Abstract

Several algorithms are already known to compute the dimension of a projective algebraic variety. But they all rely on the construction of the whole standard basis of the defining ideal, leading to non optimal worst case complexities. We present below a new algorithm, based on a truncation idea, with better complexity.

COMBINATORIAL DIMENSION THEORY OF ALGEBRAIC VARIETIES

Marc Giusti [1]
Centre de Mathématiques
Ecole Polytechnique
91128 Palaiseau Cedex
Unité de Recherche Associée au CNRS D.0169
and
GRECO de Calcul Formel No. 60
uucp : giusti@cmep.poly.fr
bitnet : cfmagi@frpoly11

February 17, 1995

[1] Partially supported by a grant from the PRC "Mathématiques et Informatique"

INTRODUCTION

How can one compute the dimension of a projective algebraic subset, given by a system of equations ? There are different definitions, and their equivalence is part of the classical dimension theory in algebraic geometry. The game is then the following : to make some definition of dimension effective enough to get an algorithm.

A first method consists to think *algebraically* and to use the Hilbert function of the quotient ring. It can be easily computed once a particular set of generators (a so called standard basis (= Gröbner basis) of the defining ideal) is known. In fact such a basis yields a monomial ideal with the same Hilbert function, hence the same Hilbert polynomial, whose degree is the dimension. So it is the order at infinity of this numerical function, attained for example through the maximal dimension of a coordinate plane containing no elements of the monomial ideal.
Based on this idea there are different algorithms already known in the litterature (see [CF] [KR] [KW] [LJ]). Unfortunately this method needs to construct a whole standard basis from a given set of generators, and leads necessarily to a disastrous upper bound for the worst case complexity, as shown by the explicit examples of MAYR-MEYER [MM] [D] : there are ideals for which deciding whether a given polynomial belongs to them needs exponential space. As the knowledge of a standard basis easily solves the previous problem, computing such a basis needs also exponential space...

In order to bypass that, why not to determine the Hilbert polynomial by interpolation, if we know an upper bound for the regularity of the Hilbert function ? Alas, it happens that the same catastrophic behaviour cannot be avoided, as indicated in [GI].

Another way is to think *geometrically* and to cut the variety by linear subspaces, as proposed by LAZARD [LA2] [LA3]. Once again this dimension can be read on a standard basis, this time for a particular ordering [GI]. But it involves the costly introduction of generic coordinates.

We will propose below an approach combining the combinatorial point of vue (standard bases) and the geometric ones (section/projection). We shall introduce two new characterizations of the dimension, which come in between the classical approaches in a remarkable way, since this gives a new proof of the dimension theorem through their relationships with the classical definitions.

Furthermore we do not need a whole standard basis, which is a goal much too complicated, in order to extract a very partial useful information. Actually, a part in rather low degree is enough. Using this truncation idea, we will give an algorithm computing the dimension, whose time and space complexity are polynomial in a suitable measure of the input data.

1 STANDARD BASES

Let k be a field, and R the polynomial algebra $k[x_0, x_1, \ldots, x_n]$, with the usual graduation induced by the total degree. To study homogeneous ideals of R, an essential idea going back to MACAULAY [MA], consists in totally ordering the monomials of the polynomial ring, in one-to-one correspondence with the points of $\mathbf{N}^{n+1}$, but in a compatible way with the multiplication of R. We will use the following orderings :

1.1 Definition : lower (resp. upper) lexicographic ordering

A point $a = (a_0, \ldots, a_n)$ of $\mathbf{N}^{n+1}$ is smaller than a point $b = (b_0, \ldots, b_n)$ for the lower lexicographic ordering (resp. larger for the upper lexicographic ordering) if and only if there exists an index i $(0 \leq i \leq n)$ such that :

$$a_0 = b_0, \ldots, \; a_{i-1} = b_{i-1}, \; a_i < b_i$$

(resp.

$$a_n = b_n, \ldots, \; a_{i+1} = b_{i+1}, \; a_i > b_i)$$

1.2 Definitions : lower (resp. upper) lexicographic filtration

To every non zero homogeneous polynomial :

$$f = \sum_{a \in \mathbf{N}^{n+1}} f_a \, x^a$$

is then associated its support $\{a \in \mathbf{N}^{n+1} \mid f_a \neq 0\}$ in $\mathbf{N}^{n+1}$. The smallest (resp. largest) element of the support of f for the lower (resp. upper) lexicographic ordering is called its *leading monomial* $exp(f)$. The *leading* or *initial form* $in(f)$ is the term

$$f_{exp(f)} \, x^{exp(f)}$$

We shall speak from now on of the lower (resp. upper) filtration of R.

1.3 Definition : mixed lexicographic filtration of order m

Let us fix an integer m between 0 and $n-1$. After BAYER and STILLMAN [BS], we introduce now the following total ordering : by definition a point $a = (a_0, \ldots, a_n)$ of $\mathbf{N}^{n+1}$ is smaller than a point $b = (b_0, \ldots, b_n)$ if the point $(a_0 + \cdots + a_m, a_0, \ldots, a_{n-1})$ is smaller than the point $(b_0 + \cdots + b_m, b_0, \ldots, b_{n-1})$ for the lower lexicographic ordering.

The leading monomial of a non zero polynomial is then the smallest element of its support.

1.4 Definition : stable subsets

Given a non zero homogeneous ideal I, the set $E(I)$ of all the leading monomials of its non zero elements form a so called *stable* subset of $\mathbf{N}^{n+1}$, i.e. :

$$a \in E(I) \Longrightarrow a + \mathbf{N}^{n+1} \subseteq E(I)$$

By convention, the empty set is associated to the trivial ideal (0).

1.5 Dickson's lemma

Every stable subset E of $\mathbf{N}^{n+1}$ is finitely generated, and there exists a unique minimally generating finite family $a^{(1)}, \ldots, a^{(p)}$, i.e. :

$$E = \bigcup_{i=1}^{p} (a^{(i)} + \mathbf{N}^{n+1})$$

The proof is easy by induction on n.

