J. Symbolic Computation (2001) **11**, 1–000

Minimally generating ideals of rational parametric curves in polynomial time

G. ALBANO*, F. CIOFFI**, F. ORECCHIA** AND I. RAMELLA**

**D.I.I.M.A., Univ. di Salerno, Fisciano (SA), Italy*
***Dip. di Mat. e Appl. "R. Caccioppoli", Univ. di Napoli "Federico II", Napoli, Italy*

(Received)

We present an algorithm for computing a minimal set of generators for the ideal of a rational parametric projective curve in polynomial time. The method exploits the availability of polynomial algorithms for the computation of minimal generators of an ideal of points and is alternative to the existing Gröbner bases techniques for the implicitization of curves. The termination criterion is based on the Castelnuovo-Mumford regularity of a curve. The described computation yields also the Hilbert function and, hence, the Hilbert polynomial and the Poincaré series of the curves. Moreover, it can be applied to unions of rational curves. We have compared the implementation of our algorithm with the Hilbert driven elimination algorithm included in CoCoA 3.6 and Singular 1.2, obtaining, in general, significant improvements in timings.

1. Introduction

The problem of computing a minimal set of generators for the ideal of a rational parametric projective curve has been tackled by elimination theory and can be solved by the computation of Gröbner bases (see, for example, Kalkbrener (1991), Licciardi and Mora (1994), Fix *et al.* (1996), Gao and Chou (1992), and references therein). These methods have been implemented in CoCoA 3.6 and Singular 1.2 and have exploited the Hilbert driven algorithm (Traverso, 1995).

In this paper, developing ideas of Ramella (1994), Cioffi (1996, 1999) and Orecchia (1998) we present an alternative method based on the computation of the generators for the ideal of a suitably chosen finite set of points on the curve. This has been made possible due to the availability of algorithms that construct a minimal set of generators of ideals of projective points in polynomial time (Ramella (1990), for points in generic position; Marinari *et al.* (1993); Cioffi (1999)). Let C be the union of h rational curves represented parametrically over a field K which contains at least $d(d \cdot m+1)$ distinct elements, where d is the degree of C and m is an upper bound for the Castelnuovo-Mumford regularity of $I(C)$. The algorithm presented in this paper actually determines a minimal set of generators and computes the Hilbert function (then the Hilbert polynomial and the Poincaré series) of the ideal $I(C)$. The described procedure is performed in a time polynomial in the degree of the curve and in the minimal dimension of a linear variety containing the curve. The algorithm becomes efficient by using a good termination criterion for the

0747–7171/90/000000 + 00 $03.00/0 © 2001 Academic Press Limited

minimal generators based on finding a suitable bound for the Castelnuovo-Mumford regularity of the curves. For smooth curves this is given in (Orecchia, 1998). For singular curves a good bound for the regularity is developed in this paper and is based on the properties of saturated ideals and of the Hilbert function of a general hyperplane section (Theorem 2.4). Since to use this bound it is important to know the degree of the given curve, by Lemma 2.3 and by Proposition 2.3 we give a tool to compute the degree of a curve given by a parametrical rational representation.

Using C++, we have implemented the described algorithm in a software called Points (available by anonymous ftp on `matna3.dma.unina.it`, directory `pub/Points99`, or at `http://cds.unina.it/~orecchia/Edownload.html`). We provide examples worked out with Points compared with the performances of the Hilbert driven algorithm (Traverso, 1995) for the implicitization via Gröbner bases, implemented in CoCoA 3.6 and in Singular 1.2. We do not report the timings of Singular 1.2 because in general they are higher. It turns out that Points is particularly suitable for curves whose parametric representation is dense. The implementation of our algorithm is based on the computation of minimal generators of an ideal of points given in (Cioffi, 1999) since it also gives the polynomials of a reduced Gröbner basis of the ideal for each degree t considered in the computation (see section 3) . This is crucial for the termination criterion given by Theorem 2.4.

In the following, if $S = K[x_0, \dots, x_r]$ is a ring of polynomials over a field K and $\bar{K}$ is the algebraic closure of K, we say that a point $[y_0 : \dots : y_r]$ of $\mathbb{P}^r_{\bar{K}}$ is a "rational point" over K if there exist $y'_0, \dots, y'_r$ of K such that $[y_0 : \dots : y_r] = [y'_0 : \dots : y'_r]$. By a projective algebraic variety we mean the set of points of $\mathbb{P}^r_{\bar{K}}$ that are the zeros of the polynomials of a homogeneous ideal of S. In particular, by a (projective) curve we mean a projective variety of pure dimension 1. A rational curve C is a reduced irreducible curve birational to $\mathbb{P}^1_{\bar{K}}$ or, equivalently, by Lüroth's theorem, it is a curve which has a parametric rational representation. With $deg(C)$ we denote the degree of C. If I is a homogeneous ideal of S and $I_t = \{f \in S \mid \partial f = t\}$ we say that $H(I,t) = \binom{t+r}{r} - dim_K I_t$ is the Hilbert function of I (or of the graded algebra $\frac{S}{I}$). Recall that, for $t >> 0$, the Hilbert function is equal to a polynomial $p(I,t)$ which we call the Hilbert polynomial of I (or of S/I).

