Abstract

This paper is the continuation of a previous one devoted to the complexity of standard bases in projective dimension zero (see Giusti, 1989). We improve the upper bound on the maximal degree of elements in a standard basis, with respect to any choice of coordinates and any compatible ordering, given in *loc.cit.* This bound is sharp, being attained for complete intersections and lexicographic ordering.

COMPLEXITY OF STANDARD BASES IN PROJECTIVE DIMENSION ZERO II

Marc Giusti *
SDI CNRS 6176 "Calcul formel, Algèbre et Géométrie algorithmiques"
(associée au Centre de Mathématiques, URA CNRS D.0169)
Laboratoire d'Informatique
Ecole Polytechnique
91128 PALAISEAU CEDEX
giusti@cmep.polytechnique.fr
cfmagi@frpoly11.BITNET

February 23, 1995

INTRODUCTION

Let us consider an algebraic projective subvariety of $\mathbf{P}^n$, defined by a homogeneous ideal I of the polynomial algebra $R = k[x_0, \ldots, x_n]$ over some ground field k. A standard basis of I, w.r.t. a total compatible ordering of the monomials of R, depends strongly on the chosen order and on the coordinates, and can vary a lot.

However in low dimension, namely less or equal to zero, we can give a sharp upper bound for the maximal degree of the generators of a standard basis, with respect to any choice of coordinates and any compatible ordering. It is first expressed with intrinsic quantities (depending only on the ideal itself) associated to the Hilbert function. It improves the result given in Giusti (1989, Proposition 1.2.).

Eventually, if d is the maximal degree of the input generators of I, this bound is d^n in dimension zero. This result was obtained by I. Bermejo (1990), in the following particular case : the ideal defines an arithmetically Cohen-Macaulay projective variety of dimension zero, the coordinates are rather pleasant ("commodes" in the sense of Kouchnirenko), and the order on the monomials is the pure lexicographic one. It is sharp, being attained for complete intersections and pure lexicographic ordering, as already noticed by I. Bermejo.

The proof is essentially combinatorial, using stable subsets of $\mathbf{N}^{n+1}$, and has practically nothing to do with commutative algebra ...

*Partially supported by a grant from GDR G0060 "Calcul Formel, Algorithmes, Langages et Systèmes" and from PRC "Mathématiques et Informatique".

1 STABLE SUBSETS

1.1 Some preliminary facts

Let E be a *stable* subset of $\mathbf{N}^{n+1}$, i.e. such that for every a in E and every b in $\mathbf{N}^{n+1}$, $a+b$ is still in E. We shall recall in this section different results on stable subsets.

1.1.1 Classical definitions

A stable subset E is minimally generated by a finite subset $B(E)$ ("Dickson's lemma"). The *degree* of a point $a=(a_0,\ldots,a_n)$ of $\mathbf{N}^{n+1}$ being the integer $|a|=a_0+\cdots+a_n$, we shall denote by $D(E)$ the maximal degree of the elements of $B(E)$.

The function HF_E, which associates to every integer s the number of elements of degree s not belonging to E, is called the *Hilbert function* of E. For the argument s large enough, this function is equal to a polynomial $HP(E)$, the so-called *Hilbert polynomial* of E. The *regularity* of the Hilbert function is the smallest integer $H(E)$ after which the function coincides with the polynomial.

The degree of the Hilbert polynomial is then the *dimension* of E, and the leading coefficient multiplied by $dim(E)!$ is the *degree* of E (noted $deg(E)$). Finally by convention the degree -1 will be associated to the zero polynomial.

1.1.2 Induction on the ambient dimension

To study stable subsets, a natural idea is to proceed by induction on n, so we introduce the sections $E_i^{(j)}$ of E by the hyperplane $\{x_j=i\}$. Again by a noetherianity argument (Dickson's lemma), this section is constant for large i. Let us denote by $e^{(j)}(E)$ (or simply $e(E)$ or e if there is no ambiguity on the axis x_j) the smallest integer after which this happens. We shall speak of the "section at infinity" $E_\infty^{(j)}$, or simply E_∞ instead of this constant section $E_i^{(j)}$ ($i \geq e^{(j)}$). As an application, we have the following :

1.1.3 Lemma :

Considering sections orthogonal to any fixed axis, we obtain :

$$H(E) \leq Max\{i+H(E_i) \mid i=0,\ldots,e\}$$

Proof : it is given in Giusti (1988, proof of Proposition 3.4).