1.6 Definition : standard bases

Let I be an homogeneous ideal of R. By Dickson's lemma, $E(I)$ is minimally generated by some family, say $a_1, \ldots, a_p$. Following HIRONAKA [HI], we define a *standard basis* of I as a family of polynomials of I such that their leading monomials form this minimal generating subset.

1.7 Notation

If E is a stable subset of $\mathbf{N}^{n+1}$, we denote by $D(E)$ the maximal degree of the elements of a generating family of E, which is minimal for the inclusion.

1.8 Hironaka's division theorem

Let I be an homogeneous ideal of R. Every polynomial of R is equivalent modulo I to a unique polynomial called the remainder of the division by I, either zero or owning all its monomials outside of $E(I)$.

Proof : actually if the polynomial f to be divided is not zero, it has a leading monomial. If this last monomial belongs to $E(I)$, it can be divided by the leading monomial of some element of I, say g. The input polynomial f is then equivalent to $f - (in(f)/in(g))g$, which, if non zero, owns a strictly smaller leading monomial. Since there is only a finite numbers of monomials of given degree, the iterated process stops on a polynomial, which if not zero, has a leading monomial outside of $E(I)$. To conclude we apply recursively the same division procedure to the reductum of this last polynomial, i.e. itself minus its initial form.

The uniqueness of the remainder follows trivially from its property of having all its monomials outside of $E(I)$.

1.9 Corollary

Every standard basis of an ideal generates this ideal.

Proof : in fact, the remainder of the division of any polynomial of the ideal by a standard basis $f_1, \ldots, f_p$ must be zero : if not, its leading monomial should be simultaneously in $E(I)$ and its complementary.
Note that it proves by the way the noetherianity of polynomial rings.

1.10 Corollary

As k-vector space, the quotient R/I is isomorphic to the direct sum of the k-vector subspaces of dimension one generated by the monomials of the complementary of $E(I)$:

$$R/I = \bigoplus_{a \notin E(I)} kx^a$$

Eventually we will show that the filtrations we introduced before have a nice geometric interpretation :

1.11 Proposition : section by a linear subvariety

Fix an integer s between 0 and $n-1$. Let $f_1, \ldots, f_t$ be a standard basis of I, with respect to the lower lexicographic filtration. Then the f_i's with leading monomial not depending on $x_0, \ldots, x_s$, together with $x_0, \ldots, x_s$ form a standard basis of $I + (x_0, \ldots, x_s)$, with respect to the induced lower lexicographic filtration ; hence they define the section of $Z(I)$ by the linear subvariety $x_0 = \cdots = x_s = 0$.

Proof : it follows from the remark that if x_0 divides the leading monomial of a polynomial, it actually divides this polynomial. Hence the proposition is true for $s = 0$. The general result is clear by induction.

1.12 Proposition : projection on a linear subvariety

In this paragraph the ground field k will be algebraically closed.

Fix an integer p between 0 and $n-1$. Let $f_1, \ldots, f_t$ be a standard basis of I, with respect to the upper lexicographic filtration. Then the f_i's with leading monomial depending only on the variables $x_0, \ldots, x_p$ form a standard basis of $I \cap k[x_0, \ldots, x_p]$; hence if we assume that the linear subvariety defined by $x_0, \ldots, x_p$ does not intersect $Z(I)$, they define the projection of $Z(I)$ on the linear subvariety $x_{p+1} = \cdots = x_n = 0$.

Proof : Let p be equal to zero. The first part follows from the remark that if the leading monomial of a polynomial does not depend on x_n, the polynomial itself does not. Now let π be the morphism restriction to $Z(I)$ of the projection of $\mathbf{P}^n \backslash (0, \ldots, 0, 1)$ on the hyperplane $x_n = 0$. By abstract non-sense we get the equality of the Zariski closure of $\pi(Z(I))$ with the algebraic subset defined by $I \cap k[x_0, \ldots, x_{n-1}]$. Since the restriction of π to $Z(I)$ is proper, we obtain the wanted equality.

The general result follows easily by induction.

1.13 Geometric interpretation of the mixed filtrations

Fix an integer m between 0 and $n-1$. Let $f_1, \ldots, f_t$ be a standard basis of I, with respect to the mixed lexicographic filtration of order m.
Then the f_i's with leading monomial not depending on the variables $x_0, \ldots, x_m$ form a standard basis of $I + (x_0, \ldots, x_m)$; hence they define the section of $Z(I)$ by the linear subvariety $x_0 = \cdots = x_m = 0$.
On the other hand the f_i's with leading monomial depending only on the variables $x_0, \ldots, x_m$

form a standard basis of $I \cap k[x_0, \ldots, x_m]$ for the induced lower lexicographic filtration. Hence if we assume that linear subvariety defined by $x_0, \ldots, x_m$ does not intersect $Z(I)$, they define the projection of $Z(I)$ on the linear subvariety defined by $x_{m+1} = \cdots = x_n = 0$.

The proof is similar to the two previous ones.

2 SOME BOUNDS FOR THE REGULARITY OF THE HILBERT FUNCTION

The *degree* of a point $a = (a_0, \ldots, a_n)$ of $\mathbb{N}^{n+1}$ is the integer $|a| = a_0 + \cdots + a_n$.

2.1 Definition : Hilbert function

Let E be a stable subset of $\mathbb{N}^{n+1}$; 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 the complementary of E :

$$HF_E(s) = \#\{a \in \mathbb{N}^{n+1} \mid a \notin E, |a| = s\}$$

2.2 Definition : Hilbert polynomial

It is classical that for s large enough, the Hilbert function HF_E is equal to a polynomial HP_E (the so called *Hilbert polynomial*). Moreover there are integers $c_o, \ldots, c_d$ such that :

$$HP_E(s) = \sum_{i=0}^{d} c_i \begin{pmatrix} s \\ d-i \end{pmatrix}$$

where $\begin{pmatrix} s \\ r \end{pmatrix} = s(s-1)(\cdots)(s-r+1)/r!$ is the binomial coefficient function. By definition, d is the *dimension* of the complementary of E, and c_o its *degree*. Finally by convention the degree -1 will be associated to the zero polynomial.

