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

Implicitization of a general union of parametric varieties

F. ORECCHIA*

* *Dip. di Mat. e Appl. "R. Caccioppoli", Univ. di Napoli "Federico II", Napoli, Italy*

(Received)

We reconduct the computation of the equations defining a union V of parametric varieties, up to a given degree d, to the computation of the equations, of degree $\leq d$, vanishing on a finite set of points of V. If V is general this gives a new algorithm for implicitizing V. We have compared the implementation of this algorithm with the Hilbert driven elimination algorithm included in CoCoA 3.7 and Singular 1.2, obtaining significant improvements in timings. Moreover the implementation of the algorithm leads to two intriguing conjectures on the natural number of generators of the union of general parametric curves or surfaces.

1. Introduction

The problem of determining an implicite representation of an irreducible algebraic variety given by a rational parametrization has been faced by elimination theory and can be solved by the computation of Gröbner bases or by the computation of resultants (see, for example, Kalkbrener (1991), Gao and Chou (1992), Licciardi and Mora (1994), Fix *et al.* (1996), Manocha and Canny (1992), Chionh and Goldman (1992) and references therein). The methods based on the computation of Gröbner bases have been implemented in CoCoA3.7 and Singular1.2 and have taken advantage from the Hilbert driven algorithm (Traverso, 1996). In this paper we consider the implicitization of a general parametric variety V and we introduce an alternative method that reconducts the implicitization of V to the computation of equations that define a finite set of points of V. This allows us to use some known algorithms that construct minimal generators and Hilbert functions of ideals of projective points in a time polynomial in the number of points and in the dimension of the projective space (Orecchia (1991); Ramella (1994), Marinari *et al.* (1993); Cioffi (1999)). We show that the implementation of this new algorithm of implicitization is more efficient than the ones contained in CoCoA3.7 and Singular1.2. Moreover our approach can be applied with no significant changes to the implicitization of a general union $V = \bigcup_{i=1}^{q} V_i$ of projective parametric varieties. In this case it works much more efficiently with respect to the other procedures that first implicitize all the varieties V_i, and then compute the equations defining V by ideal intersection.

Let $\mathbb{P}^n$ denote the projective n-dimensional space over an algebraically closed field k. Let $V = \bigcup_{i=1}^{q} V_i \subset \mathbb{P}^n$ be the union of parametric varieties V_i parametrized by maps $\Phi_i : \mathbb{P}^{m_i} \to \mathbb{P}^n$, $m_i < n$ for any i, given by homogeneous polynomials of the same degree

0747–7171/90/000000 + 00 $03.00/0

r_i. Let $I(V) \subset R = k[X_0, ..., X_n]$ be the ideal of V. Fix an integer d, and let $P_1^{(i)}, ..., P_{N_i}^{(i)}$ be $N_i = \binom{dr_i+m_i}{m_i}$ be points of $\mathbb{P}^{m_i}$ in generic position such that $Q_j^{(i)} = \Phi_i(P_j^{(i)})$ form a set T of $N = \sum_{i=1}^{q} N_i$ points of $\mathbb{P}^n$. Let f be a homogeneous polynomial in $n+1$ variables with degree $\deg f \leq d$. The equation $f = 0$ defines V (i.e. $f \in I(V)$) if and only if it defines T (i.e. $f \in I(T)$). Hence the generators of degree $\leq d$ of the ideal $I(V)$ of a union of parametric varieties V are the generators of an ideal of an appropriate set of points in V.

To use this result we need an upper bound for the degrees of the forms that can generate $I(V)$. Such bound has to depend only on n, r_i and m_i, We shall use Castelnuovo-Mumford regularity to get this bound for generic unions of varieties V_i.

In fact, set $m = \max\{m_1, \ldots, m_q\}$. Denote by $H_V(d) = \binom{d+n}{n} - \dim_k I(V)_d$ the Hilbert function of the ring $R/I(V)$ and by $reg(V)$ the Castelnuovo-Mumford regularity of V. The varieties V_i are pairwise disjoint, smooth of dimension m_i and degree $r_i^{m_i}$, with parametric representation given by polynomials without base points if and only if $H_V(d) = \sum_{i=1}^{q} \binom{dr_i+m}{m}$ for some $d > 0$. If this is the case $reg(V) \leq \sigma = \min\{d \geq m \mid H_V(d) = \sum_{i=1}^{q} \binom{dr_i+m_i}{m_i}\} + 1$ and $I(V)$ is generated in degree σ. By Theorem 3.1 the situation above actually occours when $2m_i < n$, for any i, and the union V is general (i.e. the coefficients of the polynomials that represent V_i are generically chosen).

These results give an efficient algorithm (ALGORITHM II) for implicitizing a general union of parametric varieties V (actually the algorithm computes a minimal set of generators of the ideal $I(V)$ of V). We have compared the implementation of this algorithm with the Hilbert driven elimination algorithm included in the softwares CoCoA 3.7 and Singular 1.2, obtaining significant improvements in timings.

Note that the case of union $C = \bigcup_{i=1}^{q} C_i \subset \mathbb{P}^n$ of parametric curves (i.e. $m_i = 1$ for any i), which has been the starting point of the present work, was already treated in (Orecchia, 1998). In this case any set of points of $\mathbb{P}^1$ is in generic position Theorem 3.1 specialises as follows.

C is smooth of degree $r = r_1 + \ldots + r_q$ if and only if $H_C(d) = dr + q$, for some positive integer d. If this is the case $reg(C) = \min\{d \in \mathbf{N} \mid H_C(d) = dr + q\} + 1$ (Orecchia (1998), Proposition 1.5). Moreover $H_C(d) = dr + q$ for some d if C is general(Orecchia (1998), Corollary 2.6).

As a main application of ALGORITHM II, we show that its implementation over finite fields $\mathbf{Z}_p$ of integers modulo a prime p can be used to study the natural number of minimal generators of the ideal of a union $V = \bigcup_{i=1}^{q} V_i \subset \mathbb{P}^n$ of general parametric varieties V_i of same dimension, over any field of characteristic zero. We say that V is naturally generated when the two natural maps $H^0(\mathcal{O}_{\mathbb{P}^n}(d)) \to H^0(\mathcal{O}_V(d))$ and $H^0(I_V(d)) \otimes H^0(\mathcal{O}_{\mathbb{P}^r_k}(1)) \to H^0(I_V(d+1))$ have maximal rank for any $d > 0$. As a consequence in Orecchia (1998) we posed and proved by computer, for irreducible curves C of degree ≤ 80 and for reducible curves of degree ≤ 40 in projective spaces of dimension ≤ 10, the following:

Ideal Generation Conjecture for Rational Curves

Let the base field k of $\mathbb{P}^n$ have characteristic zero. For every positive integers $n, r_1, ..., r_q$, $n \geq 3$, the non-degenerate union $C = \bigcup_{i=1}^{q} C_i \subset \mathbb{P}^n$ of general parametric curves C_i of degree r_i is naturally generated except for the following q-tuples $(r_1, ..., r_q)$.

If $n = 3$: $(5); (1,2); (2,2); (2,3); (2,4); (2,5); (3,4); (1,1,2); (1,2,2); (1,2,4); (2,2,2); (2,2,3); (2,2,4); (1,1,1,1); (1,2,2,2); (2,2,2,2); (1,2,2,2,2)$.

If $n = 4 : (5); (1,3); (2,3); (1,1,2)$.

If $n = 5 : (3,4); (1,2,3); (2,2,2)$.

By using a more powerful personal computer, we prove in this paper the ideal generation conjecture for irreducible curves C of degree ≤ 120 and for reducible curves of degree ≤ 60 in projective spaces of dimension ≤ 20.

In the case of union $S = \bigcup_{i=1}^{q} S_i \subset \mathbb{P}^n$, $n \geq 5$ of parametric surfaces in this paper we prove for irreducible surfaces C of degree ≤ 64 and for reducible surfaces of degree ≤ 40 in projective spaces of dimension ≤ 20, the following

Ideal Generation Conjecture for General Parametric Surfaces

Let the base field k of $\mathbb{P}^n$ have characteristic zero. For every positive integers $n, r_1, ..., r_q$, $n \geq 5$, the non-degenerate union $V = \bigcup_{i=1}^{q} V_i \subset \mathbb{P}^n$ of general parametric surfaces V_i of degree r_i^2 is naturally generated except for the following q-tuples $(r_1, ..., r_q)$.

If $n = 5 : (1,1,1); (1,1,2); (1,1,1,1)$.

If $n = 6 : (1,2); (2,2); (1,1,1); (2,2,2)$.

If $n = 7 : (3); (2,2); (1,1,1); (2,1,1); (1,1,1,1)$.

If $n = 8 : (1,3); (1,2,2); (2,1,1,1)$.

If $n = 10 : (3,2,1)$.

In all the paper $\mathbb{P}^n$ denotes the projective space of dimension n over an algebraically closed field k.

