

# Quelques remarques sur la complexité du calcul des projections d'une courbe projective

Isabel Bermejo\*

Monique Lejeune-Jalabert<sup>†</sup>

1996

## Abstract

Our main result is that the complexity of computing linear projections of an equidimensional, but non necessarily reduced, curve  $\mathcal{C}$  in  $\mathbb{P}_K^n$ , (or equivalently the degree-complexity of the Gröbner basis computation for elimination orders) has its maximal value, namely Bayer's bound  $m_0$ , if and only if the smallest linear subspace containing  $\mathcal{C}$  is a plane. If this is so,  $m_0$  coincides with the degree of  $\mathcal{C}$  and with the degree-complexity of the reverse lexicographic ordering.

## Introduction

Soit  $K$  un corps algébriquement clos et soit  $I$  un idéal homogène de l'anneau de polynômes à  $n+1$  variables  $K[X_0, \dots, X_n]$  définissant un sous-schéma  $\mathcal{V}$  de  $\mathbb{P}_K^n$ . On sait que le calcul de la projection de  $\mathcal{V}$  sur  $\mathbb{P}_K^{r-1} = \text{Proj } K[X_{n-r+1}, \dots, X_n]$ ,  $1 \leq r \leq n$ , se ramène à celui d'une base de Gröbner minimale de  $I$  pour un ordre multiplicatif  $(n-r)$ -séparant quelconque sur les monômes en  $X_0, \dots, X_n$ ; voir définitions ci-dessous. L'expérience montre que la complexité du calcul d'une telle base, mesurée par le degré maximal des polynômes qui y figurent, dépend fortement de l'ordre  $(n-r)$ -séparant choisi et qu'elle dépasse en général strictement celle du calcul d'une base de Gröbner minimale de  $I$  pour l'ordre lexicographique inverse. Bayer et Stillman ont fait apparaître le rôle joué par un invariant cohomologique, la régularité, dans ces inégalités ([3], [4]).

---

\*Facultad de Matemáticas, Universidad de La Laguna, 38271-La Laguna, Tenerife (España); email: ibermejo@ull.es

<sup>†</sup>Institut Fourier, Université J. Fourier, CNRS, UMR 5582, BP 74, 38402-Saint Martin d'Hères (France); email: lejeune@puccini.ujf-grenoble.fr

Toutefois, si  $I$  est saturé (i.e. si c'est le plus grand idéal définissant  $\mathcal{V}$ ), la complexité des différents calculs précédents peut atteindre l'entier  $m_0$ , dépendant uniquement du polynôme de Hilbert de  $I$ , borne universelle de la complexité du calcul de n'importe quelle base de Gröbner de  $I$ , obtenue auparavant par Bayer dans [1].

Dans ce travail, nous nous intéressons principalement au cas où la dimension de  $\mathcal{V}$  est un et où l'idéal  $I$  est équidimensionnel (i.e. tous les idéaux premiers associés à  $I$  sont de même hauteur), mais non nécessairement radical. L'entier  $m_0$  est alors supérieur ou égal au degré de  $\mathcal{V}$ . Nous montrons (th.2) que si  $\mathcal{V}$  ne rencontre pas le sous-espace  $X_{n-1} = X_n = 0$  - nous disons que les variables  $X_0, \dots, X_n$  sont commodés pour  $\mathcal{V}$  - la borne  $m_0$  est atteinte pour un ordre multiplicatif quelconque vérifiant  $X_i > X_{n-1}$  et  $X_i > X_n$ ,  $0 \leq i \leq n-2$ , si et seulement si  $\mathcal{V}$  est un sous-schéma d'un plan de  $\mathbb{P}_K^n$ . Ces inégalités étant satisfaites par l'ordre lexicographique, par les ordres d'élimination et par l'ordre lexicographique inverse (voir ci-dessous), la complexité de ces différents ordres est alors la même. Il se trouve qu'elle coïncide avec le degré de  $\mathcal{V}$  et la régularité de  $I$ .

Par ailleurs, un exemple (ex. 3) d'une courbe intègre, arithmétiquement intersection complète dans  $\mathbb{P}_K^3$  montre que la complexité du calcul de la projection d'une courbe qui n'est pas contenue dans un plan peut dépasser strictement son degré, même si l'ordre utilisé est un ordre d'élimination. Il suffit, par contre, qu'une courbe intègre de  $\mathbb{P}_K^3$  soit définie par des équations binomiales pour empêcher ce dépassement (th. 3).

Nos démonstrations sont basées sur une démonstration combinatoire élémentaire des inégalités de Bayer [1] et Möller-Mora [10], spécifique à la dimension un. C'est l'objet du §1. Les énoncés précédents sont démontrés aux §2 et 3.

Nous rappelons maintenant quelques définitions et résultats classiques et nous fixons quelques notations qui seront utilisées dans toute la suite.

Pour tout polynôme  $f \neq 0$ ,  $f = \sum c_\alpha \underline{X}^\alpha \in K[\underline{X}] := K[X_0, \dots, X_n]$  on note  $\exp f$  le plus grand  $\alpha$  pour l'ordre  $>$  tel que  $c_\alpha \neq 0$  et on pose  $\text{in} f = c_{\exp f} \underline{X}^{\exp f}$ . Pour tout idéal homogène  $I \neq (0)$  de  $K[\underline{X}]$ , l'ensemble

$$\exp I = \bigcup_{f \in I \setminus \{0\}} \exp f + \mathbb{N}^{n+1}$$

est stable par l'addition de  $\mathbb{N}^{n+1}$ . On dit que c'est un *E-ensemble*. Tout E-ensemble possède une unique frontière (i.e. une famille génératrice) de

cardinal minimal qu'on appelle son *escalier*. On désigne l'escalier de  $\text{expI}$  par  $\text{escI}$ . On note  $D(E)$  (resp.  $D(I)$ ) le degré maximal des éléments de l'escalier d'un  $E$ -ensemble  $E \subset \mathbb{N}^{n+1}$  (resp.  $\text{escI}$ ).

L'ensemble  $\{\underline{X}^\alpha; \alpha \in \text{escI}\}$  est un système de générateurs minimal de l'idéal monomial  $\text{inI}$  engendré par  $\{\text{inf}; f \in I \setminus \{0\}\}$ . Une *base de Gröbner* de  $I$  pour l'ordre  $>$  est un ensemble fini de polynômes homogènes  $\{g_1, \dots, g_t\}$  de  $I$  tel que  $\{\text{ing}_1, \dots, \text{ing}_t\}$  engendre  $\text{inI}$ . Si  $g_1, \dots, g_t$  est une base de Gröbner minimale de  $I$ , on a donc  $D(I) = \max_{1 \leq i \leq t} \deg(g_i)$ .

Quelque soit l'ordre considéré, la valeur en  $s \in \mathbb{N}$  de la fonction de Hilbert  $H_I$  d'un idéal homogène  $I$  est

$$H_I(s) = \# \left\{ \alpha \in \mathbb{N}^{n+1} \setminus \text{expI}; |\alpha| = \alpha_0 + \dots + \alpha_n = s \right\}.$$

La régularité  $H(I)$  de  $H_I$  est le plus petit entier à partir duquel la valeur de la fonction de Hilbert coïncide avec celle du polynôme de Hilbert  $P_I$ . On désigne le degré d'un sous-schéma  $\mathcal{V}$  de  $\mathbb{P}_K^n$  par  $\deg \mathcal{V}$  et son genre arithmétique par  $p_a$ . Si la dimension de  $\mathcal{V}$  est  $d-1$ , on dit que les variables  $X_0, \dots, X_n$  sont *commodes* pour  $\mathcal{V}$  si  $\mathcal{V}$  ne rencontre pas le sous-espace de  $\mathbb{P}_K^n$  défini par  $X_{n-d+1} = \dots = X_n = 0$ .