2.3 Definition : regularity of the Hilbert function

The *regularity* $H(E)$ of the Hilbert function is the smallest integer where it becomes equal to the Hilbert polynomial of E.

2.4 Proposition

$$H(E) \leq (n+1)(D(E)-1)+1$$

Proof : by induction on n. The claim is clear for $n = 0$. Then from Dickson's lemma, the section E_i of E by the hyperplane $\{x_n = i\}$ is constant for i at least some integer e and not before. Let us consider the following expansion of the Hilbert function :

$$HF_E(s) = \sum_{i=0}^{s} HF_{E_i}(s-i)$$

which breaks into three pieces as soon as s is large enough :

$$\begin{aligned} HF_E(s) &= \sum_{0\le i\le e-1} HF_{E_i}(s-i) + \sum_{e\le i\le s-H(E_e)} HF_{E_e}(s-i) + \sum_{s-H(E_e)+1\le i\le s} HF_{E_e}(s-i) \\ &= \sum_{0\le i\le e-1} HF_{E_i}(s-i) + \sum_{H(E_e)\le i\le s-e} HF_{E_e}(i) + \sum_{0\le i\le H(E_e)-1} HF_{E_e}(i) \end{aligned}$$

For s large enough this function becomes :

$$HF_E(s) = \sum_{0\le i\le e-1} HP_{E_i}(s-i) + \sum_{H(E_e)\le i\le s-e} HP_{E_e}(i) + \sum_{0\le i\le H(E_e)-1} HF_{E_e}(i)$$

which is the Hilbert polynomial HP_E since $\sum_{H(E_e)\le i\le s-e} HP_{E_e}(i)$ is effectively a polynomial in s. This is a consequence of the following classical lemma :

Lemma : let P be a polynomial of degree d with rational coefficients. For any two integers r and s, $\sum_{r\le i\le s} P(i)$ is a polynomial in s of degree $d+1$, with integral coefficients on the binomial basis if it was the case for P.

The proof is straightforward : as the binomial coefficient functions $\binom{s}{0}, \dots, \binom{s}{d}$ form a basis on $\mathbf{Q}$ of the vector space of all polynomials of degree less or equal to d, it is enough to prove the first claim on these particular polynomials, where it becomes trivial.

More precisely this expression is true as soon as s is larger than $Sup\{i + H(E_i) \mid 0 \le i \le e\}$, which occurs through the induction hypothesis if s is bigger than $(n+1)(D(E)-1)+1$.

(Note that we reproved by the way the classical facts on the Hilbert polynomial recalled in 2.2).

2.5 Example

Given a sequence of $n+1$ positive integers $a_0, \dots, a_n$, consider the ideal $(x_0^{a_0}, \dots, x_n^{a_n})$. This set of generators form a standard basis, and the associated stable subset E is the complement of a parallelepiped, whose point of maximal degree is $(a_0-1, \dots, a_n-1)$. Hence the regularity is $1 + \sum_{i=0}^{n}(a_i-1)$. Note that it is larger than $D(E)$ which is the maximum of the a_i's ; this remark will be developped below.

The particular case where all the a_i's are equal show that the previous bound of the regularity is sharp.

2.6 Proposition

If E is a negative dimensional stable subset, its regularity $H(E)$ is at least $D(E)$.

Proof : First let us discard the trivial case $E = \mathbf{N}^{n+1}$ where $D(E) = H(E) = 0$. Then consider an element $A = (A_0, \dots, A_n)$ of a minimally generating family of E. Since the degree of A is positive, there exists an index i for which A_i is positive, and the point $(A_0, \dots, A_i - 1, \dots, A_n)$ does not belong to E. Thus the Hilbert function is not zero for the argument $\mid A \mid -1$, hence is not equal to the Hilbert polynomial. So the regularity is at least $\mid A \mid$, and in particular at least $D(E)$.

2.7 Remark

If I is an homogeneous ideal of R, the Hilbert function of $E(I)$ is independant of the ordering by 1.10 and is called the *Hilbert function* of R/I.

3 DIMENSION THEORY

From now on, the ground field k is assumed to be algebraically closed. Let I be an homogeneous ideal of R defined by a given system of generators, and $Z(I)$ the projective algebraic subset defined in $\mathbf{P}^n$.

3.1 Various definitions of dimension

First an *algebraic* definition : the *Hilbert dimension* is the degree d of the Hilbert polynomial of R/I.

Then two *geometrical* definitions : the *section dimension* is the smallest integer s such that there exists a linear subvariety of codimension $s+1$ not intersecting $Z(I)$.

The *projection dimension* is the biggest integer p such that there exists a linear subvariety of dimension p on which $Z(I)$ can be surjectively projected.

It is classical that the three notions of dimension recalled above coincide, and their common value is called the *dimension* of the projective algebraic subset $Z(I)$. We will now introduce two combinatorial definitions :

3.2 Definitions : lower (resp. upper) lexicographic dimension

Let x be a system of coordinates on $\mathbf{P}^n$. We denote by $linf_x$ (resp. $lsup_x$) the smallest (resp. largest) integer e such that $E_x(I)$ relative to the lower (resp. upper) lexicographic filtration intersects the last $n-e$ coordinate axes of $\mathbf{N}^{n+1}$ (resp. does not intersect the plane of the first $e+1$ coordinates).

The minimum $linf$ of all $linf_x$ (resp. the maximum $lsup$ of all $lsup_x$) when x ranges through all systems of coordinates of $\mathbf{P}^n$ is called the *lower* (resp. *upper*) *lexicographic dimension.*

3.3 Dimension theorem

The lower and upper lexicographic dimensions are equal to the dimension of the projective algebraic subset.

