Implicitization of Algebraic Varieties

Günter Landsmann
Research Institute for Symbolic Computation
Johannes Kepler University
A-4040 Linz, Austria
landsmann@risc.uni-linz.ac.at

ABSTRACT

The concept of the implicit representation of a rationally parametrized algebraic variety is presented. After a brief introduction to the general theory of implicitization, various methods for finding this representation are discussed. From a theoretical point of view Gröbner basis methods seem to work best for finding the implicit equations. But the actual computation of Gröbner bases is often very time consuming. For this reason classical resultant methods are considered as an alternative. Since such methods fail in the presence of base points, the concept of moving varieties being free from restrictions of this kind is discussed. **Keywords:** Implicitization, Interpolation, Gröbner Bases, Resultants, Moving Lines. [1]

1. INTRODUCTION

An affine algebraic variety is the set of solutions of a system of polynomial equations. Given a set of polynomials $f_1, \ldots, f_m$, the geometric aspects of finding and describing their common zeros may be summarized by the phrase 'parametrization of varieties'. Powerful algorithms for deciding existence of a rational parametrization and providing one in the affirmative case have been developed by various research groups in recent time [30, 25].

While there is an obvious need for a concise description of the solution set of a polynomial system, in applications the problem often arises just the other way round. For instance, in Computer Aided Geometric Design one often asks for a finite set of polynomial equations, whose set of solutions contains all image points of a given parametrized surface in 3-space. Of course the solutions of the desired set of polynomials should contain these image points in a minimal way. The process of finding such a system from a given parametrization is called 'implicitization'. Thus, implicitization is concerned with the problem of finding the smallest algebraic variety that contains a given parametrized set.

Several methods of computing the implicit form have been developed. Among others, they make use of Gröbner Bases [14, 1], resultants [15], and interpolation techniques [24]. All these methods are related to Elimination Theory [16, 32] which, in its modern developments [19, 9] lies at the heart of implicitization. Recently a new method, based on syzygies, was developed and proved its power in many cases [12, 29, 33, 13, 2]. For any field $\mathbf{K}$, $\mathbb{A}^n(\mathbf{K})$ denotes the $n-$dimensional affine space $\mathbf{K}^n$. The $n-$dimensional projective space is $\mathbb{P}^n(\mathbf{K}) = (\mathbb{A}^n(\mathbf{K}) \setminus 0) / \sim$ where $x \sim y$ iff $y = \lambda x$ for a nonzero scalar λ.

2. THEORY OF IMPLICITIZATION

Consider a fixed field extension $\mathbf{k} \subseteq \mathbf{K}$. For any set $X \subseteq \mathbb{A}^n(\mathbf{K})$ its ideal is $\mathbf{I}X = \{f \in \mathbf{k}[x_1, \ldots, x_n] \mid f(X) \subseteq 0\}$. For any set $S \subseteq \mathbf{k}[x_1, \ldots, x_n]$, its zero set is $\mathbf{V}S = \{p \in \mathbf{K}^n \mid f(p) = 0 \ \forall f \in S\}$. The sets $\mathbf{V}S$ are the closed sets of the Zariski Topology on $\mathbb{A}^n(\mathbf{K})$. It is easy to see that $\mathbf{VI}X = \overline{X}$, so the association $X \mapsto \mathbf{I}X$ defines an injection from the set of algebraic varieties in $\mathbb{A}^n(\mathbf{K})$ into the set of radical ideals. In case $\mathbf{K}$ is algebraically closed this gives a one-one correspondence[2] whose inverse is given by $\mathbf{V}$. We write $\mathbf{K}[X]$ for the $\mathbf{k}$-algebra of polynomial functions on X i.e., $\mathbf{K}[X] = \{f\colon X \longrightarrow \mathbf{K} \mid \exists F \in \mathbf{k}[x_1, \ldots, x_n] \ \forall x \in X : f(x) = F(x)\}$. For irreducible X the ring $\mathbf{K}[X]$ is an integral domain. Then a tupel $\varphi = (\varphi_1, \ldots, \varphi_r) \in \mathbf{K}(X)^r$ where $\mathbf{K}(X)$ is the quotient field of $\mathbf{K}[X]$ defines a continuous map on an open subset $U \subseteq X$ with values in $\mathbb{A}^r(\mathbf{K})$. The ideal of its image is $\mathbf{I}(\text{im } \varphi) = \{G \in \mathbf{k}[y_1, \ldots, y_r] \mid G(\varphi_1, \ldots, \varphi_r) = 0\}$. If Y is an arbitrary subset of $\mathbb{A}^r(\mathbf{K})$ then φ is called a rational map $X \longrightarrow Y$ if $\varphi(p) \in Y \ \forall p \in U$. If Y is also irreducible then φ is birational if there is a rational map $\psi\colon Y \longrightarrow X$ with $\psi \circ \varphi = 1_X \wedge \varphi \circ \psi = 1_Y$ (on open subsets of X and Y). In case X equals the whole affine space $\mathbb{A}^n(\mathbf{K})$ we say that $Y = \overline{\text{im } \varphi}$ is rationally parametrized by φ. From continuity of φ one observes that Y is an irreducible variety. If all components of φ are regular functions, i.e., elements of $\mathbf{K}[X]$, Y is said to be polynomially parametrized by φ.

For any ideal $a \subseteq \mathbf{k}[x_1, \ldots, x_n]$ and $1 \leq l \leq n-1$, the lth elimination ideal of a is $a_l\colon = a \cap \mathbf{k}[x_{l+1}, \ldots, x_n]$. Obviously a_l is an ideal in $\mathbf{k}[x_{l+1}, \ldots, x_n]$ which conceptually depends on an ordering of the variables $x_1 > \cdots > x_n$. The following sequence of theorems indicates the significance of the notion of elimination ideal.

