Lieber Bruno,
ich hoffe, Du hast meine e-mail von 12.8. erhalten. Diese 29 Seiten sind der ausgedruckte File, den ich Dir am 12.8. geschickt habe.

Viele Grüße,
~~Michael~~ Kalkbrener

Chapter 1

Implicitization and Birational Projection of Varieties

1.1 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 ([?] or [?]). In 1984 the problem has been solved for rational parametric curves in 2D and rational parametric surfaces in 3D by using resultants (see [?]). Resolvents have been applied ~~to~~ find the implicit representation of rational parametric cubic curves in 3D ([?]). Arnon and Sederberg used Gröbner bases for the implicitization of polynomial parametric varieties of dimension $n-1$ in n-dimensional space ([?]). In 1987 Buchberger generalized their method to the case of polynomial parametric varieties of arbitrary dimension ([?]).

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 space given by parametrizations consisting of homogenous polynomials and proceed as described in [?]. Unfortunately, the introduction of the two homogenizing variables makes the computation of the Gröbner bases much more costly (see computing times in Subsection 4.6).

Given the rational parametrization

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

where $p_1, \ldots, p_n, q_1, \ldots, q_n$ are polynomials in $y_1, \ldots, y_m$ over a field K, 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

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

where z is a new variable and GB is the Gröbner basis with respect to the lexical ordering with $x_1 \prec \ldots \prec x_n \prec y_1 \prec \ldots \prec y_m \prec z$.

Implicitization of varieties in 3D-space is of particular importance for geometric modeling. We have developed algorithms that solve this special problem without introducing additional variables. In this paper the main result concerning the implicitization of varieties in 3D-space is the following: The implicit form of a curve or surface given by the rational parametrization

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

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 $x_1 \prec x_2 \prec x_3 \prec y_1 \prec y_2$, 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.

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.

It is well-known that not every implicitly given variety can be represented by a rational parametrization. But, as a consequence of the Theorem of the Primitive Element, every irreducible d-dimensional variety V in n-dimensional space is - after a suitable linear transformation of coordinates - birationally projectable onto an irreducible d-dimensional variety V' in $d+1$-dimensional space. At least $n-d$ polynomials are required to represent V implicitly, whereas V' can be represented by one irreducible polynomial. Because of this fact many problems arising in geometric modeling can be solved more easily if V is given by this irreducible polynomial and the rational map from V' to V (see [?]). Furthermore, the rational map can be considered as a rational parametrization of a $d+1$-dimensional variety containing V.

Recently in several papers ([?], [?], [?]) this data structure has been proposed to represent curves in 3D-space. Each of the algorithms presented in these papers is restricted to space curves given as the intersection of two surfaces. In this paper we are concerned with the following more general problem.

Given: an irreducible variety V, represented by finitely many polynomials $f_1, \ldots, f_r$ in n variables over a field K of characteristic zero. (In fact we will demand that the polynomials generate a prime ideal). Let d be the dimension of V.

Find: an irreducible polynomial g in $d+1$ variables over K such that after a suitable linear transformation of coordinates the variety V is birationally projectable on the variety V' given by the polynomial g. Furthermore, we compute the rational map from V' to V.

We present an algorithm based on the computation of Gröbner bases ([?], [?], [?]) for solving this problem and prove its termination and correctness. This algorithm consists of three parts. In the first part the dimension d of the variety V and a subset $\{x_{i_1}, \ldots, x_{i_d}\}$ of the set of variables $\{x_1, \ldots, x_n\}$ is computed such that $f_1, \ldots, f_r$ generate a zero-dimensional prime ideal in $K(x_{i_1}, \ldots, x_{i_d})[x_{i_{d+1}}, \ldots, x_{i_n}]$, where $\{x_{i_{d+1}}, \ldots, x_{i_n}\} := \{x_1, \ldots, x_n\} - \{x_{i_1}, \ldots, x_{i_d}\}$. In the second part the variety of this zero-dimensional prime ideal is birationally projected on a zero-dimensional variety in one-dimensional space by using an algorithm that solves the birational projection problem stated above for arbitrary zero-dimensional irreducible varieties. In the third part we show how the above problem can be solved for the variety V in $K[x_1, \ldots, x_n]$ given by $f_1, \ldots, f_r$ if it is solved for the variety of the ideal in $K(x_{i_1}, \ldots, x_{i_d})[x_{i_{d+1}}, \ldots, x_{i_n}]$ generated by the same polynomials $f_1, \ldots, f_r$.

In Section 2 and 3 we give some definitions and state a few well-known theorems and properties of Gröbner bases that we need for proving the correctness of our conversion algorithms. In Subsection 4.1 a more formal specification of the implicitization problem is given. In Subsection 4.2 Buchberger's implicitization algorithm for polynomial parametric varieties is reviewed. In Subsection 4.3 and 4.4 we present our general implicitization algorithms and prove their correctness. In Subsection 4.5 we deal with the implicitization of curves and surfaces in 3D-space. Again, all the proofs of correctness of the algorithms presented in this subsection are given. In Subsection 4.6 some examples are computed and the computing times of the different algorithms are compared. In Subsection 5.1 the birational projection problem is stated more formally. In Subsection 5.2, 5.3, and 5.4 the algorithm that solves this problem is presented together with the proof of its correctness.

1.2 Definitions and Theorems

Throughout the paper let K be a field and $\bar{K}$ an algebraically closed field which has infinite transcendence degree over K (a so-called universal domain).

