Complexity of Zero-dimensional Gröbner Bases

Amir Hashemi, Daniel Lazard

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Complexity of Zero–dimensional Gröbner Bases

Amir Hashemi — Daniel Lazard

N° 5660

August 2005

Thème SYM

ISSN 0249-6399 ISRN INRIA/RR--5660--FR+ENG

Complexity of Zero–dimensional Gröbner Bases

Amir Hashemi , Daniel Lazard

Thème SYM — Systèmes symboliques
Projet SALSA

Rapport de recherche n° 5660 — August 2005 — 29 pages

Abstract: In this paper, it is shown that the Gröbner basis (for any monomial ordering) of a zero–dimensional ideal may be computed within a *bit complexity* which is essentially polynomial in D^n where n is the number of unknowns and D the mean value of the degrees of input polynomials. Therefore, if all input polynomials have the same degree, this complexity is polynomial in the maximum of the input size and of the output size, for almost all inputs.

The proof is designed in order that it may be generalized to the case of an ideal generated by a regular sequence and for the degree reverse lexicographic ordering, when the last variables are in generic position for the ideal. But one step of the proof is yet lacking in this case.

Key-words: Gröbner basis, complexity, Castelnuovo-Mumford regularity

Complexité du calcul de bases de Gröbner en dimension zéro

Résumé : Dans cet article, on montre que la base de Gröbner (pour tout ordre monomial) d'un idéal zéro–dimensionnel peut être calculée avec une *complexité binaire* qui est essentiellement polynomiale en D^n, où n est le nombre d'inconnues et D la valeur moyenne des degrés des polynômes d'entrée. Par conséquent, si tous les polynômes d'entrée ont le même degré, cette complexité est polynomiale en le maximum de la taille d'entrée et de la taille de sortie pour presque toutes les entrées.

La preuve est organisée pour être généralisée au cas d'un idéal engendré par une suite régulière et pour l'ordre (du degré) lexicographique inverse, quand les dernières variables sont en position générique pour l'idéal. Mais une étape de la preuve manque encore dans ce cas.

Mots-clés : Base de Gröbner, complexité, régularité de Castelnuovo-Mumford

1 Introduction

The aim of this paper is to show that any reduced Gröbner basis of a zero–dimensional ideal may be computed within a bit complexity which is essentially polynomial in D^n where n is the number of unknowns and D the mean value of the degrees of input polynomials. The proof shows also that the same complexity may arise for an ideal generated by a regular sequence and the degree reverse lexicographic monomial ordering, when the last variables are in generic position for the ideal (a definition of this notion of generic position is provided). However there is a step of the proof which is not yet extended to this case.

More precisely, we prove that this complexity is polynomial in the maximum of D^n and of the input size for the dense representation of polynomials. If all input polynomials have the same degree $d = D$, Bézout theorem asserts that, generically, the polynomials in the Gröbner basis have D^n monomials. This means that in this case, *the complexity is polynomial in the maximum of the input size and of the output size for almost all inputs.* This allows to speak of a *quasi-optimal complexity.* The precise statements of our result are given in Section 2.

The few existing results in this direction are the following. If the homogenization of the input polynomials either defines a zero–dimensional projective variety or is a regular sequence then a bound of complexity $d^{O(n)}$ (where d is the maximal degree of the input polynomials) is given in [Laz83] for the degree reverse lexicographic ordering. This result uses the methods of [Laz81], which will also be used through this paper. The extension of this result to any monomial ordering (zero–dimensional case) results from [FGLM93]. Lakshman [Lak91] has removed, in the zero–dimensional case, the condition on the homogenized polynomials, but he has replaced the bit complexity by the *arithmetic complexity.* On the other hand, Dickenstein et al. [DFGS91] give the bit complexity bound of $d^{O(n^2)}$ for zero–dimensional ideals.

In all these results the maximal degree d of the input polynomials may be replaced by their mean value as shown in [HL05]. However, this improvement does not change the algorithms but results from a more accurate estimation of this complexity.

Thus our algorithm is the first to have a quasi-optimal complexity for the whole class of zero–dimensional ideals (without condition "at infinity").

It should be noted that although our algorithm has the best known complexity, (and is therefore interesting from a theoretical point of view), it is not designed to be implemented. In fact, as a counterpart of this quasi optimality, this algorithm may not be practical for effective computations for several reasons. First of all, it uses a Smith normal form computation which implies that the complexity is a rather high power of d^n.

Secondly, our algorithm does not test the specification of the input (zero–dimensionality of the ideal or regularity of the sequence). Also, a random linear transformation on the input polynomials should be done in the overdetermined zero–dimensional case. The probability of a bad choice is almost 0 but the algorithm does not test this. The lack of verification of the specification of the input detracts from the practical interests of our algorithm: on an input which does not satisfy the specification, it provides a wrong output without any warning.

Finally, although our algorithm has a good worst case complexity, there exist algorithms which have a much better complexity on almost all inputs. Namely, the algorithm F_5 [Fau02] computes the Gröbner basis with Gaussian elimination instead of Smith normal form computation, and uses smaller matrices than our algorithm, if the degrees do not increase much higher than Macaulay bound. The exceptional cases where the working degrees of F_5 exceed the Macaulay bound seem extremely rare and no example is yet known. It is not even known if F_5 has or not a complexity which is polynomial in d^n on zero–dimensional ideals or non homogeneous regular sequences. Thus although we have no formal proof of what preceded, F_5 seems definitively better in practice than our algorithm.

The general strategy of the proofs is the following:

- We consider first an ideal I generated by a regular sequence $f_1, \ldots, f_k$. In this case, we homogenize them to $F_1, \ldots, F_k$. Then we deform F_i to $G_i = (1-s)F_i + sx_i^{d_i}$ for any i where s is a new indeterminate (see Section 3);
- With the deformed polynomials, we reduce Macaulay matrices as in [Laz81] and [Laz83], but we replace Gaussian elimination on Macaulay matrices by Smith normal form. This allows to get a convenient result after substituting s by zero, which removes the components at infinity of higher dimension;
- Then a localization by the variable of homogenization removes the remaining components at infinity and provides the Macaulay matrix of the homogenization of the initial ideal (generated by a regular sequence);
- In the zero–dimensional case, the preceding computation are done on a regular sequence of n elements extracted from the input ideal. The remaining generators of the ideal are introduced to get the Macaulay matrix of the homogenization of the input ideal (see Section 8);
- The Gröbner basis for the degree reverse lexicographical ordering is got as the columns of the echelon form of this Macaulay matrix. The Gröbner bases for the other orderings are deduced, using [FGLM93].

Now, we give the structure of the paper. In Section 2, we state our main results. In Section 3, we give the general notations used through this paper and we show some properties of homogenization and deformation of the input polynomials which is used later. Section 4 contains the definition of Macaulay matrices and recall how these matrices may be used to test Castelnuovo-Mumford regularity through Quillen's theorem. In Section 5, we show that it make sense to substitute 0 the parameter of the deformation, if the Macaulay matrix is in Smith normal form. In Section 6, a kind of localization of the resulting matrix gives a Macaulay matrix of the homogenization of the initial ideal. In Section 7, we dehomogenize in the case of an ideal generated by a regular sequence. For this purpose, we introduce a precise definition of variable in generic position. Finally, the end of the proof for zero–dimensional case is the object of Section 8.

2 Statement of the main results and first reductions

In this section, we fix our notations in order to state our main results. We describe also some easy reductions which are down at the beginning of the algorithm.

We work with polynomials over a *computable field* K over which the linear algebra has a polynomial complexity. This means that all matrix operations over K, including determinant computation and transformation to echelon form may be done in a time which is bounded by a polynomial in the size of the input. This implies also that the size of the output is similarly polynomially bounded. Thus K may be the field of rational numbers or a finite field, but it may also be the field of rational functions in a finite number of variables over such a field.

In all this paper we consider polynomials $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$ and the ideal $I = \langle f_1, \ldots, f_k \rangle$ generated by these polynomials. We suppose that f_i is not zero and we call d_i its total degree. If there are $\ell > 0$ non linear polynomials among the f_i we number the f_i in order that $d_2 \geq \cdots \geq d_\ell \geq d_1 \geq 2 > 1 = d_{\ell+1} = \cdots = d_k$. If $k < n$ we set $d_{k+1} = \cdots = d_n = 1$. Let $D = (d_1 + \cdots + d_n)/n$.

We define T, the total size of the input polynomials, as the sum of their sizes in the *dense representation*. That is in the representation where all monomials of degree at most d_i are written, even if they have a zero coefficient. Thus the size of f_i is bounded by $hn\binom{n+d_i}{n}$ where h is the maximal size of the coefficients; the factor n comes from the representation of the vector of the exponents of the variables. Note that this bound become an equality if all the coefficients have the same size. We denote also by $\mathcal{T}$ the maximum of T and D^n.

Let us recall the definition of the *degree reverse lexicographic ordering*, denoted by $\prec$, on the monomials of $K[x_1, \ldots, x_{n+1}]$ with $x_{n+1} = x_0$. For this we denote respectively by $\deg(m)$ and $\deg_i(m)$ the total degree and the degree in x_i of a monomial m. If m and m' are monomials, $m \prec m'$ if and only if either $\deg(m) < \deg(m')$ or $\deg(m) = \deg(m')$ and there exists $i \leq n+1$ such that $\deg_i(m) > \deg_i(m')$ and $\deg_j(m) = \deg_j(m')$ for $j = i+1, \ldots, n+1$. Thus $x_{n+1} \prec x_n \prec \cdots \prec x_1$.

With these definitions we may state precisely our results.

Theorem 2.1 *Suppose that I is a zero–dimensional ideal in $K[x_1, \ldots, x_n]$. Then the reduced Gröbner basis of I with respect to any ordering may be computed within a bit complexity which is polynomial in $\mathcal{T}$.*

Moreover, the elements of the reduced Gröbner basis of I with respect to the degree reverse lexicographic ordering have a degree at most $nD - n + 1$.

Recall that a sequence of polynomials $f_1, \ldots, f_k$ in the ring $R = K[x_1, \ldots, x_n]$ is called a *regular sequence* if f_i is a non zero divisor in the ring $R/\langle f_1, \ldots, f_{i-1} \rangle$ for $i = 2, \ldots, k$. This is equivalent to the condition that f_i does not belong to any associated prime of $\langle f_1, \ldots, f_{i-1} \rangle$. We say that the variables $x_{k+1}, \ldots, x_n$ are in *generic position* for $I = \langle f_1, \ldots, f_k \rangle$ if the ideals $I + \langle x_{k+1}, \ldots, x_n \rangle$ of $K[x_1, \ldots, x_n]$ and $I + \langle A_{k+1,0} + \sum_{i=1}^n A_{k+1,i} x_i, \ldots, A_{n,0} + \sum_{i=1}^n A_{n,i} x_i \rangle$ of $K(A_{k+1,0}, \ldots, A_{n,n})[x_1, \ldots, x_n]$ have the same Hilbert series, the $A_{i,j}$ being new indeterminates. This is not the usual definition, but it implies any previous definition.

The proof of the above theorem is designed such that it may be generalized to the case of a regular sequence $f_1, \ldots, f_k$ when the last variables are in generic position for the generated ideal. One step of the proof (Lemma 6.1), which is yet a conjecture to be true, is lacking for this generalization.

