Math. Nachr. 149 (1990) 231–253

# Nullstellensatz effectif et Conjecture de Serre (Théorème de Quillen-Suslin) pour le Calcul Formel

Par NOAÏ FITCHAS[1]) (Buenos Aires) et ANDRÉ GALLIGO (Nice)

(Reçu le 16 novembre 1988)

**Abstract.** Let $k$ be an arbitrary field, $X_1, \ldots, X_n$ indeterminates over $k$ and $F_1, \ldots, F_s \in k[X_1, \ldots, X_n]$ polynomials of maximal degree $d := \max_{1 \leq i \leq s} \deg(F_i)$. We give an elementary proof of the following effective Nullstellensatz: Assume that $F_1, \ldots, F_s$ have no common zero in the algebraic closure of $k$. Then there exist polynomials $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ such that $1 = \sum_{1 \leq i \leq s} P_i F_i$ and

$$\max_{1 \leq i \leq s} (\deg(P_i F_i)) \leq \begin{cases} d^n & \text{for } n > 1 \text{ and } d \geq 3, \\ 3^n & \text{for } n > 1 \text{ and } d = 2, \\ 2d - 1 & \text{for } n = 1. \end{cases}$$

This result has many applications in Computer Algebra. To exemplify this, we give an effective quantitative and algorithmic version of the QUILLEN-SUSLIN Theorem based on our effective Nullstellensatz.

## § 1. Introduction

Le Nullstellensatz de HILBERT démontre que, sur un corps algébriquement clos, l'idéal de polynômes définissant une variété algébrique affine contient 1 si et seulement si la variété est vide. L'objet de ce travail est d'étudier des versions effectives de cet énoncé en vue d'applications en Calcul Formel et en théorie de la Complexité.

Soit $k$ un corps (commutatif) quelconque et $X_0, \ldots, X_n$ des indéterminées sur $k$. Nous notons $\deg(F)$ le degré total du polynôme $F$ de $k[X_0, \ldots, X_n]$.

Nous appelons Nullstellensatz effectif relatif à la fonction $\psi: \mathbb{N}^2 \to \mathbb{N}$ (qu'on appelle une borne) l'énoncé suivant:

soient $F_1, \ldots, F_s \in k[X_1, \ldots, X_n]$ et $d := \max \deg(F_i)$,

alors $1 \in (F_1, \ldots, F_s)$ ssi il existe des polynômes $P_1 \in k[X_0, \ldots, X_n]$ tels que:

$$1 = \sum_{1 \leq i \leq s} P_i F_i \quad \text{et} \quad \max_{1 \leq i \leq s} \left(\deg(P_i F_i)\right) \leq \psi(d, n).$$

[1]) Groupe de travail constitué par Leandro Caniglia, Guillermo Cortiñas, Silvia Danón, Joos Heintz, Teresa Krick, Pablo Solernó.

Des versions de Nullstellensatz existent depuis le début du siecle, de façon implicite chez MACAULAY (voir par exemple [23], chapter I, Art. 16) puis de façon complétement explicite relativement à des fonctions $\psi$ *doublement exponentielles* en $n$ et polynomiales en $d$ (voir [16] et [26]). Ces résultats s'obtiennent essentiellement en bornant les degrés de certains résultants après avoir convenablement préparé les données.

Une borne $\psi(d, n) := d^n$ a été conjecturé depuis longtemps. Un exemple proposé par plusieurs auteurs: MORA, LAZARD, MASSER et PHILIPPON (voir par exemple dans [3]) montre qu'il n'existe pas de borne inférieure à $d^n - d^{n-1}$.

Le premier Nullstellensatz effectif relativement à une $\psi$ *simple exponentielle* en $n$: $\psi(d, n) := 3n^2d^n$ mais pour un corps $k$ *de caractéristique* 0, est dû à BROWNAWELL [3]. La démonstration est difficile: elle utilise des connaissances spécialisée d'analyse complexe notamment un théorème de SKODA (voir [3]) et une théorie de l'elimination assez spécifique [25].

Après cette percée, nous avons démontré dans [4] et [5] un Nullstellensatz effectif pour un corps de caractéristique quelconque et relativement à une borne $\psi$ simple exponentielle:

$$\psi(d, n) := d^{(n+1)(n+2)/2}.$$

Enfin, J. KOLLAR a démontré dans [19] le meilleur résultat actuellement connu pour un corps de caractéristique quelconque, une borne

$$\psi(d, n) := \max\{d^n, 3^n\}, \quad \text{pour } n > 1.$$

La démonstration de [19] est élégante mais fait appel à de le géométrie algébrique approfondie: théorie des faisceaux, cohomologie à support, théorie de l'intersection. Elle reste donc hermétique à la plupart des non spécialistes, notamment aux chercheurs en Calcul Formel qui utilisent plutôt de l'algèbre "classique".

Du point de vue du Calcul Formel, la connaissance d'un Nullstellensatz effectiv avec une borne simple exponentielle permet d'améliorer la compléxité de nombreux algorithmes séquentiels ou parallèles. Par exemple le calcul de la dimension d'une variété algébrique affine, le calcul d'une base standard d'une variété affine de dimension zéro, le test d'appartenance d'un polynôme à un idéal équidimensionel (voir [4], [6], [7]). Egalement, sur un corps algébriquement clos, l'élimination des quantificateurs dans les formules prenexes à nombre d'alternations de quantificateurs fixé (voir [8], [11]) ou le test de "consistence" d'un ensemble semi-algébrique (voir [15]).

Pour illustrer ce type d'application nous donnons, dans la deuxième partie de présent travail, une version effective et tout à fait élémentaire de l'ex-conjecture de SERRE (démontrée en 1976 indépendamment par SUSLIN et QUILLEN). Notre résultat peut être amélioré: une version plus générale et plus précise que nous énonçons sera publiée ultérieurement par le premier auteur [9]. (Voir aussi [27].)

Quoiqu'il existe encore une petite différence entre la borne inférieure de l'exemple de MASSER-PHILIPPON et les bornes supérieures de [3], [4], [5], [19] et [6], du point de vue de la théorie de la complexité et du Calcul Formel le pas essentiel est fait. Nous pensons que dans ces domaines, la recherche va plutôt s'orienter vers l'étude d'algorithmes adaptés à des situations spécifiques: polynômes creux ou donnés par des straight-line-programs (voir [13], [14], [18]).

Dans la première partie de ce travail, nous démontrons un Nullstellensatz effectif relativement à une fonction en $d^{0(n)}$, plus précisément

$$\psi(d, n) := \begin{cases} d^n & \text{pour } n > 1 \text{ et } d \geqq 3, \\ 3^n & \text{pour } n > 1 \text{ et } d = 2, \\ 2d - 1 & \text{pour } n = 1. \end{cases}$$

Notre preuve est complète et élémentaire: nous n'utilisons que des connaissances usuelles que l'on trouve dans les manuels d'algèbre commutative. Nous pensons que cette démonstration pourra être comprise par les chercheurs en Calcul Formel et nous espérons qu'elle contribuera à améliorer les algorithmes existants.

Nous discutons ensuite du lien entre le Nullstellensatz effectif et l'existence d'une syzygie finale (voir aussi [28] et [4]) qui correspond à la notion d' "inconsistance stable" d'une famille de polynômes.

Une autre méthode de recherche explicite d'une famille $(P_i)$ telle que $1 = \sum P_i F_i$ est décrite dans [1]. Cette approche a été exploité dans [3] et parait très prometteuse.

### Schéma de notre preuve du Nullstellensatz effectif

Le cas $n = 1$ étant bien connu, nous nous restreindrons au cas $n > 1$ et $d \geqq 3$. La borne que nous obtiendrons ainsi impliquera également la borne $3^n$ pour $n > 1$ et $d = 2$.

1ère étape: On se ramène au cas $1 \in \mathfrak{I}$ où $\mathfrak{I} = (F_1, \ldots, F_s)$ est une intersection complète de $k[X_1, \ldots, X_n]$, avec $s \leqq n + 1$ et $\deg(F_i) \leqq d$. On homogénéise chaque $F_i$ en un polynôme de même degré $G_i$ de $R := k[X_0, \ldots, X_n]$.

On veut alors majorer $m$ tel que $X_0^m \in (G_1, \ldots, G_s)$.

Pour chaque $i = 1$ à $s$, on regroupe les composantes primaires de $(G_1, \ldots, G_i)$ en composantes à "distance finie" et composantes contenues dans l'hyperplan à l'infini. On note $B_i$ l'intersection des composantes "à distance finie".

On remarque que $B_1 = (G_1)$ et $B_s = (1)$.

2ème étape: Pour chaque $i = 1$ à $s$, on décompose de même

$$(B_i, G_{i+1}) = B_{i+1} \cap \Gamma_{i+1} \cap \Delta_{i+1}.$$

$\Gamma_{i+1}$ désigne l'intersection des composantes *isolées* "à l'infini" et $\Delta_{i+1}$ l'intersection des composantes *immergées* "à l'infini".

Une inégalité de Bézout permet alors de borner $l_{i+1}$ tel que

$$X_0^{l_{i+1}} B_{i+1} \subseteq \Gamma_{i+1}.$$

Plus précisément si $b_i$ désigne la somme des degrés des composantes de $B_i$ (compte tenu des multiplicités) on a $b_{i+1} + l_{i+1} \leqq d b_i$, donc par récurrence $l_{i+1} \leqq d^{i+1}$.

3ème étape: On démontre que pour $c_i$, $1 \leqq i < s$, satisfaisant la formule de récurrence $c_{i+1} \leqq 3c_i + l_{i+1}$, et $c_1 = 0$; on a

$$X_0^{c_i + l_{i+1}} B_{i+1} \subseteq \Delta_{i+1}; \quad \text{d'où} \quad X_0^{c_i + l_{i+1}} B_{i+1} \subseteq (B_i, G_{i+1}).$$

La preuve procède par "dualité": on montre facilement qu'il suffit de majorer $c$ tel que $X_0^c \operatorname{Hom}_R\left(R/\Delta_{i+1}, R/(B_i, G_{i+1})\right) = 0$, et nécessite l'utilisation d'un argument élémentaire d'algèbre homologique que nous avons complétement explicité.

$4^{\text{ème}}$ étape: On utilise cette dernière inclusion pour construire une suite de polynômes $R_i \in B_i$ et une suite de polynômes $A_i$ tels que

$$X_0^{c_i+l_{i+1}} R_{i+1} = R_i + A_i G_{i+1} \quad \text{avec} \quad R_s = 1 \quad \text{et} \quad R_1 \in (G_1).$$

D'où $X_0^m \in (G_1, \ldots, G_s)$, avec $m := \sum c_i + l_{i+1}$ que l'on sait borner par $d^s$ lorsque $d \geqq 3$.

$5^{\text{ème}}$ étape: On améliore cette borne en majorant directement $l_{n+1}$ lorsque $s = n + 1$.

Cette preuve reprend donc l'approche inductive que nous avions décrit dans [4] et [5]. La différence essentielle provient de la $3^{\text{ème}}$ étape (comparer avec [19]). Cette étape permet de profiter complétement des majorations obtenues à chaque pas de la récurrence.

