

# Implicitization of Rational Parametric Curves and Surfaces

Michael Kalkbrener\*

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

March 5, 1990

## Abstract

The automatic conversion of parametrically defined curves or surfaces into their implicit form is of fundamental importance in geometric modeling. Different methods in elimination theory, like resultants and Gröbner bases, have been used for solving this problem. The advantage of the Gröbner bases method is that no extraneous factors are introduced.

In this paper we use Gröbner bases for the implicitization of rational parametric curves and surfaces. One way to solve this problem is to homogenize the given curve or surface and to proceed as in the case of polynomial parametric curves or surfaces. As the introduction of additional variables makes the computation process more costly we have tried to cope with this problem without homogenization.

In this paper we prove that the implicit form of a curve or surface given by the rational parametrization

$$x_1 := \frac{p_1}{q_1} \quad x_2 := \frac{p_2}{q_2} \quad x_3 := \frac{p_3}{q_3},$$

where the  $p$ 's and  $q$ 's are univariate polynomials in  $y_1$  or bivariate polynomials in  $y_1, y_2$  over a field  $K$ , can always be found by computing

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

where  $GB$  is the Gröbner basis with respect to the lexical ordering with  $x_1 < x_2 < x_3 < y_1 < y_2$ , if for every  $i, j \in \{1, 2, 3\}$ ,  $i \neq j$ :

$p_i, q_i, p_j, q_j$  have no common zeros.

Since we can always assume that  $p_i$  and  $q_i$  are relatively prime ( $i = 1, 2, 3$ ), the above condition is always satisfied, if the  $p$ 's and  $q$ 's are univariate. Therefore, the above result leads immediately to an implicitization algorithm for arbitrary rational parametric curves.

Furthermore, we present an algorithm for the implicitization of arbitrary rational parametric surfaces and prove its termination and correctness.

*also in the case where ...*

*für  $\vec{v}$ ,  
C,  $y_j$   
innerhalb von  
 $x_1, x_2, x_3$  total  
ist!  $\rightarrow$   $y_1, y_2$ .*

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

*Warum  $\frac{1}{y_1}$  zum  $n$ -dim. Fall,  
siehe [Bou07].*

# 1 Introduction

The automatic conversion of parametrically defined curves or surfaces into their implicit form is of fundamental importance in geometric modeling. Different methods in elimination theory, like resultants (see for instance [SAG84]) and Gröbner bases (see [AS84], [Buc87]), have been used for solving this problem. The advantage of the Gröbner bases method is that no extraneous factors are introduced.

In this paper we use Gröbner bases for the implicitization of rational parametric curves and surfaces. One way to solve this problem is to homogenize the given curve or surface and to proceed as in the case of polynomial parametric curves or surfaces (see [AS84] and [Buc87]). As the introduction of additional variables makes the computation process more costly we have tried to cope with this problem without homogenization.

In this paper we prove that the implicit form of a curve or surface given by the rational parametrization

$$x_1 := \frac{p_1}{q_1} \quad x_2 := \frac{p_2}{q_2} \quad x_3 := \frac{p_3}{q_3},$$

where the  $p$ 's and  $q$ 's are univariate polynomials in  $y_1$  or bivariate polynomials in  $y_1, y_2$  over a field  $K$ , can always be found by computing

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

where  $GB$  is the Gröbner basis with respect to the lexical ordering with  $x_1 < x_2 < x_3 < y_1 < y_2$ , if for every  $i, j \in \{1, 2, 3\}$ ,  $i \neq j$ :

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

Since we can always assume that  $p_i$  and  $q_i$  are relatively prime ( $i = 1, 2, 3$ ), the above condition is always satisfied, if the  $p$ 's and  $q$ 's are univariate. Therefore, the above result leads immediately to an implicitization algorithm for arbitrary rational parametric curves.

Furthermore, we present an algorithm for the implicitization of arbitrary rational parametric surfaces and prove its termination and correctness.

In section 2 we state the problems we are concerned with. In section 3 a few theorems are proved which are necessary for showing the correctness of the algorithms, which we present in section 4.