THEOREM 1 (EXTENSION THEOREM). *Assume $\mathbf{K}$ is algebraically closed, $a = \langle f_1, \ldots, f_s \rangle \subseteq \mathbf{k}[x_1, \ldots, x_n]$ is an ideal, a_1 its first elimination ideal. For each $1 \leq i \leq s$, write f_i as a polynomial in $\mathbf{k}[x_2, \ldots, x_n][x_1]$*

$$f_i = g_i(x_2, \ldots, x_n)x_1^{N_1} + terms\ of\ lower\ x_1 - degree,$$

where $N_i \geq 0$ and $g_i \neq 0$. Suppose that $(\lambda_2, \ldots, \lambda_n) \in \mathbf{V}(a_1) \setminus \mathbf{V}(g_1, \ldots, g_s)$. Then $\exists \lambda_1 \in \mathbf{K}$ such that $(\lambda_1, \lambda_2, \ldots, \lambda_n) \in \mathbf{V}(a)$.

[1] This work has been supported by the Austrian Science Fund (FWF) under the special research area SFB F013, subproject 04.

[2] This is one formulation of Hilberts Nullstellensatz.

This theorem gives a sufficient condition for extending partial solutions of a polynomial system to proper solutions. It is a key theoretical result in the area of zero dimensional systems. In order to use it for implicitization we give an equivalent geometric formulation.

THEOREM 2. $\mathbf{K}$ *algebraically closed,* $a = \langle f_1, \dots, f_s \rangle \subseteq \mathbf{k}[x_1, \dots, x_n]$, g_i *as in Theorem 1,* $X = \mathbf{V}(a)$. *Then*

$$\mathbf{V}(a_1) = \pi_1(X) \cup (\mathbf{V}(g_1, \dots, g_s) \cap \mathbf{V}(a_1))$$

where $\pi_1 \colon \mathbb{A}^n(\mathbf{K}) \longrightarrow \mathbb{A}^{n-1}(\mathbf{K})$ *is projection onto the last* $n-1$ *components.*

THEOREM 3 (CLOSURE THEOREM). *Assume* $\mathbf{K}$ *is algebraically closed,* $a \subseteq \mathbf{k}[t_1, \dots, t_m, x_1, \dots, x_n]$ *is an ideal and* $\pi \colon \mathbf{K}^m \times \mathbf{K}^n \longrightarrow \mathbf{K}^n$ *the projection. Then* $\overline{\pi(\mathbf{V}(a))} = \mathbf{V}(a_m)$. *Moreover, when* $\mathbf{V}(a) \neq \emptyset$, *there is an affine variety* $Y \subset \mathbf{V}(a_m)$ *such that* $\mathbf{V}(a_m) \setminus Y \subseteq \pi(\mathbf{V}(a))$.

Theorems 1, 2, 3 provide the main technical tools for proving the central theoretical results on implicitization.

THEOREM 4 (POLYNOMIAL IMPLICITIZATION). *Let* $\mathbf{K}$ *be infinite and let the variety* $X \subseteq \mathbb{A}^n(\mathbf{K})$ *be given by the polynomial parametrization*[3] $\rho = (f_1, \dots, f_n)$ *with* $f_1, \dots, f_n \in \mathbf{k}[t_1, \dots, t_m]$. *Let* a *be the ideal* $a = \langle x_1 - f_1, \dots, x_n - f_n \rangle \subseteq \mathbf{k}[t_1, \dots, t_m, x_1, \dots, x_n]$. *Then* $X = \mathbf{V}(a_m)$.

Rationally parametrized varieties can be treated in a similar way. The difficulty arising from denominators in the parametrizing functions can be captured by the invention of an additional condition.

THEOREM 5 (RATIONAL IMPLICITIZATION). *Let* $X \subseteq \mathbb{A}^n(\mathbf{K})$ *be parametrized by*

$$\rho = \left(\frac{f_1}{g_1}, \dots, \frac{f_n}{g_n} \right). \tag{1}$$

Let g *be a common multiple of* $g_1, \dots, g_n$ *and* a *the ideal in* $\mathbf{k}[y, t_1, \dots, t_m, x_1, \dots, x_n]$ *(where* y *is a new indeterminate) defined by* $a = \langle g_1 x_1 - f_1, \dots, g_n x_n - f_n, gy - 1 \rangle$. *If* $\mathbf{K}$ *is infinite then* $X = \mathbf{V}(a_{m+1})$.

Proofs of these fundamental theorems can be found e.g. in [14].

Every rational parametrization of an affine variety can be extended to a parametrization of the corresponding projective variety. In many situations the implicitization problem can be treated more conveniently in projective language.

DEFINITION 1. *Let* $F = (F_0, \dots, F_n) \in \mathbf{k}[t_0, \dots, t_m]_d^{n+1}$ *a tuple of homogeneous polynomials of equal degree* d, $B = \mathbf{V}(F_0, \dots, F_n)$ *the projective algebraic set of basis points.* F *defines a map* $\mathbb{P}^m(\mathbf{K}) \setminus B \longrightarrow \mathbb{P}^n(\mathbf{K})$. *We say that* $\overline{\mathrm{im}(F)}$ *is parametrized by* F.

A base point is a point $p \in \mathbb{P}^m(\mathbf{K})$ where F cannot be given a value in $\mathbb{P}^n(\mathbf{K})$, that means, p is given by coordinates $(\lambda_0, \dots, \lambda_m)$, where $F_0(\lambda_0, \dots, \lambda_m) = \cdots = F_n(\lambda_0, \dots, \lambda_m) = 0$ (and, of course, $(\lambda_0, \dots, \lambda_m) \neq 0$).

