Minimal generators from reduced Gröbner bases obtained by interpolation methods

Francesca Cioffi[1] and Ferruccio Orecchia*[1]

[1] *Dip. di Matematica e Applicazioni "R. Caccioppoli", Università di Napoli "Federico II", Via Cintia, 80126 Napoli - Italy*

Abstract

In 1982 Buchberger and Möller described a polynomial algorithm to compute a reduced Gröbner basis of the ideal of affine points basing on interpolation methods. This algorithm was an incisive step for a worthwhile progress in computation of zero-dimensional schemes and their applications. The consequent generalization of the original algorithm of Buchberger and Möller to projective points gave space to the problem of minimalizing a homogeneous Gröbner basis even without computing syzygies. Answers to this problem have been already given and applied in several particular cases. The purpose of this paper is to illustrate in a more general context and to improve a method to minimalize reduced Gröbner bases that we have already successfully used in several applications of zero-dimensional computation.

1. Introduction

The Gröbner basis of a polynomial ideal I is a particular set of generators of I introduced by Buchberger in 1965 together with an algorithm for computing them (see, for example, [7] and the references therein for a survey about Gröbner bases). It is very well known that this algorithm takes any set of generators of I as input and is based on a characterization of a Gröbner basis by S-polynomials. This means that the construction of the Gröbner basis involves the construction of syzygies in such a way that minimal generators of a homogeneous ideal I can be singled out among the polynomials of the Gröbner basis itself. Hence, the minimalization of a Gröbner basis of a homogeneous ideal I can occur meanwhile the Gröbner basis is constructed.

However, it can happen that the Gröbner basis is constructed by the algorithm of Buchberger and Möller [8] which takes a set of points as input and is based

*Corresponding author: orecchia@unina.it, tel +39 81 675649, fax +39 81 7662106

on interpolation methods. In this case it can make sense to ask for a minimalization of a reduced Gröbner basis. Answers to this problem have already been given in [17], [11, 12] and, although they are described in the particular case of computation on points, they works well in a more general context. As the study of zero-dimensional schemes can give information also on positive dimensional schemes, in several cases the algorithm of Buchberger and Möller, which is applied to points [1, 2, 13, 17], turns out to be useful also for positive dimensional varieties: for example, it is the starting point in [3, 20] for implicitation methods that are alternative to the Gröbner bases technique, in [10] for the construction of elliptic curves and in [19] for the study of minimally generated rational curves. Moreover, the fact that in [5, 6] the shape of reduced Gröbner bases of some affine space curves is described quite only by geometric tools contributes to not excluding that in some cases a Gröbner basis could be constructed by alternative methods.

Hence, it seemed worthwhile to us to stress in this paper the applicability of the method of minimalization arisen for points in [11, 12] to any homogeneous ideal together with an improvement that we describe in details in section 4. An implementation of just this algorithm has been prepared in the object-oriented language C++ over a field K of positive characteristic p in a program compiled using g++ and NTL 5.2 [23] that is available at `http://cds.unina.it/~cioffifr`. It is applicable to reduced Gröbner bases with respect to (w.r.t.) the graded reverse lexicographic (deg-rev-lex) term order, because this order is the most suitable for a minimalization [4]. In section 3 we illustrate the algorithm and in section 5 report some tests.

2. Notation and basic facts

Let $S = K[x_0, \ldots, x_r]$ be the ring of polynomials in $r+1$ variables over a field K, S_d be the K-vector space that consists of the homogeneous polynomial of S of degree d and $I = \bigoplus_{d\geq 0} I_d$ be a homogeneous ideal of S, where I_d is the K-vector space of all homogeneous polynomials of degree d of I. Then $S/I = \bigoplus_{d\geq 0}(S/I)_d \tilde{=} \bigoplus_{d\geq d\geq 0} S_d/I_d$ is a graded algebra and its Hilbert function is the numerical function $H_{S/I} : \mathbb{N} \to \mathbb{N}$ such that $H_{S/I}(d) := dim_K(S_d/I_d)$.

