Записки научных
семинаров ПОМИ
Том 316, 2004 г.

A. Ayad

COMPLEXITY BOUND OF ABSOLUTE FACTORING OF PARAMETRIC POLYNOMIALS

Abstract. An algorithm is constructed for the absolute factorization of polynomials with algebraically independent parametric coefficients. It divides the *parameter space* into pairwise disjoint pieces such that the absolute factorization of the polynomials with coefficients in each piece is given uniformly. Namely, for each piece there exist a positive integer $l \leq d$, l variables $C_1, \dots, C_l$ algebraically independent over a ground field F and rational functions $b_{J,j}$ of the parameters and of the variables $C_1, \dots, C_l$ such that for any parametric polynomial f with coefficients in this piece, there exist $c_1, \dots, c_l \in \overline{F}$ with $f = \prod_j G_j$ where $G_j = \sum_{|J|} B_{J,j} Z^J$ is absolutely irreducible. Where $Z = (Z_0, \dots, Z_n)$ are the variables of f, each $B_{J,j}$ is the value of $b_{J,j}$ at the coefficients of f and $c_1, \dots, c_l$. $\overline{F}$ denotes the algebraic closure of F.

The number of pieces does not exceed $(2d^2+1)^{2n+3d+5}$ and the algorithm performs the following number of arithmetic operations in F (being exponential in the number of the coefficients $r = \binom{n+1+d}{n+1}$ of f): $d^{O(ndr^2)}$ and its binary complexity is bounded
if $F = \mathbb{Q}$ by $d^{O(ndr^2)}$ and if $F = \mathbb{F}_p$ by $\left(pd^{ndr^2}\right)^{O(1)}$
where d is an upper bound on the degrees of the polynomials.

The technique used include the Hensel lemma and the *quantifier elimination* in the theory of algebraically closed fields.

1. Introduction and notation

The problem of the factorization of multivariate polynomials with coefficients in a field was studied by many mathematicians. Kronecker worked on this problem in the case of polynomials with integer coefficients. An exposition of Kronecker's algorithm with its exponential complexity could be found in [12] and [15].

In 1967, Berlekamp described an algorithm which factorizes a univariate polynomial with coefficients in a finite field of q elements with the polynomial complexity: $O(d^3 q)$ where d is the degree of this polynomial (see, e.g., [2, 3, 15]).

Basing on the algorithm of Berlekamp and the Hensel lemma (see, e.g., [5, 7, 10, 15, 17, 18, 20]), Zassenhaus (see, e.g., [15, 20]) has designed an algorithm of factorization of polynomials in $\mathbb{Z}[X]$ but also with an exponential complexity in the size of the input. The first algorithm for univariate factorization over $\mathbb{Q}$ with polynomial-time complexity in the size of the input polynomial was published in [14] by Lenstra, Lenstra, and Lovasz. D. Grigoriev [7] and A. Chistov [5] described in 1982 a polynomial time algorithm of factorization of polynomials in several variables with coefficients in a field which is a finite extension of a purely transcendental extension of its prime subfield.

A multivariate polynomial with coefficients in an extension of F is called an absolute irreducible polynomial if it is irreducible over the algebraic closure $\overline{F}$ of F. The absolute factorization of a multivariate polynomial is its decomposition into absolute irreducible factors. For more details on the algorithms of the absolute factorization of polynomials, one can look the paper of A. Chistov [5] and the thesis of J-F. Ragot [19]. In [5], Chistov has presented an algorithm with polynomial complexity, of reduction of the absolute factorization to the factorization over the ground field.

A parametric polynomial is a polynomial whose coefficients are polynomials (over F) of the parameters. In this text we restrict our attention to the case when all the coefficients of the parametric polynomials are algebraically independent; cf. Remark 1.1 for a discusion of the general case.

Let $d \in \mathbb{N} \setminus \{0\}$ and $F_d[Z_0, \ldots, Z_n] = \{f \in F[Z_0, \ldots, Z_n], \deg(f) = d\}$ be the set of all the polynomials of degree *exactly* d. Then there exists a bijection between this set and the set $\mathcal{P} = \left(F^{\binom{n+d}{n}} \setminus \{(0, \ldots, 0)\}\right) \times F^{\binom{n+d}{n+1}}$ of the coefficients of these polynomials, which will be called the *parameter space* where the first factor corresponds to the monomials of degree d, the second corresponds to the monomials of degree less than d. Each $f = \sum_{|I| \leq d} a_I Z^I \in F_d[Z_0, \ldots, Z_n]$ is in bijection with the tuple $(a_I)_{|I| \leq d} \in \mathcal{P}$ where $I = (i_0, \ldots, i_n) \in \mathbb{N}^{n+1}$, $|I| = i_0 + \cdots + i_n$ is the weight of the $(n+1)$-tuples I and $Z^I = Z_0^{i_0} \cdots Z_n^{i_n}$, the family $\{a_I\}_{|I| \leq d}$ is the set of the parameters of the parametric polynomial f.

The input of the algorithm is the vector of parametric coefficients taking values in the *parameter space*. Its output consists of the three following items:

1) The decomposition of the *parameter space* into pairwise disjoint

pieces in the form:

$$\mathcal{P} = \bigsqcup_{1\leq i\leq (2d^2+1)^{2n+3d+5}} V_i,$$

where the symbol $\bigsqcup$ is a disjoint union.

2) Each piece V_i is presented as a constructible set defined by a quantifier-free formula of the first order theory of algebraically closed fields, i.e., the algorithm gives a finite family of polynomials $B_{i,\delta}^{(\beta)}$, $C_i^{(\beta)} \in F[\{a_I\}_{|I|\leq d}]$ such that $V_i = \bigcup_\beta \left\{\bigwedge_\delta (B_{i,\delta}^{(\beta)} = 0) \wedge (C_i^{(\beta)} \neq 0)\right\}$.

3) For each piece V_i, the absolute factorization of the polynomials with coefficients in V_i (by the bijection above) is given uniformly, i.e., there exist a positive integer $l_i \leq d$, l_i variables $C_1, \dots, C_{l_i}$ algebraically independent over F and rational functions $b_{J,j}^{(i)} \in F\left(\{a_I\}_{|I|\leq d}, C_1, \dots, C_{l_i}\right)$ such that for any polynomial f with coefficients $(a_I)_{|I|\leq d} \in W_i$, there exist $c_1, \dots, c_{l_i} \in \overline{F}$ with $f = \prod_j G_j$ and $G_j = \sum_{|J|} b_{J,j}^{(i)}\left(\{a_I\}_{|I|\leq d}, c_1, \dots, c_{l_i}\right) Z^J$ absolutely irreducible. Note that there exists a bounded number of possibilities for $c_1, \dots, c_{l_i}$ (see Remark 7.4).

The main result of this paper is to give explicitly all the pieces V_i (Corollary 6.2) and the rational functions $b_{J,j}^{(i)}$ for each V_i of the item 3) of the output of the algorithm (Theorem 7.3), and its complexity bound (Sec. 8).

Remark 1.1. In the case when the parameters are not independent, e.g., the parameters are contained in a constructible set $V \subset \mathcal{P}$ given as above, we consider the partition

$$V = \bigsqcup_{1\leq i\leq (2d^2+1)^{2n+3d+5}} \left(V_i \cap V\right).$$

Each set $V_i \cap V$ can be found by the algorithm of [5], [7] and the absolute factorization of parametric polynomials from $V_i \cap V$ can be represented as in 3). In this paper, we study the complexity of this algorithm only in the case where the parameters are independent (Sec. 8), i.e., we do not consider the complexity of representation of V.

Example. For $F = \mathbb{Q}$, we consider the parametric polynomial

$$f = (a^2 + b)X^2 + aXY + bX + aY + b$$

with two variables X and Y, a and b are the parameters. We obtain a decomposition of the parameter space in the form:

$$\mathbb{Q}^2 = W_1 \sqcup W_2 \sqcup W_3,$$

where $W_1 = \{(a,b) \in \mathbb{Q}^2,\ a^2 + b = 0\}$, for each $(a,b) \in W_1$ we have the absolute factorization

$$f = (X+1)(aY+b)$$

$W_2 = \{(a,b) \in \mathbb{Q}^2,\ a^2+b \neq 0,\ a \neq 0\}$, for each $(a,b) \in W_2$, f is absolutely irreducible. $W_3 = \{(a,b) \in \mathbb{Q}^2,\ a = 0, b \neq 0\}$, for each $(a,b) \in W_3$, we obtain

$$f = b(X-j)(X-j^2),$$

where j is a primitive cubic root of unity.

The tools used in this paper are the Hensel lemma and the *quantifier elimination* in the theory of algebraically closed fields [4].

In Secs. 2 and 3, we will present an initial decomposition of the *parameter space* (Corollary 2.2) with its complexity in order to prepare it to applying the parametric Hensel's lemma in Secs. 4 and 5. This lemma and the *quantifier elimination* will be used in Secs. 5, 6, and 7 to complete the decomposition of the *parameter space* (Theorem 7.3). A study of the total complexity of this algorithm will be made in Sec. 8.