## § 2. Un Nullstellensatz effectif

Dans toute la suite $k$ sera un corps commutatif fixé, de caractéristique positive ou nulle. Nous désignerons par $\bar{k}$ la clôture algébrique de $k$, et par $X_0, \ldots, X_n$ des indéterminées sur $k$.

On considère des polynômes $F_1, \ldots, F_s \in k[X_1, \ldots, X_n]$ dont le maximum des degrés est égal à un entier $d$, on désigne comme d'habitude par $(F_1, \ldots, F_s)$ l'idéal qu'ils engendrent. Nous allons démontrer le théorème suivant.

**Théorème 1** (Hilbert Nullstellensatz effectif; voir [3], [4], [5], [19], [6]). *Supposons $n > 1$ et $d \geqq 3$. $1 \in (F_1, \ldots, F_s)$ si et seulement si il existe des polynômes $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ tels que $1 = \sum_{1 \leqq i \leqq s} P_i F_i$ et $\max_{1 \leqq i \leqq s} \deg(P_i F_i) \leqq d^n$.*

Démonstration. Comme nous l'avons indiqué à la fin de l'introduction, la démonstration est constituée de 5 étapes.

La *$1^{\text{ère}}$ étape* consiste en une préparation des données.

Comme il s'agit de trouver des polynômes $P_i$ de degrés majorés par une constante explicite, la question peut être reformulée en termes d'algèbre linéaire sur $k$, et ne dépend que du plus petit sous-corps qui contient les coefficients des $F_i$. Nous allons donc supposer, sans restriction de généralité, que $k$ est algébriquement clos, soit $k = \bar{k}$ qui est donc infini.

Soit $r$ le degré de transcendance de l'extension de corps $k \subseteq k[F_1, \ldots, F_s]$, alors $r \leqq n$ et $r \leqq s$. Il existe alors $r$ combinaisons linéaires des $F_i$ (à coefficients dans $k$) qui sont algébriquement indépendantes et forment une suite régulière $F_1', \ldots, F_r'$; le degré maximum des $F_i'$ est $d$. D'où une suite d'idéaux équidimensionels de hauteurs $1, 2, \ldots, r$:

$$(F_1') \subset (F_1', F_2') \subset \cdots \subset (F_1', \ldots, F_r') \text{ inclus dans } (F_1, \ldots, F_s) = (1).$$

(Voir [17].)

De plus $k[F_1', \ldots, F_r'] \subseteqq k[F_1, \ldots, F_s]$ est une extension algébrique finie. Sur chaque composante irréductible de l'ensemble des zéros $\{F_1' = \cdots = F_r' = 0\}$, chacune des $F_i$

est nécessairement constante (éventuellement nulle). Donc il existe une autre combinaison linéaire "générique" $F'_{r+1}$ des $F_i$ qui écarte les composantes superflues i.e. telle que

$$\{F'_1 = \cdots = F'_{r+1} = 0\} = \{F_1 = \cdots = F_s = 0\} = \emptyset.$$

Donc $1 \in (F'_1, \ldots, F'_{r+1})$. On peut alors supposer, sans restriction de généralité, $s = r + 1$ et $F'_i = F_i$.

Pour $1 \leqq i \leqq s$, soit $G_i \in k[X_0, \ldots, X_n]$, l'homogénéisé de $F_i$, on a $\deg(G_i) = d$. Pour chaque $i$, $1 \leqq i \leqq s$, on note $B_i$ l'intersection des composantes primaires de $(G_1, \ldots, G_i)$ qui ne contiennent pas $X_0$ dans leur radical, on dira qu'elles sont à "distance finie". En particulier, on a $B_1 = (G_1)$ et $B_s = (1)$.

Dans toute la suite, on est donc réduit à un problème projectif, on utilisera la terminologie et les notations suivantes (voir [24]):

$cf(A)$ désignera le corps de fraction d'un anneau intégre $A$.

$R := k[X_0, \ldots, X_n]$, $R$ est une $k$-algèbre munie de la graduation par le degré total.

$\mathfrak{I}$ étant un idéal homogène de $R$, on notera $\mathrm{rad}(\mathfrak{I})$ le radical de $\mathfrak{I}$ et $\{\mathfrak{I} = 0\}$ la sous-variété fermée de $\mathbb{P}^n$ définie par $\mathfrak{I}$, à laquelle correspond une dimension $\dim\{\mathfrak{I} = 0\}$ et un degré $\deg\{\mathfrak{I} = 0\}$.

Soit $A := R/\mathfrak{I}$, $A$ est une $k$-algèbre graduée et un $R$-module, nous noterons $\dim(A)$ la dimension de Krull (affine) de $A$ et $\deg(A)$ le degré défini par la fonction d'Hilbert de $A$. On a alors $\dim(A) = 1 + \dim\{\mathfrak{I} = 0\}$. Explicitons ceci dans les seuls cas que nous utiliserons dans cet article.

Si $\mathfrak{I}$ est un idéal premier donc $A$ une algèbre intégre, $\dim(A)$ est le degré de transcendance de $cf(A)$ sur $k$, et $\deg(A) = \deg\{\mathfrak{I} = 0\}$.

Si $\mathfrak{I}$ est primaire, $\pi := \mathrm{rad}(\mathfrak{I})$ est premier, $\dim(R/\mathfrak{I}) = \dim(R/\pi)$, $\deg(R/\mathfrak{I})$ est un multiple de $\deg(R/\pi)$. Plus précisément, notons $R_\pi$ la localisation de $R$ en $\pi$ et $l$ la longueur du localisé de $R/\mathfrak{I}$ en $\pi$ (considéré comme module sur $R_\pi$), $l$ est la longueur maximum d'une suite:

$$0 \subset S_1 \subset \cdots \subset S_l = R/\mathfrak{I} \text{ telle que } S_j/S_{j-1} \cong R/\pi \text{ pour } 1 \leqq j \leqq l;$$

on a alors:

$$\deg(R/\mathfrak{I}) = l \deg(R/\pi).$$

Dans le cas où $\mathfrak{I}$ est de dimension pure (i.e. toutes les composantes primaires donnent la même dimension), le degré est la somme des degrés correspondant aux composantes primaires.

Soit $M$ un $R$-module gradué de type fini, on notera $\dim(M)$ la dimension de Krull de $M$, soit $\dim\big(R/\mathrm{ann}(M)\big)$. On notera $M_{X_0}$ le localisé de $M$ en $X_0$.

Avec ces notations, remarquons que pour tout $i$, $1 \leqq i \leqq s$,

(1) $\quad B_i = (G_1, \ldots, G_i)_{X_0} \cap R,$

(2) $\quad B_1 = (G_1),$

(3)' $\quad R/B_i$ est de dimension pure $n - i + 1$;

et $G_{i+1}$ n'est pas diviseur de zéro dans $R/B_i$.

**Notations.** *Pour chaque $i$, $1 \leqq i \leqq s$, on considère une décomposition primaire irredondante, puis on regroupe les composantes en:*

$$(B_i, G_{i+1}) = B_{i+1} \cap \Gamma_{i+1} \cap \Delta_{i+1}.$$

*$\Gamma_{i+1}$ est l'intersection des composantes isolées dont le radical contient $X_0$, $A_{i+1}$ l'intersection des composantes immergées dont le radical contient $X_0$. Ce sont des idéaux homogènes, $\Delta_{i+1}$ n'est pas uniquement déterminé.*

*Lorsque l'on fixera $i$, on notera $A := R/B_i$, $B := B_{i+1}/B_i$, $\Gamma := \Gamma_{i+1}/B_i$, $\Delta := \Delta_{i+1}/B_i$, et $g$ la classe de $G_{i+1}$ dans $A$. D'où*

$$Ag = B \cap \Gamma \cap \Delta.$$

*En raisonnant sur les composantes irréductibles, on voit que $R/\Gamma_{i+1}$ aussi est de dimension pure $n - i$.*

Dans la *2ème étape* nous allons démontrer une version simple et utile de l'inégalité de BÉZOUT (voir aussi [12] Theorem 1, et [4] Proposition 5). Ce résultat est difficilement accessible dans les livres spécialisés (tel que celui de W. FULTON [10]) qui ne traite et même n'énonce que des résultats sur des situations plus sophistiquées. Commençons par bien préciser la définition du degré et à démontrer un lemme simple.

Soient $A$ une $k$-algèbre graduée, $\pi_1, \ldots, \pi_t$ ses idéaux premiers minimaux de hauteur minimale (géométriquement cela correspond aux composantes irréductibles de dimension maximale). On sait qu'il existe une suite de composition $(M_i)_{0 \leqq i \leqq m}$ de $A$, i.e. $0 \subset M_m \subset \cdots \subset M_0 = A$, telle que $M_i/M_{i+1}$ soit isomorphe à $A/p_i$ où $p_i$ est un idéal premier de $A$. Pour $j$ fixé, $1 \leqq j \leqq t$, le nombre de fois où $p_i = \pi_j$ est la longueur long $(A_{\pi_j})$ du localisé de $A$ en $\pi_j$.

**Définition.** $\deg(A) = \sum_{1 \leqq j \leqq t} \text{long}\,(A_{\pi_j}) \deg(A/\pi_j)$.

**Lemme 2.** *Soit $K$ un corps (commutatif) et $D$ une $K$-algèbre de dimension finie. Soit $\mathfrak{I}_1 \cap \cdots \cap \mathfrak{I}_t$ une décomposition primaire irredondante de l'idéal (0) de* D. POSONS *$\pi_j := \text{rad}\,(\mathfrak{I}_j)$, $\lambda_j := \min\{\lambda; \pi_j^\lambda \subset \mathfrak{I}_j\}$ et considérons $\text{long}\,(D_{\pi_j})$ pour tout $j$, $1 \leqq j \leqq t$. Alors:*

$$\sum_{1 \leqq j \leqq t} \lambda_j \dim_K (D/\pi_j) \leqq \sum_{1 \leqq j \leqq t} \text{long}\,(D_{\pi_j}) \dim_K (D/\pi_j) = \dim_K D.$$

Preuve. Remarquons tout d'abord que puisque $D$ est de dimension 0, $\deg(D) = \dim_K(D)$ et pour $1 \leqq j \leqq t$, $\pi_j$ est un idéal maximal, $\deg(D/\pi_j) = \dim_K(D/\pi_j)$, de plus $D/\mathfrak{I}_j = D_{\pi_j}$.

Par le Théorème du Reste Chinois, on a $D \cong D/\mathfrak{I}_1 \oplus \cdots \oplus D/\mathfrak{I}_t$ ce qui entraîne $\dim_K D = \sum_{1 \leqq j \leqq t} \dim_K (D/\mathfrak{I}_j)$. Il suffit donc de considérer les cas $t = 1$, c'est à dire le cas où $D$ est local.

Notons alors $\pi$ l'idéal maximal de $D$ et soit $\lambda$ entier tel que $\pi^\lambda = (0)$ et $\pi^{\lambda-1} \neq (0)$. Dans ce cas nous avons les $\lambda$ inclusions strictes:

$$(0) = \pi^\lambda \subset \pi^{\lambda-1} \subset \pi^{\lambda-2} \subset \cdots \subset \pi \subset D$$

il est alors clair que $\lambda \leqq \text{long}\,(D_\pi)$.

**Proposition 3.** *Soit* $\Gamma = \mathfrak{J}_1 \cap \cdots \cap \mathfrak{J}_s$ *une décomposition primaire irredondante dans l'algèbre* $A$.

