Decomposition of multihomogeneous polynomials: minimal number of variables

Jérémy Berthomieu

Decomposition of multihomogeneous polynomials: minimal number of variables

Jérémy Berthomieu
Laboratoire d'Informatique de Paris 6
UMR CNRS 7606, CR INRIA Paris – Rocquencourt
Université Pierre-et-Marie-Curie, Équipe-projet PolSys
Boîte courrier 169, 4 place Jussieu
75252 Paris Cedex 05 FRANCE
jeremy.berthomieu@lip6.fr

ABSTRACT

In this paper, we generalize Hironaka's invariants, the ridge and the directrix, of homogeneous ideals, to multihomogeneous ideals. These invariants are the minimal number of additive polynomials or linear forms to write a given ideal. We design algorithms to compute both these invariants which make use of the multihomogeneous structure of the ideal and study their complexities depending on the number of blocks of variables, the number of variables in each block and the degree of the polynomials spanning the considered ideal. We report our implementation in MAPLE using FGB library.

Keywords

Functional decomposition, Algebraic system resolution, Multihomogeneous polynomials, Invariants, Complexity.

1. INTRODUCTION

In the field of homogeneous polynomial systems solving, the problem of decomposing polynomials is classical. Indeed, as the complexity is exponential in the number of variables, decomposing the polynomials might be seen as a way to reduce the number of variables involved in the system. For instance, given a system of homogeneous polynomials $(F_1(X_1,\ldots,X_n),\ldots,F_r(X_1,\ldots,X_n))$, with coefficients in a field $\mathbb{K}$. One would want to determine polynomials $(G_1,\ldots,G_r) \in \mathbb{K}[U_1,\ldots,U_e]$ and $(H_1,\ldots,H_e) \in \mathbb{K}[X_1,\ldots,X_n]$ such that $F_i(X_1,\ldots,X_n) = G_i(H_1,\ldots,H_e)$ for all i. In this case, if $e < n$, then $U_1,\ldots,U_e$ can be seen as new variables. Then, it remains to solve new systems involving $H_j(X_1,\ldots,X_n)$ whose degrees are lesser than the original system.

In [10, 11], the authors study the case where $e = n$ and all polynomials G_i have the same degree. In [1], the authors are interested in the case where $H_1,\ldots,H_e$ are homogeneous additive polynomials or linear forms. They determine an algorithm to compute the least number of additive polynomial $H_1,\ldots,H_e$, called the *ridge*, such that $\exists G_i(U_1,\ldots,U_e)$ such that $F_i = G_i(H_1,\ldots,H_e)$. Furthermore, whenever the field of coefficients is perfect, then they can also determine the least number of linear forms $L_1,\ldots,L_c$, the *directrix*, such that $F_i = G_i(L_1,\ldots,L_c)$. Therefore, it allows one to retrieve the least number of a polynomial system.

A motivation to compute the ridge and the directrix comes from the *desingularization problem*. Thanks to Hironaka's work [16, 17, 18], the desingularization problem is well understood when $F_1,\ldots,F_r$ are defined over a field $\mathbb{K}$ of characteristic 0. However, because in characteristic p the *ridge* can define a singular variety, Hironaka's work cannot be easily transposed to the positive characteristic case. In consequence, one cannot effectively desingularize any variety of dimension 3 or more in characteristic p (see [5, 6] for a theoretical, but non effective, proof of threefolds desingularization).

In this paper, we are interested in the case of multihomogeneous polynomial systems [12, 21, 23, 24]. First of all, it is not clear that the ridge and the directrix as defined and computed in [1, 15] will preserve the multihomogeneous structure of the ideal. For instance, let us take a bilinear form $F = X_1Y_1 + X_2Y_1 + X_1Y_2 + X_2Y_2$. It is clear that F is bilinear in $\mathbf{X} = (X_1, X_2)$ and $\mathbf{Y} = (Y_1, Y_2)$. Furthermore, it can be factored as $F = (X_1 + X_2)(Y_1 + Y_2)$ which is the first step in the Gaussian reduction of quadratic form. However, in this algorithm, one has to do one more step which is writing $F = \frac{1}{4}[(X_1+X_2+Y_1+Y_2)^2-(X_1+X_2-Y_1-Y_2)^2]$. While at the end of the first step of the Gaussian reduction, F is written with two linear forms $L_1 = X_1 + X_2$, $L_2 = Y_1 + Y_2$ which are themselves bihomogeneous in $(\mathbf{X}, \mathbf{Y})$, at the end of the second step, because the variables are mixed altogether, the two linear forms $(X_1 + X_2) \pm (Y_1 + Y_2)$ are not. Furthermore, it must be noticed that this second step does not reduce the number of variables to write the equation.

Another classical transformation on polynomials, namely univariate ones, is Tschirnhaus transformation (see [28, 29]). For instance, if F is a univariate polynomial in X of degree n, it can allow one to make the term in X^{n-1} vanish. However, problems occur if $n-1$ is not invertible in $\mathbb{K}$.

Our algorithm can be seen as a generalization of Tschirnhaus transformation and Gaussian reduction of quadratic forms, without the second step described above for the latter, yielding only multihomogeneous polynomial in the same

ISSAC '13 Boston, Massachusetts USA

blocks of variables as the input.

In particular, our algorithm for computing the ridge makes use of the multihomogeneous structure of the system to improve the complexity compared to the algorithm of [1] and and lead to important speed-ups.

1.1 Organization of the paper

In order to be self-contained, we recall the definitions of the *ridge* and the *directrix* of a homogeneous ideal and extend their definitions to multihomogeneous ideals in Section 2. In Section 3, we prove the existence and the uniqueness of the ridge for the multihomogeneous case. We give an algorithm to compute it in Section 3.2 and study its complexity in Section 3.3. In Section 4, we show how to retrieve the directrix from the ridge when the field of coefficients is perfect and design an algorithm dedicated to this in Section 4.2. Unfortunately, when the field of coefficient is not perfect, computing the directrix can be difficult (see Section 4.3) and we do not know any exact method to manage this case. Finally, in Section 5, we give timings of our implementation in Maple [20] using FGb library [9].

1.2 Notations

Let $\mathbb{K}$ be a field of any characteristic. Let $X_1, \ldots, X_n$ be n variables, we will denote $\mathbf{X} = (X_1, \ldots, X_n)$.

For a multi-index $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$, we will write $|\mathbf{a}| = a_1 + \cdots + a_n$ and will denote $\mathbf{X}^{\mathbf{a}} = X_1^{a_1} \cdots X_n^{a_n}$. Then, the degree of $\mathbf{X}^{\mathbf{a}}$ is $|\mathbf{a}|$.

We recall that a polynomial $F \in \mathbb{K}[\mathbf{X}] = \mathbb{K}[X_1, \ldots, X_n]$ is homogeneous of degree d if every monomials in F has degree d.