We set $\Delta H(I,t) = H(I,t) - H(I,t-1)$ and $\Delta^i H(I,t) = \Delta^{i-1} H(I,t) - \Delta^{i-1} H(I,t-1)$, for each $i > 1$. We denote by $P(S/I) = \sum_{i \geq 0} H(I,t) z^t$ the Poincaré series of S/I which can be expressed as a rational function $\frac{h(z)}{(1-z)^k}$ where $h(z)$ is a polynomial.

We say that a homogeneous ideal of S or a standard graded module is generated in degree n if it can be generated by elements of degree $\leq n$.

2. Computation of minimal generators and Hilbert function of ideals of rational curves

Let m be a positive integer.

Definition 2.1. *A coherent sheaf $\mathcal{F}$ is m-regular if $H^q(\mathcal{F}(m-q)) = 0$ for all $q > 0$.*

Definition 2.2. *A homogeneous ideal I is m-regular if its j^{th} module of syzygies is generated in degree $\leq m-j$, for each $j > 0$. In particular if I is m-regular, I is generated in degree m. The regularity $reg(I)$ of I is the smallest integer m for which I is m-regular.*

Definition 2.3. *The saturation I^{sat} of a homogeneous ideal I is $I^{sat} = \{f \in S | \forall i = 0, \dots, r, \exists n : x_i^n f \in I\}$. The ideal I is saturated if $I^{sat} = I$. The ideal I is m-saturated if $I_t^{sat} = I_t$ for each $t \geq m$.*

Proposition 2.1. *A homogeneous ideal I is m-regular if and only if I is m-saturated and its saturation I^{sat} is m-regular.*

Proof. (see, for example, Green (1996) Prop. 2.6). □

The following result is well known.

Proposition 2.2. *If I is the ideal of a curve and $m \geq reg(I)$, then*

1. $H(I,t) = p(I,t)$, *for* $t \geq m-1$;
2. $p(I,t) = \Delta H(I,m)t + H(I,m-1) - \Delta H(I,m)(m-1)$;
3. $P(S/I) = \frac{\sum_{i=1}^{m} h_i z^i}{(1-z)^2}$, *with* $h_i = \Delta^2 H(I,i)$.

Proof. (1.) See, for example, (Nagel (1990), Lemma 4(i)).

(2.) Since the Hilbert polynomial $p(I,t)$ has degree 1, it is sufficient to determine the unique polynomial of degree 1 in a variable t which assumes the values $H(I,m)$ and $H(I,m-1)$ respectively for $t = m$ and $t = m-1$.

(3.) See, for example, (Migliore (1998), section 1.4). □

In conclusion, if I is m-regular, by the computation of the Hilbert function of I at each degree $\leq m$ we obtain the Hilbert polynomial and the Poincaré series of $I(C)$ too.

Lemma 2.1. *Let C be a reduced curve of degree d, $I = I(C)$ its ideal and $C_1, \dots, C_h$ its irreducible components of degree $d_1, \dots, d_h$ respectively ($d = \sum_{i=1}^{h} d_i$). Let $m \geq reg(C)$. Suppose that every curve C_i, $i = 1, \dots, h$, contains $d_i m + 1$ distinct points and let J be the ideal of these $d \cdot m + h$ points of C. Then, the polynomials of degree $\leq m$ of a minimal set of generators for J form a minimal set of generators for I. Hence $H(I,t) = H(J,t)$, for $t \leq m$.*

Proof. Clearly $I \subseteq J$ and it is well known that a hypersurface of degree $t \leq m$ containing $d_i m + 1$ points of C_i must contain C_i. Hence, $I_t = J_t$ for each degree $t \leq m$. It remains to observe that, since I is generated in degree m, then I is generated by $\bigoplus_{t \leq m} I_t = \bigoplus_{t \leq m} J_t$. □

Let C be an irreducible rational parametric curve. Its parametric representation can be easily reduced to the following form:

$$C : \begin{cases} x_0 & = & f_0(u,v) \\ \vdots & & \vdots \\ x_r & = & f_r(u,v) \end{cases} \tag{2.1}$$

where $f_i(u,v)$ are polynomials of the same degree d and without common factors. Then points on the curve are immediately found by giving values to the parameters u, v.

LEMMA 2.2. *If the field K contains at least $d(d \cdot m+1)$ distinct elements, the rational curve C has at least $d \cdot m + 1$ points.*

Proof. Since $deg(C) \leq d$, each point of C corresponds to no more than d points of $\mathbb{P}^1$ by the representation (2.1). So, $d \cdot m+1$ points of C correspond no more than $d(d \cdot m+1)$ points of $\mathbb{P}^1$. But by the hypothesis $\mathbb{P}^1$ has at least $d(d \cdot m+1)$ points. $\square$

In (Gruson *et al.*, 1983) an upper bound for the regularity of a reduced curve C, depending on r and on the degree $deg(C)$ of the curve, is determined.

THEOREM 2.1. *Let C be a projective curve and let $C_1, \dots, C_h$ be its irreducible components of degree respectively $d_1, \dots, d_h$. If r_i is the smallest dimension of a linear variety containing C_i, let*

$$m_i = \begin{cases} d_i + 2 - r_i, & if \quad d_i \geq 2 \\ 1, & if \quad d_i = 1 \end{cases}, \quad m = \sum_{i=1}^{h} m_i. \tag{2.2}$$

Then the curve C is m-regular and, hence, is generated in degree m. In particular, if C is irreducible and non degenerate of degree $d > 1$, then C is $(d+2-r)$-regular and, hence, is generated in degree $(d+2-r)$.