Conjecture 2.1 *Suppose that $f_1, \ldots, f_k$ is a regular sequence and that $x_{k+1}, \ldots, x_n$ are in generic position for I. Then the reduced Gröbner basis of I with respect to the degree reverse lexicographic ordering may be computed within a bit complexity which is polynomial in $\mathcal{T}$.*

Proposition 2.1 *Under the hypotheses of Conjecture 2.1, the elements of the reduced Gröbner basis of I with respect to the degree reverse lexicographic ordering have a degree at most $nD - n + 1$.*

To prove these results, we proceed by successive reductions which will be the object of different sections. All these reductions will increase the size of the coefficients, but our hypothesis on K will imply that the size of these coefficients at the end of any of these steps remains bounded by a polynomial in $\mathcal{T}$.

If $D \geq 2$, then the input size satisfies $T \leq hkD^{2.45n}$ (see [HL05]) where h is the maximal size of the coefficients of the f_i. This inequality shows immediately the following corollary.

Corollary 2.1 *If $D \geq 2$ (and if Conjecture 2.1 is true), the arithmetic complexity of both problem is polynomial in kD^n and the bit complexity is polynomial in hkD^n, where h is a bound of the size of input coefficients.*

The first step of reductions consists in eliminating the linear polynomials as described in [HL05]. This shows

Corollary 2.2 *To prove Theorem 2.1, Conjecture 2.1 and Proposition 2.1 one may suppose without lost of generality that $d_i \geq 2$ for any i.*

Thus we will suppose in the remainder of the paper that all the d_i and therefore D are not lower than 2.

If $k > n$ we will need that $f_1, \ldots, f_n$ is a regular sequence. We may suppose that it is the case because of the following.

Proposition 2.2 *Suppose that K is infinite. For $i = 2, \ldots, n$ let $g_i = f_i + a_{i,i+1}f_{i+1} + \ldots + a_{i,k}f_k$ where $a_{i,j} \in K$. For almost all choices of the $a_{i,j}$ the sequence $f_1, g_2, \ldots, g_n$ is regular and $\deg(g_i) = \deg(f_i)$.*

Proof The assertion on the degrees follows from the choice of the numbering of the f_i. The other assertion is proved in [Kap74] or [GC83]. □

Corollary 2.3 *If $k \geq n$, we may suppose without lost of generality that the sequence $f_1, \ldots, f_n$ is regular.*

Proof If K is infinite, it suffices to choose randomly the $a_{i,j}$. In the other case we do the computation in an infinite extension of K, say $K(t)$, using the fact that the reduced Gröbner basis is not modified by an extension of the field of the coefficients. □

Thus from now until Section 8 we consider as input polynomials the regular sequence $f_1, \ldots, f_{\min\{k,n\}}$ which will be denoted by $f_1, \ldots, f_k$ by an abuse of notation.

3 Homogenization and deformation

In this section, we reduce the problem to another one to which the hypothesis of [Laz83] may be applied. However, the main difficulty lies in transforming back the result to our original problem. Therefore, most of the section is devoted on the algebraic results needed for this back substitution (Proposition 3.1).

We homogenize first the f_i. This means that we introduce a new variable x_0 and associate to each f_i the homogeneous polynomial $F_i = x_0^{d_i} f_i(x_1/x_0, \ldots, x_n/x_0) \in K[x_0, \ldots, x_n]$. Then $f_i = F_i(1, x_1, \ldots, x_n)$ is obtained by substitution of x_0 by 1 in F_i.

Unfortunately, the homogenization of a regular sequence is *not* necessarily a regular sequence and if $\langle f_1, \ldots,$
$f_k\rangle$ is zero–dimensional, the projective variety defined by the F_i may have components "at infinity" of high dimension. To remove these *"alien"* components we use a deformation which was used already by Grigoriev and Chistov [GC83], Canny [Can90], Lakshman [Lak90] and Lakshman and Lazard [LL91] in other contexts.

From now on, we will use the following notation, which extends the preceding one.

Notation 3.1 *The polynomials $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$ are of respective total degree $d_1, \ldots, d_k$. Recall that the above reduction allows to suppose that $d_2 \geq \cdots \geq d_k \geq d_1 \geq 2$. If $k < n$ we set $d_{k+1} = \cdots = d_n = 1$. Let $D = (d_1 + \cdots + d_n)/n$. Denote by F_i the homogenized polynomial of f_i with respect to a new variable x_0. Let s be a new indeterminate and $G_i = (1-s)F_i + sx_i^{d_i}$ for any i. We consider the ideals $I = \langle f_1, \ldots, f_k\rangle$, $\tilde{I} = \langle F_1, \ldots, F_k\rangle$ and $J = \langle G_1, \ldots, G_k\rangle$ which belong respectively to $R = K[x_1, \ldots, x_n]$, $\tilde{R} = K[x_0, \ldots, x_n]$ and $S = K[s, x_0, \ldots, x_n]$.*

The remainder of this section is devoted to the properties of J which are needed to translate back to the original problem the result of the computation which will be done on J.

We could not find any reference for the next lemma, although it is certainly well-known. We recall that the dimension $\dim X$ of an ideal X is the dimension of the corresponding quotient ring.

Lemma 3.1 *Let $L = \langle P_1, \ldots, P_k\rangle$ be a homogeneous ideal of the ring $\tilde{R} = K[x_0, \ldots, x_n]$ such that $\dim L = n + 1 - k$. Then $P_1, \ldots, P_k$ is a regular sequence in $\tilde{R}$.*

Proof Let $\sum_{i=1}^{\ell} H_i P_i = 0$ for $\ell = 2, \ldots, k$ be a relation between the P_i; we have to prove that $H_\ell \in \langle P_1, \ldots, P_{\ell-1} \rangle$. For this, let $\mathfrak{m}$ be the unique maximal homogeneous ideal of $\tilde{R}$ and let $\tilde{R}_\mathfrak{m}$ be the local ring of $\tilde{R}$ at $\mathfrak{m}$ (for more details see [Mat89] for example). Since $L\tilde{R}_\mathfrak{m}$ is an ideal generated by k elements and of dimension $n+1-k$ then $P_1, \ldots, P_k$ is a regular sequence in $\tilde{R}_\mathfrak{m}$ by Theorem 17.4 of [Mat89]. Thus we find that there exist $\beta, \alpha_1, \ldots, \alpha_{\ell-1} \in \tilde{R}$ and $\beta \notin \mathfrak{m}$ (which are not necessarily homogeneous) such that $\beta H_\ell = \sum_{i=1}^{\ell-1} \alpha_i P_i$. Let α'_i be the homogeneous part of α_i of degree $\deg(H_\ell) - \deg(P_i)$ and $\beta' \in K - \{0\}$ be the homogeneous part of degree 0 of β. Then we have $H_\ell = \sum_{i=1}^{\ell-1} \alpha'_i/\beta' P_i$ which is in $\langle P_1, \ldots, P_{\ell-1} \rangle$. □

Lemma 3.2 *With above notation, the sequence $G_1, \ldots, G_k, x_0, x_{k+1}, \ldots, x_n$ is a regular sequence in the ring $K(s)[x_0, \ldots, x_n]$.*

Proof Recall that the resultant of $n+1$ homogeneous polynomials $H_0, \ldots, H_n \in K[x_0, \ldots, x_n]$ of degree $d_0, \ldots, d_n$, which is denoted by $\mathrm{Res}(H_0, \ldots, H_n)$, is a polynomial in the coefficients of the H_i such that we have $\mathrm{Res}(x_0^{d_0}, \ldots, x_n^{d_n}) = 1$ and that the the existence of a non trivial common zero of the H_i over an algebraic closure of K is equivalent to $\mathrm{Res}(H_0, \ldots, H_n) = 0$(see [CLO98] for example). Moreover, if the coefficients of the H_i depend on some variables, the substitution of these variables by some values is an operation which commutes with the resultant.

Now set $G_i = x_i$ for $i = 0, k+1, \ldots, n$. By substitution of s by 1 in $\mathrm{Res}(G_0, \ldots, G_n)$ we obtain

$$\mathrm{Res}(x_0, x_1^{d_1}, \ldots, x_k^{d_k}, x_{k+1}, \ldots, x_n) = 1.$$

Thus $\mathrm{Res}(G_0, \ldots, G_n) \neq 0$ and the ideal $\langle G_0, \ldots, G_n \rangle = \langle G_1, \ldots, G_k, x_0, x_{k+1}, \ldots, x_n \rangle$ has dimension zero which implies that the sequence $G_1, \ldots, G_k, x_0, x_{k+1}, \ldots, x_n$ is a regular sequence by Lemma 3.1. □

The following theorem is a generalization of Zariski Principal Ideal Theorem which seems to be new (except in [LR05]).

Theorem 3.1 *Let $I = \langle f_1, \ldots, f_k \rangle$ be an ideal of the ring $R = K[x_1, \ldots, x_n]$ and let $P \in \mathrm{Ass}(I)$ be an associated prime of I such that $\dim P < n - k$. Then there exists $Q \in \mathrm{Ass}(I)$ such that $\dim Q > n - k$ and $Q \subset P$.*

Proof Let R_P be the local ring of R at P. If ℓ is the dimension of R_P, then by the hypothesis $\ell > k$. If $f_1, \ldots, f_k$ was a regular sequence in R_P then any associated prime ideal of I_P would have dimension $\ell - k > 0$. But P_P is an associated prime ideal of I_P of dimension zero which is a contradiction. Thus $f_1, \ldots, f_k$ is not a regular sequence in R_P. This implies that there exists an associated prime ideal, say Q_P, of I_P of dimension $> \ell - k$ by Theorem 17.4 of [Mat89]. Hence $Q = Q_P \cap R$ is an associated prime ideal of I which is contained in P and has a dimension $> n - k$. □

If X is an ideal in $S = K[s][x_0, \ldots, x_n]$ we denote by $X|_{s=0}$ (resp. $X|_{x_0=1}$) the ideal in $K[x_0, \ldots, x_n]$ (resp. $K[s][x_1, \ldots, x_n]$) obtained by substitution s by 0 (resp. x_0 by 1) in X.

Lemma 3.3 *With Notation 3.1, suppose that $f_1, \ldots, f_k$ is a regular sequence in the ring $K[x_1, \ldots, x_n]$ and let P be an associated prime ideal of $\tilde{I} + \langle s \rangle$ of dimension $\geq n + 2 - k$ in $S = K[s, x_0, \ldots, x_n]$. Then $x_0 \in P$.*

Proof Let P' be a minimal prime ideal which contains $\tilde{I}$ and is contained in $P|_{s=0}$. Suppose that $x_0 \notin P'$. Since $P'S \subset P$ and $s \notin P'S$, then $P'S$ has dimension $> n+2-k$ and P' has dimension $> n+1-k$. On the other hand, from $x_0 \notin P'$ we can conclude that $P'|_{x_0=1}$ is an associated prime ideal of the ideal generated by $f_1, \ldots, f_k$ (see [Frö97] p. 110 for example) which is a regular sequence by the hypothesis. This implies that P' is of dimension $n+1-k$ which is a contradiction. Thus $x_0 \in P' \subset P$. □

If X is an ideal in $S = K[s][x_0, \ldots, x_n]$, we recall that the ideal $X : f^\infty$ for $f \in S$ is defined by

$$X : f^\infty = \left\{ g \in S \mid \exists\, t \in \mathbb{N} \text{ s.t. } gf^t \in X \right\}.$$

We denote by $X|_{s=0,x_0=1}$ the ideal of $K[x_1, \ldots, x_n]$ obtained by substitution of s by 0 and of x_0 by 1 in X. Now we state the main result of this section.

