HAL open science

Computing Hironaka's invariants: Ridge and Directrix

Jérémy Berthomieu, Pascal Hivert, Hussein Mourtada

To cite this version:

Jérémy Berthomieu, Pascal Hivert, Hussein Mourtada. Computing Hironaka's invariants: Ridge and Directrix. Papers from the 12th Conference (AGC2T 12) held in Marseille, March 30–April 3, 2009, the 1st Geocrypt Conference held in Pointe-à-Pitre, April 27-May 1, 2009, and the European Science Foundation Exploratory Workshop on Curves, Coding Theory and Cryptography held in Marseille, March 25-29, 2009., Mar 2009, Marseille, France. pp.12, 10.1090/conm/521 . hal-00492824

HAL Id: hal-00492824

https://hal.science/hal-00492824v1

Submitted on 17 Jun 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Computing Hironaka's invariants: Ridge and Directrix

Jérémy Berthomieu, Pascal Hivert, and Hussein Mourtada

Abstract. In this note we present Hironaka's invariants as developped by Giraud: the ridge and the directrix. We give an effective definition and a functorial one and show their equivalence. The fruit is an effective algorithm that computes the additive generators of the "ridge", and the generators of its invariant algebra.

Introduction

The problem of the resolution of singularities has made a tremendous progress thanks to Hironaka's contribution. In this article, we want to present some objects that he introduced to resolve singularities, in particular we compute the subtle invariant: the *ridge* (The notion "ridge" is "faîte" in the original (French) literature). Take an ideal $I \subset R$, for instance R a polynomial ring (or a localization thereof) over any field. Take $x \in \mathrm{Spec}(R/I)$. The directrix and the ridge live in the tangent cone at x. The directrix is a vector space, the ridge an additive group. These two objects are given only by the *class of isomorphisms* of R/I. Even more, these invariants "commute with smooth morphisms" [**5**]. In particular, for any isomorphism:

$$\phi : \ R/I \longrightarrow S/J,$$

both R/I and S/J have isomorphic tangent cone, directrix and ridge at x and $\phi(x)$.

Giraud shows in [**5**] that the ridge is the tangent cone of a "maximal contact variety" (see [**9**]). The ridge as we will see is generated by *additive* polynomials. In characteristic 0, this means that the ridge is a linear space, therefore a "maximal contact variety" is smooth. In characteristic $p > 0$, additive polynomials may not be linear, therefore the ridge may not be linear and a "maximal contact variety" may not be smooth. This is the crucial fact why Hironaka's proof is not generalized for free to positive characteristic. This generates a major difficulty, still not overcome in the desingularization problem. An another difficulty is that if you blow up a singular variety X along a singular point $x \in X$, the points "near" to x are on the Proj of the ridge of the tangent cone. In [**8**], Hironaka shows that, in characteristic $p > 0$ there are examples of points "near" to x which are not on the Proj of the directrix of the tangent cone. In the 70's a large literature about "Hironaka's groups" appeared: people has tried to classify the cases where "near" points are not on the Proj of the Directrix of the tangent cone. The Ridge and "Hironaka's groups" are closely

Key words and phrases. Algebraic geometry, invariants, resolution of singularities.
AMS Classification 32S45, 14Q99, 14L30.

related, but we do not want to say more about this classification problem which is known to be quite difficult. Nowadays, the ridge seems to be forgotten though it is a very interesting object.

The contribution of this paper is the computation of a basis of the ideal of the ridge whose elements are additive polynomials. Indeed, in [**4, 5**], Giraud shows how to compute a set of generators of this ideal, but they are not additive polynomials in general: see Example 3.7. We also hope that we clarified Giraud's proofs.

Acknowledgement. V. Cossart[1] gave a talk on this topic in Geocrypt[2] and he initiated us in a working group about desingularization in positive characteristic. He is at the origin of this work, we would like to thank him for his helpful remarks. The authors are very grateful to both the referees for their constructive comments about this paper.

1. Notation and prerequisites, naive definitions of Ridge and Directrix

Until the end of this article, k denotes a field of any characteristic. We give in this section an overview about cones, ridges and directrices.

A linear space of dimension n is $\mathbb{A}^n := \operatorname{Spec} R$, where $R := k[X_1, \ldots, X_n]$. A *cone* $\mathcal{C}$ embedded in $\mathbb{A}^n$ is given as $\operatorname{Spec} k[X_1, \ldots, X_n]/I$ where $I \subset k[X_1, \ldots, X_n]$ is a *homogeneous* ideal.

Definition 1.1 (**Directrix**). The *directrix* of $\mathcal{C}$ is the linear space of equations in $Y_1, \ldots, Y_\tau$, the smallest set of linear forms such that

$$I = (I \cap k[Y_1, \ldots, Y_\tau])k[X_1, \ldots, X_n]. \tag{1.1}$$

In a few words, the smallest list of variables to define I. Geometrically, there are linear subspaces $W \subset \mathbb{A}^n$ such that $\mathcal{C} + W = \mathcal{C}$ (take $W = 0$ for instance), and if W_1 and W_2 are such, then so is $W_1 + W_2$. The directrix corresponds to the *biggest* linear subspace W of $\mathbb{A}^n$ such that $\mathcal{C} + W = \mathcal{C}$.