Proof. (Gruson *et al.*, 1983), Theorem 1.1 and Remark (1) p.497. $\square$

Then, if C is the union of rational irreducible curves represented parametrically, Lemma 2.1 and Theorem 2.1 reduce the computation of a minimal set of generators of the ideal of C to the computation of the minimal generators of an ideal of points which can be found by giving values to the parameters. All this has interest because polynomial algorithms that compute a minimal set of generators of ideals of projective points have been constructed by Ramella (1990), for points in generic position, Marinari *et al.* (1993), Cioffi (1999) (see section 3).

Summarizing:

THEOREM 2.2. *Let C be a union of h rational curves represented parametrically over a field K that contains at least $d(d \cdot m+1)$ distinct elements, where $d = deg(C)$ and $m \geq reg(C)$. Then there exists a polynomial algorithm to determine a set of minimal generators of $I(C)$.*

Proof. The proof of the statement follows from the above considerations and from the fact that there exist polynomial algorithms that compute minimal generators of ideals of points (see section 3). $\square$

In section 3 we will describe the main steps of the algorithm and determine its computational cost. The termination criterion yielded by Theorem 2.1 has a theoretical value because it is constant for all curves with fixed r_i and d_i but in practice is not very tight. So in the following we collect some results about the computation of the regularity of the curve that improve the performance of the algorithm.

Let $C = \bigcup_{i=1}^{n} C_i \subset \mathbb{P}^r$ be a non-degenerate curve, such that C_i are rational irreducible curves parametrized by polynomials of degree d_i, for each i. Let $d = \sum_{i=1}^{s} d_i$.

THEOREM 2.3. *In $\mathbb{P}^r$, $r \geq 3$, we have $H(I, n) = d \cdot n + h$, for some positive integer n*

if and only if C has degree d and is a disjoint union of h distinct smooth curves. In this case $m = Min\{n \in \mathbf{N} | H(I,n) = d \cdot n + h\} + 1$ is the regularity of C.

Proof. (Orecchia (1998), Propositions 1.3 and 1.5). □

Theorem 2.3 gives a very good improvement of the termination criterion for the computation of minimal generators since it finds exactly the regularity of unions of smooth curves (which in $\mathbb{P}^r$, $r \geq 3$, is the general case) but is not effective for singular curves. In this case one can use the criteria described below.

From now on assume that the hyperplane $x_r = 0$ does not contain any of the curves $C_1, ..., C_h$ (this is immediately satisfiable; in fact if in (2.1) the equation $x_r = 0$ is one of the the parametric equations of a curve C_i one can change, in (2.1), $x_r = 0$ with $x_r = f_j(u,v)$ for some j for which $f_j(u,v)$ is not identically zero). Then the class $\overline{x}_r$ of x_r is not a zero-divisor on S/I, where $I = I(C)$ is the ideal of C.

Let $G = \{g_1, \ldots, g_n\}$ be the reduced Gröbner basis of I with respect to the degree reverse lexicographic order. Recall that, if $T(g_i)$ is the leading term of the polynomial g_i and $T(I)$ is the ideal generated by the leading terms of all polynomials of I, then $T(I) = (T(g_1), \ldots, T(g_n))$ and $H(T(I),t) = H(I,t)$.

Since G is the reduced Gröbner basis with respect to the degree reverse lexicographic order and $\overline{x}_r$ is not a zero-divisor on S/I, then $\overline{x}_r$ is not a zero-divisor on $S/T(I)$ either and, hence, x_r does not divides any $T(g_i)$. Then $(T(I), x_r) = T(I, x_r)$ (Bayer and Stillman (1987), Lemma 2.2 (a)). Note also that $reg(I, x_r) = reg(I)$ (Bayer and Stillman (1987), Lemma 1.8).

Hence $reg(T(I, x_r)) \geq reg(I, x_r)$ (Bayer and Stillman (1987), Section 1) and then

$$reg(I) = reg(I, x_r) \leq reg(T(I, x_r)) = reg((T(I), x_r)) \tag{2.3}$$

Since $\overline{x}_r$ is not a zero-divisor in S/I then $H((I, x_r), t) = \Delta H(I, t)$ for each positive degree t and then

$$deg(C) = p((I, x_r), t) = p((T(I), x_r), t). \tag{2.4}$$

Moreover it is well known that if $J \subset S$ is a saturated ideal and $dim(S/J) = 1$ the Hilbert function of the saturated ideal J is strictly increasing until it becomes constantly equal to its Hilbert polynomial $p(J,t)$. Moreover, if $\sigma = min\{t : H(J,t) = H(J, t-1)\}$, then J is σ-regular and then $H(J,t) = P(J,t)$, for $t \geq \sigma$.