The usefullness of universal domains is based on the following theorem (see [?], p.158).

Theorem 1 *Let L be a finite extension field of K, i.e. there exist finitely many elements $a_1, \ldots, a_m$ in L with $K(a_1, \ldots, a_m) = L$. Then*

L is isomorphic to a subfield of $\bar{K}$.

Let F be a subset of $K[x_1,\ldots,x_n]$. $Ideal(F)$ denotes the *ideal* generated by F in $K[x_1,\ldots,x_n]$ and $V(F)$ denotes the *variety* of F, i.e. the set

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

Let I be an ideal in $K[x_1,\ldots,x_n]$. The *radical* of I is denoted by $\sqrt{I}$. The element a of $\bar{K}^n$ is a *generic point* of I if for every $f \in K[x_1,\ldots,x_n]$:

$$f \in I \quad \text{iff} \quad f(a) = 0.$$

Theorem 2 *Let P be a proper ideal in $K[x_1,\ldots,x_n]$. Then*

P is prime

iff

P has a generic point in $\bar{K}^n$.

Proof: see [?], p.159 and p.160.

When ideal I is written as a finite intersection of primary ideals in $K[x_1,\ldots,x_n]$, say

$$I = Q_1 \cap \ldots \cap Q_r,$$

we call this a *primary decomposition* of I. A primary decomposition such that $\sqrt{Q_1},\ldots,$ $\sqrt{Q_r}$ are distinct and I cannot be expressed as an intersection of a proper subset of the primary ideals $\{Q_1,\ldots,Q_r\}$ is said to be *reduced.*

Theorem 3 *(Lasker-Noether Decomposition Theorem).*
For every ideal I in $K[x_1,\ldots,x_n]$ there exists a reduced primary decomposition of I.

Proof: see [?], p.136.

Theorem 4 *Let $I = Q_1 \cap \ldots \cap Q_r = R_1 \cap \ldots \cap R_s$ be reduced primary decompositions of I. Then*

$$r = s \text{ and } \{\sqrt{Q_1},\ldots,\sqrt{Q_r}\} = \{\sqrt{R_1},\ldots,\sqrt{R_s}\}.$$

Proof: see [?], p.137.

Theorem 5 *Let $I = Q_1 \cap \ldots \cap Q_r$ be a reduced primary decompositions of I and P a prime ideal in $K[x_1,\ldots,x_n]$. Then*

$$I \subseteq P$$

iff

$$\text{there exists an } i \in \{1,\ldots,r\} \text{ with } \sqrt{Q_i} \subseteq P.$$

Proof: see [?], p.139.

Let $Q_1 \cap \ldots \cap Q_r$ be a reduced primary decomposition of I and let $i \in \{1,\ldots,r\}$. We call Q_i an *embedded primary component* of I if there exists a $j \in \{1,\ldots,r\}$, $i \neq j$ with

$$\sqrt{Q_j} \subseteq \sqrt{Q_i}.$$

Otherwise, Q_i is called an *isolated primary component* of I. If the prime ideal P is an element of the uniquely determined set $\{\sqrt{Q_1},\ldots,\sqrt{Q_r}\}$ then we say that P is *associated* with I.

In ([?], p.161) the following definition of the dimension of an ideal is given:

Let P be a prime ideal in $K[x_1,\ldots,x_n]$ and $(a_1,\ldots,a_n)$ a generic point of P. The *dimension* of P is the transcendence degree of the extension field $K(a_1,\ldots,a_n)$ over K. (The dimension is independent of the choice of a particular generic point.) The *dimension* of the proper ideal I, abbreviated $dim(I)$, is the maximal dimension of its associated prime ideals.

A different but equivalent definition of the dimension of an ideal can be found in ([?], p.38):

Let $\{i_1,\ldots,i_d\}$ be a subset of $\{1,\ldots,n\}$. The set $\{x_{i_1},\ldots,x_{i_d}\}$ is said to be *independent modulo* I if

$$I \cap K[x_{i_1},\ldots,x_{i_d}] = \{0\}.$$

The *dimension* of the proper ideal I is the maximal number of elements in any set of variables independent modulo I.

The ideal I is called *unmixed d-dimensional* if each of its associated prime ideals is of dimension d. The varieties of unmixed 1-dimensional ideals are called *curves*, the varieties of unmixed 2-dimensional ideals are called *surfaces*, and the varieties of unmixed $(n-1)$-dimensional ideals are called *hypersurfaces*.

Theorem 6 *Let I be an ideal in $K[x_1,\ldots,x_n]$. Then*

$$dim(I) = n-1 \text{ and } I \text{ is generated by a single polynomial}$$

$$\textit{iff}$$

$$I \text{ is unmixed } (n-1)\text{-dimensional.}$$

Proof: see [?], p.179.

Theorem 7 *(Primidealkettensatz of Krull).*
Let the ideal I in $K[x_1,\ldots,x_n]$ be generated by $\{g_1,\ldots,g_k\} \subseteq K[x_1,\ldots,x_n]$ and let P' be a prime ideal in $K[x_1,\ldots,x_n]$ such that

$$I \subseteq P' \quad \textit{and} \quad I \subseteq P \subseteq P' \textit{ implies } P = P'$$

for every prime ideal P in $K[x_1,\ldots,x_n]$. Then

$$dim(P') \geq n-k.$$

Proof: see [?], p.142.