Definition 1.2 (**Naive definition of the ridge**). The *ridge* [**8**] of $\mathcal{C}$ is the additive space of equations in $P_1, \ldots, P_e$, the smallest set of *additive polynomials* such that

$$I = (I \cap k[P_1, \ldots, P_e])k[X_1, \ldots, X_n]. \tag{1.2}$$

This definition looks inconsistent, existence is not clear. Consistance is given in Section 2.2. Obviously, they coincide in characteristic 0, but in characteristic $p > 0$, they are in general different. In this paper, following Giraud [**4, 5**], we show that it is easy to compute the ridge (easier than the directrix). Let us note that the ridge has good properties (commutes to base changes, for example) that the directrix has not. For instance, suppose that k has characteristic $p > 0$ and that $\lambda \in k$ is not a p-power, take $I = (X^p + \lambda Y^p)k[X, Y]$, then the directrix is $\mathrm{V}(X, Y)$, the ridge is $\mathrm{V}(I)$, where $\mathrm{V}(\mathcal{I})$ stands for the variety defined by ideal $\mathcal{I}$. Change k in $\hat{k}$ its algebraic closure, then the directrix is $\mathrm{V}(X + \sqrt[p]{\lambda} Y)$, the ridge is still $\mathrm{V}(I)$.

[1]Université de Versailles–St-Quentin-en-Yvelines, CNRS LMV, UMR 8100
[2]GEOCRYPT2009

2. The Ridge: formal definition, main properties.

2.1. Ridge as a functor. Let $\mathbb{A}^n_k$ be the n-dimensional affine space over k. As above let $\mathcal{C}$ be the cone defined in $\mathbb{A}^n_k$ by the homogeneous ideal I, and let G be the quotient R/I. The natural k-algebra homomorphism

$$\begin{array}{cccc} \Delta & : & k[X_1,\dots,X_n] & \longrightarrow & k[X_1,\dots,X_n]\otimes k[Y_1,\dots,Y_n] \\ & & X_i & \mapsto & X_i+Y_i \end{array}$$

gives $\mathbb{A}^n_k$ the natural structure of a group scheme. We will call $+$ the law that it defines. If we see $\mathbb{A}^n_k$ as its functor of points, then we can define the sub-functor of the category of Schemes over k to the category of Sets as follows: for a k-Scheme S, $F(S)$ is the subset of of the S-points v in $\mathbb{A}^n_k$ such that $v+c\in\mathcal{C}(S)$ for every S-point c of $\mathcal{C}(S)$.

Now, we give some consequences of the definition. Let S be a k-Scheme, firstly, 0 is a S-point which lies in $\mathcal{C}(S)$, so for all v in $F(S)$, $0+v$ is an element of $\mathcal{C}(S)$, that is to say $F(S)\subset\mathcal{C}(S)$. Therefore, seen as functors F is a subset of $\mathcal{C}$. Secondly, $F(S)$ is a group scheme. The S-point 0 lies trivially in $F(S)$. Let two S-points v and w in $F(S)$, the definition ensures that translations by v and w send the cone $\mathcal{C}(S)$ to itself, so the composition, which is just the translation by $v+w$ has the same property. This forces $(v+w)$ to be in $F(S)$. Moreover, the inverse of the translation by v, which is the translation by $-v$, preserves $\mathcal{C}(S)$, that is to say $-v\in F(S)$.

Proposition-Definition 2.1. *The functor F is representable by a scheme F. We call this scheme the ridge of $\mathcal{C}$.*

The remarks below say that F, the ridge of $\mathcal{C}$ is a group scheme, subscheme of $\mathcal{C}$, so the ridge of F (seen as a subscheme of $\mathcal{C}$) is the ridge F.

Proof. 1. Let N be the maximum degree of a set of generators $f_1,\dots,f_m$ of I. Let G_ℓ be the homogeneous component of degree ℓ of G (G is a graded algebra because I is homogeneous). Let $H:=\bigoplus_{\ell\le N}G_\ell$ the k-vector space which is of finite dimension, we can find a k-basis of H formed by monomials e_i, $i\in\Lambda$. It is easy to compute it, $f_i=\underline{X}^{A_i}+\sum_{B\in\mathbb{N}^n,B<A_i}\lambda_B\underline{X}^B$. So H is spanned by $\underline{X}^B$, with $|B|\le N$ and $B\notin\bigcup_{1\le i\le m}A_i+\mathbb{N}^n$. This family is a basis of H. Note that H generates G as a k-algebra.

2. Let s be the composed morphism

$$s: R\longrightarrow R\otimes_k R\longrightarrow R\otimes_k G,$$

where the first morphism is Δ and the second morphism is the canonical one. For every $d\in\mathbb{N}, d\le N$ and $f\in I_d$, $s(f)$ is homogeneous of degree d, therefore $s(f)\in R\otimes H$ and it can be uniquely written

$$s(f)=\sum_{\ell\in\Lambda}s_\ell(f)\otimes e_\ell,\quad \text{with } s_\ell(f)\in R_{d-\deg(e_\ell)}.$$

This follows from the fact that $R\otimes_k H$ is a free R-module generated by the $1\otimes e_\ell$'s. Now, $f_1,\dots,f_m$ span I, so we define J the ideal generated by $s_\ell(f_i),\ell\in\Lambda,1\le i\le m$.