*Pour tout* $j$, $1 \leqq j \leqq s$, *posons* $\lambda_j := \min\{\lambda ; (\mathrm{rad}(\mathfrak{J}_j))^\lambda \subset \mathfrak{J}_j\}$. *Alors,* $\sum_{1 \leqq j \leqq s} \deg\big(A/\mathrm{rad}(\mathfrak{J}_j)\big)\lambda_j + \deg(A/B) \leqq \deg(A)\, d$.

**Conséquence.** *Comme* $X_0 \in \mathrm{rad}(\mathfrak{J}_j)$ *pour tout* $1 \leqq j \leqq t$, *on obtiendra* $X_0^{\lambda_j} \in \mathfrak{J}_j$; *donc en posant* $l := \max(\lambda_j)$, *on obtiendra* $X_0^l \in \Gamma$ et $\deg(A/B) + l \leqq \deg(A)\, d$.

Preuve. Rappelons que $A$ est gradué de dimension pure $n - 1 + i$, et que $g$, homogène de degré $d$, est non-diviseur de zéro dans $A$.

Soient $x_0, \ldots, x_n$ les images de $X_0, \ldots, X_n$ dans $A$ et $y_0, \ldots, y_{n-i}$ des combinaisons linéaires "génériques" de $x_0, \ldots, x_n$; elles sont homogènes de degré 1. Les ensembles $\{g, y_1, \ldots, y_{n-i}\}$ et $\{y_0, \ldots, y_{n-i}\}$ sont chacun algébriquement indépendants sur $k$.

Notons $C := k[g, y_1, \ldots, y_{n-1}]$ et $E := k[y_0, \ldots, y_{n-i}]$, ce sont des sous algèbres graduées de $A$.

Par une forme convenable du théorème de normalisation de NOETHER (voir par example [12], Lemma 1) $A$ est un $E$-module de type fini, autrement dit l'extension de $k$-algèbres graduées $E \subseteq A$ est entière.

Par conséquent, il existe une relation de dépendance intégrale de degré minimal $r$ de $g$ sur $E$:

$$(*) \qquad g^r + a_{r-1}g^{r-1} + \cdots + a_0 = 0.$$

Les $a_j$ pour $1 \leqq j \leqq r - 1$ sont nuls ou homogènes de degré $(r - j)\, d$ et $a_0$ est non nul de degré $rd$.

On considère les $a_j \not\equiv 0$ comme des polynômes homogènes en $y_0, \ldots, y_{n-1}$ de degré $(r - j)\, d$. Quitte à effectuer encore un changement linéaire générique des $y_0, \ldots, y_{n-i}$, on peut supposer que le degré en $y_0$ de $a_j \not\equiv 0$ est $(r - j)\, d$. On interprète maintenant (*) comme une relation de dépendance intégrale (de degré $rd$) de $y_0$ sur $C$. Donc $y_0$ est entier sur $C$, ce qui implique que:

$A$ est une extension entière de $C$.

Soient $(0) = \mathfrak{J}_1 \cap \cdots \cap \mathfrak{J}_t$ une décomposition primaire irredondante dans $A$ et soient $\pi_1, \ldots, \pi_t$ les idéaux premiers minimaux de $A$. Fixons momentanément $j$, $1 \leqq j \leqq t$, $\pi := \pi_j$, c'est un idéal homogène. Comme $g$ est non diviseur de zéro et que les $y_0, \ldots, y_n$ sont génériques, les applications canoniques $E \to A/\pi$ et $C \to A/\pi$ sont injectives. Elles définissent donc des extensions entières d'algèbres graduées. Nous identifierons $g, y_0, \ldots, y_n$ avec leurs images dans $A/\pi$.

En considérant les corps de fractions, on obtient des extensions algébriques de corps: $cf(E) \subseteq cf(A/\pi)$ et $cf(C) \subseteq cf(A/\pi)$. $g$ comme élément de $A/\pi$ est entier sur $E$ et $E$ comme anneau de polynômes sur $k$, est intégralement clos. On en déduit que le polynôme minimal de $g \in A/\pi$ sur $cf(E)$ est de la forme (*) avec $r := [cf(E[g]) : cf(E)]$.

On peut de nouveau interpréter ce polynôme comme une relation de dépendance intégrale de $y_0$ sur $C$. D'où:

$$[cf(C[y_0]) : cf(C)] \leqq [cf(E[g]) : cf(E)]\, d.$$

Notons par ailleurs que $C[y_0] = E[g]$ et que le choix générique des $y_0, \ldots, y_{n-i}$ implique, par le théorème de normalisation, que $[cf(A/\pi) : cf(E)] = \deg(A/\pi)$.

En rassemblant ces résultats, on obtient:

$$\begin{aligned}[cf(A/\pi) : cf(C)] &= [cf(A/\pi) : cf(C[y_0])] \cdot [cf(C[y_0]) : cf(C)] \\ &\leqq [cf(A/\pi) : cf(E[g])] \cdot [cf(E[g]) : cf(E)]\, d \\ &\leqq \deg(A/\pi)\, d.\end{aligned}$$

En reprenant les anciennes notations, nous énonçons:

$$\text{pour tout } j,\ 1 \leqq j \leqq t,\ [cf(A/\pi_j) : cf(C)] \leqq \deg(A/\pi_j)\, d.$$

Soient $K' := cf(C)$ et $D' := A \otimes_C K'$. Montrons que $\dim_{K'} D' \leqq \deg(A)\, d$. Comme $A$ est entier sur $C$, on voit que $D'$ est une $K'$-algèbre de dimension finie. On voit que $\pi_1' = \pi_1 D', \ldots, \pi_t' = \pi_t D'$ sont les idéaux maximaux de $D'$. Soit $(0) = \mathfrak{Y}_1' \cap \cdots \cap \mathfrak{Y}_t'$ la décomposition primaire irredondante de (0), avec $\operatorname{rad}(\mathfrak{Y}_j') = \pi_j'$. Pour $1 \leqq j \leqq t$, on a:

$$D'/\pi_j' = A/\pi_j \otimes_C cf(C) = cf(A/\pi_j) \text{ d'où:}$$

$$\begin{aligned}\dim_{K'}(D'/\pi_j') &= [cf(A/\pi_j) : cf(C)] \leqq \deg(A/\pi_j)\, d, \text{ et } \operatorname{long}(D'_{\pi_j'}) \\ &= \operatorname{long}(A_{\pi_j}) \text{ donc:} \\ \dim_{K'}(D'/\mathfrak{Y}_j') &= \operatorname{long}(D'_{\pi_j'}) \dim_{K'}(D'/\pi_j') \\ &\leqq \operatorname{long}(A_{\pi_j}) \deg(A/\pi_j)\, d = \deg(A/\mathfrak{Y}_j)\, d.\end{aligned}$$

En sommant puisque $D' = \bigoplus_j D'/\mathfrak{Y}_j'$, on obtient:

$$\dim_{K'} D' \leqq \sum_{1 \leqq j \leqq t} \deg(A/\mathfrak{Y}_j)\, d = \deg(A)\, d.$$

Soient $K = k(y_1, \ldots, y_{n-i})$ et $D = A/Ag \otimes_{k[y_1, \ldots, y_{n-i}]} K$. Montrons que $\dim_K(D) \leqq \deg(A)\, d$.

On a $C/Cg \cong k[y_1, \ldots, y_{n-i}]$, on la considère comme une sous-algèbre de $A/Ag$ car les images des $y_j$ sont algèbriquement indépendantes dans $A/Ag$. On obtient ainsi un diagramme commutatif:

$$\begin{array}{ccc} A/Ag & \cong & A \otimes_C C/Cg \\ | & & | \\ k[y_1, \ldots, y_{n-i}] & \cong & C/Cg. \end{array}$$

Comme $A$ est un $C$ module de type fini, comme de plus $g$ n'est pas diviseur de zéro dans $A$, $Cg$ est un idéal premier principal, $C$ est un anneau de polynômes, alors il existe d'après le théorème des diviseurs élémentaires un $b \in C \setminus Cg$ tel que $A_b$ est un $C_b$ module libre de rang égal à $\dim_{K'} D'$.

Donc $(A/Ag)_b \cong A_b \otimes_C (C/Cg)_b$ est un $(C/Cg)_b$-module libre de même rang. D'où:

$$\dim_K D = \dim_{cf(C/Cg)} A \otimes_C cf(C/Cg) = \dim_{K'} D' \leqq \deg(A)\, d.$$

$D$ est une $K$-algèbre de dimension finie, nous pouvons donc appliquer le lemme 2. Vérifions qu'on trouve bien le résultat cherché.

Pour tout idéal $\mathfrak{Y}$ de $A$, notons $\tilde{\mathfrak{Y}}$ son extension $\mathfrak{Y}D$ dans $D$. Reprenons les décompositions:

$$Ag = B \cap \Gamma \cap \Delta \quad \text{et} \quad B \cap \Gamma = \mathfrak{Y}_1 \cap \cdots \cap \mathfrak{Y}_r,$$

dont $\Gamma = \mathfrak{J}_1 \cap \cdots \cap \mathfrak{J}_s$ et $B = \mathfrak{J}_{s+1} \cap \cdots \cap \mathfrak{J}_r$ sont les décompositions primaires de $\mathfrak{J}$ et de $B$.

Comme $\Delta$ contient une intersection de composantes immergées, donc de dimension inférieures, on obtient une décomposition primaire de $(\bar{0})$ dans $D$:

$$\bar{0} = (\overline{Ag}) = \bar{B} \cap \bar{\Gamma} = \bar{\mathfrak{J}}_1 \cap \ldots \cap \bar{\mathfrak{J}}_r;$$

$D$ étant une localisation de $A/Ag$, on voit que:

$$\lambda_j = \min \{\lambda; \operatorname{rad}(\mathfrak{J}_j)^\lambda \subseteqq \mathfrak{J}_j\} = \min \{\lambda; \operatorname{rad}(\bar{\mathfrak{J}}_j)^\lambda \subseteqq \bar{\mathfrak{J}}_j\}$$

rappelons que par le choix générique des $y_1, \ldots, y_{n-i}$ on $a$:

$$\deg\big(A/\operatorname{rad}(\mathfrak{J}_j)\big) = \big[c/\big(A/\operatorname{rad}(\mathfrak{J}_j)\big): K\big].$$

On conclue en regroupant les composantes de $B$ et en appliquant le lemme 2 aux composantes de $\Gamma$.