Theorem 8 *Let P and P' be prime ideals in $K[x_1,\ldots,x_n]$ with $P \subseteq P'$. Then*

1. *the dimension of P' is less equal the dimension of P,*
2. *if P and P' have the same dimension then $P = P'$.*

Proof: see [?], p.163.

At the end of this section we will show the following easy lemma that we will use in some of the proofs in Section 4.

Lemma 1 *Let b be an element of the algebraic closure of K, p an irreducible polynomial in $K[x_1]$ with $p(b) = 0$ and f a polynomial in $K[x_1,\ldots,x_n]$ with $f(b,x_2,\ldots,x_n) = 0$. Then*

$$p \text{ divides } f.$$

Proof: Let the subset $\{b_2,\ldots,b_n\}$ of $\bar{K}$ be algebraically independent over K and let P be the prime ideal in $K[x_1,\ldots,x_n]$ with $(b,b_2,\ldots,b_n)$ as a generic point. As the transcendence degree of $K(b,b_2,\ldots,b_n)$ is $n-1$,

$$dim(P) = n - 1.$$

Since P is prime and therefore unmixed $(n-1)$-dimensional we obtain from Theorem 6 that P is generated by a single polynomial. As $p \in P$ and p is irreducible,

$$p \text{ generates } P.$$

From $f(b,b_2,\ldots,b_n) = 0$ we obtain $f \in P$. Therefore,

$$p \text{ divides } f. \quad \bullet$$

1.3 Gröbner Bases

Each of the conversion algorithms presented in this chapter is based on the computation of Gröbner bases. In 1965 the method of Gröbner bases has been introduced by B. Buchberger in his Ph.D. thesis (see [?] or [?]). This method, 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 a few properties which we need in the sequel. For a complete reference of the Gröbner bases method see [?] or [?].

Let F be a finite subset of $K[x_1,\ldots,x_n]$. Then $GB(F)$, the reduced Gröbner basis of F with respect to the lexical ordering $\prec$ 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)),
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 $K[x_1,\ldots,x_i]$,
4. $Ideal(F)$ is zero-dimensional iff

   for every $i \in \{1,\ldots,n\}$ there exists an $f \in GB(F)$ such that the leading power product of f with respect to $\prec$ is a power of x_i,
5. for every $f,g \in GB(F)$, $f \neq g$:

   there does not exist a power product in f that is a multiple of the leading power product of g,
6. for every $f \in GB(F)$: the coefficient of the leading power product of f is 1.

1.4 Implicitization of Rational Parametric Varieties

Throughout the section 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

$$(\frac{p_1}{q_1},\ldots,\frac{p_n}{q_n}) \in \bar{K}^n$$

as generic point. (Because of Theorem 1 we can consider $\{y_1,\ldots,y_m\}$ as subset of $\bar{K}$ and therefore

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

as element of $\bar{K}^n$.

1.4.1 The Implicitization Problem

Intuitively, the implicitization problem is the problem of finding a subset F of $K[x_1,\ldots,x_n]$ such that the set represented parametrically by

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

i.e. the set

$$R := \{(\frac{p_1(b)}{q_1(b)},\ldots,\frac{p_n(b)}{q_n(b)}) \mid b \in \bar{K}^m \text{ and } q_i(b) \neq 0 \text{ for } i = 1,\ldots,n\},$$

is implicitly represented as the set of common zeros of F. As it has been pointed out in [?] it is possible that there does not exist a subset F in $K[x_1,\ldots,x_n]$ with

$$V(F) = R,$$

because the parametrization is not "general enough" and therefore some points are missing in R.

Example 1 If

$$p_1 = 2y_2, \qquad p_2 = 2y_1y_2, \qquad p_3 = y_2^2 - y_1^2 - 1, \qquad q_1 = q_2 = q_3 = 1 + y_1^2 + y_2^2$$

Then, for every $(b_1,b_2) \in \bar{K}^2$ with $q_1(b_1,b_2) \neq 0$

$$(\frac{p_1(b_1,b_2)}{q_1(b_1,b_2)}, \frac{p_2(b_1,b_2)}{q_2(b_1,b_2)}, \frac{p_3(b_1,b_2)}{q_3(b_1,b_2)})$$

is a zero of the polynomial

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

and for almost all elements $(a_1,a_2,a_3) \in V(\{x_1^2+x_2^2+x_3^2-1\})$ there exists a $(b_1,b_2) \in \bar{K}^2$ such that

$$(a_1,a_2,a_3) = (\frac{p_1(b_1,b_2)}{q_1(b_1,b_2)}, \frac{p_2(b_1,b_2)}{q_2(b_1,b_2)}, \frac{p_3(b_1,b_2)}{q_3(b_1,b_2)}).$$

But there does not exist a $(b_1,b_2) \in \bar{K}^2$ such that

$$(0,1,0) = (\frac{p_1(b_1,b_2)}{q_1(b_1,b_2)}, \frac{p_2(b_1,b_2)}{q_2(b_1,b_2)}, \frac{p_3(b_1,b_2)}{q_3(b_1,b_2)}),$$

although $(0,1,0) \in V(\{x_1^2 + x_2^2 + x_3^2 - 1\})$. •

Hence, what we really want to find is a finite subset F of $K[x_1,\ldots,x_n]$ such that $V(F)$ is the smallest variety containing R.