3. <u>Claim</u> The subscheme of $\mathbb{A}^n_k$ defined by J represents the functor f. Indeed, it is sufficient to verify that for a k-algebra B, the functor of points of $\mathrm{Spec}(R/J)$

applied to B coincides with $F(B)$. The data of a B-point of $\mathbb{A}_k^n$ is a equivalent to the data of a homomorphism $v : R \longrightarrow B$, which gives rise to

$$R \xrightarrow{\Delta} R \otimes_k R \longrightarrow R \otimes_k G \xrightarrow{v \otimes 1} B \otimes G.$$

If we want the translation by v to map $\mathcal{C}$ in $\mathcal{C}$, i.e. that v belongs to $F(B)$, $(v \otimes 1) \circ s$ must annihilate I. This means that I should be in the kernel of $(v \otimes 1) \circ s$ and therefore the image of the translation by v is included in $\mathcal{C}$. This is equivalent to $(v \otimes 1) \circ s(f) = \sum_{\ell \in \Lambda} v(s_\ell(f)) \otimes e_\ell = 0$ for every $f \in I_d, d \leq N$. But since $B \otimes_k H$ is free of base $1 \otimes e_\ell$, $\ell \in \Lambda$, this is equivalent to $v(s_\ell(f)) = 0$, therefore v factors by R/J and it is a an R/J-point. □

Recall that F is an additive group and there is no reason for the $s_i(f_j)$'s to be additive polynomials in the general case. The idea of Giraud is to find a condition on $f_1, \ldots, f_m$ to have this property.

We define by the Taylor formula, derivations of f, homogeneous polynomial of degree s, $\mathrm{D}_A^X f$ with $A \in \mathbb{N}^n$ by $f(\underline{X} + \underline{Y}) = \sum_{A \in \mathbb{N}^n, |A| \leq s} \mathrm{D}_A^X f(\underline{X}) \underline{Y}^A$. This derivations D_A^X are known as "Hasse-Schmidt" derivations.

Notations 2.2. From now on, we will only use the graded lexical order (grlex). Hence "Gröbner basis" will always mean "Gröbner basis with respect to the grlex order". The ideal of the Ridge will be denoted by J.

For any $P = \sum_{A \in \mathbb{N}^n} \lambda_A \underline{X}^A \in k[\underline{X}]$, $P \neq 0$, $\exp(P)$ is the greatest A such that $\lambda_A \neq 0$.

For any homogeneous ideal $I \neq \{0\}$ in $k[\underline{X}]$, the set $\{\exp(P); P \in I - \{0\}\}$ is denoted $\exp(I)$ and is called the exponent of the ideal I.

Corollary 2.3 (**Giraud**). *If $f_1, \ldots, f_m$, the homogeneous generators of I, satisfy $\mathrm{D}_A^X f_i = 0$ with $A \in \exp(I)$ and $|A| < \deg(f_i)$, then J is spanned by the $\mathrm{D}_A^X f_i$'s with $A \in \mathbb{N}^n$, $|A| < \deg(f_i)$.*

Proof. We keep the same notations as in Proposition 2.1 and we identify $R \otimes_k R$ with $k[\underline{X}, \underline{Y}]$. Let $\bar{Y}_i$ be the class of Y_i in $R \otimes_k R/I$. Since the Y_i^A's, $A \notin \exp(I)$, represent a k-basis of R/I, the $\bar{Y}_i^A$'s, $A \notin \exp(I)$, give a basis of the free R-module $R \otimes_k R/I$. So with respect to this basis using the Taylor formula, we have that the $s_\ell(f)$'s, defined as above, are the $\mathrm{D}_A^X f_i$'s, when the f_i's are as above. □

Definition 2.4. A basis of I which verifies the statement of Lemma 2.3 will be called a "Giraud basis" of the cone.

By the definition of the Hasse-Schmidt derivations above and for $f \in R$ we have

$$f(\underline{X} + \underline{Y}) - f(\underline{X}) - f(\underline{Y}) = \sum_{0 < |A| < d} \left(\mathrm{D}_A^X f\right)(\underline{X}) \underline{Y}^A. \tag{2.1}$$

Remark 2.5. We consider

$$U = \{f \in R \mid |f(\underline{X} + \underline{Y}) - f(\underline{Y}) \in J \otimes_k k[\underline{Y}]\}. \tag{2.2}$$

Clearly this is a subalgebra of R, and it is the invariant algebra of the ridge in $\mathbb{A}_k^n$.

Indeed, since the diagonal morphism from R to $R \otimes_k R$ identifies with

$$\begin{aligned} k[\underline{X}] &\to k[\underline{X}, \underline{Y}], \\ f(\underline{X}) &\mapsto f(\underline{X} + \underline{Y}), \end{aligned}$$

then U is the algebra of functions on $\mathbb{A}_k^n$ such that for every k-scheme S and every S-point (u, v) of $F \times_k \mathbb{A}_k^n$, we have $f(u + v) = f(u)$. Let's call Π the following morphism

$$\begin{array}{cccccc} \Pi & : & R & \to & R \otimes_k R & \to & R/J \otimes_k R \\ & & f(\underline{X}) & \mapsto & f(\underline{X}) & \mapsto & f(\underline{X}). \end{array}$$

Elements of U are those whose images by Δ and by Π are the same, hence it is the kernel of $\Delta - \Pi$. This means it is the kernel of the double morphisme (Δ, Π). Since R has a graded structure, it inherits also a graded structure and from Formulae (2.1) and (2.2), for $d \in \mathbb{N}$ we have

$$U_d = \left\{ f \in J_{d'} \mid \mathrm{D}_A^X f \in J, d \leq d', d = d' - |A| \right\}. \tag{2.3}$$

By Taylor formula, for all $f \in U_d$ and for all multi-indices A, $|A| \leq d$, $\mathrm{D}_A^X f \in U_{d-|A|}$.

