COMPUTATION OF MINIMAL GENERATORS OF IDEALS OF FAT POINTS

FRANCESCA CIOFFI AND FERRUCCIO ORECCHIA
DIP. DI MATEMATICA E APPLICAZIONI "R. CACCIOPPOLI"
UNIV. DI NAPOLI "FEDERICO II"
VIA CINTIA, 80126 NAPOLI - ITALY

Abstract. We present an implementation of an algorithm for computing minimal homogeneous generators of ideals of fat points. First we construct a set of generators by an interpolating method which is based on the Hermite interpolation and generalizes the algorithm of [15] to projective space. Then, we minimalize the generators by the same algorithm which has been developed in [6] by exploiting results of [18] and [14] and which has been already successfully applied to ideals of points, to ideals of rational curves [3] and to ideals of general parametric varieties [17].

1. **Introduction**

Let $p_1, \dots, p_n$ be n distinct points on the projective space $\mathbb{P}^r$ of dimension r over a field K and $\mathcal{P}_i$ the ideal of the point p_i, for every $i = 1, \dots, n$. The points $p_1, \dots, p_n$ are called *fat points* with multiplicity $m_1, \dots, m_n$ respectively when they are the support of the projective scheme $\mathbb{X}$ whose saturated ideal is $I = \mathcal{P}_1^{m_1} \cap \dots \cap \mathcal{P}_n^{m_n}$. If $m = max_{i=1,\dots,n}\ m_i$ is the maximum of the multiplicities, then a homogeneous polynomial f belongs to I if and only if f has degree higher than $m-1$ and its derivatives of order $m_i - 1$ vanish on the point p_i for each $i = 1, \dots, n$.

If $S = K[x_0, \dots, x_r]$ is the ring of polynomials in $r+1$ variables over K then S_d is the K-vector space of all homogeneous polynomials of degree d of S. The ideal I is homogeneous, i.e. $I = \bigoplus_{d \geq 0} I_d$, where I_d is the K-vector space of all homogeneous polynomials of degree d of I. Then S/I is a graded standard algebra and it is $(S/I)_d \hat{=} S_d/I_d$. The Hilbert function of S/I (or of $\mathbb{X}$) is the numerical function $H_{S/I} : \mathbb{N} \to \mathbb{N}$ such that $H_{S/I}(d) := dim_K(S_d/I_d)$. Since I is saturated and S/I is a ring of Krull-dimension 1, then R/I is a Cohen-Macaulay ring. So the Hilbert function of $\mathbb{X}$ is strictly increasing until it assumes constantly the value of the Hilbert polynomial $HP = \sum_{i=1}^{n} \begin{pmatrix} m_i - 1 + r \\ r \end{pmatrix}$ of S/I (see, for example, [18]).

In 1982 Buchberger and Möller [15] describe an algorithm for computing reduced Gröbner bases of ideals of n points on $\mathbb{A}^r$ in a time that is polynomial in n and in r. For many authors this algorithm has been the starting point for computing on zero-dimensional varieties in polynomial time. The idea of Buchberger and Möller have been generalized to the projective space $\mathbb{P}^r$ by careful applications of the Hermite interpolation (see, for example, [12, ch. 4] for a survey about the Hermite interpolation). Hence now, if I is the ideal of n projective points, we can compute in polynomial time Gröbner bases of I [14, 1], a minimal set of homogeneous generators of I [14, 6] and, more in general, Gröbner bases of ideals of zero-dimensional schemes [14, 2]. In [18] a method for computing minimal generators of an ideal of points, which is based only on linear algebra, has been described for the first time, with a computational cost that is polynomial if the points are in generic position.

So, computations on zero-dimensional schemes have been already described. In particular, basing on linear functionals introduced in [14], in [1] there is an outline of a modular version of the Buchberger-Möller algorithm best suited for the computation over $\mathbb{Q}$ and in [2] analogous results for ideals of zero-dimensional schemes are obtained with a particular attention to ideals of fat points. But the implemention of this algorithm for fat points is not yet available. Moreover this algorithm doesn't compute a minimal set of generators but only a set of generators of the ideal of fat points.