THEOREM 2.4. *Let τ be a positive integer and $J(\tau) = (T(I)_{\leq \tau}, x_r)$ be the monomial ideal generated by x_r and by the leading terms of the polynomials, of degree $\leq \tau$, of the reduced Gröbner basis G of I.*

If for some τ:

(a) $dim(S/J(\tau)) = 1$;
(b) $deg(C) = H(J(\tau), \tau) = H(J(\tau)^{sat}, \tau - 1)$

then I is τ-regular

Proof. Let $J = (T(I), x_r)$. By (2.3) it is enough to prove that $reg(J) \leq \tau$. If (a) and (b) hold, then $deg(C) = H(J(\tau)^{sat}, \tau - 1) \leq H(J(\tau)^{sat}, \tau) \leq H(J(\tau), \tau) = deg(C)$ and so $J(\tau)^{sat}$ is τ-regular and $J(\tau)$ is τ-saturated. Then by Proposition 2.1 also $J(\tau)$ is τ-regular. Thus, if we prove that $J(\tau) = J$ we are done. Clearly $J(\tau) \subseteq J$ and then it is enough to prove that $H(J(\tau),t) \leq H(J,t)$, for any t. By the previous inclusion we have $J(\tau)^{sat} \subseteq J^{sat}$. But, since the Hilbert polynomial doesn't change by saturation, by (2.4) we have $p(J^{sat},t) = deg(C) = p(J(\tau)^{sat},t)$, and then $J(\tau)^{sat} = J^{sat}$. Thus $H(J(\tau),t) = H(J(\tau)^{sat},t) = H(J^{sat},t) \leq H(J,t)$, for $t \geq \tau$. But $H(J(\tau),t) = H((T(I),x_r),t)$ for $t \leq \tau$ by construction. $\square$

To check the hypotheses of Theorem 2.4 in the implementation of our algorithm it is enough to know all the monomials of degree t that do not belong to $J(\tau)$. Moreover, recall that the dimension of an ideal J is equal to the largest integer k for which there exist k variables $x_{i_1},\ldots,x_{i_k}$ such that $J \cap K[x_{i_1},\ldots,x_{i_k}] = (0)$ and it is very easy to check this condition for a monomial ideal such as $J(\tau)$.

It can happen that the curve is not properly represented, i.e. its degree is less than the degree of the polynomials that represent the curve. For example, the following curve Γ has degree 20, although the degree of the polynomials that represent Γ is $d = 40$

$$\Gamma : \left\{ \begin{array}{lcl} x_0 & = & u^{40} + v^{40} \\ x_1 & = & u^{27}v^{13} + u^{13}v^{27} \\ x_2 & = & u^{29}v^{11} + u^{11}v^{29} \\ x_3 & = & u^{20}v^{20} \end{array} \right. .$$

The following proposition gives a practical method to see if a curve C is well represented (that is if the degree of the polynomials that represent C coincides with the degree of the curve), which works in most cases.

LEMMA 2.3. *Let C be an irreducible rational curve represented by polynomials of the same degree d without a common factor. Then $d = k \cdot deg(C)$ for some positive integer k.*

Proof. By the Primbasis theorem, any parametric representation of C is of type [1,k], for some integer k. So, by the representation (2.1), a general point of C is determined by k points of $\mathbb{P}^1$. Let $\pi : a_0x_0 + \ldots + a_rx_r = 0$ be a general hyperplane and consider the following equation:

$$a_0f_0(u,v) + \ldots + a_rf_r(u,v) = 0; \tag{2.5}$$

For each point of $C \cap \pi$, the equation (2.5) has k solutions. Since $|C \cap \pi| = deg(C)$ and $\partial(f_i) = d$, it follows that $d = k \cdot deg(C)$. $\square$

PROPOSITION 2.3. *Suppose that C is a rational irreducible curve parametrically represented by polynomials of degree d. Let $\bar{d}$ be the highest proper positive divisor of d. If $H(I,t) > \bar{d} \cdot t + 1$ for some t, then $deg(C) = d$.*

Proof. The proof follows immediately from the fact that $H(I,t) \leq deg(C) \cdot t + 1$. Indeed, the Hilbert function of an irriducible curve is always no higher than the Hilbert function of its normalization and the Hilbert function of an irreducible smooth curve Γ is no higher than $deg(\Gamma) \cdot t + 1$ for each degree t (Orecchia (1998), Proposition 1.3). $\square$

Applying Proposition 2.3 we can compute the degree of the given curve, also if the curve is not properly represented. For example, for the curve Γ we see that $H(J(9),9) = H(J(9)^{sat},8) = 20$. Since $J(9) = J(9)^{sat}$ and $dim(S/J(9)) = 1$, we can conclude that $(T(I), x_r)$ contains a 9-regular ideal of dimension 1 and of degree 20. Hence, $deg(T(I), x_r) \leq 20$. Furthermore, $H(I, 8) = 127 > 10 \cdot 8 + 1$ and so, by Proposition 2.3, $deg(\Gamma) = 20$ and $\tau = 9$. In the case in which the curve is not properly represented we have to check also the condition $J(\tau) = J(\tau)^{sat}$.

3. The algorithm and computational cost

As we stated in the introduction, we base our method for the implicitization of projective rational curves on the algorithm formulated in (Cioffi, 1996, 1999) for the construction of minimal generators of ideals of projective points. Here, for the sake of completeness, we recall the main points of this algorithm and then describe the algorithm for rational curves.