Let $n_1, \ldots, n_m$, and $d_1, \ldots, d_m$ be in $\mathbb{N}$ and let $\mathbf{X}_1 = (X_{1,1}, \ldots, X_{1,n_1}), \ldots, \mathbf{X}_m = (X_{m,1}, \ldots, X_{m,n_1})$ be variables over $\mathbb{K}$. We will say that $F \in \mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$ is *multihomogeneous* of multidegree $(d_1, \ldots, d_m)$ if, for each i, F is homogeneous of degree d_i for the set of variables $\mathbf{X}_i$. This is equivalent to asking that every monomial $\mathbf{X}_1^{\mathbf{a}_1} \cdots \mathbf{X}_m^{\mathbf{a}_m}$ of F has multidegree $(d_1, \ldots, d_m)$. An ideal $I \in \mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$ is also said *multihomogeneous* if it can be spanned by multihomogeneous polynomials.

It is clear and classical that a multihomogeneous polynomial in $(\mathbf{X}_1, \ldots, \mathbf{X}_m)$ is homogeneous in all the variables $(X_{1,1}, \ldots, X_{1,n_1}, \ldots, X_{m,n_m})$, of degree $d_1 + \cdots + d_m$.

Given any monomial ordering $\succ$, we denote $\mathrm{lm}(F)$, the leading monomial of a polynomial F for $\succ$. For an ideal I, $\mathrm{lm}(I)$ stands for the ideal spanned by monomials $\mathrm{lm}(F)$, for all $F \in I$. Unless specified otherwise, we will only use the degree reverse lexicographic (DRL, see [7]) ordering such that $X_{1,1} \succ \cdots \succ X_{1,n_1} \succ \cdots \succ X_{m,n_m}$ when computing Gröbner bases.

When talking about a polynomial of degree a p-power p^ℓ, we will only mean "of degree 1" in characteristic $p = 0$.

2. RIDGE AND DIRECTRIX

2.1 Definitions

First of all, let us recall the definition of additive polynomials.

Definition 1. A polynomial $H \in \mathbb{K}[X_1, \ldots, X_n]$ is *additive* if $H(\mathbf{X} + \mathbf{Y}) = H(X_1 + Y_1, \ldots, X_n + Y_n) = H(\mathbf{X}) + H(\mathbf{Y})$.

Remark 1. *It is clear that linear forms are additive polynomials. In fact, in characteristic* 0*, these are the only ones. However, because in characteristic p Frobenius map is an endomorphism, many more polynomials are additive. Indeed, in* $\mathbb{K}[X_1, \ldots, X_n]$*, the* $\mathbb{K}$*-vector subspace of additive polynomials is spanned by monomials* $\left\{X_1^{p^\ell}, \ldots, X_n^{p^\ell} \,\middle|\, \ell \in \mathbb{N}\right\}$.

Let $H = \sum_{1 \le j \le n} a_j X_j^{p^\ell}$ *be a homogeneous additive polynomial over* $\mathbb{K}$ *of characteristic* $p > 0$*. Field* $\mathbb{K}$ *is perfect if, and only if, every element of* $\mathbb{K}$ *is a pth power and thus a* p^ℓ*th power. In fact, each* $a \in \mathbb{K}$ *is the pth power of a unique element of* $\mathbb{K}$*, and thus, the* p^ℓ*th power of another unique element of* $\mathbb{K}$*. Therefore* H *is the* p^ℓ*th power of a unique linear form*

$$L = \sum_{1 \le j \le n} \sqrt[p^\ell]{a_j} X_j.$$

Definition 2. Let I be a multihomogeneous ideal of polynomial ring $\mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$.

The *ridge* of I is the smallest set of additive polynomials $\mathbf{H}_1 = (H_{1,1}, \ldots, H_{1,e_1}), \ldots, \mathbf{H}_m = (H_{m,1}, \ldots, H_{m,e_m})$ such that

$$\forall\, i, j,\ 1 \le i \le m,\ 1 \le j \le e_i,\ H_{i,j} \in \mathbb{K}[\mathbf{X}_i],$$

$$I = (I \cap \mathbb{K}[\mathbf{H}_1, \ldots, \mathbf{H}_m])\mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m].$$

That is, the smallest set of additive polynomials allowing one to write I.

Likewise, the *directrix* of I is the smallest set of linear forms $\mathbf{L}_1 = (L_{1,1}, \ldots, L_{1,c_1}), \ldots, \mathbf{L}_m = (L_{m,1}, \ldots, L_{m,c_m})$ such that

$$\forall\, i, j,\ 1 \le i \le m,\ 1 \le j \le c_i,\ L_{i,j} \in \mathbb{K}[\mathbf{X}_i],$$

$$I = (I \cap \mathbb{K}[\mathbf{L}_1, \ldots, \mathbf{L}_m])\mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m].$$

That is, the smallest set of variables allowing one to write I.

Example 2. *Let* I *be the ideal of* $\mathbb{F}_3[\mathbf{X}, \mathbf{Y}]$ *where* $\mathbf{X} = (X_1, X_2, X_3)$ *and* $\mathbf{Y} = (Y_1, Y_2, Y_3)$ *spanned by* $F_1 = (X_1 + X_2 + X_3)^3 Y_1^2 + X_3^3 (Y_2 + Y_3)^2$ *and* $F_2 = (X_1 + X_2)^3 (Y_1 - Y_2 - Y_3)^3$.

Let $L_1 = X_1 + X_2$*,* $L_2 = X_3$*,* $M_1 = Y_1$ *and* $M_2 = Y_2 + Y_3$*, then one can write* $F_1 = (L_1 + L_2)^3 M_1^2 + L_2^3 M_2^3$ *and* $F_2 = L_1^3 (M_1 - M_2)^3$*. Thus, the directrix of* I *is the set* $\{\mathbf{L} = (L_1, L_2), \mathbf{M} = (M_1, M_2)\}$.

Furthermore, as cubing is additive over $\mathbb{F}_3$*, one can also write* $F_1 = (L_1^3 + L_2^3) M_1^2 + L_2^3 M_2^2$ *and* $F_2 = L_1^3 (M_1^3 - M_2^3)$*. Thus,* F_1 *and* F_2 *are polynomials in* $H_1 = L_1^3$*,* $H_2 = L_2^3$*,* $K_1 = M_1$ *and* $K_2 = M_2$*. So that the ridge of* I *is* $\{\mathbf{H} = (H_1, H_2), \mathbf{K} = (K_1, K_2)\}$.

