Implicitization by Using Gröbner Bases

Michael Kalkbrener*
Research Institute for Symbolic Computation (RISC)
Johannes Kepler University Linz, Austria

June 17, 1990

Abstract

In this paper Gröbner bases are used for computing the implicit representations of varieties given by rational parametrizations. Two algorithms for the implicitization of varieties of arbitrary dimension are presented and their termination and correctness are proved. Furthermore, algorithms that are particularly suited for the implicitization of curves and surfaces in 3D-space are given. Each of the algorithms presented in this paper has been implemented in the computer algebra system Maple. Several examples are computed and the computing times of the different algorithms are given.

1 Introduction

The automatic conversion of parametrically defined varieties into their implicit form is of fundamental importance in geometric modeling. The reason for this is that implicit and parametric representations are appropriate for different classes of problems. For instance, it is universally recognized that the parametric representation is best suited for generating points along a variety, whereas the implicit representation is most convenient for determining whether a given point lies on a specific variety. It is also well-known that the problem of intersecting two varieties is greatly simplified if one variety can be expressed implicitly and the other parametrically.

For some time the implicitization problem has been deemed unsolvable in the CAD literature ([FP81] or [Tim77]). In 1984 the problem has been solved for rational parametric curves in 2D and rational parametric surfaces in 3D by using resultants (see [SAG84]). Resolvents have been applied to find the implicit representation of rational parametric cubic curves in 3D ([Gol85]). Arnon and Sederberg used Gröbner bases for the implicitization of polynomial parametric varieties of dimension $n-1$ in n-dimensional space ([AS84]). In 1987 Buchberger generalized their method to the case of polynomial parametric varieties of arbitrary dimension ([Buc87]).

In this paper we deal with the most general case and use Gröbner bases for the implicitization of varieties of arbitrary dimension given by rational parametrizations.

One way to solve this problem is the following: Instead of working with varieties in the affine space given by rational parametrizations we consider varieties in the projective

*Supported by the Austrian Fonds zur Förderung der wissenschaftlichen Forschung, Projekt Nr. P6763

space given by parametrizations consisting of homogenous polynomials and proceed as described in [Buc87]. Unfortunately the introduction of the two homogenizing variables makes the computation of the Gröbner bases much more costly (see computing times in section 6).
Given the rational parametrization

$$x_1 := \frac{p_1}{q_1} \quad \dots \quad x_n := \frac{p_n}{q_n},$$

where $p_1, \dots, p_n, q_1, \dots, q_n$ are polynomials in $y_1, \dots, y_m$, our second general implicitization algorithm computes the squarefree form q of the polynomial $q_1 \cdots q_n$. Then the implicit representation of the given variety can be found by computing

$$GB(\{p_1 \cdot x_1 - q_1, \dots, p_n \cdot x_n - q_n, q \cdot z - 1\}) \cap K[x_1, \dots, x_n],$$

where z is a new variable and GB is the Gröbner basis with respect to the lexical ordering with $x_1 \prec \dots \prec x_n \prec y_1 \prec \dots \prec y_m \prec z$.
Implicitization of varieties in 3D-space is of particular importance for geometric modeling. Recently we have developed algorithms based on Gröbner bases computations that solve this special problem without introducing additional variables ([Kal90]). In this paper we present these algorithms without correctness proofs.
We have implemented each of the algorithms presented in this paper in *Maple*. It turned out that in almost every example the implicitization algorithm that works in the projective space was the slowest algorithm. Furthermore, in 3D-space the general implicitization algorithms were much slower than the algorithms designed for this special problem.
In section 2 and 3 we state the problem we are concerned with and a few properties of Gröbner bases that we need for proving the correctness of our implicitization algorithms. In section 4 we present the general implicitization algorithms and prove their correctness. In section 5 we deal with implicitization of curves and surfaces in 3D-space. In section 6 some examples are computed and the computing times of the different algorithms are compared.

2 The Problem

Throughout the paper let K be a field and $\bar{K}$ the algebraic closure of K.
Let J be an ideal and $g_1, \dots, g_r$ polynomials in $K[x_1, \dots, x_n]$. $V(J)$ denotes the *variety* of J, i.e. the set

$$\{a \in \bar{K}^n \mid f(a) = 0 \text{ for every } f \in J\}.$$

Instead of $V(Ideal(\{g_1, \dots, g_r\}))$ we will often write $V(\{g_1, \dots, g_r\})$.
Let L be a field with $K \subseteq L$. Then $(a_1, \dots, a_n) \in L^n$ is a *generic point* of J if for every $f \in K[x_1, \dots, x_n]$:

$$f \in J \text{ if and only if } f(a_1, \dots, a_n) = 0.$$

It is well-know that an ideal is prime if and only if it has a generic point with coordinates in a universal domain (see for instance [vdW67]).