Recall that the number of minimal homogeneous generators of I is an invariant for I. Indeed the number of homogeneous generators of I of a given degree d is one of the invariants that are called graded Betti numbers of I which appears in the first step of the minimal free resolution of I. Since one fundamental step in the construction of the minimal free resolution of I is just the computation of minimal generators of submodules of a free module over S, we point out that the described algorithm is applicable also to such submodules.

In [22] a method is described to compute minimal generators of an ideal I of projective points without using the theory of Gröbner bases: if B_d is a K-basis of the K-vector space I_d, then the dependent generators belonging to B_d are detected by checking linear dependences in the set $\{x_0, \ldots, x_r\} \cdot B_{d-1} \cup B_d$. This

method has a computational cost that is polynomial in the number of points and in the number $r+1$ of variables if the points are in generic position. And the minimalization step is applicable to any ideal with the condition that it is possible to construct a basis B_d.

As we reminded in the introduction, in the construction of Gröbner bases by the algorithm of Buchberger it is classical to get minimal generators by looking at the constant components of the syzygies: if $\{f_1, \ldots, f_t\}$ is a set of homogeneous generators of I and $Syz(I) = \{(h_1, \ldots, h_t) \in S^t | \sum_{i=1}^{t} h_i f_i = 0\}$ is a first module of syzygies of I, then a polynomial f_k depends if and only if there is a homogeneous generator $(h_1, \ldots, h_t)$ of $Syz(I)$ such that $h_k \in K$. There are many improvements of this approach and one can see [9] for a very recent result. However, in this paper we are interested in minimalizing Gröbner bases computed by the Buchberger and Möller algorithm.

In [17] an algorithm is described that minimalizes a reduced Gröbner basis of a homogeneous ideal computing only the constant components of the syzygies. Its computational cost is evaluated for ideals defined by functionals and is polynomial in the number of functionals and in the number $r+1$ of variables.

The algorithm that now we are going to illustrate here does not compute syzygies or a piece of them, although it exploits a result of [17] about syzygies for obtaining that in the algorithm of [22] it is sufficient to consider only a subset of particular bases B_{d-1} and B_d.

Recall that I is a homogeneous ideal of the polynomial ring $S = [x_0, \ldots, x_r]$ in $r+1$ variables over a field K and let $\mathcal{T} = \{x_0^{\alpha_0} \ldots x_r^{\alpha_r} \mid (\alpha_0, \ldots, \alpha_r) \in \mathbb{N}^{r+1}\}$ be the set of all terms of S ordered with respect to a term order $<$, i.e. a monoid order on $\mathcal{T}$ for which 1 is the smallest term. We say that a term T is a *multiple* of a term H if there is a term $\bar{H}$ such that $T = H\bar{H}$. If $\bar{H}$ is a variable, H is a *predecessor* of T. If p is a polynomial of $S = K[x_0, \ldots, x_r]$, $LT(p)$ is the leading term of p. If $\mathcal{P}$ is a set of polynomials of S, $LT(\mathcal{P})$ is the ideal generated in S by the leading terms of the polynomials of $\mathcal{P}$, and $\mathcal{P}_d$ is the set of elements of $\mathcal{P}$ of degree d.

Recall that a set $G \subset I$ of non-null polynomials of I is a Gröbner basis of I, with respect to a given term order $<$, if $LT(G) = LT(I)$. From the definition it follows that a Gröbner basis is a set of generators. A Gröbner basis is called *reduced* if its polynomials are monic and any term with a non-null coefficient in one of the polynomials of G is not divided by a leading term of a polynomial of G.

A rewriting procedure, with respect to a finite subset F of S and to a set term order, is an algorithmic method for substituting a polynomial f with a polynomial f' (called *remainder*) such that $f - f'$ belongs to the ideal generated by F and such that every coefficient of a term that belongs to $LT(F)$ vanishes in f'. The polynomial f' is unique if F is a Gröbner basis (see the Division Algorithm, for example, in [15] Th. 1.6.4).

If G is a Gröbner basis of I and T is a term which belongs to the monomial ideal $LT(G)$, then the *normal form* $NF(T)$ of T is the reminder of the Division

Algorithm of T with respect to G. Hence, it is a linear combination of terms not belonging to $LT(G)$ such that $b(T) := T - NF(T)$ belongs to I. If a term T belongs to the ideal $LT(G)$, then we say that T is *dependent*, otherwise we say that it is *independent*.