Un ordre multiplicatif  $>$  sur l'ensemble des monômes de  $K[X_0, \dots, X_n]$  identifié avec  $\mathbb{N}^{n+1}$  est  $(n-r)$ -séparant ( $1 \leq r \leq n$ ) s'il vérifie la condition suivante:

$$\forall \alpha \in \mathbb{N}^{n+1-r} \setminus \{0\} \text{ et } \forall \beta \in \mathbb{N}^r \setminus \{0\} : (\alpha, 0) > (0, \beta).$$

L'ordre lexicographique ( $\alpha > \beta$  si la première coordonnée non nulle de  $\alpha - \beta$  est positive) est  $(n-r)$ -séparant pour tout  $r$ ,  $1 \leq r \leq n$ . Par contre, pour tout  $r$ ,  $1 \leq r \leq n$ , l'ordre lexicographique inverse ( $\alpha = (\alpha_0, \dots, \alpha_n) > \beta = (\beta_0, \dots, \beta_n)$  si  $|\alpha| = \alpha_0 + \dots + \alpha_n > |\beta| = \beta_0 + \dots + \beta_n$ , ou si  $|\alpha| = |\beta|$  et la dernière coordonnée non nulle de  $\alpha - \beta$  est négative) n'est pas  $(n-r)$ -séparant.

Pour tout  $r$ ,  $1 \leq r \leq n$ , le  $(n-r)$ -ordre d'élimination ( $\alpha = (\alpha_0, \dots, \alpha_n) > \beta = (\beta_0, \dots, \beta_n)$  si  $\alpha_0 + \dots + \alpha_{n-r} > \beta_0 + \dots + \beta_{n-r}$ , ou si  $\alpha_0 + \dots + \alpha_{n-r} = \beta_0 + \dots + \beta_{n-r}$  et  $\alpha > \beta$  pour l'ordre lexicographique inverse) est aussi  $(n-r)$ -séparant.

Si l'ordre est  $(n-r)$ -séparant, les polynômes d'une base de Gröbner de  $I$  qui ne dépendent que des variables  $X_{n-r+1}, \dots, X_n$  forment une base de Gröbner de  $I \cap K[X_{n-r+1}, \dots, X_n]$  pour l'ordre induit, en particulier un système de générateurs.

## 1. Les inégalités

**Théorème 1** Soit  $I \neq (0)$  un idéal homogène (resp. saturé) de  $K[X_0, \dots, X_n]$  définissant une courbe ( non nécessairement réduite )  $\mathcal{C}$  de  $\mathbb{P}_K^n$ . Si les variables  $X_0, \dots, X_n$  sont commodes pour  $\mathcal{C}$ , pour tout ordre multiplicatif vérifiant  $X_i > X_{n-1}$  et  $X_i > X_n$ ,  $0 \leq i \leq n-2$ , on a  $D(I) \leq \max \{H(I), m_0\}$  (resp.  $D(I) \leq m_0$ ), où  $m_0 = \frac{\deg \mathcal{C}(\deg \mathcal{C} - 1)}{2} + 1 - p_a$ .

La démonstration du théorème comporte plusieurs étapes préliminaires. Tout d'abord, on décompose  $\mathbb{N}^{n+1} \setminus \exp I$  en la réunion disjointe d'un "cylindre" ayant pour base le complémentaire d'un E-ensemble dans  $\mathbb{N}^{n-1} \times (0,0)$  et pour directrice  $(0, \dots, 0) \times \mathbb{N}^2$ , et d'une partie "résiduelle"  $\mathcal{R}$ , et on exprime le polynôme de Hilbert de  $I$  comme une perturbation du polynôme de Hilbert de l'idéal monomial  $\tilde{I}$  tel que  $\mathbb{N}^{n+1} \setminus \exp \tilde{I}$  se réduise à la partie cylindrique de  $\mathbb{N}^{n+1} \setminus \exp I$  (lemme 1).

On majore ensuite  $D(\tilde{I})$ , la régularité de la fonction de Hilbert de  $\tilde{I}$  et le genre arithmétique de la courbe  $\tilde{\mathcal{C}}$  de  $\mathbb{P}_K^n$ , de même degré que  $\mathcal{C}$ , définie par  $\tilde{I}$  en fonction du degré de  $\tilde{\mathcal{C}}$  (lemme 2).

Puis on examine les perturbations apportées au genre arithmétique et à la régularité de la fonction de Hilbert de  $I$  par la présence de  $\mathcal{R}$  (lemme 3).

Enfin, on exploite une remarque élémentaire sur les escaliers de  $\mathbb{N}^2$ , pour déduire du lemme 3 une majoration du degré de certains éléments significatifs de  $\exp I$  (lemme 4).

Soit  $p: \mathbb{N}^{n+1} \rightarrow \mathbb{N}^{n-1}$  la projection  $p(\alpha_0, \dots, \alpha_n) = (\alpha_0, \dots, \alpha_{n-2})$ . Remarquons d'abord que  $p(\exp I \cap [\mathbb{N}^{n-1} \times (0,0)])$  et  $p(\exp I)$  sont des E-ensembles de  $\mathbb{N}^{n-1}$  emboîtés.

Pour tout  $j$ ,  $0 \leq j \leq n-2$ , il existe un entier positif  $r_j$  tel que  $X_j^{r_j} \in \exp I$ . En effet, puisque les variables  $X_0, \dots, X_n$  sont commodes pour  $\mathcal{C}$ , pour tout  $j$ ,  $0 \leq j \leq n-2$ , il existe un polynôme homogène non constant à coefficients dans  $K[X_{n-1}, X_n]$ ,  $X_j^{r_j} + A_{j_1} X_j^{r_j-1} + \dots + A_{j_{r_j}}$ , qui est dans  $I$ . On vérifie par récurrence sur  $\gamma = \alpha + \beta$  qu'on a  $X_j^\gamma > X_{n-1}^\alpha X_n^\beta$  pour tout  $j \neq n-1, n$  en utilisant le fait que l'ordre est multiplicatif et que  $X_j > X_{n-1}, X_n$ .

Il en résulte que

$$\mathbb{N}^{n-1} \setminus p(\exp I) \text{ et } F := p(\exp I) \setminus p(\exp I \cap [\mathbb{N}^{n-1} \times (0,0)])$$

sont des sous-ensembles finis de  $\mathbb{N}^{n-1}$  et on a la partition

$$\mathbb{N}^{n+1} \setminus \text{expI} = \left\{ \left[ \mathbb{N}^{n-1} \setminus \text{p}(\text{expI}) \right] \times \mathbb{N}^2 \right\} \cup \mathcal{R}$$

où  $\mathcal{R} = \bigcup_{\alpha \in F} \{ \alpha \times [\mathbb{N}^2 \setminus E_\alpha] \}$  avec  $E_\alpha = \{ (\alpha_{n-1}, \alpha_n) \in \mathbb{N}^2; (\alpha, \alpha_{n-1}, \alpha_n) \in \text{expI} \}$ .

Par définition de F, si  $\alpha \in F$  on a  $E_\alpha \neq \emptyset$  et  $E_\alpha \neq \mathbb{N}^2$  et c'est un E-ensemble de  $\mathbb{N}^2$ . Nous désignerons par  $H(E_\alpha)$  ou *régularité* de  $E_\alpha$  (resp.  $H(\mathcal{R})$  ou *régularité* de  $\mathcal{R}$ ) le plus petit entier s à partir duquel

$$\# \{ (\alpha_{n-1}, \alpha_n) \in \mathbb{N}^2 \setminus E_\alpha; \alpha_{n-1} + \alpha_n = s \} \quad (\text{resp. } \# \{ \beta \in \mathcal{R}; |\beta| = s \})$$

est constant et par  $\text{deg}E_\alpha$  ou *degré* de  $E_\alpha$  (resp.  $\text{deg}\mathcal{R}$  ou *degré* de  $\mathcal{R}$ ) la valeur de cette constante.