THEOREM 6 (PROJECTIVE IMPLICITIZATION). *Assume* $\mathbf{K}$ *is infinite, and let* $X \subseteq \mathbb{P}^n(\mathbf{K})$ *be parametrized by the tuple* $F \in \mathbf{k}[t_0, \dots, t_m]_d^{n+1}$. *Then* $X = \mathbf{V}(a_{m+1})$ *where* $a = \langle x_0 - F_0, \dots, x_n - F_n \rangle \subseteq \mathbf{k}[t_0, \dots, t_m, x_0, \dots, x_n]$ *and* $a_{m+1} = a \cap \mathbf{k}[x_0, \dots, x_n]$.

In the rest of the paper we study several methods for practical computation of the implicit representation of an parametrized variety.

3. INTERPOLATION

Finding the implicit representation of a parametrized variety means finding the coefficients of a finite set of polynomials. So, if we know bounds for the degrees of the desired polynomials, we may evaluate the given parametrizing functions in some finite set of interpolation nodes, thereby obtaining a linear system L. A nontrivial solution of L yields an answer to the implicitization problem. The following result for curves can be found in [28]:

PROPOSITION 1. *Let* $\left(\frac{u_1(t)}{v_1(t)}, \frac{u_2(t)}{v_2(t)} \right)$ *with* $\mathrm{GCD}(u_1, v_1) = \mathrm{GCD}(u_2, v_2) = 1$ *be a proper parametrization of an irreducible plane curve defined by* $f(x, y) = 0$. *Then*

$$\deg_x(f(x, y)) = \max\{\deg(u_2), \deg(v_2)\} \textit{ and}$$

$$\deg_y(f(x, y)) = \max\{\deg(u_1), \deg(v_1)\}.$$

A similar result holds for surfaces. The determination of such degree bounds is simple but the brute force approach often fails due to the huge size of the linear system. There has been progress in recent time as to development of methods that take advantage of the special type of such a linear system [24].

4. GRÖBNER BASES

The last theorems [4 and 5], describe the variety $\overline{\mathrm{im}(\rho)}$ with the aid of elimination ideals which therefore are of central interest. The theory of Gröbner bases yields a powerful tool for treating such ideals. The details can be found in [6].

THEOREM 7 (ELIMINATION). *Consider an ideal*

$$a \subseteq \mathbf{k}[t_1, \dots, t_m, x_1, \dots, x_n]$$

and let G *be a Gröbner basis of* a *with respect to an elimination order* $t_i >> x_j$. *Then* $G \cap \mathbf{k}[x_1, \dots, x_n]$ *is a Gröbner basis*[4] *of* $a \cap \mathbf{k}[x_1, \dots, x_n]$.

The acronym $t_i >> x_j$ means that any monomial involving one of $t_1, \dots, t_m$ is greater than all monomials in $\mathbf{k}[x_1, \dots, x_n]$.

EXAMPLE 1. *Consider the variety* X *parametrized by the tuple*

$$F = (s^2 - t^2 - u^2, 2su, 2st, s^2 + t^2 + u^2) \in \mathbf{k}[s, t, u]_2^4.$$

Applying Theorem 6 we construct the ideal

$$a = \langle x - (s^2 - t^2 - u^2), y - 2su, z - 2st, w - (s^2 + t^2 + u^2) \rangle.$$

[3] Note that this means that X equals the Zariski closure of $\mathrm{im}(\rho)$.

[4] with respect to the induced order on monomials in $\mathbf{k}[x_1, \dots, x_n]$

A Gröbner basis of a with respect to pure lexicographic order $s > t > u > x > y > z > w$ is

$$\begin{aligned}&x^2 + z^2 + y^2 - w^2, 2u^2z^2 + 2y^2u^2 + xy^2 - y^2w,\\ &-y^2 + 2u^2x + 2u^2w, ty - zu, -wy + 2yu^2 + xy + 2tzu,\\ &2tux + 2tuw - zy, -w + 2t^2 + 2u^2 + x, sz - xt - tw,\\ &sy - ux - uw, tz - sw + sx + yu, -y + 2su, -z + 2st,\\ &2s^2 - x - w.\end{aligned}$$

By Theorem 7 the Gröbner basis of the elimination ideal $a \cap \mathbf{k}[x, y, z, w]$ is $\{x^2 + z^2 + y^2 - w^2\}$. Therefore X is the unit sphere in 3-space.

Taking into account the existence of algorithms for computing the reduced Gröbner basis out of any ideal basis [7], the problem of finding the implicit representation of varieties given by rational parametrizations is completely solved. It is well known, however, that computing Gröbner bases for the ideals under consideration is a costly task which often stifles in its intermediate expression swell. This is the reason why different methods, though with their own disadvantages, are considered.

5. RESULTANTS

Consider positive degrees $d_0, \ldots, d_n$ representing linear spaces of homogeneous polynomials in $\mathbf{k}[x_0, \ldots, x_n]$. For each pair of indices i, α where $0 \leq i \leq n$ and $\alpha \in \mathbb{N}^{n+1}$ with $|\alpha| = d_i$ we introduce a variable $y_{i,\alpha}$ constructing the polynomial ring $\mathbb{Z}[y_{i,\alpha}]$. If $\Omega \in \mathbb{Z}[y_{i,\alpha}]$ and $F_i = \sum_{|\alpha|=d_i} c_{i,\alpha}x^\alpha$ are homogeneous polynomials in $\mathbf{k}[x_0, \ldots, x_n]$ of degree d_i $(0 \leq i \leq n)$ then $\Omega(F_0, \ldots, F_n)$ is the result of replacing in Ω the variable $y_{i,\alpha}$ by the scalar $c_{i,\alpha}$.

THEOREM 8. *Let $\mathbf{K}$ be algebraically closed and fix positive integers $d_0, \ldots, d_n$. Then there is a unique polynomial* Res $\in \mathbb{Z}[y_{i,\alpha}]$ *with the following properties:*

1. *If $F_0, \ldots, F_n \in \mathbf{K}[x_0, \ldots, x_n]$ are homogeneous of degrees $d_0, \ldots, d_n$ then $\mathbf{V}(F_0, \ldots, F_n) \neq \emptyset$ if and only if* $\mathrm{Res}(F_0, \ldots, F_n) = 0$.
2. $\mathrm{Res}(x_0^{d_0}, \ldots, x_n^{d_n}) = 1$.
3. Res *is irreducible in* $\mathbf{K}[y_{i,\alpha}]$.