Remark 3. *The original definitions of the ridge and the directrix of a homogeneous ideal* $I \subseteq \mathbb{K}[X_1, \ldots, X_n]$ *(see [1, 15, 18]) only mention the existence of the smallest sets of additive polynomials* $H_1, \ldots, H_e$ *and linear forms* $L_1, \ldots, L_c$ *such that*

$$I = (I \cap \mathbb{K}[H_1, \ldots, H_e])\mathbb{K}[X_1, \ldots, X_n],$$
$$I = (I \cap \mathbb{K}[L_1, \ldots, L_c])\mathbb{K}[X_1, \ldots, X_n].$$

We prove in Section 3, that the fact that a generator the ridge or the directrix can be written in only one set of variables $\mathbf{X}_i$ *is true.*

In Example 2, it seems that the directrix was computed first and the ridge last. In fact, the ridge is easier to compute and the directrix is retrieved from the ridge.

2.2 Hasse-Schmidt derivatives

The algorithm for computing the ridge is based on the computation of the partial derivatives of the given polynomials. This method is classical, see [4, 10, 11]. However, in characteristic p, problems occur when computing the derivatives of monomials with powers greater than p. This is why, we rather use the defined below Hasse-Schmidt derivatives.

Definition 3. Let $F \in \mathbb{K}[\mathbf{X}]$ be a polynomial of degree d. Hasse-Schmidt derivatives $\mathrm{D}^{\mathbf{X}}_{\mathbf{a}} F$ of F are the coefficients appearing in the following Taylor expansion:

$$F(\mathbf{X}+\mathbf{Y}) = \sum_{0\leq|\mathbf{a}|\leq d} \mathrm{D}^{\mathbf{X}}_{\mathbf{a}} F(\mathbf{X})\mathbf{Y}^{\mathbf{a}}.$$

Remark 4. *In characteristic 0, these are just classical partial derivatives multiplied by the right factorial.*

Example 5. *Let us give an example in positive characteristic $p \neq 2$. Let $F(X) = X^{2p}$, then $F(X+Y) = X^{2p} + 2X^pY^p + Y^{2p}$.*
Thus, $\mathrm{D}^X_0 F(X) = X^{2p}$, $\mathrm{D}^X_p F(X) = 2X^p$ and $\mathrm{D}^X_{2p} F(X) = 1$, while $\frac{\mathrm{d}^k F}{\mathrm{d}X^k}(X) = 0$ if $k > 0$.

The following Giraud's Lemma makes use of these Hasse-Schmidt derivatives.

Lemma 6 ([15], Lemma I.5.4.3). *Given any monomial ordering on variables $\mathbf{X}$. If $F_1, \ldots, F_r$ are homogeneous generators of an ideal $I \subseteq \mathbb{K}[\mathbf{X}]$, satisfying $\mathrm{D}^{\mathbf{X}}_{\mathbf{a}} F_i(\mathbf{X}) = 0$ whenever $\mathbf{X}^{\mathbf{a}} \in (\mathrm{lm}(I))$ and $|\mathbf{a}| < \deg F_i$, for $1 \leq i \leq r$, then the ridge of I is spanned by the $\mathrm{D}^{\mathbf{X}}_{\mathbf{a}} F_i(\mathbf{X})$ with $\mathbf{a} \in \mathbb{N}^n$ and $|\mathbf{a}| < \deg F_i$.*
Such a family of generators is called a Giraud basis *of I.*

Proposition 7. *Let $I \subseteq \mathbb{K}[\mathbf{X}]$ be an ideal spanned by homogeneous polynomials $(F_1, \ldots, F_r)$, all of degree d. Then, $(F_1, \ldots, F_r)$ is already a Giraud basis of I*

Proof. This is a direct consequence of Lemma 6. Since $\deg F_1 = \cdots = \deg F_r = d$, if $\mathbf{X}^{\mathbf{a}} \in (\mathrm{lm}(I))$, then $|\mathbf{a}| \geq d$. Therefore, $F_1, \ldots, F_r$ naturally verify the hypotheses on $\mathrm{D}^{\mathbf{X}}_{\mathbf{a}} F_i$ and they form a Giraud basis. □

Proposition 8. *Any minimal reduced Gröbner basis of I is a Giraud basis.*

Proof. Let us assume that $(F_1, \ldots, F_r)$ is a minimal reduced Gröbner basis of I such that $\deg F_1 \leq \cdots \leq \deg F_r$. Let $\mathbf{a} \in \mathbb{N}^n$ be such that $|\mathbf{a}| < \deg F_i$. If a monomial $\mathbf{Y}^{\mathbf{a}}$ appears in $F_i(\mathbf{X}+\mathbf{Y})$, then it is coming from the expansion of (at least one) $(\mathbf{X}+\mathbf{Y})^{\mathbf{b}}$, where $\mathbf{X}^{\mathbf{a}} \mid \mathbf{X}^{\mathbf{b}}$, and thus $\mathbf{X}^{\mathbf{b}}$ appears in $F_i(\mathbf{X})$. If such a $\mathbf{X}^{\mathbf{a}}$ is in $(\mathrm{lm}(I))$, then it is a multiple of one of the monomials $\mathrm{lm}(F_1), \ldots, \mathrm{lm}(F_{i-1})$. Therefore, so is $\mathbf{X}^{\mathbf{b}}$. This contradicts the fact that $(F_1, \ldots, F_r)$ is a minimal reduced Gröbner basis of I. □

3. MINIMIZING THE NUMBER OF ADDITIVE POLYNOMIALS

3.1 Main result

Let I be an ideal of $\mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$. Let us recall that I is multihomogeneous if it can be spanned by multihomogeneous polynomials $(F_1, \ldots, F_r)$.

As a homogeneous ideal, the ridge of I exists. In this section, we will prove that the ridge of I verifies the assumptions of Definition 1 and we will use the multihomogeneous structure to compute this ridge.

Theorem 9. *The ridge of I as a multihomogeneous ideal is the ridge of I as a homogeneous ideal.*

Proof. We will prove that each generator of the ridge of I computed as in [1] is a homogeneous polynomial in only one set of variables $\mathbf{X}_i$.
For a multihomogeneous polynomial F with multidegree $(d_1, \ldots, d_m)$, one can write

$$F(\mathbf{X}+\mathbf{Y}) = \sum_{1\leq i\leq m} \sum_{0\leq|\mathbf{a}_i|\leq d_i} \mathrm{D}^{\mathbf{X}_1,\ldots,\mathbf{X}_m}_{\mathbf{a}_1,\ldots,\mathbf{a}_m} F(\mathbf{X}_1, \ldots, \mathbf{X}_m)\mathbf{Y}_1^{\mathbf{a}_1} \cdots \mathbf{Y}_m^{\mathbf{a}_m}.$$