1.1.4 Saturation

For every index j ($j=0,\ldots,n$), let us consider the cartesian product of the section at infinity $E_\infty^{(j)}$ by the corresponding axis x_j. This product is a stable subset of $\mathbf{N}^{n+1}$ containing E. The intersection of all these cylinders ($j=0,\ldots,n$) is still stable, and contains E. We call it the *saturation* of E, or the *saturated* stable subset $G(E)$ associated to E. A useful property of the couple $E \subseteq G(E)$ is :

1.1.5 Lemma :

The Hilbert polynomials of a stable subset and its saturation coincide, since the difference $F(E) = G(E) - E$ *is a finite subset.*

Proof : Let us discard first the trivial case where $F(E)$ is empty. Then let $A = (A_0, \ldots, A_n)$ be a point of $F(E)$, and let us draw from A the $n+1$ lines $A + \mathbf{N}^{\{0,\ldots,0,j,0,\ldots,0\}}$. Any of this lines intersects E, because if not it should also intersect the complementary of the corresponding section at infinity, and A should not belong to the saturation. So there is a point of E on each line, which implies that $F(E)$ is finite.

This notion of saturation is general, but was already used by Giusti (1989, Lemma 1.2.1.) in the case of 0-dimensional stable subsets for the same purpose.

1.2 Negative dimensional case

In this situation, the complement $\mathbf{N}^{n+1} - E$ is finite, say of volume $vol(E)$ (we say also that this last integer is the covolume of E). In particular, the integers $vol(E_i)$ are zero for i greater or equal to e, and not before.

1.2.1 Lemma :

Let E *be a stable subset of negative dimension. Then :*

$$vol(E) \geq Max\{i + vol(E_i) \mid i = 0, \ldots, e\}$$

Proof : The integers $vol(E_i)$, $(i = 0, \ldots, e-1)$ form a decreasing sequence of integers at least 1. Thus :

$$\begin{aligned} vol(E) &= \sum_{i=0}^{e-1} vol(E_i) \geq vol(E_0) + (e-1) \\ &= Max\{vol(E_i) \mid i = 0, \ldots, e-1\} + Max\{i \mid i = 0, \ldots, e-1\} \\ &\geq Max\{vol(E_i) + i \mid i = 0, \ldots, e-1\} \end{aligned}$$

Furthermore, E_e being the whole ambiant space is of covolume zero. As the point $(0, \ldots, 0, e)$ is a generator of E, there are e points on the x_n-axis not belonging to E, and $vol(E)$ is at least e. Thus the proof is complete.

1.2.2 Lemma :

Let E *be a stable subset of negative dimension. Then :*

$$D(E) \leq H(E) \leq vol(E)$$

Proof : the first inequality is proved in Giusti (1988, Proposition 3.6.), the second by induction on n. The assertion is clear when n is equal to 0. Then :

$$\begin{aligned} vol(E) &\geq Max\{vol(E_i) + i \mid i = 0, \ldots, e\} \ (1.2.1) \\ &\geq Max\{H(E_i) + i \mid i = 0, \ldots, e\} \ \text{(induction hypothesis)} \\ &\geq H(E) \ (1.1.3) \end{aligned}$$

1.3 Zero dimensional case

1.3.1 Structure of saturated subsets

We are first interested in a saturated stable subset G of dimension zero, which is in this case an intersection of cylinders whose section is of zero or finite covolume :

$$G = \bigcap_{j=0}^{n} (G_\infty^{(j)} \times \mathbf{N}^{\{0,\ldots,0,j,0,\ldots,0\}})$$

Let us call *trivial* a cylinder corresponding to the whole ambiant space. The Hilbert polynomial is a non zero constant, whose value is the degree of the saturated subset, and :

$$deg(G) = \sum_{j=0}^{n} vol(G_\infty^{(j)})$$

1.3.2 Regularity of the sections

Unfortunately a section G_i is in general no more saturated, which prevents us from straightforward inductions. Nevertheless, an upper bound of the regularity is the following :