Because of Theorem 1, $\{y_1,\ldots,y_m\}$ can be considered as a subset of $\bar{K}$ and therefore

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

can be considered as an element in R. Thus,

$$V(F) \text{ must contain } (\frac{p_1}{q_1},\ldots,\frac{p_n}{q_n}). \tag{1.1}$$

Let f be an element of $K[x_1,\ldots,x_n]$ such that

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

and let $b \in \bar{K}^m$ with

$$q_i(b) \neq 0 \text{ for every } i \in \{1,\ldots,n\}.$$

Obviously,

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

Therefore,

$$(\frac{p_1}{q_1},\ldots,\frac{p_n}{q_n}) \in V(F) \text{ implies } R \subseteq V(F).$$

Thus, $V(P)$ contains R. As $V(P)$ is the smallest variety that contains

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

it follows from (1.1) that $V(P)$ is the smallest variety containing R.

Hence, we can state the implicitization problem in the following way.

Implicitization Problem:

Given: rational parametrization of a variety

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

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

$$(\frac{p_1}{q_1},\ldots,\frac{p_n}{q_n}) \in \bar{K}^n$$

as generic point.

Example 2 For the rational parametrization

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

the implicit representation

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

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

1.4.2 Implicitization of Polynomial Parametric Varieties

If the given rational parametrization

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

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 [?]).

Example 3 For the variety given by the polynomial representation

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

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

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

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 4 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

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

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

1.4.3 Homogenization

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

Example 5 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

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

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

$$(\frac{p_1}{q_1},\ldots,\frac{p_n}{q_n}) \in \bar{K}^n$$

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 I be 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 $f' \in K[x_0, x_1, \ldots, x_n]$ 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

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

As $h_0, \ldots, h_n$ are homogenous polynomials of total degree s,

$$f'(h_0, \ldots, h_n) \text{ is a homogenous polynomial in } K[y_0, y_1, \ldots, y_m]. \tag{1.2}$$

If $f'(h_0(1, y_1, \ldots, y_m), \ldots, h_n(1, y_1, \ldots, y_m)) = 0$ we obtain from Lemma 1 that $y_0 - 1$ divides the polynomial $f'(h_0(y_0, y_1, \ldots, y_m), \ldots, h_n(y_0, y_1, \ldots, y_m))$ in $K[y_0, y_1, \ldots, y_m]$ and therefore, because of (1.2), $f'(h_0, \ldots, h_n) = 0$. 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,

$$f \in P \quad \text{iff} \quad f' \in I. \tag{1.3}$$

Let e be a non-zero polynomial in I and $e_0, \ldots, e_d$ homogenous polynomials in $K[x_0, \ldots, x_n]$ such that for every $i \in \{0, \ldots, d\}$

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

As $e_0(h_0, \ldots, h_n), \ldots, e_d(h_0, \ldots, h_n)$ 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

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

and therefore

$$e_i \in I \quad (i = 0, \ldots, d).$$

By (1.3),

$$e_i(1, x_1, \ldots, x_n) \in P \quad (i = 0, \ldots, d).$$

Hence, for every $(a_1, \ldots, a_n) \in V(P)$

$$e(1, a_1, \ldots, a_n) = e_d(1, a_1, \ldots, a_n) + \ldots + e_0(1, a_1, \ldots, a_n) = 0$$

and therefore

$$(1, a_1, \ldots, a_n) \in V(I).$$

Let $p \in P$. Then there exists a homogenous polynomial p' in $K[x_0, \ldots, x_n]$ with

$$p'(1, x_1, \ldots, x_n) = p(x_1, \ldots, x_n).$$

By (1.3),

$$p' \in I.$$

Hence, for every $(1, a_1, \ldots, a_n) \in V(I)$

$$p(a_1, \ldots, a_n) = 0$$

and therefore

$$(a_1, \ldots, a_n) \in V(P).$$

Thus, we have proved that for every $(a_1, \ldots, a_n) \in \bar{K}^n$

$$(a_1, \ldots, a_n) \in V(P) \quad \text{iff} \quad (1, a_1, \ldots, a_n) \in V(I). \tag{1.4}$$

From the result stated in the previous subsection we obtain that

$$V(I) = V(GB(\{x_0 - h_0, \ldots, x_n - h_n\})) \cap K[x_0, \ldots, x_n] = V(G).$$

Hence, for every $(a_1, \ldots, a_n) \in \bar{K}^n$

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

Together with (1.4),

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

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 Subsection 4.6).
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 [?]).

1.4.4 The Rabinowitsch Trick

Example 6 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 $x_1 \prec x_2 \prec x_3 \prec y_1 \prec y_2 \prec z$. $\bullet$

This strategy always works:

Theorem 9 *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,

$$\{g_1,\ldots,g_r\}\subseteq P. \tag{1.5}$$

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

$$\bar{f}:=(\prod_{i=1}^{n}q_i^{s_i})\cdot f-\sum_{i=1}^{n}(q_i\cdot x_i-p_i)\cdot h_i\in K[y_1,\ldots,y_m]. \tag{1.6}$$

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 (1.6),

$$(\prod_{i=1}^{n}q_i^{s_i})\cdot f=\sum_{i=1}^{n}(q_i\cdot x_i-p_i)\cdot h_i. \tag{1.7}$$

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 Property 2 and 3 in Section 3,

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

Together with (1.5),

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

1.4.5 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 subsections.
Throughout this subsection let us assume that $n = 3$ and $m = 2$, i.e. 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 $(i = 1, 2, 3)$. Furthermore, let

$$I := Ideal(\{q_1 \cdot x_1 - p_1,\ q_2 \cdot x_2 - p_2,\ q_3 \cdot x_3 - p_3\}) \text{ in } K[x_1, x_2, x_3, y_1, y_2],$$

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

$$Q_1 \cap \ldots \cap Q_r$$

is a reduced primary decomposition of I.

