# Implicitization of parametric hypersurfaces via points 

Ferruccio Orecchia, Isabella Ramella<br>Dipartimento di Matematica e Appl., Università di Napoli "Federico II", Via Cintia, 80126 Napoli, Italy<br>orecchia@unina.it ramella@unina.it


#### Abstract

Given a parametric polynomial representation of an algebraic hypersurface $\mathbf{S}$ in the projective space we give a new algorithm for finding the implicit cartesian equation of $\mathbf{S}$. The algorithm is based on finding a suitable finite number of points on $\mathbf{S}$ and computing, by linear algebra, the equation of the hypersurface of least degree that passes through the points. In particular the algorithm works for plane curves and surfaces in the ordinary three-dimensional space. Using C++ the algorithm has been implemented on an intel Pentium running Linux. Since our algorithm is based only on computations of linear algebra it reveals very efficient if compared with others that do not use linear algebra for the computations.


A.M.S. Subject Classification : 14Q10

Key Words: implicitization, hypersurfaces

## Introduction

The hypersurface implicitization problem has attracted many authors, also recently and in the case of ordinary curves and surfaces has applications to Computer aided Geometric Design and Geometric Modelling. The problem consists in determining an implicit representation of an irreducible parametric algebraic hypersurface in the projective space $\mathbb{P}^{n}$ (in particular a plane curve or a surface). It has been classically faced by elimination theory and can be solved by the computation of Gröbner bases or by the computation of resultants. New methods have been recently introduced in [1]. All these methods have been implemented in various softwares of Computer Algebra (see [1]). For doing these computations on the computer the hysurface has to be parametrically represented by polynomials with coefficients rational numbers (or
more simply integers) and the result is an equation whose coefficients are rational numbers (or integers). Another possible representation of the coefficients of the parametric polynomials is in the set of integers modulo a prime number. In this paper, we introduce a new alternative method that reconducts the implicitation of $\mathbf{S}$ to the computation of the equation of the hypersurface that contains a suitable set of points on $\mathbf{S}$. The algorithm works both on rational (or integers) numbers and on integers modulo a prime number. The algorithm is based on the fact that, if we find an appropriate set $T$ of general points on $\mathbf{S}$, a polynomial $F$ vanishes on the polynomials that represent parametrically $\mathbf{S}$ if and only if $F$ vanishes on $T$. This gives rise to a homogeneous linear system of equations. A non null solution of the system (which can be found very easily by Gauss reduction) gives the coefficients of the implicit equation of $\mathbf{S}$. The algorithm of this paper applies to plane curves and surfaces in the ordinary space. The notations and results tacitly assumed in this article can be found in [3] and in [6].

## 1 Computing the implicit equation of a parametric hypersurface by points

Let $\mathbb{P}^{n}$ be the $n$-dimensional projective space over a field $k$.
Definition 1.1 We say that an irreducible (algebraic) hypersurface $\mathbf{S} \subset \mathbb{P}^{n}$ is parametric if there exists a rational map $\Phi: \mathbb{P}^{m} \rightarrow \mathbb{P}^{n}$,

$$
\Phi\left(t_{0}, t_{1}, \ldots, t_{m}\right)=\left(f_{0}\left(t_{0}, t_{1}, \ldots, t_{m}\right), \ldots, f_{n}\left(t_{0}, t_{1}, \ldots, t_{m}\right)\right)
$$

given by homogeneous polynomials $f_{i}\left(t_{0}, t_{1}, \ldots, t_{m}\right), i=0,1,2, \ldots, n$ of the same degree $r$ whose image is a dense subset of $\mathbf{S}$. We set

$$
\mathbf{S}=\left\{\left(x_{0}, x_{1}, \ldots, x_{n}\right) \in \mathbb{P}^{n} \mid x_{i}=f_{i}\left(t_{0}, t_{1}, \ldots, t_{m}\right), i=0,1,2, \ldots, n\right\}
$$

Since $\mathbf{S}$ is a hypersurface of $\mathbb{P}^{n}$ it is also the set of solutions of a homogeneous polynomial $F \in k\left[X_{0}, \ldots, X_{n}\right]$ in $n+1$ variables. We consider the polynomial $F$ of least degree $d$ that vanishes on $\mathbf{S}$. The corresponding equation $F=0$ is said to implicitize the parametric hypersurface $\mathbf{S}$ and $F$ is said to be the polynomial defining $\mathbf{S}(F$ is unique modulo constant terms of $k)$.

