GRÖBNER BASES, GAUSSIAN ELIMINATION AND RESOLUTION OF SYSTEMS OF ALGEBRAIC EQUATIONS

D. Lazard
Mathématiques - Informatique
Université de Poitiers
F 86022 Poitiers Cedex

In the past few years, two very different methods have been developed for solving systems of algebraic equations : the method of Gröbner bases or standard bases [Buc 1, Buc 2, Tri, P.Y] and the one which I presented in Eurosam 79 [Laz 2, Laz 3] based on gaussian elimination in some matrices.

Although they look very different, they are, in fact, very similar, at least if we restrict ourselves to the first step of my method.

On the other hand Gröbner base algorithms are very close to the tangent cone algorithm of Mora [Mor].

All of these algorithms are related to Gaussian elimination.

In the first part of this paper, we try to develop all these relations and to show that this leads to improvements in some of these algorithms.

In the second part we give upper and lower bounds for the degrees of the elements of a Gröbner base. These bounds are based on projective algebraic geometry. The choice of the ordering appears to be critical : lexicographical orderings give Gröbner bases of high degree, while reverse lexicographical orderings lead to low degrees.

I - RESULTANT

To understand the above similarity, it is useful to begin with the simplest case of two univariate polynomials

$$A = a_o+a_1X+\dots+a_mX^m \qquad a_m \neq 0$$

$$B = b_o+b_1X+\dots+b_nX^n \qquad b_n \neq 0$$

Here the standard method for computing Gröbner bases is exactly the Euclidean algorithm for computing GCDs and resultants.

The second way to compute the resultant consists of evaluating the Sylvester determinant

$$\begin{pmatrix} \underbrace{\begin{matrix} a_m & & \\ a_{m-1} & \ddots & a_m \\ \vdots & \ddots & a_{m-1} \\ \vdots & & \vdots \\ a_o & & \vdots \\ & \ddots & a_o \end{matrix}}_{n\ \text{columns}} & \underbrace{\begin{matrix} b_n & & \\ b_{n-1} & \ddots & b_n \\ \vdots & \ddots & b_{n-1} \\ \vdots & & \vdots \\ b_o & & \vdots \\ & \ddots & b_o \end{matrix}}_{m\ \text{columns}} \end{pmatrix}$$

For this purpose, Gaussian elimination seems to have $O((m+n)^3)$ complexity, but a simple modification of it gives $O(mn)$ complexity and an algorithm strictly equivalent to Euclid's one :

The Gaussian method consists of subtracting b_n/a_m times the first column from the (n+1)-th one. If $n \geq m$, the same computations allow us to subtract b_n/a_m times the i-th column from the $(n+i)$-th for $i = 1,\ldots,m$; this operation amounts to replacing the coefficients of B by those of $C:=B-(b_n/a_m)X^{n-m}A$. Thus, the Sylvester determinant of A and B is reduced to a_m times the Sylvester determinant of A and C.

If we iterate this process, we simulate Euclid's algorithm in the reduction of a Sylvester matrix. On the other hand, Euclid's algorithm can be viewed as a way to save memory (and time) in the reduction of a Sylvester matrix.

Some years ago, I asked for such an economical method for elimination theory [Laz 1] ; it appears that Gröbner base computation provides a solution.

II - GRÖBNER BASES AS INFINITE LINEAR BASES

Let $A = K[X_1,\ldots,X_n]$ be a polynomial ring over a field K and $I = (f_1,..f_k)$ an ideal generated by a finite set of polynomials $f_1,\ldots,f_k$. As a K-vector space, I is generated by the mf_i's where $i = 1,\ldots,k$ and m runs through all the monomials $X_1^{a_1}\ldots X_n^{a_n}$. On the base of A consisting of all the monomials, this generating set defines a (infinite) matrix which has the following properties :

1/ The non-zero entries of each column are finite in number and consist of coefficients of one of the f_i's.

2/ Each row has a finite number of non-zero entries : if the row corresponds to some monomial m, then the non-zero entries must correspond to generators $m'f_i$ where m' is a monomial dividing m.