On en déduit immédiatement l'inégalité

$$H(\mathcal{R}) \leq \max_{\alpha \in F} \{ |\alpha| + H(E_\alpha) \} \quad (\star)$$

ainsi que le

**Lemme 1** Soit  $\tilde{I}$  l'idéal de  $K[X_0, \dots, X_n]$  engendré par  $\underline{X}^\alpha$ ,  $\alpha \in \text{p}(\text{expI})$ . On a  $P_I(T) - P_{\tilde{I}}(T) = \text{deg}\mathcal{R} = \sum_{\alpha \in F} \text{deg}E_\alpha$ .

**Lemme 2** Soit  $\tilde{C}$  la courbe de  $\mathbb{P}_K^n$  (de même degré que  $C$ ) définie par l'idéal  $\tilde{I}$  ci-dessus. On a  $P_{\tilde{I}}(T) = \sum_{\alpha \in \mathbb{N}^{n-1} \setminus \text{p}(\text{expI})} (T+1 - |\alpha|)$  et les inégalités:

$$(i) \quad D(\tilde{I}) \leq \text{deg}\tilde{C}.$$

$$(ii) \quad H(\tilde{I}) \leq \text{deg}\tilde{C} - 2.$$

$$(iii) \quad 0 \leq \tilde{p}_a \leq \frac{(\text{deg}\tilde{C}-1)(\text{deg}\tilde{C}-2)}{2} \quad \text{où } \tilde{p}_a \text{ est le genre arithmétique de } \tilde{C}.$$

De plus,  $\tilde{p}_a = \frac{(\text{deg}\tilde{C}-1)(\text{deg}\tilde{C}-2)}{2}$  si et seulement si il existe  $i$ ,  $0 \leq i \leq n-2$ , tel que

$$\tilde{I} = (X_0, \dots, X_{i-1}, X_i^{\text{deg}\tilde{C}}, X_{i+1}, \dots, X_{n-2}).$$

*Démonstration.* Pour  $s \gg 0$ , le nombre de points du réseau  $\mathbb{Z}^{n+1}$  de degré s dans le cylindre  $\mathbb{N}^{n+1} \setminus \text{expI}$  est  $\sum_{\alpha \in \mathbb{N}^{n-1} \setminus \text{p}(\text{expI})} (s+1 - |\alpha|)$ . D'où le calcul de

$P_{\tilde{I}}$ . En particulier,  $\text{deg}\tilde{C} = \# [\mathbb{N}^{n-1} \setminus \text{p}(\text{expI})]$  et pour tout  $\alpha \in \mathbb{N}^{n-1} \setminus \text{p}(\text{expI})$ , on a  $|\alpha| \leq \text{deg}\tilde{C} - 1$ . D'où (i) et (ii).

On déduit aussi de l'expression de  $P_{\tilde{I}}(T)$  que

$$\tilde{p}_a = 1 + \sum_{\alpha \in \mathbb{N}^{n+1} \setminus \exp \tilde{I}} (|\alpha| - 1) = \sum_{\alpha \in \mathbb{N}^{n+1} \setminus \exp \tilde{I}} |\alpha| - (\deg \tilde{\mathcal{C}} - 1).$$

Si  $\alpha_0 < \alpha_1 < \dots < \alpha_{\deg \tilde{\mathcal{C}} - 1}$  sont les éléments de  $\mathbb{N}^{n+1} \setminus \exp \tilde{I}$  rangés par ordre croissant pour un ordre multiplicatif gradué (par exemple l'ordre lexicographique inverse), on a  $|\alpha_i| \leq i$ . D'où  $\sum_{\alpha \in \mathbb{N}^{n+1} \setminus \exp \tilde{I}} |\alpha| \leq \frac{\deg \tilde{\mathcal{C}} (\deg \tilde{\mathcal{C}} - 1)}{2}$ .

D'où (iii) et la caractérisation du cas d'égalité.

**Lemme 3** *On a les inégalités  $0 \leq \tilde{p}_a - p_a \leq m_0 - \deg \mathcal{C}$ . De plus, ou bien  $H(I)$  et  $H(\mathcal{R}) \leq \deg \mathcal{C} - 2$ , ou bien  $H(I) = H(\mathcal{R}) > \deg \mathcal{C} - 2$ .*

*Démonstration.* L'encadrement de  $\tilde{p}_a - p_a$  est une reformulation de la majoration de  $\tilde{p}_a$  obtenue au lemme 2 et de l'inégalité  $\deg \mathcal{R} \geq 0$ . La deuxième assertion est une conséquence immédiate de l'inégalité (ii) du lemme 2.

**Lemme 4** *Soit  $a = (\alpha_0, \dots, \alpha_n) \in \exp I$  tel que  $(\alpha_{n-1}, \alpha_n) \in \text{esc } E_{p(a)}$ . Si  $(\alpha_{n-1}, \alpha_n) \neq (0, 0)$  ou si  $a \in \text{esc } I \cap [\mathbb{N}^{n-1} \times (0, 0)]$  et  $p(a) \notin \text{esc } p(\exp I)$ , alors  $\mathcal{R} \neq \emptyset$  et on a:*

$$(i) |a| \leq \max\{\deg \mathcal{C} - 1, H(I) + 1\}, \text{ si } H(\mathcal{R}) = \max_{\alpha \in F} \{|\alpha| + H(E_\alpha)\}.$$

$$(ii) |a| \leq m_0, \text{ si } H(\mathcal{R}) < \max_{\alpha \in F} \{|\alpha| + H(E_\alpha)\}.$$

La démonstration de ce lemme utilise la remarque suivante:

**Remarque.** Soit  $E$  un  $E$ -ensemble de  $\mathbb{N}^2$  non vide et distinct de  $\mathbb{N}^2$ . Si  $H(E)$  est sa régularité,  $\deg E$  son degré et  $D(E)$  le degré maximal des éléments de l'escalier de  $E$ , alors

(i)  $\#\{\alpha \in \mathbb{N}^2 \setminus E ; |\alpha| = H(E) - 1\}$  est strictement plus petit que  $\deg E$  si et seulement si l'escalier de  $E$  n'a qu'un seul élément. Dans ce cas,  $D(E) = \deg E$  et  $H(E) = D(E) - 1$ .

(ii) Si l'escalier de  $E$  se compose de plus d'un élément, alors  $D(E) \leq H(E)$ .

*Démonstration du lemme 4.* Supposons d'abord que  $(\alpha_{n-1}, \alpha_n) \neq (0, 0)$ . Alors  $p(a) \in F$ ,  $\alpha_{n-1} + \alpha_n \leq H(E_\alpha) + 1$  et  $|a| \leq \max_{\alpha \in F} \{|\alpha| + H(E_\alpha) + 1\}$ , d'après la remarque ci-dessus.

Puisque  $H(\mathcal{R}) \leq \max\{\deg \mathcal{C} - 2, H(I)\}$  d'après le lemme 3, si on se trouve dans le cas (i) on a fini.