The proof goes as follows, showing actually through five successive inequalities that the five notions of dimension coincide, thus reproving the classical dimension theorem for projective algebraic subsets :

3.3.1 $d \geq lsup$

Let us assume that there exists coordinates of $\mathbf{P}^n$ such that, with respect to some compatible ordering, for example the upper lexicographic ordering, $E(I)$ does not intersect the plane of the first $e+1$ coordinates of $\mathbf{P}^n$. Then $HF(s)$ is bounded below by the number of monomials of degree s on $e+1$ letters, which is a $O(s^e)$ when s is going to infinity. Hence d is bounded below by $lsup$.

3.3.2 $lsup \geq p$

Let us assume that $Z(I)$ can be projected surjectively on a plane P of dimension p. We can choose coordinates such that this plane is defined by the equations $x_{p+1} = \cdots = x_n = 0$. Then the ideal $I \cap k[x_0, \ldots, x_p]$ reduces to (0).
For if there is a non zero polynomial $f(x_0, \ldots, x_p)$ in I, it does not vanish on the whole plane P and the algebraic subset $Z(I)$ contained in the proper cylinder of equation $f = 0$ cannot be projected on the whole plane P.
Let us look now at $E(I)$ for such coordinates with respect to the upper lexicographic filtration. If a polynomial owns a leading form depending only on the first $p+1$ variables, it has the same property ; hence $E(I)$ does not intersect the plane of the first $p+1$ variables.

3.3.3 $p \geq s$

From the definition of s, there exists a linear subvariety L of codimension $s+1$ not intersecting $Z(I)$. On the other hand it is always possible to choose a linear subvariety B of dimension s avoiding L. The projection of center L sends $Z(I)$ surjectively on B since s is minimal ; for if b is a point of B, the linear subvariety generated with L is of codimension s, hence intersects $Z(I)$ in at least one point with image b.

3.3.4 $s \geq linf$

From the definition of s, there exists a linear subvariety L of codimension $s+1$ avoiding $Z(I)$. We can choose coordinates such that L is defined by the equations $x_0 = \cdots = x_s = 0$. The ideal $J = I + (x_0, \ldots, x_s)$ defines the empty subvariety, therefore contains a power of the ideal $(x_0, \ldots, x_n)$, according to the Nullstellensatz. For any choice of the ordering, $E(J)$ intersects all coordinate axes. From now on let us consider only the lower lexicographic filtration, and look at a polynomial whose leading monomial lies in one of the axes $x_{s+1}, \ldots, x_n$. This last polynomial is then equivalent to some polynomial g of I modulo $(x_0, \ldots, x_s)$, which cannot be zero, and whose leading monomial is equal the one of f. Hence the section of $E(I)$ by the plane of the last $n-s$ coordinates has points on all axes.

3.3.5 $linf \geq d$

Let us assume there are coordinates of $\mathbf{P}^n$ such that, with respect to some compatible ordering, for example the lower lexicographic one, $E(I)$ intersects the last $n - linf$ axes. In degree u large enough, the complementary of $E(I)$ contains only monomials with last $n - linf$ components bounded above by some fixed integer, hence a fixed integer times the number of monomials of degree u on $linf + 1$ letters. So the Hilbert function $HF(u)$ is bounded above by $O(u^{linf})$ when u goes to infinity.

3.4 Note added in proof

Given a stable subset E of $\mathbf{N}^{n+1}$, following several authors [CF], [KW] let us consider independant variables for E, i.e. such that E does not contain an element in just those variables. Call

$m(E)$ the cardinality of a maximal set of such independant variables.

Actually we prove in 3.3.1 that the dimension of the complementary of E is greater or equal to the cardinality of every set of independant variables minus one, hence to $m(E)-1$. On the other hand, it is easy to prove by double induction on r and n that this dimension is smaller or equal to $m(E)-1$. The assertion is clear for $m=0$ and trivial for $n=0$. Then going back to the proof of 2.4, let us remark that if every r-plane of coordinates contains a point of E, every r-plane of coordinates of $\mathbf{N}^n$ contains a point of any section E_i, and every $(r-1)$-plane of coordinates of $\mathbf{N}^n$ contains a point of the section at infinity E_e. Hence the degree of the Hilbert polynomial of E is smaller or equal to r using the induction hypotheses.

Hence we reproved a result of G. CARRÀ FERRO [CF], see also [KW]. Remark that this assertion is independant of the ordering chosen.

4 COMPLEXITY OF COMPUTATION OF THE DIMENSION

4.1 Measure of the complexity of the input data

An algebraic projective set $Z = Z(I)$ is defined by some homogeneous ideal I of a polynomial algebra $k[x_0, \ldots, x_n]$, where k is an algebraically closed field. The ideal I is given by generators, as usual. So the complexity of the input data should include their number t and their maximal degree d. So the number $\binom{d+n}{n}$ of monomials of degree d over $n+1$ letters occurs naturally, through the space required to store one input polynomial with the dense representation. Asymptotically this is $O(d^n)$ if d goes to infinity with fixed n.

If the nature of the ground field k is not specified, we shall denote below by *elementary time complexity* the number of elementary operations in k (additions, multiplications, comparisons, each counting for one) needed to perform an algorithm. Furthermore, if we want to consider the cost of each of these elementary operations, we shall speak of the *total time complexity.* For example if the generators are defined over the integers, we need their size or maximal number of bits M needed to write any coefficient.

We will now successively study the time complexity of the naive algorithms computing the Hilbert dimension, show that they all lead to a disastrous lower bound for the worst case complexity, study the complexity of the naive geometric approach, which is not bad but not the best, and introduce a new algorithm based on a truncation idea with subexponential complexity. Actually its time complexity is bounded above by a polynomial in td^{n^2}.

Furthermore, if the input generators are defined over the integers the space complexity is bounded above by a polynomial in Mtd^{n^2}. So even if we keep track of the growth of intermediate computations, at the ultimate level of manipulations of bits the time complexity stays definitely polynomial in Mtd^{n^2}.