This finiteness property allows one to triangulate the matrix by column operations. This is a finite process for each pivot, which enumerates a base of the vector space I. Although the whole enumeration is not finite, one can give a finite description of a linear base of I ; such a description is provided by Gröbner bases.

For this purpose, we choose any total order on the monomials of A, which is compatible with products (i.e. $m \le n \Rightarrow mp \le np$) and mean by the leading monomial of a polynomial P, the greatest monomial which appears in P with non-zero coefficient ; this we denote lead(P).

It is easy to prove that $f_1, \dots, f_n$ is a Gröbner base for the ideal I if and only if the following set of polynomials is a base of the vector space I :

$$\{mf_i \ ; \ 1 \le i \le k, \ m \ \text{monomial}, \ \text{lead}(mf_i) \ \text{not multiple of} \ \text{lead}(f_j) \ \text{for} \ j<i\}$$

There are three classical orderings which are used for computing Gröbner bases : the purely lexicographical ordering

$$1<x<x^2<x^3<\dots<y<xy<x^2y<\dots<y^2<xy^2<\dots,$$

the total degree ordering

$$1<x<y<x^2<xy<y^2<x^3<x^2y<\dots$$

which satisfies $m \le n \Rightarrow \text{degre}(m) \le \text{degre}(n)$,

the reverse degree ordering

$$1>x>y>x^2>xy>y^2>x^3>x^2y>\dots$$

which satisfies $m \ge n \Rightarrow \text{degre}(m) \le \text{degre}(n)$.

The first two are well-orderings and often used. The last one is useful when dealing with formal power series or local singularities [Mor].

For the latter, the termination criterion is not easy (see [Mor]), but it is the only one for which Gröbner base computation and Gaussian elimination are related exactly as in section I : for example, in the univariate case, the Sylvester matrix becomes the infinite matrix

$$\left|\begin{array}{ccccc}
a_0 & 0 \cdots\cdots & 0 \cdots\cdots & b_0 \cdots & 0 \cdots\cdots \\
\ddots & a_0 \ddots & \vdots & \vdots & b_0 \ddots \\
a_1 \ddots & & 0 & \vdots & \\
& a_1 \ddots & a_0 \ddots & & \vdots \\
\vdots & & & b_n \ddots & \vdots \\
\vdots & \vdots & a_1 \ddots & 0 \ddots & b_n \ddots \\
a_m \ddots & & & \vdots & 0 \ddots \\
& a_m \ddots & & \vdots & \vdots \\
0 & 0 & a_m \ddots & \vdots & \vdots \\
0 & \vdots & \vdots & \vdots & \vdots \\
0 & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots
\end{array}\right|$$

In the two first cases however, the ordering on monomials is not compatible with any numbering of the rows of the above infinite matrix. It follows that our analogy between Gaussian elimination and Gröbner base computation does not work any longer unless we restrict the computations to finite submatrices. We shall do this in the following section.

III - HOMOGENEIZATION

In the rest of the paper, we shall study homogeneous polynomials. This is not really a restriction because every polynomial can be made homogeneous by adding a new variable :

$$x^2+y^2+2x+1 \rightarrow x^2+y^2+2xt+t^2 \quad ,$$

the computations can be done on homogeneous polynomials and the desired inhomogeneous result can be retrieved by setting the new variable to 1.

Homogeneous polynomials are as useful as projective geometry. For our purposes, the advantages are :

a/ high degree intermediate computations are not cancelled in the result ;

b/ the infinite matrix of the preceding section will appear as a direct sum of finite matrices ; thus with an appropriate order on the rows corresponding to a given degree the analogy between Gaussian elimination and a Gröbner base algorithm can be pursued ;

c/ in the homogeneous case each degree appears as a separate domain and we never need to compare monomials of different degrees ; we only need total orderings on the monomials of each total degree which are compatible with respect to multiplication, i.e. $m < m' \Rightarrow mm'' < m'm''$; the ineqality $m < mm'$, which is generally required in Gröbner base algorithms, is no longer necessary.