3.1. Construction of minimal generators of an ideal of points

Let I be the ideal of s distinct points $P_1, \ldots, P_s$ of $I\!P^r_K$. As in (Ramella, 1989) and in (Marinari *et al.*, 1993), for each degree homogeneous generators of I can be computed by an interpolation method based on linear functionals, which is a generalization to projective space of the algorithm of Möller and Buchberger (1982). Let $\mathcal{T}$ be the set of all terms T in the variables $x_0, \ldots, x_r$ ordered with respect to a term ordering $<$, i.e. a well-ordering on $\mathcal{T}$ compatible with the multiplication of the monoid $\mathcal{T}$. A term T is a multiple of a term T' if there is a term $\bar{T}'$ such that $T = T'\bar{T}'$. If $\bar{T}'$ is a variable, T' is a predecessor of T. If p is a polynomial of $S = K[x_0, \ldots, x_r]$, let $T(p)$ be the leading term of p. In general, if $\mathcal{P}$ is a set of polynomials of S, $\mathcal{P}_t$ will be the set of elements of $\mathcal{P}$ of degree t.

For each degree t, we consider a matrix G^s_t such that the j-th column is the vector of the evaluations at the given points of the j-th term T of degree t. Let $T^{(t)}_1 < \ldots < T^{(t)}_{q_t}$ be the terms of degree t corresponding to the first columns of G^s_t that form a maximal set of linearly 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 $a_1, \ldots, a_{q_t}$ be the scalars of the linear combination of the columns corresponding to $T^{(t)}_1, \ldots, T^{(t)}_{q_t}$ which is equal to the column of T. With a notation similar to that introduced in (Marinari *et al.*, 1993), we consider the following polynomial

$$b(T) = T - \sum_{i=1}^{q_t} a_i T^{(t)}_i. \tag{3.1}$$

For each dependent term T we obtain the scalars $a_1, \ldots, a_{q_t}$ by computing the reduced row-echelon form of the matrix G^s_t . Let $\mathcal{S}_t$ be the set of all polynomials of degree t computed by the described method. Of course $\mathcal{S}_t$ is a K-basis of the K-vector space I_t. Moreover, $\mathcal{S} = \cup^s_{t=1}\mathcal{S}_t$ is a Gröbner basis for I with respect to the given term-ordering $<$ (Cioffi (1999), Proposition 2.1).

Polynomials of $\mathcal{S}$ having leading term a multiple of the leading term of another polynomial of $\mathcal{S}$ are dependent in $\mathcal{S}$. So we can eliminate such polynomials from $\mathcal{S}$, obtaining a particular subset G of $\mathcal{S}$, i.e. the reduced Gröbner basis of I with respect to $<$. The integer $\sigma = min\{d \in N \mid H(I, t) = H(I, t-1)\}$ is not higher than s and is the regularity of the ideal I. Thus, instead of G, we may consider the set G' of all polynomials of G of degree not higher than σ.

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. But, in order to minimaze G', we need all polynomials of $\mathcal{S}$ of degree less than σ with leading term a multiple of at least one independent term. Let $\mathcal{B}'$ the set of such polynomials. Since the number of independent terms of each degree t is always less than or equal to s, it is obvious that $|\mathcal{B}'_t| \leq (r+1)s$ and $|G'_t| \leq (r+1)s$. Let B' be the set of leading terms of polynomials of $\mathcal{B}'$. Let $\bar{G}^s_t$ be the submatrix of G^s_t computed by taking only the terms of B'_t. It is noteworthy that $H(I,t) = rank(\bar{G}^s_t)$.

Let $G = \{f_1, \ldots, f_n\}$ be the reduced Gröbner basis of I with respect to a term-order $<$ and let

$$\mathcal{V}_t \quad = \quad \{x_i f_l \mid f_l \in \mathcal{B}'_{t-1}, i = 0, \ldots, r\} = \{p^*_1, \ldots, p^*_q\}.$$

Exploiting an observation of Marinari *et al.* (1993), in (Cioffi, 1999) the following statement is proved and is employed to design a minimalization procedure analogous to Ramella's one, but always with polynomial cost.

PROPOSITION 3.1. *A polynomial f_i of degree t of the reduced Gröbner basis G depends on $G - \{f_i\}$ if, and only if, it depends linearly on polynomials of the set $(G_t - \{f_i\}) \cup \mathcal{V}_t$.*

Proof. Cioffi (1999), Proposition 3.2. $\square$

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 $|G'_t| \neq 0$, then we consider a matrix M_t such that each row corresponds to one of the terms of B'_t. The last columns of M_t are the vectors of coefficients of the terms B'_t in the polynomials of G'_t. The first columns are computed in the following way. We consider all polynomials of $\mathcal{V}_t$ one after the other: if a polynomial p^*_i has a leading term belonging to B'_t, then we put the column of its coefficients in M_t; otherwise, if we have already considered a polynomial p^*_k such that $T(p^*_k) = T(p^*_i) \notin B'_t$, we put the column of coefficients of $p^*_i - p^*_k$ in M_t. Notice that the dimensions of M_t are of order $sr \times sr^2$. By Proposition 3.1, a polynomial f of G'_t is dependent if, and only if, the column corresponding to f does not contain a pivot of a row-echelon form of M_t.