Proposition 3.1 *With Notation 3.1, suppose that $f_1, \ldots, f_k$ is a regular sequence. Then*

- $J \subset J : s^\infty \subset J : x_0^\infty$;
- $\tilde{I} \subset J : s^\infty|_{s=0} \subset \tilde{I} : x_0^\infty$;
- $I = J : s^\infty|_{s=0,x_0=1} = J : x_0^\infty|_{s=0,x_0=1}$.

Proof Let $\bigcap_{i=1}^t Q_i$ be an irredundant primary decomposition of J as an ideal of the ring $S = K[s][x_0, \ldots, x_n]$. It is well-known that we have $J : f^\infty = \bigcap_{i=1}^t (Q_i : f^\infty) = \bigcap_{f \notin \sqrt{Q_i}} Q_i$ for any $f \in S$ (see [CLO97] for example). Hence for proving the first item it is enough to show $Q_i : s^\infty \subset Q_i : x_0^\infty$ for any i.

Let $\mathrm{Ass}(J) = \{P_1, \ldots, P_t\}$ be the set of associated prime ideals of J such that $\sqrt{Q_i} = P_i$ for any i. For a given i two cases are possible: If $s \notin P_i$ we can check simply that $Q_i : s^\infty = Q_i \subset Q_i : x_0^\infty$. In the other case i.e. $s \in P_i$ we have $Q_i : s^\infty = S$ and we have to prove $Q_i : x_0^\infty = S$ i.e. $x_0 \in P_i$. If $\dim P_i \geq n + 2 - k$ then let P be a minimal prime ideal of $J + \langle s \rangle$ such that $P \subset P_i$. If $\dim P_i < n + 2 - k$ then, by Theorem 3.1, there exists a prime ideal $P \in \mathrm{Ass}(J)$ such that $\dim P > n + 2 - k$ and $P \subset P_i$. Then $\dim P|_{s=0} \geq n + 2 - k$ in the two cases which implies that $x_0 \in P \subset P_i$ by Lemma 3.3.

The first inclusion of the second item follows from definition of J and by setting $s = 0$ in this ideal. To prove the second inclusion, we have immediately that $J : x_0^\infty|_{s=0} \subset \tilde{I} : x_0^\infty$ from the definition of J. Then using $J : s^\infty \subset J : x_0^\infty$ (by the first item) we can conclude the claim.

Now, for deducing the third item from the first one it is enough to prove that $I = J : x_0^\infty|_{s=0,x_0=1}$. From the proof of the second item we have $J|_{s=0} \subset J : x_0^\infty|_{s=0} \subset \tilde{I} : x_0^\infty$ thus the assertion follows from the simple equalities $I = \tilde{I} : x_0^\infty|_{x_0=1} = J : x_0^\infty|_{s=0,x_0=1}$. □

4 Macaulay matrix and regularity

The main idea of our algorithm consists in doing linear algebra on the usual Macaulay matrix of J in order to get the Macaulay matrices of, successively, $J' = J : s^\infty|_{s=0}$ and $J' : x_0^\infty = \tilde{I} : x_0^\infty$ in a special degree which is the Castelnuovo-Mumford regularity of these ideals. Thus in this section we recall the definitions of these concepts and the related properties which will be needed.

Definition 4.1 *Let $\mathcal{S} = \mathcal{K}[x_0, \ldots, x_n]$ be a ring where $\mathcal{K}$ is either K or $K[s]$ and let $P_1, \ldots, P_k \in \mathcal{S}$ be polynomials which are homogeneous in $x_0, \ldots, x_n$. Let δ be a fixed integer and let $\mathcal{G}$ be any finite generating set of the module of the homogeneous polynomials of degree δ in the ideal generated by $P_1, \ldots, P_k$.*

We call a Macaulay matrix *of $\langle P_1, \ldots, P_k\rangle$ in degree δ the matrix of the elements of $\mathcal{G}$ over some monomial basis. Thus any column transformation of a Macaulay matrix is yet a Macaulay matrix. The* usual Macaulay *matrix is the matrix for which $\mathcal{G}$ consists in all the products of the P_i by any monomial of degree $\delta - \deg(P_i)$.*

In the following, we recall the definition of the Castelnuovo-Mumford regularity of a homogeneous ideal. For this we denote by X_d the set of homogeneous elements of degree d in X where X is a graded object (ring, ideal, module,...).

Definition 4.2 *Let L be a homogeneous ideal of $\tilde{R} = K[x_0, \ldots, x_n]$. A homogeneous polynomial $P \in \tilde{R}$ of degree d is called* almost regular *in degree m on L if the multiplication*

$$P : \left(\frac{\tilde{R}}{L}\right)_{m-d} \longrightarrow \left(\frac{\tilde{R}}{L}\right)_m$$

is injective.

Definition 4.3 *A sequence of homogeneous polynomials $P_1, \ldots, P_k$ is called an* almost regular sequence *in degree m on L if P_i is almost regular in degree m on $L + \langle P_1, \ldots, P_{i-1}\rangle$ for any i.*

Definition 4.4 (D. Quillen) *Let L be a homogeneous ideal of the ring $\tilde{R} = K[x_0, \ldots, x_n]$. The ideal L is called* m-regular *if there exist $y_1, \ldots, y_i \in \tilde{R}_1$ for some $i \geq 0$ so that $y_1, \ldots, y_i$ is an almost regular sequence in degree m on L and $(L + \langle y_1, \ldots, y_i\rangle)_m = \tilde{R}_m$.*

Definition 4.5 *The* Castelnuovo-Mumford regularity *of L is the smallest m such that L is m-regular; we note it by* $\mathrm{reg}(L)$.

For more details on the regularity, we refer to [Qui64], [Mum66], [EG84], [BS87] and [BCG+91].

In this paper we use an interpretation in term of Macaulay matrices of Quillen's definition of the Castelnuovo-Mumford regularity. For this, let L be a m-regular homogeneous ideal

in the ring $\tilde{R} = K[x_0, \ldots, x_n]$. Then there exist $y_1, \ldots, y_i$ in $\tilde{R}_1$ for some i such that the multiplication

$$y_j : \left(\frac{\tilde{R}}{L + \langle y_1, \ldots, y_{j-1}\rangle}\right)_{m-1} \longrightarrow \left(\frac{\tilde{R}}{L + \langle y_1, \ldots, y_{j-1}\rangle}\right)_m$$

is injective for any j (Definition 4.4). This implies that the following sequence is exact:

$$0 \longrightarrow \left(\frac{\tilde{R}}{L + \langle y_1, \ldots, y_{j-1}\rangle}\right)_{m-1} \xrightarrow{y_j} \left(\frac{\tilde{R}}{L + \langle y_1, \ldots, y_{j-1}\rangle}\right)_m \longrightarrow \left(\frac{\tilde{R}}{L + \langle y_1, \ldots, y_j\rangle}\right)_m \longrightarrow 0.$$

So from additivity of the dimension of vector spaces we have:

$$\dim_K \left(\frac{\tilde{R}}{L + \langle y_1, \ldots, y_{j-1}\rangle}\right)_m = \dim_K \left(\frac{\tilde{R}}{L + \langle y_1, \ldots, y_{j-1}\rangle}\right)_{m-1} + \dim_K \left(\frac{\tilde{R}}{L + \langle y_1, \ldots, y_j\rangle}\right)_m.$$

Let Λ_δ^j be a Macaulay matrix in degree δ of the ideal $L + \langle y_1, \ldots, y_j\rangle$. Let also $\mathrm{cork}(X)$ denotes the corank of a matrix X, i.e. difference between its number of rows and its rank.

Proposition 4.1 *The ideal L is m-regular if and only if we have:*

$$\mathrm{cork}(\Lambda_m^{j-1}) = \mathrm{cork}(\Lambda_{m-1}^{j-1}) + \mathrm{cork}(\Lambda_m^j)$$

for $j = 1, \ldots, i$ and $\mathrm{cork}(\Lambda_m^i) = 0$.

We will also need the following results on the Castelnuovo-Mumford regularity.

Proposition 4.2 ([BS87]) *Let L be a homogeneous ideal of the ring $K[x_0, \ldots, x_n]$ and $\dim L = d$. Let $y_i = \sum_{j=0}^n A_{i,j} x_j$ for $i = 1, \ldots, d$ be d generic linear forms (the $A_{i,j}$ being the new indeterminates). Then L is m-regular if and only if the y_i satisfy the conditions of Definition 4.4 in the ring $K(A_{1,0}, \ldots, A_{d,n})[x_0, \ldots, x_n]$.*

Proposition 4.3 *Let $L = \langle P_1, \ldots, P_k\rangle \subset K[x_0, \ldots, x_n]$ where $P_1, \ldots, P_k$ are homogeneous polynomials of respective degrees $d_1, \ldots, d_k$ which form a regular sequence (or an almost regular sequence in degree $\delta = d_1 + \cdots + d_k - k + 1$). Then L is a δ-regular ideal.*

Proof Since a regular sequence is an almost regular sequence in any degree δ on L, the assertion follows from Theorem 2.2 of [CH03]. □

5 Using Smith normal form

In this section we show that the Macaulay matrix in degree $\delta = nD - n + 1$ of $J : s^\infty|_{s=0}$ may be obtained from the Smith normal form of a Macaulay matrix of J in the same degree. We show also that thees ideals are δ-regular, which is a key result for the next section.

Recall that a matrix in $K[s]^{r\times c}$ is said in *Smith normal form*, if it is a diagonal matrix bordered by zero entries on the right and the bottom:

$$\begin{bmatrix} u_1 & & \\ & \ddots & \\ & & u_t \\ & & \end{bmatrix}$$

A matrix in $K[s]^{r\times c}$ is called *unimodular* if it is invertible i.e. its determinant is a non zero element of K. The matrices M and N in $K[s]^{r\times c}$ are *equivalent* if there are unimodular matrices U in $K[s]^{c\times c}$ and V in $K[s]^{r\times r}$ such that $N = UMV$. Two equivalent matrices represent the same linear map over different basis. A matrix N is called the Smith normal form of a matrix M if and only if it is in Smith normal form and they are equivalent.

Lemma 5.1 *Given a matrix M over K, then there exist a matrix M' in Smith normal form and unimodular matrices U and V such that $M' = UMV$, which may be computed in a polynomial time in the size of M (the size of M is bounded by the product of the number of its entries by the maximal size of these entries, the size of an entry being bounded by the product of its degree by the maximal size of its coefficients).*

Proof This is the main result of [Vil95] (see also [Vil03] and [Sto00]). However it was only stated when K is either the field of rational numbers or a finite field, despite the fact that the proof is true for any field on which the computation of the echelon form of a matrix may be done in a polynomial time. □

Proposition 5.1 *Let δ be a fixed integer. With Notation 3.1, let M be the usual Macaulay matrix in degree δ of J and let UMV be its Smith normal form. Then MV is a Macaulay matrix of J. Moreover, if we divide as much as possible the columns of MV by s we get a Macaulay matrix in degree δ of $J : s^\infty$. By setting $s = 0$ in this latter matrix we get a Macaulay matrix in degree δ of $J : s^\infty|_{s=0}$.*

Proof The first assertion follows from the definition of a Macaulay matrix. To prove the second one, let $M' = UMV$. There exists a diagonal matrix V' with powers of $1/s$ as the entries on its diagonal such that the entries of $M'V'$ are in $K[s]$ and not multiple of s. The same property is clearly true for the entries of $U^{-1}M'V' = MVV'$. We claim that this is a Macaulay matrix in degree δ of the ideal $J : s^\infty$. Let $P_1, \ldots, P_\ell$ be the polynomials corresponding to the columns of MVV'. It follows from the definition of V and V' that $P_i \in J : s^\infty$ for any i and thus $J \subset \langle P_1, \ldots, P_\ell\rangle \subset J : s^\infty$. Conversely, if $P \in J : s^\infty$ there exists α such that $s^\alpha P = \sum_{i=1}^{\ell} a_i P_i$. As the non zero columns of M' are linearly independent, the same is true for $U^{-1}M'V'$ and s^α divides $a_i P_i$ and also a_i for any i.