That would be interesting to obtain a lower bound on the complexity of absolute factoring of parametric polynomials.

To the author's best knowledge, algorithms for factoring of parametric polynomials (and moreover, studying the complexity of the latter problem) have never been published.

Let us mention also that an algorithm for solving systems of parametric univariate polynomials was designed in [8].

In a forthcoming paper we are going to apply the described algorithm to solving parametric systems of multivariate algebraic equations.

2. Preparation to the Hensel lemma

Since the Hensel lemma which, will be used below (Lemma 4.1), is only applicable to the polynomials $f \in F[X, Y_1, \ldots, Y_n]$ monic as polynomials in X and $f_0(X) = f(X, 0, \ldots, 0)$ square-free in $F[X]$, one should partition the *parameter space* $\mathcal{P}$ into pairwise disjoint subsets W such that to each W one can uniformly associate a polynomial $g \in F(\{a_I\}_{|I|\leq d})[X, Y_1, \ldots, Y_n]$ (i.e., a polynomial whose coefficients are rational functions of the parameters $\{a_I\}_{|I|\le d}$) such that for each evaluation $\{a_I\}_{|I|\le d} \in W$ we obtain

$$lc_X(g) = 1, \quad g(X, 0, \dots, 0) \text{ is square-free in } F[X],$$

where $lc_X(g)$ denotes the leading coefficient of g w.r.t. X as a univariate polynomial in $F[Y_1, \dots, Y_n][X]$.

With an $(n+1) \times (n+1)$-matrix T with entries in F and $f \in F_d[Z_0, \dots, Z_n]$, we associate a polynomial $g_{f,T} \in F[X, Y_1, \dots, Y_n]$ defined by $g_{f,T}(X, Y_1, \dots, Y_n) = f(T(X, Y_1, \dots, Y_n))$.

For technical reasons w.l.o.g. one can suppose that $|F| \ge \max\{2d^2, r\}$ (in the case $\text{char}(F) = p > 0$).

Proposition 2.1. *One can produce explicitly a family* $\{T_1, \dots, T_{N_1}\}$ *of nonsingular matrices of the size* $(n+1) \times (n+1)$ *with coefficients in* F *such that for any polynomial* $f \in F[Z_0, \dots, Z_n]$ *of total degree* d*, there exists* $1 \le i \le N_1 = (d+1)^n$ *such that the polynomial* g_{f,T_i} *fulfils* $0 \ne lc_X(g_{f,T_i}) \in F$.

Proof. Let $f = \sum_{|I|\le d} a_I Z^I \in F_d[Z_0, \dots, Z_n]$ and $T = (t_{i,j})_{1\le i,j\le n+1}$, then

$$g_{f,T}(X, Y_1, \dots, Y_n) = \left(\sum_{i_0+\cdots+i_n=|I|=d} a_I t_{1,1}^{i_0} t_{2,1}^{i_1} \cdots t_{n+1,1}^{i_n} \right) X^d + h$$

with $\deg_X(h) < d$ and

$$0 \ne lc_X(g_{f,T}) = \sum_{i_0+\cdots+i_n=|I|=d} a_I t_{1,1}^{i_0} t_{2,1}^{i_1} \cdots t_{n+1,1}^{i_n} \in F[t_{1,1}, t_{2,1}, \dots, t_{n+1,1}]$$

is a homogeneous polynomial in $t_{1,1}, t_{2,1}, \dots, t_{n+1,1}$ of degree d, $\deg_{t_{i,1}}(lc_X(g_{f,T})) \le d$, $1 \le i \le n+1$.

We fix $b_0, \dots b_d \in F$, pairwise distinct (if $\text{char}(F) = 0$ then we take $b_i = i$ and if $\text{char}(F) = p > 0$, then $b_i \in F_{p^m}$ where $p^{m-1} \le d < p^m$). For each f fixed, there exists $(t_{1,1}, t_{2,1}, \dots, t_{n+1,1}) \in \{b_0, \dots b_d\}^{(n+1)}$ with $lc_X(g_{f,T})(t_{1,1}, t_{2,1}, \dots, t_{n+1,1}) \ne 0$, as can be easly seen by applying induction on n. Since $lc_X(g_{f,T})$ is homogeneous, one can take $t_{1,1} = 1$. As $\det(T) \ne 0$, thus we take

$$T = \begin{pmatrix} 1 & & & 0 \\ t_{2,1} & 1 & & \\ \vdots & & \ddots & \\ t_{n+1,1} & 0 & & 1 \end{pmatrix},$$

where the entries of the matrix T vanish except the first column and the diagonal. This completes the proof of the proposition by taking $N_1 = (d+1)^n$. $\square$

Proposition 2.1 implies that $\mathcal{P} = \bigcup_{1\le i\le N_1} W_i$, where $W_i = \{f \equiv (a_I)_{|I|\le d} \in \mathcal{P}, 0 \neq lc_X(g_{f,T_i}) \in F\}$.

Let $\widetilde{W_i} = W_i \setminus \bigcup_{1\le j<i} W_j$, $1 \le i \le N_1$, then

$$\mathcal{P} = \bigsqcup_{1\le i\le N_1} \widetilde{W_i}.$$

In the rest of this section, we decompose each $\widetilde{W_i}$ into constructible sets W and we associate to each W a parametric polynomial g with coefficients are rational functions of the parameters such that $g(X,0,\ldots,0)$ is squarefree in $F[X]$ for any value of the parameters in W.

Case $\mathrm{char}(F) = p > 0$**.** For all $f \equiv (a_I)_{|I|\le d} \in \widetilde{W_i}$, let t be the smallest integer such that p^t divides all the exponents of X in the monomials in $X, Y_1, \ldots, Y_n$ with nonzero coefficients of the polynomial $\frac{1}{lc_X(g_{f,T_i})} g_{f,T_i}(X, Y_1, \ldots, Y_n)$, then

$$\frac{1}{lc_X(g_{f,T_i})} g_{f,T_i}(X, Y_1, \ldots, Y_n) = g^{(t)}_{f,T_i}(X^{p^t}, Y_1, \ldots, Y_n)$$

with $g^{(t)}_{f,T_i}$ satisfying:

$$\frac{\partial}{\partial X}(g^{(t)}_{f,T_i}) \neq 0, \quad \deg_X(g^{(t)}_{f,T_i}) = dp^{-t}, \quad \deg_{Y_j}(g^{(t)}_{f,T_i}) \le d, \quad 1 \le j \le n,$$

where $g^{(t)}_{f,T_i}$ is monic as a polynomial in X and the coefficients of $g^{(t)}_{f,T_i}$ are rational functions of the parameters $\{a_I\}_{|I|\le d}$ and the factorization:

$$g^{(t)}_{f,T_i} = \prod_k g_k \quad \text{where the } \; g_k \; \text{ are absolutely irreducible}$$

provides the absolute factorization of f by means of using the inverse transformation T_i^{-1}.

Setting

$$\widetilde{W}_{i,t} = \left\{ f \in \widetilde{W_i},\ \frac{\partial}{\partial X}(g^{(t)}_{f,T_i}) \neq 0 \right\} \tag{1}$$

we get

$$\widetilde{W_i} = \bigsqcup_{0\le t\le \lfloor \frac{\log_2 d}{\log_2 p} \rfloor} \widetilde{W}_{i,t},$$

where $\lfloor * \rfloor$ is the integer part of $*$.

Case $\mathrm{char}(F) = 0$**.** We obtain $\widetilde{W}_i = \widetilde{W}_{i,0}$ which is defined by (1) under the convention $0^0 = 1$.

For any $f \equiv (a_I)_{|I| \le d} \in \widetilde{W}_{i,t}$, let

$$Disc_X(g^{(t)}_{f,T_i}) = \mathrm{res}_X\left(g^{(t)}_{f,T_i}, \frac{\partial}{\partial X}(g^{(t)}_{f,T_i})\right) \in F[Y_1, \ldots, Y_n].$$

Then

$$\deg_{Y_j}(Disc_X(g^{(t)}_{f,T_i})) \le d(2dp^{-t} - 1) = d_1,\ 1 \le j \le n.$$

Let $W^{(1)}_{i,t} = \{f \in \widetilde{W}_{i,t}, Disc_X(g^{(t)}_{f,T_i}) \equiv 0\}$, $W^{(2)}_{i,t} = \{f \in \widetilde{W}_{i,t}, Disc_X(g^{(t)}_{f,T_i}) \ne 0\}$, then

$$\widetilde{W}_{i,t} = W^{(1)}_{i,t} \sqcup W^{(2)}_{i,t}.$$

We fix $b_0, \ldots, b_{d_1} \in F$ pairwise distinct (if $\mathrm{char}(F) = p > 0$, one takes $b_i \in F_{p^m}$ where $p^{m-1} \le d_1 < p^m$). For each $f \in W^{(2)}_{i,t}$, there exists $c^{(j)} = (c^{(j)}_1, \ldots, c^{(j)}_n) \in \{b_0, \ldots, b_{d_1}\}^n$ such that $Disc_X(g^{(t)}_{f,T_i})(c^{(j)}) \ne 0$, as can be easily seen by applying induction on n, then $g^{(t)}_{f,T_i}(X, c^{(j)}_1, \ldots, c^{(j)}_n)$ is square-free in $F[X]$.