From now we fix only graded term orders. Let $B_d = \{b(T)|T \in LT(G)_d\}$ be the set of the polynomials of type $b(T)$ where T is a dependent term of degree d. If $G = \{f_1, \ldots, f_t\}$ is the reduced (homogeneous) Gröbner basis of I with respect to a graded term order $<$, then $G_d \subset B_d$.

Remark: The set $B_d = \{b(T)|T \in LT(G)_d\}$ is a K-basis of I_d. In fact, the definition of Gröbner basis itself makes possible to rewrite any polynomial of I_d by polynomials of B_d.

From now we suppose that G is reduced and that a and b are respectively the minimum and the maximum degree of the polynomials of G.

Let $\bar{B}_d = \{b(T) \in B_d \mid \exists x_i : \frac{T}{x_i} \notin LT(G)\} \subset B_d$ be the set of the polynomials of B_d whose leading term has at least one independent predecessor. Then

$$G_d = \{b(T) \in \bar{B}_d \mid \frac{T}{x_i} \notin LT(G),\ \forall i = 0, \ldots, r\}.$$

Remark: Since $H_{S/I}(d) = H_{S/LT(I)}(d)$ [16] it follows that

$$H_{S/I}(d) = |\{T \in \mathcal{T}_d \mid T \notin LT(G)\}|$$

and, hence, $|\bar{B}_d| \leq r \cdot |\{T \in \mathcal{T}_{d-1} \mid T \notin LT(G)\}| = r \cdot H_{S/I}(d-1)$.

3. Minimalization without computing syzygies

With the notation already introduced in section 2, let

$$T_i = LT(f_i), \quad T_{i,j} = l.c.m.(LT(f_i), LT(f_j)),$$

$$f_{i,j} = (T_{i,j}/T_i)\ f_i - (T_{i,j}/T_j)\ f_j.$$

It is well known that, from all the identities of type $f_{i,j} = \sum_{k=1}^{t} h_k f_k$, where $LT(h_k f_k) \leq LT(f_{i,j}) < T_{i,j}$, it is possible to obtain the following set of generators of the syzygies of G (see, for example, [15]):

$$\{(-h_1, \ldots, -h_{i-1}, \frac{T_{i,j}}{T_i} - h_i, \ldots, -h_{j-1}, \frac{T_{i,j}}{T_j} - h_j, \ldots, -h_t) \mid 1 \leq i < j \leq t\}.$$

In [17] it is observed that, using a rewriting procedure, a set of generators of syzygies of G can be computed also from all the identities of the following type:

$$x_\alpha b(x_\beta m) - x_\beta b(x_\alpha m) = -\sum_{T \notin LT(G)} c_T x_\beta T + \sum_{T \notin LT(G)} d_T x_\alpha T, \tag{1}$$

where m is an independent term, x_α is different from x_β and there are two polynomials f_i and f_j such that $x_\alpha x_\beta m = T_{i,j}$, x_α divides $LT(f_i)$ and x_β divides $LT(f_j)$. From the proof of Lemma 13.1 of [17] it follows that $x_\alpha m$ and $x_\beta m$ are dependent terms. As in [11] and in [12], we will employ the observation of [17] to design a minimalization procedure analogous to Ramella's one ([22]) but having always polynomial cost and applicable to each homogeneous polynomial ideal.

Since G is a Gröbner basis, it is not surprising that, in this context, we prove statements using a rewriting procedure. Let

$$\mathcal{V}_d \;=\; \{x_0,\ldots,x_r\}\cdot \bar{B}_{d-1} = \{x_i f_l \mid f_l \in \bar{B}_{d-1}, i=0,\ldots,r\} = \{p_1^*,\ldots,p_q^*\}.$$

Recall that, if f_l belongs to $\bar{B}_{d-1}$, then $LT(f_l)$ has an independent predecessor.