The last assertion follows immediately from the definition of a Macaulay matrix. □

Corollary 5.1 *With Notation 3.1, a Macaulay matrix in degree $\delta = nD - n + 1$ of the ideal $J : s^\infty|_{s=0}$ may be computed within a bit complexity which is polynomial in $\mathcal{T}$.*

Proof With Notation of Proposition 5.1, the number of the entries of M is polynomial in the number of monomials of degree δ in $n+1$ variables thus it is polynomial in $\mathcal{T}$ by Lemma 3.2 of [HL05]. On the other hand the degree of the entries of M is bounded by δ and the assertion therefore follows from Lemma 5.1 and Proposition 5.1.

□

In the following, we show that the ideal $J : s^\infty|_{s=0}$ is $(nD - n + 1)$-regular.

Lemma 5.2 *With Notation 3.1, let $S' = K(s)[x_0, \ldots, x_n]$. Then*

$$J : s^\infty + \langle s \rangle = JS' \cap S + \langle s \rangle.$$

Proof We prove first that $J : s^\infty \subset JS' \cap S$. For this let $G \in S$ such that $s^\alpha G \in J$ for an integer α. We have clearly $G \in JS' \cap S$. Conversely, if $G \in JS' \cap S$ there exists an integer α such that

$$s^\alpha G = \frac{\sum_{i=1}^k H_i G_i}{P}$$

where P is a polynomial in $K[s]$ such that $P(0) = 1$ and $H_i \in S$. Let $P = 1 - sQ$ where $Q \in K[s]$. Thus we may write $1/P$ as

$$\frac{1}{P} = \frac{1}{1 - sQ} = 1 + sQ + (sQ)^2 + \cdots + (sQ)^\alpha + \frac{(sQ)^{\alpha+1}}{P}.$$

Setting $G' = (1 + sQ + \cdots + (sQ)^\alpha)\frac{\sum_{i=1}^k H_i G_i}{s^\alpha}$, we have $s^\alpha G' \in J$ and

$$G = \frac{\sum_{i=1}^k H_i G_i}{s^\alpha P} = G' + sQ^{\alpha+1}\frac{\sum_{i=1}^k H_i G_i}{P} = G' + sQ^{\alpha+1}G.$$

This implies that $G \in J : s^\infty + \langle s \rangle$. □

Recall that a homogeneous ideal is said *equidimensional* if all its associated primes have the same dimension.

Lemma 5.3 *With Notation 3.1, suppose that $f_1, \ldots, f_k$ is a regular sequence. Let $y_i = \sum_{j=0}^n A_{i,j} x_j$, $i = 1, \ldots, n-k+1$ be generic linear forms (the $A_{i,j}$ being the new indeterminates). Then we have:*

$$\left(\left(J\tilde{R}'[s] + \langle y_1, \ldots, y_{n-k+1}\rangle\right) : s^\infty|_{s=0}\right)_\delta = \left(J\tilde{R}'[s] : s^\infty|_{s=0} + \langle y_1, \ldots, y_{n-k+1}\rangle\right)_\delta$$

where $\tilde{R}' = K(A_{1,0}, \ldots, A_{n-k+1,n})[x_0, \ldots, x_n]$ and $\delta = nD - n + 1$.

Proof The inclusion "$\supset$" is immediate from the definition of the notation. To prove the other inclusion, we proceed by induction on the number of y_i. For $i = 0$, this is clear. For $i = 1$, let $P \in \left(J\tilde{R}'[s] + \langle y_1\rangle\right) : s^\infty|_{s=0}$ be a polynomial of degree δ. Then there exists an integer α and a polynomial $H \in \tilde{R}'[s]$ such that

$$s^\alpha(P + sH) \in J\tilde{R}'[s] + \langle y_1\rangle \subset J\tilde{R}'[s] : s^\infty + \langle y_1\rangle.$$

Let α be minimal such that there exists H such that:

$$s^\alpha(P + sH) = P' + y_1H' \in J\tilde{R}'[s] : s^\infty + \langle y_1\rangle. \tag{1}$$

We have to prove that $\alpha = 0$. If it would not be the case then let us write $P' = P'_1 + sP''_1$ and $H' = H'_1 + sH''_1$ with $P'_1, H'_1 \in \tilde{R}'$ and $P''_1, H''_1 \in \tilde{R}'[s]$. By substituting s by 0 in (1) we get $P'_1 + y_1H'_1 = 0$. We claim that y_1 is a non zero divisor in $\tilde{R}'/(J\tilde{R}'[s] : s^\infty|_{s=0})$. Since $P'_1 \in J\tilde{R}'[s] : s^\infty|_{s=0}$ this claim implies that $H'_1 \in J\tilde{R}'[s] : s^\infty|_{s=0}$. Let $H'_1 = H'_2 + sH''_2$ with $H'_2 \in J\tilde{R}'[s] : s^\infty$. We may replace P' by $P' + y_1H'_2$ and H' by $H' - H'_2$ which means that (1) may be rewritten with $P' \in J\tilde{R}'[s] : s^\infty$ and H' multiple of s. If $\alpha \geq 1$ this implies that P' is also a multiple of s, by (1) and α may be replaced by $\alpha - 1$ which is a contradiction with the assumption of minimality.

Proof of the claim: By Lemma 5.2 we have to show that y_1 is a non zero divisor in $\tilde{R}'[s]/(J' + \langle s\rangle)$ where $J' = J\tilde{R}'(s) \cap \tilde{R}'[s]$. Recall that J is generated by the regular sequence $G_1, \ldots, G_k$ in $K(s)[x_0, \ldots, x_n]$ (Lemma 3.2) and is therefore δ-regular in this ring (Proposition 4.3). Thus the multiplication

$$y_1 : \left(\frac{\tilde{R}'(s)}{J\tilde{R}'(s)}\right)_{\delta-1} \longrightarrow \left(\frac{\tilde{R}'(s)}{J\tilde{R}'(s)}\right)_{\delta}$$

is injective (Proposition 4.2 and Definition 4.4), and this implies the injectivity of the restriction of this map to sub-modules:

$$y_1 : \left(\frac{\tilde{R}'[s]}{J'}\right)_{\delta-1} \longrightarrow \left(\frac{\tilde{R}'[s]}{J'}\right)_{\delta}.$$

Clearly, s is a non zero divisor in $\tilde{R}'[s]/J'$. Thus the generic linear form $y_1 + A_0s$ where A_0 is a new indeterminate is also a non zero divisor in this ring. If $y_1F \in J' + \langle s\rangle$ for some F we have $(y_1 + A_0s)F \in J' + \langle s\rangle$. This implies that $F \in J' + \langle s\rangle$ and this proves the claim.

Now, let $i \geq 2$ and suppose the claim is true for $i - 1$. Let $P \in \left(J\tilde{R}'[s] + \langle y_1, \ldots, y_i\rangle\right) : s^\infty|_{s=0}$. By applying the above proof with $J\tilde{R}'[s]$ replaced by $J\tilde{R}'[s] + \langle y_1, \ldots, y_{i-1}\rangle$ we get

$$P \in \left(J\tilde{R}'[s] + \langle y_1, \ldots, y_{i-1}\rangle\right) : s^\infty|_{s=0} + \langle y_i\rangle$$

using the fact that the ideal $J + \langle y_1, \ldots, y_{i-1}\rangle \subset \tilde{R}'(s)$ remains δ-regular (Lemma 1.8 of [BS87]). So we have $P \in J\tilde{R}'[s] : s^\infty|_{s=0} + \langle y_1, \ldots, y_i\rangle$ which ends the proof, by induction on i. □

Proposition 5.2 *With Notation 3.1, suppose that $f_1, \ldots, f_k$ is a regular sequence. Then the ideal $J : s^\infty|_{s=0} \subset \tilde{R} = K[x_0, \ldots, x_n]$ is δ-regular with $\delta = nD - n + 1$ and has dimension $n - k + 1$.*

Proof With notations of Lemma 5.3 and by Proposition 4.2, we prove the δ-regularity of $J' = J\tilde{R}'[s] : s^\infty|_{s=0}$ by using the conditions of Definition 4.4. The δ-regularity of J in $K(s)[x_0, \ldots, x_n]$ (see the proof Lemma 5.3) and Proposition 4.2 imply that

$$\Big(\Big(J\tilde{R}'[s] + \langle y_1, \ldots, y_{n-k+1}\rangle\Big) : s^\infty|_{s=0}\Big)_\delta = \tilde{R}'_\delta.$$

Thus the the equality $(J' + \langle y_1, \ldots, y_{n-k+1}\rangle)_\delta = \tilde{R}'_\delta$ with $J' = J\tilde{R}'[s] : s^\infty|_{s=0}$ follows from Lemma 5.3. The fact that the sequence of generic linear forms $y_1, \ldots, y_{n-k+1}$ is almost regular in degree δ on J' comes from the claim which is proved in Lemma 5.3. Hence the ideal J' is δ-regular. This implies that the ideal $J : s^\infty|_{s=0}$ which is the same ideal over the field K is also δ-regular in the ring $\tilde{R}$ by Lemma 2.1 of [BG03].

The last assertion follows from the above proof and from the Quillen definition of the Castelnuovo-Mumford regularity of an ideal. □

The following theorem summarizes the results of this section.

Theorem 5.1 *The ideal $J : s^\infty|_{s=0}$ is δ-regular and its Macaulay matrix may be computed in a time which is polynomial in $\mathcal{T}$.*

6 Localizing by x_0

The aim of this section is to show that from the Macaulay matrix in degree $nD - n + 1$ of $J' = J : s^\infty|_{s=0}$ we can compute that of the ideal $J' : x_0^\infty = \tilde{I} : x_0^\infty$ within a bit complexity which is polynomial in $\mathcal{T}$.

To pass from a Macaulay matrix of J' to a Macaulay matrix of $J' : x_0^\infty$ we have to prove first that the regularity do not increases and then all the computations may be done without changing the degree.

We have not succeed to prove the following lemma when $\dim L > 1$. This is the only step which keeps us from proving Conjecture 2.1.

Lemma 6.1 *Let $L \subset \tilde{R} = K[x_0, \ldots, x_n]$ be a homogeneous ideal of dimension 1 which is δ-regular for a positive integer δ. Then the ideal $L : x_0$ is δ-regular.*

Proof By Proposition 4.2 we have to check the conditions of Definition 4.4. Let $y = \sum_{i=0}^n A_i x_i$ be a generic linear form where the A_i are new indeterminates. We show first that y is almost regular in degree δ on $L : x_0$. Let P be a homogeneous polynomial of degree $\delta - 1$ such that $yP \in L : x_0$. Thus $yx_0P \in L$. The δ-regularity of L implies that the generic form y is a non zero divisor in degree $\delta + 1$ in $\tilde{R}'/L$ with $\tilde{R}' = K(A_0, \ldots, A_n)[x_0, \ldots, x_n]$. It

follows that $x_0 P \in L$ and y is almost regular in degree δ on $L : x_0$. We have also (Proposition 4.2 and Definition 4.4)

$$(L : x_0 + \langle y \rangle)_\delta \supset (L + \langle y \rangle)_\delta = \tilde{R}'_\delta$$

and this ends the proof. □

Conjecture 6.1 *Lemma 6.1 is true without the hypothesis on the dimension.*

The remainder of the paper has been written in a way which would prove Conjecture 2.1 if Conjecture 6.1 is true. We will quote the results depending on this by the words "under the hypotheses of Lemma 6.1".