For $g^{(t,j)}_{f,T_i}(X, Y_1, \ldots, Y_n) = g^{(t)}_{f,T_i}(X, Y_1 + c^{(j)}_1, \ldots, Y_n + c^{(j)}_n)$ the following holds : $g^{(t,j)}_{f,T_i}$ is monic as a polynomial in X; $g^{(t,j)}_{f,T_i}(X, 0, \ldots, 0)$ is square-free in $F[X]$; $\deg_X(g^{(t,j)}_{f,T_i}) = dp^{-t}$; $\deg_{Y_1,\ldots,Y_n}(g^{(t,j)}_{f,T_i}) \le d$ and its coefficients are rational functions of the parameters $\{a_I\}_{|I| \le d}$. For the decomposition $g^{(t,j)}_{f,T_i} = \prod_k h_k$ into absolutely irreducible factors h_k, then

$$\begin{aligned} g^{(t)}_{f,T_i}(X, Y_1, \ldots, Y_n) &= g^{(t,j)}_{f,T_i}(X, Y_1 - c^{(j)}_1, \ldots, Y_n - c^{(j)}_n) \\ &= \prod_k h_k(X, Y_1 - c^{(j)}_1, \ldots, Y_n - c^{(j)}_n) \end{aligned}$$

is an absolute factorization of $g^{(t)}_{f,T_i}$.

Let

$$\begin{aligned} W^{(2,j)}_{i,t} &= \{f \in W^{(2)}_{i,t},\ Disc_X(g^{(t)}_{f,T_i})(c^{(j)}) \ne 0\} \\ &= \{f \in W^{(2)}_{i,t},\ g^{(t,j)}_{f,T_i}(X, 0, \ldots, 0) \text{ is square-free in } F[X]\}. \end{aligned}$$

Then

$$W^{(2)}_{i,t} = \bigcup_{1 \le j \le N_2} W^{(2,j)}_{i,t} \quad \text{where , } N_2 = (d_1 + 1)^n.$$

To obtain a partition of $W_{i,t}^{(2)}$ one puts $\widetilde{W}_{i,t}^{(2,j)} = W_{i,t}^{(2,j)} \setminus \bigcup_{1\le j_1<j} W_{i,t}^{(2,j_1)}$, $1 \le j \le N_2$. Then

$$W_{i,t}^{(2)} = \bigsqcup_{1\le j\le N_2} \widetilde{W}_{i,t}^{(2,j)}.$$

Note that $G_{f,T_i}^{(t)} = GCD\left(g_{f,T_i}^{(t)}, \frac{\partial}{\partial X}(g_{f,T_i}^{(t)})\right)$ is a nontrivial divisor of $g_{f,T_i}^{(t)}$ and $1 \le \deg_X(G_{f,T_i}^{(t)}) \le dp^{-t}-1$ for any $f \in W_{i,t}^{(1)}$.
One sets $\widetilde{W}_{i,t}^{(1,j')} = \{f \in W_{i,t}^{(1)},\ \deg_X(G_{f,T_i}^{(t)}) = j'\}$. Then

$$W_{i,t}^{(1)} = \bigsqcup_{1\le j'\le dp^{-t}-1} \widetilde{W}_{i,t}^{(1,j')}.$$

We represent $G_{f,T_i}^{(t)}$ in the form $G_{f,T_i}^{(t)} = A_{dp^{-t}-1}X^{dp^{-t}-1} + \cdots + A_1X + A_0$ where the A_i's are rational functions in $Y_1, \ldots, Y_n$ and in the parameters. Then $\widetilde{W}_{i,t}^{(1,j')}$ is a constructible set defined by the following equations and inequation:

$$A_{dp^{-t}-1} = \cdots = A_{j'+1} = 0,\ A_{j'} \ne 0.$$

For each $f \in \widetilde{W}_{i,t}^{(1,j')}$, the polynomial $G_{f,T_i}^{(t,j')} = \frac{g_{f,T_i}^{(t)}}{G_{f,T_i}^{(t)}}$ satisfies the following: $G_{f,T_i}^{(t,j')}$ is monic as a polynomial in X; $G_{f,T_i}^{(t,j')}(X,0,\ldots,0)$ is square-free in $F[X]$; $\deg_X(G_{f,T_i}^{(t,j')}) = dp^{-t} - j'$; $\deg_{Y_1,\ldots,Y_n}(G_{f,T_i}^{(t,j')}) \le d$ and its coefficients are rational functions of the parameters $\{a_I\}_{|I|\le d}$.

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

Corollary 2.2. *The parameter space $\mathcal{P}$ is decomposed into $M_1 \le (2d^2+1)^{2n+2}$ disjoint subsets in the form:*

$$\mathcal{P} = \bigsqcup_{1\le i\le N_1} \bigsqcup_{0\le t\le \lfloor \frac{\log_2 d}{\log_2 p}\rfloor} \left(\bigsqcup_{1\le j'\le dp^{-t}-1} \widetilde{W}_{i,t}^{(1,j')} \bigsqcup \bigsqcup_{1\le j\le N_2} \widetilde{W}_{i,t}^{(2,j)} \right).$$

3. Complexity of the preparatory partition of the *parameter space*

Definition 3.1. 1) *The length of an element $a \in F_{p^m}$ is equal to $\log_2 p^m$.* 2) *For an integer a, we denote by $l(a)$ its binary length that is defined in* [10].

3) *The length of a polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$, denoted by $l(f)$, is the maximum of the lengths of its coefficients in $\mathbb{Z}$.*

Properties of the lengths
i) If $a, b \in \mathbb{Z} \setminus \{0\}$, then

$$\max\{l(a), l(b)\} \leq l(a+b) \leq \max\{l(a), l(b)\} + 1$$

and

$$l(a) + l(b) - 1 \leq l(ab) \leq l(a) + l(b).$$

ii) If $f, g \in \mathbb{Z}[X_1, \ldots, X_n]$ then $l(f+g) \leq \max\{l(f), l(g)\} + 1$ and $l(fg) \leq l(f) + l(g) + 1$.

If $\mathrm{char}(F) = 0,\ b_i = i,\ 0 \leq i \leq d,\ |b_i| \leq d$ then $l(b_i) \leq \log_2 |b_i| \leq \log_2 d$.

If $\mathrm{char}(F) = p > 0,\ b_i \in F_{p^m}$ with $p^{m-1} \leq d_1 < p^m$ then $l(b_i) \leq \log_2(p^m) \leq \log_2(pd_1) \leq \log_2(2pd^2)$.

The evaluation of the homogeneous polynomial $lc_X(g_{f,T_i})$ of degree d at the point $(t_{1,1}, \ldots, t_{n+1,1}) \in \{b_0, \ldots, b_d\}^{n+1}$ can be executed in $\left(\binom{n+1+d}{n+1} - 3\right)$ multiplications and $\left(\binom{n+d}{n} - 1\right)$ additions in F. Hence the construction of all the $\widetilde{W}_i$ costs $C_1 = N_1 \left(\binom{n+1+d}{n+1} + \binom{n+d}{n} \right) \leq (d+2)^{2n+1}$ arithmetic operations in F and its binary complexity can be bounded as follows:
if $F = \mathbb{Q}$ by

$$C_1' \leq N_1 \left(\binom{n+1+d}{n+1} O(d^2 (\log_2 d)^2) + \binom{n+d}{n} O(d \log_2 d) \right)$$
$$\leq (d+2)^{2n+1} O\Big(d^2 (\log_2 d)^2\Big).$$

and if $F = \mathbb{F}_p$ by

$$C_1' \leq (d+2)^{2n+1} O\Big((\log_2 p)^2\Big).$$

The complexity of the computation of $Disc_X(g_{f,T_i}^{(t)})$ is $O\left((2dp^{-t} - 1)^{2.376}\right) \leq O(d^{2.376})$ [9].

The construction of all $\widetilde{W}_{i,t}^{(2,j)}$ costs $C_2 = N_2 \binom{n+d_1}{n} \leq (2d^2+1)^{2n}$ arithmetic operations in F. Its binary complexity can be bounded as follows:

if $F = \mathbb{Q}$ by

$$C_2' \leq N_2 \binom{n+d_1}{n} \Big(O\Big(d^2(\log_2 d)^2\Big) + O\Big(d \log_2 d\Big) \Big)$$
$$\leq (2d^2+1)^{2n} O\Big(d^2(\log_2 d)^2\Big).$$

and if $F = \mathbb{F}_p$ by

$$C_2' \leq (2d^2+1)^{2n} O\Big((\log_2 p)^2\Big).$$

The complexity of the computation of $G^{(t)}_{f,T_i}$ is $O\Big(d^2(dp^{-t})^2\Big) \leq O(d^4)$. Thus the total complexity of this partition of the *parameter space* is $C \leq C_1 + C_2 + O(d^{2.376}) + O(d^4) \leq O\Big((2d^2+1)^{2n+1}\Big)$. Its binary complexity is
if $F = \mathbb{Q}$

$$C' \leq (2d^2+1)^{2n+1} O\Big(d^2(\log_2 d)^2\Big).$$

and if $F = \mathbb{F}_p$

$$C' \leq (2d^2+1)^{2n+1} O\Big((\log_2 p)^2\Big).$$

4. Hensel's lemma

We want at the second stage to parametrize the Hensel lemma (see, e.g., [5, 7, 10, 15, 17, 18] and [20]).