Lemma 2.6. *With notations as above, let H be a k-graded subalgebra of $k[\underline{X}]$, then the following assertions are equivalent.*

(1) *For all $f \in H_d$, for all multi-index A, $|A| \leq d$, $\mathrm{D}_A^X f \in H_{d-|A|}$.*
(2) *There exist additive homogeneous polynomials $\theta_1, \ldots, \theta_s, \ldots$ such that*

$$H = k[\theta_1, \ldots, \theta_s, \ldots].$$

Furthermore, in positive characteristic p, if the conditions above are fulfilled, up to a re-indexation of the variables, one can take

$$\theta_i = X_i^{p^{\alpha_i}} + t_i(X_{i+1}, \ldots, X_n), \ 1 \leq i \leq s < \infty, \tag{2.4}$$

$\alpha_i \leq \alpha_{i+1}$, $1 \leq i \leq s - 1$ and t_i, additive polynomials, in $k[X_{i+1}, \ldots, X_n]$.

Proof. For $1 \Rightarrow 2$, we follow Giraud's idea [**4**] pages I-29, 30. Let K be the subalgebra of H generated by all additive homogeneous polynomials. Let $N \in \mathbb{N}$ such that $H_d = K_d$ for all $d < N$. Let $f = \sum_{A, |A| = N} f_A \underline{X}^A \in H_N$, $f_A \in k$, we will prove that $f \in K_N$. Let K_{N-} be the algebra generated by $K_0, \ldots, K_{N-1}$, we will prove that f is the sum of elements in K_{N-} and of an additive polynomial.

Let A be the greatest multi-index for lex such that $\underline{X}^A$ is not additive. If A is in $\exp(K_{N-})$, let g be a polynomial in K_{N-} such that its greatest monomial for lex is $\underline{X}^A$. Then the greatest monomial of $(f - f_A g)$ is a $\underline{X}^B$ with $B < A$. By induction, we can find a suitable f such that its greatest non additive monomial for lex is not in $\exp(K_{N-})$. We may assume that A is not the exponent (see Notations 2.2) of an element of K_{N-}. $A := (a_1, \ldots, a_n)$, $a_i = p^{\beta_i} q_i$, q_i relatively prime to p. There exist multi-indices C and D such that $A = C + D$, $\mathrm{D}_C^X \underline{X}^A \neq 0$ and $\mathrm{D}_D^X \underline{X}^A \neq 0$. Indeed, either there are two indices $1 \leq i_0 < i_1 \leq n$ such that $a_{i_0} a_{i_1} \neq 0$, take $C = A - (0, \ldots, 0, i_0, 0, \ldots, 0)$, $D = (0, \ldots, 0, i_0, 0, \ldots, 0)$, either there is only one index $1 \leq i_0 \leq n$ with $a_{i_0} \neq 0$ and $q_{i_0} > 1$, take $C = (0, \ldots, 0, p^{\beta_{i_0}}, 0, \ldots, 0)$ and $D = (0, \ldots, 0, p^{\beta_{i_0}}(q_i - 1), 0, \ldots, 0)$. We have $\mathrm{D}_C^X \underline{X}^A \mathrm{D}_D^X \underline{X}^A = a \underline{X}^A$, $a \in k^*$. By hypothesis, $\mathrm{D}_C^X f \in H_{N-|C|} = K_{N-|C|}$ and $\mathrm{D}_D^X f \in H_{N-|D|} = K_{N-|D|}$, A is the exponent of $\mathrm{D}_C^X \underline{X}^A \mathrm{D}_D^X \underline{X}^A \in K_{N-}$. This is a contradiction and A does not exist, hence f is additive.

Let us prove the converse. We denote $g = \sum \lambda_B \theta^B \in k[\theta_1, \dots, \theta_s, \dots]$. We have

$$\begin{aligned} g(\underline{X} + \underline{X}') &= \sum \lambda_B \theta(\underline{X} + \underline{X}')^B \\ &= \sum \lambda_B (\theta(\underline{X}) + \theta(\underline{X}'))^B \\ &= \sum \lambda_B \binom{B}{B'} \theta(\underline{X})^{B-B'} \theta(\underline{X}')^{B'} \\ g(\underline{X} + \underline{X}') &= \sum_C P_C(\theta(\underline{X})) \underline{X}'^C, \end{aligned}$$

with $P_C \in k[\theta_1, \dots, \theta_s, \dots]$.

The next lemma applied to $I = H_{>0}$ ends the proof. □

Lemma 2.7. *Let* $\operatorname{char} k = p > 0$, *with notations as above, let K be a k-graded subalgebra of $k[\underline{X}]$, and I be an ideal generated by a set of additive homogeneous polynomials $\phi_1, \dots, \phi_m, \dots$, then, up to a re-indexation of the variables, we can take*

$$\theta_i = X_i^{p^{\alpha_i}} + t_i(X_{i+1}, \dots, X_n),\ 1 \le i \le s \le n < \infty, \tag{2.5}$$

$\alpha_i \le \alpha_{i+1}$, $1 \le i \le s-1$ and t_i, additive polynomials, in $k[X_{i+1}, \dots, X_n]$.

Proof. We may assume $\deg(\phi_i) \le \deg(\phi_{i+1})$, $1 \le i \le m-1$. By making linear combinations among the ϕ_i of smallest degree, up to a re-indexation of the variables, we may assume that

$$\phi_i = X_i^{p^{\alpha_i}} + t_i(X_{i+1}, \dots, X_n), \tag{2.6}$$

with $\mu_i \neq 0$, ϕ_i of smallest degree.