2. Computing the equations of a union of parametric varieties to any given degree via points.

Definition 2.1. *We say that an algebraic variety $V \subset \mathbb{P}^n$ of dimension > 0 is parametric if there is a rational map $\Phi : \mathbb{P}^m \to \mathbb{P}^n$, $m < n$, given by homogeneous polynomials of the same degree r whose image is a dense subset of V.*

Let $A = R/I(V)$ be the homogeneous coordinate ring of V. From now on $H_V(d) = \dim_k A_d = \dim_k R_d - \dim_k I(V)_d = \binom{d+n}{n} - \dim_k I(V)_d$ will always denote the *Hilbert function* of V and $P_V(d)$ the *Hilbert polynomial* of V.

Definition 2.2. (*Orecchia*, 1981) *A set $S = \{P_1, ..., P_N\} \subset \mathbb{P}^m$ of $N = \binom{d+m}{m}$ points is in generic position if it is not contained in a hypersurface of degree d.*

Lemma 2.1. *Let $V = \bigcup_{i=1}^{q} V_i \subset \mathbb{P}^n$ be the union of parametric varieties V_i parametrized by maps $\Phi_i : \mathbb{P}^{m_i} \to \mathbb{P}^n$, $m_i < n$ for any i, given by homogeneous polynomials of the same degree r_i. Let d be a fixed integer, and $P_1^{(i)}, ..., P_{N_i}^{(i)}$ be $N_i = \binom{r_i d + m_i}{m_i}$ points of $\mathbb{P}^{m_i}$ in generic position such that $Q_j^{(i)} = \Phi_i(P_j^{(i)})$ form a set T of $N = \sum_{i=1}^{q} N_i$ points of $\mathbb{P}^n$. If f is a polynomial in $n+1$ variables with degree $\deg f \leq d$ then $f = 0$ is an equation* *defining V if and only if $f = 0$ is an equation defining T. In other terms the two sets $I(V)_{d'} = \{f \in I(V) \mid \deg f = d'\}$ and $I(T)_{d'} = \{f \in I(T) \mid \deg f = d'\}$ are equal for any $d' \leq d$. Hence $H_V(d') = H_T(d')$, for any $d' \leq d$.*

Proof. Let V be irreducible (i.e. $q = 1$). We set $m = m_1$, $r = r_1$, $\Phi = \Phi_1$, $P_j = P_j^{(1)}$. Let $f_i \in k[t_0, ..., t_m]$, $i = 0, ..., n$, be the polynomials of degree r that represent parametrically V. Clearly $I(V)_{d'} \subseteq I(T)_{d'}$. We prove the other inclusion by contradiction. For any $f \notin I(V)_{d'}$ there exists a point $P \in \mathbb{P}^m$ such that $f(\Phi(P)) \neq 0$, so that $f(f_0, \ldots, f_n)$ is a non-zero polynomial of degree $d'r \leq dr$. Suppose now $f \in I(T)_{d'}$. The polynomial $f(f_0, \ldots, f_n)$ vanishes on the $N = \binom{dr+m}{m}$ points P_j and this contradicts the assumption of generic position.

To prove the reducible case it is enough to observe that $I(V) = \bigcap_{i=1}^{q} I(V_i) = \bigcap_{i=1}^{q} I(T_i) = I(T)$ where $I(T_i)$ is the ideal of the points $Q_j^{(i)}$, $j = 1, ..., N_i$. □

By Lemma 2.1 the computation of the generators of $I(V)$ is reconducted to the computation of the generators of a finite set of points.

Before starting the computation one has to find a set of points in generic position. Almost all sets of $N = \binom{d+m}{m}$ points $S = \{P_1, \ldots, P_N\} \subset \mathbb{P}^m$ are in generic position (Geramita and Orecchia, 1981). It follows that a random choice for the coordinates of the $P_j^{(i)}$ gives points in generic position. A systematic way of finding points in generic position in $\mathbb{P}^m$ is given by the following two results.

Proposition 2.1. *Let d and m be fixed positive integers and $a_{ij} \in k$, $i = 0, \ldots, d$, $j = 1, \ldots, m$. Suppose $a_{im} \neq a_{i'm}$, for any $i \neq i'$. No hypersurface of degree $\leq d$ contains The $N = \binom{d+m}{m}$ affine points in the set $S = \{(a_{i_1 1}, \ldots, a_{i_m m}) \in k^m \mid (i_1, \ldots, i_m) \in \mathbf{N}^m, i_1 + \ldots + i_m \leq d\}$. Hence the set of $N = \binom{d+m}{m}$ projective points*

$$S' = \{(a_{i_1 1} : \ldots : a_{i_m m} : 1) \in \mathbb{P}^m \mid i_1 + \ldots + i_m \leq d\}$$

is in generic position.

Proof. We shall prove the first part of the statement by induction. The second part follows then easily.

When $m = 1$ the set $S = \{a_i \in k \mid i \leq d\}$ consists of $d + 1$ points and no non-zero polynomial in one variable of degree d can have $d + 1$ distinct roots; hence the claim is true for any d.

Suppose now the claim true for $m - 1$. It follows that for any d, the set of the $N = \binom{d+m-1}{m-1}$ affine points $S_0 = \{(a_{i_1 1}, \ldots, a_{i_{m-1} m-1}) \in k^{m-1} \mid (i_1, \ldots, i_{m-1}) \in \mathbf{N}^{m-1}, i_1 + \ldots + i_{m-1} \leq d\}$ is not contained in a hypersurface of degree $\leq d$. We want to prove that any non-null polynomial $F(x_1, \ldots, x_m)$ vanishing on all points in S has degree greater then d.The polynomial $G_0(x_1, \ldots, x_{m-1}) = F(x_1, \ldots, x_{m-1}, a_{0m})$ vanishes on S_0, hence is null by the inductive hypothesis, then $F(x_1, \ldots, x_m) = (x_m - a_{0m})F_1$ where $\deg F_1 \leq d - 1$. Repeating the same argument for the polynomial $F_1(x_1, \ldots, x_{m-1}, a_{1m})$ and the set $S_1 = \{(a_{i_1 1}, \ldots, a_{i_{m-1} m-1}) \in k^{m-1} \mid (i_1, \ldots, i_{m-1}) \in \mathbf{N}^{m-1}, i_1 + \ldots + i_{m-1} \leq d - 1\}$ and so on, we get $F(x_1, \ldots, x_m) = \Pi_{q=0}^{d}(x_m - a_{qm})F'$ so that F has degree greater then d. □

From Proposition 2.1 the following result is immediately deduced .

Corollary 2.1. *Let d and m be fixed positive integers and $char(k) = 0$ or $char(k) \geq d$.*

The of $N = \binom{d+m}{m}$ *projective points, where* $i_j \in \mathbf{N}$ *is identified with* $i \cdot 1_k \in k$*, is in generic position*

$$S' = \{(i_1 : \ldots : i_m : 1) \in I\!\!P^m \mid (i_1, \ldots, i_m) \in \mathbf{N}^m, i_1 + \ldots + i_m \leq d\}$$

.

Corollary 2.1 suggests an algorithmic way to find a set of $N = \binom{dr+m}{m}$ distinct points $T = \{\Phi(P_1), \ldots, \Phi(P_N)\} \subset I\!\!P^n$ of a parametric variety V, such that $\{P_1, \ldots, P_N\}$ are in generic position. The following example concerns surfaces represented by polynomials without base points.

Example 2.1. *Let* $V \subset I\!\!P^n$ *be a parametric surface parametrized by the map* $\Phi : I\!\!P^2 \to I\!\!P^n$, $\Phi(t_0, t_1, t_2) = (f_0(t_0, t_1, t_2) : \ldots : f_n(t_0, t_1, t_2))$*, where* $f_i \in \mathbf{C}[t_0, t_1, t_2]$ *are homogeneous polynomials of degree* r*, without base points.The coordinates* $t_0 = 0$, $t_2 = 1$ *and* $t_1 = 0,1,2,3,\ldots,dr$ *give* $dr + 1$ *points in* $I\!\!P^2$*. The coordinates* $t_0 = 1$, $t_2 = 1$ *and* $t_1 = 0, 1, 2, 3, \ldots, dr - 1$ *give then* dr *points of* $I\!\!P^2$*, and* $t_0 = 2, t_2 = 1, t_1 = 0, 1, 2, 3, \ldots, dr - 2$ *give* $dr-1$ *points. At the end of this process we have* $(dr+1)(dr)(dr-1)\ldots 2 = N = \binom{dr+2}{2}$ *points* $\{P_1, \ldots, P_N\}$ *of* $I\!\!P^2$ *that are in generic position, by Corollary 1.5.*

By the previous results for determining a minimal set of generators up to a given degree d of the ideal of a union of parametric varieties, one can compute a minimal set of generators, up to d, of the ideal of a finite set of points. This last computation can be reconducted to the computation of ranks and bases of null spaces of matrices with coefficients in k as we are going to show.