Lemma 4.1. *Let $R_N = F[Y_1, \ldots, Y_n]/((Y_1, \ldots, Y_n)^N)$, where $1 \leq N < \infty$, and $R_\infty = F[Y_1, \ldots, Y_n]$.*
Let $N > 1$ and $g \in R_N[X]$ satisfy the following properties:
(H1) *$lc_X(g) = 1$.*
(H2) *$g_0(X) = g(X, 0, \ldots, 0)$ is square-free in $F[X]$.*
Then for each decomposition of g_0 in the form $g_0 = g_0^{(1)} \cdots g_0^{(s)}$ where $g_0^{(1)}, \ldots, g_0^{(s)} \in F[X]$ are monic, the following holds:
For each multi-index $I \in \mathbb{N}^n$ such that $N > |I| \geq 1$, there exist unique polynomials $g_I^{(1)}, \ldots, g_I^{(s)} \in F[X]$ which satisfy the following:
i) *$\deg(g_I^{(j)}) < \deg(g_0^{(j)})$, $|I| \geq 1$, $1 \leq j \leq s$*
ii) *In the completion of $R_N[X]$ w.r.t. $(Y_1, \ldots, Y_n)$ one has decomposition*
$g = G^{(1)} \cdots G^{(s)}$, where $G^{(j)} = g_0^{(j)} + \sum_{|I|\geq 1} g_I^{(j)} Y^I, \quad 1 \leq j \leq s.$

For $N' < N$ the decomposition ii) of the image of g under the natural homomorphism $\nu : R_N[X] \to R_{N'}[X]$ is obtained by applying ν.

Proof. The last part of the lemma is obvious. To prove the rest, note that for any ideal $I \subseteq F[Y_1, \ldots, Y_n] = F[Y]$ the completion of $F[Y]$ w.r.t. $(Y_1, \ldots, Y_n)$ equals $F[[Y]]/IF[[Y]]$ (see e.g. page 179 of [6]). This observation with $I = (Y_1, \ldots, Y_n)^N$, and e.g. [6] (Thm 7.18 and Ex. 7.22) completes the proof. (Cf. also [5, 7, 17, 18].) □

Let us write g in the form $g = g_0 + \sum_{|I|\geq 1} g_I Y^I$ where $g_I \in F[X]$, $\deg(g_I) < \deg(g_0)$ because $lc_X(g) = 1$.
The condition ii) of Lemma 4.1 is equivalent to:

$$g_I = \sum_{\cup_{0\leq l\leq s} J_l = I} \prod_{0\leq k\leq s} g_{J_k}^{(k)}.$$

Then

$$g_I = \sum_{1\leq j\leq s} g_0^{(1)} \cdots g_0^{(j-1)} g_I^{(j)} g_0^{(j+1)} \cdots g_0^{(s)} + V_I, \quad |I| \geq 1. \qquad (2)$$

where V_I depends only on the polynomials $g_J^{(j)}$, $|J| < |I|$, $1 \leq j \leq s$.
Thus for $|I|$ fixed, the coefficients of $g_I^{(1)}, \ldots, g_I^{(s)}$ form a vector of F^d which is the unique solution of the linear system $Bx = b$ obtained by (2), where B is a $d \times d$ matrix whose coefficients depend only on the coefficients of $g_0^{(1)}, \ldots, g_0^{(s)}$ (B is invertible by the uniqueness of $g_I^{(1)}, \ldots, g_I^{(s)}$ in Lemma 4.1).
In the case when $s = 2$, we obtain that $B = Sylv(g_0^{(1)}, g_0^{(2)})$ is the Sylvester matrix of $g_0^{(1)}$ and $g_0^{(2)}$.
One sets $g_I^{(j)} = \sum_{0\leq i<k_j} \alpha_i^{(j,I)} X^i$, $g_0^{(j)} = X^{k_j} + \sum_{0\leq i<k_j} \alpha_i^{(j)} X^i$, $1 \leq j \leq s$,
where $k_j = \deg(g_0^{(j)})$, $\deg(g_0) = d = \sum_j k_j$, and $g_I = \sum_{0\leq i<d} b_{i,I} X^i$.

Theorem 4.2. *Under the assumptions of Lemma 4.1, for each $|I| \geq 1$, the coefficients of $g_I^{(j)}$, $1 \leq j \leq s$ are rational functions of the coefficients of $g_0^{(1)}, \ldots, g_0^{(s)}$ and the coefficients of g as follows:*

$$\alpha_i^{(j,I)} = \frac{P_i^{(j,I)}}{(\det(B))^{2|I|-1}}, \quad 1 \leq j \leq s, \quad 0 \leq i < k_j.$$

where $P_i^{(j,I)}$ is a polynomial whose variables are the coefficients of $g_0^{(1)}, \ldots, g_0^{(s)}$ and the coefficients of g. Its coefficients are in the field

H where $H=\mathbb{Q}$ if $\mathrm{char}(F)=0$ *and* $H=F_p$ *if* $\mathrm{char}(F)=p>0$, $\deg_{\alpha_i^{(j)}}(P_i^{(j,I)})\leq(2|I|-1)(d-1)(s-1)$, $\deg_{\alpha_i^{(j)}}(\det(B))\leq(d-1)(s-1)$.

Proof. We give the proof in the case $s=2$, the general case is analogous to it.
For $s=2$, we prove the theorem by induction on $|I|$.
For $|I|=1$, let us write the Cramer formulas of the linear system $Bx=b$ (see above):
$\alpha_i^{(j,I)}=\frac{\det(\Delta)}{\det(B)}$ where Δ is the matrix obtained starting from B by replacing a certain column (which corresponds to j,i) by the vector b which is formed in this case only by the coefficients $b_{i,I}$ of g_I.
By developing $\det(\Delta)$ according to the column b, one obtains: $\det(\Delta)=\sum_{0\leq i\leq d-1}(-1)^{\epsilon_{i,j}}b_{i,I}\det(B_i)$, where B_i is a submatrix of B, then $\deg_{\alpha_i^{(1)},\alpha_i^{(2)}}(\det(\Delta))\leq d-1$, thus take $P_i^{(j,I)}=\det(\Delta)$.
Let us suppose that this property is true until $|I|=t\geq 1$. For $|I|=t+1$, the coefficients of b are given by:

$$b_{d-1}=b_{d-1,I}, b_i=b_{i,I}-\sum_{1\leq|J|\leq|I|-1}\sum_{0\leq l\leq i}\alpha_l^{(1,J)}\alpha_{i-l}^{(2,I-J)},\quad 0\leq i\leq d-2.$$

By using the induction hypothesis one obtains:

$$b_i=\frac{1}{(\det(B))^{2|I|-2}}\left(b_{i,I}(\det(B))^{2|I|-2}-\sum_{1\leq|J|\leq t}\sum_{0\leq l\leq i}P_l^{(1,J)}P_{i-l}^{(2,I-J)}\right).$$

Also the Cramer formulas give: $\alpha_i^{(j,I)}=\frac{\det(\Delta)}{\det(B)}$, one again develops $\det(\Delta)$ with respect to b:

$$\det(\Delta)=\sum_{0\leq i\leq d-1}(-1)^{\epsilon_{i,j}}b_i\det(B_i)=(-1)^{\epsilon_{d-1,j}}b_{d-1,I}\det(B_{d-1})$$

$$+\frac{1}{(\det(B))^{2|I|-2}}\sum_{0\leq i\leq d-2}(-1)^{\epsilon_{i,j}}\Bigg(b_{i,I}(\det(B))^{2|I|-2}$$

$$-\sum_{1\leq|J|\leq t}\sum_{0\leq l\leq i}P_l^{(1,J)}P_{i-l}^{(2,I-J)}\Bigg)\det(B_i),$$

thus $\alpha_i^{(j,I)} = \frac{P_i^{(j,I)}}{(\det(B))^{2|I|-1}}$ with

$$\begin{aligned}\deg_{\alpha_i^{(1)},\alpha_i^{(2)}}(P_i^{(j,I)}) &\le \max\{(2|I|-2+1)(d-1), (2|J|-1)(d-1)\\ &+(2|I-J|-1)(d-1)+(d-1)\}\\ &\le (2|I|-1)(d-1). \qquad \square\end{aligned}$$

5. Partition of the parameter space by the Hensel lemma

We fix i,t,j and the set $W = \widetilde{W}_{i,t}^{(2,j)}$ as in Sec. 2 (in the case where $\mathrm{char}(F) = 0$, we have $t = 0$, $0^0 = 1$). We associated to W a polynomial $g = g_{f,T_i}^{(t,j)} \in F(\{a_I\}_{|I|\le d})[X, Y_1, \dots, Y_n]$ (i.e., a polynomial with coefficients are rational functions of the parameters $\{a_I\}_{|I|\le d}$) such that for any evaluation $\{a_I\}_{|I|\le d} \equiv f \in W$ we obtain $lc_X(g) = 1$, $g(X, 0, \dots, 0)$ is square-free in $F[X]$, $\deg_X(g) = dp^{-t}$ and $\deg_{Y_1,\dots,Y_n}(g) \le d$ (then g satisfies the conditions of Lemma 4.1).