Since $F(\mathbf{X}+\mathbf{Y}) = F(\mathbf{X}_1+\mathbf{Y}_1, \ldots, \mathbf{X}_m+\mathbf{Y}_m)$ is multihomogeneous in $((\mathbf{X}_1, \mathbf{Y}_1), \ldots, (\mathbf{X}_m, \mathbf{Y}_m))$ of multidegree $(d_1, \ldots, d_m)$, then each $\mathrm{D}^{\mathbf{X}_1,\ldots,\mathbf{X}_m}_{\mathbf{a}_1,\ldots,\mathbf{a}_m} F$ is multihomogeneous in $(\mathbf{X}_1, \ldots, \mathbf{X}_m)$ of multidegree $(d_1 - |\mathbf{a}_1|, \ldots, d_m - |\mathbf{a}_m|)$. Thus the ridge is spanned by a set of polynomials which are both additive and multihomogeneous. But each monomial of an additive polynomials is in one variable, therefore a multihomogeneous additive polynomial must be in one set of variables. □

3.2 Algorithm for computing the ridge

The main advantage of multihomogeneous ideals is that, in this case, one does not need Hasse-Schmidt derivatives which are polynomials in variables of two or more different blocks. These are the ones obtained from the expansions of all $F(\mathbf{Y}_1, \ldots, \mathbf{Y}_{i-1}, \mathbf{X}_i + \mathbf{Y}_i, \mathbf{Y}_{i+1}, \ldots, \mathbf{Y}_m)$.
By switching $\mathbf{X}$ and $\mathbf{Y}$, this means that mixed Hasse-Schmidt derivatives with respect to variables from two different blocks are not needed but that only such Hasse-Schmidt derivatives $\mathrm{D}^{\mathbf{Y}_1,\ldots,\mathbf{Y}_{i-1},\mathbf{Y}_i,\mathbf{Y}_{i+1},\ldots,\mathbf{Y}_m}_{0,\ldots,0,\mathbf{a}_i,0,\ldots,0} F$ are.

Algorithm 1 Computation of the ridge.

Input Multihomogeneous polynomials $F_1, \ldots, F_r$ verifying Giraud's Lemma hypotheses and spanning ideal I.

Output Generators of the ridge of $(F_1, \ldots, F_r)$.

1. $M := \emptyset$.
2. **For** i **from** 1 **to** r
   a. **For** j **from** 1 **to** m
      i. $\tilde{F}_{i,j} := F_i(\mathbf{Y}_1, \ldots, \mathbf{X}_j + \mathbf{Y}_j, \ldots, \mathbf{Y}_m)$.
      ii. **For each** monomial $\mathbf{Y}^{\mathbf{a}}$ **in** $\tilde{F}_{i,j}$
         α. $f := \mathrm{coeff}(\tilde{F}_{i,j}, \mathbf{Y}^{\mathbf{a}})$.
         β. **If** $\deg f = p^\ell$ **then** $M := M \cup \{f\}$.
3. **Return** InterReduce(M)

Theorem 10. *Algorithm 1 is correct.*

Proof. By Theorem 9, it is clear that if, at step 2.a.i., one were to compute $\tilde{F}_i := F_i(\mathbf{X}_1 + \mathbf{Y}_1, \ldots, \mathbf{X}_m + \mathbf{Y}_m)$ and take the innermost **For** loop away, the result would be

correct. Therefore, we just need to prove that we only need to compute $\tilde{F}_i := F_i(\mathbf{Y}_1, \ldots, \mathbf{Y}_{j-1}, \mathbf{X}_j + \mathbf{Y}_j, \mathbf{Y}_{j+1}, \ldots, \mathbf{Y}_m)$ for each j.

Let F be a multihomogeneous polynomial of multidegree $(d_1, \ldots, d_m)$, then F can be decomposed as

$$F(\mathbf{X}) = \sum_{0 \leq k \leq K} F_{k,1}(\mathbf{X}_1) \cdots F_{k,m}(\mathbf{X}_m).$$

We may assume that for each j, the family $(F_{1,j}, \ldots, F_{K,j})$ is interreduced. Thus,

$$F(\mathbf{X}+\mathbf{Y}) = \sum_{0 \leq k \leq K} \prod_{1 \leq i \leq m} F_{k,i}(\mathbf{X}_i + \mathbf{Y}_i)$$

$$F(\mathbf{X}+\mathbf{Y}) = \sum_{0 \leq k \leq K} \prod_{1 \leq i \leq m} \sum_{0 \leq |\mathbf{a}_i| \leq d_i} \mathrm{D}^{\mathbf{X}_i}_{\mathbf{a}_i} F_{k,i}(\mathbf{X}_i) \mathbf{Y}_i^{\mathbf{a}_i}$$

$$F(\mathbf{X}+\mathbf{Y}) = \sum_{\substack{0 \leq k \leq K \\ 0 \leq |\mathbf{a}_1| \leq d_1 \\ \vdots \\ 0 \leq |\mathbf{a}_m| \leq d_m}} \prod_{1 \leq i \leq m} \mathrm{D}^{\mathbf{X}_i}_{\mathbf{a}_i} F_{k,i}(\mathbf{X}_i) \mathbf{Y}_i^{\mathbf{a}_i}.$$

So that $\sum_{0 \leq k \leq K} \mathrm{D}^{\mathbf{X}_1}_{\mathbf{a}_1} F_{k,1}(\mathbf{X}_1) \cdots \mathrm{D}^{\mathbf{X}_m}_{\mathbf{a}_m} F_{k,m}(\mathbf{X}_m)$ is the coefficient of $\mathbf{Y}_1^{\mathbf{a}_1} \cdots \mathbf{Y}_m^{\mathbf{a}_m}$. Let us fix k and $\mathbf{a}_2, \ldots, \mathbf{a}_m$ such that $\mathrm{lm}(F_{k,2}) = \mathbf{X}_2^{\mathbf{a}_2}, \ldots, \mathrm{lm}(F_{k,m}) = \mathbf{X}_m^{\mathbf{a}_m}$. Then, for all $j \neq 1$, $\mathrm{D}^{\mathbf{X}_j}_{\mathbf{a}_j} F_{k,j}(\mathbf{X}_j) \in \mathbb{K}^*$. Furthermore, for all $\ell \neq k$ and $j \neq 1$, $\mathrm{D}^{\mathbf{X}_j}_{\mathbf{a}_j} F_{\ell,j}(\mathbf{X}_j) = 0$. Therefore, for any $\mathbf{a}_1$, the coefficient of such a $\mathbf{Y}_1^{\mathbf{a}_1} \cdots \mathbf{Y}_m^{\mathbf{a}_m}$ is $\mathrm{D}^{\mathbf{X}_1}_{\mathbf{a}_1} F_{k,1}(\mathbf{X}_1)$. Analogously, we can have all the $\mathrm{D}^{\mathbf{X}_i}_{\mathbf{a}_i} F_{k,i}(\mathbf{X}_i)$.

It remains to prove that we do not miss important coefficients by collecting only such Hasse-Schmidt derivatives of degree a p-power.