LEMMA 3.1: *Let f be a homogeneous polynomial of degree d. If any term appearing in f has an independent predecessor, then f can be described as a K-linear combination of polynomials in $G_d \cup \mathcal{V}_d$.*

Proof: By the hypothesis, $LT(f)$ has an independent predecessor, i.e. there exist a variable x_k and an independent term H such that $deg(H) = d-1$ and $Hx_k = LT(f)$. If $LT(f)$ does not have a dependent predecessor, there exists a polynomial f_i of G_d such that $LT(f) = LT(f_i)$. Then we consider $F_1 = f - f_i$ in the place of f. If $LT(f)$ has a dependent predecessor, there is a variable x_i, $i \neq k$, such that $(H/x_i)x_k$ is dependent. Notice that, since H is independent, H/x_i must be independent too. Thus, there is a polynomial p of $\bar{B}_{d-1}$ such that $LT(p) = (H/x_i)x_k$ and there is a polynomial p^* of $\mathcal{V}_d$ with $LT(p^*) = Hx_k = LT(f)$. Hence we can consider the polynomial $F_1 = f - p^*$ in the place of f. If $F_1 = 0$, the proof ends. Otherwise, by construction F_1 satisfies the hypothesis and $LT(F_1)$ is lower than $LT(f)$. Since $<$ is a term order, after a finite number of steps we must obtain the null polynomial so that f must be equal to a linear combination of polynomials of $G_d \cup \mathcal{V}_d$. □

PROPOSITION 3.1: *Let $f_{x_\alpha x_\beta m} = x_\beta b(x_\alpha m) - x_\alpha b(x_\beta m)$, where m is an independent term. Then:*

$$f_{x_\alpha x_\beta m} = \sum_{f\in G_d} c_f f + \sum_{i=1}^{q} d_i p_i^*. \tag{2}$$

Proof: The thesis follows by Lemma 3.1 since by formula (2) the polynomial $f_{x_\alpha x_\beta m}$ satisfies the hypothesis of such lemma. □

We point out that the cited observation of [17] about syzygies means that a polynomial f_i of G depends if and only if, its dependence is shown by a syzygy computed from an identity of type (2) by a rewriting procedure. Therefore, we can state the following result.

PROPOSITION 3.2: *A polynomial f_i of degree d of the reduced Gröbner basis G depends on $G-\{f_i\}$ if, and only if, it depends linearly on polynomials of the set $(G_d-\{f_i\})\cup\mathcal{V}_d$.*

Proof: The "if" implication is obvious. Notice that the polynomials $x_\beta b(x_\alpha m)$ and $x_\alpha b(x_\beta m)$ of formula (2) belong to $\mathcal{V}_d$, where m is an independent term of degree $d-2$. By definition of syzygy, f_i depends on $G-\{f_i\}$ if, and only if, the i-th component of a syzygy computed from an identity of type (2) is constant. From proposition 3.1 it follows that this dependence is equivalent to the existence of an identity of type (3) with a nonzero coefficient c_{f_i}, since formula (3) has been obtained by a rewriting procedure. □

This result allows us to formulate the following procedure to minimalize G. If α is the minimum degree of the polynomials of G, it is easy to observe that the polynomials of G_α are already independent. Hence, for each degree d such that $\alpha+1\leq d$ and $|G_d|\neq 0$, we consider a matrix M_d whose rows correspond to the terms of degree d which are multiples of independent terms of degree $d-1$, i.e. to the leading terms of the polynomials of $\bar{B}_d$.

The first columns of M_d are computed in the following way. For each polynomial p of $\mathcal{V}_d=\{x_0,\ldots,x_r\}\cdot\bar{B}_{d-1}$, we distinguish two cases: if the polynomial p has a leading term with an independent predecessor, then we put the column of its coefficients in M_d; otherwise, if we have already considered a polynomial p' of $\mathcal{V}_d$ such that $LT(p')=LT(p)$ does not have an independent predecessor, we put the column of coefficients of $p-p'$ in M_d. The last columns of M_d are the vectors of coefficients of the polynomials of G_d.