Let G be a stable saturated subset of dimension zero. Considering sections orthogonal to some fixed axis, we get :

$$H(G_i) \leq Max(H(G(G_i)), vol(G_\infty))$$

Proof : we can assume, without loss of generality, that we are looking at sections orthogonal to the last axis x_n. From :

$$G = \bigcap_{j=0}^{n} (G_\infty^{(j)} \times \mathbf{N}^{\{0,\ldots,0,j,0,\ldots,0\}})$$

we can deduce, intersecting by $\{x_n = i\}$:

$$G_i^{(n)} = G_\infty^{(n)} \bigcap_{j \neq n} (G_\infty^{(j)} \cap \{x_n = i\}) \times \mathbf{N}^{\{0,\ldots,0,j,0,\ldots,0\}} \tag{1}$$

By abstract non-sense, we see that the second part of the previous intersection is the saturation of G_i, and that $F(G_i)$ is a subset of the complementary of $G_\infty^{(n)}$. In particular, the Hilbert functions of G_i and its saturation coincide for any argument larger or equal to $vol(G_\infty^{(n)}) \geq H(G_\infty^{(n)})$ by 1.2.2. Hence the regularity of G_i is at most $Max(H(G(G_i)), vol(G_\infty))$.

1.3.3 Constancy of the sections

Let G be a stable saturated subset of dimension zero. Considering sections orthogonal to the last axis, we get :

$$e^{(n)}(G) \leq Max\{vol(G_\infty^{(j)}) \mid j \neq n\}$$

Proof : let j be an index not equal to n. For i larger or equal to $vol(G_\infty^{(j)})$, 1.2.2 implies that $G_\infty^{(j)} \cap \{x_n = i\}$ is equal to its whole ambiant space, hence for i larger or equal to $Max\{vol(G_\infty^{(j)}) \mid j \neq n\}$, the decomposition (1) yields that G_i is constant equal to G_∞.

Let us turn now to the degree and the regularity of G itself. We know already the following fact established in Giusti (1989, Lemma 1.2.2.) :

1.3.4 Lemma :

Let G be a stable saturated subset of dimension zero. Then :

$$D(G) \leq deg(G)$$

The behaviour of the regularity is the same :

1.3.5 Lemma :

$$H(G) \leq deg(G)$$

Proof : The proof goes by induction on the number of the non trivial cylinders.

The first case is when this number is one, where it is clear since G is the cylinder $G_\infty \times \mathbf{N} = G_0 \times \mathbf{N}$: by 1.2.2, the regularity of G_0 is at most its covolume, which is nothing else than the degree of G. Hence $H(G) = H(G_0) - 1$ is at most $deg(G) - 1$.

In the general case, the saturated subset is an intersection of more than two cylinders, and assume without loss of generality that the last axis x_n corresponds to one of them. So using successively 1.1.3 , 1.3.2 and the induction hypothesis, :

$$\begin{aligned}
H(G) &\leq Max\{i + H(G_i) \mid i = 0, \ldots, e\} \\
&\leq Max(Max\{i + H(G(G_i)) \mid i = 0, \ldots, e\}, Max\{i + vol(G_\infty) \mid i = 0, \ldots, e\}) \\
&\leq Max(Max\{i + deg(G(G_i)) \mid i = 0, \ldots, e\}, e + vol(G_\infty)) \\
&\leq Max(Max\{i + deg(G_i) \mid i = 0, \ldots, e\}, e + vol(G_\infty))
\end{aligned}$$

By 1.3.3 , the second term is at most $Max\{vol(G_\infty^{(j)}) \mid j \neq n\} + vol(G_\infty^{(n)})$, itself at most $deg(G)$. Now :

$$\begin{aligned}
i + deg(G_i) &= i + \sum_{j \neq n} vol(G_\infty^{(j)} \cap \{x_n = i\}) \\
&\leq \sum_{j \neq n} i + vol(G_\infty^{(j)} \cap \{x_n = i\})
\end{aligned}$$

Taking the maximum of all these quantities, for i running from 0 to e, yields the lemma using 1.2.1 and 1.3.3.

