4 Application: Intersection of Superellipsoids

Superellipsoids (Barr 1981) are surfaces in 3D space that have a compact implicit representation as the set of points (x, y, z) such that

$$((\frac{x}{a})^{2/\epsilon_3} + (\frac{y}{b})^{2/\epsilon_2})^{\epsilon_3/\epsilon_1} + (\frac{z}{c})^{2/\epsilon_1} - 1 = 0$$

Superellipsoids are topologically equivalent to spheres. They can be considered as ellipsoids with axes a, b, c whose curvature in the $x-, y-, z-$ directions is distorted by the influence of the exponents $\epsilon_1, \epsilon_2, \epsilon_3$. (The above equation is the implicit equation for the case where the superellipsoid is in standard position with its midpoint at the origin.) The exponents $\epsilon_1, \epsilon_2, \epsilon_3$ open an enormous flexibility for adjusting the shape of superellipsoids in order to approximate real objects. Some basic problems in geometric modeling, for example, the problem of deciding whether a point is inside or outside an object can be easily solved for superellipsoids. Recently, superellipsoids have been proposed for approximating parts of robots and obstacles in order to test for collision. The collision detection problem of robots is thereby reduced to an intersection test for superellipsoids.

Unfortunately, for general superellipsoids, no good intersection tests are known. In this section we report on first attempts to apply Gröbner bases for this question. We restrict our attention to the case of a sphere (with midpoint (A, B, C) and radius R) and a superellipsoid (in standard position) whose exponents satisfy $\epsilon_1 = \epsilon_2 = \epsilon_3 < 2$ (a convex superellipsoid). In this case, the two objects intersect iff the minimal distance between the midpoint of the sphere and the superellipsoid is less or equal to the radius of the sphere. Using Lagrange factors, this approach leads to the following system of equations for the coordinates (x, y, z) of the point on the superellipsoid having minimal distance to (A, B, C):

(Equations for Minimal Distance)

$$(\tfrac{x}{a})^{2/\epsilon} + (\tfrac{y}{b})^{2/\epsilon} + (\tfrac{z}{c})^{2/\epsilon} - 1 = 0$$
$$(x - A) + \lambda.\tfrac{1}{\epsilon.a}.(\tfrac{x}{a})^{(2/\epsilon-1)} = 0$$
$$(y - B) + \lambda.\tfrac{1}{\epsilon.b}.(\tfrac{y}{b})^{(2/\epsilon-1)} = 0$$
$$(z - C) + \lambda.\tfrac{1}{\epsilon.c}.(\tfrac{z}{c})^{(2/\epsilon-1)} = 0$$

If ϵ is of the form $1/k$ (which is sufficiently general for practical purposes), this (System for Minimal Distance) is an algebraic system. We consider a, b, c, A, B, C as parameters, i. e. we work over $K(a, b, c, A, B, C)[x, y, z, \lambda]$. For computing the Gröbner bases, we use the lexical ordering defined by $x \prec y \prec z \prec \lambda$. For $\epsilon = 1$ (which is, actually, the ellipsoid case) we get the Gröbner basis

(Gröbner Basis for Minimal Distance)

$$x^6 - p(x) = 0$$
$$y - q(x) = 0$$
$$z - r(x) = 0$$
$$\lambda - s(x) = 0.$$

Here, $p(x), q(x), r(x), s(x)$ are univariate polynomials in x of degree 5 with coefficients that are rational expressions in the parameters a, b, c, A, B, C. The equation

for λ is not interesting for the problem at hand and may be dropped. The printout of these rational expressions consumes approximately 2 pages. (Some simplification by extracting common subexpressions would be possible.) Again, the Gröbner basis has all the advantageous features described in the inverse kinematics application. Note in particular that, in this Gröbner basis, the second, third and fourth equations are linear in the variables y, z, λ, respectively. Therefore the Gröbner basis presents an explicit symbolic solution to the problem as soon as the solution value for x is numerically determined from the first equation, which is univariate in x.

If we change ϵ to $1/2$, the resulting Gröbner basis will again have the structure displayed in (Gröbner Basis for Minimal Distance). The only difference is that the degree of the univariate polynomials $p(x), q(x), r(x), s(x)$ will be 11. We conjecture that the structure of the system will stay unchanged for arbitrary ϵ of the form $1/k$.