Theorem 10 *There exists an $i \in \{1,\ldots,r\}$ such that Q_i is prime and has*

$$(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}, y_1, y_2) \in \bar{K}^5$$

as generic point. Furthermore, for every $j \in \{1,\ldots,r\} - \{i\}$:

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

In the proof of this theorem we will use the following notation:
For a given ideal J 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 J is denoted by J^*.
The proof is based on Theorem 11 which can be found in ([?], p.47 and p.92) in a more general form.

Theorem 11 *Let J be an ideal in $K[x_1, x_2, x_3, y_1, y_2]$ with $J \cap K[y_1, y_2] = \{0\}$ and $R_1, \ldots, R_k$ be primary ideals in $K[x_1, x_2, x_3, y_1, y_2]$ with*

$$J = R_1 \cap \ldots \cap R_k$$

ordered in such a way that there exists an $l \in \{1,\ldots,k\}$ with

$$R_i \cap K[y_1, y_2] = \{0\} \text{ for } i = 1,\ldots,l \quad \text{and} \quad R_i \cap K[y_1, y_2] \neq \{0\} \text{ for } i = l+1,\ldots,k.$$

Then

1. *$J^* = R_1^* \cap \ldots \cap R_l^*$ and R_i^* is primary for every $i \in \{1,\ldots,l\}$,*
2. *if J is primary then $J^* \cap K[x_1, x_2, x_3, y_1, y_2] = J$,*
3. *if J is a prime ideal of dimension 2 then J^* is a zero-dimensional prime ideal.*

Proof of Theorem 10: Let

$$M := \{i \in \{1,\ldots,r\} \mid Q_i \cap K[y_1, y_2] = \{0\}\}.$$

As I^* is generated by $\{q_1 \cdot x_1 - p_1,\ q_2 \cdot x_2 - p_2,\ q_3 \cdot x_3 - p_3\}$,

$$I^* \text{ is a zero-dimensional prime ideal and } I \cap K[y_1, y_2] = \{0\}.$$

Thus,

$$M \neq \emptyset.$$

Furthermore, it follows from Theorem 11.1 that

$$I^* = \bigcap_{i \in M} Q_i^*.$$

As I^* is prime there exists an $i \in M$ with

$$I^* = Q_i^*. \tag{1.8}$$

If there exists another element j in M with $j \neq i$ then

$$Q_i^* \subseteq Q_j^*.$$

From Theorem 11.2 we obtain

$$Q_i \subseteq Q_j.$$

This is a contradiction that to the fact that $Q_1 \cap \ldots \cap Q_r$ is a reduced primary decomposition. Therefore, for every $j \in \{1, \ldots, r\} - \{i\}$

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

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

$$(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}, y_1, y_2) \in \bar{K}^5$$

as generic point. By Theorem 11.3,

$$R^* \text{ is a zero-dimensional prime ideal.}$$

From $I \subseteq R$ we obtain $I^* \subseteq R^*$ and therefore, by Theorem 8 and (1.8),

$$R^* = I^* = Q_i^*.$$

By Theorem 11.2,

$$Q_i = R. \ \bullet$$

For the rest of the subsection let us assume that Q_1 is the prime ideal with

$$(\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}, y_1, y_2) \in \bar{K}^5$$

as generic point and that $Q_2, \ldots, Q_r$ are ordered in such a way that there exists a $v \in \{1, \ldots, r\}$ such that

$$Q_1, \ldots, Q_v \text{ are isolated primary components and}$$

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

Obviously,

$$V(I) = V(P_1) \cup \ldots \cup V(P_v), \tag{1.9}$$

where P_i is the radical of Q_i for $i = 1, \ldots, r$.

Furthermore, the following result holds

Theorem 12 *Let j be an element of $\{1,\ldots,v\}$. Then the dimension of P_j is greater equal 2.*

Proof: Let R be a prime ideal in $K[x_1,x_2,x_3,y_1,y_2]$.
By Theorem 5,

$$I \subseteq R$$

iff

$$\text{there exists a } j \in \{1,\ldots,r\} \text{ with } P_j \subseteq R.$$

Hence,

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

As ideal I is generated by $\{q_1 \cdot x_1 - p_1,\ q_2 \cdot x_2 - p_2,\ q_3 \cdot x_3 - p_3\}$ we obtain the desired result from Krull's Primidealkettensatz. •

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 7 We consider again 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. Then for $(0,0),\ (i,0) \in \bar{\mathbb{Q}}^2$:

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

Theorem 13 *Let $j \in \{2,\ldots,v\}$ and let (a_1,a_2,a_3,b_1,b_2) be the generic zero of the prime ideal P_j in $K[x_1,x_2,x_3,y_1,y_2]$. Then*

$$b_1 \text{ and } b_2 \text{ are in the algebraic closure of } K \text{ and } dim(P_j) \leq zero(b_1,b_2).$$

Proof: First of all, we know from Theorem 10 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 $i \in \{1,2,3\}$. By Theorem 6, every one-dimensional prime ideal in $K[y_1,y_2]$ is generated by a single non-constant polynomial. Since p_i and q_i are relatively prime it follows that no one-dimensional prime ideal is a superideal of $Ideal(\{p_i,q_i\})$, where $Ideal(\{p_i,q_i\})$ is considered as an ideal in $K[y_1,y_2]$. Thus,

