. the statement of Lemma 4.

Now, to prove the theorem for the initial input data $((a_1, \ldots, a_\nu), f)$, it is sufficient to consider the tree $T_d^{(7)}(f)$, see the definition in [1] (roughly speaking, to obtain $T_d^{(7)}(f)$, one should substitute the coefficients from $k[a_1, \ldots, a_\nu]$ of the polynomial f in place of $b_1, \ldots, b_\mu$ everywhere in the objects of $T_d^{(7)}$). The leaves $L(T_d^{(7)}(f))$ are in a one-to-one correspondence with $L(T_d^{(7)})$. We have $l(T_d^{(7)}(f)) = l(T_d^{(7)}) + 1$. For every leaf $w \in L(T_d^{(7)}(f))$, the degrees with respect to $a_1, \ldots, a_\nu$ of all polynomials from the output corresponding to w are bounded from above by $d'd^{O(1)}$. The quasiprojective algebraic variety $\mathcal{W}_w$ can be represented in the form (30) where $\psi_{w,r} \in k[a_1, \ldots, a_\nu, \{Z_{i,j}\}_{1 \leq i,j \leq d}]$. The degrees of all polynomials $\psi_{w,r}$ are bounded from above by $d'd^{O(1)}$.

For every leaf $w \in L(T_d^{(7)}(f))$ corresponding to a leaf of the first kind from $L(T_d^{(7)})$, by definition, the quasiprojective algebraic variety $\mathcal{W}'_w$ is the projection of $\mathcal{W}_w$ to $\mathbb{A}^\nu(\overline{k})$ (here this affine space has the coordinate functions $a_1, \ldots, a_\nu$).

Denote by $L'(T_d^{(7)}(f))$ the set of leaves w from $L(T_d^{(7)}(f))$ such that w corresponds to a leaf from $L'(T_d^{(7)})$. For every leaf $w \in L'(T_d^{(7)}(f))$, for every point $(a_1^*, \ldots, a_\nu^*) \in \mathcal{W}'_w$, the ouput corresponding to w determines a decomposition of the polynomial $f(a_1^*, \ldots, a_\nu^*, X_1, \ldots, X_n)$ into absolutely irreducible factors.

Finally, we replace the tree $T_d^{(7)}(f)$ by the irredundant tree $\mathrm{IRD}(T_d^{(7)}(f))$, see [1]. The number of leaves of the tree $\mathrm{IRD}(T_d^{(7)}(f))$ is bounded from above by $(d')^\nu d^{O(\nu)}$ by Theorem 1 of [1]. Put $T_d^{(8)} = \mathrm{IRD}(T_d^{(7)}(f))$ and $L'(T_d^{(8)}) = L(\mathrm{IRD}(T_d^{(7)}(f))) \cap L'(T_d^{(7)}(f))$.

The family $\{\mathcal{W}'_w\}_{w \in L'(T_d^{(8)})}$ is a covering of the space $\mathbb{A}^\nu(\overline{k})$. One can obtain a stratification $\{\mathcal{W}_\beta\}_{\beta \in B_2}$ of this space applying Lemma 5 to the covering under consideration. By Lemma 5 (e), the number of elements $\#B_2$ is bounded from above by $(d')^\nu d^{O(\nu)}$. Now one can take A to be the subset of all $\beta \in B_2$ such that $\mathcal{W}_\beta \neq \varnothing$ (here the notation $(\beta, \mathcal{W}_\beta)$ corresponds to $(\alpha, \mathcal{W}_\alpha)$ from the statement of Theorem 1). Thus, the initial case $((a_1, \ldots, a_\nu), f)$ is reduced to the generic case $((b_1, \ldots, b_\mu), F)$. The theorem is proved. □

Translator A. L. Chistov.

REFERENCES

1. A. L. Chistov, "Computations with parameters: a theoretical background," *J. Math. Sci.*, **215**, No. 6, 769–781 (2016).
2. A. L. Chistov, "A bound for the degree of a system of equations determining the variety of reducible polynomials," *St.Petersburg Math. J.*, **24**, No. 3, 513–528 (2013).
3. G. E. Collins, "Subresultants and reduced polynomial remainder sequences," *J. ACM*, **14**, No. 1, 128–142 (1967).
4. A. Chistov, H. Fournier, L. Gurvits, and P. Koiran, "Vandermonde matrices, NP-completeness, and transversal subspaces," *Found. Comput. Math.*, **3**, No. 4, 421–427 (2003).