If one were to apply Algorithm 3.10 of [1], then one would also collect all $\sum_{0 \leq k \leq K} \mathrm{D}^{\mathbf{X}_1}_{\mathbf{a}_1} F_{k,1}(\mathbf{X}_1) \cdots \mathrm{D}^{\mathbf{X}_m}_{\mathbf{a}_m} F_{k,m}(\mathbf{X}_m)$ of degree a p-power. This polynomials are spanned by all the $\mathrm{D}^{\mathbf{X}_j}_{\mathbf{a}_j} F_{k,j}(\mathbf{X}_j)$ which are spanned, themselves as polynomials in the ridge, by additive polynomials. Therefore, one only needs to collect the $\mathrm{D}^{\mathbf{X}_j}_{\mathbf{a}_j} F_{k,j}(\mathbf{X}_j)$ of degree a p-power.

Once we have all these derivatives, we need to find a minimal set of generators. Interreducing all of them starting with those of minimal degree and going on by increasing degrees ensures us to find such a minimal set. □

Remark 11. *As seen in Proposition 8, any minimal reduced Gröbner basis of I is a family of polynomials verifying Giraud's Lemma hypotheses. However, as the ideal is multihomogeneous, it is not necessary to compute a full Gröbner basis. A truncated one is enough. In particular, one can compute a basis up to multidegree $(d_1, \ldots, d_r)$ where each d_j is the maximum of the degrees in $\mathbf{X}_j$ of the polynomials generating I. This means that during the Gröbner basis computation, when one computes the S-polynomial $S(F_1, F_2)$ of two polynomials F_1 and F_2, if for any j, $\deg_{\mathbf{X}_j} S(F_1, F_2) > d_j$, then it is unnecessary to store it. Let us notice, that in fact, one can add many more tests on the degrees but as their number is 2^m, they might lead to an unnecessary overhead and are not so easy to implement. In practice, we only compute a truncated Gröbner basis up to degree $d_1 + \cdots + d_r$ as in the homogeneous case.*

3.3 Complexity of Algorithm 1

In this section, we study the complexity of the algorithm for computing the ridge. In the following, we will denote by $\mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m]_{(d_1, \ldots, d_m)}$ the $\mathbb{K}$-vector space of multihomogeneous polynomials of multidegree $(d_1, \ldots, d_m)$ over $\mathbb{K}$. The notation $\mathsf{M}(d)$ will stand for the complexity of multiplying two univariate polynomials of degree at most $d-1$ over $\mathbb{K}$. It is classical that $\mathsf{M}(d) \in O(d \log d \log\log d)$ (see [3]).

Theorem 12. *Let us denote $n = \max_{1 \leq j \leq m} n_j$ and $d = \max_{1 \leq i \leq r, 1 \leq j \leq m} d_{i,j}$. The number of operations done in $\mathbb{K}$ by Algorithm 1 to output generators of the ridge of the ideal spanned by the input polynomials is less than*

$$O\left(r \binom{d+n-1}{d}^{m-1} \mathsf{M}(2^n d^n) mn \log d + m \binom{n+d}{n}^{\omega}\right).$$

Proof. Assuming one has generators $F_1, \ldots, F_r$ verifying Giraud's Lemma (see Lemma 6), then one needs to compute all the compositions $\tilde{F}_{i,j} = F_i(\mathbf{Y}_1, \ldots, \mathbf{Y}_{j-1}, \mathbf{X}_j + \mathbf{Y}_j, \mathbf{Y}_{j+1}, \ldots, \mathbf{Y}_m)$ for $1 \leq i \leq r$ and $1 \leq j \leq m$.

In this case, we see F_i as an element of vector space $\mathbb{K}[\mathbf{Y}_1, \ldots, \mathbf{Y}_{j-1}, \mathbf{Y}_{j+1}, \ldots, \mathbf{Y}_m]_{(d_{i,1}, \ldots, d_{i,m})}[\mathbf{X}_j]$ which is isomorphic to $\mathbb{K}^{\Delta_{i,j}}[\mathbf{X}_j]$, where $\Delta_{i,j} = \prod_{\substack{1 \leq k \leq m \\ k \neq j}} \binom{d_{i,k}+n_k-1}{d_{i,k}}$. By [2], Chapter 1, Section 8, the shift of such a homogeneous multivariate polynomial over a field can be done in $O(\mathsf{M}(2^n d_{i,j}^{n_j}) n_j \log d_{i,j})$ operations in $\mathbb{K}$. Thus, $\tilde{F}_{i,j}$ can be computed in at most $O(\Delta_{i,j} \mathsf{M}(2^n d_{i,j}^{n_j}) n_j \log d_{i,j})$ operations in $\mathbb{K}$. As there are at most $\Delta_{i,j} \binom{d_{i,j}+n_j-1}{d_{i,j}} \in O(\Delta_{i,j} d_{i,j}^{n_j})$ monomials $\mathbf{Y}^{\mathbf{a}}$ in $\tilde{F}_{i,j}$, the remaining part is not dominant.

Let d and n be the maxima defined as in the hypotheses, then for all i, j, $1 \leq i \leq r$, $1 \leq j \leq m$, $\Delta_{i,j} \leq \binom{d+n-1}{d}^{m-1}$. Thus, each turn of the outermost **For** loop is done in at most $O\left(\binom{d+n-1}{d}^{m-1} \mathsf{M}(2^n d^n) mn \log d\right)$ operations in $\mathbb{K}$.

Finally, one needs to interreduce the polynomials in each block of variables. This cost is bounded by the cost of the computation of a Gröbner basis in n variables truncated to degree d which can be done with F5 algorithm [8] in $O\left(\binom{n+d}{n}^{\omega}\right)$ operations in $\mathbb{K}$. □

Remark 13. *Let us still assume that d and n are the maxima defined in the hypotheses of the previous theorem. We will give a lower bound and an upper bound of the complexity of [1], Algorithms 3.5 and 3.10 applied to a multihomogeneous ideal. First of all, one would have to compute the shift of r homogeneous polynomials in mn variables. Each polynomial has degree at most d in each variable and is itself of degree md. Then, one would have to interreduce a set of polynomials by computing a truncated Gröbner basis in mn variables.*

On the one hand, this can be lower-bounded by the shifts of homogeneous polynomials of degree d and a Gröbner basis computation up to degree d, which yield at least

$$O\left(r \mathsf{M}(2^{mn} d^{mn}) mn \log d + \binom{mn+d}{mn}^{\omega}\right)$$

operations in $\mathbb{K}$.