4.2 Calculability of the Hilbert dimension

The principle of the computation of the Hilbert function, once a standard basis is known follows easily from 1.10, and goes back at least to MACAULAY [MA]. A key point is now to construct a standard basis of I from a given set of generators : the first algorithms are due to BUCHBERGER [BU*], see also [GA], [GI], [LA4]. Actually in the homogeneous case we are concerned by, the computation of $HF(s)$ (as well as the construction of such a basis in degree s) is reduced to a pure linear algebra process, i.e. a triangulation by column operations (see also [LA4] [GI]).

It still remains to determine the Hilbert polynomial by interpolation, and this is possible through the upper bound of the regularity given in 2.4 ; and indeed upper bounds of $D(E(I))$ are known in terms of the input data, at least in some particular case [GI]. Anyway it is shown in [GI] that the regularity is bounded below by the maximal degree needed to compute the syzygy modules occuring in a free resolution of the quotient ring R/I. But the study of the pathological examples of MAYR-MEYER yields a double exponential behaviour for this number ([D], [GL]).

The method proposed by G. CARRÀ FERRO presents the same drawback. The worst case complexity of any algorithm computing the dimension based on the construction of a whole standard basis is necessarily catastrophic, since MAYR-MEYER [MM] showed that the space required to obtain such a basis can be exponential in the input data.

4.3 Generic coordinates

We observe now that $linf$ (resp. $lsup$) (3.2) is reached for generic coordinates. To give a precise meaning to this assertion, we must first as usual define a parameter space. Coordinates of the projective space are determined by a simplex configuration of $n+1$ linearly independent hyperplanes $\check{h}_0, \ldots, \check{h}_n$ (elements of $\check{\mathbf{P}}^n$) and $n+1$ linearly independent points $h_0, \ldots, h_n$ (elements of $\mathbf{P}^n$) ; the equation of $\check{h}_i$ is $x_i = 0$, and the point h_i has all coordinates zero except the i^{th} one. The parameter space is then the non empty Zariski open subset $\check{\Omega}$ (resp. Ω), complement of the determinant hypersurface in $(\check{\mathbf{P}}^n)^{n+1}$ (resp. in $(\mathbf{P}^n)^{n+1}$).

4.3.1 Definition

Let $Z(I)$ be an algebraic subset of dimension l. We shall denote by U the non empty Zariski open subset of the Grassmanian $G(n-l-1, n)$ of all linear subvarieties of codimension $l+1$, which do not intersect $Z(I)$.

A coordinate system x of the projective space, such that the linear subvariety defined by $x_0 = \cdots = x_l = 0$ belongs to U is called *generic* for this algebraic subset.

4.3.2 Proposition

The subset of coordinates systems where $linf_x(I)$ (resp. $lsup_x(I)$) reaches its minimum $linf(I)$ (resp. its maximum $lsup(I)$) contains the following non empty Zariski open subset of $\check{\Omega}$ (resp. Ω) :

$$\check{\Gamma} = \{(\check{h}_0, \ldots, \check{h}_n) \in (\check{\mathbf{P}}^n)^{n+1} \mid \check{h}_0 \cap \ldots \cap \check{h}_l \in U\} \cap \check{\Omega}$$

(*resp.* :

$$\Gamma = \{(h_0, \ldots, h_n) \in (\mathbf{P}^n)^{n+1} \mid < h_{l+1}, \ldots, h_n > \in U\} \cap \Omega)$$

Proof : let $(\check{h}_0, \ldots, \check{h}_n)$ be a point of $\check{\Gamma}$ (resp. $(h_0, \ldots, h_n)$) defining a system x of coordinates. For this choice let us consider the subset $E_x(I)$ for the lower (resp. upper) lexicographic filtration. The linear subvariety L defined by $x_0 = \cdots = x_l = 0$ does not intersect $Z(I)$. Hence $linf_x(I)$, being at most l (take the proof of 3.3.4), is equal to l. On the other hand, $Z(I)$ can be projected surjectively on the linear subvariety B generated by the points $h_0, \ldots, h_l$ from the center L (take the proof of 3.3.3), thus $lsup_x(I)$ being at least l (take the proof of 3.3.2) is equal to l.

4.3.3 Remark

So the competition is open between two approaches : computing the dimension through $linf$ involves the construction of a standard basis with respect to the lower lexicographic filtration, which is known to have a better complexity behaviour as the upper lexicographic one. Unfortunately it is difficult to characterize $\check{\Gamma}$, since one needs to recognize successive parameters for a ring ..., which are precisely defined through dimension !

On the other hand, we can easily find a point in Γ if we know how to find a point outside of a hypersurface. We describe below an algorithm leading to a generic system of $n+1$ points, i.e. such that the first $n-l$ generate a linear subvariety of codimension $l+1$, which does not intersect $Z(I)$.

4.3.4 An algorithm to find generic coordinates for the upper lexicographic filtration

Input data : a list I of polynomials. Output data : a list of points.

```
PROJ_GENERIC(I) := PROJ_GENERIC2(I NIL)

PROJ_GENERIC2(I l) :=
          IF I = (0)
          THEN l
          ELSE (h H) : EXTERIOR(I)
               PROJ_GENERIC2(PROJECT(I (h H))
                        CONS(h l))
```

```
PROJECT(I (h H))
```

performs first the change of basis sending the point h on the point $(0, \ldots, 0, 0, 1)$ and the hyperplane H on the hyperplane $x_n = 0$. Then it gives an ideal defining the projection of $Z(I)$ from $(0, \ldots, 0, 0, 1)$ on the hyperplane $x_n = 0$ using 1.12 and any algorithm of construction mentioned in 4.2.

```
EXTERIOR(I)
```

gives a point outside of $Z(I)$ and a hyperplane not passing through this point. It is of course enough to pick up among the generators of I an element, say P, for instance of minimal degree, say δ, and to find a point which is not a zero of this polynomial (function `OUTSIDE(P)`).