As deduced in (Marinari *et al.*, 1993), the computational cost in field operation of the construction of G is of order $O(s^4 r)$. The same holds for G' and for $\mathcal{B}'$. In fact, the dimensions of a matrix $\bar{G}^s_t$ are always of order $s \times sr$ and a reduction of such a matrix is of order $O(s^3 r)$. Since we compute no more than s matrices $\bar{G}^s_t$, the cost of the construction of $\mathcal{B}'$ is of order $O(s^4 r)$.

Computing the matrix M_t needs no more than $s^2(r+1)^3$ subtractions. The computational cost of the reduction of M_t to a row-echelon form is of order $O(s^3 r^4)$. Thus the order of the cost of the described method of minimalization is $O(s^4 r^4)$. Notice that the cost of the computation and of the evaluation of the terms is lower than $O(s^4 r^4)$. The ordering of terms needs no more than $s^2(r+1)^2$ comparisons.

As it is stated in (Cioffi, 1999), in case the points are in generic position or all the points have the same i-th coordinate non null, the computational cost is of order $O(s^3 r^4)$.

3.2. Computing minimal generators of the ideal of a union of rational curves via points

We can now formulate the main steps of an algorithm to construct minimal homogeneous generators of a union C of parametric projective curves $C_1, \ldots, C_h$ in polynomial time.

ALGORITHM

Input: number h of irreducible rational parametric components $C_1, \ldots, C_h$ of a curve C; functions of a rational representation of each C_i over a field K.
Output: a minimal set of homogeneous generators of the ideal of the curve $I(C)$, the Hilbert function $H(I(C), t)$, the Hilbert polynomial and the Poincaré series of $I(C)$.

begin

1. $t = 0$, $m = 1$, $X = \emptyset$
2. for every curve C_i, determine a polynomial representation where the polynomials have not a common factor; let $d_i \geq deg(C_i)$ be the degree of such polynomials and set $d = \sum_{i=1}^{h} d_i$
3. **while** $t < m$ **do**

  3.1. set $t = t + 1$
  3.2. **for** $i = 1, \ldots, h$ **do**

    if $t = 1$ **then**

      compute a set X_1^i of $d_i + 1$ points of C_i
      determine the integer r_i of Theorem 2.1 and set $m = \sum_{i=1}^{h}(d_i + 2 - r_i)$

    else

      compute a set X_t^i of d_i rational points of C_i disjoint from $\cup_{j=1}^{t-1} X_j^i$

    endif

  endfor
  3.3. set $X = X \cup (\cup_{i=1}^{h} X_t^i)$
  3.4. construct minimal generators of degree t of the ideal of X and compute $H(I, t)$ by the algorithm of (Cioffi, 1999)
  3.5. **if** $H(I, t) = dt + h$ (Theorem 2.3) and $m \neq t$ **then**

    $m = t + 1$

  else

    if the hypotheses of Theorem 2.4 are true **then** $m = t$ **endif**

  endif

endwhile
4. compute the Hilbert polynomial and the Poincaré series of $I(C)$

end

The computational cost is polynomial in the degree d of the curve C, in the dimension

r of the projective space and in the number h of irreducible components of C. Indeed, the procedure consists of the application of the algorithm of (Cioffi, 1999) over a set of computed points of the assigned curve, but with a different termination criterion. The cost depends on the number of points of the curve which we need to compute: recall that we determine at most $d\left(\sum_{i=1}^{h} m_i\right) + h$ points, where $d_i\left(\sum_{i=1}^{h} m_i\right) + 1$ of them belong to the irreducible components C_i of degree d_i and have to be different. We stop the execution of the algorithm for points at a degree no higher than $m = \sum_{i=1}^{h} m_i$. Thus, in output we obtain a minimal set of homogeneous generators of $I(C)$. Notice that $\sum_{i=1}^{h} m_i$ is no higher than $\sum_{i=1}^{h} d_i = d$. If we have s points, the algorithm of (Cioffi, 1999) has a computational cost of order $O(r^4 M s^3)$, where M is the maximum degree of polynomials constructed. In the case of curves, M can be no higher than the upper bound m for the regularity.

If C is an irreducible curve of degree d and r_1 is the minimum dimension of a linear variety containing C, the computation of a minimal generators of $I(C)$ is of order

$$O(r^4(d+2-r_1)(d(d+2-r_1)+1)^3) = O(r^4 d^3 (d+2-r_1)^4). \tag{3.2}$$

In general, let C be the union of h rational parametric curves $C_1, \ldots, C_h$ of degrees respectively no higher than $d_1, \ldots, d_h$. Hence, the degree of C is no higher than $d = \sum_{i=1}^{h} d_i$. Then, with the notation of Theorem 2.1, we need at most $d\left(\sum_{i=1}^{h} m_i\right) + h$ points of C. It can happen that an irreducible component C_i is a line. So, we suppose that the last q components of C are lines $(0 \leq q \leq h)$ and that the others are not lines. Notice that

$$\sum_{i=1}^{h} m_i = \sum_{i=1}^{h} d_i + 2(h-q) - \sum_{i=1}^{h-q} r_i = d + 2(h-q) - \sum_{i=1}^{h-q} r_i, \tag{3.3}$$

$$d\sum_{i=1}^{h} m_i + h = d\left(d + 2(h-q) - \sum_{i=1}^{h-q} r_i\right) + h. \tag{3.4}$$

Of course, h is no higher than d and so the cost of the algorithm is of the following order

$$O\left(r^4\left(d+2(h-q)-\sum_{i=1}^{h-q} r_i\right)\left(d\left(d+2(h-q)-\sum_{i=1}^{h-q} r_i\right)+t\right)^3\right) =$$
$$= O\left(r^4 d^3\left(d+2(h-q)-\sum_{i=1}^{h-q} r_i\right)^4\right). \tag{3.5}$$

The previous formula includes the case of an irreducible curve, with $h = 1$, $q = 0$ and so with $\sum_{i=1}^{h-q} r_i = r_1$.