La *3ème étape* contient le résultat essentiel qui permet d'améliorer les bornes de [4] et [5]. Comme nous l'avons expliqué dans le schéma de la démonstration, il s'agit de montrer que les entiers $\{c_i\}$ qui vérifient la relation de récurrence $c_{i+1} \leqq 3c_i + l_{i+1}$, $c_1 = 0$, satisfont:

$$X_0^{c_i + l_{i+1}} B_{i+1} \subseteqq (B_i, G_{i+1}).$$

Autrement dit, avec les notations posées pour $i$ fixé (i.e. $c := c_i$, $A = R/B_i$ etc. ...) et le résultat de la 2ème étape qui entraine $X_0^l B \subseteqq \Gamma$, on doit montrer

$$X_0^{c+l} B \subseteqq Ag \text{ ou de façon équivalente } X_0^{c+l} B \subseteqq \Delta.$$

**Lemme 4.** *On a les implications suivantes* $(4) \Rightarrow (3) \Rightarrow (2) \Rightarrow (1) \Leftrightarrow (1')$:

(1) $X_0^{c+l} B \subseteqq \Delta$, $\quad (1')\ X_0^{c+l}(B/Ag) = 0$,

(2) $X_0^c \operatorname{Hom}_R(A/\Delta, A/Ag) = 0$,

(3) $X_0^c \operatorname{Ext}_R^j(A/\Delta, A) = 0$, *pour* $j = 0$ *à* $\dim(A) - \dim(A/\Delta) - 1$,

(4) $X_0^c \operatorname{Ext}_R^j(R/\mathfrak{J}, A) = 0$, *pour* $j = 0$ *à* $\dim(A) - \dim(R/\mathfrak{J}) - 1$,

*et pour tout les idéaux* $\mathfrak{J}$ *de* $R$ *tels que* $(G_1, \ldots, G_{i+1}) \subseteqq \mathfrak{J}$, $X_0 \in \operatorname{rad}(\mathfrak{J})$.

Preuve. (1) $\Leftrightarrow$ (1') est triviale. (4) $\Rightarrow$ (3) s'obtient en considérant l'image inverse $\mathfrak{J} := \Delta_{i+1}$ de $\Delta$ par le morphisme $\pi: R \to A = R/B_i$ et en se rappellant que $(G_1, \ldots, G_i) \subseteqq B_i$ et que $X_0 \in \operatorname{rad}(\Delta_{i+1})$.

(3) $\Rightarrow$ (2) s'obtient maintenant par un argument homologique simple: le fait que $\pi(G_{i+1}) = g \in \Delta$ et que $g$ n'est pas diviseur de zéro dans $A$ impliquent que $\dim(A/\Delta) < \dim(A)$ et que $\operatorname{Hom}_R(A/\Delta, A) = 0$. Par ailleurs, la multiplication par $g$ induit une suite exacte courte:

$$0 \to A \to A \to A/Ag \to 0.$$

On considère le fragment suivant de la suite exacte longue associée:

$$\operatorname{Hom}_R(A/\Delta, A) \to \operatorname{Hom}_R(A/\Delta, A/Ag) \to \operatorname{Ext}_R^1(A/\Delta, A).$$

Comme $\mathrm{Hom}_R(A/\Delta, A) = 0$ et $\dim(A) - \dim(A/\Delta) \geqq 2$, on voit que $\mathrm{Hom}_R(A/\Delta, A/Ag)$ est un sous-module de $\mathrm{Ext}^1_R(A/\Delta, A)$ et que $X_0^c \mathrm{Ext}^1_R(A/\Delta, A) = 0$, d'où $X_0^c \mathrm{Hom}_R(A/\Delta, A/Ag) = 0$.

(2) $\Rightarrow$ (1) s'obtient par un argument de "dualité": pour tout $b \in B$, on sait que $X_0^l b$ appartient à $B \cap \Gamma$ donc pour tout $\delta \in \Delta$, $X_0^l b\delta \in B \cap \Gamma \cap \Delta = (g)$. Ainsi la multiplication par $X_0^l b$ est un élément bien défini $\varphi_b$ de $\mathrm{Hom}_R(A/\Delta, A/Ag)$. De plus $X_0^c \varphi_b = 0$ si et seulement si $X_0^{c+l} b \in (g)$ soit si et seulement si $X_0^{c+l} b \in \Delta$, pour tout $b \in B$.

**Notation.** *Pour tout $R$-module de type fini $M$, et pour tout $i$, $1 \leqq i \leqq s$, on définit l'entier $c(i, M)$ en posant:*

$c(i, M) = \min\{c;\ X_0^c \cdot \mathrm{Ext}^j_R(R/\mathfrak{F}, M) = 0$, *pour tout les idéaux $\mathfrak{F}$ de $R$ tels que* $(G_1, \ldots, G_{i+1}) \subseteq \mathfrak{F}$, $X_0 \in \mathrm{rad}(\mathfrak{F})$, $\dim(R/\mathfrak{F}) < \dim(M)$, *et pour tout les $j$ tels que* $0 \leqq j < \dim(M) - \dim(R/\mathfrak{F})\}$.

**Remarque.** *Pour tout $M$, $c(i+1, M) \leqq c(i, M)$.*

**Lemme 5.** *Soient $0 \to M' \to M \to M'' \to 0$ une suite exacte courte de $R$-modules de type fini avec $\dim(M'') < \dim(M')$ et $i$, $1 \leqq i \leqq s$. Alors $c(i, M) < \infty$ et $c(i, M') < \infty$ impliquent $c(i, M'') \leqq c(i, M) + c(i, M') < \infty$.*

Preuve. Remarquons tout d'abord que $\dim(M) = \dim(M')$. Pour tout $\mathfrak{F}$ tel que dans la définition de $c(i, M'')$, on considère la suite exacte longue des $\mathrm{Ext}_R(R/\mathfrak{F}, -)$. Pour tout $j < \dim(M'') - \dim(R/\mathfrak{F})$, on en extrait la suite exacte suivante de $R$-modules (on note $\varphi$ et $\psi$ les morphismes):

$$\mathrm{Ext}^j_R(R/\mathfrak{F}, M) \xrightarrow{\varphi} \mathrm{Ext}^j_R(R/\mathfrak{F}, M'') \xrightarrow{\psi} \mathrm{Ext}^{j+1}_R(R/\mathfrak{F}, M').$$

Comme $X_0^{c(i,M)} \mathrm{Ext}^j_R(R/\mathfrak{F}, M) = 0$ et $X_0^{c(i,M')} \mathrm{Ext}^{j+1}_R(R/\mathfrak{F}, M') = 0$, pour tout $\alpha \in \mathrm{Ext}^j_R(R/\mathfrak{F}, M'')$ on a $X_0^{c(i,M')}\alpha \in \mathrm{Ker}(\psi) = \mathrm{Im}(\varphi)$, donc $X_0^{c(i,M)+c(i,M')}\alpha = 0$.

**Corollaire.** $c(1, R/G_1) = 0$.

Preuve. On déduit le résultat de la considération de la résolution libre de $R/G_1$: $0 \to R \to R \to R/G_1 \to 0$ et du fait que $\mathrm{Ext}^j_R(R/\mathfrak{F}, R) = 0$ pour tout $j \leqq n - \dim(R/\mathfrak{F})$ (comparer [24], p. 97, Corollary).

**Corollaire.** *Pour $1 \leqq i < s$, si $c(i, R/B_i) < \infty$, on a*

$$c\big(i+1, R/(B_i, G_{i+1})\big) \leqq 2c(i, R/B_i) < \infty.$$

Preuve. Du fait que $G_{i+1}$ n'est pas diviseur de zéro dans $R/B_i$, on déduit que $\dim\big(R/(B_i, G_{i+1})\big) < \dim(R/B_i)$ et que l'on a la suite exacte courte associée à la multiplication par $G_{i+1}$:

$$0 \to R/B_i \to R/B_i \to R/(B_i, G_{i+1}) \to 0.$$

D'où $c\big(i+1, R/(B_i, G_{i+1})\big) \leqq c\big(i, R/(B_i, G_{i+1})\big) \leqq 2c(i, R/B_i)$.

**Lemme 6.** *Pour $1 \leqq i < s$, si $c\big(i+1, R/(B_i, G_{i+1})\big) < \infty$, on a*

$$c(i+1, R/B_{i+1}) \leqq l_{i+1} + c(i, R/B_i) + c\big(i+1, R/(B_i, G_{i+1})\big).$$

Preuve. Avec les notations abrégées, il s'agit de prouver que $c(i+1, A/H) \leqq l + c(i, A) + c(i+1, A/Ag)$. D'après le lemme 4, $X_0^{l+c(i,A)}$ est dans l'annulateur du

$R$-module $B/Ag$, il est donc dans l'annulateur de $\mathrm{Ext}^j_R(R/\mathfrak{I}, B/Ag)$ pour tout $j$ et tout $\mathfrak{I}$. Considérons la suite exacte courte induite par l'inclusion de $B$ dans $Ag$:

$$0 \to B/Ag \to A/Ag \to A/B \to 0$$

et le fragment suivant de la suite exacte longue associée:

$$\mathrm{Ext}^j_R(R/\mathfrak{I}, A/Ag) \to \mathrm{Ext}^j_R(R/\mathfrak{I}, A/B) \to \mathrm{Ext}^{j+1}_R(R/\mathfrak{I}, B/Ag)$$

pour tous $\mathfrak{I}$ et $j$ comme dans la définition de $c(i+1, A/B)$. Un raisonnement identique à celui de la preuve du lemme précédent donne $c(i+1, A/B) \leqq c(i, A) + l + c(i+1, A/Ag)$.

On résume la situation dans la proposition suivante.

**Proposition 7.** *Pour* $1 \leqq i < s$ *on a:*

(1) $\quad X_0^{c_i + l_{i+1}} B_{i+1} \subseteqq (B_i, G_{i+1})$

(2) $\quad c_1 = 0$ *et* $c_{i+1} \leqq 3c_i + l_{i+1}$.

Preuve. On pose $c_i := c(i, R/B_i)$, les nombres $l_i$ pour $1 \leqq i \leqq s$ sont déterminés par la 2ème étape. D'après le premier corollaire, $c_1 = 0$. Le second corollaire et le Lemme 6 mis bout à bout donne:

$$\begin{aligned} c(i+1, R/B_{i+1}) &\leqq l_{i+1} + c(i, R/B_i) + c\big(i+1, R/(B_i, G_{i+1})\big) \\ &\leqq 3c(i, R/B_i) + l_{i+1}. \end{aligned}$$

Ceci montre inductivement que tous les $c(i, R/B_i)$ et $c\big(i+1, R/(B_i, G_{i+1})\big)$ sont finis et justifie l'utilisation de ces résultats. Le (1) est démontré par le Lemme 4.

Dans *la 4ème étape* on résoud les relations de récurrence liant $d$, $n$, la borne cherchée $m$ et les $l_i$, $c_i$, et $b_i$. On a posé $b_i := \deg(B_i)$.

Pour cela on introduit les nombres intermédiares $d_1, \ldots, d_s$ définis de la façon suivante, et qui seront les degrés de polynômes que nous allons construire:

$$d_s := 0$$

$$d_i := d_{i+1} + l_{i+1} + c_i.$$

Ils sont liés par les relations:

$$c_{i+1} \leqq 3c_i + l_{i+1} \quad \text{avec} \quad c_1 = 0,$$

$$b_{i+1} + l_{i+1} \leqq b_i d \quad \text{avec} \quad b_1 = d.$$

Pour $s = 2$, on a $d_1 = l_2 \leqq d^2$.