Claim. We may assume Formula (2.4) for every ϕ_i. Indeed, let i_0 be the smallest index such that we have not this formula for ϕ_{i_0}, then

$$\phi_{i_0} = \sum_{1 \le j \le m} \mu_{i_0,j} X_j^{p^{\alpha_{i_0}}},$$

where $\mu_{i_0,j} \in k$. Assume for instance that $\mu_{i,1} \neq 0$, then we change ϕ_{i_0} in

$$\phi_{i_0,1} := \phi_{i_0} - \frac{\mu_{i,1}}{\mu_1} \phi_1^{p^{\alpha_{i_0} - \alpha_1}} \in k[X_2, \dots, X_n],$$

by an easy induction, we change ϕ_{i_0} in $\phi_{i_0, i_0-1} \in k[X_{i_0}, \dots, X_n]$, the reader ends the claim. □

Corollary 2.8. *Let U be $k[\theta_1, \dots, \theta_s]$, then it is a polynomial algebra of variables $\theta_1, \dots, \theta_s$.*

Proof. Left to the reader. □

Corollary 2.9. *With notations as above, R is a free module over U of basis*

$$\underline{X}^A,\ A = (a_1, \dots, a_n), a_i < p^{\alpha_i},\ 1 \le i \le s.$$

Indeed, if $\exp\left(\underline{X}^A \underline{\theta}^B\right) = \exp\left(\underline{X}^{A'} \underline{\theta}^{B'}\right)$ with $A = (a_1, \dots, a_n), a_i < p^{\alpha_i}$, $1 \le i \le s$, $A' = (a'_1, \dots, a'_n), a'_i < p^{\alpha_i}$, $1 \le i \le s$, $B, B' \in \mathbb{N}^n$, by Formula (2.4), $(A, B) = (A', B')$. So the set of $\underline{X}^A$ is U-free.

Furthermore,

$$\left\{\exp\left(\underline{X}^A\underline{\theta}^B\right);\ A=(a_1,\dots,a_n), a_i<p^{\alpha_i},\ 1\le i\le s,\ B\in\mathbb{N}^n\right\}=\mathbb{N}^n,$$

the set of $\underline{X}^A$ generates S over U.

Proposition 2.10. *Let $(f_1,\dots,f_m)$ be a Giraud basis of I. The $\mathrm{D}_A^X f_i$'s for $|A|<\deg f_i$, $i=1,\dots,m$ generate U.*

Proof. Let V be the subalgebra of R generated by the $\mathrm{D}_A^X f_i$'s for $|A|<\deg f_i$, $i=1,\dots,m$. Since U is as in Formula (2.3), $V\subset U$. The polynomials $\mathrm{D}_A^X f_i$ are homogeneous, so V is a graded subalgebra of U. Denote by U_+ and V_+ the ideals $\bigoplus_{d>0}U_d$ and $\bigoplus_{d>0}V_d$. From Corollary 2.3, we have that $V_+R=J$ therefore $U_+R=V_+R=J$. On the other hand since R is faithfully flat over U (see Corollary 2.9), we have that $V_+U=U_+$. And we deduce by induction on the degree that $V=U$. □

2.2. Naive and formal definitions coincide.

Proposition 2.11. *Let $J\subset k[X_1,\dots,X_n]$ be a homogeneous ideal generated by additive polynomials, then there exists $\mathcal{G}:=\{\phi_1,\dots,\phi_s\}$, a reduced homogeneous Gröbner basis of J, such that, up to a re-indexation of the variables,*

$$\phi_i=\mu_i X_i^{p^{\alpha_i}}+t_i(X_{i+1},\dots,X_n), \tag{2.7}$$

with $\mu_i\neq 0$, $1\le i\le s$, $\alpha_i\le\alpha_{i+1}$, $1\le i\le s-1$ and t_i, additive polynomials, in $k[X_{i+1},\dots,X_n]$.

Furthermore, up to a re-indexation of the variables, Formula (2.7) is true for all reduced homogeneous Gröbner bases of J.

Proof. The first assertion is a direct consequence of Lemma 2.7: it is clear that a set of generators verifying Formula (2.4) is a reduced homogeneous Gröbner basis of J. □

Corollary 2.12. *Let I be a homogeneous ideal of $k[X_1,\dots,X_n]$, let $\mathcal{G}:=\{\gamma_1,\dots,\gamma_s\}$ be any reduced homogeneous Gröbner basis of J the ideal of the ridge of $V(I)$, then*

$$I=(I\cap k[\gamma_1,\dots,\gamma_s])k[X_1,\dots,X_n],$$

$U=k[\gamma_1,\dots,\gamma_s]$ and if K is a k-algebra generated by additive polynomials such that

$$I=(I\cap K)k[X_1,\dots,X_n], \tag{2.8}$$

then $U\subset K$.

Proof. Let $(f_1,\dots,f_m)$ be a Giraud basis of I, by Lemma 2.3, the $\mathrm{D}_A^X f_i$'s generate U, so Proposition 2.10 forces that there exists a reduced Gröbner basis $(\theta_1,\dots,\theta_s)$ of J whose the form is

$$\theta_i=X_i^{p_i^\alpha}+t_i(X_{i+1},\dots,X_n).$$

It follows that $(\theta_1,\dots,\theta_s)$ is a basis of U as a k-algebra. Now, the particular case $A=0$ gives that the f_i's are elements of U, so $I=(I\cap K)k\left[X_1,\dots,X_n\right]$.

Futhermore, as the ridge of J is J, if $\mathcal{G}:=\{\mu_1,\dots,\mu_s\}$ is any reduced homogeneous Gröbner basis of J, Lemma 2.3 and Proposition 2.10 applied to $\mathcal{G}$ give that $U=k[\mu_1,\dots,\mu_s]$.