Various methods for computing such a resultant can be found e.g. in [19, 15, 5]. The following consequence of Theorem 8 expresses the application of resultants to the implicitization problem.

THEOREM 9. *Let $\mathbf{K}$ be algebraically closed, and $f_0, \ldots, f_n \in \mathbf{K}[x_1, \ldots, x_n]$ be of positive degrees $d_0, \ldots, d_n$. Write*

$$f_j = f_{j,d_j} + \cdots + f_{j,0} \quad (0 \leq j \leq n)$$

as sum of its homogeneous components, and let $F_j \in \mathbf{K}[x_0, x_1, \ldots, x_n]$ be the homogenization of f_j. If the system of equations

$$f_{0,d_0} = \cdots = f_{n,d_n} = 0$$

has only the trivial solution, then, for a given tupel $(y_0, \ldots, y_n) \in \mathbf{K}^{n+1}$, the equations

$$\begin{aligned} y_0 &= f_0(x_1, \ldots, x_n) \\ &\vdots \\ y_n &= f_n(x_1, \ldots, x_n) \end{aligned} \tag{2}$$

have a common solution $(s_1, \ldots, s_n) \in \mathbf{K}^n$ if and only if

$$\mathrm{Res}(F_0 - y_0x_0^{d_0}, \ldots, F_n - y_nx_0^{d_n}) = 0.$$

Roughly speaking, the implicit representation of a parametrized variety is given by the resultant of a family of homogeneous polynomials. The problem is that the resultant vanishes identically when the given parametrization has base points. In this case sparse resultants or perturbation techniques can be used for implicitization [22]. Another way is given by the following concept.

6. MOVING VARIETIES

Again consider an affine variety $X \subseteq \mathbb{A}^n(\mathbf{K})$ given in parametrized form

$$X = \left(\frac{f_1}{f_0}, \ldots, \frac{f_n}{f_0}\right)$$

where $f_\mu \in \mathbf{k}[t_1, \ldots, t_m]$. A moving variety of type d and multi-degree $(\sigma_1, \ldots, \sigma_m)$ is a polynomial

$$\sum_{i_1=0}^{\sigma_1} \cdots \sum_{i_m=0}^{\sigma_m} \sum_{|\alpha|=d} A^\alpha_{i_1 \ldots i_m} x^\alpha t_1^{i_1} \cdots t_m^{i_m} \tag{3}$$

where $\alpha = (\alpha_0, \ldots, \alpha_n) \in \mathbb{N}^{n+1}$ and $x^\alpha = x_0^{\alpha_0} \cdots x_n^{\alpha_n}$. For each fixed value of $t_1, \ldots, t_m$ (3) is the implicit representation of a variety in $\mathbb{P}^n(K)$. The moving variety is said to follow X if

$$\sum_{i_1=0}^{\sigma_1} \cdots \sum_{i_m=0}^{\sigma_m} \sum_{|\alpha|=d} A^\alpha_{i_1 \ldots i_m} f^\alpha t_1^{i_1} \cdots t_m^{i_m} = 0 \tag{4}$$

$(f^\alpha = f_0(t_1, \ldots, t_m)^{\alpha_0} \cdots f_n(t_1, \ldots, t_m)^{\alpha_n})$. Moving varieties following X can be computed by solving a linear system. In case $n = 2$, if (3) is linear in x_0, x_1, x_2, it is called a `moving line`, when $n = 3$ and (3) is linear in $x_0, \ldots, x_3$ it is called a `moving plane` etc.

Classical Implicitization of Curves

In its simplest instances the method of moving varieties presents itself as a generalization of the classical resultant method. For example, consider the case $n = 2, m = 1$, i.e., we deal with a parametrized curve

$$\mathcal{C}: \qquad x = \frac{x(t)}{w(t)}, \quad y = \frac{y(t)}{w(t)} \tag{5}$$

where we may assume that $\mathrm{GCD}(x(t), y(t), w(t)) = 1$. This means that the parametrization (5) has no base points. Invoking the classical implicitization method, we construct auxiliary polynomials

$$f = xw(t) - x(t), \quad g = yw(t) - y(t). \tag{6}$$

The implicit representation of (5) is then given by the resultant

$$\mathrm{Res}_t(f, g) = 0.$$

The standard tools for computing the resultant are the Sylvester matrix $Syl(f, g)$ and the Bezout matrix $Bez(f, g)$.

Given two degree n polynomials

$$\varphi = \sum_{i=0}^{n} u_it^i, \quad \psi = \sum_{i=0}^{n} v_it^i,$$

the **Sylvester resultant** is the determinant of the $2n \times 2n$ matrix

$$Syl(f,g) = \begin{pmatrix} u_0 & v_0 & & & & & \\ u_1 & v_1 & u_0 & v_0 & & & \\ \vdots & \vdots & u_1 & v_1 & \ddots & & \\ u_{n-1} & v_{n-1} & \vdots & \vdots & \ddots & u_0 & v_0 \\ u_n & v_n & u_{n-1} & v_{n-1} & \ddots & u_1 & v_1 \\ & & u_n & v_n & \ddots & \vdots & \vdots \\ & & & & & u_n & v_n \end{pmatrix}$$

where void space is occupied by 0. $Syl(\varphi,\psi)$ is of order$=$ $2n$, sparse, with repetitive entries and easy to compute. In the special case of polynomials (6) are the entries of $\mathrm{Syl}(f,g)$ linear expressions in x and y.