Corollary 6.1 *With Notation 3.1, suppose that $f_1, \ldots, f_k$ is a regular sequence. Then the ideal $\tilde{I} : x_0^\infty$ is δ-regular with $\delta = nD - n + 1$.*

Proof By the second item of Proposition 3.1 we have $\tilde{I} : x_0^\infty = J' : x_0^\infty$ where $J' = J : s^\infty|_{s=0}$. Thus the assertion follows from δ-regularity of J' (Proposition 5.2) and from the fact that the saturated ideal of a δ-regular ideal is always δ-regular (because localization preserves regularity). □

Now we show that all the computations needed to compute a Macaulay matrix of $J' : x_0^\infty$ with $J' = J : s^\infty|_{s=0}$ may be done in degree δ.

Lemma 6.2 *Under the hypotheses and the notations of Lemma 6.1 we have:*

$$(L : x_0)_\delta = L_\delta + (\langle (L : x_0)_{\delta-1} \rangle)_\delta \,.$$

Proof To prove the assertion, it is enough to show that any polynomial $P \in L : x_0$ of degree δ belongs to $L + \langle (L : x_0)_{\delta-1} \rangle$. The δ-regularity implies the existence of generic linear forms $y_i = \sum_{j=0}^n A_{i,j} x_j$ for $i = 1, \ldots, d = \dim L$ such that

$$(L + \langle y_1, \ldots, y_d \rangle)_\delta = \tilde{R}'_\delta.$$

Hence P may be written as $P = P' + \sum_{i=1}^d y_i H_i$ with $P' \in L$ and $H_i \in \tilde{R}'$. We have to prove that $\sum_{i=1}^d y_i H_i \in \langle (L : x_0)_{\delta-1} \rangle$. From the latter equality we have $y_d H_d \in L : x_0 + \langle y_1, \ldots, y_{d-1} \rangle$. This implies that $H_d \in L : x_0 + \langle y_1, \ldots, y_{d-1} \rangle$. In fact, Lemma 6.1 ($\delta$-regularity of $L : x_0$) and Lemma 1.8 of [BS87] (adding a sequence of generic linear forms to an ideal does not change its δ-regularity) show that $L : x_0 + \langle y_1, \ldots, y_{d-1} \rangle$ is δ-regular, and thus that the generic form y_d is almost regular in degree δ on $L : x_0 + \langle y_1, \ldots, y_{d-1} \rangle$. Thus H_d may be written as $H_d = P'_d + \sum_{i=1}^{d-1} y_i H'_i$ with $P'_d \in L : x_0$ of degree $\delta - 1$ and $H'_i \in \tilde{R}'$ for any i. By replacing H_d by $P'_d + \sum_{i=1}^{d-1} y_i H'_i$ we have $\sum_{i=1}^d y_i H_i = y_d P'_d + \sum_{i=1}^{d-1} y_i H''_i$ where $y_d P'_d \in \langle (L : x_0)_{\delta-1} \rangle$ and $H''_i \in \tilde{R}'$ for any i. Thus it suffices to show that $\sum_{i=1}^{d-1} y_i H''_i \in \langle (L : x_0)_{\delta-1} \rangle$ which can be proved as above by induction on d. □

These results show that the Macaulay matrix in degree δ of $L : x_0^\infty$ may be deduced from that of L by linear algebra operations. However, $L : x_0^\infty$ is obtained by iterating

the construction of $L : x_0$. Without care this would induce an exponential growth of the coefficients, which may be avoided by the following method.

Given a matrix of the shape $\begin{bmatrix} M & M_0 \\ 0 & M_i \end{bmatrix}$. We carry out a partial Gaussian elimination on its columns in the following way: We label the pivots in the upper most row and in the upper part, as long as possible. Then we permute the columns in order to get a matrix of the shape $\begin{bmatrix} M'_0 & 0 \\ M'_i & M' \end{bmatrix}$ such that the ranks of M'_0 and M'_i are equal to their number of columns.

Lemma 6.3 *Under the hypotheses of Lemma 6.1, let M (which will be denoted by Λ) and M_i for $i = 0, \ldots, n$ be Macaulay matrices in degree δ of L and $\langle x_i \rangle$. Then after above Gaussian elimination, M' is a Macaulay matrix in degree δ of $x_i \langle L : x_0 \rangle_{\delta-1}$.*

Proof The columns of M_0 (resp. M_i) are the representation on the basis of the monomials of a generating set of the polynomials of degree δ of the form $x_0 P$ (resp. $x_i P$). The way in which the Gaussian elimination is done shows that the columns of M' represent the polynomials of the form $x_i P$ such that $x_0 P \in L$.

□

With the notations of Lemma 6.3, let r be the number of rows of Λ. For a given matrix $X = \left[\frac{X_1}{X_2}\right]$ such that X_2 has r rows, let $G(X, i)$ be the following matrix

$$\left[\begin{array}{c|c|c} X_1 & 0 & 0 \\ \hline X_2 & M_0 & 0 \\ \hline 0 & M_i & \Lambda \end{array}\right].$$

Define $\Gamma_0^{(0)} = \Lambda$, $\Gamma_j^{(i)} = G(\Gamma_{j-1}^{(i)}, j)$ for $j = 1, \ldots, n$ and $\Gamma_0^{(i)} = \Gamma_n^{(i-1)}$ for any positive integer i. Thus the matrix $\Gamma_n^{(i)}$ (denoted by $\Gamma^{(i)}$) has the shape

$$\begin{bmatrix}
\Lambda & M_0 & & & & & & & & & & \\
 & M_1 & \Lambda & M_0 & & & & & & & & \\
 & & & \ddots & & & & & & & & \\
 & & & & M_n & \Lambda & M_0 & & & & & \\
 & & & & & & M_1 & \Lambda & M_0 & & & \\
 & & & & & & & & \ddots & & & \\
 & & & & & & & & & M_n & \Lambda & M_0 \\
 & & & & & & & & & & & M_n \quad \Lambda
\end{bmatrix}$$

with $in+1$ blocks of r rows. Therefore with these notations we have the following corollary.

Corollary 6.2 *With the notations of Lemma 6.3, let $L(0) = L_\delta$ and $L(i) = (L(i-1))_{\delta,i}$ for any i. Let also $L^{(0)} = L_\delta$ and $L^{(i)} = L^{(i-1)}(n)$. A Macaulay matrix in degree δ of the ideal $L^{(i)}$ in echelon form appears as a sub-matrix of the result of the Gaussian elimination on $\Gamma^{(i)}$. This sub-matrix consists in the last r rows and in the columns which are null outside of these last r rows.*

Proof A Gaussian reduction on $\Gamma^{(i)}$ is equivalent to a succession of Gaussian elimination on sub matrices with the shape of lemma 6.3, with $M = \Lambda$ at the first step and $M = \begin{bmatrix} M' & \Lambda \end{bmatrix}$ otherwise with M' the output of the preceding step.

□

Lemma 6.4 *Under the hypotheses of Lemma 6.1 and with notations of Corollary 6.2 we have:*

$$(L : x_0^i)_\delta \subset L^{(i)} \subset (L : x_0^\infty)_\delta$$

for any positive integer i.

Proof The second inclusion is trivial from the definition of the notation. To prove the first one, we proceed by induction on i. For $i = 1$, let $P \in L : x_0$ be a homogeneous polynomial of degree δ. Thus using Lemma 6.2, P may be written as $P_0 + \sum_{i=1}^n x_i P_i$ where $P_0 \in L$ and $P_i \in L : x_0$. This implies that $P \in L^{(1)}$ because $P_0 \in L^{(1)}$ and $x_i P_i \in L_{\delta,i} \subset L^{(1)}$ by the definition of the notation.

Now, let $i \geq 2$ and suppose that the assertion is true for $i-1$. Thus the δ-regularity of $L : x_0$ (Lemma 6.1) implies that

$$((L : x_0) : x_0^{i-1}) \subset (L : x_0)^{(i-1)}$$

by the hypothesis of induction. Thus the assertion follows from the fact that $(L : x_0)^{(i-1)}$ is contained in $(L^{(1)})^{(i-1)} = L^{(i)}$ by the definition of the notation. □

Proposition 6.1 *Let $L \subset \tilde{R} = K[x_0, \ldots, x_n]$ be a homogeneous ideal which is δ-regular for a positive integer δ. If the Macaulay matrices of $L^{(i)}$ and $L^{(i+1)}$ obtained by Corollary 6.2 have the same number of columns then i is less than or equal to the number of monomials of degree $\delta - 1$ in $n+1$ variables and, under the hypotheses of Lemma 6.1, we have $L^{(i)} = (L : x_0^\infty)_\delta$.*

Proof To prove the first assertion, let Λ be the Macaulay matrix in degree δ of L. Then we have

$$\dim_K L^{(0)} \leq \dim_K L^{(1)} \leq \cdots \leq \dim_K L^{(i)}$$

where $\dim_K L^{(0)}$ is the rank of Λ and $\dim_K L^{(i)}$ is not greater than the number of columns of $\left[\begin{array}{c|c} M_0 & \Lambda \end{array}\right]$. Thus i is at most the number of columns of M_0 which is equal to the number of monomials of degree $\delta - 1$ in $n+1$ variables.

As $L^{(i)}$ is included in $L^{(i+1)}$, if their Macaulay matrices have the same number of columns then they are equal. It follows immediately that $L^{(i)} = L^{(i+\ell)}$ for any positive integer ℓ. As $L : x_0^\infty = L : x_0^t$ for a positive integer t, Lemma 6.4 implies that $L^{(i)} = (L : x_0^\infty)_\delta$. □

Theorem 6.1 *With Notation 3.1, suppose that $f_1, \ldots, f_k$ is a regular sequence. Then the computation of a Macaulay matrix in degree $\delta = nD - n + 1$ of the ideal $J' : x_0^\infty$ with $J' = J : s^\infty|_{s=0}$ may be done in a time which is polynomial in $\mathcal{T}$. The resulting coefficients have a size bounded by a polynomial in $\mathcal{T}$.*

Proof We split the computation into two steps. We compute first the Macaulay matrix in degree δ of J' which may be done within a bit complexity polynomial in $\mathcal{T}$ by Corollary 5.1. Then from δ-regularity of J' (Proposition 5.2) $J' : x_0^\infty$ may be computed from the latter matrix by doing a Gaussian elimination on $\Gamma^{(i)}$ where i is at most the number r of monomials of degree δ in $n+1$ variables. Thus $\Gamma^{(i)}$ has at most $r(rn+1)$ rows and $r(2rn+1)$ columns. As $n < r \leq \mathcal{T}^{2.5}$ by Lemma 3.2 of [HL05], the size of $\Gamma^{(i)}$ is polynomial in $\mathcal{T}$ and the same is true for the complexity of its Gaussian elimination.

□

7 Generic position and proof of Proposition 2.1

In this section, we give a precise definition of the notion of variables in generic position for an ideal $I = \langle f_1, \ldots, f_k \rangle \subset K[x_1, \ldots, x_n]$. We give also the proof of Proposition 2.1 on the degree of the Gröbner basis of an ideal generated by a regular sequence. Therefore we suppose in all this section that $f_1, \ldots, f_k$ is a regular sequence.