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

Hence,

$$(b_1,b_2) \text{ is no common zero of } p_i \text{ and } q_i.$$

As $q_i \cdot x_i - p_i$ is an element of P_j,

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

Thus,

$$dim(P_j) = 1.$$

This is a contradiction to Theorem 12.
Therefore,

$$b_1 \text{ and } b_2 \text{ are in the algebraic closure of } K.$$

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

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

Thus, the transcendence degree of $K(a_1, a_2, a_3, b_1, b_2)$ is less equal $zero(b_1, b_2)$. Therefore, by van der Waerden's definition of dimension,

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

In Example 4 we have shown 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 we use the parametrization of the unique sphere defined by

$$p_1 := 2y_2, \qquad p_2 := 2y_1y_2, \qquad p_3 := y_2^2 - y_1^2 - 1, \qquad q_1 := q_2 := q_3 := 1 + y_1^2 + y_2^2.$$

In Example 7 we have considered the same parametrization and we have found out that there exists an element (b_1, b_2) in $\bar{\mathbb{Q}}^2$ with

$$zero(b_1, b_2) = 3.$$

In the following theorem it is stated that these two facts are equivalent.

Theorem 14

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

$$iff$$

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

Proof: ($\Rightarrow$:) If

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

then there exists a $j \in \{2, \ldots, r\}$ 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 $k \in \{2, \ldots, v\}$ with

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

Therefore, Gröbner's definition of dimension,

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

By Theorem 13 and the definition of *zero*,

$$zero(b_1, b_2) = 3,$$

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

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

$$zero(b_1, b_2) = 3.$$

The element

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

of $\bar{K}^5$ is a common zero of $q_1 \cdot x_1 - p_1$, $q_2 \cdot x_2 - p_2$, $q_3 \cdot x_3 - p_3$ and therefore a zero of every polynomial in I. Hence,

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

Theorem 15

$$V(I) \neq V(P_1)$$

implies

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

Proof: If

$$V(I) \neq V(P_1)$$

then, by (1.9),

$$v \geq 2.$$

Let $(a_1, a_2, a_3, b_1, b_2)$ be the generic point of P_2.
By Theorem 12 and Theorem 13,

$$zero(b_1, b_2) \geq 2. \quad \bullet$$

Note that

$$P_1 \cap K[x_1, x_2, x_3] = P$$

and that, by Property 2 and 3 in Section 3,

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

where GB has to be computed using the lexical ordering determined by $x_1 \prec x_2 \prec x_3 \prec y_1 \prec y_2$. Hence, if for every $(b_1, b_2) \in \bar{K}^2$ $zero(b_1, b_2) < 2$ then, by Theorem 15,

$$V(P) = V(P_1 \cap K[x_1, x_2, x_3]) = V(I \cap K[x_1, x_2, x_3]) =$$

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

Therefore, 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 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

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

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 $i \in \{1,2,3\}$.)

As we have seen this simple algorithm does not work for arbitrary rational parametrizations (see Example 4 or Theorem 14). The implicit representation of surfaces given by arbitrary rational parametrizations can be found by using an algorithm which we will present in the sequel. This algorithm decides whether the variety given by the rational 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 non-zero 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: $p_1, p_2, p_3 \in K[y_1, y_2]$, $q_1, q_2, q_3 \in K[y_1, y_2] - \{0\}$ and

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

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**
$G_{(i,j)} := GB(\{q_i \cdot x_i - p_i,\ q_j \cdot x_j - p_j\}) \cap K[x_1, x_2, x_3, y_1]$
$F_{(i,j)} := \{h_{/y_1} \mid h \in G_{(i,j)}\}$
$G := GB(F_{(1,2)} \cup F_{(1,3)} \cup F_{(2,3)} \cup \{q_1 \cdot x_1 - p_1,\ q_2 \cdot x_2 - p_2,\ q_3 \cdot x_3 - p_3\}) \cap K[x_1, x_2, x_3]$
$g := gcd(G)$

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 8 Again we consider the unit sphere given by

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

Using **implicit_surface** we obtain

$G_{(1,2)} := \{x_2 + y_1^2x_2 - x_1y_1 - y_1^3x_1\}$,
$F_{(1,2)} := \{-x_2 + x_1y_1\}$,
$G_{(1,3)} := \{x_1^2 + 2x_1^2y_1^2 - y_1^2 - 1 + y_1^4x_1^2 + x_3^2 + y_1^2x_3^2\}$,
$F_{(1,3)} := \{x_1^2y_1^2 + x_1^2 - 1 + x_3^2\}$,
$G_{(2,3)} := \{-x_2^2 - 2y_1^2x_2^2 + y_1^4 + y_1^2 - y_1^4x_2^2 - y_1^2x_3^2 - y_1^4x_3^2\}$,
$F_{(2,3)} := \{y_1^2x_2^2 + x_2^2 - y_1^2 + y_1^2x_3^2\}$,
$G := \{x_1^2 + x_2^2 + x_3^2 - 1\}$,
$g := x_1^2 + x_2^2 + x_3^2 - 1$, the implicit representation of the unit sphere. •

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

Lemma 2 *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 $J := Ideal(\{h\}) \cap R$. Let $\{f_1, \ldots, f_k\}$ be a basis of R and $\{g_1, \ldots, g_l\}$ a basis of J. Then*

1. $gcd(f_1, \ldots, f_k) = 1$,
2. $gcd(g_1, \ldots, g_l) = h$.