Let $T = \{P_1, ..., P_s\}$ be a set of points in the projective space $I\!\!P^n$. Let d be a positive integer. The vector space $I(T)_d$ is easily given by the null space of a matrix with elements in k. In fact if $R_d = \{f \in k[X_0, ..., X_n] \mid deg(f) = d\}$ then:

$$I(T)_d = \{f \in R_d \mid f(P_i) = 0, i = 1, ..., s\} \tag{2.1}$$

Denoted by $\mathcal{T}_i$, $i = 1, ..., u$, the terms of degree d in the indeterminates $X_0, ..., X_n$ ordered with respect to any term ordering, the set $S = \{\mathcal{T}_1, ..., \mathcal{T}_u\}$ is a basis of the k-vector space R_d. We consider now a $\binom{d+n}{n} \times s$ matrix:

$$G_d(T) = (\mathcal{T}_i(P_j)) \tag{2.2}$$

whose generic element $\mathcal{T}_i(P_j)$ is the evaluations of the term $\mathcal{T}_i$ at the point P_j

We also set

$$(f)_S = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_u \end{pmatrix}$$

if $f = a_1\mathcal{T}_1 + ... + a_u\mathcal{T}_u \in k[X_0, ..., X_n]$.

We have:

$$I(T)_d = \{f \in R_d \mid G_d(T)(f)_S = 0\} \tag{2.3}$$

In other words $f \in I(T)_d$ if and only if $(f)_S$ is a vector of the null space $N_d(T)$ of the matrix $G_d(T)$. In (Geramita and Orecchia, 1981) some elementary linear algebra is used to show that $dim_k(I(T)_d = \binom{d+n}{n} - rk(G_d(T))$ $(rk = rank)$ i.e.

$$rk(G_d(T)) = H_T(d) \tag{2.4}$$

.

Let $I(T)_d \neq 0$ and $\{(g_1)_S, ..., (g_e)_S\}$ a basis of $N_d(T)$, $e = \binom{d+n}{n} - rk(G_d(T))$. Denote by W_{d+1} the vector space generated by the $e(r+1)$ polynomials g_iX_j of $I(T)_{d+1}$. Let:

$$M_{n+1}(T) = ((g_1X_1)_S \vdots \cdots \vdots (g_iX_j)_S \vdots \cdots \vdots (g_eX_{n+1})_S) \tag{2.5}$$

be the $\binom{d+n+1}{n} \times e(n+1)$ matrix whose columns are $(g_iX_j)_S$, for any i, j.

Note that an entry of $(g_iX_j)_S$ is zero, if it corresponds to a term that does not appear in the polynomial g_iX_j, or is a coefficient of g_iX_j that is a component of the vector $(g_i)_S$.

We have:

$$dim_k(W_{d+1}) = rk(M_{d+1}(T)) \tag{2.6}$$

Now consider the columns of $M_{d+1}(T)$ which contain a non-null minor of order $rk(M_{d+1}(T))$. These are linearly independent vectors of the null space $N_{d+1}(T)$ of the matrix $G_{d+1}(T)$and then they can be completed to a basis of $N_{d+1}(T)$ by Gauss reduction). If $\{(h_1)_S, ..., (h_e)_S\}$ are the vectors of this completion, then $\{h_1, ..., h_e\}$ are the elements of degree d in a minimal set of generators of $I(T)$. These results allow to construct an algorithm (Ramella, 1994) that computes the Hilbert function and a minimal set of generators of the ideal $I(T)$ of s points up to a given degree d by using only Gauss reduction of matrices with coefficients in the base field k. This algorithm has been firstly refined in (Orecchia, 1991), to an algorithm that computes the Hilbert function of the ideal $I(T)$ of s points up to a given degree d with polynomial computational cost of order $O(nds^3)$, and later on in Cioffi (1999) (by using results of (Marinari *et al.*, 1993)) to an algorithm that computes also a minimal set of generators of $I(T)$ up to a given degree d with polynomial computational cost of order $O(n^4ds^3)$. The implementation of the algorithm of (Cioffi, 1999) is available in (Orecchia *et al.*, 1999). Thus using this last algorithm, Lemma 2.1 and Corollary 2.1 it is easy to construct the following algorithm that computes the elements of degree $\leq d$ in a minimal set of generators of the ideal of a parametric variety to any given degree d.

ALGORITHM I

Input: degrees and coefficients of the polynomials that represent a union of parametric varieties V; maximum degree d of the generators of V to compute.
Output: Elements of degree $\leq d$ in a minimal set of homogeneous generators of the ideal $I(V)$ and Hilbert function of V.

1. Set $d' = 1$.
2. Computation, relatively to degree d', of the set T of points of Lemma 2.1 (using Proposition 2.1).
3. Application to the computed points of V of the algorithm of (Cioffi, 1999), in which the elements of degree $= d'$ of a minimal set of generators of $I(T)$ are constructed and the Hilbert function, in degree t is computed.
4. $d' = d' + 1$
5. If $d' = d + 1$ stop else goto **2**

By the previous considerations, fixed the integers n, m_i, r_i, d, if $V = \bigcup_{i=1}^{q} V_i \subset \mathbb{P}^n$ is the union of parametric varieties V_i parametrized by maps $\Phi_i : \mathbb{P}^{m_i} \to \mathbb{P}^n$, $m_i < n$ for any i, given by homogeneous polynomials of the same degree r_i, the computational cost of Algorithm I is polynomial of order $O(n^4 d s^3)$, where $s = \sum_{i=1}^{q} \binom{r_i d + m_i}{m_i}$.

Now we give two simple examples to show how the algorithm works. In both examples we consider the Lexicographic Order on the monomials of $k[X_0, ..., X_n]$.

Example 2.2 was also considered in (Manocha and Canny, 1992) and Fix *et al.* (1996).

EXAMPLE 2.2. *Consider the parametric surface $V \subset \mathbb{P}^3$, over a field of characteristic zero, parametrized by the map $\Phi : \mathbb{P}^2 \to \mathbb{P}^3$, $\Phi(s : t : u) = (st^2 - tu^2 : stu + su^2 : 2su^2 - 2tu^2 : st^2)$. As input in Algorithm I we consider $d = 2$. If $d' = 1$ by Lemma 2.1 we have to compute a set T of $\binom{2 \cdot 1 + 2}{2} = 6$ ($r_i = r_1 = 2$, $m_i = m_1 = 2$) points on V that are the image under Φ of six points in generic position in $\mathbb{P}^2$. Using Proposition 2.1 we find the following six points*

$$P_1 = (0 : 1 : 1), P_2 = (1 : 1 : 1), P_3 = (2 : 1 : 1), P_4 = (0 : 2 : 1),$$
$$P_5 = (1 : 2 : 1), P_6 = (0 : 3 : 1)$$

of $\mathbb{P}^2$ which are obtained by setting in Proposition 2.1 $a_{ij} = i + j - 1$, $d = m = 2$.

Note that the point $P = (0 : 0 : 1)$ is a base point of the representation so we cannot use the points of Example 2.1. The corresponding points on V are

$$Q_1 = (-1 : 0 : -2 : 0), Q_2 = (0 : 2 : 0 : 1), Q_3 = (1 : 4 : 2 : 2),$$
$$Q_4 = (-2 : 0 : -4 : 0), Q_5 = (3 : 3 : -2 : 4), Q_6 = (-3 : 0 : -6 : 0)$$

and the matrix $G_1(T)$ is

$$\begin{pmatrix} -1 & 0 & 1 & -2 & 2 & -3 \\ 0 & 2 & 4 & 0 & 3 & 0 \\ -2 & 0 & 2 & -4 & -2 & -6 \\ 0 & 1 & 2 & 0 & 4 & 0 \end{pmatrix}$$

whose null space $N_1(T)$ has no solutions. Thus there are no generators of degree 1 in $I(V)$. Then we set $d' = 2$ in Algorithm I. By Lemma 2.1 and Proposition 2.1 we can consider the following set T of $\binom{2 \cdot 2 + 2}{2} = 15$ points on V:

$Q_1 = (-1 : 0 : -2 : 0), Q_2 = (0 : 2 : 0 : 1), Q_3 = (1 : 4 : 2 : 2), Q_4 = (-2 : 0 : -4 : 0),$
$Q_5 = (3 : 3 : -2 : 4), Q_6 = (-3 : 0 : -6 : 0), Q_7 = (2 : 6 : 4 : 3), Q_8 = (3 : 8 : 6 : 4),$
$Q_9 = (6 : 6 : 0 : 8), Q_{10} = (10 : 9 : 2 : 12), Q_{11} = (6 : 4 : -4 : 9), Q_{12} = (15 : 8 : -2 : 18),$
$Q_{13} = (-4 : 0 : -8 : 0), Q_{14} = (12 : 5 : -6 : 16), Q_{15} = (-5 : 0 : -10 : 0)$

corresponding to the points in generic position in $\mathbb{P}^2$

$P_1 = (0 : 1 : 1), P_2 = (1 : 1 : 1), P_3 = (2 : 1 : 1), P_4 = (0 : 2 : 1), P_5 = (1 : 2 : 1),$
$P_6 = (0 : 3 : 1), P_7 = (3 : 1 : 1), P_8 = (4 : 1 : 1), P_9 = (2 : 2 : 1), P_{10} = (3 : 2 : 1)$
$P_{11} = (1 : 3 : 1), P_{12} = (2 : 3 : 1), P_{13} = (0 : 4 : 1), P_{14} = (1 : 4 : 1), P_{15} = (0 : 5 : 1)$

obtained by setting in Proposition 2.1 $a_{ij} = i + j - 1$, $d = 4, m = 2$. *Note that* $Q_{13} = Q_{15} = (1 : 0 : 2 : 0)$. *This is not a contradiction: it can happen that two distinct points* P_j *and* $P_{j'}$ *of* $\mathbb{P}^2$ *have the same image* $Q_j = \Phi(P_j) = Q_{j'} = \Phi(P_{j'})$. *It comes out that we can consider only* 14 *points instead of* 15. *The matrix* $G_2(T)$ *is*

$$\begin{pmatrix}
1 & 0 & 2 & 0 & 0 & 0 & 0 & 4 & 0 & 0 \\
0 & 0 & 0 & 0 & 4 & 0 & 2 & 0 & 0 & 1 \\
1 & 4 & 2 & 2 & 16 & 8 & 8 & 4 & 4 & 4 \\
1 & 0 & 2 & 0 & 0 & 0 & 0 & 4 & 0 & 0 \\
4 & 6 & -4 & 8 & 9 & -6 & 12 & 4 & -8 & 16 \\
9 & 0 & 18 & 0 & 0 & 0 & 0 & 36 & 0 & 0 \\
2 & 6 & 4 & 3 & 18 & 12 & 9 & 8 & 6 & 9 \\
9 & 24 & 18 & 12 & 64 & 48 & 32 & 36 & 24 & 16 \\
36 & 36 & 0 & 48 & 36 & 0 & 48 & 0 & 0 & 64 \\
100 & 90 & 20 & 120 & 81 & 18 & 108 & 4 & 24 & 144 \\
36 & 24 & -24 & 54 & 16 & -16 & 36 & 16 & -36 & 81 \\
225 & 120 & -30 & 270 & 64 & -16 & 144 & 4 & -36 & 324 \\
16 & 0 & 32 & 0 & 0 & 0 & 0 & 64 & 0 & 0 \\
144 & 60 & -72 & 192 & 25 & -30 & 80 & 36 & -96 & 256
\end{pmatrix}$$

and a basis of the null space $N_2(T)$ *is* $(4, 8, -4, -4, 4, -4, -8, 1, 2, 0)$ *which are the coefficients of the irreducible quadric* $4x_0^2 + 8x_0x_1 - 4x_0x_2 - 4x_0x_3 + 4x_1^2 - 4x_1x_2 - 8x_1x_3 + x_2^2 + 2x_2x_3 = 0$. *Since* V *is irreducible this is the implicit equation of the parametrization of* V.

EXAMPLE 2.3. *Consider the rational curve* $V \subset \mathbb{P}^3$, *over a field of characteristic zero, parametrized by the map* $\Phi : \mathbb{P}^1 \to \mathbb{P}^3$, $\Phi(s,t) = (s^6 : s^5t : s^4t^2 : t^6)$. *We set* $d = 3$ *in Algorithm I. If* $d' = 1$ *following Lemma 2.1 we consider the set* $T = \{(s^6, s^5, s^4, 1) \mid s = 0, ..., 6\}$ $(t = 1)$ *of* $6 \cdot 1 + 1 = 7$ $(r_i = r_1 = 6,\ m_i = m_1 = 1)$ *points on* V. *The matrix* $G_1(T)$ *has rank* 4 *and then* $N_1(T) = 0$ *and there is no generator of degree 1 in the ideal* $I(V)$. *Then we set* $d' = 2$ *in Algorithm I. Let* $T' = \{(s^6, s^5, s^4, 1) \mid s = 0, ..., 12\}$ *be a set of* $6 \cdot 2 + 1 = 13$ *points on* V. *A basis of the null space* $N_2(T')$ *of the matrix* $G_2(T')$ *is* $(0, 0, -1, 1, 0, 0)$. *This gives the coefficients of the generator* $f = x_1^2 - x_0x_2$ *of degree 2 of* $I(V)$. *Then we set* $d' = 3$ *in Algorithm I. Let* $T" = \{(s^6, s^5, s^4, 1) \mid s = 0, ..., 18\}$ *be a set of* $6 \cdot 3 + 1 = 19$ *points on* V. *To find the elements of degree 3 in a minimal set of generators of* $I(V)$ *we have to complete the vectors of coefficients of the polynomials* fX_0, fX_1, fX_2, fX_3 *to a basis of the null space of* $G_3(T)$. *This completion is (0,0,0,-1,0,0,0,0,0,1). It gives the coefficients of the generator* $g = x_2^3 - x_02x_3$ *of degree 3 of* $I(V)$. *So far we have computed a minimal set of generators up to degree* 3. *But it is easily seen that* $f = g = 0$ *defines an irreducible curve which thus coincides with* V. *Finally we have the implicitization required*

$$C : \begin{cases} x_1^2 = x_0x_2 \\ x_2^3 = x_02x_3 \end{cases}$$

In general Algorithm I is not so efficient as in the previous examples. To find an implicitization of V one has to know a bound for the degrees of a minimal set of generators of $I(V)$. There are various results in the literature (see Bayer *et al.* (1993)) concerning bounds for the maximum degree in a minimal set of generators of the ideal $I(V)$ of an irreducible projective variety but none of them is very useful as an efficient stop to Algorithm I. Moreover we do not know of any bound in the case of a union of irreducible varieties, unless these varieties are rational curves. In this case an efficient bound has been determined in Orecchia (1998) for smooth curves and in Albano *et al.* (1999) in the general case. In regularity will be used to get a very efficient bound for general unions of parametric varieties, which will lead to an algorithm of polynomial computational cost for implicitizing V.

3. Implicitization of a general union of parametric varieties

We need some geometric preliminaries.

A coherent sheaf $\mathcal{F}$ on $\mathbb{P}^n$ is d-regular if $H^i(\mathcal{F}(d-i)) = 0$ for $i > 0$. If $\mathcal{F}$ is d-regular, $\mathcal{F}$ is $d+1$-regular (Mumford (1966), Lecture 14).

Definition 3.1. *A variety $V \subset \mathbb{P}^n$ is d-regular if the sheaf $\mathcal{I}_V$ associated to the ideal $I(V)$ of V is d-regular. We set: $reg(V) = \min\{d \mid \mathcal{I}_V$ is d-regular$\}$.*

In the following we say that V *is generated in degree* n if the ideal $I(V)$ of V can be generated by forms of degree $\leq n$.

Proposition 3.1. *V is generated in degree $reg(V)$.*

Proof. see (Mumford (1966), p.99) □

Theorem 3.1. *Let $V = \bigcup_{i=1}^q V_i \subset \mathbb{P}^n$ be the union of parametric varieties V_i parametrized by maps $\Phi_i : \mathbb{P}^{m_i} \to \mathbb{P}^n$, $m_i < n$ for any i, $\Phi_i([t_{i0} : ... : t_{im_i}]) = [f_{i0}([t_{i0} : ... : t_{im_i}]) : ... : f_{in}([t_{i0} : ... : t_{im_i}])]$, where $f_{ij} = a_{ij_1}\mathcal{T}_1 + ... + a_{ij_u}\mathcal{T}_u$, $u = \binom{m_i+r_i}{m_i}$, are homogeneous polynomials of the same degree r_i. Set $m = \max\{m_1, \ldots, m_q\}$. Then:*

(a) $H_V(d) \leq \min\{\binom{d+n}{n}, \sum_{i=1}^q \binom{dr_i+m_i}{m_i}\}$, for any d;

(b) the varieties V_i are disjoint, smooth of dimension m_i and degree $r_i^{m_i}$. The parametrization is given by polynomials without base points, for any $i = 1, ..., q$, if and only if $H_V(d) = \sum_{i=1}^q \binom{dr_i+m_i}{m_i}$ for some $d > 0$. In this case $P_V(d) = \sum_{i=1}^q \binom{dr_i+m_i}{m_i}$ and $H_V(d') = \sum_{i=1}^q \binom{d'r_i+m_i}{m_i})\}$ for any $d' \geq d$;

(c) If there exists an integer $\sigma = \min\{d \geq m \mid H_V(d) = \sum_{i=1}^q \binom{dr_i+m_i}{m_i})\} + 1$, then $reg(V) \leq \sigma$, the ideal $I(V)$ is generated in degree σ and $H_V(d) = P_V(d)$, for any $d \geq \sigma - 1$;

(d) let $n > 2m_i$ for any i and denote with $(a_1, ..., a_s) = (a_h^{(ij)})$ the s-tuple ($s = \sum_{i=1}^q (n+1)\binom{m_i+r_i}{m_i}$)) of the coefficients of the polynomials that parametrize V_i. There exists an open non-empty subset U of the affine space $\mathbf{A}^s$ such that, for any $(a_1, \ldots, a_s) \in U$, $H_V(d) = \sum_{i=1}^q \binom{dr_i+m_i}{m_i}$ for any d.