Definition $1.2[9] A$ set $S=\left\{P_{1}, \ldots, P_{N}\right\} \subset \mathbb{P}^{m}$ of $N=\binom{d+m}{m}$ points is in generic position (or simply the points are in generic position) if it is not contained in a projective hypersurface of degree $\leq d$.

Example 1.3 Six points that do not lie on a conic and ten points that do not lie on a quadric surface are in generic position.

Lemma 1.4 Let $\mathbf{S}=\left\{\left(x_{0}, \ldots, x_{n}\right) \in \mathbb{P}^{n} \mid x_{i}=f_{i}\left(t_{0}, \ldots, t_{m}\right), i=0, \ldots, n\right\}$ be a parametric hypersurface given by homogeneous polynomials of the same degree $r$. Let $d$ be a fixed integer, and $P_{1}, \ldots, P_{N}$ be $N=\binom{r d+m}{m}$ points of $\mathbb{P}^{m}$ in generic position such that $Q_{i}=\Phi\left(P_{i}\right)$ form a set $T$ of $N$ points of $\mathbb{P}^{n}$. If $F^{\prime}$ is a homogeneous polynomial of $K\left[X_{0}, \ldots, X_{n}\right]$ with degree $d^{\prime} \leq d$ then $F^{\prime}$ vanishes on $\mathbf{S}$ if and only if $F^{\prime}$ vanishes on $T$.

Proof. Clearly, since $T \subset \mathbf{S}$, a a polynomial vanishing on $\mathbf{S}$ vanishes on $T$. We prove the converse by contradiction. Let $F^{\prime}$ be a homogeneous polynomial of degree $d^{\prime}$ vanishing on the set of points $T$ and assume that there exists a point $P \in \mathbb{P}^{m}$ such that $F(\Phi(P)) \neq 0$. Then $F^{\prime}\left(f_{0}, \ldots, f_{n}\right)$ is a non-zero polynomial of degree $d^{\prime} r \leq d r$ vanishing on the $N=\binom{r d+m}{m}$ points $P_{i}$ and this contradicts the assumption of generic position.
By Lemma 1.5 the computation of the equation that defines $\mathbf{S}$ is reconducted to the computation of the equation that vanishes on 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 $S=\left\{P_{1}, \ldots, P_{N}\right\} \subset \mathbb{P}^{m}$ are in generic position ([7]). It follows that a random choice for the coordinates of the $P_{i}$ 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 1.5 Let $d$ and $m$ be fixed positive integers and $a_{i j} \in k, i=0, \ldots, d$, $j=0, \ldots, m$, Suppose $a_{i j} \neq a_{i^{\prime} j}$, for any $i \neq i^{\prime}, j=1, \ldots, m$. No hypersurface of degree $\leq d$ contains the $N=\binom{d+m}{m}$ affine points of the set

$$
S=\left\{\left(a_{i_{1} 1}, \ldots a_{i_{m} m}\right) \in k^{m} \mid\left(i_{1}, \ldots, i_{m}\right) \in \mathbf{N}^{m}, i_{1}+\ldots+i_{m} \leq d\right\}
$$

Hence the set of $N$ projective points

$$
S^{\prime}=\left\{\left(a_{i_{1} 1}, \ldots, a_{i_{m} m}, 1\right) \in \mathbb{P}^{m} \mid i_{1}+\ldots+i_{m} \leq d\right\}
$$