Dans le cas (ii), d'après la remarque précédente, il existe  $\alpha_0 \in F$  tel que

$$|\alpha_0| + H(E_{\alpha_0}) = \max_{\alpha \in F} \{|\alpha| + H(E_\alpha)\},$$

l'escalier de  $E_{\alpha_0}$  se compose d'un seul élément et  $\deg E_{\alpha_0} = H(E_{\alpha_0}) + 1$ . Donc,

$$|a| \leq |\alpha_0| + H(E_{\alpha_0}) + 1 = |\alpha_0| + \deg E_{\alpha_0}.$$

La réunion de  $\{\alpha \in F; \deg E_\alpha = 0\}$  et de  $p(\exp I \cap [\mathbb{N}^{n-1} \times (0, 0)])$  est un E-ensemble  $G$  contenu dans  $p(\exp I)$  et  $\alpha_0 \in (p(\exp I) \setminus G) := F_0$ . On a

$$\deg \mathcal{R} = \sum_{\alpha \in F} \deg E_\alpha = \sum_{\alpha \in F_0} \deg E_\alpha \geq \deg E_{\alpha_0} + \#F_0 - 1.$$

D'où compte tenu du lemme 3,

$$|\alpha_0| + \deg E_{\alpha_0} \leq m_0 - [\deg \mathcal{C} + \#F_0 - |\alpha_0| - 1].$$

Or  $\deg \mathcal{C} + \#F_0 = \#[\mathbb{N}^{n-1} \setminus G]$ . Enfin puisque  $\alpha_0 \in \mathbb{N}^{n-1} \setminus G$ , on a  $|\alpha_0| \leq \#[\mathbb{N}^{n-1} \setminus G] - 1$ . D'où l'inégalité annoncée dans le cas (ii).

Supposons maintenant que  $a \in \text{esc} I \cap [\mathbb{N}^{n-1} \times (0, 0)]$  et que  $p(a)$  ne soit pas un élément de l'escalier de  $p(\exp I)$ . Il existe  $a' \in \mathbb{N}^{n-1} \times (0, 0)$  tel que  $a' \notin \text{exp} I$ ,  $a \in a' + \mathbb{N}^{n+1}$ ,  $|a'| = |a| - 1$  et  $p(a') \in p(\exp I)$ . Donc  $p(a') \in F$ . Si on se trouve dans le cas (i), on a fini puisque

$$\max_{\alpha \in F} |\alpha| \leq H(\mathcal{R}) \leq \max\{\deg \mathcal{C} - 2, H(I)\}.$$

Si on se trouve dans le cas (ii),

$$\max_{\alpha \in F} |\alpha| \leq |\alpha_0| + H(E_{\alpha_0}) = |\alpha_0| + \deg E_{\alpha_0} - 1,$$

où  $\alpha_0$  est comme ci-dessus. On conclut en réutilisant la majoration déjà obtenue.

*Démonstration du théorème 1 (cas général).* Tout élément de l'escalier de  $I$  qui n'est pas dans l'escalier de  $\tilde{I}$  satisfait les hypothèses du lemme 4. Puisque  $0 \leq \deg \mathcal{R} \leq m_0 - \deg \mathcal{C}$  (lemme 3), il résulte de l'inégalité (i) du lemme 2 et du lemme 4 que  $D(I) \leq \max\{m_0, H(I)+1\}$ .

Supposons maintenant que  $D(I) > \max\{m_0, H(I)\}$ . Il existe alors un élément  $a = (\alpha, \alpha_{n-1}, \alpha_n) \in \text{esc} I$  tel que  $|a| = D(I) = H(I) + 1 > m_0$ . Donc, d'après l'inégalité (i) du lemme 2,  $a$  satisfait les hypothèses du lemme 4 et  $H(\mathcal{R}) = \max_{\alpha \in F} \{|\alpha| + H(E_\alpha)\}$ . De plus compte tenu du lemme 3, on a  $H(I) = H(\mathcal{R})$ .

Supposons que  $a \notin \mathbb{N}^{n-1} \times (0,0)$ , alors  $\alpha := p(a) \in F$  et  $(\alpha_{n-1}, \alpha_n)$  est un élément de l'escalier de  $E_\alpha$ . On a

$$H(I)+1 = |a| \leq |\alpha| + D(E_\alpha) \leq |\alpha| + H(E_\alpha) + 1 \leq H(\mathcal{R}) + 1 = H(I) + 1$$

d'où  $\alpha_{n-1} + \alpha_n = D(E_\alpha) = H(E_\alpha) + 1$ . On déduit alors de la remarque précédente que  $\deg E_\alpha = \alpha_{n-1} + \alpha_n$  d'où  $\deg \mathcal{R} \geq \alpha_{n-1} + \alpha_n$ .

On vérifie que  $\alpha$  n'est pas un élément de l'escalier de  $p(\text{exp} I)$ . En effet, s'il en était autrement, d'après (i) du lemme 2, on aurait  $|\alpha| \leq \deg \mathcal{C}$  et

$$m_0 + 1 \leq H(I) + 1 = |\alpha| + \alpha_{n-1} + \alpha_n \leq \deg \mathcal{C} + \deg \mathcal{R} \leq m_0.$$

Il existe donc  $\alpha^{(1)} \in F$  tel que  $\alpha \in \alpha^{(1)} + \mathbb{N}^{n-1}$  et  $|\alpha^{(1)}| = |\alpha| - 1$ . Mais le  $E$ -ensemble  $E_{\alpha^{(1)}}$  est contenu dans  $E_\alpha$ , d'où  $\deg E_{\alpha^{(1)}} \geq \deg E_\alpha = \alpha_{n-1} + \alpha_n$  et  $\deg \mathcal{R} \geq 2(\alpha_{n-1} + \alpha_n)$ .

L'élément  $\alpha^{(1)}$  n'est pas non plus un élément de l'escalier de  $p(\text{exp} I)$ . S'il en était autrement, on aurait encore  $|\alpha^{(1)}| \leq \deg \mathcal{C}$  et

$$m_0 + 1 \leq H(I) + 1 \leq |\alpha^{(1)}| + 2(\alpha_{n-1} + \alpha_n) \leq \deg \mathcal{C} + \deg \mathcal{R} \leq m_0.$$

On construirait ainsi une suite infinie  $\alpha, \alpha^{(1)}, \alpha^{(2)}, \dots$  d'éléments de  $F$ . Mais c'est impossible car  $F$  est un ensemble fini.

Supposons maintenant que  $a \in \mathbb{N}^{n-1} \times (0,0)$ . Puisque  $\alpha := p(a)$  n'est pas un élément de l'escalier de  $p(\text{exp} I)$ , il existe  $\alpha^{(1)} \in F$  tel que  $|\alpha^{(1)}| = |\alpha| - 1$  et  $\alpha \in \alpha^{(1)} + \mathbb{N}^{n-1}$ . On a  $H(I) \leq |\alpha^{(1)}| + H(E_{\alpha^{(1)}}) \leq H(\mathcal{R}) = H(I)$  d'où  $H(E_{\alpha^{(1)}}) = 0$ . Il en résulte que l'escalier de  $E_{\alpha^{(1)}}$  n'a qu'un seul élément,  $(\alpha_{n-1}^{(1)}, \alpha_n^{(1)})$ , et que  $\deg E_{\alpha^{(1)}} = \alpha_{n-1}^{(1)} + \alpha_n^{(1)} = 1$ .

Soit  $a^{(1)} = (\alpha^{(1)}, \alpha_{n-1}^{(1)}, \alpha_n^{(1)})$ . Puisque  $a^{(1)} \notin \mathbb{N}^{n-1} \times (0,0)$  et  $|a^{(1)}| = H(I) + 1$ , le même raisonnement que ci-dessus montre que il existe une suite infinie  $\alpha^{(1)}, \alpha^{(2)}, \dots$  d'éléments de  $F$ .