Let K be a k-algebra generated by additive polynomials such that

$$I = (I \cap K)k\left[X_1, \ldots, X_n\right].$$

We can find a basis $(g_1, \ldots, g_s)$ of I, with $g_i \in K$, and then by Lemma 2.3, the $\mathrm{D}_A^X g_i$'s, with $|A| < \deg f_i$, generate U. But Proposition 2.6 ensures that this derivations are in K. Finally, $U \subset K$. □

Proposition 2.13. *There is a one-to-one correspondance between algebras generated by homogeneous additive polynomials included in $k\left[\underline{X}\right]$ and ideals generated by homogeneous additive polynomials of $k[\underline{X}]$.*

$$\left\{\begin{array}{c}\textit{algebras generated by}\\ \textit{homogeneous additive}\\ \textit{polynomials}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{ideals generated by}\\ \textit{homogeneous additive}\\ \textit{polynomials}\end{array}\right\}$$

$$\begin{array}{ccc} A & \rightarrow & A_+k\left[\underline{X}\right] \\ k\left[\underline{X}\right]^{V(J)} & \leftarrow & J \end{array}$$

This correspondance preserves the inclusion.

Example 2.14. Let us explain the correspondance with an example in an algebraic closed field of characteristic 3. Denote by U the algebra generated by X^3 and $Y^3 + Z^3$. It is clear that the ideal J, image of U by the first arrow, is spanned by these polynomials.

For the reverse, it is enough to find homogeneous additive polynomials in the algebra (as in the proof of Lemma 2.6). Let such a polynomial $P = \alpha X^{3^a} + \beta Y^{3^a} + \gamma Z^{3^a}$ be in this algebra. We have

$$P(\underline{X} + \underline{X}') - P(\underline{X}') = \alpha X^{3^a} + \beta Y^{3^a} + \gamma Z^{3^a}.$$

So the condition $P(\underline{X} + \underline{X}') - P(\underline{X}') \in J \otimes k[\underline{X}']$ implies $\beta = \gamma$ that is to say $P = \alpha X^{3^a} + \beta\left(Y^3 + Z^3\right)^a$. This algebra is also equal to U.

Proof. The first arrow is well-defined. The construction of the second arrow is a consequence of Lemma 2.7 and Corollary 2.8. The bijection is easy to verify. □

Corollary 2.15. *Let I_1 and I_2 be homogeneous ideals of $k[X_1, \ldots, X_n]$, the following assertions are equivalent:*

(1) *the ridge of I_2 contains (as a subscheme) the ridge J_1 of I_1,*
(2) *$I_2 = (I \cap k[\theta_1, \ldots, \theta_s])\, k[X_1, \ldots, X_n]$, where $\mathcal{G} := (\theta_1, \ldots, \theta_s)$ is any reduced homogeneous Gröbner basis of J_1.*

Proof. Left to the reader. □

Now the reader should be convinced that the naive definition 1.2 and the formal definition 2.1 of the *ridge* coincide.

3. An algorithm to compute the ridge and the directrix

3.1. An algorithm to compute a "Giraud basis" of the cone. We want to point out that a "Giraud basis" is far from a "reduced Gröbner basis". Let us give an exemple to explain it.

Example 3.1. $I = (f_1, f_2) \subset k[X, Y]$ where $f_1 = XY$, $f_2 = X^3 + Y^3$. Then (f_1, f_2) is a "Giraud basis" and not a "reduced Gröbner basis", $(f_1, f_2, f_3 = Y^4)$ is a "reduced Gröbner basis".

Remark 3.2. A reduced Gröbner basis of the cone truncated to the degree of the greatest given generator is a "Giraud basis".

We use this easy remark. Our algorithm to compute a "Giraud basis" is almost a Gröbner basis algorithm except we trash out any computed S-polynomial whose degree is greater than the greatest given generator. Actually, since we can know the degree of a S-polynomial before calculating it (recall all our polynomials are homogeneous), if the degree doesn't match our condition, we skip the computing part. Although they have not been implemented, any known improvement for computing a Gröbner basis, such as in [**10, 1**], can be used in this algorithm.

Algorithm 3.3. Giraud basis algorithm.
Input : Homogeneous polynomials $f_1, \ldots, f_m$, such that $\deg f_1 \leq \cdots \leq deg f_m$, generating I.
Ouput : Homogeneous polynomials $g_1, \ldots, g_r$, such that $\deg g_i \leq \deg f_m$, generating I and verifying Giraud's lemma hypotheses.

(1) for i from 1 to m, $f_i \leftarrow f_i / \operatorname{lc}(f_i)$;
(2) compute a Gröbner basis of I by trashing the polynomials with higer degrees than $\deg f_m$;
(3) minimalize and reduce this basis;
(4) return the truncated reduced Gröbner basis.

It should be noted that this kind of algorithm has already been implemented in computer algebra softwares such as Singular.

Example 3.4. Let $I = (f_1, f_2) \subset k[X, Y]$, where $f_1 = X$, $f_2 = X^p + Y^p$ and $p = \operatorname{char} k$. As f_2 is additive, $\mathrm{D}_A^{(X,Y)}(f_2) = 0$, for all A, $|A| < p$, $A \in \exp(I)$. Then (f_1, f_2) is a "Giraud basis" and not a truncated "reduced Gröbner basis" as in Example 3.1. Let us note that the monomial X^p which occurs in the expansion of f_2 is in $\exp(f_1)$, so our algorithm will make an unnecessary computation and give (f_1, Y^p) in output.

3.2. From the "Giraud basis" to the ridge. Following Giraud's Corollary 2.3, once we computed a Giraud basis $(f_1, \ldots, f_m)$ of the ideal of the tangent cone, we compute the set $\mathcal{E} := \left\{\mathrm{D}_A^X f_i,\ 1 \leq i \leq m, |A| < n(i)\right\}$ of generators of the ideal of the ridge. There are two very different cases:

(1) $\operatorname{char} k = 0$;
(2) $\operatorname{char} k = p > 0$.

