COMPLEXITY OF STANDARD BASES IN PROJECTIVE DIMENSION ZERO

Marc Giusti *
Centre de Mathématiques
Ecole Polytechnique
91128 Palaiseau Cedex
Unité associée au CNRS No. 169
and
GRECO de Calcul Formel No. 60
uucp: ... mcvax!inria!cmep!giusti

February 23, 1995

Abstract

We prove in this paper that the maximal degree of elements in a standard basis, with respect to any choice of coordinates and any compatible ordering, is essentially linear in the degree of the projective variety if its dimension is zero. This implies that the time and space complexities of constructing a standard basis in this case are essentially polynomial in the degree of the variety.

INTRODUCTION

The aim of this technical report is to prove that the maximal degree of elements in a standard basis, with respect to any choice of coordinates and any compatible ordering, is essentially linear in the degree of the projective variety if its dimension is zero.

1 STABLE SUBSETS OF DIMENSION ZERO

1.1 Preliminaries

We shall use freely in this section classical results on stable subsets, as recalled in [GI]. A stable subset E of $\mathbf{N}^{n+1}$ is minimally generated by a finite subset $B(E)$. We shall denote by $D(E)$ the maximal degree of the elements of $B(E)$ and by $H(E)$ the regularity of the Hilbert function HF_E. The degree of the Hilbert polynomial is then the *dimension* $dim(E)$ of E, and the coefficient of the term of maximal degree multiplied by $dim(E)!$ is the *degree* $deg(E)$ of E.

1.2 Proposition

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

$$D(E) \leq Max((n+1)deg(E), H(E))$$

*Partially supported by a grant from the PRC "Mathématiques et Informatique"

Proof : If the dimension is 0, the Hilbert function becomes constant for large values of the argument. Hence the complement of any section
$E_i = E \cap \{x_i = s\}$ is constant for large s, either empty or of finite volume smaller than the degree of E. Call e the number of indices corresponding to a non empty section (*admissible* indices) . The complement of E contains any such cylinder based on E_i whose fiber is the corresponding i^{th} axis. This leads to the following decomposition of the complement of E :

1.2.1 Lemma

Let us define $G(E)$ as the complement of the union of the previously defined cylinders, i.e.

$$G(E) = \{A \in \mathbf{N}^{n+1} \mid \forall \; admissible \; i, \; \forall w \gg 0 \,, (A_0, \ldots, A_i + w, \ldots, A_n) \in E\}$$

Then $G(E)$ is a stable subset, and the complement $F(E) = G(E) \backslash E$ is finite.

Proof : Since the Hilbert function of E and $G(E)$ are equal for large values of their argument, $F(E)$ is finite.

Now let us turn to the stability of $G(E)$. By construction, $G(E)$ contains E : so if a point of $G(E))$ belongs already to E, there is no problem for any positively translated point to belong to E, hence to $G(E)$. If not, let us consider a point A in $F(E)$. As $F(E)$ is finite, for any index i the translated point $(A_0, \ldots, A_i + B_i, \ldots, A_n)$ goes outside of $F(E)$ for large B_i, hence belongs to $G(E)$.

1.2.2 Lemma

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

Proof : Let $A = (A_0, \ldots, A_n)$ be an element of $B(G(E))$. Fix an admissible index i ; then for every index j different from i, the point
$(A_0, \ldots, A_j - 1, \ldots, A_n)$ is no longer in $G(E)$, which means that the projection of A on the coordinate hyperplane $x_i = 0$ is an element of $B(E_i)$. Moreover if v_i is the volume of the complement of E_i, the degree of this projection is upper bounded by v_i, that is :

$$A_0 + \ldots + A_n \leq A_i + v_i$$

If there is only one admissible index, the corresponding A_i is zero, and we are done. If not, summing over all indices we obtain that the degree of A is bounded above by $1/(e-1)$ times the degree $deg(E)$, and a fortiori by the degree.

1.2.3 End of the proof

We divide the basis $B(E)$ into two classes : the first ones belong to $B(G)$, the others do not. Furthermore if $A = (A_0, \ldots, A_n)$ is in the last class, 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 its degree is always smaller than $(n+1)deg(E)$, and the conclusion holds using the lemma 1.2.2 ; or not, and then using again the lemma 1.2.2, we see that the maximal degree $D(E)$ is attained for an element A not in $B(G(E))$. As we have already remarked, there exists a point in $F(E)$ of degree one less, so let us compute the Hilbert function in this degree ; with the notations of [GI]

$$HF_E(D(E)-1) = HF_F(D(E)-1) + HF_G(D(E)-1)$$

The regularity of HF_G is bounded above by $(n+1)D(G(E))$, hence by lemma 1.2.2 by $(n+1)deg(E)$, itself by $D(E)-1$. Putting all together we get

$$HF_E(D(E)-1) > HF_G(D(E)-1)$$

Since $F(E)$ is finite, the Hilbert functions of E and $G(E)$ are the same, and we conclude that $H(E)$ is at least $D(E)$.

So in all cases we have proved the proposition.

2 A COMPLEXITY THEOREM

Let k be a field, R the polynomial algebra $k[x_0, \ldots, x_n]$ and I a homogeneous ideal of R generated by polynomials $f_1, \ldots, f_t$ of degree at most d and of maximal size 2^M. 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. Call δ the modified degree of $V(I)$, i.e. the maximum of the degree of $V(I)$ and of d.

2.1 Theorem

If the dimension of $V(I)$ is zero, the maximal degree of elements of a standard basis, with respect to any compatible ordering, is smaller than $n+1$ times the modified degree of the variety.

Proof : Let us apply the proposition 1.2 to the stable subset $E(I)$ of $\mathbf{N}^{n+1}$, of dimension zero. By a result showed by D. Lazard [LA], the regularity $H(E(I))$ is smaller than $(n+1)d$.

2.2 Corollary

The time or space complexity needed to construct a standard basis in projective dimension zero is polynomial in the modified degree of the variety, δ, more precisely polynomial in $MtO(\delta^n)$.

REFERENCES

[GI] M. GIUSTI, Théorie combinatoire de la dimension d'une variété algébrique, Notes informelles de Calcul Formel VI, prépublication du Centre de Mathématiques de l'Ecole Polytechnique (1985), et Compt. Rend. du Colloque Algèbre et Algèbre effective de Rennes (1985).

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