In this paper we want to solve the following problem:

Implicitization Problem:
given: rational parametrization of a variety

$$x_1 = \frac{p_1}{q_1} \quad \ldots\ldots \quad x_n = \frac{p_n}{q_n},$$

where $p_1, \ldots, p_n \in K[y_1, \ldots, y_m]$, $q_1, \ldots, q_n \in K[y_1, \ldots, y_m] - \{0\}$ and

$$p_i \text{ and } q_i \text{ are relatively prime} \quad (i = 1, \ldots, n).$$

find: implicit representation of this variety, i.e. polynomials $g_1, \ldots, g_r$ in $K[x_1, \ldots, x_n]$ such that

$$V(\{g_1, \ldots, g_r\}) = V(P),$$

where P is the prime ideal in $K[x_1, \ldots, x_n]$ with

$$(\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}) \in K(y_1, \ldots, y_m)$$

as generic point.

Example 1 *If the rational parametrization*

$$x_1 = \frac{2y_2}{1 + y_1^2 + y_2^2} \qquad x_2 = \frac{2y_1y_2}{1 + y_1^2 + y_2^2} \qquad x_3 = \frac{y_2^2 - y_1^2 - 1}{1 + y_1^2 + y_2^2}$$

is given then the implicit representation

$$x_1^2 + x_2^2 + x_3^2 - 1$$

of the unit sphere is a solution of the above problem. •

3 The Method

Each of the implicitization algorithms presented in the following sections is based on the computation of Gröbner bases. In 1965 this method has been introduced by B. Buchberger in his Ph.D. thesis (see [Buc65] or [Buc70]). The method of Gröbner bases, as its central objective, solves the simplification problem for polynomial ideals and, on this basis, gives easy solutions to a large number of other algorithmic problems. During the last years Gröbner bases have become one of the most popular methods in computer algebra.
In this paper we will not give a definition of Gröbner bases. We will only state some properties which we need for proving the correctness of our implicitization algorithms. For a complete reference of the Gröbner bases method see [Buc85] or [Buc87].

Let F be a finite subset of $K[x_1, \ldots, x_n]$. Then $GB(F)$, the Gröbner basis of F with respect to the lexical ordering of power products with $x_1 \prec \ldots \prec x_n$ has the following properties:

1. $GB(F)$ is a finite subset of $K[x_1, \ldots, x_n]$,

2. $Ideal(F) = Ideal(GB(F))$, *(property of ideal equality)*

3. for every $i \in \{1, \ldots, n\}$:

$$Ideal(GB(F)) \cap K[x_1, \ldots, x_i] = Ideal(GB(F) \cap K[x_1, \ldots, x_i]),$$

where the ideal on the right hand side is formed in $K[x_1, \ldots, x_i]$.
(elimination property)

4 Implicitization of Rational Parametric Varieties

Throughout the paper let $p_1, \ldots, p_n \in K[y_1, \ldots, y_m]$ and $q_1, \ldots, q_n \in K[y_1, \ldots, y_m] - \{0\}$ such that

$$p_i \text{ and } q_i \text{ are relatively prime} \qquad (i = 1, \ldots, n)$$

and let P be the prime ideal in $K[x_1, \ldots, x_n]$ which has

$$(\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}) \in K(y_1, \ldots, y_m)$$

as generic point.

4.1 Implicitization of Polynomial Parametric Varieties

If the given rational parametrization

$$x_1 = \frac{p_1}{q_1} \quad \ldots\ldots \quad x_n = \frac{p_n}{q_n}$$

is a polynomial parametrization, i.e.

$$q_1 = \ldots = q_n = 1,$$

then the implicit representation of this variety can be found very easily by computing

$$\{g_1, \ldots, g_r\} := GB(\{x_1 - p_1, \ldots, x_n - p_n\}) \cap K[x_1, \ldots, x_n],$$

where GB has to be computed using the lexical ordering determined by $x_1 \prec \ldots \prec x_n \prec y_1 \prec \ldots \prec y_m$ (see [Buc87]).

Example 2 *If a variety is given by the polynomial representation*

$$x_1 = y_1 + y_2 \quad x_2 = y_1 + 2y_2^2 - 1 \quad x_3 = y_1 y_2 \quad x_4 = y_2^2 - 1$$

then this implicit representation

$$\begin{gathered}\{\ 4x_4^2 - 4x_4x_2 + 5x_4 + 2 - x_1^2 + 2x_3 - 2x_2 + x_2^2, \\ 4x_4x_3 + 2x_4x_2 + x_4 + x_1^2 + 2x_1x_3 - 2x_2x_3 - x_2^2, \\ x_4 + 1 - x_1^2 + x_3 - 2x_4x_1 - x_1 + x_2x_1, \\ 1 - 2x_1^2 + 5x_3 - x_1 - x_2x_1 + 2x_2 - 2x_2x_1^2 + 4x_2x_3 - 6x_1x_3 + x_2^2 + 4x_3^2 + 2x_1^3\ \}\end{gathered}$$

can be found by computing the Gröbner basis

$$GB(\{x_1 - (y_1 + y_2),\ x_2 - (y_1 + 2y_2^2 - 1),\ x_3 - y_1y_2,\ x_4 - (y_2^2 - 1)\}) \cap K[x_1, x_2, x_3, x_4]. \bullet$$

If not all q's are 1 then it seems reasonable to assume that the implicitization problem can be solved by computing

$$\{g_1,\ldots,g_r\} := GB(\{q_1\cdot x_1 - p_1,\ldots,q_n\cdot x_n - p_n\})\cap K[x_1,\ldots,x_n].$$

Unfortunately, this is not true as the following example shows.