If t is the homogeneizing variable, the first and third orderings of the last section become lexicographical orderings in each degree, with respective orders

$$t < x < y$$

$$\text{or} \quad y < x < t$$

on the variables. On the other hand, the second one becomes the reverse lexicographical ordering relative to

$$t < x < y$$

The reverse lexicographical ordering is the ordering on exponents such that $(a_1,\ldots,a_n) < (b_1,\ldots,b_n) \Longleftrightarrow \exists k,\ a_k > b_k$ and $a_i = b_i$ for $i > k$.

These remarks have many computational implications :

A/ Computation of the tangent cones

The first and third orderings become isomorphic. It follows that the analogy between Mora's algorithm for the tangent cone and Buchberger's one for Gröbner bases may be pursued much further than is asserted in [Mor] : every algorithm for a Gröbner base can be used for the tangent cone when working with homogeneized polynomials. Some experimentation is needed to decide if this remark actually improves Mora's algorithm.

B/ Resolution of algebraic systems

The characterization of Gröbner bases of the last section may be used to make the following.

Définition. *Let* I *be an ideal generated by homogeneous polynomials, and* I^d *the set of homogeneous polynomials in* I *which are of degree* d. *A set* $F = (f_1,\dots,f_k)$ *of homogeneous polynomials is called a* Gröbner base of I for degree d *or* Gröbner base of I^d *if*

$\{mf_i,$ m monomial, $i \in \{1,\dots k\}$, lead(mf_i) not a multiple of lead(f_j) for $j < i$, degree(mf_i) = d$\}$.

is a linear base for I^d.

The two following facts are straightforward.

1/ F is a Gröbner base if and only if it is a Gröbner base in every degree.

2/ Every algorithm which computes Gröbner bases yields an algorithm which computes Gröbner bases in degree d by cancelling all computations in degrees greater than d.

In view of theses remarks the first step of the algorithm of [Laz 2, Laz 3] (called "Réduction de la matrice ϕ" or "Reduction of the numerical part") may be modified as follows.

(R1) Compute a Gröbner base in degree DD for the ideal generated by the input polynomials (after homogeneization). Let $(F_1,\dots,F_k)$ be the result.

(R2) Let NL be the number of monomials of degree DD and M be the matrix with NL rows, whose columns are the coefficients of the polynomials mF_i, $i=1,\dots,k$, such that m is a monomial, mF_i is of degree DD, lead(mF_i) is not a multiple of lead(F_j) for $j < i$. The matrix MM [Laz 2] or CC [Laz 3] is the matrix of relations between the rows of the (triangular) matrix M.

This modification shows the relationship between my algorithm which uses Gaussian reduction and Gröbner base algorithms. Some experimentation is needed to decide which method is the best.

C/ The choice of the ordering on monomial has many repercussions on the complexity of the computation of a Gröbner base :

With the lexicographical ordering, the element of the Gröbner base with minimal leading term depends on a small number of variables (at most one plus the dimension of the variety of the ideal) and has a high degree (in general the degree of the variety of the ideal which is essentially the product of the degrees of the generators of the ideal).

On the other hand, with a reverse lexicographical ordering, the element of the Gröbner base with minimal leading term depends on many variables and has small degrees except in the last variable.

IV - BOUNDS ON DEGREE

It is clear that the complexity of Gröbner base algorithms depends on the degrees of the elements of the Gröbner base.

The above remark shows that these degrees depend strongly on the choice of ordering, the extreme cases being lexicographical and reverse lexicographical orderings. These collapse for homogeneous polynomials in two variables.

Some notation is required : let I be the ideal of $K[X_1,\dots,X_n]$ generated by $(f_1,\dots,f_k)$, $\tilde{I}$ the homogeneous ideal of $K[X_o,\dots,X_n]$ generated by the homogeneized polynomials $\tilde{f}_1,\dots,\tilde{f}_k$ where $\tilde{f}_i$ is the homogeneized polynomial corresponding to f_i, i.e. $\tilde{f}_i = X_o^{d_i} f_i(\frac{X_1}{X_o},\dots,\frac{X_n}{X_o})$ with d_i = degree(f_i).