Let $k = (k_1, \dots, k_s)$ be a partition of dp^{-t}, i.e $dp^{-t} = k_1 + \cdots + k_s$, $k_1 \ge \cdots \ge k_s$, one associates to this partition a subset $U_k^{(2)}$ of W defined by: $U_k^{(2)}$ is the set of the tuples $f \equiv (a_I)_{|I|\le d} \in W$ such that the associated polynomial $g = X^{dp^{-t}} + \sum_{0\le|I|\le d, 0\le i<dp^{-t}} b_{i,I}X^iY^I = g_0 + \sum_{1\le|I|\le d} g_IY^I$ satisfies the following condition: (H3): there exist monic $g_0^{(1)}, \dots, g_0^{(s)} \in \overline{F}[X]$, $\deg(g_0^{(j)}) = k_j$, $\quad 1 \le j \le s$, $g_0 = g_0^{(1)} \cdots g_0^{(s)}$ and such that by application of Lemma 4.1 one obtains a factorization of g. In other terms the elements $G^{(j)}$ $(1 \le j \le s)$ given by Lemma 4.1 are in $\overline{F}[X, Y_1, \dots, Y_n]$. The conditions that the $G^{(j)}$'s are polynomials are called the termination conditions.

For each $0 \le |I| \le d$ and $0 \le i < dp^{-t}$, $b_{i,I}$ is a rational function of the parameters in the form:

$$b_{i,I} = \frac{S_{i,I}^{(2)}}{R_{i,I}^{(2)}} \quad \text{with} \quad S_{i,I}^{(2)}, R_{i,I}^{(2)} \in F[\{a_J\}_{|J|\le d}]$$

where $R_{i,I}^{(2)}(\{a_J\}_{|J|\le d}) \ne 0$ for all $(a_J)_{|J|\le d} \in W$. The condition $g_0 = g_0^{(1)} \cdots g_0^{(s)}$ is equivalent to:

$$S_{i,0}^{(2)}(\{a_J\}_{|J|\le d}) = R_{i,0}^{(2)}(\{a_J\}_{|J|\le d}) \sum_{0=l_0\le l_1\le\cdots\le l_s=i} \prod_{1\le m\le s} \alpha_{l_m-l_{m-1}}^{(m)}. \quad (3)$$

with $0 \le i \le dp^{-t} - 1$, $\alpha_{k_j}^{(j)} = 1, \quad 1 \le j \le s$.

Lemma 5.1. *Let I be a multi-index such that $|I| > d$, then $g_I^{(j)} = 0$ for all $1 \leq j \leq s$ if and only if $V_I = 0$, for V_I defined in (2).*

Proof. Since $g_I = 0$ (because $\deg_{Y_1,\dots,Y_n}(g) \leq d$), $V_I = 0$ if and only if the right-hand side b of the linear system $Bx = b$ is zero this equivalent to that this system admits 0 as its unique solution, which proves the lemma. $\square$

Theorem 5.2. *The termination conditions are equivalent to $V_I = 0$, $d < |I| \leq sd$.*

Proof. The termination conditions are equivalent to $\deg_{Y_1,\dots Y_n}(G^{(j)}) \leq d$ for all $1 \leq j \leq s$, thus equivalent to $g_I^{(j)} = 0$ for all $1 \leq j \leq s$ and $|I| > d$, and by Lemma 5.1 to the equalities $V_I = 0, \quad |I| > d$. We shall prove the theorem in the case $s = 2$, the general case is considered in a similar way.

If $s = 2$ then $V_I = \sum_{1 \leq |J| \leq |I|-1} g_J^{(1)} g_{I-J}^{(2)}$. The only thing to show is that $V_I = 0$ for all $d < |I| \leq 2d$ imply $V_I = 0$ for all $|I| > d$. Lemma 5.1 gives $g_I^{(1)} = g_I^{(2)} = 0, \quad d < |I| \leq 2d$, we shall show by induction on t that $V_I = 0, \quad |I| = d + t, \quad t \geq d + 1$. Indeed, for $t = d + 1$ ($|I| = 2d + 1$), we get

$$V_I = \sum_{1 \leq |J| \leq 2d} g_J^{(1)} g_{I-J}^{(2)} = \sum_{1 \leq |J| \leq d} g_J^{(1)} g_{I-J}^{(2)} + \sum_{d < |J| \leq 2d} g_J^{(1)} g_{I-J}^{(2)}$$

for $d < |J| \leq 2d, \quad g_J^{(1)} = 0$, then the second quantity in the right hand side is zero and for $1 \leq |J| \leq d$ one obtains $d < |I - J| \leq 2d$ and $g_{I-J}^{(2)} = 0$, and hence the first item in the right hand side is zero, so $V_I = 0$. Let us suppose now that $V_I = 0, \quad d < |I| \leq d + t, \quad t \geq d + 1$. For $|I| = d + t + 1$ one has

$$V_I = \sum_{1 \leq |J| \leq d+t} g_J^{(1)} g_{I-J}^{(2)} = \sum_{1 \leq |J| \leq d} g_J^{(1)} g_{I-J}^{(2)} + \sum_{d < |J| \leq d+t} g_J^{(1)} g_{I-J}^{(2)}$$

for $d < |J| \leq d + t$, one obtains $g_J^{(1)} = 0$ (by the inductive hypothesis) and for $1 \leq |J| \leq d$ one obtains $d < |I - J| \leq d + t$ and $g_{I-J}^{(2)} = 0$, thus $V_I = 0$. $\square$

Now we give the equations on the parameters those are equivalent to the termination conditions by Theorem 5.2. Each polynomial $V_I \in F[X]$ is given by (2), depends only on the polynomials $\{g_J^{(j)}\}_{|J| < |I|, 1 \leq j \leq s}$.

Replacing the coefficients of the polynomials $\{g_J^{(j)}\}_{1\leq |J|\leq sd, 1\leq j\leq s}$ in the termination conditions $V_I = 0$, $d < |I| \leq sd$ by their values given in Theorem 4.2, one obtains polynomial equations of the form:

$$Q_i^{(I)} = 0, \quad d < |I| \leq sd, \quad 0 \leq i \leq dp^{-t} - 2. \qquad (4)$$

Each $Q_i^{(I)}$ is a polynomial whose variables are the coefficients $\alpha_i^{(j)}$ of $g_0^{(1)}, \ldots, g_0^{(s)}$ and the parameters $\{a_J\}_{|J|\leq d}$, being its coefficients are in H.

Corollary 5.3. *For all $d < |I| \leq sd$, $0 \leq i \leq dp^{-t} - 2$ one has:*

$$\begin{aligned}\deg_{\alpha_i^{(j)}}(Q_i^{(I)}) &\leq 2(|I|-1)(dp^{-t}-1)(s-1)\\ &\leq 2(sd-1)(dp^{-t}-1)(s-1).\end{aligned}$$

Proof (case $s = 2$).

$$Q_i^{(I)} = \sum_{1\leq |J| < |I|, 0\leq l\leq i} P_l^{(1,J)} P_{i-l}^{(2,I-J)}$$

$$\begin{aligned}\deg_{\alpha_i^{(j)}}(Q_i^{(I)}) &\leq (2|J|-1)(dp^{-t}-1) + (2|I-J|-1)(dp^{-t}-1)\\ &= 2(|I|-1)(dp^{-t}-1). \qquad \square\end{aligned}$$

Corollary 5.4. *Let $k = (k_1, \ldots, k_s)$, $s \geq 2$ be a partition of dp^{-t}, then $U_k^{(2)}$ is the set of the tuples $(a_I)_{|I|\leq d} \in W$ satisfying the formula:*

$$\exists\ \alpha_i^{(j)}, \quad 1 \leq j \leq s, \quad 0 \leq i < k_j \quad \text{which satisfy (3) and (4).} \qquad (5)$$

Proof. It given by Theorem 5.2 and the above description. $\square$

Lemma 5.5 (Hadamard inequality) [10]. *Let $A = (a_{ij})$ be a $n \times n$ real matrix, $b_1, \ldots, b_n \in \mathbb{R}^n$ be its columns and $L \in \mathbb{R}$ be an upper bound of the absolute values of a_{ij}. Then*

$$|\det(A)| \leq \|b_1\| \ldots \|b_n\| \leq n^{\frac{n}{2}} L^n,$$

where

$$\|b_j\| = \left(\sum_{1\leq i\leq n} |a_{ij}|^2\right)^{\frac{1}{2}}, \quad 1 \leq j \leq n.$$

Now we will establish an upper bound $M^{(2)}$ on the binary lengths of the polynomials $Q_i^{(I)}$, $d < |I| \leq sd$, $0 \leq i \leq dp^{-t} - 2$ of (7.2).
If $\mathrm{char}(F) = p > 0$ then $H = F_p$, one takes $M^{(2)} = \log_2 p$.
If $\mathrm{char}(F) = 0$ then $H = \mathbb{Q}$, in this case one starts to calculate an upper bound on the lengths of the polynomials $P_i^{(j,I)}$ by the following theorem.