For our definition of generic position, we need to recall the definition of the *Hilbert series* of an ideal $I \subset R = K[x_1, \ldots, x_n]$ (not necessarily homogeneous). It is the series

$$\mathrm{HS}_I(t) = \sum_{i=0}^{\infty} \dim_K \left(\frac{R}{I}\right)_{\leq d} t^i$$

where $\dim_K (R/I)_{\leq d}$ denotes the dimension as a vector space over K, of the set of elements of degree at most d of R/I. Remark that by this definition, the Hilbert series of I and that of its homogenization are equal (see Theorem 12 of [CLO97] page 434).

Now, we are able to define variables in generic position.

Definition 7.1 *Let I be an ideal of the ring $K[x_1, \ldots, x_n]$. A linear polynomial $y \in R$ is in* generic position *for I if the ideal $I + \langle y \rangle$ has the same Hilbert series as that of the ideal $I + \langle A_0 + \sum_{i=1}^n A_i x_i \rangle$ in the ring $K(A_0, \ldots, A_n)[x_1, \ldots, x_n]$, where the A_i are the new indeterminates.*

Definition 7.2 *A linear sequence $y_1, \ldots, y_\ell$ is in* generic position *for I if y_i is in generic position for $I + \langle y_1, \ldots, y_{i-1} \rangle$ for $i = 1, \ldots, \ell$.*

In the following proposition we show that almost all of the linear sequences in the ring $K[x_1, \ldots, x_n]$ are in generic position for a given ideal. For this, we recall first some definitions. Let A be a set of indeterminates and X be a set of unknowns. Let also $<_A$ (resp. $<_X$)

be a degree ordering on monomials in A (resp. X). By a *degree block ordering* we mean an ordering $<$ such that, if a, a' (resp. m, m') are monomials in A (resp. X) then $am < a'm'$ if and only if $m < m'$ or ($m = m'$ and $a < a'$). Recall also that the *Zariski topology* on K^n is the topology which has the algebraic sets as closed sets, i.e. a set V is closed if and only if there exists a (finite) family of polynomials $f_1, \ldots, f_k$ such that:

$$V = \{x \in K^n \mid \ f_1(x) = \cdots = f_k(x) = 0\}.$$

It is well-known that a non empty Zariski open set is dense.

Proposition 7.1 *Let I be an ideal of the ring $R = K[x_1, \ldots, x_n]$. If K is infinite, the set of linear sequences in generic position for I contains a dense Zariski open set.*

Proof Let us consider the linear forms $Y_i = A_{i,0} + \sum_{j=1}^n A_{i,j}x_j$ where the $A_{i,j}$ are new indeterminates and $y_i = a_{i,0} + \sum_{j=1}^n a_{i,j}x_j$ where $a_{i,j} \in K$ for $i = 1, \ldots, \ell$. We have to compare the Hilbert series of $I + \langle y_1, \ldots, y_i\rangle \subset R$ and that of $I + \langle Y_1, \ldots, Y_i\rangle \subset K(A_{1,0}, \ldots, A_{i,n})[x_1, \ldots, x_n]$ for $i = 1, \ldots, \ell$. The Hilbert series of an ideal is the same as that of its initial ideal, which is generated by the initials (leading terms) of the elements of a Gröbner basis for a degree compatible ordering (see [CLO97] p. 433 for example). Let G_i be a Gröbner basis of $I + \langle Y_1, \ldots, Y_i\rangle \subset K[A_{1,0}, \ldots, A_{i,n}][x_0, \ldots, x_n]$ for a degree block ordering and let C_i be the product of the initial coefficient of its elements. It is easy and classical that if $C_i(a_{1,0}, \ldots a_{i,n}) \neq 0$ then the substitution of the $A_{i,j}$ by the $a_{i,j}$ in G_i gives a Gröbner basis of $I + \langle y_1, \ldots, y_i\rangle$ (see [CLO97] p. 279 for example). Thus the set of the $y_1, \ldots, y_\ell$ which are in generic position for I contains the complement of the hyper-surface of equation $\prod_{i=1}^{\ell} C_i = 0$, which is open and dense. □

We prove below that if the last variables $x_{k+1}, \ldots, x_n$ are in generic position for an ideal generated by a regular sequence then $x_{k+1}, \ldots, x_n, x_0$ is a regular sequence in the quotient of $\tilde{R}$ by the homogenized ideal.

Lemma 7.1 *Let I be an ideal of the ring $R = K[x_1, \ldots, x_n]$, and let $y \in R$ be a linear polynomial. Then y is a non zero divisor in R/I if and only if*

$$\dim_K \left(\frac{R}{I + \langle y\rangle}\right)_{\leq i+1} = \dim_K \left(\frac{R}{I}\right)_{\leq i+1} - \dim_K \left(\frac{R}{I}\right)_{\leq i}$$

for any positive integer i. In the homogeneous case, the same equality holds with $\leq$ removed.

Proof By hypotheses we have the following exact sequence of vector spaces

$$\left(\frac{R}{I}\right)_{\leq i} \xrightarrow{y} \left(\frac{R}{I}\right)_{\leq i+1} \longrightarrow \left(\frac{R}{I + \langle y\rangle}\right)_{\leq i+1} \longrightarrow 0.$$

By the additivity property of the dimension, the first map is injective if and only if the above equality on the dimensions holds, and we have this injectivity for all i if and only if y is a non zero divisor in R/I. In the homogeneous case, the proof is exactly the same. □

Recall that an ideal I is called *equidimensional* if any associated prime ideal of I has dimension $\dim I$.

Lemma 7.2 *With Notation 3.1, suppose that $f_1, \ldots, f_k$ is a regular sequence and $k < n$. Let $y \in R$ be a homogeneous linear polynomial which is in generic position for $I = \langle f_1, \ldots, f_k \rangle$. Then*

- *y is a non zero divisor in R/I and in $\tilde{R}/(\tilde{I} : x_0^\infty)$;*
- *$(\tilde{I} + \langle y \rangle) : x_0^\infty = \tilde{I} : x_0^\infty + \langle y \rangle$.*

Proof We know that an ideal generated by a regular sequence is equidimensional and that an element is a non zero divisor if and only if it is not contained in any associated prime of the ideal. Thus the inequality $k < n$ implies that a generic linear form is a non zero divisor, and the definition of generic position implies the first assertion. The assertion on $\tilde{R}/(\tilde{I} : x_0^\infty)$ is proved similarly using the fact that $\tilde{I} : x_0^\infty$ is equidimensional of dimension $n - k + 1$ (see [Frö97] p. 109 for example).

The inclusion "$\supset$" of the second item is immediate from the definition of the notation. Therefore, it is enough to show that the vector spaces $\left(\tilde{R}/(\tilde{I} + \langle y \rangle) : x_0^\infty\right)_i$ and $\left(\tilde{R}/(\tilde{I} : x_0^\infty + \langle y \rangle)\right)_i$ have the same dimension for any i. By Lemma 7.1 the dimension of the first space is equal to

$$\dim_K \left(\frac{R}{I + \langle y \rangle}\right)_{\leq i} = \dim_K \left(\frac{R}{I}\right)_{\leq i} - \dim_K \left(\frac{R}{I}\right)_{\leq i-1}$$

and the dimension of the second one is

$$\dim_K \left(\frac{\tilde{R}}{\tilde{I} : x_0^\infty + \langle y \rangle}\right)_i = \dim_K \left(\frac{\tilde{R}}{\tilde{I} : x_0^\infty}\right)_i - \dim_K \left(\frac{\tilde{R}}{\tilde{I} : x_0^\infty}\right)_{i-1}.$$

The conclusion follows from the equality $\dim_K \left(\frac{R}{I}\right)_{\leq i} = \dim_K \left(\frac{\tilde{R}}{\tilde{I} : x_0^\infty}\right)_i$ which is true for any ideal and any i. □

Theorem 7.1 *With Notation 3.1, suppose that $f_1, \ldots, f_k$ is a regular sequence and that the sequence $x_{k+1}, \ldots,$*
x_n is in generic position for I. Then $x_{k+1}, \ldots, x_n, x_0$ is a regular sequence in $\tilde{R}/(\tilde{I} : x_0^\infty)$.

Proof It suffices to prove that the sequence $x_{k+1}, \ldots, x_n$ is a regular in R/I and in $\tilde{R}/(\tilde{I} : x_0^\infty)$ and that

$$(\tilde{I} + \langle x_{k+1}, \ldots, x_n \rangle) : x_0^\infty = \tilde{I} : x_0^\infty + \langle x_{k+1}, \ldots, x_n \rangle.$$

We prove these three assertions by an induction on i, the number of variables in generic position for I. For $i = 1$ this is Lemma 7.2. Let $i \geq 2$ and suppose that the assertions are true for $i - 1$. Thus the regularity of the sequence $f_1, \ldots, f_k, x_{k+1}, \ldots, x_{i-1}$ (hypothesis of the induction) implies that x_i is a non zero divisor in

$$\frac{\tilde{R}}{(\tilde{I} + \langle x_{k+1}, \ldots, x_{i-1} \rangle) : x_0^\infty} = \frac{\tilde{R}}{\tilde{I} : x_0^\infty + \langle x_{k+1}, \ldots, x_{i-1} \rangle}$$

and this proves the first part of the claim. The second one comes from the hypothesis and the second item of Lemma 7.2. □

We prove now Proposition 2.1. Recall that the degree reverse lexicographic monomial ordering, denoted by $\prec$, in $\tilde{R} = K[x_1, \ldots, x_{n+1}]$ with $x_{n+1} = x_0$ is defined on monomials of the same degree by $x_1^{\alpha_1} \cdots x_{n+1}^{\alpha_{n+1}} \prec x_1^{\beta_1} \cdots x_{n+1}^{\beta_{n+1}}$ if the last non-zero entry of the vector $(\beta_1 - \alpha_1, \ldots, \beta_{n+1} - \alpha_{n+1})$ is negative. (This ordering on the variables is important in what follows.) For $P \in \tilde{R}$, let $\mathrm{in}(P) \in \tilde{R}$ be the greatest monomial (leading term) of P with respect to $\prec$.

Recalling also that the rows of a Macaulay matrix are indexed by monomials, we suppose in the following that the rows are indexed by $\prec$ in decreasing order.

Proposition 7.2 *With Notation 3.1, let M be a Macaulay matrix in column echelon form of $\tilde{I} : x_0^\infty$ in the degree of regularity of this ideal, and let $x_{k+1}, \ldots, x_n$ be in generic position for I. If $P_1, \ldots, P_t$ are the polynomials defined by the columns of M then $\{P_1|_{x_0=1}, \ldots, P_t|_{x_0=1}\}$ is a Gröbner basis of $I = \tilde{I} : x_0^\infty|_{x_0=1}$ with respect to $\prec$.*

Proof Let $f \in I$ be an arbitrary polynomial and let F be its homogenization with respect to x_0. If $\deg(f) < \delta$ where δ is the regularity of $I' = \tilde{I} : x_0^\infty$, then we replace F by $x_0^{\delta - \deg(f)} F$. Thus it is enough to show that F, which has a degree at least δ, is reducible by $G = \{P_1, \ldots, P_t\}$. If $deg(F) = \delta$ we are done because G generates I'_δ as vector space. If $\deg(F) > \delta$ two cases are possible.