In this paper we propose an algorithm that first computes generators of ideals of fat points and then minimizes them. The construction of the generators is based on the Hermite interpolation and on the theory of Gröbner bases. The minimization procedure reproduce the method that is described in [6] and in [3] for simple points and that has been developed basing on results of [18, 14]. The adopted method is able to compute also the Hilbert function of S/I, as suggested in [15, 16, 18], and in [5] has already been applied to improve computational results of [4] and of [11]. In this paper we show applications to the study of the natural number of minimal generators of an ideal of fat points [**??**].

The algorithm has been implemented in the object oriented language C++ over a field of positive characteristic p in a software called `Points`. All the computations are performed on $K = \mathbb{Z}_p$, with $p = 32003$, on an Intel Pentium III 686 MHz with 124 MB RAM + 240 MB swap, running Linux (kernel 2.2.14).

2. Construction of the generators

Recall that $p_1, \dots, p_n$ are n distinct points on the projective space $\mathbb{P}^r$ of dimension r over a field K and $\mathcal{P}_i$ is the ideal of the point p_i, for every $i = 1, \dots, n$. The points $p_1, \dots, p_n$ are *fat points* with multiplicity $m_1, \dots, m_n$ respectively when they are the support of the projective scheme $\mathbb{X}$ whose saturated ideal is $I = \mathcal{P}_1^{m_1} \cap \ldots \cap \mathcal{P}_n^{m_n}$. It is well known that the integer $HP = \sum_{i=1}^n \begin{pmatrix} m_i - 1 + r \\ r \end{pmatrix}$ is the Hilbert polynomial of S/I.

As in [18, 14], for each degree d homogeneous generators of I are computed by a method based on the Hermite interpolation, generalizing the algorithm of [15] to projective spaces. Let $\mathcal{T}$ be the set of all terms $x_0^{\alpha_0} \dots x_r^{\alpha_r}$ in the variables $x_0, \dots, x_r$ ordered with respect to a term ordering $<$, i.e. a well-ordering on $\mathcal{T}$ compatible with the multiplication of the monoid $\mathcal{T}$. 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 $S = K[x_0, \dots, x_n]$, let $T(p)$ be the leading term of p.

If $\mathcal{P}$ is a set of polynomials of S, $T(\mathcal{P})$ 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. A set of non-null polynomials $G \subset I$ is a Gröbner basis of I with respect to a given term order if $T(G) = T(I)$. A Gröbner basis is *reduced* if its polynomials are monic and any non-leading 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. It is important that a Gröbner basis of an ideal J is also a set of generators for J. DEFINIRE la "rewritig procedure".

Recall that if $m = max_i\ m_i$ is the maximum of the multiplicities, then a homogeneous polynomial f belongs to I if and only if f has degree higher than $m - 1$ and its derivatives of order $m_i - 1$ vanish on the point p_i for each $i = 1, \ldots, n$. Hence, for each degree $d \geq m$, we consider a matrix G_d^n such that the j-th column is the vector of the evaluations on the assigned points $p_1, \ldots, p_n$ respectively of the $(m_i - 1)$-th partial derivatives of the j-th term T of degree d. Let $T_1^{(d)} < \ldots < T_{r_d}^{(d)}$ be the terms of degree d corresponding to the first columns of G_d^n that form a maximal set of linear independent columns. We say that such terms are *independent* and that the others are *dependent*.

Now, suppose that the j-th term T is dependent and let $a_1, \ldots, a_{s_d}$ be the scalars of the linear combination of the columns corresponding to $T_1^{(d)}, \ldots, T_{s_d}^{(d)}$ which is equal to the column of T. With a notation analogous to that introduced in [14], we consider the following polynomial

$$b(T) = T - \sum_{i=1}^{s_d} a_i T_i^{(d)}. \tag{1}$$

For each dependent term T we obtain the scalars $a_1, \ldots, a_{s_d}$ by computing the reduced row-echelon form of the matrix G_d^s. Let $\mathcal{S}_d$ be the set of all polynomials of degree d of type (1). Of course $\mathcal{S}_d$ is a basis of the K-vector space I_d. Let $\mathcal{S} = \cup_{d=1}^{HP} \mathcal{S}_d$.