## 2 Problems

Throughout the paper let  $K$  be a field and  $\bar{K}$  the algebraic closure of  $K$ .

Let  $J$  be an ideal and  $g_1, \dots, g_m$  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  $V(\text{Ideal}(\{g_1, \dots, g_m\}))$  we will often write  $V(\{g_1, \dots, g_m\})$ .

Let  $L$  be a field with  $K \subseteq L$ . Then  $(a_1, \dots, a_n) \in L^n$  is a generic zero of  $J$  if for every  $f \in K[x_1, \dots, x_n]$ :

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

Was nimmt man z.B., wenn  $K = \mathbb{Q}$ ?

para-graphs!

2 ganz versch. Bedeutgn!

Nicht notw., weil

$$V(\text{Ideal}(\{g_1, \dots, g_m\})) =$$

$$V(\{g_1, \dots, g_m\})$$

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

In this paper we want to solve the following two problems:

### Implicitization Problem for Rational Parametric Curves:

Given: rational parametrization of a curve

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

where  $p_1, p_2, p_3 \in K[y_1]$ ,  $q_1, q_2, q_3 \in K[y_1] - \{0\}$  and

$p_i$  and  $q_i$  are relatively prime ( $i = 1, 2, 3$ ).

Find: implicit representation of this curve, i.e. polynomials  $g_1, \dots, g_m$  in  $K[x_1, x_2, x_3]$  such that

$$V(\{g_1, \dots, g_m\}) = V(P'),$$

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

$$\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}\right) \in K(y_1)$$

as generic point.

geht das immer?

Erklären, warum das eine "natürliche" Formulierung des "intuit." Problems ist.

### Implicitization Problem for Rational Parametric Surfaces:

Given: rational parametrization

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

where  $p_1, p_2, p_3 \in K[y_1, y_2]$ ,  $q_1, q_2, q_3 \in K[y_1, y_2] - \{0\}$  and

$p_i$  and  $q_i$  are relatively prime ( $i = 1, 2, 3$ ).

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

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

Ist das Def. oder Sak?

(over  $K$ ) is 2. In this case

Find: implicit representation of this surface, i.e. a polynomial  $g$  in  $K[x_1, x_2, x_3]$  such that

$$V(\{g\}) = V(P'),$$

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

$$\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}\right) \in K(y_1, y_2)$$

as generic point.

Ist das sicher immer ein Poly?

Warum  
itdies?

Warum nicht  
"If... then..."

Example 1 <sup>Fr.</sup> If the rational parametrization

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

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.

•  $\sqrt{3}$  Besser  $\square$  \ B box

### 3 Theorems

Throughout the paper let  $p_1, p_2, p_3 \in K[y_1, y_2]$  and  $q_1, q_2, q_3 \in K[y_1, y_2] - \{0\}$  such that

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

Let

$$f_1 := q_1 \cdot x_1 - p_1, \quad f_2 := q_2 \cdot x_2 - p_2, \quad f_3 := q_3 \cdot x_3 - p_3,$$

$$I := \text{Ideal}(\{f_1, f_2, f_3\}) \text{ in } K[x_1, x_2, x_3, y_1, y_2]$$

and  $Q_1, \dots, Q_r$  primary ideals in  $K[x_1, x_2, x_3, y_1, y_2]$  such that

$$I \subseteq Q_1 \cap \dots \cap Q_r$$

is a reduced primary decomposition of  $I$ . Furthermore, let  $P$  be the prime ideal in  $K[x_1, x_2, x_3, y_1, y_2]$  which has

$$\left( \frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}, y_1, y_2 \right) \in K(y_1, y_2)$$

as generic point.

**Theorem 1** There exists an  $i \in \{1, \dots, r\}$  with

$$Q_i = P$$

and for every  $j \in \{1, \dots, r\} - \{i\}$ :

$$Q_j \cap K[y_1, y_2] \neq \{0\}.$$

**Proof:** In this proof we use the following notation:

For a given ideal  $F$  in  $K[x_1, x_2, x_3, y_1, y_2]$  the ideal in  $K(y_1, y_2)[x_1, x_2, x_3]$  generated by  $F$  is denoted by  $F^*$ .