Example 3 *We consider again the parametrization of the unit sphere*

$$x_1 = \frac{2y_2}{1+y_1^2+y_2^2} \qquad x_2 = \frac{2y_1y_2}{1+y_1^2+y_2^2} \qquad x_3 = \frac{y_2^2-y_1^2-1}{1+y_1^2+y_2^2}.$$

By computing

$$GB(\{(1+y_1^2+y_2^2)x_1 - 2y_2,\ (1+y_1^2+y_2^2)x_2 - 2y_1y_2,\ (1+y_1^2+y_2^2)x_3 - (y_2^2-y_1^2-1)\})$$
$$\cap K[x_1,x_2,x_3]$$

we do not obtain an implicit representation of the unit sphere but the empty set. •

4.2 Homogenization

One possibility to overcome this difficulty is by working in the projective space with projective parametrizations:

Example 4 *Instead of the parametrization*

$$x_1 = \frac{2y_2}{1+y_1^2+y_2^2} \qquad x_2 = \frac{2y_1y_2}{1+y_1^2+y_2^2} \qquad x_3 = \frac{y_2^2-y_1^2-1}{1+y_1^2+y_2^2}$$

of the unit sphere in the affine space we consider the projective parametrization

$$x_0 = y_0^2+y_1^2+y_2^2 \qquad x_1 = 2y_2y_0 \qquad x_2 = 2y_1y_2 \qquad x_3 = y_2^2-y_1^2-y_0^2$$

of the projective unit sphere (x_0 and y_0 are homogenizing variables). Now we can proceed as in the case of polynomial parametrizations and obtain

$$\{x_1^2+x_2^2+x_3^2-x_0^2\} =$$

$$GB(\{x_0-(y_0^2+y_1^2+y_2^2),\ x_1-2y_2y_0,\ x_2-2y_1y_2,\ x_3-(y_2^2-y_1^2-y_0^2)\})\cap K[x_0,x_1,x_2,x_3],$$

where GB has to be computed using the lexical ordering determined by $x_0 \prec x_1 \prec x_2 \prec x_3 \prec y_0 \prec y_1 \prec y_2$.
After dehomogenizing, i.e. substituting 1 for x_0, we obtain the desired polynomial

$$x_1^2+x_2^2+x_3^2-1. \quad \bullet$$

The general algorithm has the following form

projective_implicitization (in: $p_1, \ldots, p_n, q_1, \ldots, q_n$; out: $\{g_1, \ldots, g_r\}$)

input: $p_1, \ldots, p_n \in K[y_1, \ldots, y_m]$, $q_1, \ldots, q_n \in K[y_1, \ldots, y_m] - \{0\}$ and

p_i and q_i are relatively prime $\quad (i = 1, \ldots, n)$.

output: $\{g_1, \ldots, g_r\}$, a finite subset of $K[x_1, \ldots, x_n]$ such that

$$V(\{g_1, \ldots, g_r\}) = V(P),$$

where P is the prime ideal in $K[x_1, \ldots, x_n]$ with

$$(\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}) \in K(y_1, \ldots, y_m)$$

as generic point.

$p_0 := 1$
$q_0 := 1$
$q :=$ *least common multiple of* $q_1, \ldots, q_n$
$s := max(tdeg(p_1 \cdot q/q_1), \ldots, tdeg(p_n \cdot q/q_n), tdeg(q))$, where *tdeg* denotes the total degree of a polynomial
for i **from** 0 **to** n **do**
  $f_i := p_i \cdot q/q_i$
  $h_i := y_0^s \cdot f_i(y_1/y_0, \ldots, y_m/y_0)$
$G := GB(\{x_0 - h_0, \ldots, x_n - h_n\}) \cap K[x_0, \ldots, x_n]$
$\{g_1, \ldots, g_r\} := \{g(1, x_1, \ldots, x_n) \mid g(x_0, \ldots, x_n) \in G\}$

where GB has to be computed using the lexical ordering determined by $x_0 \prec \ldots \prec x_n \prec y_0 \prec \ldots \prec y_m$.

Since the termination of **projective_implicitization** is obvious we only have to show its correctness.