Pour $s > 2$, on a $d_1 = l_s + \sum_{2 \leqq i \leqq s-1} l_i + \sum_{1 \leqq i \leqq s-1} c_i$; la première inégalité de liaison donne pour $2 \leqq i \leqq s-1$:

$$3^{-i} c_i \leqq \sum_{2 \leqq j \leqq i} 3^{-j} l_j, \quad \text{d'où}$$

$$\sum_{2 \leqq i \leqq s-1} c_i \leqq \sum_{2 \leqq i \leqq s-1} \sum_{2 \leqq j \leqq i} 3^{i-j} l_j = \sum_{2 \leqq j \leqq s-1} (3^{s-j} - 1)\, l_j/2;$$

en regroupant on trouve:

$$d_1 \leqq l_s + 1/2 \sum_{2 \leqq i \leqq s-1} l_i + 1/2 \sum_{2 \leqq i \leqq s-1} 3^{s-i} l_i.$$

En sommant de $i = 1$ à $s - 2$ les instances de la deuxième inégalité de liaison:

$$\sum_{2 \leqq i \leqq s-1} l_i \leqq (d-1) \sum_{2 \leqq i \leqq s-2} b_i - b_{s-1} + d^2$$

en portant pour $i \leqq s - 2$, $b_i \leqq d^i$ et en effectuant la somme on obtient:

$$\sum_{2 \leqq i \leqq s-1} l_i \leqq d^{s-1} - b_{s-1};$$

de même en remplaçant $l_i$ par $3^{-i}l^i$, $b_i$ par $3^{-i}b_i$ et $d$ par $d/3$, et en se rappellant que par hypothèse $d \geqq 3$, on obtient:

$$\sum_{2 \leqq i \leqq s-1} 3^{s-i} l_i \leqq 3(d^{s-1} - b_{s-1});$$

en gardant $l_s \leqq b_{s-1}d$, on obtient alors:

$$\begin{aligned} d_1 &\leqq b_{s-1}d + 1/2(d^{s-1} - b_{s-1}) + 3/2(d^{s-1} - b_{s-1}) \\ &= 2d^{s-1} + (d-2)\, b_{s-1} = d^s - (d-2)\,(d^{s-1} - b_{s-1}) \leqq d^s. \end{aligned}$$

Construisons, par récurrence sur $i$, des polynômes homogènes $R_i$ qui satisfont pour $1 \leqq i \leqq s$ les conditions suivantes:

$$R_i \in B_i, \qquad \deg(R_i) = d_i,$$

$$R_i = X_0^{d_i} + \sum_{i<j \leqq s} A_j^{(i)} G_j \quad \text{pour certains polynômes } A_j^{(i)}.$$

Comme $B_s = (1)$, posons $R_s = 1$. Supposons construit $R_{i+1}$ pour $s > i \geqq 1$. Appliquons la Proposition 7 de la 3ème étape,

$$X_0^{c_i + l_{i+1}} R_{i+1} \in (B_i, G_{i+1})$$

donc il existe des polynômes homogènes $R_i$ dans $B_i$ et $A_i$ tels que:

$$X_0^{c_i + l_{i+1}} R_{i+1} = R_i + A_i G_{i+1}$$

on pose $A_{i+1}^{(i)} = -A_i$; et on remarque que:

$$\deg(R_i) = d_i = d_{i+1} + l_{i+1} + c_i.$$

Comme $B_1 = (G_1)$, il existe un polynôme homogène $A_0$ tel que:

$$R_1 = X_0^{d_1} + \sum_{1<j \leqq s} A_j^{(1)} G_j = A_0 G_1,$$

Donc

$$X_0^{d_1} \in (G_1, \ldots, G_s).$$

La *5ème étape* consiste à améliorer, lorsque $s = n + 1$, la majoration de $d_1$ trouvée dans la 4ème étape. On avait établi que:

$$d_1 \leqq d_n + l_n + 2(d^{n-1} - b_{n-1}).$$

Dans ce cas $\{B_{n-1} = 0\}$ est formé de courbes de $k^n$, son prolongement à l'infini n'a donc que des points, qui ne peuvent intersecter $\{G_n = 0\}$ qu'en des points. Reprenons les notations: $(B_{n-1}, G_n) = B_n \cap \Gamma_n \cap \Delta_n$, $\{B_n = 0\}$ est aussi formé de points, $\{\Delta_n = 0\}$ est vide.

On a aussi $(B_n, G_{n+1}) = \Gamma_{n+1} \cap \Delta_{n+1}$.

En reprenant complétement l'étude géométrique et en la précisant, on conçoit bien que l'on peut remplacer le terme $(d_n + l_n)$ par une borne fine après avoir redéfini la valeur de $d_n$.

Nous nous contenterons ici de démontrer que $d_n$ peut être remplacé par $b_n + d - 1$ dans les inégalités précédentes, ce qui donnera:

$$\begin{aligned} d_1 &\leqq d_n + l_n + 2(d^{n-1} - b_{n-1}) \\ &\leqq b_n + l_n + 2(d^{n-1} - b_{n-1}) + d - 1 \\ &\leqq b_{n-1}d + 2(d^{n-1} - b_{n-1}) + d - 1 \\ &= d^n - (d-2)(d^{n-1} - b_{n-1}) + d - 1. \end{aligned}$$

Comme $d \geqq 3$, si $d^{n-1} - b_{n-1} \geqq 2$ on obtient $d_1 \leqq d^n - d + 3 \leqq d^n$.

Si $d^{n-1} - b_{n-1} = 1$, les inégalités de liaisons impliquent

$$l_1 = \cdots = l_{n-2} = 0, \qquad l_{n-1} = 1 \quad \text{et} \quad c_1 = \cdots = c_{n-2} = 0,$$

d'où $B_{n-2} = (G_1, \ldots, G_{n-2})$. Comme $G_{n-1}$ n'est pas diviseur de zéro dans $B_{n-2}$ cela implique que $G_1, \ldots, G_{n-1}$ est une suite régulière dans $R$.

On a donc $c_{n-1} = 0$, d'où $d_1 = d_n + l_n + l_{n-1} = d_n + l_n + 1$. Maintenant on voit que:

$$d_1 = d_n + l_n + 1 \leqq b_n + l_n + d \leqq b_{n-1}d + d = d^n.$$

Enfin, si $d^{n-1} - b_{n-1} = 0$, comme auparavant on obtient:

$$l_1 = \cdots = l_{n-1} = 0 \quad \text{et} \quad c_1 = \cdots = c_n = 0,$$

c'est à dire que $G_1, \ldots, G_n$ est une suite régulière dans $R$ définissant une sous-variété projective de dimension zéro.

Par conséquent $G_1, \ldots, G_{n+1}$ n'ont que des points communs à l'infini; par un raffinement de l'argument que nous détaillerons à la fin de notre démonstration (voir aussi [2], [22] et [19] on obtient

$$X_0^{\max\{d^n, (n+1)d\}} \in (G_1, \ldots, G_{n+1}).$$

On conclue en utilisant l'hypothèse $n > 1$ et $d \geqq 3$ qui implique

$$(n+1)\, d \leqq d^n.$$

Reste donc à montrer que $d_n$ peut être remplacé par $b_n + d - 1$. En tenant compte de la construction des polynômes homogènes $R_{n+1}, \ldots, R_1$ de la $4^{\text{ème}}$ étape, il suffit de démontrer que $X_0^{b_n+d-1} \in (B_n, G_{n+1})$.

Pour cela, on considère l'idéal $\mathfrak{F} = (F_1, \ldots, F_n)$ de $k[X_1, \ldots, X_n]$, il correspond à une intersection complète affine formée par des points dont la somme des degrés est égale à $b_n$. On a donc $\dim_k k[X_1, \ldots, X_n]/(F_1, \ldots, F_n) = b_n$.

Soit $H_1, \ldots, H_t$ une base standard réduite de $\mathfrak{F}$ relativement au degré total raffiné, par exemple, par l'ordre lexicographique inverse. Notons $\overline{H}_i$ les homogénéisés des $H_i$, $1 \leqq i \leqq t$ et $\overline{\mathfrak{F}}$ l'idéal de $R = k[X_0, \ldots, X_n]$ qu'ils engendrent. Alors $(\overline{H}_1, \ldots, \overline{H}_t)$ est une base standard réduite de $\overline{\mathfrak{F}}$ relativement à l'ordre lexicographique inverse: en

effet s'il y avait un élément $\overline{H}$ de $\overline{\mathfrak{I}}$ dont le terme dominant ne serait pas multiple du terme dominant de l'un des $H_i$ (qui d'après nos choix, ne contient pas de $X_0$) il en serait de même en faisant $X_0 = 1$.

On en déduit que $(\overline{\mathfrak{I}} : X_0) = \overline{\mathfrak{I}}$, autrement dit $\overline{\mathfrak{I}}$ n'a pas de composante à l'infini, donc $\overline{\mathfrak{I}}$ est égal à notre ancien $B_n$.

De plus, puisque l'idéal des termes dominant $lt(B_n)$ est engendré par des monômes qui ne dépendent pas de $X_0$, on peut borner par $b_n - 1$ ($b_n$ est le nombre de points "sous l'escalier") la régularité de la fonction de HILBERT de $M = R/B_n$ ceci signifie que, en notant $M = \bigoplus_{0 \leq i \leq \infty} M_i$ la graduation de $M$, on a $\dim_k (M_i) = \dim_k (M_j)$ pour tout $i$ et $j \geqq b_n - 1$.

Considérons enfin $G_{n+1}$ qui induit dans $M$ un élément $g$ non diviseur de zéro et de degré $d$. Notons $\varphi$ la multiplication par $g$ dans $M$, c'est un morphisme injectif et gradué de degré $d$; $\varphi$ définit donc une application $k$-linéaire bijective en degrés $a \geqq b_n - 1$

$$\varphi : M_a \to M_{a+d}.$$

Le $R$-module gradué $N := R/(B_n, G_{n+1})$ est le conoyau de $\varphi$, on déduit de ce qui précède que $N$ est nul en degré $a \geqq b_n + d - 1$, c'est à dire

$$(X_0, \ldots, X_n)^a = (B_n, G_{n+1}).$$

Donc,

$$X_0^{b_n+d-1} \in (B_n, G_{n+1}). \qquad \text{cqfd.}$$

Le lecteur pourra remarquer que dans la démonstration du théorème 1 on a seulement utilisé le fait que $G_1, \ldots, G_s$ forment une suite régulière à distance finie, c'est à dire hors de l'hypersurface $\{X_0 = 0\}$. En particulier, le fait que $X_0$ est de degré 1 n'intervient pas. Dans notre démonstration on peut donc remplacer $X_0$ par un polynôme homogène $G$ et obtenir la version projective suivante du (HENTZELT) Nullstellensatz effectif:

**Théorème 10.** *Soit $k$ un corps quelconque et soient $G, G_1, \ldots, G_s$ des polynômes homogènes de $k[X_0, \ldots, X_n]$ tels que $d := \max_{1 \leq i \leq s} \deg (G_i)$. Posons*

$$\psi(d, n) := \begin{cases} d^n & \text{pour } n > 1 \text{ et } d \geqq 3, \\ 3^n & \text{pour } n > 1 \text{ et } d = 2, \\ 2d - 1 & \text{pour } n = 1. \end{cases}$$

*Si $G \in \operatorname{rad} (G_1, \ldots, G_s)$ alors*

$$G^{\psi(d,n)} \in (G_1, \ldots, G_n).$$

Pour une démonstration détaillée du théorème 10 voir [6].

## § 3. Remarques sur l'inconsistence stable

Dans ce paragraphe on supposera $k$ algébriquement clos.