Proof. First we prove the statements in the case of V irreducible (i.e. $q = 1$). We set $m = m_1$, $r = r_1$, $\Phi = \Phi_1$, $P_j = P_j^{(1)}$.

Let $\Phi(t_0, ..., t_m) = (f_0(t_0, \ldots, t_m), \ldots, f_n(t_0, \ldots, t_m))$, (where $f_i \in k[t_0, \ldots, t_m]$) are homogeneous polynomials of degree r) be the map that represents V.

(a) Since $H_V(d)$ is the dimension of A_d, the claim easily follows from the natural map:

$$\alpha : A_d \to K[t_0, \ldots, t_m]_{dr}$$

which is injective . In fact for all $F \in A_d = (k[X_0, \ldots, X_n]/I(V))_d$ put

$$\alpha(F) = F(f_0(t_0, \ldots, t_m), \ldots, f_n(t_0, \ldots, t_m)) \in k[t_0, \ldots, t_m]$$

and observe that α vanishes on all polynomials F which are 0 on V; conversely, if $F(P) \neq 0$ for some $P \in V$, then the same holds for some point in the image of Φ, i.e. there is a point $Q \in \mathbb{P}^m$ with $\alpha(F)(Q) \neq 0$, so that $\alpha(F)$ is not null. Hence the kernel of α is exactly $I(V)_d$ and α is injective.

(b) Assume that the equality $H_V(d) = \sum_{i=1}^{q} \binom{dr_i+m_i}{m_i}$ holds for a certain integer d. Then the polynomials $f_0(t_0, \ldots, t_m), \ldots, f_n(t_0, \ldots, t_m)$ generate all polynomials of degree d in $t_0, \ldots, t_m$ and this is clearly impossible unless they have no base points and separate points and tangent vectors; it follows that Φ is a regular embedding. Hence V is smooth of dimension m, degree r^m and its parametrization has no base point. Conversely, if V is isomorphic to $\mathbb{P}^m$, then its Hilbert polynomial is $\binom{dr+m}{m}$.

(c) Note that if σ exists, then V is isomorphic to $\mathbb{P}^m$ and the restriction map $H^0(\mathcal{O}_{\mathbb{P}^n}(\sigma - 1)) \to H^0(\mathcal{O}_V(\sigma - 1))$ surjects; this implies $H^1(\mathcal{I}_V(\sigma - 1)) = 0$ and $H^i(\mathcal{I}_V(\sigma - i)) = H^{i-1}(\mathcal{O}_V(\sigma - i)) = H^{i-1}(\mathcal{I}_{\mathbb{P}^m}(r(\sigma - i)))$ for $n > i > 1$. Since $\sigma \geq m$ these cohomology groups vanish for $i > 0$. Hence V is σ-regular. By the previous results this fact implies (c).

(d) First we prove that for any $m, r > 0$ and $n > 2m$ there exists a V_0 which is smooth, of dimension m and degree r^m. Take a general projection in $\mathbb{P}^n$ of the Veronese embedding of $\mathbb{P}^m$, which is defined by a basis for the space of homogeneous polynomials of degree n; the corresponding map Φ_0 is a smooth embedding, so there exists a d_0 such that $H_{V_0}(d) = \binom{dr+m}{m}$ for all $d \geq d_0$. By (Geramita and Orecchia, 1981) $H_{V_0}(d)$ is equal to the rank $\rho(M)$ of a matrix M whose elements are monomials evaluated at the coordinates of the points of the set T of Lemma 2.1 (relatively to degree d_0). Then, by (a) $\rho(M) \leq \binom{d_0r+m}{m}$, and $\rho(M)$ is maximal if and only if $\rho(M) = \binom{d_0r+m}{m}$ that is $(a_0, ..., a_q)$ is not the solution of a finite set of polynomials, i.e. it belongs to an open set of $\mathbf{A}^q$.

The general case follows easily from the previous results and from the following well known facts about Hilbert functions: $H_V(d) \leq \sum_{i=1}^{q} H_{V_i}(d)$ and equality holds, for one d, if and only if V_i and V_j are disjoint for any i, j. $\square$

Then, by Theorem 3.1, if in algorithm I the input of the polynomials is given authomatically by choosing random coefficients we have a generic variety, and by stopping the algorithm at $\min\{d \geq m \mid H_V(d) = \sum_{i=1}^{q} \binom{dr_i+m_i}{m_i}\} + 1$ we obtain a minimal set of generators of $I(V)$.

The previous results give easily the following algorithm.

ALGORITHM II

Input: $n, m_1, ..., m_q$, $m = \max\{m_1, \ldots, m_q\}$, $(2m_i < n$, for any i) and the degrees $r_1, ..., r_q$ and coefficients (randomly generated by the computer) of the polynomials that represent the parametric varieties $V_1, ..., V_q$.

Output: Elements of a minimal set of homogeneous generators of the ideal $I(V)$ and Hilbert function of V.

1. Set $t = 1$.
2. Computation, relatively to degree t, of the set T of points of Lemma 2.1 (using Corollary 2.1).
3. Application to the computed points of V of the algorithm of (Cioffi, 1999), in which the elements of degree $= t$ of a minimal basis of $I(T)$ (and then of $I(V)$) are constructed.
4. $t = t + 1$
5. If $t = \min\{d \geq m \mid H_V(d) = \sum_{i=1}^{q} \binom{dr_i + m_i}{m_i}\} + 2$ stop else goto **2**

4. An implementation:tests and results

The described algorithms I and II to implicitize union of rational parametric vareties have been implemented in C++ using the software Points99 (Orecchia *et al.*, 1999) which has been constructed for algorithms related to the computation of the generators of the ideal of a finite set of points.

In order to test the software, we ran it on randomly generated varieties V for increasing dimension n of the projective spaces and degree d of the polynomials that parametrically represent V, on $k = \mathbf{Z}_p$, $p = 31991$. The tests have been performed on a Intel Pentium 200 MHz with 40 MB RAM (for curves) and on a Intel Pentium-III 500 MHz with 128 MB RAM (for others varieties) both running Linux (kernel 2.0.31),.

We have compared our results, relatively to Algorithm II, with the performance of the HilbertDriven algorithm to eliminate variables and to minimalize a set of generators implemented in CoCoA3.7 and Singular1.2.2 (same examples and same computer were considered for Points, CoCoA and Singular) getting a significant saving of time.

In tables 1,2,3,4 we have reported four type of examples: a generic curve, unions of generic curves, a generic surface, unions of generic surfaces. We didn't report the timings of Singular because in general they are much higher (for example, for a general 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 $\mathbb{P}^5$). The sign —- means that CoCoA didn't finish the computation. This happened also for curves of large degree e.g. a generic curve of degree 80 in $\mathbb{P}^{10}$. (Points takes 133 seconds).

We did'n make tables for varieties of higher dimensions because the computational times of CoCoA and Singular are very high and in most of the cases they are not able to finish the computation. We quote only that for one general threefold of degree 27 in $\mathbb{P}^9$ Points99 takes 74 sec while Cocoa3.7 takes 5807 sec. and for one general threefold of degree 27 in $\mathbb{P}^{11}$ Points99 takes 13 sec. while Cocoa3.7 takes 2688sec.

The implementation we have described can be used to formulate conjectures about the natural number of minimal generators of the ideal of a general union of varieties as we will show in the next section.

5. An application: natural number of generators of the ideal of a general union of parametric varieties

Definition 5.1. *Let $V \subset \mathbb{P}^n$ be a smooth variety and $\rho(d) : H^0(\mathcal{O}_{\mathbb{P}^n}(d)) \to H^0(\mathcal{O}_V(d))$ be the natural restriction map. We say that V has maximal rank if, for every integer $d \geq 0$, $\rho(d)$ has maximal rank as a map of vector spaces i.e. it is injective or surjective.*

Theorem 5.1. *Let $V = \bigcup_{i=1}^{q} V_i \subset \mathbb{P}^n$ be the union of parametric varieties V_i*

Table 1. generic smooth curves

d	n	Points	CoCoA3.6	d	n	Points	CoCoA3.7
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

Table 2. unions of generic smooth curves

n	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 $deg = 8$	97.82	3243.83

parametrized by maps $\Phi_i : I\!P^{m_i} \to I\!P^n$, $m_i < n$ for any i, given by homogeneous polynomials of the same degree r_i. Let $\alpha = \min\{\binom{d+n}{n} > \sum_{i=1}^{q}\binom{r_i d+m_i}{m_i}\}$ The following conditions are equivalent:

(a) the varieties V_i are disjoint, smooth of dimension m_i, degree $r_i^{m_i}$ and V has maximal rank;

(b) $H_V(d) = \min\{\binom{d+n}{n}, \sum_{i=1}^{q}\binom{r_i d+m_i}{m_i}\}$.