Proposition 2.1. *$\mathcal{S}$ is a Gröbner basis for I with respect to the set term-ordering $<$.*

Proof. It is sufficient to show that $T(I) = T(\mathcal{S})$. Since $\mathcal{S} \subseteq I$, obviously $T(\mathcal{S}) \subseteq T(I)$. First we consider a polynomial f of I_d, where d is lower than or equal to HP. By construction, all polynomials of $\mathcal{S}_d$ have different leading terms. Furthermore, each leading term does not appear (i.e. the corrisponding coefficient vanishes) in the polynomials in which it is not the leading term. Thus, since every polynomial f of I_d is a linear combination of polynomials of $\mathcal{S}_d$, $T(f)$ must be the leading term of a polynomial of $\mathcal{S}$. Now, let d be higher than HP. It is known that $H(T(I), d) = H(I, d)$ [13]. By construction, for each $d \leq HP$, $T(\mathcal{S})_d = T(I)_d$ and $T(\mathcal{S}) \subseteq T(I)$. Thus

$$H_{S/T(\mathcal{S}}(d) = H_{S/T(I)}(d) = H_{S/I}(d), \ \forall d \leq HP$$

$$H_{S/T(\mathcal{S})}(d) \geq H_{S/T(I)}(d) = HP, \ \forall d > HP.$$

Since, for example by [8, Theor. 3.3], for each $d > HP$, we have

$$HP \geq H(T(\mathcal{S}), d) \geq H(T(I), d) = H(I, d) = HP,$$

it follows that $T(\mathcal{S}) \supseteq T(I)$. □

By some linear algebra it is possible to show that a polynomial of $\mathcal{S}$ having a leading term multiple of the leading term of another polynomial of $\mathcal{S}$ is dependent in $\mathcal{S}$. So we can eliminate such polynomials, obtaining a particular subset G of $\mathcal{S}$, i.e. the reduced Gröbner basis of I with respect to $<$. As already observed in [14], this computation of G is a generalization of the computation of the reduced Gröbner basis of an ideal J of distinct affine points described in [15]. Moreover, it is possible to improve it employing the integer $\sigma = min\{d \in N \mid H(I, d) = H(I, d-1)\}$ which is not higher than HP. Since the ring R/I is a one-dimensional Cohen-Macaulay ring, polynomials of a minimal set of generators of I have degree not higher than σ [18]. Thus, instead of G, we may consider the set G' of all polynomials of G of degree not higher than σ: G' consists of all polynomials of degree $\leq \sigma$ of the reduced Gröbner basis with respect to the fixed term-order.

Notice that all the polynomials of G' are polynomials of $\mathcal{S}$ of degree not higher than σ with a leading term that is multiple *only* of independent terms and that $G'_d = G_d$. But, in order to minimize G', we will need all polynomials of $\mathcal{S}$ of degree lower than σ with leading term multiple of *at least* one independent term. Let $\mathcal{B}'$ the set of such polynomials. Since the number of independent terms of each degree d is always not higher than HP, it is obviuos that $|\mathcal{B}'_d| \leq (r+1)\cdot HP$ and $|G'_d| \leq (r+1)\cdot HP$. As in [14], let B' be the set of leading terms of polynomials of $\mathcal{B}'$. Let $\bar{G}'^s_d$ be the submatrix of G^s_d computed by taking only the terms of B'_d.

3. Minimalization of the generators

With the same notation introduced in section 2, let $G = \{f_1, \dots, f_t\}$ be the reduced Gröbner basis of I with respect to a term-order $<$. Let:

$$T_i = T(f_i),$$

$$T_{i,j} = l.c.m.(T(f_i), T(f_j)),$$

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

It is well known that, from all the identities $f_{i,j} = \sum_{k=1}^{t} h_k f_k$, where $T(h_k f_k) \leq T(f_{i,j}) < T_{i,j}$, a set of generators

$$\{(-h_1, \dots, -h_{i-1}, T_{i,j}/T_i - h_i, -h_{i+1}, \dots, -h_{j-1},$$
$$T_{i,j}/T_j - h_j, -h_{j+1}, \dots, -h_t) | 1 \leq i < j \leq t\}$$