In case 1, where $\operatorname{char} k = 0$, to compute the ridge (which is also the directrix by Section 1), we propose the following algorithm. Let us note that, in this case, where $\operatorname{char} k = 0$, up to multiplication by invertibles, the D_A^X's are the usual differential operators, hence in step 2, our algorithm may be apparently improved when we have a good implementation of the D_A^X's.

Algorithm 3.5. Ridge generators in characteristic 0 algorithm.
Input : $f_1, \ldots, f_m$ homogeneous polynomials verifying Giraud's lemma hypotheses.
Output : $\mathrm{D}_A^X f_i$'s of degree 1 for all i, $1 \leq i \leq m$.

(1) $L \leftarrow \emptyset$;
(2) for i from 1 to m
    (a) $g_i \leftarrow f_i\left(\underline{X} + \underline{X}'\right)$;
    (b) for each monomial $\underline{X}'^A$ in g_i

(i) $h \leftarrow \text{coeff}\left(g_i, \underline{X}'^A\right)$;
(ii) if $\deg h = 1$, then $L \leftarrow L \cup \{h\}$.

(3) return L.

The case 2 is the most interesting and the most difficult. By Giraud's Corollary 2.3, up to a change of indices on the variables, there is a basis

$$\mathcal{A}F := < \phi_1, \cdots, \phi_\tau >,$$

where $\phi_i = X_i^{p^{q_i}} + \sum_{i+1 \leq j \leq n} \lambda_j X_j^{p^{q_i}}$, with $\lambda_j \in k, 1 \leq i \leq \tau$, $q_1 \leq q_2 \leq \cdots \leq q_\tau$. There is no hope that $\mathcal{A}F \subset \mathcal{E}$, see the example below.

Lemma 3.6. *With hypotheses and notations as above, let us denote*

$$\mathcal{E}_p := \{\psi \in \mathcal{E}, \deg(\psi) \text{ is a } p\text{-power}\}.$$

Then $\mathcal{E}_p$ generates the ideal of the ridge.

Let us note that this generalizes the case 1.

Proof. We start with an example and a remark.

Example 3.7. $I = (f), f = X^p + Y^{p-1}X + Z^p \in k[X, Y]$. Then

$$\begin{aligned} \mathcal{E} &= \{X^p + Y^{p-1}X + Z^p, Y^jX, Y^i,\ 1 \leq i \leq p-1,\ 0 \leq j \leq p-1\}, \\ \mathcal{E}_p &= \{X, Y, X^p + Y^{p-1}X + Z^p\}, \\ \mathcal{A}F &= \{X, Y, Z^p\}. \end{aligned}$$

Remark 3.8. With hypotheses and notations as above, elements of minimal degree of J are additive polynomials.

Indeed, elements of minimal degree of J are linear combinations with coefficients in k of elements of minimal degree of a set of generators. As J is generated by additive polynomials (by a general argument or by Proposition 3.9 below), these elements are linear combinations of additive polynomials, hence they are additive.

Let us go back to the proof of Lemma 3.6. Take any $\psi_0 \in \mathcal{E}$ of minimal degree such that $\deg(\psi_0)$ is not a p-power, let $d := \deg(\psi_0)$. Then the ideals of R, the first generated by $\psi \in \mathcal{A}F$, with $\deg \psi < d$, and the second generated by $\phi_1, \cdots, \phi_i$, $n(i) < d$, $n(i)$ maximal, are equal.

Let $i_1 = \max\{i, \quad n(i) < d\}$, thanks to the fact that $\deg \phi_i > d$ for $i > i_1$, one must have $\psi_0 \in (\phi_1, \ldots, \phi_{i_1})$. Then replace $\mathcal{A}F$ by $\mathcal{A}F - \{\psi_0\}$ and make an induction on the cardinality of the set of generators. □

Proposition 3.9. *Let $\mathcal{G} := (\theta_1, \ldots, \theta_s)$ be a reduced homogeneous Gröbner basis of J the ideal of the ridge of $V(I)$, I be a homogeneous ideal of $k[X_1, \ldots, X_n]$, with $\deg(\theta_i) \leq \deg(\theta_{i+1})$, $1 \leq i \leq s-1$. Then θ_i is an additive polynomial for all i, $1 \leq i \leq s$.*

Proof. By contradiction. Let $\theta_{i_0} \in \mathcal{G}$ with i_0 minimal such that θ_{i_0} is not an additive polynomial, let $d = \deg(\theta_{i_0})$. Then

$$\theta_{i_0} = \sum_{\substack{B \in \mathbb{N}^n, |B| = d \\ B \neq (0, \ldots, p^\alpha, 0, \ldots, 0)}} \mu_B \underline{X}^B + \sum_{\substack{C \in \mathbb{N}^n, |C| = d \\ C = (0, \ldots, p^\alpha, 0, \ldots, 0)}} \mu_C \underline{X}^C,$$

where $\mu_B \in k$ and $\mu_C \in k$

$$\theta_{i_0} =: \tilde{\theta}_{i_0} + \bar{\theta}_{i_0},$$

with $\tilde{\theta}_{i_0} \neq 0$, $\bar{\theta}_{i_0}$ additive.

Let $B_0 := \exp(\tilde{\theta_{i_0}}) =: (b_1, \ldots, b_n)$.