Theorem 5.6. *For all $1 \leq j \leq s$, $0 \leq i \leq k_j - 1$, $|I| \geq 1$ one has:*

$$l(P_i^{(j,I)}) \leq \left(\frac{2|I| - 1}{2}\right)(dp^{-t} - 1)\log_2(dp^{-t} - 1) + 6|I| - 4.$$

Proof. We show the theorem only in the case $s = 2$, for $s \geq 3$ one obtains the same bound (independent of s), therefore we assume $s = 2$, one shows this theorem by induction on $|I|$. For $|I| = 1$,

$$P_i^{(j,I)} = \det(\Delta) = \sum_{0 \leq i \leq dp^{-t}-1} (-1)^{\epsilon_{i,j}} b_{i,I} \det(B_i),$$

where Δ is given by the proof of Theorem 4.2, let us apply the Hadamard inequality to $\det(B_i)$: $L = 1$ is an upper bound on the absolute values of the coefficients of the monomials of B_i in $\alpha_i^{(j)}$, then

$$|\text{coefficients of } \det(B_i)| \leq (dp^{-t} - 1)^{\frac{dp^{-t}-1}{2}} . 1^{(dp^{-t}-1)} = (dp^{-t} - 1)^{\frac{dp^{-t}-1}{2}},$$

hence

$$\begin{aligned} l(\text{coefficients of } \det(B_i)) &\leq \log_2 |\text{coefficients of } \det(B_i)| + 1 \\ &= \frac{(dp^{-t} - 1)}{2} \log_2(dp^{-t} - 1) + 1, \end{aligned}$$

thus,

$$l(P_i^{(j,I)}) \leq \max_i \{l(\det(B_i))\} + 1 \leq \frac{(dp^{-t} - 1)}{2} \log_2(dp^{-t} - 1) + 2.$$

Let us suppose that for all $|J| < |I|$ one has:

$$l(P_i^{(j,J)}) \leq \left(\frac{2|J| - 1}{2}\right)(dp^{-t} - 1)\log_2(dp^{-t} - 1) + 6|J| - 4.$$

In the proof of Theorem 4.2 one has obtained:

$$P_i^{(j,I)} = (-1)^{\epsilon_{dp^{-t}-1,j}} b_{dp^{-t}-1,I} \det(B_{dp^{-t}-1})(\det(B))^{2|I|-2}$$

$$+\sum_{0\le i\le dp^{-t}-2}(-1)^{\epsilon_{i,j}}\Big(b_{i,I}(\det(B))^{2|I|-2}$$
$$-\sum_{1\le|J|<|I|}\sum_{0\le l\le i}P_l^{(1,J)}P_{i-l}^{(2,I-J)}\Big)(\det(B_i))$$

$l(\det(B))$, $l(\det(B_i)) \le \frac{(dp^{-t}-1)}{2}\log_2(dp^{-t}-1)+1$.

By property ii) of the lengths, we get

$$l\left((\det(B))^{2|I|-2}\right)\le(|I|-1)(dp^{-t}-1)\log_2(dp^{-t}-1)+4|I|-5,$$

hence

$$l\left(b_{i,I}\det(B_i)(\det(B))^{2|I|-2}\right)$$
$$\le\frac{(2|I|-1)}{2}(dp^{-t}-1)\log_2(dp^{-t}-1)+4|I|-3=(*)$$

and by the inductive hypothesis we obtain

$$l\left(\det(B_i)P_l^{(1,J)}P_{i-l}^{(2,I-J)}\right)$$
$$\le\frac{(2|I|-1)}{2}(dp^{-t}-1)\log_2(dp^{-t}-1)+6|I|-5=(**),$$

so

$$l(P_i^{(j,I)})\le\max\{(*),(**)\}+1=(**)+1$$
$$=\frac{(2|I|-1)}{2}(dp^{-t}-1)\log_2(dp^{-t}-1)+6|I|-4$$

which proves the theorem. □

Corollary 5.7. *For all $d<|I|\le sd$, $0\le i\le dp^{-t}-2$ one has:*

$$l(Q_i^{(I)})\le(|I|-1)(dp^{-t}-1)\log_2(dp^{-t}-1)+6(|I|-1)$$
$$\le(sd-1)(dp^{-t}-1)\log_2(dp^{-t}-1)+6(sd-1).$$

Proof (case $s=2$). We know that:

$$Q_i^{(I)}=\sum_{1\le|J|<|I|,0\le l\le i}P_l^{(1,J)}P_{i-l}^{(2,I-J)},$$

thus

$$l(Q_i^{(I)})\le\max_{l,J}\left\{l\left(P_l^{(1,J)}P_{i-l}^{(2,I-J)}\right)\right\}+1$$
$$=(|I|-1)(dp^{-t}-1)\log_2(dp^{-t}-1)+6(|I|-1).$$ □

Corollary 5.8. *The number of equations in* (5) *is* $N^{(2)} = (dp^{-t} - 1)\left(\binom{n+sd}{n} - \binom{n+d}{n}\right) + dp^{-t}$, *the number of quantifiers is* dp^{-t}, *the degrees of its equations as a polynomials in* $\alpha_i^{(j)}$, $1 \le j \le s$, $0 \le i < k_j$ *are less than* $D^{(2)} = 2(sd-1)(dp^{-t}-1)(s-1)$ *and* $M^{(2)} = (sd-1)(dp^{-t} - 1)\log_2(dp^{-t}-1) + 6(sd-1)$ *in the case when* $\mathrm{char}(F) = 0$ *(or, respectively,* $M^{(2)} = \log_2 p$ *if* $\mathrm{char}(F) = p > 0$*) is an upper bound on the lengths of its equations.*

6. Quantifier elimination

An algorithm is described in [4] which eliminates the quantifiers in a formula of the form:

$$\exists X_1, \dots, X_s \Big(\bigwedge_{1 \le j \le k} f_j(z_1, \dots, z_{n-s}, X_1, \dots, X_s) = 0 \Big), \tag{6}$$

where $f_1, \dots, f_k \in H[Z_1, \dots, Z_{n-s}, X_1, \dots, X_s]$, $\deg_{X_1,\dots,X_s}(f_j) < d$, $l(f_j) \le M$, $1 \le j \le k$. The complexity bound of this algorithm is given by the following lemma.

Lemma 6.1. *The set* $U = \{(z_1, \dots, z_{n-s}) \in \overline{F}^{n-s}, (6)\}$ *is a constructible set given by*

$$\bigcup_{\beta} \Big\{ \bigwedge_{\delta} (B_\delta^{(\beta)} = 0) \wedge (C^{(\beta)} \ne 0) \Big\}$$

where

$$B_\delta^{(\beta)},\ \ C^{(\beta)} \in H[Z_1, \dots, Z_{n-s}],\ \ \deg_{Z_1,\dots,Z_{n-s}}(B_\delta^{(\beta)}) \le (kd)^{4(n+2)(2s+3)},$$

$$\deg_{Z_1,\dots,Z_{n-s}}(C^{(\beta)}) \le (3kd)^{2s+3},\ \ l(B_\delta^{(\beta)}) \le M\Big((kd)^{(s+1)n}\Big)^{O(1)},$$

$$l(C^{(\beta)}) \le M\Big((kd)^{(s+1)}\Big)^{O(1)},\ \ \delta \le (s+1)^2(3kd)^{4(2s+3)(n+2)},$$

$$\beta \le (kd)^{12(s+2)(n+s+3)}$$

with a polynomial complexity in

$$M,\ \ (kd)^{sn^2},\ \ p,$$

where $p = \mathrm{char}(H)$.

By application of Lemma 6.1 to (5) and by taking into account the estimates of Corollary 5.8, one obtains:

Corollary 6.2. *Let k be a partition of dp^{-t}, then one can produce the decomposition*

$$U_k^{(2)} = \bigcup_\beta \left\{ \bigwedge_\delta (B_\delta^{(\beta)} = 0) \wedge (C^{(\beta)} \neq 0) \right\},$$

where

1) $B_\delta^{(\beta)}, C^{(\beta)} \in H[\{a_I\}_{|I| \leq d}]$
2) $\deg_{a_I}(B_\delta^{(\beta)}) \leq (N^{(2)}D^{(2)})^{4(dp^{-t}+r+2)(2dp^{-t}+3)}$
3) $\deg_{a_I}(C^{(\beta)}) \leq (3N^{(2)}D^{(2)})^{2dp^{-t}+3}$
4) $l(B_\delta^{(\beta)}) \leq M^{(2)} \left((N^{(2)}D^{(2)})^{(dp^{-t}+1)(dp^{-t}+r)}\right)^{O(1)}$
5) $l(C^{(\beta)}) \leq M^{(2)} \left((N^{(2)}D^{(2)})^{(dp^{-t}+1)}\right)^{O(1)}$
6) $\delta \leq (dp^{-t}+1)^2 \left(3N^{(2)}D^{(2)}\right)^{4(2dp^{-t}+3)(dp^{-t}+r+2)}$
7) $\beta \leq \left(N^{(2)}D^{(2)}\right)^{12(dp^{-t}+2)(2dp^{-t}+r+3)}$

with a polynomial complexity in

$$M^{(2)}, \quad \left(N^{(2)}D^{(2)}\right)^{dp^{-t}(dp^{-t}+r)^2}, \quad p,$$

where $p = \operatorname{char}(H)$, $r = \binom{n+1+d}{n+1}$ is the number of parameters, $N^{(2)}$, $D^{(2)}$, and $M^{(2)}$ are as in Corollary 5.8.