of the syzygies of G [19, Corollary 13.15] can be obtained. In [14] it is observed that a set of generators of syzygies of G can be computed, using a rewriting procedure, also from all the identities of the following type:

$$x_\alpha b(x_\beta m) - x_\beta b(x_\alpha m) =$$
$$= -\sum_{k=1}^{s_{d-1}} c_k x_\beta T_k^{(d-1)} + \sum_{h=1}^{s_{d-1}} d_h x_\alpha T_h^{(d-1)}, \tag{2}$$

where: m is an independent term, x_α is different from x_β, there are two polynomials f_i and f_j such that $x_\alpha x_\beta m = T_{i,j}$, x_α divides $T(f_i)$ and x_β divides $T(f_j)$. From the proof of Lemma 13.1 of [14] it follows that $x_\alpha m$ and $x_\beta m$ are dependent terms. This observation can be proved by the same technique used in [19]. We will employ it to design a minimization procedure analogous to Ramella's one [18] but having always polynomial cost.

Contrary to [14], we avoid to compute the terms $T_{i,j}$ and the constant components of a system of generators of syzigies and we choose instead to compute all polynomials of degree not higher than σ.

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

$$\begin{aligned} \mathcal{V}_d &= \{x_i f_l \mid f_l \in \mathcal{B}'_{d-1}, i = 0, \dots, n\} = \\ &= \{p_1^*, \dots, p_q^*\} \\ \mathcal{D}_d &= \mathcal{S}_d - (\mathcal{B}'_d - G_d). \end{aligned}$$

Recall that, if f_l belongs to $\mathcal{B}'_d$, then $T(f_l)$ has an independent predecessor.

Lemma 3.1. *$\mathcal{D}_d \cup \mathcal{V}_d$ is a set of generators of the K-vector space I_d.*

Proof. It is sufficient to show that the polynomials of $\mathcal{B}'_d - G_d$ depend linearly on $\mathcal{D}_d \cup \mathcal{V}_d$. Let $\bar{p}$ be a polynomial of $\mathcal{B}'_d - G_d$; then $T(\bar{p})$ has an independent predecessor, i.e. there exist a variable x_k and an independent term H such that $deg(H) = d-1$ and $Hx_k = T(\bar{p})$. Since $\bar{p}$ does not belong to G, $T(\bar{p})$ must have a dependent predecessor too, i.e. 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 f of $\mathcal{B}'_{d-1}$ such that $T(f) = H/x_i x_k$ and there is a polynomial p^* of $\mathcal{V}_d$ with $T(p^*) = Hx_k = T(\bar{p})$. Now we can consider the polynomial $F_1 = \bar{p} - p^*$. If $F_1 = 0$, the proof ends. Otherwise, $T(F_1)$ is lower than $T(\bar{p})$ and it has a non null coefficient in p^*. Thus, by construction, $T(F_1)$ has an independent predecessor. Now, we can consider $T(F_1)$ in place of $T(\bar{p})$. Since $<$ is a term ordering, after a finite number of steps we must obtain the null polynomial so that $\bar{p}$ must be equal to a linear combination of polynomials of $(\mathcal{V}_d \cup G_d) \subseteq (\mathcal{V}_d \cup \mathcal{D}_d)$. □

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:*

$$f_{x_\alpha x_\beta m} = \sum_{f \in G_d} c_f f + \sum_{i=1}^{q} d_i p_i^*. \tag{3}$$

Proof. Since $f_{x_\alpha x_\beta m}$ belongs to I and since its leading term is a dependent term with at least one independent predecessor, the proof follows from the proof of Lemma 3.1 and from (2). □