In the first case, there exists some i in $\{k+1, \ldots, n+1\}$ such that $x_i \mid \mathrm{in}(F)$. Choose i maximal for this property. In this case, we show that F may be replaced by a polynomial which has degree δ and thus F is reducible by G. Let F' be the sum of the terms m of F such that $x_i \mid m$. Then $F - F'$ belongs to $\langle x_{i+1}, \ldots, x_{n+1} \rangle$ by definition of the ordering $\prec$, and $F' \in I' + \langle x_{i+1}, \ldots, x_{n+1} \rangle$. It follows that $F'/x_i \in I' + \langle x_{i+1}, \ldots, x_{n+1} \rangle$ because x_i is non zero divisor in $\tilde{R}/(I' + \langle x_{i+1}, \ldots, x_{n+1} \rangle)$ by Theorem 7.1 (any permutation of a homogeneous regular sequence remains a regular sequence). Let $P \in I'$ such that $F'/x_i - P \in \langle x_{i+1}, \ldots, x_{n+1} \rangle$. As, by assumption, $x_{i+1}, \ldots, x_{n+1}$ do not appear in $\mathrm{in}(F)/x_i = \mathrm{in}(F')/x_i$, the definition of $\prec$ implies that $\mathrm{in}(P) = \mathrm{in}(F')/x_i = \mathrm{in}(F)/x_i$. Thus $\mathrm{in}(F)$ is reducible by an element of I' of degree $\deg(F) - 1$. By induction on $\deg(F)$, this implies that $\mathrm{in}(F)$ is multiple of $\mathrm{in}(F'')$ where $F'' \in I'$ has degree δ.

In the other case we use the fact that $I' + \langle x_{k+1}, \ldots, x_{n+1} \rangle$ is a zero–dimensional ideal which is δ-regular. In fact it is zero–dimensional because of the dimension $n - k + 1$ of I' (Proposition 5.2) and of the regularity in $\tilde{R}/I'$ of the sequence $x_{k+1}, \ldots, x_{n+1}$ (Theorem 7.1). This δ-regularity comes from the fact that the δ-regularity of an ideal does not change if one adds a regular sequence to it (Lemma 1.8 of [BS87]). By Lemma 1.7 of [BS87] this proves

$$(I' + \langle x_{k+1}, \ldots, x_{n+1} \rangle)_\delta = \tilde{R}_\delta.$$

Now let m be any monomial of degree δ dividing $\mathrm{in}(F)$. It may be written $m = F' + x_{k+1}H_{k+1} + \cdots + x_{n+1}H_{n+1}$ with $F' \in I'$ and $H_i \in \tilde{R}$ for any i. This implies that m is the leading term of F' by the definition of $\prec$ and F is reducible by F' which is itself reducible by G, by above proof. □

Corollary 7.1 (Proposition 2.1) *With Notation 3.1, the Macaulay matrix in degree* $\delta = nD - n + 1 = d_1 + \cdots + d_k - k + 1$ *of the ideal* $\tilde{I} : x_0^\infty$ *gives a Gröbner basis of* I *with respect to the degree reverse lexicographic ordering. If* $k = n$ *this Gröbner basis may be computed in a time which is polynomial in* $\mathcal{T}$ *(Theorem 6.1)*

Proof Since $\tilde{I} : x_0^\infty$ is a δ-regular ideal by Corollary 6.1 then the assertions follows from Proposition 7.2. □

Remark 1 *To prove Conjecture 2.1 i.e. that this Gröbner basis may be computed within a bit complexity which is polynomial in* $\mathcal{T}$ *it would "suffice" to prove that the algorithm of Section 6 computes a Macaulay matrix of* $J' : x_0^\infty$ *if* $k < n$.

8 Zero–dimensional Gröbner basis

In this section, we suppose that $I = \langle f_1, \ldots, f_k \rangle$ is a zero–dimensional ideal. Following Corollary 2.2 we suppose that the total degrees of the f_i satisfy $d_2 \geq \cdots \geq d_k \geq d_1 \geq 2$ and we set $D = (d_1 + \cdots + d_n)/n$. We will prove Theorem 2.1. More precisely, we give the bound $nD - n + 1$ for the degree of the elements of the reduced Gröbner base of I with respect to the degree reverse lexicographic ordering and the bound D^n for any ordering. We provide also an algorithm which computes any reduced Gröbner basis of I within a bit complexity which is polynomial in $\mathcal{T} = \max\{T, D^n\}$ with T the total size of the input polynomials. Finally, we prove the upper bound $(n-1)D^n + 1$ for the number of the elements of the reduced Gröbner basis of I with respect to any ordering.

To prove the main theorem of this section (Theorem 8.1) we use the following lemmas.

Lemma 8.1 *Let* $L \subset \tilde{R} = K[x_0, \ldots, x_n]$ *be a homogeneous ideal of dimension* 1 *which is* δ*-regular for some integer* δ. *Let* $P_1, \ldots, P_\ell \in \tilde{R}$ *be the homogeneous polynomials of degree at most* d. *Then* $L + \langle P_1, \ldots, P_\ell \rangle$ *is* $(\delta + d)$*-regular.*

Proof By Proposition 4.2 we have to check the conditions of Definition 4.4 for the ideal $L + \langle P_1, \ldots, P_\ell \rangle$. From δ-regularity of L and its dimension there exists a generic linear form $y = \sum_{i=0}^n A_i x_i$ such that the multiplication

$$y : \left(\frac{\tilde{R}'}{L}\right)_{\delta-1} \longrightarrow \left(\frac{\tilde{R}'}{L}\right)_{\delta} \tag{2}$$

with $\tilde{R}' = K(A_0, \ldots, A_n)[x_0, \ldots, x_n]$ is an isomorphism. Thus it suffices to show that y is almost regular in degree $\delta + d$ on $L + \langle P_1, \ldots, P_\ell \rangle$. For this let F be a homogeneous polynomial of degree $\delta + d - 1$ such that $yF \in L + \langle P_1, \ldots, P_\ell \rangle$. Thus we have

$$yF + \sum_{i=1}^{\ell} H_i P_i \in L_{\delta+d} \tag{3}$$

with $H_i \in \tilde{R}'$. This implies that H_i has a degree at least δ (by the hypotheses $\deg(P_i) \leq d$), and it may therefore be written as $H_i = G_i + yH_i'$ with $G_i \in L$ and $H_i' \in \tilde{R}'$, by the surjectivity of (2). So by replacing the H_i by $G_i + yH_i'$ in (3) we have $yF + \sum_{i=1}^{\ell} yH_i'P_i \in L_{\delta+d}$. The δ-regularity of L implies that the generic form y is a non zero divisor in degree $\delta + d$ in $\tilde{R}'/L$. It follows that $F + \sum_{i=1}^{\ell} H_i'P_i \in L_{\delta+d-1}$, which ends the proof. □

Let us recall that the *saturated* ideal of a homogeneous ideal $L \subset \tilde{R} = K[x_0, \ldots, x_n]$ is defined by

$$L^{sat} = L : \mathfrak{m}^{\infty}$$

where $\mathfrak{m}$ is the unique maximal homogeneous ideal of $\tilde{R}$ and

$$L : \mathfrak{m}^{\infty} = \{P \in \tilde{R} \mid x_i^t P \in L \text{ for some } t \text{ and for any } i\}.$$

We will use the fact that $L^{sat}.K(A_0, \ldots, A_n)[x_0, \ldots, x_n] = L : y^{\infty}$ where $y = \sum_{i=0}^{n} A_i x_i$ is a generic linear form.

Lemma 8.2 *Under the hypotheses of Lemma 8.1 suppose that $L = L : x_0$. Then we have*

$$((L + \langle P_1, \ldots, P_\ell \rangle) : x_0^{\infty})_{\delta+d} = (L + \langle P_1, \ldots, P_\ell \rangle)_{\delta+d}.$$

Proof The inclusion "$\supset$" is immediate. To prove the other inclusion, let $F \in L_1 : x_0^{\infty}$ with $L_1 = L + \langle P_1, \ldots, P_\ell \rangle$ be a polynomial of degree $\delta + d$. We claim that $F \in L_1^{sat}$. It follows that $y^t F \in L_1$ for some t and therefore $F \in L_1$ by the $(\delta + d)$-regularity of L_1 (Lemma 8.1).

Proof of the claim: We show that $L_1 : x_0^{\infty} = L_1^{sat}$. To prove it, we have to show that the saturation of L_1 by x_0 is the same as its saturation by $\mathfrak{m}$ or, equivalently, that $\mathfrak{m}$ is the only associated prime of L_1 which contains x_0. For this let $Q \in \mathrm{Ass}(L_1)$ be an associated prime of L_1. Thus $Q \supset Q'$ for some $Q' \in \mathrm{Ass}(L)$. Then two cases are possible: If $\dim Q = \dim Q'$, we have $Q = Q'$, and therefore Q does not contain x_0 because $L = L : x_0$. In the other case we have $Q = \mathfrak{m}$ (and therefore it contains x_0) because $\dim Q < \dim Q' \leq \dim L = 1$ by the hypotheses, and this proves the claim. □

Now we state the main result of this section.

Theorem 8.1 *Let $I = \langle f_1, \ldots, f_k \rangle$ be a zero–dimensional ideal of $R = K[x_1, \ldots, x_n]$ such that the degrees of the f_i satisfy $d_2 \geq \cdots \geq d_k \geq d_1 \geq 2$. Let G be the reduced Gröbner basis of I with respect to the degree reverse lexicographic ordering . Then G may be computed within a bit complexity which is polynomial in $\mathcal{T} = \max\{T, D^n\}$ where T is the total size of the input polynomials and $D = (d_1 + \cdots + d_n)/n$.*

Moreover, the elements of G have a degree at most $nD - n + 1$.

Proof By Corollary 2.3 we may suppose without lost of generality that $f_1, \ldots, f_n$ is a regular sequence in R. Let $\delta = nD - n + 1$ and let $I' = \langle F_1, \ldots, F_n \rangle : x_0^{\infty}$ where F_i is the homogenization of f_i with respect to x_0. The ideal I' is δ-regular (Lemma 6.1) and this implies (Lemma 8.2) that

$$\left(\tilde{I} : x_0^{\infty}\right)_{\delta+d} = (I' + \langle F_{n+1}, \ldots, F_k \rangle)_{\delta+d} \tag{4}$$

where $\tilde{I}$ is the ideal generated by $F_1, \ldots, F_k$ and $d = d_{n+1}$ is the maximum of the degrees of $F_{n+1}, \ldots, F_k$. So $\tilde{I} : x_0^\infty$ is an ideal $(\delta + d)$-regular by Lemma 8.1 and Proposition 7.2 shows that the Gröbner basis G may be deduced from the column echelon form of a Macaulay matrix of $\tilde{I} : x_0^\infty$ in degree $\delta + d$. This Macaulay matrix may be obtained by the concatenation of the Macaulay matrices of I' and $\langle F_{n+1}, \ldots, F_k \rangle$. By Theorem 6.1, a Macaulay matrix in echelon form of I' in degree δ may be computed within a complexity polynomial in $\mathcal{T}$ and the size of its coefficients is also polynomial in $\mathcal{T}$. Let $C_1, \ldots, C_\ell$ be the polynomials (of degree δ) associated to the columns of this matrix. The Macaulay matrix in degree $\delta + d$ we are looking for is the usual Macaulay matrix of $\langle C_1, \ldots, C_\ell, F_{n+1}, \ldots, F_k \rangle$. Its number of rows is

$$\binom{\delta + d + n}{n} < \binom{n(2D) + 1}{n} < (2eD)^n$$

by Lemma 3.2 of [HL05]. Its number of columns is bounded by $(\ell + k - n)\binom{\delta+d+n}{n}$. As the Macaulay matrix of I' is supposed to be in column echelon form, its number of columns is less than its number of rows. It follows that the number of columns of the Macaulay matrix in degree $\delta + d$ is less than $(T + (2eD)^n)(2eD)^n$, which is polynomial in $\mathcal{T}$. Thus the bit complexity of the computation of the echelon form of this Macaulay matrix, and the Gröbner basis G is polynomial in $\mathcal{T}$.