*Démonstration du théorème 1 (cas saturé).* Si  $I$  est un idéal saturé, puisque  $D(I) \leq \max\{H(I), m_0\}$ , le résultat est une conséquence immédiate de la proposition suivante:

**Proposition 1** *Si  $I \subset K[X_0, \dots, X_n]$  est un idéal saturé de hauteur  $n-1$ , alors  $H(I) < m_0$ .*

*Démonstration.* Supposons que les variables  $X_0, \dots, X_n$  soient commodes pour  $I$ . Puisque  $I$  est saturé, ou bien  $X_n$  ou bien  $X_{n-1}$  est non diviseur de zéro dans  $K[X_0, \dots, X_n]/I$ .

Supposons que  $X_n$  soit non diviseur de zéro dans  $K[X_0, \dots, X_n]/I$  et munissons l'ensemble des monômes de  $K[X_0, \dots, X_n]$  de l'ordre lexicographique inverse (si  $X_{n-1}$  est non diviseur de zéro dans  $K[X_0, \dots, X_n]/I$ , on échange les rôles de  $X_n$  et  $X_{n-1}$ ).

Si  $F = \emptyset$ , d'après (ii) du lemme 2 et le lemme 3, on a  $H(I) \leq \deg \mathcal{C} - 2 < m_0$ .

Si  $F \neq \emptyset$ , puisque  $X_n$  est non diviseur de zéro dans  $K[X_0, \dots, X_n]/I$  et l'ordre choisi est l'ordre lexicographique inverse,  $\mathbb{N}^m \setminus \exp I$  est un cylindre ayant pour directrice  $(0, \dots, 0) \times \mathbb{N}$ , d'où pour tout  $\alpha \in F$ , l'escalier de  $E_\alpha$  n'a qu'un seul élément de la forme  $(\alpha_{n-1}, 0)$  et  $H(\mathcal{R}) = \max_{\alpha \in F} \{|\alpha| + H(E_\alpha)\} = \max_{\alpha \in F} \{|\alpha| + \deg E_\alpha - 1\}$ . Supposons que  $H(I) \geq m_0$ . Comme  $m_0 \geq \deg \mathcal{C}$ , il résulte du lemme 3 que  $H(I) = H(\mathcal{R}) \geq m_0$ . Soit  $\alpha$  un élément de  $F$  tel que  $|\alpha| + \deg E_\alpha - 1 = H(\mathcal{R})$ . On a l'inégalité  $\deg E_\alpha + |\alpha| \geq m_0 + 1$ , d'où  $|\alpha| \geq \deg \mathcal{C} + 1 + \sum_{\alpha' \in F \setminus \{\alpha\}} \deg E_{\alpha'} \geq \deg \mathcal{C} + 1$  d'après le lemme 3. Par suite

$\alpha$  n'est pas un élément de l'escalier de  $p(\exp I)$  et il existe  $\alpha^{(1)}$  dans  $F$  tel que  $\alpha$  appartient à  $\alpha^{(1)} + \mathbb{N}^{m-1}$  et  $|\alpha^{(1)}| = |\alpha| - 1$ . Comme  $\deg E_{\alpha^{(1)}} \geq 1$ , on en déduit que  $|\alpha^{(1)}| \geq \deg \mathcal{C} + 1 + \sum_{\alpha' \in F \setminus \{\alpha, \alpha^{(1)}\}} \deg E_{\alpha'}$ , d'où  $\alpha^{(1)}$  n'est

pas un élément de l'escalier de  $p(\exp I)$ . On construit ainsi une suite infinie  $\alpha, \alpha^{(1)}, \dots$  d'éléments de  $F$ , ce qui n'est pas possible. On conclut donc que  $H(I) < m_0$ .

## 2. Le cas limite

Les inégalités du théorème 1 sont optimales comme le montrent les deux exemples suivants:

**Exemple 1 (cas non saturé).** Soit  $I$  l'idéal de  $K[X_0, X_1, X_2, X_3]$  engendré par  $\{X_0^2, X_0 X_2, X_0 X_3^2 + X_1^3, X_1^5\}$ . Cet idéal n'est pas saturé car  $X_2$  et  $X_3$  sont diviseurs de zéro dans  $K[\underline{X}]/I$ . On vérifie, en utilisant [5], que  $B = \{X_0^2, X_0 X_2, X_0 X_3^2 + X_1^3, X_1^5, X_1^3 X_2, X_0 X_1^3\}$  est la base de Gröbner réduite de  $I$  pour l'ordre lexicographique et pour le 0-ordre d'élimination, et que

$$B' = \{X_0^2, X_0 X_2, X_0 X_3^2 + X_1^3, X_0 X_1^2 X_3^2\}$$

est la base de Gröbner réduite de  $I$  pour l'ordre lexicographique inverse. On constate que pour ces ordres  $D(I) = H(I) = m_0 = 5$ .

**Exemple 2 (cas saturé).** Soit  $I$  l'idéal de  $K[X_0, X_1, X_2, X_3]$  engendré par  $\{X_0 - X_1, X_0 X_2, X_0 X_1 - X_1 X_2\}$ . Cet idéal est saturé mais il n'est pas équidimensionnel car  $X_2$  est diviseur de zéro dans  $K[\underline{X}]/I$ . On vérifie que

$$B = \{X_0 - X_1, X_1 X_2, X_1^2\}$$

est la base de Gröbner réduite de  $I$  pour l'ordre lexicographique, le 0-ordre d'élimination et l'ordre lexicographique inverse. On constate que  $D(I) = m_0 = 2$ .

Dans les deux exemples précédents, si on désigne par  $\mathcal{C}$  la courbe de  $\mathbb{P}_K^3$  définie par  $I$ , on a l'inégalité  $D(I) > \deg \mathcal{C}$ . Le théorème suivant montre que si  $I$  est équidimensionnel et la borne  $m_0$  est atteinte, alors  $D(I) = \deg \mathcal{C}$ .

**Théorème 2** Soit  $I \subset K[X_0, \dots, X_n]$  un idéal homogène équidimensionnel définissant une courbe (non nécessairement réduite)  $\mathcal{C}$  de  $\mathbb{P}_K^n$ . Si les variables  $X_0, \dots, X_n$  sont commodes pour  $\mathcal{C}$ , pour tout ordre multiplicatif vérifiant  $X_i > X_{n-1}$  et  $X_i > X_n$ ,  $0 \leq i \leq n-2$ , les assertions suivantes sont équivalentes:

- (a)  $D(I) = m_0$ ,
- (b)  $m_0 = \deg \mathcal{C}$ ,
- (c)  $\mathcal{C}$  est contenue dans un plan de  $\mathbb{P}_K^n$ ,
- (d) il existe  $i$ ,  $0 \leq i \leq n-2$ , tel que  $in I = (X_0, \dots, X_{i-1}, X_i^{\deg \mathcal{C}}, X_{i+1}, \dots, X_{n-2})$ .

Pour démontrer le théorème on a besoin de la remarque et du lemme suivants:

**Remarque.** Sous les hypothèses du théorème 2, pour tout  $j=0, \dots, n-2$ ,  $X_j^{\deg \mathcal{C}} \in \text{inI}$ . En effet, puisque les variables  $X_0, \dots, X_n$  sont commodes pour  $\mathcal{C}$ , pour tout  $j=0, \dots, n-2$ , il existe un entier positif  $r_j$  tel que  $X_j^{r_j} \in \text{inI}$ . L'idéal  $I$  étant équidimensionnel, il résulte alors de [7], §2, cor. 6 que pour tout  $j=0, \dots, n-2$ ,  $I \cap K[X_j, X_{n-1}, X_n]$  est un idéal principal. Le degré de la courbe projective définie par cet idéal est au plus  $\deg \mathcal{C}$ .