Obviously,

$I^*$  is a zero-dimensional prime ideal.

By [Grö70] p.92, there exists exactly one element  $i$  of  $\{1, \dots, r\}$  with

$$Q_i \cap K[y_1, y_2] = \{0\}.$$

Handwritten notes and diagrams:

- A diagram showing a mapping from  $K[y_1, \dots, y_r]$  to  $K[x_1, x_2, x_3, y_1, y_2]$ .
- Equation:  $g \in K[x_1, x_2, x_3, y_1, y_2]$
- Equation:  $g(\frac{p_1}{q_1}, \dots, \frac{p_r}{q_r}, y_1, y_2) = 0$
- Text: "is prime?"
- Other scribbles and symbols.

Furthermore,

$$I^* = Q_i^*$$

Hence,  $Q_i^*$  is prime and therefore, by [Grö70] p.92,

$Q_i$  is prime.

Warum? [ As the dimension of  $Q_i$  is 2 and

$$\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}, y_1, y_2\right)$$

$$f \in Q_i \Rightarrow \left(\frac{p_i}{q_i}\right) = 0$$

Warum? [ is a zero of  $Q_i$ ,

$$Q_i = P_i \quad \square$$

Warum?  $f \in P$

For the rest of the paper let us assume that

$$Q_i = P_i$$

$$Q_1 = P_1$$

and that  $Q_2, \dots, Q_r$  are ordered in such a way that ~~there exists~~ <sup>for</sup> a  $v \in \{1, \dots, r\}$  such that

$Q_1, \dots, Q_v$  are isolated primary components and

$Q_{v+1}, \dots, Q_r$  are embedded primary components.

It is well-known that [ Obviously,

$$V(I) = V(P_1) \cup \dots \cup V(P_v), \tag{1}$$

where  $P_i$  is the radical of  $Q_i$  for  $i = 1, \dots, v$ .

Let  $R$  be a prime ideal in  $K[x_1, x_2, x_3, y_1, y_2]$ .

We know from [vdW67] p.139 that

[vdW67, p.139].

irgendeine  
Interpretation  $I \subseteq R$   
iff

there exists a  $j \in \{1, \dots, v\}$  with  $P_j \subseteq R$ .

$$I \subseteq P_k \subseteq R \subseteq P_j$$

Hence,

for every  $j \in \{1, \dots, v\}$ :  $I \subseteq R \subseteq P_j$  implies  $R = P_j$ .

By Krull's Primidealkettensatz (see for instance [Grö70] p. 179),

$$\dim(P_j) \geq 2 \quad (j = 1, \dots, v), \tag{2}$$

where  $\dim(P_j)$  denotes the dimension of  $P_j$ .

**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  $\text{zero}(b_1, b_2)$ .

kommt ja schon früher vor:  
in die Notation!

**Example 2** We consider again the parametrization of the unit sphere

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

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

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

schon vorne bei Notation

**Theorem 2** Let  $j \in \{2, \dots, v\}$  and  $(a_1, a_2, a_3, b_1, b_2)$  the generic zero of the prime ideal  $P_j$  in  $K[x_1, x_2, x_3, y_1, y_2]$ . Then

$$b_1, b_2 \in \bar{K} \quad \text{and} \quad \dim(P_j) \leq \text{zero}(b_1, b_2).$$

**Proof:** First of all, we know from Theorem 1 that the transcendence degree of  $K(b_1, b_2)$  is smaller than 2.

Let us assume that the transcendence degree of  $K(b_1, b_2)$  is 1.

Let  $i \in \{1, 2, 3\}$ . From the fact that

$p_i, q_i$  are relatively prime

it follows that

$$\dim(\text{Ideal}(\{p_i, q_i\})) = 0,$$

where  $\text{Ideal}(\{p_i, q_i\})$  is considered as an ideal in  $K[y_1, y_2]$ . Hence,

$(b_1, b_2)$  is not common zero of  $p_i$  and  $q_i$ .

As  $f_i$  is an element of  $P_j$ ,

$a_i$  is algebraically dependent on  $\{b_1, b_2\}$ .