Let us consider now the assertion on the degrees. By Proposition 2.1, the elements of the reduced Gröbner basis of the ideal $\langle f_1, \ldots, f_n \rangle$ with respect to the degree reverse lexicographic ordering have a degree at most δ. The zero–dimensionality of this ideal and the δ-regularity of I' imply that its initial ideal (the ideal generated by initial terms of the elements of the ideal) contains all monomials of degree δ. Thus the degree of the elements of the reduced Gröbner basis may only decrease when adding the polynomials $f_{n+1}, \ldots, f_k$ to the ideal, and this ends the proof.

□

Now, let us consider another monomial ordering. For this we use [FGLM93], where it is provided an algorithm for transforming a Gröbner basis of a zero–dimensional ideal with respect to any ordering into a Gröbner basis with respect to another ordering. Under the hypotheses of Theorem 8.1 the bit complexity of this algorithm is polynomial in hnD^n where h is the maximal size of the coefficients of the polynomials of the input basis (see Theorem 5.1 of [HL05]). Thus we have:

Corollary 8.1 *Under the hypotheses of Theorem 8.1 there is an algorithm which computes any reduced Gröbner base of I within a bit complexity which is polynomial in $\mathcal{T}$.*

We give now a bound on the degrees of the elements of any reduced Gröbner basis of a zero–dimensional ideal. Let $\deg(I, <)$ denote the maximum degree of the elements of the reduced Gröbner basis of I with respect to the monomial ordering $<$ and $\mathrm{Deg}(I)$ denote the dimension of K-vector space R/I. Let $\mathrm{in}(f) \in R$ be the initial (greatest) monomial of a polynomial $f \in R$ with respect to the ordering $<$ and

$$\mathrm{in}(I) = \{\mathrm{in}(f) \mid f \in I\}.$$

Proposition 8.1 *Let $I = \langle f_1, \ldots, f_k \rangle$ be a zero–dimensional ideal of $R = K[x_1, \ldots, x_n]$ and let $<$ be a monomial ordering on R. Then*

$$\deg(I, <) \leq \mathrm{Deg}(I).$$

Proof By definition $\mathrm{Deg}(I)$ is the number of monomials m such that $m \notin \mathrm{in}(I)$ (Proposition 4 of Chapter 5, §3 of [CLO97] for example). Let G be the reduced Gröbner basis of I with respect to $<$ and $g \in G$. Let x_i be a variable dividing $\mathrm{in}(g)$. We have $\mathrm{in}(g)/x_i \notin \mathrm{in}(I)$ because G is reduced. Similarly if m is any other monomial of g, then $m \notin \mathrm{in}(I)$. Thus it is enough to show that $\deg(m) < \mathrm{Deg}(I)$ for any monomial m such that $m \notin \mathrm{in}(I)$. Let ℓ be the degree of m. For any $0 \leq i \leq \ell$ there is at least a monomial m_i of degree i dividing m and if $m \notin \mathrm{in}(I)$ the same is true for all the m_i, thus $\ell + 1 < \mathrm{Deg}(I)$ which proves the result. □

Remark 2 With Notation 3.1, if I is a zero–dimensional ideal then we have $\deg(I, <) \leq D^n$. This follows from the facts that the degree of I is bounded by $d_1 \cdots d_n$ (Bézout's theorem) and that $d_1 \cdots d_n \leq D^n$ by the well-known fact that the geometric mean is less than the arithmetic mean.

Example 8.1 We give here a well-known example due to Mora-Lazard- Masser-Philippon-Kollár (see [Bro87] for example) which shows that the degree bound of Proposition 8.1 is optimal. For this, let $<_{lex}$ be the lexicographical ordering on $K[x_1, \ldots, x_n]$ such that $x_1 <_{lex} \cdots <_{lex} x_n$.

For all n and $d_1, \ldots, d_n$, let us consider the following sets of polynomials in $K[x_1, \ldots, x_n]$:

$$A = \{x_1^{d_1} - x_2, x_2^{d_2} - x_3, \ldots, x_{n-1}^{d_{n-1}} - x_n, x_n^{d_n}\}$$

and

$$B = \{x_1^{d_1 \cdots d_n}, x_2 - x_1^{d_1}, x_3 - x_1^{d_1 d_2}, \ldots, x_{n-1} - x_1^{d_1 \cdots d_{n-2}}, x_n - x_1^{d_1 \cdots d_{n-1}}\}.$$

By first Buchberger's criterion (see [CLO97] for example) we can see easily that the set A (resp. B) is a reduced Gröbner basis with respect to any degree ordering (resp. $<_{lex}$). In the other hand by a simple computation we have that any element of A is reducible to 0 by B and vice-versa. Thus these sets generate the same ideal, say I. This implies that $\deg(I, <_{lex}) = d_1 \cdots d_n$. So the claim deduces from the fact that $d_1 \cdots d_n$ is the product of the degrees of the generators of I (I is also generated by A), and it is therefore equal to the degree of I.

In the following, we give a bound for the number of the elements of the reduced Gröbner base of a zero–dimensional ideal with respect to any ordering. Dickenstein et al. [DFGS91] have proved the bound d^{n^2} where d is the maximum degree of the generators of the given ideal and n is the number of the variables, while Faugère et al. [FGLM93] have proved the bound nd^n. We provide a more shaper bound where $|A|$ denotes the number of the elements of a set A.

Theorem 8.2 *Let $I = \langle f_1, \ldots, f_k \rangle$ be a zero–dimensional ideal of the ring $K[x_1, \ldots, x_n]$ and $d_i = \deg(f_i)$ indexed in order that $d_2 \geq \cdots \geq d_k \geq d_1$. Let G be the reduced Gröbner base of I with respect to some ordering. Then the number of polynomials in G is at most*

$$(n-1)\mathrm{Deg}(I) + 1 \leq (n-1)D^n + 1.$$

Proof We apply the idea which is used to prove Corollary 2.1 of [FGLM93]. For this let B be the set of monomials m such that $m \notin \mathrm{in}(I)$. It is easy to see that $|B| + |G|$ is less than or equal to the number of the elements of the set

$$\{1\} \cup \{x_i m \mid m \in B, i = 1, \ldots, n\}.$$

But the number of elements of this set is equal to $1+n\mathrm{Deg}(I)$ because the zero–dimensionality of I implies that $|B| = \mathrm{Deg}(I)$ (Proposition 4 of Chapter 5, §3 of [CLO97]). Thus $|G| \leq (n-1)\mathrm{Deg}(I) + 1$ which is less than $(n-1)D^n + 1$ by Remark 2. □

References

[BCG+91] R. L. Bryant, S. S. Chern, R. B. Gardner, H. L. Goldschmidt, and P. A. Griffiths. *Exterior differential systems*, volume 18 of *Mathematical Sciences Research Institute Publications*. Springer-Verlag, New York, 1991.

[BG03] Isabel Bermejo and Philippe Gimenez. Saturation and Catelnuovo-Mumford regularity of a homogenous ideal. Preprint, 2003.

[Bro87] W. Dale Brownawell. Bounds for the degrees in the Nullstellensatz. *Ann. of Math. (2)*, 126(3):577–591, 1987.

[BS87] David Bayer and Michael Stillman. A criterion for detecting m-regularity. *Invent. Math.*, 87(1):1–11, 1987.

[Can90] John Canny. Generalised characteristic polynomials. *J. Symbolic Comput.*, 9(3):241–250, 1990.

[CH03] Aldo Conca and Jürgen Herzog. Castelnuovo-Mumford regularity of products of ideals. *Collect. Math.*, 54(2):137–152, 2003.

[CLO97] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997. An introduction to computational algebraic geometry and commutative algebra.

[CLO98] David Cox, John Little, and Donal O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998.

[DFGS91] Alicia Dickenstein, Noaï Fitchas, Marc Giusti, and Carmen Sessa. The membership problem for unmixed polynomial ideals is solvable in single exponential time. *Discrete Appl. Math.*, 33(1-3):73–94, 1991. Applied algebra, algebraic algorithms, and error-correcting codes (Toulouse, 1989).

[EG84] David Eisenbud and Shiro Goto. Linear free resolutions and minimal multiplicity. *J. Algebra*, 88(1):89–133, 1984.

[Fau02] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). *ISSAC, ACM Press*, pages 75–83, 2002.

[FGLM93] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symbolic Comput.*, 16(4):329–344, 1993.

[Frö97] Ralf Fröberg. *An introduction to Gröbner bases.* Pure and Applied Mathematics (New York). John Wiley & Sons Ltd., Chichester, 1997.

[GC83] D. Grigoriev and A. Chistov. Subexponential-time solving systems of algebraic equations. I, II. In *LOMI E-9-83, E-10-83, 119 p.* Leningerad, 1983.

[HL05] Amir Hashemi and Daniel Lazard. Sharper complexity bounds for zero–dimensional Gröbner bases and polynomial system solving. Research Report RR-5491, INRIA, February 2005.

[Kap74] Irving Kaplansky. *Commutative rings.* The University of Chicago Press, Chicago, Ill.-London, revised edition, 1974.

[Lak90] Y. N. Lakshman. On the complexity of computing a Gröbner basis for the radical of a zero dimensional ideal. In *Proc. of 22nd ACM Symposium on Theory of computing (STOC)*, pages 555–563. 1990.

[Lak91] Y. N. Lakshman. A single exponential bound on the complexity of computing Gröbner bases of zero-dimensional ideals. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 227–234. Birkhäuser Boston, Boston, MA, 1991.

[Laz81] Daniel Lazard. Résolution des systèmes d'équations algébriques. *Theoret. Comput. Sci.*, 15(1):77–110, 1981.

[Laz83] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Computer algebra (London, 1983)*, volume 162 of *Lecture Notes in Comput. Sci.*, pages 146–156. Springer, Berlin, 1983.

[LL91] Y. N. Lakshman and Daniel Lazard. On the complexity of zero-dimensional algebraic systems. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 217–225. Birkhäuser Boston, Boston, MA, 1991.

[LR05] Daniel Lazard and Fabrice Rouillier. Solving parametric polynomial systems. Technical Report RR-5322, INRIA, October 2005.

[Mat89] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.

[Mum66] David Mumford. *Lectures on curves on an algebraic surface*. With a section by G. M. Bergman. Annals of Mathematics Studies, No. 59. Princeton University Press, Princeton, N.J., 1966.

[Qui64] Daniel Quillen. *Formal properties of overdetermined systems of linear partial equations*. PhD thesis, Harvard University, 1964.

[Sto00] Arne Storjohann. *Algorithms for Matrix Canonical Forms*. PhD thesis, Swiss Federal Institute of Technology, 2000.

[Vil95] Gilles Villard. Generalized subresultants for computing the Smith normal form of polynomial matrices. *J. Symbolic Comput.*, 20(3):269–286, 1995.

[Vil03] Gilles Villard. Algorithmique en algèbre linéaire exacte. Mémoire d'habilitation à diriger des recherches, Université Claude Bernard Lyon 1, 2003.

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)

Unité de recherche INRIA Futurs : Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)
Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399