We point out that the observation in [14] 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 main 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. First 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 minimize G'. We need all polynomials of $\mathcal{B}'$. If d is lower than or equal to σ and $|G_d| \neq 0$, then we consider a matrix M_d such that each row corresponds to one of the terms of degree d which are multiple of independent terms of degree $d-1$, i.e. to one of the terms of B'_d. The last columns of M_d are the vectors of coefficients of the terms of B'_d in polynomials of G_d. The first columns are computed in the following way. We consider all polynomials of degree d which are products of variables times polynomials of $\mathcal{B}'_{d-1}$, i.e. polynomials of $\mathcal{V}_d$. We consider these polynomials one after the other: if a polynomial p of $\mathcal{V}_d$ has a leading term belonging to B'_d, then we put the column of its coefficients in M_d; otherwise, if we have already considered a polynomial p' such that $T(p') = T(p) \notin B'_d$, we put the column of coefficients of $p - p'$ in M_d. Notice that the dimensions of M_d are of order $HP \cdot r \times HP \cdot r^2$. By proposition 3.2, a polynomial f of G_d depends if, and only if, the column corresponding to f does not contain a pivot of a row-echelon form of M_d and, moreover, we know how f depends on $(G_d - \{f\}) \cup \mathcal{V}_d$.

Algorithm

Input: n distinct points of $\mathbb{P}^r_K$, their multiplicities $m_1, \dots, m_n$ and a term-ordering on S.
Output: a minimal set of generators of the ideal I of the assigned fat points. **begin**
$m := max_i\ m_i$, $d := 0$, $d_0 := 0$
repeat
    $d := d + 1$, $N := \left(\begin{array}{c} d+r \\ r \end{array} \right)$
    Computation of $\bar{G}^n_d = G^n_d$
    Reduction of $\bar{G}^n_d$ to a row-echelon-form
    $H_{S/I}(d) = rank(\bar{G}^n_d)$
    if $rank(\bar{G}^n_d) < N$ **then**
        $d_0 := d$
        Computation and sorting of all terms of degree d
        Computation of the reduced row-echelon form of $\bar{G}^n_d$ and of the polynomials of degree d_0 of $G_{d_0} = \mathcal{B}'_{d_0}$
    endif
until $d_0 \neq 0$
while $rank(\bar{G}^n_d) \neq rank(\bar{G}^n_{d-1})$
    $d := d + 1$
    Computation of $\bar{G}^n_d (\neq G^n_d)$
    Reduction of $\bar{G}^n_d$ to a row-echelon form
    Computation and sorting of the terms of degree d multiples of the independent terms of degree $d - 1$. Let $N(<= (r + 1) \cdot HP)$ be the number of such terms
    if $rank(\bar{G}^n_d) < N$ **then**
        Computation of the reduced row-echelon form of $\bar{G}^n_d$ and of polynomials of degree d of $\mathcal{B}'_d$ and identification of polynomials of G'_d
    endif
    $H_{S/I}(d) = rank(\bar{G}^n_d)$
    if $|G'_d| \neq 0$ **then**
        Computation of M_d
        Reduction of M_d to a row-echelon form and identification of the dependent polynomials of G'_d
    endif
endwhile
$\sigma = d$
end

4. **The computational cost**

The computational cost in field operations of the described algorithm is of order $O(HP^4 r^4)$, i.e. is polynomial in HP and in r. In fact the construction of G is of order $O(HP^4 r)$. The same holds for G' and for $\mathcal{B}'$. In fact, the dimensions of a matrix $\bar{G}^n_d$ are always of order $HP \times HP \cdot r$ and a reduction of such a matrix is of order $O(HP^3 r)$. Since we compute no more than HP matrices $\bar{G}^n_d$, the cost of the construction of $\mathcal{B}'$ is of order $O(HP^4 r)$. Computing the matrix M_d needs no more than $HP^2(r+1)^3$ subtractions. The computational cost of the reduction of M_d to a row-echelon form is of order $O(HP^3r^4)$. Thus the order of the cost of the described method of minimalization is $O(HP^4r^4)$. Notice that the cost of the computation and of the evaluation of the terms is lower than $O(HP^4r^4)$. The ordering of terms needs no more than $HP^2(r+1)^2$ comparisons.

5. An implementation and some applications

The described algorithm for constructing minimal generators of ideals of fat points has been implemented in a program called `Points` [7]using C++ and NTL ("a Library for doing Number Theory", version 4.3a [20]). In we have used the software for proving the following conjecture for multiplicities $m_1 = \ldots = m_n \leq 20$

conjecture

(Harbourne-Hirschowitz)[9][10] A linear system

$\mathcal{L}_d(m_1, \ldots, m_n)$ of plane

curves with general multiple base points is

special if and only if is (-1)-special.