Furthermore if $\alpha \geq m = \max\{m_1, \ldots, m_q\}$ the previous conditions are equivalent to:

(c) $H_V(\alpha-1) = \binom{\alpha+n-1}{n}$ and $H_V(\alpha) = \sum_{i=1}^{q}\binom{r_i\alpha+m_i}{m_i}$;

(d) the varieties V_i are disjoint, smooth of dimension m_i, degree $r_i^{m_i}$ and $reg(V) \leq \alpha+1$ (in particular the ideal $I(V)$ of V is generated by forms of degree α and $\alpha+1$).

Proof. First note that over a field of characteristic zero if the varieties V_i are smooth of dimension m_i and degree $r_i^{m_i}$ then their parametrization is given by polynomials without base points (to see this one can easily adapt the proof given in Example 18.13 of (Harris, 1995) for Veronese varieties to our case). Then in (a) and (d) one can omit

Table 3. generic smooth surfaces

d	n	Points	CoCoA3.7	d	n	Points	CoCoA3.7
5	5	133.04	171.03	6	5	824.05	980.09
	6	23.54	358.39		6	172.22	256.11
	7	8.18	213.05		7	33.27	113.10
	8	3.62	162.51		8	23.77	103.29
	9	2.06	141.57		9	10.49	904.81
	10	2.37	175,71		10	9.10	811.03
	11	1.01	191.5		11	7.15	875.93
	13	1.29	208.66		13	3.15	1178.51
	15	1.03	242.27		15	5.48	1511.90
7	5	19311.66	—	8	5	114524.03	—
	6	2126.65	—		6	2355.18	—
	7	196.82	413.87		7	962.11	—
	8	81.99	261.94		8	390.38	—
	9	32.04	198.75		9	182.03	3321.04
	10	27.71	188.33		10	131.98	3213.17
	11	28.55	197.66		11	65.99	3524.01
	13	17.39	232.83		13	55.40	3951.80
	15	14.35	291.57		15	61.25	4616.95

Table 4. unions of generic smooth surfaces

n	example	Points	CoCoA3.7
5	1 surface with $d = 1$ + 3 surfaces with $d = 2$	0.04	0.54
5	2 surface with $d = 3$	25.58	66.33
5	3 surface with $d = 3$	313.03	598.11
5	4 surface with $d = 3$	506.33	—
8	5 surface with $d = 2$	3.43	7.51
8	6 surface with $d = 2$	12.73	303.11
10	3 surface with $d = 3$	4.44	106.83
10	2 surface with $d = 5$	34.56	—
20	3 surface with $d = 5$	51.13	—

this last statement. $(a) \Leftrightarrow (b)$ Since $h^0(\mathcal{O}_{\mathbb{P}^n}(d)) = \binom{d+n}{n}$ and $h^0(\mathcal{O}_V(d)) = P_V(d)$ the statement follows easily from Theorem 3.1.

$(b) \Rightarrow (c)$ Clear by the definition of α.

$(c) \Rightarrow (b)$ On has $H_V(d) = \binom{d+n}{n} - dim_k I(V)_d$, then $H_V(d) = \binom{d+n}{n}$ is equivalent to $I(V)_d = 0$ and then $H_V(\alpha - 1) = \binom{\alpha+n-1}{n}$ implies $H_V(d) = \binom{d+n}{n}$, for $d < \alpha$. Furthermore by Theorem 3.1 $H_V(\alpha) = \sum_{i=1}^{q} \binom{r_i\alpha+m_i}{m_i}$ implies that V is $\alpha + 1$ regular and then $H_V(d) = \binom{dr+m}{m}$ for any $d \geq \alpha$.

$(c) \Rightarrow (d)$ Since $H_V(\alpha) = \sum_{i=1}^{q} \binom{r_i\alpha+m_i}{m_i}$, by Theorem 3.1,the varieties V_i are disjoint, smooth of dimension m_i, degree $r_i^{m_i}$ and $reg(V) \leq \alpha + 1$. Hence, by Proposition 3.1, V is generated in degree $\alpha + 1$.

$(d) \Rightarrow (c)$ If the varieties V_i are disjoint, smooth of dimension m_i, degree $r_i^{m_i}$ then by

Theorem 3.1 $P_V(d) = \sum_{i=1}^{q} \binom{dr_i+m_i}{m_i}\}$. Furthermore if V is $\alpha+1$ regular the restriction map $H^0(\mathcal{O}_{I\!P^n}(\alpha-1)) \to H^0(\mathcal{O}_V(\alpha-1))$ surjects. It follows that $H_V(\alpha) = P_V(\alpha) = \sum_{i=1}^{q} \binom{r_i\alpha+m_i}{m_i}\}$ and since V has no generator of degree $< \alpha$, we have $H_V(\alpha-1) = \binom{\alpha+n-1}{n}$ $\square$

Remark 5.1. The assumption $\alpha \geq m = \max\{m_1, \ldots, m_q\}$ of Theorem 5.1 is necessary. For example if $V \subset I\!P_k^n$ is a Veronese variety with $r \geq m > 3$, it is well known that V has maximal rank since $H_V(d) = \binom{dr+m}{m}$, for any $d \geq 0$, and $reg(V) = m$ but $\alpha = 2$. In the case of curves and non-degenerate surfaces the assumption is clearly always fullfilled. if V has maximal rank it is easily seen that also in the case $r_i \geq \frac{m_i}{n_i}$, for at least one i, we have $\alpha \geq m = \max\{m_1, \ldots, m_q\}$

Let $V = \bigcup_{i=1}^{q} V_i \subset I\!P^n$ be the union of q parametric smooth disjoint varieties V_i parametrized by maps $\Phi_i : I\!P^{m_i} \to I\!P^n$, $m_i < n$ for any i, given by homogeneous polynomials of the same degree r_i and denote with $\nu(V)$ the minimal number of generators of the ideal $I(V)$ of V.

Assume that V has maximal rank and let

$$\alpha = Min\{d \in I\!N \mid \binom{d+n}{n} > \sum_{i=1}^{q} \binom{r_i d + m_i}{m_i}\} \geq m = \max\{m_1, \ldots, m_q\}$$

.

By Theorem 5.1 the ideal $I(V) = \bigoplus_{n\geq 0} I(V)_n$ of V can be generated by forms of degree α and $\alpha+1$. If we set

$$W_{\alpha+1} = X_0 I(V)_\alpha + \ldots + X_r I(V)_\alpha \subset I(V)_{\alpha+1}$$

we have

$$\nu(V) = dim_k I(V)_\alpha + dim_k I(V)_{\alpha+1} - dim_k W_{\alpha+1}$$

Furthermore:

$$dim_k W_{\alpha+1} \leq Min\{(r+1) dim_k I(V)_\alpha, dim_k I(V)_{\alpha+1}\} \tag{5.1}$$

Hence:

$$\nu(I(V))) \geq dim_k I(V)_\alpha + dim_k I(V)_{\alpha+1} - Min\{(r+1) dim_k I(V)_\alpha, dim_k I(V)_{\alpha+1}\}$$

DEFINITION 5.2. *V is said to be naturally generated when it has maximal rank and the natural map:*

$$\sigma(\alpha) : H^0(I_V(\alpha)) \otimes H^0(\mathcal{O}_{I\!P^r}(1)) \to H^0(I_V(\alpha+1))$$

is of maximal rank i.e.

$$dim_k W_{\alpha+1} = Min\{(r+1) dim_k I(V)_\alpha, dim_k I(V)_{\alpha+1}\}$$

This means that V has the least possible number of minimal generators:

$$\nu(V) = dim_k I(V)_\alpha + dim_k I(V)_{\alpha+1} - Min\{(r+1) dim_k I(V)_\alpha, dim_k I(V)_{\alpha+1}\}$$

THEOREM 5.2. *Let $V = \bigcup_{i=1}^{q} V_i \subset I\!P^n$ be the non-degenerate union of q parametric smooth disjoint varieties V_i parametrized by maps $\Phi_i : I\!P^{m_i} \to I\!P^n$, $m_i < n$ for any*

i, given by homogeneous polynomials of the same degree r_i. Suppose that $\alpha = Min\{d \in I\!N \mid \binom{d+r}{r} > \sum_{i=1}^{q}\binom{r_i d+m_i}{m_i}\} \geq m = \sum_{i=1}^{q} m_i$. Consider the set T of $\sum_{i=1}^{q}\binom{r_i(\alpha+1)+m_i}{m_i}$ points of V determined as in Lemma 2.1. Then:

$rk(G_{\alpha-1}(T)) \leq \binom{\alpha+n-1}{n}$ *and* $rk(G_\alpha(T)) \leq \sum_{i=1}^{q}\binom{r_i\alpha+m_i}{m_i}$.

Furthermore the varieties V_i are smooth and disjoint and V has maximal rank if and only if

$rk(G_{\alpha-1}(T)) = \binom{\alpha+n-1}{n}$ *and* $rk(G_\alpha(T)) = \sum_{i=1}^{q}\binom{r_i\alpha+m_i}{m_i}$.