Proof of correctness:
Let $p_1, \ldots, p_n, q_1, \ldots, q_n$ satisfy the input specification, let P be the prime ideal in $K[x_1, \ldots, x_n]$ with

$$(\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n})$$

as generic point and I the prime ideal in $K[x_0, \ldots, x_n]$ with

$$(h_0, \ldots, h_n)$$

as generic point. Let $f \in K[x_1, \ldots, x_n]$ and $f' \in K[x_0, x_1, \ldots, x_4]$ such that f' is homogenous and $f'(1, x_1, \ldots, x_n) = f$. Then

$$f \in P \quad \text{iff} \quad f(\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}) = 0 \quad \text{iff} \quad f'(1, \frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}) = 0.$$

As $q \neq 0$, f' is homogenous, $p_0 = q_0 = 1$ and $h_i(1, y_1, \ldots, y_m) = p_i \cdot q/q_i$ for every $i \in \{0, \ldots, n\}$ we know that

$$f'(1, \frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}) = 0$$

iff

$$f'(\frac{p_0 \cdot q}{q_0}, \frac{p_1 \cdot q}{q_1}, \ldots, \frac{p_n \cdot q}{q_n}) = 0$$

iff

$$f'(h_0(1, y_1, \ldots, y_m), \ldots, h_n(1, y_1, \ldots, y_m)) = 0.$$

From $f'(h_0(1, y_1, \ldots, y_m), \ldots, h_n(1, y_1, \ldots, y_m)) = 0$ it follows that $y_0 - 1$ divides the polymomial $f'(h_0(y_0, y_1, \ldots, y_m), \ldots, h_n(y_0, y_1, \ldots, y_m))$ in $K[y_0, y_1, \ldots, y_m]$. As $f'(h_0, \ldots, h_n)$ is homogenous, $f'(h_0, \ldots, h_n) = 0$. Hence,

$$f'(h_0(1, y_1, \ldots, y_m), \ldots, h_n(1, y_1, \ldots, y_m)) = 0$$

iff

$$f'(h_0(y_0, y_1, \ldots, y_m), \ldots, h_n(y_0, y_1, \ldots, y_m)) = 0$$

iff

$$f' \in I.$$

Altogether,

$$f \in P \quad \text{iff} \quad f' \in I. \tag{1}$$

Let $e \in I$ and $e_0, \ldots, e_d$ be homogenous polynomials such that for every $i \in \{0, \ldots, d\}$

$$tdeg(e_i) = i \text{ and } e = e_d + \ldots e_0.$$

As $e_0(h_o, \ldots, h_n), \ldots, e_d(h_0, \ldots, h_n)$ are homogenous polynomials in $K[y_0, \ldots, y_m]$ of different total degrees it follows from $e(h_0, \ldots, h_n) = 0$ that

$$e_i(h_0, \ldots, h_n) = 0 \quad (i = 0, \ldots, n).$$

From this fact and from (1) it follows that for every $(a_1, \ldots, a_n) \in \bar{K}^n$

$$(a_1, \ldots, a_n) \in V(P) \quad \text{iff} \quad (1, a_1, \ldots, a_n) \in V(I).$$

From the result in section 4.1 we obtain that

$$(1, a_1, \ldots, a_n) \in V(I) \quad \text{iff} \quad (1, a_1, \ldots, a_n) \in V(G) \quad \text{iff} \quad (a_1, \ldots, a_n) \in V(\{g_1, \ldots, g_r\}).$$

Altogether,

$$V(P) = V(\{g_1, \ldots, g_r\}). \quad \bullet$$

The complexity of Gröbner bases computations heavily depends on the number of variables in the input polynomials and on the degrees of these polynomials. The homogenization process tends to increase the degrees of the input polynomials. Furthermore, the need for two additional homogenizing variables is another disadvantage of this method (see computing times in section 6).

The implicitization algorithm in the next subsection gets along with the introduction of just one additional variable. This variable is used in a similar way as in the proof of Hilbert's Nullstellensatz given by A. Rabinowitsch (see for instance [vdW67]).

4.3 The Rabinowitsch Trick

Example 5 *The implicit representation of the unit sphere given by the rational parametrization*

$$x_1 = \frac{2y_2}{1+y_1^2+y_2^2} \qquad x_2 = \frac{2y_1y_2}{1+y_1^2+y_2^2} \qquad x_3 = \frac{y_2^2-y_1^2-1}{1+y_1^2+y_2^2}$$

can be obtained by computing

$$\{x_1^2+x_2^2+x_3^2-1\} = GB(\{(1+y_1^2+y_2^2)z-1,\ (1+y_1^2+y_2^2)x_1-2y_2,\\ (1+y_1^2+y_2^2)x_2-2y_1y_2,\ (1+y_1^2+y_2^2)x_3-(y_2^2-y_1^2-1)\}) \cap K[x_1,x_2,x_3],$$

where z is a new variable and GB has to be computed using the lexical ordering determined by $x_1 \prec x_2 \prec x_3 \prec y_1 \prec y_2 \prec z$. •

This strategy always works:

Theorem 1 *Let q be the squarefree form of the polynomial $q_1 \cdots q_n$ and let*

$$\{g_1,\ldots,g_r\} := GB(\{q\cdot z-1, q_1\cdot x_1-p_1,\ldots,q_n\cdot x_n-p_n\}) \cap K[x_1,\ldots,x_n],$$

where z is a new variable and GB has to be computed using the lexical ordering determined by $x_1 \prec \ldots \prec x_n \prec y_1 \prec \ldots \prec y_m \prec z$. Then

$$\{g_1,\ldots,g_r\} \text{ generates } P.$$

Proof: Let I be the ideal in $K[x_1,\ldots,x_n,y_1,\ldots,y_m,z]$ that is generated by $\{q\cdot z-1, q_1\cdot x_1-p_1,\ldots,q_n\cdot x_n-p_n\}$. Obviously,

$$(\frac{p_1}{q_1},\ldots,\frac{p_n}{q_n},y_1,\ldots,y_m,\frac{1}{q})$$

is a zero of I. From the fact that

$$(\frac{p_1}{q_1},\ldots,\frac{p_n}{q_n})$$

is a generic point of P it follows that every element of $I \cap K[x_1,\ldots,x_n]$ is an element of P. Hence,

$$\{g_1,\ldots,g_r\} \subseteq P. \tag{2}$$

Let f be an element of P. It is well-known that there exists a non-negative integer s_1 and a polynomial h_1 in $K[x_1,\ldots,x_n,y_1,\ldots,y_m]$ such that

$$q_1^{s_1}\cdot f-(q_1\cdot x_1-p_1)\cdot h_1 \in K[x_2,\ldots,x_n,y_1,\ldots,y_m].$$

Thus, there exist non-negative integers $s_1,\ldots,s_n$ and polynomials $h_1,\ldots,h_n$ with

$$\bar{f} := (\prod_{i=1}^{n} q_i^{s_i})\cdot f-\sum_{i=1}^{n}(q_i\cdot x_i-p_i)\cdot h_i \in K[y_1,\ldots,y_m]. \tag{3}$$

From the fact that

$$(\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}, y_1, \ldots, y_m)$$

is a common zero of the polynomials $f, q_1 \cdot x_1 - p_1, \ldots, q_n \cdot x_n - p_n \in K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ it follows that

$$(\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}, y_1, \ldots, y_m)$$

is a zero of $\bar{f}$. As $\bar{f} \in K[y_1, \ldots, y_m]$,

$$\bar{f} \text{ is the polynomial } 0.$$

Together with (3),

$$(\prod_{i=1}^{n} q_i^{s_i}) \cdot f = \sum_{i=1}^{n} (q_i \cdot x_i - p_i) \cdot h_i. \tag{4}$$

Therefore, the set

$$M := \{g \in K[y_1, \ldots, y_m] - \{0\} \mid g \cdot f \in I \text{ and } squarefree(g) \text{ divides } \prod_{i=1}^{n} q_i\}$$

is not empty. Let $\bar{g}$ be an element of M with minimal total degree.
Assumption: The total degree of $\bar{g}$ is greater than 0.
Obviously,

$$\frac{q}{gcd(q,\bar{g})} \cdot \bar{g} \cdot f \cdot z - (\frac{\bar{g}}{gcd(q,\bar{g})} \cdot f \cdot (q \cdot z - 1)) = \frac{\bar{g}}{gcd(q,\bar{g})} \cdot f.$$

As $\bar{g} \cdot f \in I$ and $q \cdot z - 1 \in I$,

$$\frac{\bar{g}}{gcd(q,\bar{g})} \cdot f \in I.$$

Obviously,

$$squarefree(\frac{\bar{g}}{gcd(q,\bar{g})}) \text{ divides } \prod_{i=1}^{n} q_i.$$

Therefore,

$$\frac{\bar{g}}{gcd(q,\bar{g})} \in M.$$

As $gcd(q,\bar{g})$ is not 1,

$$\text{the total degree of } \frac{\bar{g}}{gcd(q,\bar{g})} \text{ is smaller than the total degree of } \bar{g}.$$

This is a contradiction to the definition of $\bar{g}$.
Hence, there exists a polynomial in M that is a constant. By definition of M,

$$f \in I$$

and therefore

$$P \subseteq I \cap K[x_1, \ldots, x_n].$$

Thus, by the elimination property of Gröbner bases,

$$P \subseteq Ideal(\{g_1, \ldots, g_r\}).$$

Together with (2),

$$\{g_1, \ldots, g_r\} \text{ generates } P. \bullet$$

5 Implicitization of Rational Parametric Curves and Surfaces in 3D-Space

Implicitization of varieties in 3D-space, i.e. varieties that are subsets of $\bar{K}^3$, is of particular importance for geometric modeling. Therefore we have tried to construct algorithms that solve this special problem considerably faster than the general implicitization algorithms described in the previous sections.
Throughout this section let us assume that a rational parametrization

$$x_1 = \frac{p_1}{q_1} \qquad x_2 = \frac{p_2}{q_2} \qquad x_3 = \frac{p_3}{q_3}$$

is given, where $p_1, p_2, p_3 \in K[y_1, y_2]$ and $q_1, q_2, q_3 \in K[y_1, y_2] - \{0\}$ and p_i and q_i are relatively prime ($i = 1, 2, 3$).

Definition: Let $(b_1, b_2) \in \bar{K}^2$. We denote the number of elements in the set

$$\{i \in \{1,2,3\} \mid p_i(b_1, b_2) = q_i(b_1, b_2) = 0\}$$

by $zero(b_1, b_2)$.