Note that previously the conjecture was proved for multiplicities $m_1 = \ldots = m_n \leq 4$ in [4] and for multiplicities $m_1 = \ldots = m_n \leq 12$ in [11]. Another application is the following HARBOURNE

METTERE TABELLE SUI TEMPI DI CALCOLO IN P2 e P3

References

1. J. Abbott, A. Bigatti, M. Kreuzer, L. Robbiano (2000). Computing Ideals of Points. *J. Symbolic Computation* **30**, no. 4, 351-356.
2. J. Abbott, M. Kreuzer, L. Robbiano (2000). Computing Zero-dimensional Schemes. Pre- print available at `http://cocoa.dima.unige. it/researchs/publications.html`.
3. G. Albano, F. Cioffi, F. Orecchia, I. Ramella (2000). Minimally generating ideals of rational parametric curves in polynomial time. *J. Symbolic Computation* **30**, no. 2, 137-149.
4. C. Ciliberto, R. Miranda (2000). Linear systems of plane curves with base points of equal multiplicity. *Trans. Amer. Math. Soc.* **352**, 4037-4050.
5. C. Ciliberto, F. Cioffi,R. Miranda, F. Orecchia (200 1). Hermite interpolation and linear systems of plane curves with base fat points. Preprint
6. F. Cioffi (1999). Minimally generating ideals of points in polynomial time using linear algebra. *Ricerche di Matematica* **XLVIII**, Fasc. 1, 55-63.
7. F. Cioffi, F. Orecchia, I. Ramella.(2000) Points (software for computations on points) available for linux platform at `http://matna3.dma.u- nina.it/~orecchia/Edownload.html` or by anonymous ftp on `matna3.dma.unina.it`, directory `pub/ Points2`.
8. A. V. Geramita, P. Maroscia, L. Roberts, *The Hilbert function of a reduced K-algebra*, J. of London Math. Soc. (2), **28**, 443-452, 1983.
9. B. Harbourne (1986). The Geometry of rational surfaces and Hilbert functions of points in the plane. *Can. Math. Soc. Conf. Pro.*, **6** (1986), 95-11.
10. A. Hirschowitz (1989), Une conjecture pour la cohomologie des diviseurs sur les surfaces

rationnelles generiques. *J. reine angew. Math.* **397**, 208-213.

11. G. G. Lorentz, R. A. Lorentz (1990). Bivariate Hermite Interpolation and Application to Algebraic Geometry. *Numer. Math.* **57**, 669-680.
12. R. A. Lorentz (1992). Multivariate Birkhoff Interpolation. LNM 1516, Springer,1992.
13. F. S. Macaulay, *Some properties of enumeration in the theory of modular systems*, Proc. London Math. Soc., (**2**), **26** (1927)
14. M. G. Marinari, H. M. Moeller, T. Mora (1993). Gröbner Bases of Ideals Defined by Functionals with an Application to Ideals of Projective Points. *AAECC*, **4**, 103-145, 1993.
15. H. M. Moeller, B. Buchberger (1982). The construction of multivariate polynomials with preassigned zeros. EUROCAM 82, L.N.C.S. 144, Springer-Verlag, 1982.
16. F. Orecchia, F. (1991). A polynomial algorithm for computing the conductor of points and of a curve with reduced tangent cone. *Queen's Papers in Pure and Applied Mathematics no* **88**, *The Curves Seminar at Queen's* **VIII**, Queen's University, Kingston, Ontario.
17. F. Orecchia (2001). Implicitization of a general union of parametric varieties. To appear in *J. Symbolic Computation.*
18. I. Ramella (1990). *Algoritmi di Computer Algebra relativi agli ideali di punti dello spazio proiettivo*, Tesi di Dottorato di Ricerca, Pre- print n. 30, Dip. di Mat. e Applic. "R. Caccioppoli", Univ. di Napoli "Federico II", 1990.
19. L. Robbiano (1987) *Introduzione all'algebra computazionale.* Corso INDAM, 1986/87, Ro- ma, Preprint n. 7, 1987, Univ. di Genova.
20. V. Shoup (2000). 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`.