Thus,

$$\dim(P_j) = 1.$$

This is a contradiction to (2).

Therefore,

$$b_1, b_2 \in \bar{K}.$$

If  $(b_1, b_2)$  is no common zero of  $p_i$  and  $q_i$  then

$a_i$  is algebraically dependent on  $\{b_1, b_2\}$ .

Thus, the transcendence degree of  $K(a_1, a_2, a_3, b_1, b_2)$  is less than  $\text{zero}(b_1, b_2)$ . Therefore,

$$\dim(P_j) \leq \text{zero}(b_1, b_2). \quad \bullet$$

Notation einführen?

$\text{Ideal}(\mathbb{F})$   
 $\text{Ideal}_K[y_1, y_2] (\mathbb{F})$

**Theorem 3**

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

*iff*

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

**Proof:** ( $\Rightarrow$ ): If

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

then there exists a  $j \in \{2, \dots, r\}$  with

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

Hence,

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

Then, by definition of  $v$ , there exists a  $k \in \{2, \dots, v\}$  with

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

Therefore,

$$\dim(P_k) \geq 3.$$

By Theorem 2,

$$b_1, b_2 \in \bar{K} \text{ and } \text{zero}(b_1, b_2) = 3,$$

where  $(a_1, a_2, a_3, b_1, b_2)$  is the generic zero of  $P_k$ .

( $\Leftarrow$ ): Let  $(b_1, b_2) \in \bar{K}^2$  such that

$$\text{zero}(b_1, b_2) = 3.$$

The element

$$(x_1, x_2, x_3, b_1, b_2)$$

of  $\bar{K}(x_1, x_2, x_3)^5$  is a common zero of  $f_1, f_2, f_3$  and therefore a zero of every polynomial in  $I$ . Hence,

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

**Theorem 4**

$$V(I) \neq V(P)$$

*implies*

*that there exists a  $(b_1, b_2) \in \bar{K}^2$  with  $\text{zero}(b_1, b_2) \geq 2$ .*

**Proof:** If

$$V(I) \neq V(P)$$

then, by (1),

$$v \geq 2.$$

Let  $(a_1, a_2, a_3, b_1, b_2)$  be the generic zero of  $P_2$ .

By Theorem 2 and (2),

$$(b_1, b_2) \in \bar{K}^2 \text{ and } \text{zero}(b_1, b_2) \geq 2. \quad \bullet$$

## 4 Algorithms

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

$p_i, q_i, p_j, q_j$  have no common zeros

then, by Theorem 4 and the elimination property of Gröbner bases, we can obtain the implicit form of the curve or the surface given by

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

by computing

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

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

Obviously, the equivalent conditions in Theorem 4 are satisfied if a polynomial parametric surface or a rational parametric curve is given:

### Corollary 1

a) (Parametrization by polynomial functions:)

If  $q_1 = q_2 = q_3 = 1$  then  $V(I) = V(P)$ .

b) (Rational parametrization of curves:)

If  $p_1, p_2, p_3, q_1, q_2, q_3 \in K[y_1]$  then  $V(I) = V(P)$ .

Hence, we have solved the implicitization problem for rational parametric curves.

**Example 3** *The implicit equation of the unit sphere cannot be found by computing*

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

Since there exists a  $(b_1, b_2) \in \bar{\mathbb{Q}}^2$  with  $\text{zero}(b_1, b_2) = 3$  (see Example 2), we know from Theorem 3 that

$$\text{Ideal}(\{q_1 \cdot x_1 - p_1, q_2 \cdot x_2 - p_2, q_3 \cdot x_3 - p_3\}) \cap K[x_1, x_2, x_3] = \{0\}$$

and therefore

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

The following algorithm masters such difficulties and solves the implicitization problem for rational parametric surfaces.

**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 let  $p$  be a polynomial 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:**  $p_1, p_2, p_3 \in K[y_1, y_2]$ ,  $q_1, q_2, q_3 \in K[y_1, y_2] - \{0\}$  and

$p_i$  and  $q_i$  are relatively prime ( $i = 1, 2, 3$ ).