**Définitions.** Par analogie avec le vocabulaire utilisé en logique, on dira qu'une famille de polynômes $F_1, \ldots, F_s$ de $k[X_1, \ldots, X_n]$ est inconsistance si $1 \in (F_1, \ldots, F_s)$. On dira

qu'elle est *stablement inconsistente* s'il existe un ouvert de ZARISKI $U$ de $k^s$, tel que $0 \in U$ et pour tout $\lambda = (\lambda_1, \ldots, \lambda_s) \in U$ on ait $1 \in (F_1 - \lambda_1, \ldots, F_s - \lambda_s)$.

On appelle *syzygie finale* (voir [28]) de $F_1, \ldots, F_s$ un polynôme $P$ de $k[Y_1, \ldots, Y_s]$, où les $Y_i$ sont de variables auxiliaires, tel que:

$$P(0, \ldots, 0) = 1 \quad \text{et} \quad P\big(F_1(X_1, \ldots, X_n), \ldots, F_s(X_1, \ldots, X_n)\big) = 0.$$

**Lemme 11** ([28], 6.4). *Il existe une syzygie finale pour la famille de polynômes $F_1, \ldots, F_s$ ssi elle est stablement inconsistente.*

Nous allons à présent retourner à la situation du théorème 1, c'est à dire $1 \in (F_1, \ldots, F_s)$ avec les hypothèses supplémentaires suivantes:

$$\deg(F_1) = \cdots = \deg(F_s) = d,$$

$$\operatorname{trdeg}_k k[\overline{F}_1, \ldots, \overline{F}_s] = n + 1, \text{ où } \overline{F}_i \text{ est l'homogénéisé de } F_i \text{ pour } 1 \leqq i \leqq s.$$

Soient $G_1, \ldots, G_{n+1}$ des combinaisons linéaires de $\overline{F}_1, \ldots, \overline{F}_s$ qui forment une suite régulière à distance finie et telles que $k[G_1, \ldots, G_{n+1}] \subseteqq k[\overline{F}_1, \ldots, \overline{F}_s]$ soit une extension entière. On a $X_0 \in \operatorname{rad}(G_1, \ldots, G_{n+1})$ et d'après l'inégalité de BÉZOUT ([4], Proposition 5) on a $[k(X_0, \ldots, X_n) : k(G_1, \ldots, G_{n+1})] \leqq d^{n+1}$.

**Proposition 12.** Avec les notations et hypothèses précédentes: $X_0$ *est entier sur* $k[G_1, \ldots, G_{n+1}]$ *ssi la famille* $F_1, \ldots, F_s$ *est stablement inconsistente.*

Preuve. Supposons que $X_0$ est entier sur $k[G_1, \ldots, G_{n+1}]$.

Comme $k[G_1, \ldots, G_{n+1}]$ est intégralement clos, le polynôme minimal de $X_0$ sur $k(G_1, \ldots, G_{n+1})$ est une relation de dépendance intégrale de degré égal à:

$$[k(G_1, \ldots, G_{n+1}, X_0) : k(G_1, \ldots, G_{n+1})] \leqq [k(X_0, \ldots, X_n) : k(G_1, \ldots, G_{n+1})] \leqq d^{n+1}.$$

Ceci signifie qu'il existe un entier $r$, $1 \leqq r \leqq d^{n+1}$ et $r$ polynômes homogènes $A_0, \ldots, A_{r-1}$ dans $k[G_1, \ldots, G_{n+1}]$ tels que:

$$X_0^r + A_{r-1}X_0^{r-1} + \cdots + A_0 = 0.$$

et $\deg(A_i) = r - i$ ou $A_i = 0$ pour $0 \leqq i \leqq r - 1$

Remarquons que $A_i$ est à priori un élément de $k[G_1, \ldots, G_{n+1}]$ tout en étant un polynôme homogène en $X_0, \ldots, X_n$; mais comme les $G_1, \ldots, G_{n+1}$ sont homogènes de degré $d$ et algébriquement indépendants sur $k$, on déduit que $A_i$ est aussi homogène de degré $\leqq d^{n+1}$ dans $k[G_1, \ldots, G_{n+1}]$. En particulier $A_i \in (\overline{F}_1, \ldots, \overline{F}_s)$.

Spécialisons $X_0$ en $1 \in k$. Les $\overline{F}_j$ se spécialisent en $F_j$, les $A_i$ en certains $A_i'$ de $k[X_1, \ldots, X_n]$ qui ont une représentation (non nécessairement unique) comme polynômes en $F_1, \ldots, F_s$ "sans terme constant" et de degré $\leqq d^{n+1}$:

$$1 + A_{r-1}' + \cdots + A_0' = 0.$$

Autrement dit, on obtient une syzygie finale de degré $\leqq d^{n+1}$ de la famille $F_1, \ldots, F_s$.

Réciproquement s'il existe une syzygie finale $P$ pour la famille $F_1, \ldots, F_s$ en homogénéisant la relation correspondante, on voit facilement que $X_0$ est entier sur $k[\overline{F}_1, \ldots, \overline{F}_s]$.

Comme $k[G_1, \ldots, G_{n+1}] \subseteq k[\overline{F}_1, \ldots, \overline{F}_s]$ est une extension entière, on en déduit que $X_0$ est entier sur $k[G_1, \ldots, G_{n+1}]$.

**Remarque.** La proposition précédente pose donc la question de déterminer si $X_0$ est entier sur $k[G_1, \ldots, G_{n+1}]$. Nous n'avons qu'une réponse partielle qui découle de ([4], Remark 9):

$k[G_1, \ldots, G_{n+1}] \subseteq k[X_0, \ldots, X_n]$ *est une extension entière ssi* $\{\overline{F}_1 = 0, \ldots, \overline{F}_s = 0\} = \emptyset$.

Donc si $F_1, \ldots, F_s$ n'ont pas de zéros communs même à l'infini, on peut conclure que cette famille est stablement inconsistante. (Voir aussi [21], [22], [2].)

**Remarque.** Dans le cas général, il est clair que l'on doit multiplier $F_1, \ldots, F_s$ par des monômes en $X_1, \ldots, X_n$ pour obtenir une syzygie finale. Si on savait borner le degré de ces monômes, on obtiendrait une démonstration vraiment élémentaire d'un Nullstellensatz effectif basée uniquement sur l'inégalité de BÉZOUT.

## § 4. L'ex-Conjecture de Serre: point de vue quantitatif et effectif

Nous allons appliquer notre Nullstellensatz effectif, Théorème 1, dans le contexte de l'ex-Conjecture de SERRE.

Cette conjecture a été résolue en plusieures étapes. Nous nous occupons seulement de la dernière où on démontre que les anneaux polynomiaux sur un corps hermitiens. Les premières démonstrations de ce fait ont été données par Suslin et Quillen indépendemment. Notre point de départ sera la démonstration de Suslin (voir [20]).

Dans ce paragraphe nous supposons que $k$ est *infini*. (Ce sera l'unique hypothèse sur $k$. En particulier la caractéristique de $k$ peut être arbitraire.)

Notons

$$R := k[X_1, \ldots, X_n].$$

Soit $F = (F_{ij})_{1 \leq i \leq r, 1 \leq j \leq s} \in R^{r \times s}$ une $r \times s$-matrice polynomiale avec $F_{ij} \in R$ pour $1 \leq i \leq r$, $1 \leq j \leq s$. Notons

$$\deg F := \max_{1 \leq i \leq r, 1 \leq j \leq s} \deg F_{ij} \text{ le degré de } F.$$

Si les $r \times r$-mineurs de $F$ engendrent l'idéal trivial $R$ nous dirons que $F$ est unimodulaire. Considérons les deux cas particuliers $r = 1$ et $r = s$.

Si $r = 1$ et $F = (F_1, \ldots, F_s)$, la condition $F$ unimodulaire signifie $RF_1 + \cdots + RF_s = R$.

Si $r = s$ la condition $F$ unimodulaire signifie $\det F \in k \setminus \{0\}$ ($\det F$ est le déterminant de $F$).

$F$ unimodulaire signifie que l'application $R$-linéaire induite par $F$

$$R^s \xrightarrow{F} R^r$$

est surjective.

Le Nullstellensatz effectif (Théorème 1) entraîne

**Théorème 13** ([9], [4]). *Soit $k$ un corps infini, $R := k[X_1, \ldots, X_n]$ et $F \in R^{r \times s}$ une matrice unimodulaire avec $d := \deg F$. Alors il existe une matrice unimodulaire $M \in R^{s \times s}$ avec les propriétés suivantes:*

(i) $F \cdot M = \begin{pmatrix} 1 & & 0 & \\ & \ddots & & 0 \\ 0 & & 1 & \end{pmatrix}$ ($r$ lignes, $s$ colonnes)

(ii) $\deg M = (rd)^{O(n)}$

(iii) *$M$ a une représentation $M = N_1 \cdot \ldots \cdot N_p$ comme produit de $p \leqq ns(rd)^{2n}$ matrices $N_h \in R^{s \times s}$ telles que pour $1 \leqq h \leqq p$:*

$\deg N_h = (rd)^{O(n)}$

*$N_h$ est élémentaire ou de la forme*

$$N_h = r + 1 \begin{pmatrix} & r+1 \\ N_h' & \\ & \end{pmatrix} s \quad \text{avec } N_h' \in SL_{r+1}(R).$$

(iv) *On peut calculer $M$ par un réseau arithmétique (voir [8]) en temps séquentiel $r^{O(n^2)} s^{O(r^2)} d^{O(n^2+r^2)}$ et en temps parallèle $O(n^4 r^4 \log^2 (srd))$.*

Le fait que $R$ est hermitien signifie, dans les hypothèses du Théorème 13, qu'il existe une matrice unimodulaire $M \in R^{s \times s}$ qui satisfait (i).

Les bornes du Théorème 13 (ii) et (iii) représentent le (nouvel) aspect quantitatif et les complexités dans (iv) l'aspect algorithmique du résultat qui est par ailleurs classique. Ce résultat dont les démonstrations classiques ne sont pas constructives implique la résolution de l'ex-Conjecture de SERRE (voir [20]).

On peut se limiter au cas $r \leqq \min\{n, s\}$. De ce point de vue Théorème 13 (iv) représente une solution algorithmique de l'ex-Conjecture de SERRE simplement exponentielle en temps séquentiel et (simultanément) polynomiale en temps parallèle.

Les propriétés Théorème 13 (i) et (ii) impliquent un Nullstellensatz effectif (poser $r = 1$ et considérer la première ligne de $M$).

On déduit de l'exemple cité de MASSER-PHILIPPON ([3]) que toute borne pour $\deg M$ est *intrinsequement* exponentielle en $n$.

**Corollaire 14.** *Soient $R$ et $F$ comme dans le Théorème 13. Considérons la suite exacte courte de $R$-modules induite par $F$:*

$$0 \to P \to R^s \xrightarrow{F} R^r \to 0,$$

*où $P$ est un sous-module de $R^s$.*

*Alors $P$ est un $R$-module libre de rang $s - r$ et on peut trouver en temps séquentiel $r^{O(n^2)} s^{O(r^2)} d^{O(n^2+r^2)}$ et en temps parallèle $O(n^4 r^4 \log^2 (srd))$ une base de $P$ décrite par une matrice $N \in R^{(s-r) \times s}$ de degré $\deg N = (rd)^{O(n)}$.*

Démonstration. Soit $R$, $F$ et $M$ comme dans la Théorème 13. Considérons le diagramme commutatif

$$\begin{array}{ccccccc} 0 \to P & \to R^s & \xrightarrow{\quad F \quad} & R^r \to 0 \\ \| & \uparrow & \| & \uparrow & \overbrace{\begin{pmatrix} 1 & 0 & \\ & \ddots & 0 \\ 0 & & 1 \end{pmatrix}}^{s} \Big\} r \\ 0 \to R^{s-r} & \to R^s & \xrightarrow{\quad} & R^r \end{array}$$

On en déduit que les $s - r$ dernières colonnes de $M$ forment une base de $P$.