Example 6 *We consider again the parametrization of the unit sphere*

$$x_1 = \frac{2y_2}{1 + y_1^2 + y_2^2} \qquad x_2 = \frac{2y_1 y_2}{1 + y_1^2 + y_2^2} \qquad x_3 = \frac{y_2^2 - y_1^2 - 1}{1 + y_1^2 + y_2^2}.$$

Then for $(0,0)$, $(i,0) \in \bar{\mathbb{Q}}^2$, *where* $\bar{\mathbb{Q}}$ *denotes the algebraic closure of* $\mathbb{Q}$*:*

$$zero(0,0) = 0 \quad and \quad zero(i,0) = 3. \bullet$$

Theorem 2 *Let*

$$\{g_1, \ldots, g_r\} := GB(\{q_1 \cdot x_1 - p_1,\ q_2 \cdot x_2 - p_2,\ q_3 \cdot x_3 - p_3\}) \cap K[x_1, x_2, x_3],$$

where GB has to be computed using the lexical ordering determined by $x_1 \prec x_2 \prec x_3 \prec y_1 \prec y_2$. *Then the following holds:*
If for all $(b_1, b_2) \in \bar{K}^2$*:*

$$zero(b_1, b_2) < 2$$

then

$$V(\{g_1, \ldots, g_r\}) = V(P).$$

Proof: see Theorem 4 in [Kal90].

Thus, if for every $(i,j) \in \{(1,2),(1,3),(2,3)\}$

$$p_i, q_i, p_j, q_j \text{ have no common zeros}$$

then, by the above theorem, we can obtain the implicit form of the variety given by

$$x_1 = \frac{p_1}{q_1} \qquad x_2 = \frac{p_2}{q_2} \qquad x_3 = \frac{p_3}{q_3}$$

by computing

$$\{g_1, \ldots, g_r\} := GB(\{q_1 \cdot x_1 - p_1,\ q_2 \cdot x_2 - p_2,\ q_3 \cdot x_3 - p_3\}) \cap K[x_1, x_2, x_3].$$

In particular, this algorithm can be applied if

$$p_1, p_2, p_3, q_1, q_2, q_3 \in K[y_1] \text{ or } p_1, p_2, p_3, q_1, q_2, q_3 \in K[y_2].$$

(Note that p_i and q_i are relatively prime for $i \in \{1, 2, 3\}$.)
Unfortunately this easy algorithm does not work for arbitrary rational parametrizations (see Example 3). In fact, it is stated in the following theorem that

$$GB(\{q_1 \cdot x_1 - p_1,\ q_2 \cdot x_2 - p_2,\ q_3 \cdot x_3 - p_3\}) \cap K[x_1, x_2, x_3] = \emptyset$$

if there exists a $(b_1, b_2) \in \bar{K}^2$ with $zero(b_1, b_2) = 3$.

Theorem 3 *Let I be the ideal in $K[x_1, x_2, x_3, y_1, y_2]$ generated by $q_1 \cdot x_1 - p_1,\ q_2 \cdot x_2 - p_2,\ q_3 \cdot x_3 - p_3$. Then*

$$I \cap K[x_1, x_2, x_3] = \{0\}$$

iff

there exists a $(b_1, b_2) \in \bar{K}^2$ with $zero(b_1, b_2) = 3$.

Proof: see Theorem 3 in [Kal90].

The implicit representation of surfaces given by arbitrary rational parametrizations can be found by using the following algorithm. This algorithm decides whether the variety given by the parametric representation

$$x_1 = \frac{p_1}{q_1} \qquad x_2 = \frac{p_2}{q_2} \qquad x_3 = \frac{p_3}{q_3}$$

is a surface, i.e. whether the transcendence degree of

$$K(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3})$$

(over K) is 2. In this case it computes an implicit representation of the surface.
Definition: Let h, g be polynomials in $K[x_1, x_2, x_3, y_1]$ such that g has no non-trivial factor in $K[y_1]$ and there exists a polynomial p in $K[y_1]$ with $h = g \cdot p$. Then

$$h_{/y_1} := g.$$

implicit_surface (in: $p_1, p_2, p_3, q_1, q_2, q_3$; out: g)

input: $p_1, p_2, p_3 \in K[y_1, y_2]$, $q_1, q_2, q_3 \in K[y_1, y_2] - \{0\}$ such that

$$p_i \text{ and } q_i \text{ are relatively prime} \quad (i = 1, 2, 3).$$

output: $g \in K[x_1, x_2, x_3]$ such that if the transcendence degree of

$$K(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3})$$

is 2 then

$$g \notin K \text{ and } V(\{g\}) = V(P),$$

where P is the prime ideal in $K[x_1, x_2, x_3]$ with the generic point

$$(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}),$$

and

$$g = 1$$

otherwise.

for every $(i, j) \in \{(1,2), (1,3), (2,3)\}$ do
$\quad G_{(i,j)} := GB(\{f_i, f_j\}) \cap K[x_1, x_2, x_3, y_1]$
$\quad F_{(i,j)} := \{h_{/y_1} \mid h \in G_{(i,j)}\}$
$G := GB(F_{(1,2)} \cup F_{(1,3)} \cup F_{(2,3)} \cup \{f_1, f_2, f_3\}) \cap K[x_1, x_2, x_3]$
$g := gcd(G)$

where GB has to be computed using the lexical ordering determined by $x_1 \prec x_2 \prec x_3 \prec y_1 \prec y_2$.