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

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

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

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

as generic point and

$$g = 1$$

otherwise.

**for every**  $(i, j) \in \{(1, 2), (1, 3), (2, 3)\}$  **do**

$$G_{(i,j)} := GB(\{f_i, f_j\}) \cap K[x_1, x_2, x_3, y_1]$$

$$F_{(i,j)} := \{h/y_1 \mid h \in G_{(i,j)}\}$$

$$G := GB(F_{(1,2)} \cup F_{(1,3)} \cup F_{(2,3)} \cup \{f_1, f_2, f_3\}) \cap K[x_1, x_2, x_3]$$

$$g := \gcd(G)$$

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

**Example 4** Again we consider the unit sphere given by

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

Using **implicit\_surface** we obtain

$$G_{(1,2)} := \{x_2 + y_1^2 x_2 - x_1 y_1 - y_1^3 x_1\},$$

$$F_{(1,2)} := \{-x_2 + x_1 y_1\},$$

$$G_{(1,3)} := \{x_1^2 + 2x_1^2 y_1^2 - y_1^2 - 1 + y_1^4 x_1^2 + x_3^2 + y_1^2 x_3^2\},$$

$$F_{(1,3)} := \{x_1^2 y_1^2 + x_1^2 - 1 + x_3^2\},$$

$$G_{(2,3)} := \{-x_2^2 - 2y_1^2 x_2^2 + y_1^4 + y_1^2 - y_1^4 x_2^2 - y_1^2 x_3^2 - y_1^4 x_3^2\},$$

$$F_{(2,3)} := \{y_1^2 x_2^2 + x_2^2 - y_1^2 + y_1^2 x_3^2\},$$

$$G := \{x_1^2 + x_2^2 + x_3^2 - 1\},$$

$$g := x_1^2 + x_2^2 + x_3^2 - 1, \text{ the implicit representation of the unit sphere. } \bullet$$

As termination of the algorithm is obvious it remains to prove its correctness.

**Lemma 1** Let  $h \in K[x_1, x_2, x_3]$ ,  $R$  an ideal in  $K[x_1, x_2, x_3]$  with  $\dim(R) < 2$  and  $I := \text{Ideal}(\{h\}) \cap R$ . Let  $\{f_1, \dots, f_m\}$  be a basis of  $R$  and  $\{g_1, \dots, g_n\}$  a basis of  $I$ . Then

- a)  $\gcd(f_1, \dots, f_m) = 1$ ,
- b)  $\gcd(g_1, \dots, g_n) = h$ .

**Proof:**

a) If  $\gcd(f_1, \dots, f_m) \neq 1$  then the two-dimensional ideal generated by  $\gcd(f_1, \dots, f_m)$  is a superideal of  $R$ . This is a contradiction to the fact that the dimension of  $R$  is less than 2.

b) As  $\{g_1, \dots, g_n\} \subseteq \text{Ideal}(\{h\})$ ,

$$h \text{ divides } \gcd(g_1, \dots, g_n).$$

Let us assume that there exists a  $p \in K[x_1, x_2, x_3] - K$  with

$$\gcd(g_1, \dots, g_n) = h \cdot p.$$

As  $\gcd(f_1, \dots, f_m) = 1$  there exists an  $f \in R$  that is not divisible by  $p$ . Hence,

$$h \cdot f \in I \text{ and } h \cdot p \text{ does not divide } h \cdot f.$$

This is a contradiction to  $\gcd(g_1, \dots, g_n) = h \cdot p$ . •

**Proof of correctness:**

Let  $(i, j) \in \{(1, 2), (1, 3), (2, 3)\}$ . If

$$\text{Ideal}(\{f_i, f_j\}) \cap K[x_1, x_2, x_3, y_1] = \{0\}$$

then

$$\gcd(f_i, f_j) \neq 1.$$

As

$$\gcd(f_i, f_j) \text{ divides } p_i \text{ and } \gcd(f_i, f_j) \text{ divides } q_i,$$

this is a contradiction to the fact that  $p_i$  and  $q_i$  are relatively prime. Hence,

$$\text{Ideal}(\{f_i, f_j\}) \cap K[x_1, x_2, x_3, y_1] \neq \{0\}$$

and therefore

$$GB(\{f_i, f_j\}) \cap K[x_1, x_2, x_3, y_1] \not\subseteq \{0\} \text{ and } F_{(i,j)} \not\subseteq \{0\}. \quad (3)$$