Moreover, if V has maximal rank, we have

$rk(M_{\alpha+1}(T)) \leq Min\{(n+1)(\binom{\alpha+n}{n} - \sum_{i=1}^{q}\binom{r_i\alpha+m_i}{m_i}), \binom{\alpha+n+1}{n} - \sum_{i=1}^{q}\binom{r_i(\alpha+1)+m_i}{m_i}\}$

and V is naturally generated if and only if

$rk(M_{\alpha+1}(T)) = Min\{(n+1)(\binom{\alpha+n}{n} - \sum_{i=1}^{q}\binom{r_i\alpha+m_i}{m_i}), \binom{\alpha+n+1}{n} - \sum_{i=1}^{q}\binom{r_i(\alpha+1)+m_i}{m_i}\}$

Proof. The claims follow easily from Lemma 2.1, (2.4), (2.6), Theorem 3.1 and Theorem 5.1. □

THEOREM 5.3. *Let $V = \bigcup_{i=1}^{q} V_i \subset I\!P^n$ be the union of parametric varieties V_i parametrized by maps $\Phi_i : I\!P^{m_i} \to I\!P^n$, $m_i < n$ for any i, $\Phi_i([t_{i0} : ... : t_{im_i}]) = [f_{i0}([t_{i0} : ... : t_{im_i}]) : ... : f_{in}([t_{i0} : ... : t_{im_i}])]$, where $f_{ij} = a_{ij_1}\mathcal{T}_1 + ... + a_{ij_u}\mathcal{T}_u$, $u = \binom{m_i+r_i}{m_i}$, are homogeneous polynomials of the same degree r_i. Let $(a_1, ..., a_s) = (a_h^{(ij)})$ denote the s-tuple ($s = \sum_{i=1}^{q}(n+1)\binom{m_i+r_i}{m_i}$) of the coefficients of the polynomials that parametrize V_i. Suppose that $\alpha = Min\{d \in I\!N \mid \binom{d+r}{r} > \sum_{i=1}^{q}\binom{r_i d+m_i}{m_i}\} \geq m = \sum_{i=1}^{q} m_i$ Then:*

(a) the set of the s-tuples $(a_1, ..., a_s) \in \mathbf{A}^s$ for which V has maximal rank is open;

(b) the set of the s-tuples $(a_1, ..., a_s) \in \mathbf{A}^s$ for which V is naturally generated is open.

Proof. For any $i = 1, ..., q$ consider a fixed set T_i of $\binom{r_i(\alpha+1)+m_i}{m_i}$ points on V_i determined by giving integer values to the parameters of the polynomials that represent V_i (see Lemma 2.1 and Corollary 2.1). Let $T = \cup_{i=1}^{s} T_i$. The matrices $G_{\alpha-1}(T)$, $G_\alpha(t)$ have entries which are terms in the coordinates of the points of T (see (2.2)). The entries of the matrix $M_{\alpha+1}(T)$ are zeroes or are the coefficients of the polynomials $g_i X_j$, that is of the polynomials $g_1, ..., g_e$ which form a basis of the null space $N_\alpha(T)$ of $G_\alpha(T)$ (see (2.5)). Then the matrices $G_{\alpha-1}(T)$, $G_\alpha(T)$ and $M_{\alpha+1}(T)$ have entries which are forms of the polynomial ring $\mathbf{Z}[a_1, ..., a_q]$ therefore also their minors are forms in $\mathbf{Z}[a_1, ..., a_q]$. Moreover by Theorem 5.2 we have

$$rk(G_{\alpha-1}(T)) \leq c = \binom{\alpha+n-1}{n} \quad rk(G_\alpha(T)) \leq c' = \sum_{i=1}^{q}\binom{r_i\alpha+m_i}{m_i}$$

and if V has maximal rank $rk(M_{\alpha+1}(T)) \leq c$" where

$$c" = Min\{(n+1)(\binom{\alpha+n}{n} - \sum_{i=1}^{q}\binom{r_i\alpha+m_i}{m_i}), \binom{\alpha+n+1}{n} - \sum_{i=1}^{q}\binom{r_i(\alpha+1)+m_i}{m_i}\}$$

. Let $M_1, ..., M_u$ be the minors of $G_{\alpha-1}(T)$ of order c, $M'_1, ..., M'_v$ be the minors of

$G_\alpha(T)$ of order c' and $M"_1, ..., M"_w$ be the minors of $M_{\alpha+1}(T)$ of order $c"$. Consider the following closed sets of $\mathbf{A}^q$, $D : M_1 = 0, ..., M_u = 0$, $D' : M'_1 = 0, ..., M'_v = 0$, $D" : M"_1 = 0, ..., M"_w = 0$ and let $U = \mathbf{A}^q_k - (D \cap D')$ and $U' = \mathbf{A}^q_k - (D \cap D' \cap D")$. If $(a_1, ..., a_q) \in U$ then the matrices $G_{\alpha-1}(T)$ and $G_\alpha(T)$ have respectively rank c and c'. Hence V has maximal rank by Theorem 5.2. If $(a_1, ..., a_q) \in U'$ then the matrix $M_{\alpha+1}(T)$ has rank $c"$. It follows that V has maximal rank and is minimally generated again by Theorem 5.2.□

Remark 5.2. For some fixed $n, q, m_1, ..., m_q, r_1, ..., r_q$ the open sets U and U' of Theorem 5.3 could be empty. For example the union C in $I\!P^3$ of two conics $C_1 \cup C_2$ is contained in a reducible quadric (the union of the two planes containing the conics) and C has not maximal rank. The union of 4 generic lines in $I\!P^3$ has maximal rank but it is non naturally generated (Ida', 1990).

Next we want to show how the computer can be used to find parametric smooth varieties V of maximal rank and naturally generated.

Let $\mathbf{Z}_p$ be the residue field of the integers modulo a prime p. If $f = b_1\mathcal{T}_1 + ... + b_u\mathcal{T}_u$ is a polynomial of $\mathbf{Z}[t_0, \ldots, t_m]$ (where $\mathcal{T}_i$ are the terms in $t_0, \ldots, t_m$) we denote with $\overline{f} = \overline{b}_1\mathcal{T}_1 + ... + \overline{b}_u\mathcal{T}_u$ the corresponding polynomial of $\mathbf{Z}_p[t_0, \ldots, t_m]$ (where the coefficient $\overline{b}_i \in \mathbf{Z}_p$ is the class of the coefficient $b_i \in \mathbf{Z}$ of f).

PROPOSITION 5.1. *Let $V = \bigcup_{i=1}^q V_i \subset I\!P^n$ be the union of parametric varieties V_i parametrized by maps $\Phi_i : I\!P^{m_i} \to I\!P^n$, $m_i < n$ for any i, $\Phi_i([t_{i0} : ... : t_{im_i}]) = [f_{i0}([t_{i0} : ... : t_{im_i}]) : ... : f_{in}([t_{i0} : ... : t_{im_i}])]$, where f_{ij} are homogeneous polynomials of degree r_i. Suppose that $\alpha = Min\{d \in I\!N \mid \binom{d+r}{r} > \sum_{i=1}^q \binom{r_i d+m_i}{m_i}\} \geq m = \sum_{i=1}^q m_i$. Denoted by $\mathbf{Z}_p^*$ the algebraic closure of $\mathbf{Z_p}$ and by $\overline{V} = \bigcup_{i=1}^q \overline{V}_i \subset I\!P^n_{\mathbf{Z}_p^*}$ the variety whose irreducible components $\overline{V}_i$ are given by the homogeneous polynomials $\overline{f}_{ij}$, then:*

(a) if $\overline{V}$ has maximal rank also V has maximal rank;

(b) if $\overline{V}$ is naturally generated also V is naturally generated.

Proof. First we recall the following straigthforward fact: if $Q = (a_{ij})$ is a $c \times d$ matrix with entries $a_{ij} \in \mathbf{Z}$ and $\overline{Q} = \overline{a}_{ij}$ is the $c \times d$ matrix whose entries are the integers a_{ij} modulo a prime p then $rk(\overline{Q}) \leq rk(Q)$ (rk=rank). Hence if $rk(\overline{Q})$ is maximal, that is $rk(\overline{Q}) = \min\{c, d\}$, also $rk(Q) = \min\{c, d\}$. Now, by Theorem 5.2, the conditions of $(a), (b)$ are conditions on the maximality of ranks of matrices whose elements are polynomials in the coefficients of the polynomials f_{ij}. □

THEOREM 5.4. *Fix integers $m_1, ..., m_q, r_1, ..., r_q, n$ such that $\alpha = Min\{d \in I\!N \mid \binom{d+n}{n} > \sum_{i=1}^q \binom{r_i d+m_i}{m_i}\} \geq m = \max\{m_1, \ldots, m_q\}$. In the same hypotheses of Proposition 5.1 if, for a prime p, there exists a $\overline{V} = \bigcup_{i=1}^q \overline{V}_i \subset I\!P^n_{\mathbf{Z}_p^*}$ which has maximal rank or (respectively) is naturally generated then, for any field k of characteristic zero, a general union of parametric varieties $V = \bigcup_{i=1}^q V_i \subset I\!P^n$ has maximal rank or (respectively) is naturally generated.*

Proof. By Theorem 5.3 if V has maximal rank or is naturally generated the s-tuples of the coefficients of the polynomials that represent the varieties V_i belong to open sets. By Proposition 5.1 these sets are non-empty.□

Theorem 5.4 and Algorithm II applied to parametric varieties defined over $\mathbf{Z}_p$ allow us to find naturally generated varieties.