2 The theorem :

Let E be a stable subset of $\mathbf{N}^{n+1}$ of dimension 0. Then :

$$D(E) \leq Max(deg(E), H(E))$$

Proof : it follows the proof given in Giusti (1989, 1.2.3), in a slightly different way. For the convenience of the reader, we give it completely.

We divide the basis $B(E)$ into two classes of generators : the first ones belong to $B(G)$, the others do not. If $A = (A_0, \ldots, A_n)$ is in the last class, being a generator of E there exists an index i such that $(A_0, \ldots, A_i - 1, \ldots, A_n)$ is no longer in E but stays in G, hence is in $F(E)$. Either the degree of any element in the second class is at most $deg(E)$, and the conclusion holds using the lemma 1.3.4 ; or not, and then using again the lemma 1.3.4, we see that the maximal degree $D(E)$ is attained for an element A not in $B(G(E))$, so $D(E)-1$ is at least $deg(E)$. Notice that there exists a point in $F(E)$ of degree $D(E)-1$, so let us compute the Hilbert function in this degree :

$$\begin{aligned} HF_E(D(E)-1) &= HF_F(D(E)-1) + HF_G(D(E)-1) \\ &> HF_G(D(E)-1) \end{aligned}$$

The regularity of HF_G is bounded above by $deg(G(E)) = deg(E)$ (1.3.5, 1.1.5) hence by $D(E)-1$. So :

$$HF_E(D(E)-1) > HP_G(D(E)-1) = HP_E(D(E)-1)$$

We conclude that $H(E)$ is at least $D(E)$, and in all cases we proved the proposition.

2.1 Corollary

Let k be a field, R the polynomial algebra $k[x_0, \ldots, x_n]$ and I a homogeneous ideal of R. Let us choose any compatible total ordering on the monomials of R. Let us consider the projective subvariety $V(I)$ of $\mathbf{P}^n$ defined by I, and let us assume that its dimension is zero.

With the notations and under the assumptions above, the maximal degree of a standard basis, w.r.t. any choice of the coordinates and of the ordering, is at most the maximum of the degree of the variety $V(I)$ and the regularity of the Hilbert function of I.

2.2 Corollary

Assume in the corollary 2.1 that the ideal I is given by generators of degree at most d. Under the same assumptions, the maximal degree of a standard basis, w.r.t. any choice of coordinates and compatible total ordering, is at most d^n.

Proof : the degree of the variety is at most d^n by Bézout's theorem. The regularity is at most $1 + (n+1)(d-1)$ by a result of Lazard (1981). After treating the limit cases, the corollary follows.

2.3 An example

In the following example the upper bound of the theorem is attained, by the regularity and not the degree, despite of the quite different asymptotic behaviours.

Let $d \geq 2$ be an integer, and let us consider the ideal $(z^d - y^d, yz - xy, xz)$ of $k[x, y, z]$. Geometrically, it defines a unique point $(1, 0, 0)$ of $\mathbf{P}^2$. A standard basis with respect to the lexicographic order induced by $z > y > x$ is easily computed, and is $(z^d - y^d, yz - xy, xz, y^{d+1}, xy^d, x^2y)$. So it is easily seen that the degree is 1, the regularity $d+1$, this last integer beeing the maximal degree of the standard basis.

REFERENCES

I. BERMEJO (1990), 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, *Notes aux Compte-Rendus de l'Académie des Sciences de Paris*, **t. 310**, Série I, 591-594.

M. GIUSTI (1988), Combinatorial dimension theory of algebraic varieties, in "Computational Aspects of Commutative Algebra", special issue, *Journal of Symbolic Computation, Academic Press* **6**, 115-131.

M. GIUSTI (1989), Complexity of standard bases in projective dimension zero, Proceedings of EUROCAL 87 (European Conference on Computer Algebra, Leipzig, RDA), *Lecture Notes in Computer Science 378, Springer Verlag*, 333-335.

D. LAZARD (1981), Résolution des systèmes d'équations algébriques, *Theoretical Computer Science* **15**, 77-110.