On the other hand, this can be upper-bounded by the shifts of homogeneous polynomials of degree md and a Gröbner basis computation truncated up to degree md. Thus, the number of operations in $\mathbb{K}$ is at most

$$O\left(r \mathsf{M}(2^{mn} (md)^{mn}) mn \log(md) + \binom{mn+md}{mn}^{\omega}\right).$$

4. MINIMAL NUMBER OF VARIABLES

4.1 From the ridge to the directrix: the perfect field case

As stated in [1], the ridge and the directrix coincide in characteristic 0. In this and the following subsections, we assume that $\operatorname{char}\mathbb{K} = p > 0$. If $\mathbb{K}$ is perfect, the directrix of I can be obtained directly from the ridge of I. We have already seen that any polynomial of degree p^ℓ spanning the ridge is in fact a p^ℓth power of a linear form. For all i, j, $1 \leq i \leq m$, $1 \leq j \leq e_i$, let us assume that $\deg H_{i,j} = p^{\ell_{i,j}}$ and let $L_{i,j}$ be the linear form $\sqrt[p^{\ell_{i,j}}]{H_{i,j}}$. Since the ridge is spanned by polynomials $((H_{1,1},\ldots,H_{1,e_1}),\ldots,(H_{m,1},\ldots,H_{m,e_m}))$, then the directrix of I is spanned by all the linear forms $((L_{1,1},\ldots,L_{1,e_1}),\ldots,(L_{m,1},\ldots,L_{m,e_m}))$.

PROPOSITION 14. *Let $\mathbf{H}_1 = (H_{1,1},\ldots,H_{1,e_1}),\ldots,\mathbf{H}_m = (H_{m,1},\ldots,H_{m,e_m})$ be minimal generators of the ridge of I of respective degrees $p^{\ell_{i,j}}$, as obtained as the output of Algorithm 1. Let $L_{i,j}$ be the linear form $\sqrt[p^{\ell_{i,j}}]{H_{i,j}}$ for all i, j such that $1 \leq i \leq m$, $1 \leq j \leq e_i$. Then, $\mathbf{L}_1 = (L_{1,1},\ldots,L_{1,e_1}),\ldots,\mathbf{L}_m = (L_{m,1},\ldots,L_{m,e_m})$ is a basis of the directrix.*

PROOF. We may assume that for all i, $1 \leq i \leq m$, and all j, $1 \leq j < e_i$, $\deg H_{i,j} \leq \deg H_{i,j+1}$. As we use the DRL ordering to interreduce the polynomials, which is in fact equivalent to the degree lexicographic ordering in our special case, if $\operatorname{lm}(H_{i,j})$ is a pth power of $X_{i,k}$, then $X_{i,k}$ does not appear in $H_{i,s}$ for $s > j$. Thus, after rearranging the variables, one can see that polynomials $H_{i,j}$ form a triangular system and so do the $L_{i,j}$. This concludes the proof. □

REMARK 15. *Although this result ensures that one obtains a basis of the directrix, the linear forms can still be interreduced.*

Indeed, over $\mathbb{F}_2$, the ridge of $F = (X_1 + X_3)X_2 + X_3^2$ is spanned by $(H_1 = X_1 + X_3, H_2 = X_2, H_3 = X_3^2)$ as output by Algorithm 1. However, linear form $L_3 = X_3$ can be used to reduce $L_1 = X_1 + X_3$ into a mere X_1.

In general, an effective perfect field of characteristic p is such that extracting a pth root of an element is effective. These are for instance finite fields $\mathbb{F}_q$, where q is a p-power. Quite the opposite, rational fractions fields in multiple variables $\mathbb{K}(t_1,\ldots,t_s)$ over an effective perfect field $\mathbb{K}$ are not perfect, as pth roots $t_1^{1/p},\ldots,t_s^{1/p} \notin \mathbb{K}(t_1,\ldots,t_s)$. In between, the field of Puiseux series [22, 25, 26, 27] in one variable t over a perfect field $\mathbb{K}$, which can be seen as $\bigcup_{n\in\mathbb{N}} \mathbb{K}((t^{1/n!}))$ is the perfect closure of the maximal tamely ramified extension of $\mathbb{K}((t))$ (see [19]). This means it is a perfect field in which one can compute any term of the pth root of an element, however it is still not effective as zero-testing is not effective for power series.

In fact, let us recall that, in general, a perfect field needs not be effective as testing if an element is a pth power may be not decidable (see [13], Section 7 and [14], Remark 5.10).

4.2 Algorithm for computing the directrix over a perfect field

As stated above, to compute the directrix, one has to compute the ridge first. This is why, in Algorithm 2, we take as input additive polynomials spanning the ridge. Then, we detail what was explained in Section 4.1 to compute generators of the directrix.

Algorithm 2 Computation of the directrix over a perfect field of characteristic $p > 0$.

Input Homogeneous additive polynomials $H_1,\ldots,H_e$ spanning the ridge of ideal I.

Output Generators of the directrix of I.

1. $M := \emptyset$.
2. **For** i **from** 1 to e
   a. $p^\ell := \deg H_i$.
   b. $L := 0$.
   c. **For each** monomial $X_j^{p^\ell}$ **in** H_i
      i. $f := \sqrt[p^\ell]{\operatorname{coeff}(H_i, X_j^d)}$.
      ii. $L := L + fX_j$.
   d. $M := M \cup \{L\}$.
3. **Return** M.

THEOREM 16. *Let us assume that $\mathbb{K}$ is a perfect field of characteristic $p > 0$. Let us denote $n = \max_{1\leq j\leq m} n_i$ and $d = \max_{1\leq i\leq r, 1\leq j\leq m} d_{i,j}$. Algorithm 2 outputs generators of the directrix of the ideal whose ridge is spanned by the input polynomials in less than $mn^2 \log_p d$ extractions of pth roots in $\mathbb{K}$.*

PROOF. First, let us prove that Algorithm 2 is correct. As proved in [1, 15] and in Proposition 14, a basis of the directrix is obtained by taking all the linear forms which are p^ℓth roots of the generators of the ridge.

Since each $H_{i,j}$ is homogeneous and additive, it has, at most, n_i monomials. Then one has to extract p^ℓth roots of at most $e_1 n_1 + \cdots + e_m n_m \leq mn^2$ coefficients for some ℓ. Now, assuming $p^\ell = \max \deg_{1\leq i\leq m, 1\leq j\leq n_i} H_{i,j}$, one has $\ell \leq \log_p d$. That is, in the worst case, Algorithm 2 extracts no more than $mn^2 \log_p d$ pth roots in $\mathbb{K}$. □

4.3 The imperfect field case

Whenever $\mathbb{K}$ is not perfect, coefficients of monomials of generators of the ridge need not be pth powers. This means that if H is additive of degree p^ℓ, then the linear form L such that $L^{p^\ell} = H$ is in general in $\mathbb{L}[\mathbf{X}]$, where $\mathbb{L}$ is an algebraic extension of $\mathbb{K}$. For instance let $F = X_1^{p-1}X_2 + X_3^p + tX_4^p$ be a polynomial over the rational fractions field $\mathbb{F}_p(t)$. It is clear that the ridge of the ideal (F) is spanned by X_1, X_2 and $X_3^p + tX_4^p$. However, the directrix of (F) is spanned by the three elements X_1, X_2 and $X_3 + t^{1/p}X_4$ only over the field $\mathbb{F}_p(t^{1/p})$. Over $\mathbb{F}_p(t)$, the directrix is spanned by X_1, X_2, X_3 and X_4.