To construct the Bezout resultant of φ,ψ we consider the polynomials

$$\begin{aligned} \varphi_k(t) &= u_n t^k + u_{n-1}t^{k-1} + \cdots + u_{n-k} \\ \psi_k(t) &= v_n t^k + v_{n-1}t^{k-1} + \cdots + v_{n-k} \\ p_{k+1}(t) &= \psi_k(t)\varphi(t) - \varphi_k(t)\psi(t) \quad (k = 0,\ldots,n-1). \end{aligned}$$

From

$$\begin{aligned} \varphi(t) &= \varphi_k(t)t^{n-k} + u_{n-k-1}t^{n-k-1} + \cdots + u_1 t + u_0 \\ \psi(t) &= \psi_k(t)t^{n-k} + v_{n-k-1}t^{n-k-1} + \cdots + v_1 t + v_0 \end{aligned}$$

it follows that $p_1,\ldots,p_n$ are polynomials of degree $n-1$ in t. The **Bezout resultant** of φ,ψ is the determinant of the $n \times n$ matrix

$$Bez(\varphi,\psi) = Coeff[p_1(t),\ldots,p_n(t)].$$

$Bez(\varphi,\psi)$ has more complicated entries but order $= n$.

In order to use the Bezout approach for implicitization of curve (5) we write the polynomials of the given rational parametrization with equal formal degree:

$$\begin{aligned} x(t) &= a_n t^n + \cdots + a_1 t + a_0 \\ y(t) &= b_n t^n + \cdots + b_1 t + b_0 \\ w(t) &= d_n t^n + \cdots + d_1 t + d_0. \end{aligned}$$

The auxiliary polynomials (6) are then

$$\begin{aligned} &f(t) = (xd_n - a_n)t^n + \cdots + (xd_1 - a_1)t + (xd_0 - a_0) \\ &g(t) = (yd_n - b_n)t^n + \cdots + (yd_1 - b_1)t + (yd_0 - b_0). \end{aligned}$$

To build $\mathrm{Bez}(f,g)$ we generate the polynomials

$$\begin{aligned} f_k(t) &= (xd_n - a_n)t^k + \cdots + (xd_{n-k} - a_{n-k}) \\ g_k(t) &= (yd_n - b_n)t^k + \cdots + (yd_{n-k} - b_{n-k}) \\ p_{k+1} &= g_k(t)f(t) - f_k(t)g(t) = \\ &= g_k(t)(xw(t) - x(t)) - f_k(t)(yw(t) - y(t)) \end{aligned}$$

where $k = 0,\ldots,n-1$. The polynomials $p_1(t),\ldots,p_n(t)$ are of degree $n-1$ in t, their coefficients are linear in x,y. Moreover they vanish along the curve $\mathcal{C}$. **They are certain moving lines following the curve.** Thus they can be written as

$$\begin{aligned} p_1(t) &= L^1_{n-1}(x,y)t^{n-1} + \cdots + L^1_1(x,y)t + L^1_0(x,y) \\ &\vdots \\ p_n(t) &= L^n_{n-1}(x,y)t^{n-1} + \cdots + L^n_1(x,y)t + L^n_0(x,y) \end{aligned}$$

with $L^j_i(x,y)$ linear in x,y. The determinant

$$\det(L^j_i(x,y)) = \mathrm{Bez}(f(t),g(t))$$

is the implicit representation of $\mathcal{C}$. Thus we can say that implizitization of curve (5) by means of the classical Bezout Resultant amounts to using n certain moving lines of degree $n-1$.

Moving Lines

In order to generalize the classical method to using more arbitrary moving varieties we first provide an overview over all moving lines of arbitrary degree following curve $\mathcal{C}$.

The general moving line of degree d is

$$(A_0 x + B_0 y + C_0 w) + \cdots + (A_d x + B_d y + C_d w)t^d \quad (7)$$

where $A_0,\ldots,C_d$ are constants. If (7) shall follow the curve (5) then

$$\sum_{j=0}^{d} \left(A_j x(t) + B_j y(t) + C_j w(t)\right) t^j = 0. \quad (8)$$

The left hand side of expression (8) is a polynomial in t of degree $n+d$ so we get a linear system

$$\mathrm{Coeff}[x(t),y(t),w(t),x(t)t,\ldots,w(t)t^d](A_0,\ldots,C_d)^T = 0$$

which is of order $n+d+1 \times 3d+3$. Hence there are at least

$$3d + 3 - (n+d+1) = 2d + 2 - n \quad (9)$$

linearly independent solutions. Therefore, by setting $d = n-1$, we obtain at least n linearly independent solutions

$$\begin{aligned} p_1(t) &= L^1_0(x,y) + \cdots + L^1_{n-1}(x,y)t^{n-1} \\ &\vdots \\ p_n(t) &= L^n_0(x,y) + \cdots + L^n_{n-1}(x,y)t^{n-1}. \end{aligned}$$

Consider the $n \times n$ matrix

$$\mathrm{Coeff[p_1(t),\ldots,p_n(t)]} = (L^j_i(x,y)).$$

Its determinant is a polynomial in x,y of degree $\leq n$ which obviously vanishes on $\mathcal{C}$. Thus it is a good candidate for the implicit polynomial of $\mathcal{C}$. If it works, we call this method **implicitization by moving lines**.

THEOREM 10. *The method of moving lines works, if the parametrized curve (5) has no basepoints.*

A proof can be found in [29].

In case the degree of the parametrization of curve $\mathcal{C}$ is even, $n = 2m$, there is the following variant of this method: For arbitrary d there are at least $2(d+1-m)$ linearly independent solutions. Specializing $d = m$ we get ≥ 2 independent moving lines p,q following the curve.

THEOREM 11. *When there are no moving lines of degree $< m$ that follow the curve then* $\det(\mathrm{Syl}(p,q)) = 0$ *is the implicit equation*[5] *of curve (5).*

[5] note that the matrix $\mathrm{Syl}(p,q)$ is a Sylvester matrix with the order of the Bezout matrix. Thus the method takes advantage of both matrix approaches.