**Lemme 5** *Sous les hypothèses du théorème 2, les éléments  $a=(\alpha_0, \dots, \alpha_n) \in \text{expI}$  considérés au lemme 4 vérifient l'inégalité stricte  $|a| < m_0$ .*

*Démonstration.* Remarquons tout d'abord que si  $\deg \mathcal{R} = m_0 - \deg \mathcal{C}$ , alors l'idéal  $\tilde{I} := (\underline{X^\alpha})_{\alpha \in \text{p}(\text{expl})}$  est engendré par  $(X_0, \dots, X_i^{\deg \mathcal{C}}, \dots, X_{n-2})$  pour un  $i$ ,  $0 \leq i \leq n-2$ . Ceci résulte en effet immédiatement du lemme 2, puisque  $m_0 - \deg \mathcal{C} = \frac{(\deg \mathcal{C} - 1)(\deg \mathcal{C} - 2)}{2} - p_a$  et  $\deg \mathcal{R} = \tilde{p}_a - p_a$ , où  $\tilde{p}_a$  et  $p_a$  désignent respectivement le genre arithmétique de la courbe  $\tilde{\mathcal{C}}$  définie par  $\tilde{I}$  et de  $\mathcal{C}$ .

Il suffit de considérer le cas où  $(\alpha_{n-1}, \alpha_n) \neq (0, 0)$  auquel on se ramène comme dans la démonstration du lemme 4. Il résulte de ce lemme et de la proposition 1 que  $|a| \leq m_0$ . Supposons maintenant que  $|a| = m_0$ .

Par hypothèse,  $(\alpha_{n-1}, \alpha_n) \in \text{escE}_{\text{p}(a)}$ . D'où,  $F$  désignant l'ensemble fini de  $\mathbb{N}^{n-1}$  introduit au §1,  $\text{p}(a) \in F$  et

$$|a| = m_0 \leq |\text{p}(a)| + D(\text{E}_{\text{p}(a)}) \leq |\text{p}(a)| + H(\text{E}_{\text{p}(a)}) + 1 \leq \max_{\alpha \in F} \{|\alpha| + H(\text{E}_\alpha)\} + 1.$$

Si l'inégalité (\*) est stricte, on a observé au cours de la démonstration du lemme 4 que le terme de droite dans les inégalités ci-dessus est majoré par  $m_0$ . Sinon il vaut  $H(\mathcal{R}) + 1$ . Mais alors  $H(\mathcal{R}) \geq m_0 - 1 \geq \deg \mathcal{C} - 1$  et d'après le lemme 3,  $H(I)$  et  $H(\mathcal{R})$  sont égaux. Or l'idéal  $I$  étant équidimensionnel,  $H(I) < m_0$  d'après la proposition 1.

Dans tous les cas, ces inégalités sont donc toutes des égalités. En particulier  $D(\text{E}_{\text{p}(a)}) = H(\text{E}_{\text{p}(a)}) + 1$ , d'où l'escalier de  $\text{E}_{\text{p}(a)}$  n'a qu'un seul élément  $(\alpha_{n-1}, \alpha_n)$  et  $\deg \text{E}_{\text{p}(a)} = \alpha_{n-1} + \alpha_n$ .

Il en résulte que  $|a| = m_0 \leq |\text{p}(a)| + \deg \mathcal{R}$ . Par ailleurs, d'après le lemme 3, on a  $\deg \mathcal{R} \leq m_0 - \deg \mathcal{C}$ , d'où  $|\text{p}(a)| \geq \deg \mathcal{C}$ . Si l'inégalité est stricte,  $\text{p}(a)$  n'appartient pas à l'escalier de  $\text{p}(\text{expl})$  d'après l'assertion (i) du lemme 2. Sinon, on a  $\deg \mathcal{R} = m_0 - \deg \mathcal{C}$  et on a remarqué que tout  $\alpha$  dans l'escalier de  $\text{p}(\text{expl})$  vérifie, ou bien  $|\alpha| = 1$ , ou bien  $(\alpha, 0, 0) \in \text{expI}$ . Puisque  $\text{p}(a) \in F$ , ceci empêche encore  $\text{p}(a)$  d'appartenir à l'escalier de  $\text{p}(\text{expl})$ . Il existe donc  $\alpha^{(1)} \in F$  tel que  $\alpha := \text{p}(a) \in \alpha^{(1)} + \mathbb{N}^{n-1}$  et  $|\alpha^{(1)}| = |\alpha| - 1$ . Ici encore  $\text{E}_{\alpha^{(1)}} \subset \text{E}_\alpha$  et  $\deg \text{E}_{\alpha^{(1)}} \geq \deg \text{E}_\alpha = \alpha_{n-1} + \alpha_n$ . D'où  $m_0 \leq \alpha^{(1)} + \deg \mathcal{R}$  et on conclut

que  $\alpha^{(1)}$  n'appartient pas à l'escalier de  $\mathfrak{p}(\exp I)$ . On construit ainsi une suite infinie  $\alpha, \alpha^{(1)}, \alpha^{(2)}, \dots$  d'éléments de  $F$ .

*Démonstration du théorème 2. (a)  $\Rightarrow$  (b)* D'après le lemme 5, si  $D(I) = m_0$ , l'escalier de  $\tilde{I}$  contient un élément de degré  $m_0$ . D'où  $m_0 \leq D(\tilde{I})$ . Or  $D(\tilde{I}) \leq \deg \mathcal{C}$  d'après le lemme 2 et  $\deg \mathcal{C} \leq m_0$  d'après le lemme 3.

*(b)  $\Rightarrow$  (c)* L'assertion à démontrer est indépendante de l'ordre choisi sur les monômes. On peut donc supposer qu'il s'agit de l'ordre lexicographique inverse. Puisque  $m_0 - \deg \mathcal{C} = \frac{(\deg \mathcal{C} - 1)(\deg \mathcal{C} - 2)}{2} - p_a$ , l'égalité (b) implique que  $\deg \mathcal{R} = 0$  et  $\tilde{p}_a = \frac{(\deg \mathcal{C} - 1)(\deg \mathcal{C} - 2)}{2}$  d'après le lemme 3.

L'ordre choisi étant l'ordre lexicographique inverse, si  $F \neq \emptyset$  on a  $\deg \mathcal{R} \neq 0$ . En effet, puisque  $X_n$  est non diviseur de zéro dans  $K[X_0, \dots, X_n]/I$ , comme dans la preuve de la proposition 1, pour tout  $\alpha$  dans  $F$ , l'escalier de  $E_\alpha$  se compose d'un seul élément de la forme  $(\alpha_{n-1}, 0) \neq (0, 0)$ , d'où  $\deg \mathcal{R} \geq \deg E_\alpha > 0$ . On a donc  $F = \emptyset$  d'où  $\text{in} I = (X_0, \dots, X_{i-1}, X_i^{\deg \mathcal{C}}, X_{i+1}, \dots, X_{n-2})$ , d'après (ii) du lemme 2. Le résultat en découle immédiatement.

*(c)  $\Rightarrow$  (d)* Les variables  $X_0, \dots, X_n$  étant commodes pour  $\mathcal{C}$ ,  $\text{in} I$  est contenu dans l'idéal  $(X_0, \dots, X_{n-2})$  et il existe  $i, 0 \leq i \leq n-2$ , tel que les variables  $X_0, \dots, \widehat{X}_i, \dots, X_{n-2}, X_i, X_{n-1}, X_n$  soient commodes pour le plan contenant  $\mathcal{C}$ . Si  $J$  est l'idéal définissant ce plan, on a donc  $\text{in} J = (X_0, \dots, \widehat{X}_i, \dots, X_{n-2}) \subset \text{in} I$ . D'où  $\text{in} I = (X_0, \dots, X_i^r, \dots, X_{n-2})$ . Comme  $\#\mathbb{N}^{n-1} \setminus \mathfrak{p}(\exp I) = \deg \mathcal{C}$ , on a  $r = \deg \mathcal{C}$ .