is in generic position.
Proof. We prove the first part of the statement by induction. the second part then follows easily. When $m=1$ the set $S=\left\{\left(a_{i} \in k \mid i \leq d\right\}\right.$ 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 that the claim is true for $m-1$. It follows that, for any $d$ the set of the $N=\binom{d+m-1}{m-1}$ affine points $S_{0}=\left\{\left(a_{i_{1} 1}, \ldots, a_{i_{m-1} m-1}\right) \in k^{m-1} \mid\right.$ $\left.\left(i_{1}, \ldots, i_{m-1}\right) \in \mathbf{N}^{m-1}, i_{1}+\ldots+i_{m-1} \leq d\right\}$ is not contained in a hypersurface of degree $\leq d$. We want to prove that any non-null polynomial $F\left(X_{1}, \ldots, X_{m}\right)$ vanishing on all points in $S$ has degree greater than $d$. The polynomial $G_{0}\left(X_{1}, \ldots, X_{m-1}\right)=$
$F\left(X_{1}, \ldots, X_{m-1}, a_{0 m}\right)$ vanishes on $S_{0}$, hence is null by the inductive hypothesis, then $F\left(X_{1}, \ldots, X_{m}\right)=\left(X_{m}-a_{0 m}\right) F_{1}$ where the degree of $F_{1}$ is less or equal to $d-1$. Repeating the same argument for the polynomial $F\left(X_{1}, \ldots, X_{m-1}, a_{1 m}\right)$ and the set $S_{1}=\left\{\left(a_{i_{1}}, \ldots, a_{i_{m-1} m-1}\right) \in k^{m-1} \mid\left(i_{1}, \ldots, i_{m-1}\right) \in \mathbf{N}^{m-1}, i_{1}+\ldots+i_{m-1} \leq d-1\right\}$ and so on, we get $F\left(X_{1}, \ldots, X_{m}\right)=\prod_{q=0}^{d}\left(X_{m}-a_{q m}\right) F^{\prime}$ so that $F$ has a greater degree than $d$.

From Proposition 1.5 we get immediately that:
Corollary 1.6 . Let $d$ a positive integer and $\operatorname{char}(k)=0$ or $\operatorname{char}(k) \geq d$. The following set of $N=\binom{d+m}{m}$ projective points, where $i_{j} \in \mathbf{N}$ is identified with $i_{j} \cdot 1_{k}$, is in generic position

$$
\left.S^{\prime}=\left\{i_{1}, \ldots i_{m}, 1\right) \in \mathbb{P}^{m} \mid\left(i_{1}, \ldots, i_{m}\right) \in \mathbf{N}^{m}, i_{1}+\ldots+i_{m} \leq d\right\}
$$

Corollary 1.6 gives an algorithmic way to find a set of $N=\binom{d r+m}{m}$ distinct projective points $T=\left\{\Phi\left(P_{1}\right), \ldots \Phi\left(P_{N}\right)\right\}$ of a hypersurface $\mathbf{S}$ such that such that $\left\{P_{1}, \ldots P_{N}\right\}$ are in generic position.

## 2 The algorithm

By the results of section 1, the problem of determining the implicit equation of a parametric hypersurface $S$ is reconducted to the problem of finding a polynomial $F$ that vanishes on a suitable set of points on $S$. In this section we construct an algorithm for solving this problem using only linear algebra.

Let $T=\left\{Q_{1}, \ldots, Q_{s}\right\}$ be a set of points in $\mathbb{P}^{n}$ and $d$ a positive integer. An homogeneous polynomial $F\left(X_{1}, \ldots, X_{m}\right)$ of degree $d$ vanishes on $T$ if and only if, for any $i=1, \ldots, s, F\left(Q_{i}\right)=0$. This gives a homogeneous linear system with coefficients in $k$ and indeterminates $X_{1}, \ldots, X_{n}$. Denoting by $\mathcal{T}_{i}, i=1, \ldots, h$ the terms of degree $d$ in the indeterminates $X_{1}, \ldots, X_{m}$, ordered with respect to any term ordering, the set $B=\left\{\mathcal{T}_{i}, \ldots, \mathcal{T}_{h}\right\}$ is a basis of the $k$ vector space of the homogeneous polynomials $F\left(X_{1}, \ldots, X_{n}\right)$ of degree $d$. Consider the matrix

$$
M_{d}(T)=\left(\mathcal{T}_{i}\left(Q_{j}\right)\right)
$$

whose generic element $\left(\mathcal{T}_{i}\left(Q_{j}\right)\right)$ is the evaluation of the term $\mathcal{T}_{i}$ at the point $Q_{j}$.
If $F=a_{1} \mathcal{T}_{1}+\ldots+a_{h} \mathcal{T}_{h}$ we set $(F)_{B}=\left(a_{1}, \ldots, a_{h}\right)$ and denote with $(F)_{B}^{t}$ the transpose of $(F)_{B}$.

Hence $F\left(X_{1}, \ldots, X_{n}\right)$ vanishes on $T$ if and only if $(F)_{B}^{t}$ is a vector of the null space of the matrix $M_{d}(T)$ and then there is a homogeneous polynomial vanishing on $T$ if and only if the rank $r k\left(M_{d}(T)\right)$ of the matrix $M_{d}(T)$ is less then $\binom{d+n}{n}$.