Example 7 *Again we consider the unit sphere given by*

$$x_1 = \frac{2y_2}{1 + y_1^2 + y_2^2} \qquad x_2 = \frac{2y_1 y_2}{1 + y_1^2 + y_2^2} \qquad x_3 = \frac{y_2^2 - y_1^2 - 1}{1 + y_1^2 + y_2^2}.$$

Using implicit_surface *we obtain*

$G_{(1,2)} := \{x_2 + y_1^2 x_2 - x_1 y_1 - y_1^3 x_1\}$,
$F_{(1,2)} := \{-x_2 + x_1 y_1\}$,
$G_{(1,3)} := \{x_1^2 + 2x_1^2 y_1^2 - y_1^2 - 1 + y_1^4 x_1^2 + x_3^2 + y_1^2 x_3^2\}$,
$F_{(1,3)} := \{x_1^2 y_1^2 + x_1^2 - 1 + x_3^2\}$,
$G_{(2,3)} := \{-x_2^2 - 2y_1^2 x_2^2 + y_1^4 + y_1^2 - y_1^4 x_2^2 - y_1^2 x_3^2 - y_1^4 x_3^2\}$,
$F_{(2,3)} := \{y_1^2 x_2^2 + x_2^2 - y_1^2 + y_1^2 x_3^2\}$,
$G := \{x_1^2 + x_2^2 + x_3^2 - 1\}$,
$g := x_1^2 + x_2^2 + x_3^2 - 1$, *the implicit representation of the unit sphere.* •

The termination of the algorithm is obvious, the proof of correctness can be found in [Kal90].

6 Examples and Computing Times

We have implemented the algorithms presented in the previous sections in Maple 4.3. All the computations have been done on an Apollo 4500.

Example 1: (*Zylinder*)

Parametric Representation:

$$x_1 = \frac{1 - y_2^2}{1 + y_2^2} \qquad x_2 = \frac{2y_2}{1 + y_2^2} \qquad x_3 = y_1$$

Implicit Representation:

$$-1 + x_2^2 + x_1^2$$

Example 2: (*Sphere*)

Parametric Representation:

$$x_1 = \frac{2y_2}{1 + y_1^2 + y_2^2} \qquad x_2 = \frac{2y_1y_2}{1 + y_1^2 + y_2^2} \qquad x_3 = \frac{y_2^2 - y_1^2 - 1}{1 + y_1^2 + y_2^2}$$

Implicit Representation:

$$x_1^2 + x_2^2 + x_3^2 - 1$$

Example 3:

Parametric Representation:

$$x_1 = \frac{y_1^2 - y_2^2}{y_2} \qquad x_2 = \frac{y_1^2 - y_2^2}{y_1} \qquad x_3 = \frac{1}{y_1 - y_2}$$

Implicit Representation:

$$-x_1 - x_2 + x_2x_1x_3$$

Example 4:

Parametric Representation:

$$x_1 = \frac{y_2 + 2y_1^4 - 1}{y_2 - y_1 - 2} \qquad x_2 = \frac{y_1^2y_2 + 1}{y_1} \qquad x_3 = \frac{1}{y_1y_2}$$

Implicit Representation:

$$\begin{gathered} -1 + 2x_3^6x_2^4x_1 + 4x_2^3x_3^5 + x_3^6x_2^3x_1 - 3x_3^5x_2^2x_1 + 10x_2^2x_3^2x_1 - \\ 8x_2^3x_3^5x_1 + 4x_2x_3^3 + 3x_2x_3^4x_1 + 12x_2^2x_3^4x_1 + x_1 - x_2^5x_3^5x_1 - 10x_2^2x_3^2 + \\ 5x_3x_2 - 10x_2^3x_3^3x_1 - 5x_2x_3x_1 - x_2^4x_3^6 - x_3^3x_1 + 10x_2^3x_3^3 - 8x_2x_3^3x_1 - \\ 6x_2^2x_3^4 - 5x_2^4x_3^4 + 5x_2^4x_3^4x_1 - x_3^2 + 2x_3^2x_1 + 2x_3^6 + x_2^5x_3^5 \end{gathered}$$

Example 5:

Parametric Representation:

$$x_1 = \frac{1}{y_3} \qquad x_2 = \frac{y_3 - y_1}{y_3} \qquad x_3 = \frac{y_3 - y_2^2}{y_3} \qquad x_4 = \frac{y_3 - y_2 y_1 + y_1^3}{y_3}$$