The proof consists in showing that

1. $\det(\mathrm{Syl}(p,q)) \neq 0$;
2. $\deg\ \det(\mathrm{Syl}(p,q)) \leq 2m$;
3. $\det(\mathrm{Syl}(p,q))$ vanishes on the curve (5).

The existence of a moving line of degree $m-1$ following the curve is equivalent to the vanishing of the $3m \times 3m$ determinant

$$\left|\mathrm{Coeff}[x(t), y(t), w(t), \ldots, x(t)t^{m-1}, y(t)t^{m-1}, w(t)t^{m-1}]\right|.$$

This is a polynomial in the coefficients of $x(t), y(t), w(t)$ and therefore almost never vanishes.

If the parametrization (5) is of odd degree, $n = 2m+1$, there is always at least one non-zero moving line of degree m and at least 3 linarly independent moving lines of degree $m+1$ that follow the curve. Therefore, there always exists a moving line p of degree m and a moving line q of degree $m+1$, where q is not a multiple of p, that follow the curve. In a similar way to the case $n = 2m$ we get:

THEOREM 12. *When there are no moving lines of degree $< m$ that follow the curve then $\det(\mathrm{Syl}(p,q)) = 0$ is the implicit equation*[6] *of curve (5).*

EXAMPLE 2. *Consider the degree 6 affine curve*

$$\begin{aligned} x(t) &= 1 + 2t^2 + 2t^5, \quad y(t) = 2 + t^6, \\ w(t) &= 1 + t + 2t^2 + 2t^3 + t^4 + t^6. \end{aligned}$$

Equation (7) gives

$$\sum_{j=0}^{5} \left(A_j x(t) + B_j y(t) + C_j w(t)\right) t^j = 0$$

where the left hand side is a polynomial of degree $2n-1 = 11$ in t. This gives 12 linear equations in 18 unknowns, hence there are at least 6 linearly independent solutions. The determinant of the matrix $R(x,y) = L_{i,j}(x,y)$ of coefficients of a set of such solutions gives the implicit equation.

On the other hand we have 2 linearly independent moving lines of degree 3:

$$\begin{aligned} p &= 209x + 317y - 843w + (427x + 83y + 250w)t \\ &+ (340y + 338w)t^2 + (-339x + 333y - 333w)t^3 \\ q &= 303x - 303w + (343x + 181y - 402w)t \\ &+ (317x - 179y + 443w)t^2 + (-132x + 413y - 413w)t^3 \end{aligned}$$

The determinant of $\mathrm{Syl}(p,q)$ *is the implicit representation of the curve. Written out this is*

$$\begin{array}{l} 16554x + 6728y - 3399x^2 - 21524xy + 18304xy^3 \\ -26902x^2y^2 - 9270xy^2 + 11648x^3y + 22550x^2y \\ -9483x^4 - 4632x^3 + 1499y^2 - 7055y^4 + 11890y^3x^2 \\ -3364y^4x^2 - 5010x^5 + 4065x^5y + 16078x^4y \\ -7910x^4y^2 - 12710x^3y^2 + 6219x^3y^3 - 739x^6 + 3852y^3 \\ +2256y^5 - 4472xy^4 - 207y^6 + 408y^5x - 7073 \end{array}$$

Existence of low dimensional Moving Lines

By our previous analysis we see that there are always moving lines of degree d following a curve of degree n if $d > \frac{n}{2} - 1$. Let μ be the lowest degree of such a moving line. Hence $\mu \leq \lfloor \frac{n}{2} \rfloor$. Let p be a moving line with the lowest degree μ that follows the curve. There are always at least $2(n-\mu) + 2 - n = n + 2 - 2\mu$ linearly independent moving lines of degree $n - \mu$ that follow the curve. Not all of them can be multiples of p, hence there is a degree $n - \mu$ moving line q that is not a multiple of p. The two moving lines p and q have the following property:

THEOREM 13. *Any degree d moving line that follows the curve (5) can be written uniquely as $Ap + Bq$, where A is a polynomial in t with $\deg A \leq d - \mu$, and B is a polynomial in t with $\deg B \leq d + \mu - n$.*

Implicitizing Curves by Moving Conics

A moving conic of degree d is a polynomial

$$A(t)x^2 + B(t)xy + C(t)y^2 + D(t)xw + E(t)yw + F(t)w^2 \quad (10)$$

where $A(t), \ldots, F(t)$ are polynomials of degree d in t. Alternatively (10) can be written as

$$C_0(x,y) + C_1(x,y)t + \cdots + C_d(x,y)t^d$$

with homogeneous polynomials $C_j(c,y)$ of degree 2. The moving conic (10) follows the curve (5) if

$$\begin{aligned} A(t)x^2(t) + B(t)x(t)y(t) + C(t)y^2(t) + D(t)x(t)w(t) \\ + E(t)y(t)w(t) + F(t)w^2(t) = 0. \end{aligned}$$

Geometrically this means that the conic corresponding to the parameter value t_0 passes through the point on curve (5) corresponding to t_0. In complete analogy to the case of moving lines we may proceed to study the situation of moving conics. We sketch the development for a rationally parametrized curve of even degree.

Assume the degree of (5) is $2n$. Searching for moving conics of degree $n-1$ following the curve leads to a system of $5n$ homogeneous linear equations in $6n$ unknowns, therefore to at least n linearly independent solutions $c_1, \ldots, c_n$. Constructing the matrix of coefficients, which now consists of quadratic polynomials, and computing its determinant should output the implicit representation of the curve. Unfortunately, in this case, this method of moving conics does not always yield the implicit representation of the curve, even if we have eliminated all base points. Here is the result for this case:

THEOREM 14. *The method of moving conics generates the implicit equation for a rational curve of degree $2n$ with no base points if and only if there is no moving line of degree $n-1$ that follows the curve. Moreover, when there is a moving line of degree $n-1$ following the curve, any determinant generated by the method of moving conics is identically zero.*

The proof is given in [29].