Pour la démonstration du Théorème 13 nous référons le lecteur à [9].

Nous allons ici considérer le cas $r = 1$. Voici une version quantitative et effective du Théorème de SUSLIN ([20]):

**Théorème 15** ([4]). *Soit $k$ infini et $R := k[X_1, \ldots, X_n]$. Soit $F = (F_1, \ldots, F_s) \in R^s$ un vecteur unimodulaire. Alors il existe une matrice unimodulaire $M \in R^{s \times s}$ avec les propriétés suivantes*

(i) $F \cdot M = (1, 0, \ldots, 0)$

(ii) $\deg M = d^{O(n)}$

(iii) *$M$ a une représentation $M = N_1 \cdot \cdots \cdot N_p$ comme produit de $p \leqq 2ns^2d$ matrices $N_h \in R^{s \times s}$ telles que pour tout $1 \leqq h \leqq p$:*

$\deg N_h = d^{O(n)}$

*$N_h$ est élémentaire ou de la forme*

$$N_h = \begin{bmatrix} N_h' & \vdots & 0 \\ \cdots & \vdots & \cdots \\ 0 & \vdots & 1 \\ & \vdots & \ddots \\ & \vdots & & 1 \end{bmatrix} \quad \text{avec } N_h' \in SL_2(R).$$

(iv) *On peut calculer $M$ en temps séquentiel $s^4d^{O(n^3)}$ et en temps parallèle $O(n^4 \log^2 sd)$.*

Pour le démonstration du Théorème 15 nous avons besoin de quelques préparations.

Soit $A := k[X_1, \ldots, X_{n-1}]$ et $X := X_n$. Nous considérons les $G \in R = A[X]$ comme polynômes en $X$ à coéfficients dans $A$. Dans ce sens on peut substituer des éléments $B \in R$ dans $G$. Nous écrivons $G(B)$ le résultat de la substitution. Evidemment $G(B) \in R$ en général, et $G(B) \in A$ si $B \in A$.

Pour un vecteur $F = (F_1, \ldots, F_s) \in R^s$ et $B \in R$ nous écrivons $F(B) = \big(F_1(B), \ldots, F_s(B)\big) \in R^s$.

Pour ce qui suit, soient $s \geqq 2$, $F = (F_1, \ldots, F_s) \in R^s$ un vecteur unimodulaire et $d := \deg F$.

**Lemme 16.** *Soit $c := \mathrm{Res}_X(F_1, F_2)$ le résultant de $F_1$ et $F_2$ comme polynômes en $X$. Etant donnés $B, B' \in R$ avec $D := \max\{\deg B, \deg B'\}$ et $B - B' \in Rc$.*

*Alors il existe une matrice unimodulaire* $N \in R^{s\times s}$ *avec*

(i) $F(B) = F(B')$

(ii) $\deg N \leqq D(d + d^2)$

(iii) $N$ *a une représentation* $N = E_1 \cdot \cdots \cdot E_{2(s-2)}S$, *où* $E_1, \ldots, E_{2(s-2)} \in R^{s\times s}$ *sont des matrices élémentaires et* $S \in R^{s\times s}$ *est de la forme*

$$S = \left[\begin{array}{c|ccc} S' & 0 & & \\ \hline & 1 & & \\ 0 & & \ddots & \\ & & & 1 \end{array}\right] \quad \text{où } S' \in SL_2(R).$$

Démonstration. Partant de la matrice de Sylvester correspondante à $F_1$ et $F_2$ on peut calculer deux polynômes $G_1, G_2 \in R$ tels que

$$(*) \qquad c = G_1F_1 + G_2F_2 \quad \text{et} \quad \deg G_1, \deg G_2 \leqq d^2.$$

On a aussi $\deg c \leqq d^2$. Comme $c \in A$ ne contient pas l'indéterminée $X$, on obtient de (*)

$$c = G_1(B)\, F_1(B) + G_2(B)\, F_2(B).$$

Soit $3 \leqq j \leqq s$. On a $F_j(B) - F_j(B') \in R(B - B') \subset Rc$, donc pour $A_j := (1/c)\big(F_j(B) - F_j(B')\big)$ on a $A_j \in R$, $\deg A_j \leqq Dd$ et $F_j(B) - F_j(B') = A_jc = A_jG_1(B)\, F_1(B) + A_jG_2(B)\, F_2(B)$.

A $A_jG_1(B)$ et $A_jG_2(B)$ correspondent deux $s \times s$-matrices élémentaires à coéfficients dans $R$ qui transforment

$$\big(F_1(B), F_2(B), \ldots, F_j(B), \ldots, F_s(B)\big) \text{ en } \big(F_1(B), F_2(B), \ldots, F_j(B'), \ldots, F_s(B)\big).$$

Avec $2(s-2)$ matrices élémentaires $E_1, \ldots, E_{2(s-2)} \in R^{s\times s}$ on obtient $F(B)\, E_1 \cdot \cdots \cdot E_{2(s-2)} = \big(F_1(B), F_2(B), F_3(B'), \ldots, F_s(B')\big)$.

Considérons maintenant la matrice

$$S := \left[\begin{array}{c|ccc} S' & & & \\ \hline & 1 & & \\ & & \ddots & \\ & & & 1 \end{array}\right] \quad \text{avec } S' := \frac{1}{c}\begin{bmatrix} G_1(B) & -F_2(B) \\ G_2(B) & F_1(B) \end{bmatrix}\begin{bmatrix} F_1(B') & F_2(B') \\ -G_2(B') & G_1(B') \end{bmatrix}.$$

On a $\det S' = 1$. A première vue $S'$ est une matrice à coéfficients dans $cf(R) = k(X_1, \ldots, X_n)$.

D'autre part $B - B' \in Rc$ implique que tous les coéfficients du produit

$$\begin{bmatrix} G_1(B) & -F_2(B) \\ G_2(B) & F_1(B) \end{bmatrix}\begin{bmatrix} F_1(B') & F_2(B') \\ -G_2(B') & G_1(B') \end{bmatrix}$$

sont divisibles par $c$.

Donc $S' \in R^{2\times 2}$. Cela implique $S' \in SL_2(R)$.

On vérifie que $\big(F_1(B), F_2(B)\big)\, S' = \big(F_1(B'), F_2(B')\big)$ et $\big(F_1(B), F_2(B), F_3(B'), \ldots, F_s(B')\big)\, S = F(B')$.

Pour $N := E_1 \cdot \cdots \cdot E_{2(s-2)}S$ on a finalement $F(B)\,N = F(B')$, d'où (i) et (iii).

On a $\deg S' \leqq D(d + d^2)$ et, pour $3 \leqq j \leqq s$ et $1 \leqq v \leqq 2$, $\deg A_j G_v(B) \leqq \deg A_j + \deg G_v(B) \leqq D(d + d^2)$. Cela implique (iii).

La matrice $N \in R^{s \times s}$ de la démonstration du Lemme 16 est calculable en temps séquentiel $(Dd)^{O(n)}$ et en temps parallèle $O(n^2 \log^2 Dd)$.

**Lemme 17.** *Supposons* $\deg_X F = \deg F_1$. *Soit* $l := (s-2)\,d + 1$ *et soient donnés* $a_1, \ldots, a_l \in k$ *tous distincts.*

*Pour* $1 \leqq i \leqq l$ *notons* $F_{2,i} := F_2 + a_i F_3 + a_i^2 F_4 + \cdots + a_i^{s-2} F_s$ *et*

$$c_i := \operatorname{Res}_X (F_1, F_{2,i}).$$

*Alors, on a* $Ac_1 + \cdots + Ac_l = A$.

Démonstration. Il suffit démontrer que $c_1, \ldots, c_l$ n'ont pas de zéro commun dans $\bar{k}^{n-1}$. (On se rappelle que $\bar{k}$ était la clôture algébrique de $k$.)

Supposons le contraire et soit $z \in \bar{k}^{n-1}$ tel que $c_1(z) = \cdots = c_l(z) = 0$.

Comme $\deg_X F_1 = \deg F_1$, cette condition implique qu'il existe des $\xi_1, \ldots, \xi_l \in \bar{k}$ tels que pour $1 \leqq i \leqq l$, $F_1(z, \xi_i) = F_{2,i}(z, \xi_i) = 0$. La relation $\deg_X F_1 = \deg F_1 \leqq d$ implique que le polynôme $F_1(z, X) \in \bar{k}[X]$ a au plus $d$ zéros. Donc $\# \{\xi_1, \ldots, \xi_l\} \leqq d$ ($\#$ désigne le cardinal).

Soit $L := \{1, \ldots, l\}$. Considérons la partition $\mathcal{P}$ de $L$ qui correspond à la relation d'équivalence sur $L$ qui identifie $k_1, k_2 \in L$ si

$$\{i \in L;\, F_{2,i}(z, \xi_{k_1}) = 0\} = \{i \in L;\, F_{2,i}(z, \xi_{k_2}) = 0\}.$$

On voit que $\mathcal{P}$ a au plus $d$ classes. Comme $l = (s-2)\,d + 1$ il existe d'après le principe des tiroirs une classe dans $\mathcal{P}$ qui contient au moins $s - 1$ éléments de $L$. Cela signifie qu'il existe un $\xi \in \{\xi_1, \ldots, \xi_l\}$ qui annule $s - 1$ des polynômes $F_{2,i}(z, X) \in \bar{k}[X]$. Sans restriction de généralité on peut supposer $F_{2,1}(z, \xi) = \cdots = F_{2,s-1}(z, \xi) = 0$. De plus, on a $F_1(z, \xi) = 0$. Considérons $x := (z, \xi) \in \bar{k}^n$. $x$ est contenu dans $\{F_1 = 0, F_{2,1} = 0, \ldots, F_{2,s-1} = 0\}$ qui est donc un ensemble non-vide.

Or, on obtient le vecteur $(F_{2,1}, \ldots, F_{2,s-1}) \in R^{s-1}$ en multipliant le vecteur $(F_2, \ldots, F_s) \in R^{s-1}$ par la matrice de VANDERMONDE inversible:

$$\begin{bmatrix} 1 & \ldots & 1 \\ a_1 & \ldots & a_{s-1} \\ \vdots & & \vdots \\ a_1^{s-2} & \ldots & a_{s-1}^{s-2} \end{bmatrix}.$$

Cela implique $\emptyset \neq \{F_1 = 0, F_{2,1} = 0, \ldots, F_{2,s-1} = 0\} = \{F_1 = 0, F_2 = 0, \ldots, F_s = 0\}$. On obtient donc une contradiction avec l'hypothèse que $F = (F_1, \ldots, F_s)$ est unimodulaire.