To single out minimal generators of I in G it is now enough to compute the row-echelon form of M_d. In fact, by proposition 3.2 the polynomials of G_d which are minimal generators correspond to columns of M_d that contain a pivot of the row-echelon form of M_d. Moreover, we can compute how a dependent polynomial f of G_d depends on $(G_d-\{f\})\cup\mathcal{V}_d$.

Remark: It is evident that in this context we need to compute the polynomials of $\bar{B}_{d-1}-G_{d-1}$ and, hence, the normal form of their leading terms. In general there is much interest in the computation of normal forms and there are several methods, the convenience of which can depend on the context (see, for example, [18]). By the scheme of [14], in ([17], section 13) it is already suggested a recursive procedure that is good for our algorithm and that is based on the following formula: if $T=x_iH$, where H is a dependent term and $NF(H)=\sum_j c_jx_jT_j$ ($c_j\in K$), then $NF(T)=\sum_j c_jNF(x_jT_j)$.

Let M be a graded submodule of the graded S-module S^t. For M it is possible to give the definitions of graded term order and of Gröbner bases analogous to the corresponding definitions for the ideal I. So we can define also the corresponding sets $\bar{B}_d^M$ and $\mathcal{V}_d^M$ for M, and it is easy to formulate Lemma 3.1 and Proposition 3.1 for M too. As a consequence, the following statement is obvious, making possible the application of the algorithm to any module of the type of M.

PROPOSITION 3.3: *Let* $G^M = \{f_1 = (f_{1,1}, \ldots, f_{1,t}), \ldots, f_h = (f_{h,1}, \ldots, f_{h,t})\}$ *be a reduced Gröbner basis of* M*. Then an element* f_i *of degree* d *depends on* $G^M - \{f_i\}$ *if and only if it depends linearly on the elements of the set* $(G_d^M - \{f_i\}) \cup \mathcal{V}_d^M$*.*

4. An improvement

The improvement that we propose concernes the matrix M_d, the construction of which has been described in section 3. We realized that it is sufficient to consider a submatrix $\bar{M}_d$ of M_d determined only by the columns corresponding to the polynomials obtained by $\mathcal{V}_d$ and only by the rows that correspond to all the dependent terms of degree d that have an independent term as predecessor. Indeed, with the notation already fixed, the following statement holds.

PROPOSITION 4.1: *Let* R *be the matrix obtained by a Gauss reduction of the transpose of* $\bar{M}_d$*. Let* G'_d *the subset of* G_d *consisting of the polynomials of* G_d *the leading term of which correspond to columns of* R *that not contain a pivot. Then* $\cup_d G'_d$ *is a set of minimal generators of the ideal* I*.*

Proof: First of all, we observe that a pivot of the matrix M_d can occur only in correspondence of a dependent term because it is the leading term of a polynomial of I, by construction. Hence, the pivots of M_d are in the same position of the pivots of $\bar{M}_d$, and in consequence the rank of M_d is equal to the rank of $\bar{M}_d$. This shows why we can avoid to consider the independent term.

Then, we note that since the rows of the transpose of $\bar{M}_d$ correspond to the polynomials and the column correspond to the terms, a Gauss reduction of this matrix cannot change the position of the terms with respect to the columns. By Proposition 3.2 it follows that to have only minimal generators we can take away off G_d the polynomials corresponding to rows of the transpose of $\bar{M}_d$ that become null by the Gauss reduction. Meanwhile it is evident that the rows corresponding to the polynomials of G'_d cannot become null and, hence, that such polynomials are minimal generators, then it is sufficient to apply a rewriting procedure such as in the proof of Lemma 3.1 to see that the polynomials of $G_d - G'_d$ are dependent. □

Applying the above result we save space memory and time for more than one reason. Indeed: (a) considering the transpose of $\bar{M}_d$ allows to save memory because one can memorize only the rows containing a pivot; (b) the number of columns (resp. of rows) of $\bar{M}_d$ (resp. the transpose of $\bar{M}_d$) is lower than the number of columns of M_d; (c) we do not need to reduce the polynomials of G_d with respect to the transpose of $\bar{M}_d$ to decide if they are or not minimal generators.