*(d)  $\Rightarrow$  (a)* Les polynômes de Hilbert de  $I$  et  $\text{in} I$  étant les mêmes, on a  $p_a = \frac{(\deg \mathcal{C} - 1)(\deg \mathcal{C} - 2)}{2}$ , d'où  $m_0 = \deg \mathcal{C}$ . Puisque  $D(I) = D(\text{in} I) = \deg \mathcal{C}$ , on a (a).

**Remarque.** L'équivalence de (b) et (c) ne fait référence à aucun choix de variables, ni d'ordre sur les monômes. On peut la reformuler ainsi:

**Proposition 2** *Soit  $\mathcal{C}$  une courbe ( non nécessairement réduite ) de  $\mathbb{P}_K^n$  n'ayant pas de points immergés. Les assertions suivantes sont équivalentes:*

(i)  $p_a = \frac{(\deg \mathcal{C} - 1)(\deg \mathcal{C} - 2)}{2}$ ,

(ii)  $\mathcal{C}$  est contenue dans un plan de  $\mathbb{P}_K^n$ .

### 3. Le cas des courbes intègres

Remarquons tout d'abord que si  $I$  est un idéal premier de  $K[X_0, \dots, X_n]$  définissant une courbe projective  $\mathcal{C}$  on a  $H(I) \leq \deg \mathcal{C} - 2$ , et si les variables

$X_0, \dots, X_n$  sont commodes pour  $\mathcal{C}$  et l'ordre choisi est l'ordre lexicographique inverse, on a  $D(I) \leq \deg \mathcal{C}$ . En effet, c'est vrai si  $\mathcal{R} = \emptyset$  d'après le lemme 2. Si  $\mathcal{R} \neq \emptyset$  on a déjà observé (proposition 1) que  $H(\mathcal{R}) = \max_{\alpha \in \mathbb{F}} \{|\alpha| + H(E_\alpha)\}$ , d'où  $D(I) \leq \max\{\deg \mathcal{C}, H(I)+1\}$  d'après le lemme 4 et (i) du lemme 2. Or  $I$  étant premier, si  $\text{reg} I$  désigne la régularité de  $I$ , on a  $H(I)+1 \leq \text{reg} I$  d'après [1], II.2.5, et  $\text{reg} I \leq \deg \mathcal{C} - 1$  d'après [8], th. 1.1, et le théorème 2 ci-dessus.

Si l'ordre choisi est l'ordre lexicographique ou un ordre d'élimination,  $D(I)$  peut être strictement plus grand que  $\deg \mathcal{C}$  comme le montre l'exemple suivant:

**Exemple 3.** Soit  $I$  l'idéal de  $K[X_0, X_1, X_2, X_3]$  engendré par

$$\{X_0^5 + X_1^5 + X_2^3 X_3^2, X_0^7 + X_0^6 X_2 + X_3^7\}.$$

Cet idéal est premier d'après l'algorithme de Gianni- Trager-Zacharias, et la courbe qu'il définit est arithmétiquement intersection complète. On vérifie, en utilisant [5], que si l'ordre choisi est l'ordre lexicographique, alors  $D(I) = 43$ . Pour le 0-ordre d'élimination, on obtient  $D(I) = 41$ .

Le théorème suivant montre que si  $I$  est un idéal premier homogène de  $K[X_0, X_1, X_2, X_3]$  engendré par des binômes (i.e.  $\underline{X}^\alpha - C\underline{X}^\beta$ , où  $C$  est dans  $K \setminus \{0\}$ ), pour ces ordres on a  $D(I) \leq \deg \mathcal{C}$ .

**Théorème 3** *Soit  $I$  un idéal premier homogène de  $K[X_0, X_1, X_2, X_3]$  engendré par des binômes définissant une courbe  $\mathcal{C}$  de  $\mathbb{P}_K^3$ . Si les variables  $X_0, \dots, X_3$  sont commodes pour  $\mathcal{C}$ , pour tout ordre 0-séparant vérifiant  $X_1 > X_2, X_3$  on a  $D(I) \leq \deg \mathcal{C}$ .*

La démonstration du théorème utilise le lemme suivant:

**Lemme 6** *Soit  $I$  un idéal premier homogène de  $K[X_0, X_1, X_2, X_3]$  définissant une courbe  $\mathcal{C}$  de  $\mathbb{P}_K^3$ . Si les variables  $X_0, \dots, X_3$  sont commodes pour  $\mathcal{C}$ , pour tout ordre 0-séparant vérifiant  $X_1 > X_2, X_3$ , l'escalier de  $p(\exp I)$  se compose de deux éléments,  $(e, 0)$  et  $(0, r_1)$ , où  $e$  est l'indice de ramification de la projection  $\Pi$  de  $\mathcal{C}$  sur  $\mathbb{P}_K^2 = \text{Proj } K[X_1, X_2, X_3]$  et  $r_1$  est le degré de  $\Pi(\mathcal{C})$ . De plus  $X_1^{r_1} \in I$ .*

*Démonstration.* On désigne par  $K[x_0, x_1, x_2, x_3]$  l'anneau des coordonnées homogènes sur  $\mathcal{C}$  et par  $K(x_0, x_1, x_2, x_3)$  son corps des fractions.

L'idéal  $I \cap K[X_1, X_2, X_3]$  est engendré par le seul élément de la base de Gröbner réduite de  $I$  qui appartient à  $K[X_1, X_2, X_3]$ , qui est de la forme  $X_1^{r_1} + A_1 X_1^{r_1-1} + \dots + A_{r_1}$ , où  $A_1, \dots, A_{r_1} \in K[X_2, X_3]$ . D'où  $X_1^{r_1} \in \text{in}I$  et  $(0, r_1)$  est un élément de l'escalier de  $p(\text{exp}I)$  et si  $K(x_2, x_3)$  est identifié à  $K(X_2, X_3)$ , alors  $T^{r_1} + A_1 T^{r_1-1} + \dots + A_{r_1}$  est le polynôme minimal de  $x_1$  sur  $K(x_2, x_3)$ , d'où  $[K(x_2, x_3)(x_1) : K(x_2, x_3)] = r_1$ .

Si  $f(T) = T^e + B_1 T^{e-1} + \dots + B_e \in K(x_1, x_2, x_3)[T]$  est le polynôme minimal de  $x_0$  sur  $K(x_1, x_2, x_3)$ , alors il existe  $C \in K[x_2, x_3]$  tel que  $Cf(T)$  soit un polynôme à coefficients dans  $K[x_1, x_2, x_3]$  et  $Cf(x_0) = 0$ . Il existe donc un polynôme  $CX_0^e + C_1 X_0^{e-1} + \dots + C_e$ , où  $C_1, \dots, C_e \in K[X_1, X_2, X_3]$ , qui appartient à  $I$ , d'où  $(e, 0)$  est un élément de  $p(\text{exp}I)$ .

Puisque  $\deg \mathcal{C} = [K(x_0, x_1, x_2, x_3) : K(x_2, x_3)] = er_1$ , on a  $\#[\mathbb{N}^2 \setminus p(\text{exp}I)] = er_1$  d'où le résultat.

Il suffit maintenant d'observer que si  $\mathcal{R} \neq \emptyset$ , alors  $H(\mathcal{R}) = \max_{\alpha \in F} \{ |\alpha| + H(E_\alpha) \}$  pour achever la démonstration du théorème 3. C'est l'objet de la proposition suivante:

**Proposition 3** *Sous les hypothèses du théorème 3, si  $\mathcal{R} \neq \emptyset$ , pour tout  $\alpha \in F$  l'escalier de  $E_\alpha$  se compose d'un seul élément.*

*Démonstration.* Remarquons tout d'abord que puisque  $\mathcal{R} \neq \emptyset$ ,  $\mathcal{C}$  n'est pas contenue dans un plan d'après le théorème 2. Les éléments de la base de Gröbner réduite de  $I$  sont donc des binômes  $\underline{X}^\alpha - C\underline{X}^\beta$ , où  $C \in K \setminus \{0\}$  et  $\text{PGCD}(\underline{X}^\alpha, \underline{X}^\beta) = 1$ .