We call $\dim(I) \le \mathrm{Dim}(\tilde{I})$ the dimension of the algebraic set V (resp. $\tilde{V}$) of common zeros of the f_i's in an algebraic closure of K (resp. of the common projective zeros of the $\tilde{f}_i$'s). It is the maximum of the i's such that *most* linear varieties of dimension $n-i-1$ do not intersect the algebraic set : here and in the following *most* or *in general* will mean always except on a Zariski closed set. The degrees $\deg(I) \le \mathrm{Deg}(\tilde{I})$ are the number of points (with multiplicities) of intersection of this algebraic set with a linear variety of dimension $n-i$ in *general* position. The inequalities between $\deg(I)$ and $\mathrm{Deg}(\tilde{I})$ or $\dim(I)$ and $\mathrm{Dim}(\tilde{I})$ come from what happens at infinity ; *in general* they are equalities.

Finally, let $d_1,\dots,d_k$ be the degrees of the f_i and choose the numbering so that $d_1 \ge d_2 \ge \dots$

Proposition 1.(Bezout's theorem) *If* $r = \dim(I)$ (*resp.* $\mathrm{Dim}(\tilde{I})$) *we have* $\deg(I) \le d_1 d_2 \dots d_{n-r}$ (*resp.* $\mathrm{Deg}(\tilde{I}) \le d_1 d_2 \dots d_{n-r}$). *Equalities hold when* $k = n-r$ *(in* general *for* $\deg(I)$ *and always for* $\mathrm{Deg}(\tilde{I})$).

Proposition 2. *The projection of the algebraic set* V (*resp.* $\tilde{V}$) *of dimension* r *into a linear variety of dimension* $r+1$ *is, in* general*, a hypersurface of degree* $\deg(I)$ (*resp.* $\deg(\tilde{I})$).

Corollary 1. *After* most *linear changes of variable the ideal* I (*resp.* $\tilde{I}$) *contains a polynomial of degree* $\deg(I)$ (*resp.* $\mathrm{Deg}(\tilde{I})$) *depending only on* $X_{n-r}, X_{n-r+1},\dots,X_n$ *where* $r = \dim(I)$ (*resp.* $\mathrm{Dim}(\tilde{I})$) *and does not contain polynomials of degree less than* $\deg(I)$ (*resp.* $\mathrm{Deg}(\tilde{I})$) *in theses variables.*

Proof. Project into the linear variety with equations $(X_o=)X_1=\ldots=X_{n-r-1}=0$. The polynomial is the equation of the hypersurface of proposition 2.

Theorem 1. *Let* I *be an ideal of* $K[X_1,\ldots,X_n]$ *generated by polynomials* $f_1,\ldots,f_k$ *of degrees* $d_1,\ldots,d_k$ $(k\le n)$. *In* most *cases, every Gröbner base for the lexicographical ordering or for the third ordering of section* II *contains a polynomial with degree* $d_1d_2\ldots d_k$.

This is an immediate consequence of the preceeding considerations. It would be useful to prove that every element of a reduced minimal Gröbner base has a degree less than or equal to this bound. This can be done in the case where $\dim(I)=0$ with the method of [Buc 3].

V - BOUNDS ON THE DEGREE. REVERSE LEXICOGRAPHICAL ORDERING

In the preceeding section we have seen that lexicographical orderings lead to Gröbner bases of high degree. Here we show that reverse lexicographical orderings lead to better bounds. We shall work only in the homogeneous case, even if the results apply in the non homogeneous case. Thus let I be an ideal of $K[X_o,\ldots,X_n]$ (K a field) generated by homogeneous polynomials $f_1,\ldots,f_k$ with degrees $d_1,\ldots,d_k$ such that $d_1\ge d_2\ldots\ge d_k$.