6. The ideal generation conjecture for a general union of parametric curves and surfaces

In this section we assume that the base field k has characteristic zero.

Let $V = \bigcup_{i=1}^{q} V_i \subset I\!P^n$ be the union of smooth disjoint parametric varieties V_i parametrized by maps $\Phi_i : I\!P^{m_i} \to I\!P^n$, $2m < n$ for any i, given by homogeneous polynomials of same degree r_i. Assume that

$$\alpha = Min\{d \in I\!N \mid \binom{d+n}{n} > \sum_{i=1}^{q} \binom{r_i d + m_i}{m_i}\} \geq m = \max\{m_1, \ldots, m_q\}$$

.

Consider the following general questions:

(a) *For which values of $m, n, q, r_1, ..., r_q$ is it true that, for general $V_1, ..., V_s$, V has maximal rank?*

(b) *For which values of $m, n, q, r_1, ..., r_q$ is it true that, for general $V_1, ..., V_s$, V is naturally generated?*

Very few answers to these questions are known and only concern curves, a context where parametric and rational are synonimous.

The answer to the question (a) where all V_i are curves is the following.

Theorem 6.1. *Let $C = \bigcup_{i=1}^{q} C_i \subset I\!P^n$, $n \geq 3$, be the union of q rational irreducible smooth disjoint curves. Then, for general $C_1, ..., C_q$, C has maximal rank, for any $n, q, r_1, ..., r_q$, except for the following q-tuples $(r_1, ..., r_q)$ of $I\!P^3$:*

$(2,2)$; $(2,4)$; $(2,2,2)$; $(2,2,4)$; $(2,2,2,2)$.

Proof. (Ballico, 1986) and (Ballico and Ellia , 1985)□

An answer to question (b) has been given where the V_i were lines and more recently irreducible curves in $I\!P^3$:

Theorem 6.2. *Let C be the union of q general lines in $I\!P^3$. Then C is naturally generated if and only if $q \neq 4$.*

Proof. (Ida', 1990)□

Theorem 6.3. *A general irreducible rational curve C of $I\!P^3$ of degree $d \leq 73$ is naturally generated if and only if $d \neq 5$.*

Proof. (Ida', 1999) □

By using the computer and the results of this paper we get new results concerning maximal rank and natural generation for curves and surfaces. Clearly, by Proposition 5.1, we get an answer to the questions above for specific values of $m, n, q, r_1, ..., r_q$, once we find an example of variety $\overline{V} \subset I\!P^n_{\mathbf{Z}_p^*}$ with coefficients in $\mathbf{Z}_p$ which has maximal rank or is naturally generated. Then by running Algorithm II on the computer we proved in

(Orecchia, 1998) for irreducible curves fo degree≤ 80 in any $\mathbb{P}^n$ and for reducible curves of degree≤ 40 in $\mathbb{P}^n$, $n \leq 10$, the following

Ideal Generation Conjecture for Rational Curves

For every positive integers $n, r_1, ..., r_q$, $n \geq 3$, the non-degenerate union $C = \bigcup_{i=1}^q C_i \subset \mathbb{P}^n$ of general parametric curves C_i of degree r_i is naturally generated except for the following q-tuples $(r_1, ..., r_q)$.

If $n = 3$: $(5); (1,2); (2,2); (2,3); (2,4); (2,5); (3,4); (1,1,2); (1,2,2); (1,2,4); (2,2,2); (2,2,3); (2,2,4); (1,1,1,1); (1,2,2,2); (2,2,2,2); (1,2,2,2,2)$.

If $n = 4$: $(5); (1,3); (2,3); (1,1,2)$.

If $n = 5$: $(3,4); (1,2,3); (2,2,2)$.

A more powerful personal computer gave us the opportunity to improve a result in (Orecchia, 1998):

THEOREM 6.4. *The ideal generation conjecture for rational curves is true for irreducible curves fo degree≤ 120 in any $\mathbb{P}^n$ and for reducible curves of degree≤ 60 in $\mathbb{P}^n$, $n \leq 20$.*

.

In the case of the non-degenerate union $S = \bigcup_{i=1}^q S_i \subset \mathbb{P}^n$, $n \geq 5$ of parametric surfaces as a consequence of computations performed on the computer using Algorithm II we formulate the following:

Ideal Generation Conjecture for General Parametric Surfaces

For every positive integers $n, r_1, ..., r_q$, $n \geq 5$, the non-degenerate union $V = \bigcup_{i=1}^q V_i \subset \mathbb{P}^n$ of general parametric surfaces V_i of degree r_i^2 is naturally generated except for the following q-tuples $(r_1, ..., r_q)$.

If $n = 5$: $(1,1,1); (1,1,2); (1,1,1,1)$.

If $n = 6$: $(1,2); (2,2); (1,1,1); (2,2,2)$.

If $n = 7$: $(3); (2,2); (1,1,1); (2,1,1); (1,1,1,1)$.

If $n = 8$: $(1,3); (1,2,2); (2,1,1,1)$.

If $n = 10$: $(3,2,1)$.

We have in fact proved the following:

THEOREM 6.5. *The ideal generation conjecture for parametric surfaces is true for irreducible surfaces of degree≤ 64 in any $\mathbb{P}^n$ and for irreducible surfaces of degree≤ 40 in $\mathbb{P}^n$, $n \leq 20$.*

Note

Some of the results of this paper have been presented by the author at EACA-99 (Tenerife, 8-11 September, 1999)

References

Albano, G., Cioffi, F., Orecchia, F., Ramella, I. (1999). Minimally generating ideals of rational parametric curves in polynomial time. *To appear in J. Symbolic Computation* .

Ballico, E. (1986). On the postulation of disjoint rational curves in a projective space*Rend. Sem. Mat. Univer. Politecn. Torino* **44**, 46–52.

Ballico, E., Ellia P., (1986). On the Postulation of Many Disjoint Rational Curves in $I\!P^n$, $n \geq 4$ *Bollettino U.M.I.* (6) **4**-B, 585-599

Bayer, D., Mumford, D. (1993). What cab be computed in Algebraic Geometry?. *Symposia Mathematica*, **34**,1–48.

Capani, A., Niesi, G., Robbiano, L. (1999). CoCoA3.7, a system for doing Computations in Commutative Algebra. *Available via anonymous ftp from cocoa.dima.unige.it* .

Chionh, Goldman (1992). Degree, multiplicity and inversion formulae for rational surfaces using u-resultants. *Comp. Aided Geom. Des.*, **9**, 93–108.

Cioffi, F. (1999). Minimally generating ideals of points in polynomial time using linear algebra. *Ricerche di Matematica*, **48**, 55–63.

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). Impli citization of Rational Parametric Equations. J. Symbolic Computation, **14**, 459–470.

Harris, J. (1995). Algebraic Geometry. *Graduate Texts in Mathematics* **133**, Springer Verlag

Geramita, A.V., Orecchia, F. (1981). On the Cohen-Macaulay type of s-lines in $\mathbf{A}^{\mathbf{n+1}}$. *J. of Algebra*, **70**, 89-133.

Geramita, A.V., Orecchia, F. (1982). Minimally Generating Ideal Defining Certain Tangent Cones *J. of Algebra* **78** 36-57

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

Ida', M. (1990). On the homogeneous ideal of the generic union of s-lines in $I\!P^3$ *J. Reine Angew. Math.*, **403**, 67–153.

Ida', M. (1999). Generators for the generic rational space curve: low degree case,*Lecture Notes in Pure and Appl. Math. Commutative algebra and algebraic geometry (Ferrara)*, **206**, Dekker, New York, 169–210

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

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.

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**, 103–145.

Mumford, D. (1966). Lectures on curves on an algebraic surface. *Ann. of Math. Studies*, **59**.

Orecchia, F. (1981). Points in generic position and conductors of curves with ordinary singularities. *J. London Math. Soc.*, **24**, 85–96.

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,G1–G8.

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

Orecchia, F., Albano, G., Cioffi, F., Ramella, I. (1999). *Points*99. *Available at http : //cds.unina.it/˜orecchia/gruppo/EPoints.html*.

Ramella, I. (1994). Ideals of points in generic position: a polynomial algorithm for computing a minimal set of generators.*Ricerche di Matematica*, **43**, 205–217.

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", U niv. di Napoli "Federico II".

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