**Remarque 18.** Puisque $\deg c_1, \ldots, \deg c_l \leqq d^2$ notre Nullstellensatz Théorème 1 et le Lemme 17 impliquent qu'il existe des $q_1, \ldots, q_l \in A$ avec $\deg q_i \leqq \max\{d^{2(n-1)}, 3^{2(n-1)}, 2d - 1\}$ pour $1 \leqq i \leqq l$, tels que $1 = \sum_{1 \leqq i \leqq l} q_i c_i$.

On peut calculer $q_1, \ldots, q_l$ en temps séquentiel $l^4 d^{O(n^2)}$ et en temps parallèle $O(n^4 \log^2 ld)$.

**Fin de la démonstration du Théorème 15**

Comme $k$ est infini nous pouvons supposer qu'après un eventuel changement linéaire des variables $X_1, \ldots, X_n$ la condition $\deg_{X_j} F_1 = \deg F$ est satisfaite pour tout $1 \leqq j \leqq n$.

Dans une première étape nous construisons une matrice unimodulaire $M_n \in R^{s \times s}$ telle que $F' M_n = F(0)$, $\deg M_n = d^{O(n)}$ et $M_n$ a une représentation $M_n = N_1 \cdot \cdots \cdot N_p$ comme produit de $p \leqq 2ds^2$ matrices $N_h \in R^{s \times s}$, $1 \leqq h \leqq p$, $N_h$ étant une matrice élémentaire ou de la forme

$$N_h = \left[\begin{array}{c|c} N_h' & 0 \\ \hline 0 & \begin{array}{ccc} 1 & & \\ & \ddots & \\ & & 1 \end{array} \end{array}\right] \quad \text{avec } N_h' \in SL_2(R).$$

En plus on a $\deg N_h = d^{O(n)}$.

On peut calculer $M_n$ en temps séquentiel $s^4 d^{O(n^2)}$ et en temps parallèle $O\big(n^4 \log^2 (sd)\big)$.

On a $\deg_{X_j} F_1(0) = \deg F_1(0) = \deg F_1$ pour $1 \leqq j \leqq n-1$ et $\deg F(0) \leqq d$.

$F$ unimodulaire implique $F(0)$ unimodulaire. Comme auparavant on trouve maintenant une $s \times s$-matrice unimodulaire $M_{n-1}$ qui transforme $F(0)$ en $F(0, 0) := \big(F_1(X_1, \ldots, X_{n-2}, 0, 0), \ldots, F_s(X_1, \ldots, X_{n-2}, 0, 0)\big)$. Donc $F M_n M_{n-1} = F(0, 0)$.

Continuant ainsi on arrive finalement à une matrice unimodulaire $M' \in R^{s \times s}$ qui transforme $F$ en $F(0, \ldots, 0) := \big(F_1(0, \ldots, 0), \ldots, F_s(0, \ldots, 0)\big) \in k^s$.

Comme $F(0, \ldots, 0)$ est unimodulaire, c'est-à-dire $F(0, \ldots, 0) \neq (0, \ldots, 0)$ on peut mettre $F(0, \ldots, 0)$ sous forme $(1, 0, \ldots, 0)$ par une transformation unimodulaire. En composant cette dernière transformation avec $M'$ on obtient une matrice unimodulaire $M \in R^{s \times s}$ qui satisfait les exigences du Théorème 15 (i).

Construisons maintenant $M_n$.

Choisissons des éléments distincts $a_1, \ldots, a_l \in k$ ($k$ est infini). Soient $c_1, \ldots, c_l \in A$ comme dans Lemme 17.

Choisissons maintenant $q_1, \ldots, q_l \in A$ d'après la Remarque 18.

Soient $P_1 := Xq_1, \ldots, P_l := Xq_l$. On a $X = \sum_{1 \leqq i \leqq l} P_i c_i$.

Pour chaque $1 \leqq i \leqq l$ appliquons le Lemme 16 avec $c := c_i$, $B := \sum_{1 \leqq h \leqq i} P_h c_h$, $B' := \sum_{1 \leqq h' \leqq i-1} P_{h'} c_{h'}$ pour transformer

$$\big(F_1(B), F_{2,i}(B), F_3(B), \ldots, F_s(B)\big) \text{ en } \big(F_1(B'), F_{2,i}(B'), F_3(B'), \ldots, F_s(B')\big).$$

Maintenant on transforme par des $s \times s$-matrices unimodulaires $F(B)$ en $\big(F_1(B), F_{2,i}(B), F_3(B), \ldots, F_s(B)\big)$, puis en $\big(F_1(B'), F_{2,i}(B'), F_3(B'), \ldots, F_s(B')\big)$ puis en $F(B')$.

Grâce au Lemme 16 on obtient une chaine de $s \times s$-matrices unimodulaires qui transforment

$$F \text{ en } F\Big(\sum_{1 \leqq h \leqq l-1} P_h c_h\Big), \text{ puis en } F\Big(\sum_{1 \leqq h' \leqq l-2} P_{h'} c_{h'}\Big), \ldots$$

... et finalement $F(P_1 c_1)$ en $F(0)$.

Les propriétés (ii) et (iii) du Théorème 15 se déduisent maintenant par application itérée des bornes des Lemme 16 et Remarque 18. Similairement on verifie la propriété (iv).

Observons que notre preuve du Théorème 15 constitue une démonstration nouvelle, élémentaire et *constructive* du Théorème de SUSLIN.

(Le Théorème de SUSLIN [20] correspond à notre Théorème 15(i).)

Une autre démonstration constructive du Théorème de SUSLIN est donnée dans [27].

Remarquons que les propriétés (ii) et (iv) du Théorème 13 ne s'obtiennent pas par simple itération du Théorème 15 (la croissance des degrés et par conséquent la croissance des complexités seraient trop grandes).

## Références


[1] C. A. BERENSTEIN, A. YGER, Effective Bezout Identities in $\mathbb{Q}[z_1, \ldots, z_n]$. Preprint University of Maryland 1987

[2] J. BRIANÇON, Sur le degré des relations entre polynômes. C. R. Acad. Sci. Paris t. 297 (1983) 553–556

[3] W. D. BROWNAWELL, Bounds for the degrees in the Nullstellensatz. Ann. math. Second Series, Vol. 126, No. 3 (1987) 287–290

[4] L. CANIGLIA, A. GALLIGO, J. HEINTZ, Some new effectivity bounds in computational geometry. — Best paper award AAECC-6. Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proc. 6th Intern. Conf. Rome 1988 (ed. T. Mora), Springer LN Comput. Sci. 357, 131–151

[5] —/—/—, Bornes simple exponentielle pour les degrés dans le théorème des zéros sur un corps de caractéristique quelconque. C. R. Acad. Sci. Paris, t. 307, Série I (1988) 255–258

[6] L. CANIGLIA, Complejidad de algorítmos en geometría computacional. Thèse Université de Buenos Aires (1989)

[7] A. DICKENSTEIN, C. SESSA, An effective residual criterion for the membership problem in $\mathbb{C}[z_1, \ldots, z_n]$. (1988) to appear in: I. Pure Appl. Algebra

[8] N. FITCHAS, A. GALLIGO, J. MORGENSTERN, Algorithmes rapides en séquentiel et en parallèle pour l'élimination de quantificateurs en géométrie élémentaire. Version préliminaire dans: Séminaire Structures Algébriques Ordonnées 1986–1987; version finale paraîtra dans Publ. Univ. Paris VII

[9] N. FITCHAS, Algorithmic aspects of Suslin's proof of Serre's Conjecture. Manuscript, Instituto Argentino de Matemática, Buenos Aires (1988). Soumis à K-Theory Yournall

[10] W. FULTON, Intersection Theory. Erg. Math., 3. Folge, 2. Bd., Springer Verlag, Berlin 1984

[11] A. GALLIGO, J. HEINTZ, J. MORGENSTERN, Parallelism and fast quantifier elimination over algebraically (and real) closed fields. Invited lecture Int. Conf. FCT '87, Kazan, USSR, 1987

[12] J. HEINTZ, Definability and fast quantifier elimination in algebraically closed fields. Theoret. Comput. Sci. 24 (1983) 239–277; Traduction en russe: Kyberneticeskij Sbornik, Novaja Serija Vyp. 22, Mir Moscow (1985) 113–158

[13] —, C. P. SCHNORR, Testing polynomials which are easy to compute. 12th Ann. Symp. ACM Comput. 1980, 262–280; et aussi dans: Logic and Algorithmic. An international Symposium held in honour of Ernst Specker, Monographie No 30 de L'Enseignement Mathématique, Genève 1982, 237–254

[14] J. HEINTZ, M. SIEVEKING, Absolute Primality of Polynomials is Decidable in Random Polynomial Time in the Number of Variables. 8th Int. Coll. Automata, Languages and Programming ICALP 81, Springer LN Comput. Sci. 115 (1981) 16–28

[15] J. HEINTZ, M. F. ROY, P. SOLERNÓ, On the complexity of semialgebraic sets. Proc. IFIP Congress '89 (San Francisco 1989) North Holland (1989) 293–298

[16] G. Hermann, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Math. Ann. **95** (1926) 736–788
[17] J. P. Jouanolou, Théorèmes de Bertini et applications. Birkhäuser PM **42** (1983)
[18] E. Kaltofen, Computing with polynomials given by straight-line programs II: sparse factorization. Proc. 26th IEEE Symp. Foundations Comp. Sci. 1985, 451–458
[19] J. Kollár, Sharp effective Nullstellensatz. I. AMS **1** (1988) 963–975
[20] T. Y. Lam, Serre's Conjecture. Springer LN Math. **635** (1978)
[21] D. Lazard, Algèbre linéaire sur $K[X_1, \ldots, X_n]$ et élimination. Bull. Soc. Math. France **105** (1977) 165–190
[22] –, Résolution des systèmes d'équations algébriques. Theoret. Comput. Sci. **15** (1981) 77–110
[23] F. S. Macaulay, Algebraic Theory of Modular Systems. Cambridge Tracts in Math. **19**, Cambridge Univ. Press 1916
[24] H. Matsumura, Commutative algebra. (First edition) Benjamin/Cummings, Reading Mass. 1970
[25] Ju. V. Nesterenko, Bounds for the characteristic function of a prime ideal. Mat. Sbornik **128**, No 1 (1984) 11–34 = Math. USSR Sbornik **51** (1985) 9–32
[26] B. Shiffman, Degree bounds for the Nullstellensatz and Bezout equation in arbitrary characteristic. Manuscript John Hopkins University 1988
[27] B. Sturmfels, An algorithmic proof of the Quillen-Suslin Theorem. Manuscript IMA, April 1988
[28] –, Computational Algebraic Geometry of Projective Configurations. IMA Preprint Series # 389, January 1988

**Post-Scriptum.** Après l'acceptation de notre article nous avons reçu la prépublication suivante:
P. Philippon, Théorème des zéros effectif d'après J. Kollár. Séminaire I.H.P. 1988
Dans ce travail l'auteur démontre un Nullstellensatz effectif à l'aide du complexe de Koszul.

*Instituto Argentino de Matematica*
*Consejo Nacional de Investigaciones*
*Cientificas y Técnicas (Conicet)*
*Viamonte 1636*
*(1055) Buenos Aires, Argentina*

*Departement de Mathématiques*
*Université de Nice*
*Parc Valrose*
*06034 Nice cedex*
*France*