Even if we show that the complexity of this algorithm is low (actually polynomial in δ^n as proved in the next section), the result will be uncertain, since the algorithm will be applied to equations of successive projections, whose degree have to be controlled. This will be done in a forthcoming paper.

4.3.5 Proposition : complexity to find a point outside of a hypersurface

Let P be a polynomial of degree δ. The elementary time complexity to find a point on which the polynomial does not vanish is polynomial in δ^n. Furthermore if the input polynomial has integral coefficients of maximal size M, the time complexity is polynomial in $M\delta^n$.

First the polynomial P cannot vanish on the $(\delta+1)^n$ following points : $x_0 = 1$ and $0 \leq x_i \leq \delta$ for $i = 1, \ldots, n$, because if so, it is identically zero. This fact is easily obtained by induction on n : it is trivial for $n = 1$, let us assume it is known for homogeneous polynomials of degree at most δ. If P is the polynomial $\sum_{i=0}^{\delta} P_i(x_0, \ldots, x_{n-1})x_n^i$ which vanishes on the $(\delta+1)^n$ given points, this means that for every point of $\mathbf{P}^{n-1}$ among the $(\delta+1)^{n-1}$ following ones : $x_0 = 1$, $0 \leq x_i \leq \delta$ for $i = 1, \ldots, n-1$, the univariate polynomial P in x_n is identically zero, hence the P_i's vanish, and are identically zero using the induction hypothesis.

Second there are at most $\begin{pmatrix} \delta+n \\ n \end{pmatrix}$ monomials in P, and to evaluate a monomial at a given point one needs at most δ multiplications in k.

Thus if we denote by ϵ, α and μ upper bounds for the cost of respectively comparison to zero, addition and multiplication, the time complexity is at most : $(\delta+1)^n(\epsilon + \begin{pmatrix} \delta+n \\ n \end{pmatrix}(\alpha + d\mu))$
Then the number of elementary operations in the base field is obtained for the uniform cost measure ($\epsilon = \alpha = \mu = 1$) and is bounded above by some polynomial in δ whose leading term is $\frac{1}{n!}\delta^{2n+1}$, anyway a rough upper bound will be

$$\frac{1}{n!}(\delta+n)^{2n+1}.$$

Eventually if I is defined over the integers, the value of P at any previous testing point is at most $2^M \begin{pmatrix} \delta+n \\ n \end{pmatrix} \delta^\delta$, hence its size is at most $M + \delta log(\delta) + log(\delta+n) + \cdots + log(\delta+1)$, itself less than say $M + (\delta+n)^2$.
Hence the cost ϵ of comparison to zero is at most $C_\epsilon M(\delta+n)^2$ where C_ϵ is some constant. The cost α of adding two monomials (resp. μ to obtain a monomial by successive multiplications) is at most $C_\alpha M\delta^2$ (resp. $C_\mu M\delta^2$) where C_α and C_μ are some constants. So finally the time complexity, whatever it is, will be at most $CM\frac{1}{n!}(\delta+n)^{3n+3}$, where C is some constant.

In conclusion, for fixed n, if δ is going to infinity the asymptotic behaviour of the time complexity is polynomial in δ^n.

We will now try to catch the dimension through $linf$.

4.4 Queen's side openings

The fundamental observation is now that degrees of elements, when constructing a standard basis with respect to the lower lexicographic filtration, grow slowly along some coordinate axes.

4.4.1 Proposition

Consider the set $E(I)$ relative to the lower lexicographic filtration ; by definition, there are points $A_{linf_x-1}, \ldots, A_n$ of $E(I)$ lying on the last $n - linf_x$ axes. Then :

$$| A_i | \leq (n - i + 1)(d - 1) + 1$$

for $linf_x + 1 \leq i \leq n$.

Proof : Let i be some integer between $linf_x + 1$ and n. The ideal $I + (x_0, \ldots, x_{i-1})$ defines the empty subvariety and is still generated by polynomials of degree at most d. By proposition 1.11, we are reduced to the particular case of $linf_x = -1$ and $i = 0$. For such an ideal, the degrees of elements of a standard basis relative to the lower lexicographic filtration are at most $1 + (n + 1)(d - 1)$. To show this it is easy to adapt the proof of Theorem 3.9 [GI] to the case of non generic coordinates and arbitrary characteristic in the following lemma :

Lemma : let I be an ideal generated by polynomials $f_1, \ldots, f_t$ of degree $d_1 \geq \ldots \geq d_t$ defining the empty subvariety. Then $D(E(I))$ is at most $1 + \sum_{i=1}^{n+1}(d_i - 1)$.

Proof: the first step consists to use 2.6 to replace $D(E(I))$ by the regularity $H(I)$, which is an upper bound. Then by generic combinations, we can extract a regular sequence of maximal length $n+1$ from I, whose elements are of degree $d_1 \geq \ldots \geq d_{n+1}$, and generate an ideal J contained in I. From the canonical exact sequence $R/J \to R/I \to 0$ we deduce that the regularity of I is at most the regularity of J. The resolution of R/J by the Koszul complex shows that the Hilbert function of R/J, hence its regularity, depends only on the degrees $d_1, \ldots, d_{n+1}$ of the generators of J. This regularity can now be easily computed in the special case $I = (x_0^{d_1}, \ldots, x_n^{d_{n+1}})$ (cf. 2.5).

4.5 A first rough estimate to compute the lower lexicographic dimension

What is the complexity to catch lower lexicographic dimension ? Due to lack of knowledge about genericity, we have to compute by brute force : we can perform a generic change of coordinates, by introducing $(n + 1)^2$ new indeterminates a_{ij}, generic entries of a change of basis matrix. The new base field is then $K = k(a_{ij})$, and the first coordinate hyperplanes form a system of parameters.