We set $A:=K[X_o,\ldots,X_n]/I$ and denote by A^d the set of elements of A which are classes of homogeneous polynomials of degree d.

We shall use freely facts from commutative algebra which can be deduced an exercices from [Kap] (for example). See also [Laz 3, Laz 4].

Lemma 1. *There exists an integer* i_o *such that* $\mathrm{ann}(x)\cap A^i=0$ *for* $i\ge i_o$ *and for* most *elements* x *of* A^1 (here $\mathrm{ann}(x)=\{y\in A\ ;\ xy=0\}$).*If* $k\le n$ *then* $i_o=0$.

Conjecture 1. *If* $k>n$ *we can take* $i_o=d_1+\ldots+d_{n+1}-n$.

Proposition 3. *If* $\mathrm{Dim}(I)\le 0$ *or* $n\le 2$, *the above conjecture is true.*

The first assertion is a part of [Laz 3, th. 3.3] ; the case $n=2$ follows from the fact that if $g=\mathrm{GCD}(f_1,\ldots,f_k)$, the ideal J generated by the f_i/g's satisfies $\mathrm{Dim}(J)\le 0$.

Define depth(A) recursively by 0 if there is no $x\in A^1$ such that $\mathrm{ann}(x)=0$, or 1+depth(A/xA) if $x\in A^1$ and $\mathrm{ann}(x)=0$. If $\mathrm{depth}(A)=\mathrm{Dim}(I)+1$, the ring A is Cohen-Macaulay (this may be a definition) ; if $k\le n$, then $\mathrm{depth}(A)\ge 1+n-k$.

We are now able to state our main result.

Theorem 2. *Suppose one of the following conditions holds :*

i) *Conjecture* 1 *is true ;*

ii) $\mathrm{depth}(A) \geq \mathrm{Dim}(I)$;

iii) $\mathrm{depth}(A) \geq n-2$

iv) $\mathrm{Dim}(I) \leq 0$

v) $n \leq 2$ *(*$n+1$ *is the number of homogeneous variables).*

Then, after most *linear changes of variable, the elements of any minimal reduced Gröbner base for the reverse lexicographical ordering have degree at most* $d_1+\ldots+d_{r+1}-r$ *where* $r = n-\mathrm{depth}(A)$ *(We have always* $r < k$*, the number of polynomials).*

We need the following lemma.

Lemma 2. *With the same hypothesis, after* most *linear changes of variable, if* $y_o,\ldots,y_n$ *are the new variables and* $s = \mathrm{Dim}(I)$*, then*

a/ every monomial of degree $d_1+\ldots+d_{r+1}-r$ *is congruent modulo* I *to an element of* $y_{n-s}A+y_{n-s+1}A+\ldots+y_nA$.

b/ If z *is a homogeneous polynomial of degree* $d > d_1+\ldots+d_{r+1}-r$ *such that* $z \in I \cap (y_{n-s}A+\ldots+y_nA)$ *then* $z \in y_{n-s}I+\ldots+y_nI$.

Proof of the theorem from the lemma : let $D = d_1+\ldots+d_{r+1}-r$; any monomial m of degree D not depending on $y_{n-s},\ldots,y_n$ satisfies a relation $G_m := m - \sum_{i=n-s}^{n} y_i g_i \in I$ and is the leading term of this element of I (recall that the reverse lexicographical order is defined by

$$y_o^{a_o}\ldots y_n^{a_n} < y_o^{b_o}\ldots y_n^{b_n} \quad \text{iff} \quad \exists i \quad a_i > b_i,\ a_{i+1} = b_{i+1},\ldots,a_n = b_n)$$

Let G a Gröbner base and G' the set of polynomials of G which are of degree at most D ; we shall prove that G' is also a Gröbner base : let $g \in I$ be a homogeneous polynomial of degree $d \geq D$; if its leading term does not depend on $y_{n-s},\ldots,y_n$, it is a multiple of the leading term of some G_m and thus of the leading term of some element of G'. If $g \in y_{n-s}A+\ldots+y_nA$, its leading term is a multiple of the leading term of some element of I of degree $d-1$ (assertion b/) ; and an induction shows that in all cases, the leading terms of elements of I are multiples of the leading terms of elements of G' ; this fact implies that G' is a Gröbner base.