Implicit Representation:

$$\begin{gathered} 1 + 6x_4x_1^2x_2 - 2x_1^3x_3x_2 + 15x_2^4 - 6x_4x_1^2x_2^2 - 6x_2 + 2x_1^2 - 2x_4x_1^2 + 15x_2^2 - \\ 6x_2x_1^2 + 6x_2^2x_1^2 - x_1^3 + x_1^4 - 6x_2^5 + x_2^2x_1^3x_3 - x_2^2x_1^3 - 2x_1^2x_2^3 + \\ x_4^2x_1^4 + 2x_1^2x_2^3x_4 + x_2^6 - 20x_2^3 - 2x_4x_1^4 + x_1^3x_3 + 2x_2x_1^3 \end{gathered}$$

Example 6:

Parametric Representation:

$$x_1 = y_1 y_2 \qquad x_2 = \frac{y_2}{y_1} \qquad x_3 = \frac{1}{y_1 - y_2} \qquad x_4 = y_2^2 - y_1$$

Implicit Representation:

$$\begin{gathered} 1 - x_2x_1x_3 + x_3x_4 + x_1x_3^2 - x_2x_1x_3^2, \\ x_1x_3 - x_2^2x_1 - x_2x_1x_3 + x_2x_4, \\ x_1x_3^2 - 2x_2x_1x_3^2 - x_2 + x_2^2x_1x_3^2 \end{gathered}$$

Example 7:

Parametric Representation:

$$x_1 = \frac{y_1}{y_3} \qquad x_2 = y_1 y_2 \qquad x_3 = \frac{1}{y_1 - y_2} \qquad x_4 = \frac{y_3 - y_1}{y_3} \qquad x_5 = y_1^2$$

Implicit Representation:

$$\begin{gathered} -x_5 + x_3^2x_2^2 - 2x_3^2x_2x_5 + x_6^2x_3^2, \\ -1 + x_1 + x_4 \end{gathered}$$

Computing times

We have compared the computing times of the algorithm **proj_implicitization** based on homogenization (subsection 4.2), the algorithm based on the Rabinowitsch trick (subsection 4.3) and the algorithm **implicit_surface** that computes the implicit representation of a surface in 3D-space (section 5). As the varieties in Example 5, 6 and 7 are not in 3D-space **implicit_surface** cannot be used. The computing times are given in milliseconds.

Example	proj_implicitization	Rabinowitsch	implicit_surface
1	18817	5184	7217
2	30683	273899	22233
3	> 10000000	1063300	26633
4	> 10000000	> 10000000	276716
5	522617	59617	– – – –
6	> 10000000	16434	– – – –
7	> 10000000	25450	– – – –

Because of Theorem 2 the implicit form of the variety in Example 1 and the variety in Example 4 can be found by computing

$$GB(\{q_1 \cdot x_1 - p_1,\ q_2 \cdot x_2 - p_2,\ q_3 \cdot x_3 - p_3\}) \cap K[x_1, x_2, x_3].$$

The computation of the implicit representation in Example 1 (Example 4) took 3217 (565850) milliseconds.

References

[AS84] D.S. Arnon and T.W. Sederberg. Implicit Equation for a Parametric Surface by Gröbner Basis. In V.E. Golden, editor, *Proceedings of the 1984 MACSYMA User's Conference*, pages 431–436, General Electric, Schenectady, New York, 1984.

[Buc65] B. Buchberger. *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal (in German).* PhD thesis, Univ. of Innsbruck (Austria), Dept. of Mathematics, 1965.

[Buc70] B. Buchberger. An Algorithmic Criterion for the Solvability of Algebraic Systems of Equations (in German). *Aequationes Mathematicae*, 4(3):374–383, 1970.

[Buc85] B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In N.K. Bose, editor, *Multidimensional Systems Theory*, pages 184–232. D. Reidel Publishing Company, Dordrecht-Boston-Lancaster, 1985.

[Buc87] B. Buchberger. Applications of Gröbner Bases in Non-Linear Computational Geometry. In *Proc. Workshop on Scientific Software*, IMA, Minneapolis, USA, 1987. Springer.

[FP81] I.D. Faux and M.A. Pratt. *Computational Geometry for Design and Manufacture.* Ellis Horwood, Chichester, 1981.

[Gol85] R.N. Goldman. The method of resolvents: A technique for the implicitization, inversion, and intersection of non-planar, parametric, rational cubic curves. *Computer Aided Geometric Design*, 2:237–255, 1985.

[Kal90] M. Kalkbrener. Implicitization of Rational Curves and Surfaces. In *Proc. of the AAECC-8 (to appear)*, 1990.

[SAG84] T.W. Sederberg, D.C. Anderson, and R.N. Goldman. Implicit Representation of Parametric Curves and Surfaces. *Computer Vision, Graphics, and Image Processing*, 28:72–84, 1984.

[Tim77] H.G. Timmer. A Solution to the Surface Intersection Problem. Technical Report NAS2-9590, McDonnell-Douglas Corp., 1977.

[vdW67] B.L. van der Waerden. *Algebra II (in German).* Springer, Berlin Heidelberg New York, 1967.