4. An implementation: tests and results

The described algorithm to implicitize rational projective curves has been implemented in a program called `Points` using C++ and NTL ("a Library for doing Number Theory", version 3.6b, http://www.shoup.net/ntl/). Our software is available by e-mail request to

Table 1. generic smooth curves

d	r	Points	CoCoA3.6	d	r	Points	CoCoA3.6
30	3	27.11	64.55	40	3	101.01	254.00
	4	6.66	35.45		4	23.43	125.87
	5	3.51	28.91		5	14.21	112.78
	6	7.23	57.81		6	11.96	99.78
	7	3.80	32.8		7	28.55	296.63
	9	12.80	86.48		9	21.03	184.85
	11	4.25	40.24		11	62.39	430.98
	13	8.07	68.77		13	15.10	148.75
	15	15.00	112.40		15	25.62	221.95
50	3	297.90	829.98	60	3	604.27	2121.70
	4	68.63	448.84		4	107.10	813.92
	5	24.92	292.87		5	75.09	684.75
	6	21.56	252.98		6	81.65	819.27
	7	33.39	410.84		7	58.85	611.20
	9	32.04	390.95		9	45.36	590.78
	11	86.15	981.65		11	125.28	1284.17
	13	26.42	477.60		13	232.25	2166.30
	15	42.99	493.47		15	67.29	1090.16

one of the authors † or at `http://cds.unina.it/~orecchia/Edownload.html` or by anonymous ftp on `matna3.dma.unina.it`, directory `pub/Points99`.

In order to test the software, we ran it on randomly generated curves for increasing dimension r and degree d, on $K = \mathbf{Z}_p$, $p = 31991$. The tests have been performed on a Intel Pentium 200 MHz with 64 MB RAM + 100 MB swap, running Linux (kernel 2.0.31).

We have compared our results with the performance of the HilbertDriven algorithm to eliminate variables and to minimize a set of generators implemented in CoCoA 3.6 and in Singular 1.2 (same curves are considered for Points, CoCoA and Singular).

We ran the programs on various examples and it turns out that Points is particular suitable for curves whose representation is dense. This is due to the fact that the computational time of the methods based on the Gröbner bases depend on the number of the monomials involved in the computation whereas the computational time of Points is independent of this number.

In tables 1,2,3 we have reported three types of examples with dense representation: generic smooth curves, singular curves and unions of generic smooth curves (the time is reported in seconds). The representation of our singular curves is of the following type:

$$x_i = a_{i_0}u^d + u^{d-1}v + a_{i_2}u^{d-2}v^2 + \sum_{j\in\{4,\ldots,d\}\cap \mathbf{N}_p} a_{i_j}u^{d-j}v^j, \quad i = 0, \ldots, r$$

where the coefficients a_{i_j} are generic. We do not report the timings of Singular because in general they are higher (for example, for a smooth curve of degree 30, Singular takes 24713.83 seconds in $\mathbb{P}^3$, 40026.67 seconds in $\mathbb{P}^4$ and 35252.15 seconds in $\mathbb{P}^5$).

We can remark that in some case CoCoA and Singular are not able to finish the computation, e.g. a generic curve of degree 80 in $\mathbb{P}^{10}$ (Points takes 132.74 seconds) or a

† albano@diima.unisa.it, {cioffi, orecchia, ramella}@matna2.dma.unina.it

Table 2. singular curves

d	r	Points	CoCoA3.6	d	r	Points	CoCoA3.6
30	2	64.42	232.11	40	2	333.11	1545.19
	3	30.73	61.27		3	120.63	250.13
	5	3.14	22.10		5	13.84	101.64
	7	3.34	24.13		7	24.08	106.41
	9	9.96	33.69		9	18.37	120.19
	11	20.73	36.70		11	42.34	130.17
	13	40.75	47.71		13	80.68	135.67
	15	8.80	54.09		15	128.27	152.91
60	5	73.83	609.23	70	5	102.97	973.21
	7	53.59	474.04		7	72.57	751.10
	9	177.38	635.11		9	241.83	1035.11
	11	102.20	893.77		11	131.51	1141.49
	13	218.37	1012.32		13	304.15	2786.92
	15	358.91	920.17		15	550.48	2130.91

Table 3. unions of generic smooth curves

r	example	Points	CoCoA3.6
3	1 curve of $deg = 1$ + 3 curves of $deg = 2$	0.04	0.54
3	4 curves of $deg = 2$	0.11	0.68
4	5 curves of $deg = 5$	4.36	36.64
5	6 curves of $deg = 6$	10.07	158.65
10	10 curves of $deg = 8$	41.37	1719.72

singular curve of degree 70 in $\mathbb{P}^3$ (Points takes 1863.68 seconds) or the union of a generic curve of degree 20 and a generic curve of degree 30 in $\mathbb{P}^3$ (Points takes 301.93 seconds and CoCoa 3.6 takes 1559.44).