Proof of the lemma :

1/ If $\mathrm{Dim}(I) \leq 0$: this is proved in [Laz 3, th. 3.3 and p. 106].

2/ If $n \leq 2$: dividing by the GCD of the generators of I we get an ideal J s.t. $\mathrm{Dim}(J) = 0$; applying the lemma to J and multiplying by the GCD, gives the result.

3/ If $\mathrm{depth}(A) > 0$, after *most* linear changes of variable, y_n is such that $\mathrm{ann}(y_n) = 0$. Let $\overline{A} = A/y_nA$. We have the exact sequence

$$0 \to A^{d-1} \xrightarrow{y_n} A^d \to \bar{A}^d \to 0$$

where $\xrightarrow{y_n}$ is multiplication by y_n. Some elementary diagram chasing permits us to deduce the lemma for A from the lemma for $\bar{A}$ and this proves ii) and iii) from iv) and v).

4/ If $\operatorname{depth}(A) = 0$ and conjecture 1 is true : the same argument as above works because we do not need the injectivity of $\xrightarrow{y_n}$ for $d \le d_1+\dots+d_{n+1}-n$.

Conjecture 2. *The conclusion of the theorem 2 is true even if conjecture 1 is not true.*

Conjecture 3. *The conclusion of the theorem 2 is true for all linear changes of variable i.e. without any change of variable.*

Remarks.

1/ We have not really used the particular ordering we have choosen, but only the following two conditions :

$$m < m' \Rightarrow mm'' < m'm''$$

every monomial not containing $y_{n-s},\dots,y_n$

is greather than every monomial containing some of these variables.

2/ The results apply to the non homogeneous case if the hyperplane at infinity is in a *general* position, and this gives not only bounds on the degrees of Gröbner bases, but also on the degrees of their expressions as linear combinations of the f_i.

3/ Our bounds are the best possible : take $f_1 = X_1^{d_1}$ and, for $i>1$, $f_i = X_{i-1}X_i^{d_i-1} + X_i^{d_i}$.

We conclude with a result which does not need any reference to "general position".

Theorem 3. *Let* I *be a (not necessarily homogeneous) ideal in* $K[X_1,\dots,X_n]$ *generated by* $f_1,\dots,f_k$ *of degrees* $d_1,\dots,d_k$ *s.t.* $d_1 \ge d_2 \dots \ge d_k$. *Choose any ordering on the monomials such that* $m \le m' \Rightarrow (mm'' \le m'm''$ *and* $\operatorname{degree}(m) \le \deg(m'))$. *Suppose one of the following conditions holds :*

i) $n \le 2$;

ii) $\operatorname{Dim}(\tilde{I}) \le 0$ *where* $\tilde{I}$ *is the ideal generated by the* $\tilde{f}_i$*'s homogeneized from the* f_i*'s.*

Then the polynomials of every minimal reduced Gröbner base have degrees at most $d_1+\dots+d_{n+1}-n+1$ *with* $d_{n+1} = 1$ *if* $k = n$.

Proof. As above, dividing the f_i' by their GCD reduces case i) to case ii). Let $\tilde{A} := K[X_o,\dots,X_n]/\tilde{I}$ and $\tilde{A}^d$ be its homogeneous part of degree d ; the results of [Laz 3, p. 106] prove that there exists $\tilde{y} \in \tilde{A}^1$ s.t. the multiplication $\tilde{A}^{d-1} \xrightarrow{\tilde{y}} \tilde{A}^d$ is surjective for $d \ge d_1+\dots+d_n-n+1$.