Implicitizing Surfaces by Moving Planes

For rational surfaces, moving lines and moving conics generalize to moving planes and moving quadrics.

[6] here the Sylvester matrix is of size $2m+1$

A moving plane of bidegree (σ_1, σ_2) is a polynomial of the form

$$\sum_{i=0}^{\sigma_1}\sum_{j=0}^{\sigma_2}(A_{ij}x + B_{ij}y + C_{ij}z + D_{ij}w)\, s^i t^j. \qquad (11)$$

For each fixed value of s, t this gives the implicit representation of a plane in $I\!P^3(K)$.

Assume given a rational surface

$$x = \frac{x(s,t)}{w(s,t)}, \quad y = \frac{y(s,t)}{w(s,t)}, \quad z = \frac{z(s,t)}{w(s,t)} \qquad (12)$$

where

$$x(s,t) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_{ij}s^i t^j, \qquad y(s,t) = \sum_{i=0}^{m}\sum_{j=0}^{n} b_{ij}s^i t^j$$

$$z(s,t) = \sum_{i=0}^{m}\sum_{j=0}^{n} c_{ij}s^i t^j, \qquad w(s,t) = \sum_{i=0}^{m}\sum_{j=0}^{n} d_{ij}s^i t^j$$

are polynomials of bidegree (m, n). The moving plane (11) is said to follow surface (12) if

$$\sum_{i=0}^{\sigma_1}\sum_{j=0}^{\sigma_2}(A_{ij}x(s,t) + B_{ij}y(s,t) + C_{ij}z(s,t) + D_{ij}w(s,t))\, s^i t^j = 0. \qquad (13)$$

Equation (13) amounts to $(\sigma_1 + m + 1)(\sigma_2 + n + 1)$ homogeneous linear equations in $4(\sigma_1 + 1)(\sigma_2 + 1)$ unknowns.

Choosing, specifically, $\sigma_1 = 2m - 1$, $\sigma_2 = n - 1$ we get $6mn$ equations in $8mn$ variables. Hence there are at least $2mn$ linearly independent solutions $p_1, \ldots, p_{2mn}$:

$$\sum_{i=0}^{2m-1}\sum_{j=0}^{n-1}\left(A^1_{ij}x + B^1_{ij}y + C^1_{ij}z + D^1_{ij}w\right) s^i t^j$$

$$\vdots$$

$$\sum_{i=0}^{2m-1}\sum_{j=0}^{n-1}\left(A^{2mn}_{ij}x + B^{2mn}_{ij}y + C^{2mn}_{ij}z + D^{2mn}_{ij}w\right) s^i t^j.$$

Each of these solutions is a moving plane that follows surface (12). The determinant of the $2mn \times 2mn$ coefficient matrix

$$\begin{array}{ccc} A^1_{00}x + B^1_{00}y + C^1_{00}z + D^1_{00}w & \cdots & A^1_{2m-1,n-1}x + \cdots + D^1_{2m-1,n-1}w \\ \vdots & & \vdots \\ A^{2mn}_{00}x + \cdots\cdots + D^{2mn}_{00}w & \cdots & A^{2mn}_{2m-1,n-1}x + \cdots + D^{2mn}_{2m-1,n-1}w \end{array}$$

vanishes whenever (x, y, z, w) lies on the surface. Hence if this determinant does not vanish identically, then it is the implicit representation of (12) [$2mn$ is the generic degree of surface (12)].

As in the case of curves the auxiliary polynomials

$$xw(s,t) - x(s,t), \; yw(s,t) - y(s,t), \; zw(s,t) - z(s,t)$$

are moving planes of bidegree (m, n) that follow the surface. So the standard resultant technique for implicitization uses 3 moving planes of bidegree (m, n) following the surface. Using the Sylvester resultant generates $6mn$ moving planes of bidegree $(3m - 1, 2n - 1)$, whereas the Dixon resultant generates $2mn$ moving planes of bidegree $(m - 1, 2n - 1)$.

Efficient Implicitization of Surfaces by Moving Planes

The last method i.e. construction of an $2mn \times 2mn$ implicitization matrix does not give anything essentially new, since such a matrix can be found more directly by computing the Dixon resultant of the auxiliary polynomials. As in the curve case there is a new method which consists in construction of an implicitization matrix that has the style of the Sylvester resultant and the order of the Dixon resultant. The following considerations go back to work from M. Zhang, R. Goldman and E. Chion [33].

Consider moving planes of bidegree $(m - 1, n)$

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n}(A_{ij}x + B_{ij}y + C_{ij}z + D_{ij}w)\, s^i t^j. \qquad (14)$$

If (14) shall follow the surface (12) we get a linear system of $2m(2n+1)$ equations with $4m(n+1)$ unknowns. Hence there are at least $4m(n+1) - 2m(2n+1) = 2m$ lin. indep. solutions:

$$p_1 \;=\; \sum_{i=0}^{m-1}\sum_{j=0}^{n}\left(A^1_{ij}x + B^1_{ij}y + C^1_{ij}z + D^1_{ij}w\right) s^i t^j$$

$$\vdots$$

$$p_{2m} \;=\; \sum_{i=0}^{m-1}\sum_{j=0}^{n}\left(A^{2m}_{ij}x + B^{2m}_{ij}y + C^{2m}_{ij}z + D^{2m}_{ij}w\right) s^i t^j$$

Let M be the matrix of coefficients of this linear system, where the rows are indexed by

$$1, \ldots, t^{2n-1}, s, \ldots, st^{2n-1}, \ldots, s^{m-1}, \ldots, s^{m-1}t^{2n-1}.$$

M is square of order $2mn$, its entries repeat and it is sparse. Moreover $\det M = 0$ for surface points, and, because the entries are linear in x, y $\deg M \le 2mn$. If surface (12) has no excess base points, the irreducible implicit representation of (12) is of degree $2mn$. Therefore, if $\det M \neq 0$, it is the implicit representation of surface (12). The condition $\det M \neq 0$ is true in almost all cases.