What we can see with this example is that, in the imperfect field case, to retrieve the generators of the directrix, one might need to split any generator of the ridge of degree p^ℓ, with $\ell \geq 1$, as a linear combination of p^ℓth powers of linear forms. Then, taking their p^ℓth roots and reducing all of them by linear algebra yields the directrix of the ideal.

But one has to be careful when splitting the generators of the ridge (see [18]). Assume that the ridge of I is spanned by $H = X_1^2 + uX_2^2 + vX_3^2 + uvX_4^2$. Over $\mathbb{K} = \mathbb{F}_2(u, v)$, it seems clear that the directrix of I is spanned by X_1, X_2, X_3 and X_4. Let us denote $\mathbb{K}^2$, the subfield of $\mathbb{K}$ formed by all the squares of elements of $\mathbb{K}$. Then, the directrix is indeed spanned by X_1, X_2, X_3, X_4, if $[\mathbb{K} : \mathbb{K}^2] = 4$. Otherwise, if $v = 1 + u$, then $H = (X_1 + X_3 + uX_4)^2 + u(X_2 + X_3 + X_4)^2$.

Assuming $H \in \mathbb{K}[\mathbf{X}]$, a generator of the ridge, has degree p^ℓ. The right idea seems to provide a p^ℓ-basis of $\mathbb{K}$, that is a basis $(b_1, \ldots, b_{p^{k\ell}})$ of $\mathbb{K}$ as a $\mathbb{K}^{p^\ell}$-vector space, to write

$$H = \sum_{1 \le i \le p^{k\ell}} H_i b_i, \ H_i \in \mathbb{K}^{p^\ell}[\mathbf{X}],$$

then to return $L_1 = \sqrt[p^\ell]{H_1}, \ldots, L_{p^{k\ell}} = \sqrt[p^\ell]{H_{p^{k\ell}}}$ and finally to reduce by linear algebra all the obtained linear forms.

However, it is not clear that this yields the minimal number of linear forms. Furthermore, one would have to compute a p^ℓ-basis of $\mathbb{K}$ which is also a difficult problem in general.

4.4 Computation of the outermost polynomials in the composition

Let us assume that $\mathbf{H}_1 = (H_{1,1}, \ldots, H_{1,e_1}), \ldots, \mathbf{H}_m = (H_{m,1}, \ldots, H_{m,e_m})$ are a minimal set of generators of the ridge. We must compute $G_1, \ldots, G_r \in \mathbb{K}[\mathbf{U}_1, \ldots, \mathbf{U}_m]$ such that, for all i, $F_i(\mathbf{X}_1, \ldots, \mathbf{X}_m) = G_i(\mathbf{H}_1, \ldots, \mathbf{H}_m)$.

Notice that, in this case, as polynomials $H_{j,k}$ need not all have the same degree, polynomials G_i are not necessarily homogeneous.

For instance, considering $F(\mathbf{X}) = X_1X_2X_3X_4 + X_5^2X_6^2 + X_7^4 \in \mathbb{F}_2[\mathbf{X}]$. Then,the ridge is spanned by $(H_i)_{1 \le i \le 3} = (X_i)_{1 \le i \le 3}$, $(H_i)_{5 \le i \le 6} = (X_i^p)_{5 \le i \le 6}$ and $H_7 = X_7^4$, yielding $G(\mathbf{U}) = U_1U_2U_3U_4 + U_5U_6 + U_7$.

Anyhow, since polynomials $H_{j,k}$ form a triangular set in $X_{j,k}$, one can retrieve each G_i.

Assuming $\mathbb{K}$ is perfect. Since there is a one-to-one correspondance between generators of the ridge and generators of the directrix, then from a decomposition $F_i(\mathbf{X}_1, \ldots, \mathbf{X}_m) = G_i(\mathbf{H}_1, \ldots, \mathbf{H}_m)$, it is easy to deduce such a decomposition $F_i(\mathbf{X}_1, \ldots, \mathbf{X}_m) = \tilde{G}_i(\mathbf{L}_1, \ldots, \mathbf{L}_m)$.

5. IMPLEMENTATION AND TIMINGS

We report on performances obtained with our implementation in Maple 16 [20], using FGb library [9], for computing the ridge of multihomogeneous ideals. The source code is available at http://www-polsys.lip6.fr/~berthomieu/.

In Tables 1, 2, 3 and 4, we display timings, in seconds obtained using one core of an Intel Xeon E7220 at 2.93 GHz running Linux with 128 GB of RAM. We compare timings for computing the ridge of a multihomogeneous ideal using algorithms of both [1] and this paper, namely Algorithm 1. In both cases, we assume that the generators of the ideal form a Giraud basis because they all have the same degree (see Proposition 7). First, we generated two random multihomogeneous polynomials over $\mathbb{F}_p$, with $p = 2$ or $p = 65521$, using the `randpoly` function with ν variables of degree d in each block of variables. Then, each variable was replaced by a linear combination of $n = k\nu$ variables. Last, an ideal is created, spanned by these polynomials.

In each table, one of the parameters: ν, k, m and d varies when all the other ones are fixed. Line Hom_p stands for Algorithm 3.10 of [1], whose complexity is both lower-bounded and upper-bounded in Remark 13, while line $\mathsf{M\text{-}H}_p$ stands for Algorithm 1 presented in here, whose complexity is given in Theorem 12, both over $\mathbb{F}_p$. Grey cells mean that no computations were run.

ν	2	8	32	128	512	2048
Hom_2	0.12	0.43	2.0	10	39	117
$\mathsf{M\text{-}H}_2$	0.23	0.40	0.54	1.5	4.8	14
Hom_{65521}	0.16	12	1 200	5 300	14 000	
$\mathsf{M\text{-}H}_{65521}$	0.27	7	410	3 200	8 800	

Table 1: Timings in seconds, for $k = 2$, $m = 2$ and $d = 2$.

In the following Table 2, we do not give timings for $p = 2$ as difference of timings for increasing k were too small to be relevant.

k	1.25	1.5	2	3	5	9
Hom_{65521}	2.1	3.7	12	46	170	320
$\mathsf{M\text{-}H}_{65521}$	1.2	2.2	7	20	59	110

Table 2: Timings in seconds, for $\nu = 8$, $m = 2$ and $d = 2$.