Now it is enough by 4.4.1 to construct $E(I)$ in degree less than $(n + 1)d$. So we remain inside the vector space of monomials of degree at most $(n + 1)d$, whose dimension $\delta(d, n)$ is anyway roughly bounded by some polynomial in $(nd)^n$. To compute the standard basis we have at most to triangulate by column operations a $\delta \times t\delta$ matrix ([LA4] [GI]), with entries polynomials in the a_{ij}'s of degree at most d. The cost in basic operations in the new field K is anyway at most polynomial in $(ntd)^n$.

And during this triangulation, the polynomial entries appearing being minors of the initial matrix, have a degree at most $d\delta$. At any step of the triangulation, the multiplication or addition of two entries needs a number of operations in the base field k which is polynomial in $(ntd)^{n^3}$.

Hence the elementary time complexity is of same nature.

Space questions, if the input polynomials have integral coefficients of size at most M : the size of any minor does not exceed a polynomial in $(Mtnd)^n$, so eventually the time complexity is still polynomial in $(Mtnd)^{n^3}$.

Finally remark that this procedure is essentially LAZARD's one ([LA1] algorithm 7.2), translated in the language of standard bases.

4.5.1 Remark : an interesting special case

The fact that the dimension is negative can be decided in a time which is polynomial in $(Mtnd)^n$, since in this case the complement of $E(I)$ is finite and inside a cube of side less than $(n+1)d$.

4.6 A last algorithm, computing simultaneously generic coordinates and dimension

4.6.1 The algorithm

To describe it more comfortably, the algorithm is written with functions having as input and output data 4-uples of the same following type :

- An integer i between 0 and $n+1$,
- A field K which is either k or an extension $k(\lambda_0, \ldots, \lambda_{n-i-1})$ over $n-i$ indeterminates.
- A system x of coordinates $x = (x_0, \ldots, x_n)$ of the projective space,
- A list J of polynomials in the variables $x_0, \ldots, x_n$ with coefficients in the field K. When K is an extension of k, the coefficients of the polynomials of J are actually in $k[\lambda_0, \ldots, \lambda_{n-i-1}]$.

```
GENERIC(i, K, x, J) :=
   IF i=n+1
      THEN (i, K, x, J)
      ELSE (i, K, x, J) : STANDARD(i, K, x, J)
           IF AXIS (i, K, x, J)
              THEN GENERIC (i+1, K, x, J)
              ELSE (i, K, x, J) : STANDARD(CHANGE(i, K, x, J))
                   A : AXIS(i, K, x, J)
                   (i, K, x, J) : SPECIALIZE(A, (i, K, x, J))
                   IF A
                      THEN GENERIC(i+1, K, x, J)
                      ELSE (i, K, x, J)
```

`STANDARD(i, K, x, J)` does not change the 3 first components, but replaces the elements of the last one, of degree at most $(i+1)(d-1)+1$, by the list of elements of a standard basis of the ideal generated by J, with respect to the lower lexicographic filtration, up to the same degree. Moreover if the field K is a non trivial extension of the ground field, the triangulation leading to the standard basis is done in an integral way, without introducing any denominators in the coefficients elements of K.

`AXIS(i, K, x, J)` does not change the 3 first components, but replaces the last one by the element of J (if any) with leading monomial depending only on the variable $n-i$.

`CHANGE(i, K, x, J)` will only act on 4-uples with a field equal to the ground field k. This function :

- does not change the first component,
- replaces the ground field by the extension $k(\lambda_0, \ldots, \lambda_{n-i-1})$,
- changes the variables in the following way :
$x_j : x_j + \lambda_j x_{n-i}$ for $0 \leq j \leq n-i-1$
$x_j : x_j$ if $j \geq n-i$,
- tranforms every polynomial of J according to the previous change of variables.

`SPECIALIZE((i, K, x, J), (i, K, x, S))` acts only in the case where K is an extension of k over $n-i$ indeterminates, and J contains at most one element. This function acts only on its second argument :

- does not change the first component,
- replaces the extension field K by the ground field k,
- does not change the coordinates,
- specializes every element of S by setting each λ_j's to some constant value a_j element of k. If J is empty, each a_j is choosen to be zero, so that `SPECIALIZE` is the inverse map of `CHANGE` and we go back to the previous coordinates. If not, let us consider the leading coefficient of the unique element of J, which is a polynomial in $\lambda_0, \ldots, \lambda_{n-i-1}$. Applying the function `OUTSIDE` introduced in 4.3.4, we can find a point $a_0, \ldots, a_{n-i-1}$ on which this leading coefficient does not vanish.

4.6.2 Theorem : the result

Starting with the following 4-uple as input data :
- i=0,
- the ground field k,
- x the given system of coordinates,
- a list J of homogeneous polynomials in $k[x_0, \ldots, x_n]$, of degree less than d, generating an ideal I,
the previous algorithm stops on the following 4-uple :
- the codimension $c = n - l$ of $Z(I)$,
- the ground field k,
- a generic system of coordinates y for $Z(I)$ as defined in 4.3.1 (denote by ϕ the change of coordinates such that $x = \phi(y)$),
- a list of homogeneous polynomials in $k[y]$, forming a standard basis of $\phi^*(I)$ truncated in degree less than $(c+1)(d-1)+1$.

In other words, if we denote by $E(J)$ the stable subset generated by the leading monomials of the elements of a list J of polynomials in $k[y_0, \ldots, y_n]$, and define similarly the integer $linf_y(J)$

(cf. 3.2), we claim that $E(J)$ is the truncated part of $E(I)$ in degree less than $(c+1)(d-1)+1$, and that it is enough to read the dimension since $linf_y(I) = linf_y(J) = l$.

Proof : Each time we enter the function `GENERIC`, the 4-uple argument $(i,\ K,\ y,\ J)$ has the following property : for every of the i axes $y_{n-i+1}, \ldots, y_n$, there is among the elements of J a polynomial whose leading monomial lies on it.

We will prove this assertion by induction on i. If i is zero, there is nothing to prove. Let us now follow the history of a 4-uple argument $(i,\ K,\ y,\ J)$. By induction hypothesis, $E(J)$ cuts the last i axes. To check if an element of a standard basis has a leading monomial on the $(n-i)^{th}$ axis, it is enough by 4.4.1 to construct it in degree less than $(i+1)(d-1)+1$. If it is the case, we enter again with an argument satisfying the assertion at level $i+1$.