Furthermore,

$$F_{(i,j)} \subseteq P$$

and therefore

$$\bar{I} \subseteq P,$$

where

$$\bar{I} := \text{Ideal}(F_{(1,2)} \cup F_{(1,3)} \cup F_{(2,3)} \cup \{f_1, f_2, f_3\}).$$

Let  $\bar{P}$  be a prime ideal in  $K[x_1, x_2, x_3, y_1, y_2]$  with

$$\bar{I} \subseteq \bar{P} \quad \text{and} \quad P \neq \bar{P}$$

and let  $(a_1, a_2, a_3, b_1, b_2)$  be the generic point of  $\bar{P}$ .

*Assumption:*  $\dim(\bar{P}) > 1$ .

Then,

$$P \not\subseteq \bar{P}.$$

As  $I \subseteq \bar{P}$  there exists an  $i \in \{2, \dots, v\}$  with

$$P_i \subseteq \bar{P}.$$

By Theorem 2,

$$b_1, b_2 \in \bar{K}.$$

As  $\dim(\bar{P}) > 1$  there exist  $j, k \in \{1, 2, 3\}$  such that  $j \neq k$  and

$\{a_j, a_k\}$  is algebraically independent over  $K$ .

From (3) we know that there exists a non-zero polynomial

$$f(x_j, x_k, y_1) \in F_{(j,k)}.$$

By definition of  $F_{(j,k)}$ ,

$$f(x_j, x_k, b_1) \neq 0.$$

This is a contradiction to the fact that  $\{a_j, a_k\}$  is algebraically independent over  $K$ .

Thus,  $P$  is the only prime ideal that is a superideal of  $\bar{I}$  and has a dimension greater than 1. Hence,  $\bar{I}$  can be written in the form

$$P \cap R,$$

where  $R$  is an ideal in  $K[x_1, x_2, x_3, y_1, y_2]$  with  $\dim(R) < 2$ . Therefore,

$$\bar{I} \cap K[x_1, x_2, x_3] = (P \cap K[x_1, x_2, x_3]) \cap (R \cap K[x_1, x_2, x_3]) \quad \text{and} \quad \dim(R \cap K[x_1, x_2, x_3]) < 2. \quad (4)$$

It follows from the elimination property of Gröbner bases that

$$G \text{ is a basis of } \bar{I} \cap K[x_1, x_2, x_3], \quad (5)$$

where  $G := GB(F_{(1,2)} \cup F_{(1,3)} \cup F_{(2,3)} \cup \{f_1, f_2, f_3\}) \cap K[x_1, x_2, x_3]$ .

*Case:*

the transcendence degree of  $K(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3})$  is 2.

In this case  $P \cap K[x_1, x_2, x_3]$  is a prime ideal of dimension 2. Thus, there exists a  $p \in K[x_1, x_2, x_3]$  with

$$\text{Ideal}(\{p\}) = P \cap K[x_1, x_2, x_3].$$

By Lemma 1, (4) and (5),

$$\gcd(G) = p.$$

Case:

the transcendence degree of  $K\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}\right)$  is less than 2.

In this case  $\dim(P \cap K[x_1, x_2, x_3])$  is less than 2 and therefore, by Lemma 1, (4) and (5),

$$\gcd(G) = 1. \bullet$$

## 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.
- [Buc87] B. Buchberger. Applications of Gröbner Bases in Non-Linear Computational Geometry. In *Proc. Workshop on Scientific Software*, IMA, Minneapolis, USA, 1987. Springer.
- [Grö70] W. Gröbner. *Algebraische Geometrie II (Algebraic Geometry II) (in German)*. Bibliographisches Institut Mannheim, 1970.
- [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.
- [vdW67] B.L. van der Waerden. *Algebra II (in German)*. Springer, Berlin Heidelberg New York, 1967.