In the following Tables 3 and 4, symbol ∞ means that the computation was stopped before ending.

m	2	3	4	5
Hom_2	0.43	57	3 200	∞
$\mathsf{M\text{-}H}_2$	0.40	2.6	120	2 300
Hom_{65521}	12	∞		
$\mathsf{M\text{-}H}_{65521}$	7	19 000		

Table 3: Timings in seconds, for $\nu = 8$, $k = 2$ and $d = 2$.

d	1	2	3	4	5	6
Hom_2	0.13	0.43	6.2	97	1 200	∞
$\mathsf{M\text{-}H}_2$	0.24	0.40	1.8	15	82	1 300
Hom_{65521}	0.16	12	∞			
$\mathsf{M\text{-}H}_{65521}$	0.27	7	5 800			

Table 4: Timings in seconds, for $\nu = 8$, $k = 2$ and $m = 2$.

Acknowledgments

We would like to thank J.-Ch. Faugère and L. Perret for very helpful discussions on multihomogeneous ideals and on the decomposition problem.

6. REFERENCES

[1] J. Berthomieu, P. Hivert, and H. Mourtada. Computing Hironaka's invariants: Ridge and Directrix. In *Arithmetic, Geometry, Cryptography and Coding Theory 2009*, volume 521 of *Contemp. Math.*, pages 9–20. Amer. Math. Soc., Providence, RI, 2010.

[2] D. Bini and V. Y. Pan. *Polynomial and matrix computations. Vol. 1.* Progress in Theoretical Computer Science. Birkhäuser Boston Inc., Boston, MA, 1994. Fundamental algorithms.

[3] D. G. Cantor and E. Kaltofen. On fast multiplication of polynomials over arbitrary algebras. *Acta Inform.*, 28(7):693–701, 1991.

[4] G. Chèze. A recombination algorithm for the decomposition of multivariate rational functions. Math. Comp., posted on November 30, 2012, PII S 0025-5718(2012)02658-5 (to appear in print).

[5] V. Cossart and O. Piltant. Resolution of singularities of threefolds in positive characteristic. I. Reduction to local uniformization on Artin-Schreier and purely inseparable coverings. *J. Algebra*, 320(3):1051–1082, 2008.

[6] V. Cossart and O. Piltant. Resolution of singularities of threefolds in positive characteristic. II. *J. Algebra*, 321(7):1836–1976, 2009.

[7] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[8] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *ISSAC '02: Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, ISSAC '02, pages 75–83, New York, NY, USA, 2002. ACM.

[9] J.-C. Faugère. FGb: A Library for Computing Gröbner Bases. In K. Fukuda, J. v. d. Hoeven, M. Joswig, and N. Takayama, editors, *Mathematical Software - ICMS 2010*, volume 6327 of *Lecture Notes in Computer Science*, pages 84–87, Berlin, Heidelberg, September 2010. Springer Berlin / Heidelberg. Available from http://www-polsys.lip6.fr/~jcf/Software/.

[10] J.-C. Faugère, J. v. z. Gathen, and L. Perret. Decomposition of generic multivariate polynomials. In *ISSAC '10: Proceedings of the 2010 international symposium on Symbolic and algebraic computation*, ISSAC '10, pages 131–137, New York, NY, USA, 2010. ACM. isbn: 0747-7171 (updated version).

[11] J.-C. Faugère and L. Perret. High order derivatives and decomposition of multivariate polynomials. In *ISSAC '09: Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, ISSAC '09, pages 207–214, New York, NY, USA, 2009. ACM.

[12] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree $(1, 1)$: algorithms and complexity. *J. Symbolic Comput.*, 46(4):406–437, 2011.

[13] A. Fröhlich and J. C. Shepherdson. Effective procedures in field theory. *Philos. Trans. Roy. Soc. London. Ser. A.*, 248:407–432, 1956.

[14] J. v. z. Gathen. Hensel and Newton methods in valuation rings. *Math. Comp.*, 42(166):637–661, 1984.

[15] J. Giraud. *Étude locale des singularités*. U.E.R. Mathématique, Université Paris XI, Orsay, 1972. Cours de 3ème cycle, 1971–1972, Publications Mathématiques d'Orsay, No. 26.

[16] H. Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II. *Ann. of Math. (2) 79 (1964), 109–203; ibid. (2)*, 79:205–326, 1964.

[17] H. Hironaka. Characteristic polyhedra of singularities. *J. Math. Kyoto Univ.*, 7:251–293, 1967.

[18] H. Hironaka. Additive groups associated with points of a projective space. *Ann. of Math. (2)*, 92:327–334, 1970.

[19] K. S. Kedlaya. The algebraic closure of the power series field in positive characteristic. *Proc. Amer. Math. Soc.*, 129(12):3461–3470, 2001.

[20] M. B. Monagan, K. O. Geddes, K. M. Heal, G. Labahn, S. M. Vorkoetter, J. McCarron, and P. DeMarco. *Maple 10 Programming Guide*. Maplesoft, Waterloo ON, Canada, 2005.

[21] Y. V. Nesterenko and P. Philippon. *Introduction to algebraic independence theory*, volume 1752 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2001. With contributions from F. Amoroso, D. Bertrand, W. D. Brownawell, G. Diaz, M. Laurent, Yuri V. Nesterenko, K. Nishioka, Patrice Philippon, G. Rémond, D. Roy and M. Waldschmidt, Edited by Nesterenko and Philippon.

[22] I. Newton. *The correspondence of Isaac Newton, Vol. II: 1676–1687*. Published for the Royal Society. Cambridge University Press, New York, 1960.

[23] P. Philippon. Lemmes de zéros dans les groupes algébriques commutatifs. *Bull. Soc. Math. France*, 114(3):355–383, 1986.

[24] T. Pruschke. On degrees in multihomogeneous ideal theory. *Acta Math. Univ. Comenian. (N.S.)*, 60(2):233–241, 1991.

[25] V. Puiseux. Recherches sur les fonctions algébriques. *J. Math. Pures Appl.*, 15:365–480, 1850.

[26] V. Puiseux. Recherches sur les fonctions algébriques. *J. Math. Pures Appl.*, 16:228–240, 1850.

[27] I. R. Shafarevich. *Basic algebraic geometry. 2*. Springer-Verlag, Berlin, second edition, 1994. Schemes and complex manifolds, Translated from the 1988 Russian edition by Miles Reid.

[28] E. W. v. Tschirnhaus. Methodus auferendi omnes terminos intermedios ex data equatione. *Nieuw Arch. Wisk. (4)*, 11(1):67–83, 1993. With translation and commentaries in Dutch by A. W. Grootendorst.

[29] E. W. v. Tschirnhaus and R. F. Green. A method for removing all intermediate terms from a given equation. *j-SIGSAM*, 37(1):1–3, mar 2003.