Definition 6.3. *One says that a partition $k' = (k'_1, \ldots, k'_h)$ of dp^{-t} is finer than a partition $k = (k_1, \ldots, k_s)$ of dp^{-t} if for all $1 \leq l \leq s$, we have $k_l = k'_{i_l} + k'_{i_l+1} + \cdots + k'_{i_{l+1}-1}$ for certain $1 \leq i_1 < \cdots < i_s \leq h$.*

Proposition 6.4. *If k' is finer than k then $U_{k'}^{(2)} \subset U_k^{(2)}$.*

Thus

$$W = \bigcup_{k \in pt(dp^{-t})} U_k^{(2)} = \bigsqcup_{k \in pt(dp^{-t})} \widetilde{U}_k^{(2)},$$

where $pt(dp^{-t})$ is the set of all the partitons of dp^{-t}. $\widetilde{U}_k^{(2)} = U_k^{(2)} \setminus \bigcup_{k' \neq k} U_{k'}^{(2)}$, the union ranges over all the partitions k' of dp^{-t} being finer than k.

Corollary 6.5. *Any polynomial $f \equiv (a_I)_{|I|\leq d} \in \widetilde{U}_k^{(2)}$ is factorized absolutely in a product of irreducible factors in $\overline{F}[Z_0, \ldots, Z_n]$ uniformly, i.e the coefficients of its factors are rational functions of the parameters $\{a_I\}_{|I|\leq d}$ and $\{\alpha_i^{(j)}\}_{1\leq j\leq s, 0\leq i<k_j}$.*

Proof. For all $f \in \widetilde{U}_k^{(2)}$, the polynomial $g \in F[X, Y_1, \ldots, Y_n]$ factorizes absolutely in a product of irreducible factors in $\overline{F}[X, Y_1, \ldots, Y_n]$ and the coefficients of its factors are rational functions of its coefficients and $\{\alpha_i^{(j)}\}_{1\leq j\leq s, 0\leq i<k_j}$ (Theorem 4.2), which proves the corollary by taking into account that the factorization of g involves that of f by the section 2 and that the coefficients of g are rational functions of the parameters $\{a_I\}_{|I|\leq d}$. □

7. Final partition of the parameter space

We fix i, t, j' and the set $W' = \widetilde{W}_{i,t}^{(1,j')}$ as in the Sec. 2. We associated to W' a polynomial $g' = G_{f,T_i}^{(t,j')} \in F(\{a_I\}_{|I|\leq d})[X, Y_1, \ldots, Y_n]$ such that for all evaluation $\{a_I\}_{|I|\leq d} \equiv f \in W'$ we obtain $lc_X(g') = 1$, $g'(X, 0, \ldots, 0)$ is square-free in $F[X]$, $\deg_X(g') = dp^{-t} - j'$ and $\deg_{Y_1,\ldots,Y_n}(g') \leq d$. We decompose W' in the same way as in Sec. 5.

Definition 7.1. *Let $k = (k_1, \ldots, k_s)$ be a partition of $dp^{-t} - j'$, then $U_k^{(1)}$ is the set of the tuples $f \equiv (a_I)_{|I|\leq d} \in W'$ such that there exist monic $g_0^{(1)}, \ldots, g_0^{(s)} \in \overline{F}[X]$, $\deg(g_0^{(j)}) = k_j$, $1 \leq j \leq s$ and $g'(X, 0, \ldots, 0) = g_0^{(1)} \cdots g_0^{(s)}$ and by application of Lemma 4.1 one obtains a factorization of g' in $\overline{F}[X, Y_1, \ldots, Y_n]$.*

A similar study (by application of the Hensel lemma on g' and the quantifier elimination as in Secs. 5 and 6) shows that one can produce $U_k^{(1)}$ as a constructible set with a polynomial complexity in

$$M^{(1)}, \quad (N^{(1)}D^{(1)})^{(dp^{-t}-j')(dp^{-t}-j'+r)^2}, \quad p,$$

where $N^{(1)} = (dp^{-t} - j' - 1)\left(\binom{n+sd}{n} - \binom{n+d}{n}\right) + dp^{-t} - j'$, $D^{(1)} = 2(sd - 1)(dp^{-t} - j' - 1)(s - 1)$, $M^{(1)} = (sd - 1)(dp^{-t} - j' - 1)\log_2(dp^{-t} - j' - 1) + 6(sd - 1)$, (we set $M^{(1)} = \log_2 p$ if $\mathrm{char}(F) = p > 0$). Thus

$$W' = \bigcup_{k\in pt(dp^{-t}-j')} U_k^{(1)} = \bigsqcup_{k\in pt(dp^{-t}-j')} \widetilde{U}_k^{(1)},$$

where $\widetilde{U}_k^{(1)} = U_k^{(1)} \setminus \bigcup_{k' \neq k} U_{k'}^{(1)}$, the union ranges over all the partitions k' of $dp^{-t} - j'$ being finer than k.

For all $f \equiv (a_I)_{|I| \leq d} \in \widetilde{U}_k^{(1)}$ where $k = (k_1, \dots, k_s)$ is a partition of $dp^{-t} - j'$, one obtains an absolute factorization of g' as a product of irreducible factors $G_1, \dots, G_s \in \overline{F}[X, Y_1, \dots, Y_n]$, $\deg_X G_i = k_i$, then $g_{f,T_i}^{(t)} = G_1^{\alpha_1} \cdots G_s^{\alpha_s}$ with $k_1(\alpha_1 - 1) + \cdots + k_s(\alpha_s - 1) = j'$. For each $\alpha = (\alpha_1, \dots, \alpha_s)$ such that $k_1(\alpha_1 - 1) + \cdots + k_s(\alpha_s - 1) = j'$ one puts:

$$\widetilde{U}_k^{(1,\alpha)} = \{f \in \widetilde{U}_k^{(1)},\ g_{f,T_i}^{(t)} = G_1^{\alpha_1} \cdots G_s^{\alpha_s}\}$$

then

$$\widetilde{U}_k^{(1)} = \bigsqcup_{\alpha} \widetilde{U}_k^{(1,\alpha)}.$$

Corollary 7.2. *Any polynomial $f \equiv (a_I)_{|I| \leq d} \in \widetilde{U}_k^{(1,\alpha)}$ factorizes absolutely in a product of irreducible factors in $\overline{F}[Z_0, \dots, Z_n]$ uniformly (i.e., as in Corollary 6.5).*

Proof. For $f \in \widetilde{U}_k^{(1,\alpha)}$, $g' = G_1 \cdots G_s$ and $g_{f,T_i}^{(t)} = G_1^{\alpha_1} \cdots G_s^{\alpha_s}$, the coefficients of G_i are rational functions of the coefficients of $g_{f,T_i}^{(t)}$ and $\{\alpha_i^{(j)}\}_{1 \leq j \leq s, 0 \leq i < k_j}$, which proves the corollary by taking into account the fact that the inverse transformation T_i^{-1} makes it possible to pass from the factorization of $g_{f,T_i}^{(t)}$ to that of f and that the coefficients of $g_{f,T_i}^{(t)}$ are rational functions of the parameters $\{a_I\}_{|I| \leq d}$. $\square$

We summarize the results of the preview sections in the following theorem, which uses the notations introduced previously in these sections.