If not, let us consider the ideal $Igen$ of the new polynomial algebra over an extension field, in the new variables introduced by the function `CHANGE` ; $Z(I)$ and $Z(Igen)$ have the same dimension. Now let us look at the stable sets $E_{lowlex}(I)$ (resp. $E_{lowlex}(Igen)$) and $E_{mixlex}(I)$ (resp. $E_{mixlex}(Igen)$) with respect to the lower and mixed (of order $n-i$) lexicographic filtrations. If there is a point in the truncated part of $E_{lowlex}(Igen)$ on the axis y_{n-i}, the same is true for the suitable specialisation, and we enter again at level $i+1$ satisfied.

If not, there is no point of $E_{mixlex}(I)$ in the plane of the first $n-i+1$ coordinates, because if so, this point would correspond to a non zero polynomial depending only this first variables, which would be pushed by the change of coordinates on the axis y_{n-i} ; but the leading monomial would not change for the other filtration, hence $E_{lowlex}(Igen)$ would have a point on the same axis, and furthermore another one in the truncated part. But in this case, looking at $E_{mixlex}(I)$, we see that the linear subvariety defined by $x_0 = \cdots = x_{n-i} = 0$ does not cut $Z(I)$, hence the dimension is at most $n-i$; and $Z(I)$ can be projected surjectively on the linear subvariety defined by $x_{n-i+1} = \cdots = x_n = 0$, hence the dimension at least $n-i$ is equal to $n-i$. And the algorithm stops with the wanted property.

Remains the case where we go further until i is $n+1$; but this is the other way to get out, and the conclusion is also fullfilled.

4.6.3 Theorem : complexity of the previous algorithm

The elementary time complexity of the previous algorithm is polynomial in $(ntd)^{n^2}$. Furthermore if the input data are defined over the integers, the time complexity is polynomial in $(Mtnd)^{n^2}$.

Once we remarked that the matrices to be triangulated have entries polynomials of at most n variables, of degree at most d, and coefficients of maximal size M, the proof involves the same technics as 4.5, with the additional study of `OUTSIDE` in 4.3.5.

REFERENCES

[BS] D. BAYER, M. STILLMAN, A theorem on refining division orders by the reverse lexicographic order, Lecture notes for the meeting on Algebraic Geometry and Computing, Trento (Italy) (1985).

[BU1] B. BUCHBERGER, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Ph. D. Dissertation, U. Innsbruck, Austria, (1965).

[BU2] B. BUCHBERGER, Ein algorithmisches Kriterium für die Lösbarkeit eines algebraisches Gleichungssystems, Aequationes Math. 4 (1970), 374-383.

[BU3] B. BUCHBERGER, A theoretical basis for the reduction of polynomials to canonical forms, ACM SIGSAM Bull., 39 (1976), 19-29.

[CF] G. CARRÀ FERRO, Some upper bounds for the multiplicity of an autoreduced subset of $\mathbf{N}^m$ and their applications, Proceedings of the third International Conference on Algebraic Algorithms and Error-Correcting Codes, AAECC-3, Grenoble (France) 1985, Lecture Notes in Computer Science 229, Springer (1986), 306-315.

[D] M. DEMAZURE, Notes informelles de calcul formel, prépublications du Centre de Mathématiques de l'Ecole Polytechnique (1985).
3. Le monoïde de Mayr-Meyer.
4. Le théorème de complexité de Mayr-Meyer.

[GA] A. GALLIGO, Algorithmes de construction de bases standard, prépublication de l'Université de Nice (1983).

[GI] M. GIUSTI, Some effectivity problems in polynomial ideal theory, in Eurosam 84, Lecture Notes in Computer Science 174, Springer (1984), 159-171.

[GL] M. GIUSTI, D. LAZARD, Complexity of standard basis computations, related algebraic problems and their common double exponential behaviour. Lecture notes for the Conference "Computer and Commutative Algebra" (Genova, Italy) (1986), Prépublication du Centre de Mathématiques de l'Ecole Polytechnique, (1986)

[GR] H. GRAUERT, Über die Deformationen isolierter Singularitäten analytischer Mengen, Inventiones Math. 15 3 (1972)

[HI] H. HIRONAKA, Resolution of singularities of an algebraic variety over a field of characteristic zero, Ann. Math. 79, (1964) 109-326.

[KR] A. KANDRI-RODY, Proceedings Combinatorial Algorithms in Algebraic Structures, Otzenhaus 1985, J. Avenhaus and K. Madlener eds., Fachbereich Informatik, Universität Kaiserslautern (FRG).

[KW] H. KREDEL, V. WEISPFENNIG, Computing dimension and independent sets for polynomial ideals, these Proceedings.

[LA1] D. LAZARD, Algèbre linéaire sur $K[x_1, \ldots, x_n]$ et élimination, Bull. Soc. Math. France, 105 (1977), 165-190.

[LA2] D. LAZARD, Résolution des systèmes d'équations algébriques, Theoretical Computer Science 15 (1981), 77-110.

[LA3] D. LAZARD, Commutative algebra and computer algebra, Lect. Notes in Comp. Sciences 144 (1982), 40-48.

[LA4] D. LAZARD, Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations, in Eurocal 83, Lecture Notes in Computer Science 162, Springer (1983).

[LJ] M. LEJEUNE-JALABERT, Effectivité des calculs polynomiaux, Cours de DEA 1984-1985, Institut Fourier, Université de Grenoble I.

[MA] F.S. MACAULAY, Some properties of enumeration in the theory of modular systems, Proc. London Math. Soc. 26 (1927), 531-555.

[MM] E. MAYR, A. MEYER, The complexity of the word problem for commutative semigroups and polynomial ideals, Adv. in Maths. 46 (1982), 305-329.