<u>Claim</u>. There exists B' coordinate wise strictly smaller than B_0 such that

$$\psi_0 := \mathrm{D}^X_{B'}(\tilde{\theta_{i_0}}) = \mathrm{D}^X_{B'}(\theta_{i_0}) \neq 0.$$

Indeed, either there exists j, such that $b_j \neq 0$ and $b_j < |B_0|$. Then we can take

$$B' = (b_1, \ldots, b_{i-1}, 0, b_{i+1}, \ldots, b_n)$$

and we have $\mathrm{D}^X_{B'}(\underline{X}^{B_0}) = X_j^{b_j}$ and

$$\psi_0 = \mu_{B_0} X_j^{b_j} + \sum_{\substack{B \neq B_0 \\ (B-B') \in \mathbb{N}^n}} \mu'_B \underline{X}^{B-B'},$$

either $B_0 = (0, \ldots, 0, p^\alpha q, 0, \ldots, 0)$ with q relatively prime to p and q is positive. We take

$$B' = (0, \ldots, 0, p^\alpha (q-1), 0, \ldots, 0),$$

$\mathrm{D}^X_{B'}\left(\underline{X}^{B_0}\right) = (q-1)X_j$ and

$$\psi_0 = (q-1)\mu_{B_0} X_j + \sum_{\substack{B \neq B_0 \\ (B-B') \in \mathbb{N}^n}} \mu'_B \underline{X}^{B-B'}.$$

As the ridge of the ridge is the ridge,

$$0 \neq \psi_0 \in J.$$

As $\deg(\psi_0) < \deg(\theta_{i_0})$, θ_{i_0} is not an element of minimal degree of J: $i_0 \geq 2$. By Lemma 2.3, $\psi_0 \in J$, so $\exp(\psi_0) = B_0 - B' \in \exp(\theta_1, \ldots, \theta_{i_0-1})$, so $B_0 - B' \in \exp(\theta_1, \ldots, \theta_{i_0-1})$, which contradicts the reducedness of $\mathcal{G}$. □

Algorithm 3.10. Computation of θ_i's.
Input : $f_1, \ldots, f_m$ homogeneous polynomials verifying Giraud's lemma hypotheses.
Output : $\mathrm{D}^X_A f_i$'s of degree a p-power for all i, $1 \leq i \leq m$.

(1) $L \leftarrow \emptyset$;
(2) for i from 1 to m
  (a) $g_i \leftarrow f_i\left(\underline{X} + \underline{X'}\right)$;
  (b) for each monomial $\underline{X'}^A$ in g_i
    (i) $h \leftarrow \mathrm{coeff}\left(g_i, \underline{X'}^A\right)$;
    (ii) if $\deg h = p^r$, then $L \leftarrow L \cup \{h\}$.
(3) return a reduced Gröbner basis of L.

This last algorithm gives us a sequence of θ_i's.

Remark 3.11. Calling a Gröbner basis algorithm means that all the computation will be done in S instead of in $k[\theta_1, \ldots, \theta_s]$. Using the techniques of Remark 2.6 and Lemma 2.7, we can find an algorithm with computations in $k[\theta_1, \ldots, \theta_s]$. We do not think we can save a good amount of time nor memory with such an algorithm that would compute the polynomial algebra $k[\theta_1, \ldots, \theta_s]$ hidden in $k\left[\underline{X}\right]$.

Remark 3.12 (Computation of the directrix). In the case where k is perfect, by Definitions 1.1 and 1.2, the directrix is the reduction of the ridge. Furthermore, the θ_i's, $1 \leq i \leq s$ are p^{α_i}-powers, then the ideal of the directrix is

$$(\sqrt[p^{\alpha_1}]{\theta_1}, \ldots, \sqrt[p^{\alpha_s}]{\theta_s}).$$

We do not know any direct method to compute it. Indeed Fröhlich and Shepherdson have even shown that testing if an element is a p-th power is not decidable in general [**2**, Section 7] (see also the example in [**3**, Remark 5.10]).

References

[1] Bardet, M., Faugère, J.-C. and Salvy, B., On the complexity of Gröbner basis computation of regular and semi-regular overdetermined algebraic equations, *Proc. International Conference on Polynomial System Solving* (ICPSS, November 24 - 25 - 26 2004, Paris, France), 71–75.

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

[3] von zur Gathen, J., Hensel and Newton methods in valuation rings, *Mathematics of Computation* **42** (1984), 637–661.

[4] Giraud, J., Étude locale des singularités, *Cours de 3e cycle, Université d'Orsay*, (1971–72).

[5] Giraud, J., Contact maximal en caractéristique positive, *Ann. Sc. ENS 4e série* **8** (1975), 201–234.

[6] Hironaka, H., Resolution of singularities of an algebraic variety over a field of characteristic zero, *Ann. Math.* **79** (1964), 109–326.

[7] Hironaka, H., Characteristic polyhedra of singularities, *J. Math. Kyoto U.* **7**(3) (1967), 251–293.

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

[9] Kollár, J., Lectures on resolution of singularities, *Annals of Mathematics Studies, Princeton University Press, Princeton, NJ* **166** (2007)

[10] Lazard, D., Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations, *Computer algebra* (London, 1983).

Laboratoire d'Informatique de l'École polytechnique, École polytechnique, Route de Saclay, 91128 Palaiseau Cedex, France

E-mail address: `berthomieu@lix.polytechnique.fr`

Laboratoire de Mathématiques de Versailles, Université de Versailles–St-Quentin-en-Yvelines, 45 avenue des États-Unis, 78035 Versailles Cedex, France

E-mail address: `hivert@math.uvsq.fr`

Laboratoire de Mathématiques de Versailles, Université de Versailles–St-Quentin-en-Yvelines, 45 avenue des États-Unis, 78035 Versailles Cedex, France

E-mail address: `mourtada@math.uvsq.fr`