Theorem 7.3. *The described algorithm yields a partition of the parameter space $\mathcal{P}$ as a union of M_1 constructible sets of the forms:*

$$W = \bigsqcup_{k \in pt(dp^{-t})} \widetilde{U}_k^{(2)}$$

and

$$W' = \bigsqcup_{k \in pt(dp^{-t} - j')} \bigsqcup_{\alpha} \widetilde{U}_k^{(1,\alpha)}.$$

The total number of pieces does not exceed $(2d^2 + 1)^{2n+3d+5}$. Each of these pieces is given by a system of algebraic equations and inequations (see Corollary 6.2). For each piece $\widetilde{U}_k^{(1,\alpha)}$ (respectively, $\widetilde{U}_k^{(2)}$), there exist *a positive integer* $l_k^{(1,\alpha)} = dp^{-t} - j' \leq d$ *(respectively* $l_k^{(2)} = dp^{-t} \leq d$*),* $l_k^{(1,\alpha)}$ *variables* $\{\Theta_i^{(j)}\}_{1\leq j\leq s, 0\leq i<k_j}$ *algebraically independent over* F *(respectively* $l_k^{(2)}$ *variables) and rational functions*

$$b_{k,I',j'}^{(1,\alpha)} \in F\Big(\{a_I\}_{|I|\leq d}, \{\Theta_i^{(j)}\}_{1\leq j\leq s,0\leq i<k_j}\Big)$$

(respectively, $b_{k,I',j'}^{(2)}$*), such that for any polynomial* $f \in F_d[Z_0, \ldots, Z_n]$ *with coefficients* $(a_I)_{|I|\leq d}$ *in* $\widetilde{U}_k^{(1,\alpha)}$ *(respectively* $\widetilde{U}_k^{(2)}$*) there exist* $\{\theta_i^{(j)}\}_{1\leq j\leq s,0\leq i<k_j} \in \overline{F}^{l_k^{(1,\alpha)}}$ *(respectively,* $\overline{F}^{l_k^{(2)}}$ *) with* $f = \prod_{j'} G_{j'}$ *where*

$$G_{j'} = \sum_{|I'|} b_{k,I',j'}^{(1,\alpha)}\Big(\{a_I\}_{|I|\leq d}, \{\theta_i^{(j)}\}_{1\leq j\leq s,0\leq i<k_j}\Big)Z^{I'}$$

is absolutely irreducible.

Proof. By Corollaries 6.5 and 7.2, it remains to compute the number of pieces. For a positive integer h, the number of elements of $pt(h)$ does not exceed

$$\begin{aligned}\sum_{2\leq s\leq h}\binom{h-1+s-1}{s} &\leq \sum_{2\leq s\leq h}(h-1)^s \\ &\leq \frac{(h-1)^{h-1}-1}{h-2}(h-1)^2 \leq h^{h+1}.\end{aligned}$$

We apply this bound to $h = dp^{-t} - j'$, $h = dp^{-t}$ $(h \leq d)$, thus the number of pieces N is bounded by:

$$\begin{aligned}N &= M_1\Big(\operatorname{card}(pt(dp^{-t} - j'))\Big)^2 \operatorname{card}(pt(dp^{-t})) \\ &\leq (2d^2+1)^{2n+2}(2d^2+1)^{3(d+1)} \leq (2d^2+1)^{2n+3d+5}. \qquad \square\end{aligned}$$

Remark 7.4. Since the factorization is unique, we observe that for any f there exists just a finite number of $\theta_i^{(j)}$ (which correspond to permutations of factors) and the degree of the extension $F[\{\theta_i^{(j)}\}_{1\leq j\leq s,0\leq i<k_j}]$ of F is bounded by $d!$, because this extension is contained in the splitting field of the polynomial $g(X, 0, \ldots, 0)$ (respectively $g'(X, 0, \ldots, 0)$).

8. Analysis of the binary complexity of the algorithm

For each multi-index I, the calculation of the coefficients of $g_I^{(j)}$, $1 \leq j \leq s$ (solving the linear system $Bx = b$) costs $O\Big((dp^{-t})^{2.376}\Big) \leq O(d^{2.376})$, therefore the complexity of the calculation of $g_I^{(j)}$, $1 \leq j \leq s$, $1 \leq |I| \leq sd$ is less than $\binom{n+sd}{n} O(d^{2.376}) \leq (sd+1)^n O(d^{2.376}) \leq (d^2 + 1)^n O(d^{2.376})$ because $s \leq dp^{-t} \leq d$. We have $M^{(1)}, M^{(2)} \leq d^3 \log_2 d + 6d^2$ (in the case $\mathrm{char}(F) = 0$), $N^{(1)}, N^{(2)} \leq d\Big((d^2+1)^n + 1\Big)$, $D^{(1)}, D^{(2)} \leq 2d^4$ and $r = \binom{n+1+d}{n+1} \leq (d+1)^{n+1}$. The complexity (Corollary 6.2) of the construction of all $\widetilde{U}_k^{(1)}$ (or $\widetilde{U}_k^{(2)}$) is

$$C_3 \leq d^{d+1} \left(2d^5 \Big((d^2+1)^n + 1 \Big) \right)^{O\left(d(d+r)^2\right)} \leq d^{O(ndr^2)}$$

and its binary complexity is if $F = \mathbb{Q}$

$$C_3' \leq \left(d^2 \Big(d \log_2 d + 6 \Big) d^{ndr^2} \right)^{O(1)} \leq d^{O(ndr^2)}$$

and if $F = \mathbb{F}_p$

$$C_3' \leq \Big(p d^{ndr^2} \Big)^{O(1)}.$$

Since $\deg_{X, Y_1, \ldots, Y_n}(g_{f,T_i}) \leq d$, then the computation of $g_{f,T_i}^{(t)}$ is performed in $C_4 = r \leq (d+1)^{n+1}$ multiplications in F. On the other hand if $F = \mathbb{Q}$, $l(lc_X(g_{f,T_i})) \leq d \log_2 d$ and if $F = \mathbb{F}_p$, $l(lc_X(g_{f,T_i})) \leq \log_2 p$, then the binary complexity C_4' of the calculation of $g_{f,T_i}^{(t)}$ can be bounded as follows: if $F = \mathbb{Q}$ by

$$C_4' \leq r O\Big(d^2 (\log_2 d)^2 \Big) \leq (d+1)^{n+1} O\Big(d^2 (\log_2 d)^2 \Big)$$

and if $F = \mathbb{F}_p$ by

$$C_4' \leq (d+1)^{n+1} O\Big((\log_2 p)^2 \Big).$$

Thus the total complexity C_t of the algorithm in Theorem 7.3 is bounded by:

$$C_t \leq C + (d^2+1)^n O(d^{2.376}) + C_3 + C_4.$$

So

$$C_t \le d^{O(ndr^2)}$$

and the total binary complexity C'_t is bounded as follows:
if $F = \mathbb{Q}$ by

$$C'_t \le d^{O(ndr^2)}$$

and if $F = \mathbb{F}_p$ by

$$C'_t \le \left(pd^{ndr^2}\right)^{O(1)}.$$

Acknowledgment. The author thanks D. Grigoriev and the Anonymous Referees for valuable remarks.

References

1. A. V. Aho, J. E. H. Hopcroft, J. D. Ullman, *The design and analysis of computer algorithms.* — Reading, Mass., Menlo Park, Cal., London, Addison-Wesley Publishing Company (1974).
2. E. R. Berlekamp, *Factoring polynomials over finite fields.* — Bell Systems Tech. J. **46** (1967), 1853–1859.
3. E. R. Berlekamp, *Factoring polynomials over large finite fields.* — Math. Comp. **24** (1970), 713–735.
4. A. Chistov, D. Grigoriev, *Complexity of quantifier elimination in the theory of algebraically closed fields.* — LNCS **176** (1985), 17–31.
5. A. L. Chistov, *Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time.* — J. Sov. Math. **34**, No. 4 (1986), 1838–1882.
6. D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry.* — Springer, New York (1995).
7. D. Grigoriev, *Factorization of polynomials over a finite field and the solution of systems of algebraic equations.* — J. Sov. Math. **34**, No. 4 (1986), 1762–1803.
8. D. Grigoriev, *Complexity of quantifier elimination in the theory of ordinary differential equations.* — Lect. Notes Computer Science **378** (1989), 11–25.
9. D. Coppersmith, S. Winograd, *Matrix multiplication via arithmetic progressions.* In: Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing (1987), pp. 1–6.
10. J. von zur Gathen, J. Gerhard. *Modern Computer algebra.* — Cambridge University Press (1999).
11. J. von zur Gathen, E. Kaltofen, *Factorization of multivariate polynomials over finite fields.* — Math. Comp. **45**, No. 171 (1985), 251–261.
12. E. Kaltofen, *On the complexity of factoring polynomials with integer coefficients.* — PhD Thesis, Rensselaer Polytechnic Instit., Troy, N. Y., December (1982).
13. E. Kaltofen, *Factorization of polynomials.* — Computer Algebra, Springer, Vienna (1983), pp. 95-113.

14. A. K. Lenstra, H. W. Lenstra (Jr), L. Lovasz, *Factoring polynomials with rational coefficients.* — Math. Ann. **261**, No. 4 (1982), 515–534.
15. M. Mignotte, D. Stefanescu, *Polynomials. An Algorithmic Approach.* — Springer (1999).
16. M. Mignotte, *Mathématiques pour le calcul formel.* — Presses Univ. de France, Paris (1989).
17. D. R. Musser, *Multivariate polynomial factorization.* — J. ACM **22**, Issue 2 (1975), 291–308.
18. D. R. Musser, *Algorithms for polynomial factorization.* — PhD Thesis and TR 134, Univ. Wisconsin (1971).
19. J-F. Ragot, *Sur la factorisation absolue des polynômes.* — Thèse à l'université de Limoges, Decembre (1997).
20. H. Zassenhaus, *On Hensel factorization.* — J. Number Theory **1** (1969), 291–311.

IRMAR, Campus de Beaulieu,
Université de Rennes 1,
France

E-mail: ali.ayad@univ-rennes1.fr

Поступило 2 декабря 2004 г.