Proof:
a) If $gcd(f_1, \ldots, f_k) \neq 1$ then, by Gröbner's definition of dimension, the superideal of R generated by $gcd(f_1, \ldots, f_k)$ has dimension 2. Another consequence of Gröbner's definition of dimension is that the dimension of a superideal of R is less equal the dimension of R. Therefore, we have obtained a contradiction to the fact that the dimension of R is less than 2.

b) As $\{g_1, \ldots, g_l\} \subseteq Ideal(\{h\})$,

$$h \text{ divides } gcd(g_1, \ldots, g_l).$$

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

$$gcd(g_1, \ldots, g_l) = h \cdot p.$$

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

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

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

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

$$Ideal(\{q_i \cdot x_i - p_i,\ q_j \cdot x_j - p_j\}) \cap K[x_1, x_2, x_3, y_1] = \{0\}$$

then, by Gröbner's definition of dimension,

$$dim(Ideal(\{q_i \cdot x_i - p_i,\ q_j \cdot x_j - p_j\})) = 4.$$

We obtain from van der Waerden's definition of dimension that there exists an associated prime ideal of $Ideal(\{q_i \cdot x_i - p_i,\ q_j \cdot x_j - p_j\})$ that has dimension 4. By Theorem 6, this prime ideal is generated by a single polynomial. This polynomial is not a constant and divides $q_i \cdot x_i - p_i$ and $q_j \cdot x_j - p_j$. Hence,

$$gcd(q_i \cdot x_i - p_i,\ q_j \cdot x_j - p_j) \neq 1.$$

The polynomial $gcd(q_i \cdot x_i - p_i,\ q_j \cdot x_j - p_j)$ is an element of $K[y_1, y_2] - K$. Therefore,

$$gcd(q_i \cdot x_i - p_i,\ q_j \cdot x_j - p_j) \text{ divides } p_i \text{ and } gcd(q_i \cdot x_i - p_i,\ q_j \cdot x_j - p_j) \text{ divides } q_i.$$

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

$$Ideal(\{q_i \cdot x_i - p_i,\ q_j \cdot x_j - p_j\}) \cap K[x_1, x_2, x_3, y_1] \neq \{0\}$$

and therefore

$$GB(\{q_i \cdot x_i - p_i,\ q_j \cdot x_j - p_j\}) \cap K[x_1, x_2, x_3, y_1] \not\subseteq \{0\} \text{ and } F_{(i,j)} \not\subseteq \{0\}. \tag{1.10}$$

Let $f \in F_{(i,j)}$. Then there exists a non-zero $p \in K[y_1]$ with

$$f \cdot p \in GB(\{q_i \cdot x_i - p_i,\ q_j \cdot x_j - p_j\}) \cap K[x_1, x_2, x_3, y_1]$$

and therefore

$$f \cdot p \in P_1.$$

As P_1 is prime and $P_1 \cap K[y_1] = \{0\}$,

$$f \in P_1.$$

Thus,

$$F_{(i,j)} \subseteq P_1$$

and therefore

$$\bar{I} \subseteq P_1,$$

where

$$\bar{I} := Ideal(F_{(1,2)} \cup F_{(1,3)} \cup F_{(2,3)} \cup \{q_1 \cdot x_1 - p_1,\ q_2 \cdot x_2 - p_2,\ q_3 \cdot x_3 - p_3\}).$$

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

$$\bar{I} \subseteq \bar{P} \quad \text{and} \quad P_1 \neq \bar{P}$$

and let $(a_1, a_2, a_3, b_1, b_2)$ be a generic point of $\bar{P}$.
Assumption: $dim(\bar{P}) > 1$.
Then, by Theorem 8,

$$P_1 \not\subseteq \bar{P}.$$

As $I \subseteq \bar{P}$ we know from Theorem 5 that there exists an $i \in \{2, \ldots, v\}$ with

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

By Theorem 13, there exist non-zero polynomials in $P_i \cap K[y_1]$ and $P_i \cap K[y_2]$ and therefore

$$b_1 \text{ and } b_2 \text{ are in the algebraic closure of } K.$$

As $dim(\bar{P}) > 1$ it follows from van der Waerden's definition of dimension that there exist $j, k \in \{1, 2, 3\}$ such that $j \neq k$ and

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

From (1.10) we know that there exists a non-zero polynomial

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

As $f(x_j, x_k, y_1)$ has no non-trivial factor in $K[y_1]$ it follows from Lemma 1 that

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

This is a contradiction to the fact that $\{a_j, a_k\}$ is algebraically independent over K.
Thus, P_1 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

$$Q \cap R,$$

where Q is a primary ideal with $\sqrt{Q} = P_1$ and R is an ideal in $K[x_1, x_2, x_3, y_1, y_2]$ with $dim(R) < 2$. Therefore,

$$\bar{I} \cap K[x_1, x_2, x_3] = (Q \cap K[x_1, x_2, x_3]) \cap (R \cap K[x_1, x_2, x_3]) \tag{1.11}$$

and, by Gröbner's definition of dimension,

$$dim(R \cap K[x_1, x_2, x_3]) < 2. \tag{1.12}$$

It follows from Property 2 and 3 in Section 3 that

$$G \text{ is a basis of } \bar{I} \cap K[x_1, x_2, x_3]. \tag{1.13}$$

Case:

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

Obviously, $Q \cap K[x_1, x_2, x_3]$ is a primary ideal and P is the radical of $Q \cap K[x_1, x_2, x_3]$, because $P = P_1 \cap K[x_1, x_2, x_3]$. Therefore, in this case the dimension of $Q \cap K[x_1, x_2, x_3]$ is 2. Thus, by Theorem 6, there exists a $p \in K[x_1, x_2, x_3]$ with

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

Because of this, (1.11), (1.12), and (1.13) we can apply Lemma 2.2 and obtain

$$gcd(G) = p.$$

Thus,

$$V(\{gcd(G)\}) = V(Q \cap K[x_1, x_2, x_3]) = V(P).$$

Case:

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

In this case $dim(Q \cap K[x_1, x_2, x_3])$ is less than 2 and therefore we obtain from (1.11) and (1.12) that

$$dim(\bar{I} \cap K[x_1, x_2, x_3]) < 2.$$

By (1.13) and Lemma 2.1,

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

1.4.6 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: (*Cylinder*)

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:

$$1 + 6x_4x_1^2x_2 - 2x_1^3x_3x_2 + 15x_2^4 - 6x_4x_1^2x_2^2 - 6x_2 + 2x_1^2 - 2x_4x_1^2 + 15x_2^2 - 6x_2x_1^2 + 6x_2^2x_1^2 - x_1^3 + x_1^4 - 6x_2^5 + x_2^2x_1^3x_3 - x_2^2x_1^3 - 2x_1^2x_2^3 + x_4^2x_1^4 + 2x_1^2x_2^3x_4 + x_2^6 - 20x_2^3 - 2x_4x_1^4 + x_1^3x_3 + 2x_2x_1^3.$$

Example 6:

Parametric Representation:

$$x_1 = y_1y_2, \qquad x_2 = \frac{y_2}{y_1}, \qquad x_3 = \frac{1}{y_1 - y_2}, \qquad x_4 = y_2^2 - y_1.$$

Implicit Representation:

$$1 - x_2x_1x_3 + x_3x_4 + x_1x_3^2 - x_2x_1x_3^2,$$
$$x_1x_3 - x_2^2x_1 - x_2x_1x_3 + x_2x_4,$$
$$x_1x_3^2 - 2x_2x_1x_3^2 - x_2 + x_2^2x_1x_3^2.$$

Example 7:

Parametric Representation:

$$x_1 = \frac{y_1}{y_3}, \qquad x_2 = y_1y_2, \qquad x_3 = \frac{1}{y_1 - y_2}, \qquad x_4 = \frac{y_3 - y_1}{y_3}, \qquad x_5 = y_1^2.$$

Implicit Representation:

$$-x_5 + x_3^2x_2^2 - 2x_3^2x_2x_5 + x_5^2x_3^2,$$
$$-1 + x_1 + x_4.$$

Computing times

We have compared the computing times of the algorithm **proj_implicitization** based on homogenization (Subsection 4.3), the algorithm based on the Rabinowitsch trick (Subsection 4.4) and the algorithm **implicit_surface** that computes the implicit representation of a surface in 3D-space (Subsection 4.5). 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 15 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.

1.5 Birational Projections of Irreducible Varieties

1.5.1 The Problem

Throughout the section let us assume that K is a field of characteristic 0.

Let P be a prime ideal in $K[x_1, \ldots, x_n]$ with generic point $(a_1, \ldots, a_n)$ and R a prime ideal in $K[x_1, \ldots, x_m]$ with generic point $(b_1, \ldots, b_m)$. The varieties $V(P)$ and $V(R)$ are said to be *birationally equivalent* if

$$K(a_1, \ldots, a_n) = K(b_1, \ldots, b_m).$$

In this case there exist $v_1, \ldots, v_m \in K(x_1, \ldots, x_n)$ and $w_1, \ldots, w_n \in K(x_1, \ldots, x_m)$ such that for every $i \in \{1, \ldots, m\}$ and every $j \in \{1, \ldots, n\}$

$$b_i = v_i(a_1, \ldots, a_n) \quad \text{and} \quad a_j = w_j(b_1, \ldots, b_m).$$

The functions $(v_1, \ldots, v_n)$ and $(w_1, \ldots, w_m)$ induce a one-to-one correspondence between "almost all" points of these varieties. If

$$n \geq m \text{ and } v_i = x_i \text{ for every } i \in \{1, \ldots, m\}$$

then we say that $V(P)$ is *birationally projectable* on $V(R)$.

In this section we will show how the following problem can be solved by using Gröbner bases:

Birational Projection Problem:

Given: $\{f_1, \ldots, f_r\} \subseteq K[x_1, \ldots, x_n]$ such that the ideal P generated by $\{f_1, \ldots, f_r\}$ is prime. Let d be the dimension of P.

Find: $g \in K[x_1, \ldots, x_{d+1}]$ such that after a suitable linear transformation of coordinates $V(\{f_1, \ldots, f_r\})$ is birationally projectable on $V(\{g\})$,
$(w_1, \ldots, w_n) \in K(x_1, \ldots, x_{d+1})^n$, the inverse map.

1.5.2 Computation of a Maximal Set of Independent Variables Modulo an Ideal

Based on Gröbner's definition of dimension and on Property 2 and 3 of Gröbner bases stated in Section 3 an algorithm **dim** can be constructed (see [?], [?], [?]) that satisfies the following specification.

dim (in: $\{f_1, \ldots, f_r\}$; out: $\{i_1, \ldots, i_d\}$)