THEOREM 15. *The method of moving planes computes the implicit equation of a generic rational surface (12) from a determinant in the style of Sylvester with the size of Dixon.*

Using the method of moving quadrics for a tensor product surface of bidegree (m, n) produces a determinant of order mn whereas usual resultant methods end up in determinants of order $2mn$. In the presence of base points, the resultant either vanishes identically, or becomes very complicated, while the moving quadrics method often simplifies.

7. REFERENCES

[1] C. ALONSO, J. GUTIERREZ AND T. RECIO. An implicitization algorithm with fewer variables. *Computer Aided Geometric Design 12* (1995), 251–258.

[2] C. D'ANDREA. Resultants and Moving Surfaces. *Journal of Symbolic Computation 31* (2001), 585–602.

[3] F. Aries and R. Senoussi. An Implicitization Algorithm for Rational Surfaces with no Base Points. *Journal of Symbolic Computation 31* (2001), 357–365.

[4] T. Becker and V. Weisspfennig. *Gröbner Bases. A Computational Approach to Commutative Algebra.* Springer 1993.

[5] P. Bikker and A.Yu. Uteshev. On the Bezout Construction of the Resultant. *Journal of Symbolic Computation 28* (1999), 45–88.

[6] B. Buchberger. Gröbner basis: an algorithmic method in polynomial ideal theory. *Multidimensional Systems Theory* (1985), N. K. Bose ed., 184–232.

[7] B. Buchberger and F. Winkler. Gröbner Bases and Applications. *London Math. Soc. Lecture Notes 251* (1998).

[8] L. Buse. Residual resultant over the projective plane and the implicitization problem. (2001)

[9] L. Buse, M. Elkadi and B. Mourrain. Generalized Resultants over Unirational Algebraic Varieties. *Journal of Symbolic Computation 29* (2000), 515–526.

[10] J. Canny. Generalised Characteristic Polynomials. *Journal of Symbolic Computation 9* (1990), 241–250.

[11] Eng-Wee Chionh, Ming Zhang and R. Goldman. Implicitization Matrices in the Style of Sylvester with the Order of Bezout. *Saint-Malo Proceedings, Nashville, TN.*, (2000) 1–10.

[12] T.A. Cox. Equations of Parametric Curves and Surfaces via Syzygies. *Contemporary Mathematics* (2000).

[13] D. Cox, R.N. Goldman and Ming Zhang. On the Validity of Implicitization by Moving Quadrics for Rational Surfaces with No Base Points. *Journal of Symbolic Computation 11* (1999), 1–23.

[14] D. Cox, J. Little and D. O'Shea. *Ideals, Varieties, and Algorithms.* Springer Verlag, New York (1996).

[15] D. Cox, J. Little and D. O'Shea. Using Algebraic Geometry. Springer Verlag, New York (1998).

[16] A. L. Dixon. The Eliminant of Three Quantics in Two Independent Variables. *Proc. London Mathematics Society 6* (1908), 49–69, 473–492.

[17] G. Fix, Chih-Ping Hsu and Tie Luo. Implicitization of Rational Parametric Surfaces. *Journal of Symbolic Computation 21* (1996), 329–336.

[18] Xiao-Shan Gao and Shang-Ching Chou. Implicitization of Rational Parametric Equations. *Journal of Symbolic Computation 14* (1992), 459–470.

[19] I. Gelfand, M. Kapranov and A. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants.* Birkhäser, Boston (1994).

[20] R.N. Goldman, T.W. Sederberg and D.C. Anderson. Vector elimination: A technique for the implicitization, inversion, and intersection of planar parametric rational polynomial curves. *Computer Aided Geometric Design 1* (1984), 327–356.

[21] L. Gonzales-Vega. Implicitization of Parametric Curves and Surfaces by using Multidimensional Newton Formulae. *Journal of Symbolic Computation 23* (1997), 137–151.

[22] D. Manocha and J.F. Canny. Algorithms for Implicitizing Rational Parametric Surfaces. *Computer Aided Geometric Design 9* (1992), 25–50.

[23] D. Manocha and J.F. Canny. MultiPolynomial Resultant Algorithms. *Journal of Symbolic Computation 15* (1993),99–122.

[24] A. Marco and J. J. Martinez. Using polynomial interpolation for implicitizing algebraic curves. Computer Aided Geometric Design 18(4) (2001), 309–319.

[25] J. Schicho. Rational Parametrization of Real Algebraic Surfaces. *RISC-report, RISC-Linz 98-01* (1998).

[26] T.W. Sederberg. Degenerate parametric curves. *Computer Aided Geometric Design 1* (1984), 301–307.

[27] T.W. Sederberg. Improperly parametrized rational curves. *Computer Aided Geometric Design 3* (1986), 67–75.

[28] J.R. Sendra and F. Winkler. A symbolic algorithm for the parametrization of algebraic plane curves. *Tech. Rep. 89-41.1, RISC-Linz* (1998).

[29] T. Sederberg, R.N. Goldman and Hang Du. Implicitizing Rational Curves by the Method of Moving Algebraic Curves. *Journal of Symbolic Computation 23* (1997), 153–175.

[30] J.R. Sendra and F. Winkler. Parametrization of Algebraic Curves over Optimal Field Extensions. *Journal of Symbolic Computation 23* (1997), 191–207.

[31] J.R. Sendra and F. Winkler. Tracing Index of Rational Parametrizations. *Tech. Rep. 01-01, RISC-Linz* (2001).

[32] B. van der Waerden. Modern Algebra 2. Ungar Publishing Co., New York (1950).

[33] Ming Zhang, R.N. Goldman and Eng-Wee Chionh. Efficient Implicitization of Rational Surfaces by Moving Planes. (2000).