Let $A = K[X_1,\ldots,X_n]/I$ and A_d be the image in A of the set of polynomials of degree at most d. We have $A_d \subset A_{d+1}$ for every d. Substituting 1 for X_o gives a surjection $\tilde{A}^d \to A_d$. If y is the image of $\tilde{y}$ under this substitution, the commutative diagram

$$\begin{tikzcd}
\tilde{A}^{d-1} \arrow[r, "\tilde{y}"] \arrow[d] & \tilde{A}^{d-1} \arrow[d] \\
A_{d-1} \arrow[r, "y"] & A_d
\end{tikzcd}$$

shows that y is a surjection and $\dim_K A_d \leq \dim_K A_{d-1}$ for $d \geq d_1+\ldots+d_n-n+1$. The inclusion $A_{d-1} \subset A_d$ thus gives equality and every monomial of degree $d_1+\ldots+d_n-n+1$ is congruent modulo I to a polynomial of lower degree. It follows that the elements of degree at most $d_1+\ldots+d_n-n+1$ of any reduced Gröbner base are also a Gröbner base by the same argument as in the proof of theorem 2.

Remark. Assertion i) of theorem 3 is a slight improvment of a result of Buchberger [Buc 3]. Theorems 2 and 3 proceed from the goal of unifying Buchberger's result with results of algebraic geometry [Laz 3] : the following theorem can be deduced from theorem 3.3 of [Laz 3] with the same reduction steps as in theorem 2.

Theorem 4. *With same hypotheses and notation as in theorem 2, let* $P(d)$ *be the Hilbert polynomial, i.e. the unique polynomial in* d *such that* $P(d) = \dim_K A^d$ *for* d *large enough. We have* $P(d) = \dim_K A^d$ *for* $d \geq d_1+\ldots+d_{r+1}-n$.

As in the case of theorem 2 we conjecture that the result is true even if conjecture 1 is not true.

REFERENCES

[Bay] D.A. Bayer. The division algorithm and the Hilbert scheme, Ph D, Harward Univ., 1982.

[Buc 1] B. Buchberger. Ein algorithmishes Kriterium fur die Lösbarkeit eines algebraischen Gleischungsystem. Aequationes Matematicea 4 (1970), p. 374-383.

[Buc 2] B. Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner bases, EUROSAM'79, Lect. Notes in Comp. Sc. n° 72 (1979), p. 3-21.

[Buc 3] B. Buchberger. A note on the complexity of constructing Gröbner bases. These proceedings.

[Kap] I. Kaplansky. Commutative rings. Allyn and Bacon (Boston, 1970).

[Laz 1] D. Lazard. Algèbre linéaire sur $K[X_1,\ldots,X_n]$ et élimination. Bull. Soc. Math. France 105 (1977), p. 165-190.

[Laz 2] D. Lazard. Systems of algebraic equations. EUROSAM 79, p. 88-94.

[Laz 3] D. Lazard. Résolution des systèmes d'équations algébriques. Theor. Comp. Sciences 15 (1981), p. 77-110.

[Laz 4] D. Lazard. Commutative Algebra and Computer Algebra, EUROCAM'82, Lect. Notes in Comp. Sc. n° 144 (1982), p. 40-48.

[Mor] F. Mora. An algorithm to compute the equations of tangent cones, EUROCAM'82, p. 158-165.

[P.Y.] M. Pohst, D.Y.Y. Yun. On solving systems of algebraic equations via ideal bases and elimination theory SYMSAC 1981, p. 206-211.

[Tri] W. Trinks, Ueber B. Buchberger Verfahren, Systeme algebraischer Gleischungen zu lösen, J. of Number Theory 10 (1978), p. 475-488.

Appendix

During the conference, F. Mora gave me the following counter-example to conjecture 3: Every Gröbner basis of the prime ideal $(X^{n+1}-Y^{n-1}ZT, XZ^{n-1}-Y^{n}, X^{n}Y-Z^{n}T)$ contains the polynomial $Y^{n^2+1} - Z^{n^2}T$ when assuming to have a reverse lexicographical ordering such that $X > Z > Y > T$.