All the previous results allow to formulate the following algorithm. Let $\mathbf{S}$ be a hypersurface:

$$
\mathbf{S}=\left\{\left(x_{0}, x_{1}, \ldots, x_{n}\right) \in \mathbb{P}^{n} \mid x_{i}=f_{i}\left(t_{0}, t_{1}, \ldots, t_{m}\right), i=0,1, \ldots, n\right\}
$$

## ALGORITHM

INPUT: degree $d$ and coefficients of the polynomials $f_{i}$
OUTPUT: Implicit equation $F=0$ of $\mathbf{S}$

1. Set $d=1$.
2. Computation, in degree $d$, of the set $T$ of points of Lemma 1.4
3. Computation of the matrix $M_{d}(T)$

4 If $r k\left(M_{d}(T)\right)<\binom{r d+m}{m}$ goto 5 else set $d=d+1$ and goto 2 .
5. Compute a solution $(F)_{\mathbf{S}}$ of the null space of $M_{d}(T)$ and stop. The vector $(F)_{\mathbf{s}}$ gives the coefficients of the implicit equation $F=0$ of $\mathbf{S}$.

Our algorithm was implemented in $\mathrm{C}++$ on an Intel Pentium running Linux.
We have tested the algorithm for the computation of the implicit equation of hypersurfaces on various examples. Our results coincide with the ones obtained by other authors which compute the implicit equation with other methods. Since our algorithm is based on computations of linear algebra it reveals very efficient if compared with others that do not use linear algebra for the computations. We only quote the following example which was considered in [5] and [8].

Example 2.1 Let $\mathbf{S}$ be the following parametric surface of $\mathbb{P}^{3}$, over a field of characteristic zero.

$$
S=\left\{\left(x_{0}, . ., x_{4}\right) \mid x_{0}=t_{1} t_{2}^{2}-t_{2} t_{3}^{2}, x_{1}=t_{1} t_{2} t_{3}+t_{1} t_{3}^{2}, x_{2}=2 t_{1} t_{3}^{2}-2 t_{2} t_{3}^{2}, x_{3}=t_{1} t_{2}^{2}\right\}
$$

By applying our algorithm we find that the implicit equation of $\mathbf{S}$ is

$$
4 x_{0}^{2}+8 x_{0} x_{1}-4 x_{0} x_{2}-4 x_{0} x_{3}+4 x_{1}^{2}-4 x_{1} x_{2}-8 x_{1} x_{3}+x_{2}^{2}+2 x_{2} x_{3}=0
$$

which agrees with the results of [5] and [8].
Remark 2.2 The problem of implicitizing a parametric space curve was tackled in [2]

## References

[1] J. Abbott, A.M. Bigatti, L. Robbiano Implicitization of Hypersurfaces, J. Symb. Comput. 30 (2016), 137-149.
[2] G. Albano, F. Cioffi, F. Orecchia, F. Ramella Minimally generating ideals of rational parametric curves in polynomial time. J. Symb. Comput. 30 (2000), 137-149.
[3] M.F. Atiyah, I.G. Macdonald Introduction to Commutative Algebra, Reading, Mass.-London-Don Mills, Ont. (1969), Addison-Wesley Publishing Company, Inc.
[4] L. Chiantini, F. Orecchia, I. Ramella Maximal rank and minimal generation of some parametric varieties. Journal of Pure and Applied Algebra 186 (2004), 21-31.
[5] G. Fix, C. Hsu, T. Luo, Implicitazion of rational parametric surfaces, J. Symb. Comput. 21 (1996), 329-336.
[6] R. Hartshorne, Algebraic Geometry, Graduate Texts in Mathematics 52 (1977), New York:Springer-Verlag.
[7] A: V. Geramita, F. Orecchia, On the Cohen-Macaulay type of s-lines in $\mathbb{A}^{n+1}$ J. Algebra 70 (1981), 89-133.
[8] D. Manocha, J. F. Canny Implicit representation of rational parametric surfaces, 13, J. Symb. Comput., 13 (1992), 485-510
[9] F. Orecchia, Points in generic position and conductors of curves with ordinary singularities, J. London Math. Soc. 24, (1981), 85-96,