5. The algorithm and some tests

On the bases of the results of section 3 and 4, we can now outline the fundamental steps of an algorithm for minimalizing reduced Gröbner bases of homogeneous polynomial ideals and evaluate its computational cost.

Algorithm `MinBase`

Input: the reduced Gröbner basis $G = \{f_1, \ldots, f_t\}$ (w.r.t a graded term order) of a homogeneous polynomial ideal I of $S = [x_0, \ldots, x_r]$.
Output: a minimal set of generators of the ideal I.

begin
$a := min\{deg(f_i) \mid f_i \in G\}$, $b := max\{deg(f_i) \mid f_i \in G\}$
$d := a$
repeat

$d := d + 1$

Computation and sorting of the terms of degree d that have at least an indepedent predecessor

$H_{S/I}(d) := |\{T \in \mathcal{T}_d \mid T \notin LT(G)_d\}|$

for $T \in LT(G)_d$ with both dependent and independent predecessors **do**

computation of $NF(T)$ (by the scheme of [14] cited in the remark of section 3)

endfor

Computation of the transpose of the matrix $\bar{M}_d$ as described in section 4

Gauss reduction of the transpose of $\bar{M}_d$ and identification of the dependent polynomials of G_d by Proposition 4.1

until $d > b$
end

Let $h = max\{H_{S/I}(d) \mid a \leq d \leq b\}$. Note that every polynomial $b(T)$ of degree $d-1$ has at most $H_{S/I}(d-1)+1$ non null coefficients because the independent terms of degree $d-1$ are $H_{S/I}(d-1)$. Hence, since the polynomials of type $b(T)$ of degree $d-1$ are at most $(r+1) \cdot H_{S/I}(d-2)$, then the computational cost of the normal form $NF(T)$ of T is of order $(r+1) \cdot h^2$. Since the terms T of which we have to compute the normal form are at most $(b-a) \cdot (r+1) \cdot h$, then the computation of the normal forms is of order $(b-a)r^2h^3$.

Although the transpose of $\bar{M}_d$ has at most $(r+1)h$ rows and columns, its construction and Gauss reduction are equivalent to a reduction of a matrix with at most $(r+1)^2 H_{S/I}(d-2)$ rows (note that $(r+1)^2 H_{S/I}(d-2)$ is an upper bound for the number of polynomials of $\mathcal{V}_d$). Hence the computational cost of the construction and of the reduction of the transpose of $\bar{M}_d$ is of order $O(h^3 r^4)$. Thus the described method of minimalization is an $O((b-a)h^3r^4)$ algorithm.

Note that the sorting of the terms needs no more than $h^2(r+1)^2$ comparisons at each degree.

The above algorithm has been implemented in a program called `minbase` in C++ compiled using g++ and NTL 5.2 [23] for reduced Gröbner bases w.r.t. the graded reverse lexicographic (deg-rev-lex) term order, because this order is the most suitable for a minimalization [4]. Our program is available at `http://cds.unina.it/~cioffifr` and, for particular applications, in a sofware called `Points` [21]. We have tested its performance on randomly generated rational curves of degrees $d = 40, 50$ in $\mathbb{P}^r$ with $r = 4, 6, 8, 10, 12, 14, 16, 18, 20$.

In the following table we report the results of our tests: r is the dimension of the projective space in which the curve is embedded; d is the degree of the curve; `time` is the timing of the performance of our program in seconds; `size` is the memory space used during the computation in kilobytes. The inputs for these tests are available at `http://cds.unina.it/~cioffifr`. All the computations are performed on $K = \mathbb{Z}_p$ with $p = 31991$, on an Intel Pentium IV 1.6 GHz with 512 MB RAM +240 MB swap, running Linux (kernel 2.4.3).

smooth rational curves

r	d	time	size	d	time	size
4	40	0.19	800	50	0.40	940
6		0.32	820		0.49	996
8		0.53	824		0.52	976
10		0.37	1016		0.86	1100
12		0.55	924		0.80	1384
14		1.63	1104		1.23	1356
16		1.54	1216		4.20	1564
18		1.51	1480		3.94	1924
20		1.55	1316		3.77	2072

References

[1] Abbott, J., Bigatti, A., Kreuzer, M., and Robbiano, L. Computing ideals of points. *J. Symbolic Computation 30*, 4 (2000), 351–356.