D'après le lemme 6 ci-dessus, pour tout  $\alpha \in F$  il existe des entiers  $k, r$ , où  $k \geq 0$  et  $0 \leq r < \deg \Pi(\mathcal{C})$ , tels que  $\alpha = (e+k, r)$ .

On démontre d'abord que si  $\alpha = (e+k, r) \in F$  et si  $(\alpha_2, \alpha_3) \in \text{esc} E_\alpha$ , alors il existe  $k', 0 \leq k' \leq k$ , tel que  $(e+k', 0, \alpha_2, \alpha_3) \in \text{esc} I$ . En effet, il existe des entiers  $k', r', 0 \leq k' \leq k, 0 \leq r' \leq r$ , tels que  $(e+k', r', \alpha_2, \alpha_3) \in \text{esc} I$ . Il s'agit de voir que  $r' = 0$ . L'idéal  $I$  étant premier, l'un des trois entiers  $r', \alpha_2, \alpha_3$  est nul. Comme  $(\alpha_2, \alpha_3) \neq (0, 0)$ , si on avait  $r' \neq 0$ , il existerait  $C \in K \setminus \{0\}$  tel que, ou bien  $B_1 := X_0^{e+k'} X_1^{r'} X_3^{\alpha_3} - C X_2^{e+k'+r'+\alpha_3} \in I$ , ou bien  $B_2 := X_0^{e+k'} X_1^{r'} X_2^{\alpha_2} - C X_3^{e+k'+r'+\alpha_2} \in I$ . Or pour l'ordre lexicographique inverse (resp. pour l'ordre lexicographique inverse où on échange les rôles de  $X_2$  et  $X_3$ ), on a  $\text{exp} B_1 = (0, 0, \deg(B_1), 0)$  (resp.  $\text{exp} B_2 = (0, 0, 0, \deg(B_2))$ ). Pour ces ordres, on aurait donc  $\#[\mathbb{N}^2 \setminus p(\text{exp}I)] = \deg \mathcal{C} = 0$ .

On démontre ensuite que si  $\alpha=(e+k,0)\in F$  et si l'escalier de  $E_\alpha$  se compose des éléments  $(\alpha_2^{(1)},\alpha_3^{(1)}),\dots,(\alpha_2^{(t)},\alpha_3^{(t)})$ , alors il existe  $k_i, 1\leq i\leq t$ , tels que  $0\leq k_1 < k_2 < \dots < k_t \leq k$  et  $(e+k_i,0,\alpha_2^{(i)},\alpha_3^{(i)})\in \text{escI}$ . Il suffit de voir que si  $i\neq j$ , il n'existe pas d'entier  $e'\geq e$  tel que  $(e',0,\alpha_2^{(i)},\alpha_3^{(i)})$  et  $(e',0,\alpha_2^{(j)},\alpha_3^{(j)})$  soient des éléments de  $\text{escI}$ . Or s'il en était autrement, le S-polynôme des deux éléments de la base de Gröbner réduite qui leur sont associés serait un binôme de la forme  $X_1^a X_2^b - C X_1^c X_3^d$  avec  $b$  et  $d\neq 0$  et  $C\in K\setminus\{0\}$  qui n'appartient pas à  $I$ .

On démontre enfin par récurrence sur  $k$  que l'escalier de  $E_\alpha$ , pour  $\alpha=(e+k,r)\in F$ , a un seul élément. Il résulte des deux observations ci-dessus que c'est vrai si  $k=0$ . On en déduit aussi, en utilisant l'hypothèse de récurrence et les inclusions  $E_{(e,0)} \subseteq E_{(e+1,0)} \subseteq \dots \subseteq E_{(e+k,0)}$  que ou bien  $\text{esc}E_\alpha$  a un seul élément ou bien  $\text{esc}E_\alpha = \{(\alpha_2^{(1)},\alpha_3^{(1)}), (\alpha_2^{(2)},\alpha_3^{(2)})\}$  et on a  $(e+k-1,0,\alpha_2^{(1)},\alpha_3^{(1)})\in \text{escI}$  et  $(e+k,0,\alpha_2^{(2)},\alpha_3^{(2)})\in \text{escI}$ . Le S-polynôme des deux éléments de la base de Gröbner réduite associés à ces éléments de  $\text{escI}$  serait alors un binôme de la forme  $X_0 X_1^a X_2^b - C X_1^c X_3^d$  ou  $X_0 X_1^a X_3^b - C X_1^c X_2^d$  avec  $b$  et  $d\neq 0$  et  $C\in K\setminus\{0\}$  selon que  $\alpha_2^{(2)} > \alpha_2^{(1)}$  et  $\alpha_3^{(2)} < \alpha_3^{(1)}$  ou que  $\alpha_2^{(2)} < \alpha_2^{(1)}$  et  $\alpha_3^{(2)} > \alpha_3^{(1)}$ .

On a déjà vu que  $a\geq c$  est impossible. Si  $a < c$ , alors  $(1,0,b,0)$  ou  $(1,0,0,b)\in \text{expI}$ . D'où  $e=1$  et  $(b,0)$  ou  $(0,b)\in E_{(e,0)}$  selon que  $\alpha_3^{(1)} > \alpha_3^{(2)}$  ou  $\alpha_2^{(1)} > \alpha_2^{(2)}$ . Or l'escalier de  $E_{(e,0)}$  a un seul élément  $(\alpha,\beta)\in E_{(e+k-1,0)} = (\alpha_2^{(1)},\alpha_3^{(1)})+\mathbb{N}^2$ . C'est encore impossible. On conclut que  $\text{esc}E_\alpha$  a un seul élément.

## Bibliographie

- [1] Bayer D.; *The Division Algorithm and the Hilbert Scheme*, Ph.D. Thesis Harvard University, 1982.
- [2] Bayer D. et Mumford D.; *What Can Be Computed in Algebraic Geometry?*, in *Computational Algebraic Geometry and Commutative Algebra*, Proceedings Cortona 1991 (D. Eisenbud and L. Robbiano, Eds.), Cambridge University Press, 1993, 1-48.
- [3] Bayer D. et Stillman M.; *A Criterion for Detecting m-regularity*, Invent. Math. 87 (1987), 1-11.
- [4] Bayer D. et Stillman M.; *A Theorem on Refining Division Orders by the Reverse Lexicographic Order*, Duke Math. Journal 55 (2) (1987), 321-328.

- [5] Bayer D. et Stillman M. ; *Macaulay, a Computer System for Computing in Commutative Algebra and Algebraic Geometry*, 1989.
- [6] Bermejo I.; *Sur les degrés d'une base standard minimale pour l'ordre lexicographique d'un idéal dont la variété des zéros est Cohen-Macaulay de dimension 1*, C.R. Acad. Sci. Paris Série I Math. 310 (1990), 591-594.
- [7] Bourbaki N.; *Algèbre Commutative*, Ch.8, Masson, 1985.
- [8] Gruson L., Lazarsfeld R. et Peskine C.; *On a Theorem of Castelnuovo, and the Equations Defining Space Curves*, Invent. Math. 72 (1983), 491-506.
- [9] Lejeune-Jalabert M.; *Effectivité de calculs polynomiaux*, Cours de D.E.A., Grenoble, 1984-85.
- [10] Möller H. et Mora F.; *Upper and Lower Bounds for the Degree of Gröbner Bases*, Proc. EUROSAM 84, Lecture Notes in Computer Science 174, 1984.