Acknowledgements

This work has been partially supported by Consiglio Nazionale delle Ricerche, Progetto Strategico “Applicazione della Matematica per la Tecnologia e la Società”, sottoprogetto “Calcolo Simbolico”, and by MURST 40%.

We thank A. De Paris for useful discussions and J. Abbott who informed us of the availability of the NTL.

References

Bayer, D., Stillman, M. (1987). A criterion for detecting m-regularity. *Invent. math.*, **87**, 1–11.

Capani, A., Niesi, G., Robbiano, L. (1995). CoCoA, a system for doing Computations in Commutative Algebra. *Available via anonymous ftp from cocoa.dima.unige.it* .

Cioffi, F. (1996). Calcolo di generatori di ideali di punti e curve algebriche. Tesi di Dottorato di Ricerca, Preprint n. 23, 1996, Dip. di Mat. e Applic. “R. Caccioppoli”, Univ. di Napoli “Federico II”.

Cioffi, F. (1999). Minimally generating ideals of points in polynomial time using linear algebra. *Ricerche di Matematica*, Vol. XLVIII, Fasc. 1^o.

Eisenbud, D., Goto, S. (1984). Linear Free Resolution and Minimal Multiplicity. *J. of Algebra*, **88**, 89–133.

Fix, G., Hsu, C., Luo, T. (1996). Implicitization of rational Parametric Surfaces. J. Symbolic Computation, **21**, 329–336.

Gao, X.-S., Chou, S.-C. (1992). Implicitization of rational Parametric Equations. J. Symbolic Computation, **14**, 459-470.

Green, M. (1996). Generic Initial Ideals. Notes of the main lectures given at the "Summer School of Commutative Algebra", CRM in Bellaterra, Spain.

Greuel, G.-M., Pfister, G., Schönemann, H. (1998). Singular version 1.2 User Manual. *Reports On Computer Algebra*, number 21. Centre for Computer Algebra, University of Kaiserslautern, June 1998. `http://www.mathematik.uni-kl.de/~zca/Singular`

Gruson, L., Lazarsfeld, R., Peskine, C. (1983). On a Theorem of Castelnuovo and the Equations Defining Space Curves. *Invent. math.*, **72**, 491–506.

Harris, J. (1992). *Algebraic Geometry: a First Course*. Springer Verlag New York, Inc.

Kalkbrener, M. (1991). Implicitization for rational parametric curves and surfaces. L.N.C.S. **508**, 249–259, Springer Verlag.

Licciardi, S., Mora, T. (1994). Implicitization of hypersurfaces and curves by the Primbasissatz and basis conversion. *Proc. of ISSAC'94*, 191–196.

Manocha, D., Canny, J.F. (1992). Implicit Representation of Rational Parametric Surfaces. J. Symbolic Computation, **13**, 485–510.

Maroscia, P., Nagel, U., Vogel, W. (1990). On degree bounds for the syzygies of a finite set of points in $\mathbb{P}^n$.*Rend. Sem. Mat. Univ. Pol. Torino*, **48**, 4 491–510.

Marinari, M. G., Möller, H. M., Mora, T. (1993). Gröbner Bases of Ideals Defined by Functionals with an Application to Ideals of Projective Points. *AAECC*, **4**, 103–14

Migliore, J.C. (1998). *Introduction to Liaison Theory and Deficiency Modules*. Progress in Mathematics 165, Birkhäuser.

Möller, H. M., Buchberger, B. (1982). The construction of multivariate polynomials with preassigned zeros. EUROCAM 82, L.N.C.S. **144**, 24–31, Springer Verlag.

Nagel, U. (1990). On Castelnuovo's regularity and Hilbert's functions. *Comp. Math* **76**, 265–279.

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.

Orecchia, F. (1998). The ideal generation conjecture for s general rational curves in $\mathbb{P}^r$. Preprint n. 42, 1998, Dip. di Mat. e Applic. "R. Caccioppoli", Univ. di Napoli "Federico II". To appear in Journal of Pure and Appl. Algebra.

Ramella, I. (1989). An algorithmic approach to ideal generation of points. *Rend. Accad. Sci. Fis. Mat.*, **56**, 72–81.

Ramella, I. (1990). Algoritmi di Computer Algebra relativi agli ideali di punti dello spazio proiettivo. Tesi di Dottorato di Ricerca, Preprint n. 30, 1990, Dip. di Mat. e Applic. "R. Caccioppoli", Univ. di Napoli "Federico II".

Ramella, I. (1994). Generators of ideals of curves: some polynomial algorithms for their computation. *Zero-Dimensional Schemes (Proc. of the International Conference held in ravello*, June 8-13, 1992; Eds. F. Orecchia, L. Chiantini). W. de Gruyter, 299–305.

Traverso, C. (1996). Hilbert Functions and the Buchberger Algorithm. *J. Symbolic Computation*, **22**, 355–376.

Shoup, V. (1999). NTL: a Library for doing Number Theory. Available at `http://www.shoup.net/ntl`.