[2] Abbott, J., Kreuzer, M., and Robbiano, L. Computing zero-dimensional schemes. Preprint available at http://cocoa.dima.unige.it/research/publica- tions.html, 2001.

[3] Albano, G., Cioffi, F., Orecchia, F., and Ramella, I. Minimally generating ideals of rational parametric curves in polynomial time. *J. Symbolic Computation 30*, 2 (2000), 137–149.

[4] Bayer, D., and Stillman, M. A criterion for detecting m-regularity. *Invent. Math. 87* (1987), 1–11.

[5] Berry, T. G. Parameterization of algebraic space curves. *J. Pure Appl. Algebra 117/118* (1997), 81–95. Algorithms for algebra (Eindhoven, 1996).

[6] Berry, T. G. Groebner bases of the ideal of a space curve. *J. Pure Appl. Algebra 148*, 1 (2000), 17–27.

[7] Buchberger, B. Introduction to Gröbner Bases. In *Gröbner Bases and Applications* (1998), vol. 251 of *London Mathematical Society, LNS*, Cambridge University Press, pp. 3–31.

[8] Buchberger, B., and Möller, H. M. The construction of multivariate polynomials with preassigned zeros. In *EUROCAM 82* (1982), vol. 144 of *LNCS*, Springer-Verlag, pp. 24–31.

[9] Caboara, M., Kreuzer, M., and Robbiano, L. Minimal Sets of Critical Pairs. Available at http://cocoa.dima.unige.it/research/publications.html, 2002.

[10] Chiantini, L., Cioffi, F., and Orecchia, F. Computing minimal generators of ideals of elliptic curves. In *Applications of algebraic geometry to coding theory, physics and computation (Eilat, 2001)*. Kluwer Acad. Publ., Dordrecht, 2001, pp. 23–35.

[11] Cioffi, F. *Calcolo di generatori di ideali di punti e curve algebriche*. PhD thesis, Università di Napoli "Federico II", 1996. Preprint n. 23, Dip. di Matematica e Applicazioni "R. Caccioppoli".

[12] Cioffi, F. Minimally generating ideals of points in polynomial time using linear algebra. *Ricerche di Matematica XLVIII*, 1 (1999), 55–63.

[13] Cioffi, F., and Orecchia, F. Computation of minimal generators of ideals of fat points. In *ISSAC 2001* (2001), ACM (Association for Computing Machinary), pp. 72–76.

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

[15] Kreuzer, M., and Robbiano, L. *Computational Commutative Algebra 1*. Springer, 2000.

[16] Macaulay, F. S. Some properties of enumeration in the theory of modular systems. *Proc. London Math. Soc. 26*, 2 (1927).

[17] Marinari, M. G., Moeller, H. M., and Mora, T. Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *AAECC 4* (1993), 103–145.

[18] Mourrain, B. A new criterion for normal form algorithms. In *Applied algebra, algebraic algorithms and error-correcting codes* (1999), vol. 1719 of *LNCS*, Springer, pp. 430–443.

[19] Orecchia, F. The ideal generation conjecture for s general rational curves in $\mathbb{P}^r$. *Journal of Pure and Appl. Algebra 155*, 1 (2001), 77–89.

[20] Orecchia, F. Implicitization of a general union of parametric varieties. *J. Symbolic Computation 31*, 3 (2001), 343–356.

[21] Orecchia, F., Cioffi, F., and Ramella, I. *Points (software for computations on points).* Available for linux platform at `http://cds.unina.it/~orecchia/ gruppo/EPoints.html`, 2001.

[22] Ramella, I. *Algoritmi di Computer Algebra relativi agli ideali di punti dello spazio proiettivo.* PhD thesis, Università di Napoli "Federico II", 1990. Preprint n. 30, Dip. di Mat. e Applic. "R. Caccioppoli", 1990.

[23] Shoup, V. *NTL: a Library for doing Number Theory.* Open source software distributed under the GNU General Public License and available at `http://www.shoup.net/ntl`, 2001.