The problem with this approach is, again, computation time. While the Gröbner basis computation for $\epsilon = 1$ needs 15 minutes (on an IBM 4341 in the SAC-2 implementation of the Gröbner bases method), the computation already needs 19 hours for $\epsilon = 1/2$. At the moment, this excludes practical applicability of the method. However, one should take into account that the source of complexity seems to be the extraneous extremal solutions that enter through the Lagrange factor method. Actually, the first equation in the Gröbner basis describes the x-coordinate of all relative extremal points on the surface and not only the x-coordinates of the minimal point. This raises the degree of the first polynomial and, hence, also of the other polynomials. More systematic study is necessary. Furthermore, it seems to be possible to guess and subsequently prove the general structure of the polynomials $p(x), q(x), r(x), s(x)$ from the Gröbner bases computations for two or three different ϵ values. This could make the Gröbner basis computation superfluous in the future. As with other symbolic computation methods, Gröbner bases computations can be applied on very different levels including the level of producing and supporting mathematical conjectures.

5 Application: Implicitization of Parametric Objects

As has been pointed out repeatedly, the automatic transition between implicit and parametric representation of curves and surfaces is of fundamental importance in geometric modeling, see for example (Sederberg, Anderson 1984). The reason for this is that the implicit and the parametric representation are appropriate for different classes of problems. For example, for generating points along curves or surfaces, the parametric representation is most convenient whereas, for deciding whether a given point lies on a specific curve or surface, the implicit representation is most natural. It is also well known that implicitization of parametric surfaces is of importance for deriving a representation of the intersection curve of two surfaces. This problem has a satisfactory solution in case one of the surfaces is expressed parametrically and the other implicitly. In this case, the parameter representation $x(s,t), y(s,t), z(s,t)$ for the first surface can be substituted into the implicit equation $f(x,y,z)$ of the other surface. This results in the implicit representation $f(x(s,t), y(s,t), z(s,t))$ of the intersection curve in parameter space.

Actually, for some time, the problem of implicitization has been deemed unsolvable in the CAD literature. (Sederberg, Anderson 1984), however, presented a solution of the implicitization problem using resultants. The solution is spelled out for surfaces in 3D and curves in 2D. In the general case of $(n-1)$-dimensional hypersurfaces, I guess, the method could yield implicit equations that introduce non-trivial extraneous solutions, see also the remarks in (Arnon, Sederberg 1984). In (Arnon, Sederberg 1984) it is shown how Gröbner bases can be used for the general implicitization problem of $(n-1)$-dimensional hypersurfaces. The authors sketch a correctness proof for the method that relies on (Algebraic Relations). In this section, we review their method and generalize it to the most general case of hypersurfaces of arbitrary dimension in n-dimensional space. Still, much research will be needed to assess the efficiencies of the methods and to determine their range of practical applicability. Also some theoretical details are not yet completely covered in the literature.

(General Implicitization Problem)
Given: $p_1, \ldots, p_m \in K[x_1, \ldots, x_n]$.
Find: $f_1, \ldots, f_k \in K[y_1, \ldots, y_m]$,
such that for all $a_1, \ldots, a_m$:
$f_1(a_1, \ldots, a_m) = \cdots = f_k(a_1, \ldots, a_m) = 0$ iff
$a_1 = p_1(b_1, \ldots, b_n), \ldots, a_m = p_m(b_1, \ldots, b_n)$ for some $b_1, \ldots, b_n$.

The problem requires to construct k polynomials implicitly defining hypersurfaces whose intersection is the hypersurface described by the parameter representation.

(Implicitization Algorithm)
$\{f_1, \ldots, f_k\} := \mathrm{GB}(\{y_1 - p_1, \ldots, y_m - p_m\}) \cap K[y_1, \ldots, y_m]$,
where GB has to be computed using the lexical ordering determined by
$y_1 \prec \cdots \prec y_m \prec x_1 \prec \cdots \prec x_n$.

Correctness Proof: Let $g_1 \prec \ldots \prec g_l$ be the polynomials in

$$\mathrm{GB}(\{y_1 - p_1, \ldots, y_m - p_m\}) - K[y_1, \ldots, y_m].$$

$\{y_1 - p_1, \ldots, y_m - p_m\}$ and the Gröbner basis $\{f_1, \ldots, f_k, g_1, \ldots, g_l\}$ have the same common zeros. If

$$f_1(a_1, \ldots, a_m) = \cdots = f_k(a_1, \ldots, a_m) = 0$$

then, by (Continuation of Partial Solutions), there exist $(b_1, \ldots, b_n)$ such that

$$g_1(a_1, \ldots, a_m, b_1, \ldots, b_n) = \cdots = g_l(a_1, \ldots, a_m, b_1, \ldots, b_n) = 0.$$

Hence, also

$$a_1 - p_1(b_1, \ldots, b_n) = 0, \ldots, a_1 - p_1(b_1, \ldots, b_n) = 0.$$

The converse is clear.

Example: Let us consider the 3D surface defined by the following parametric representation

(Parametric Representation)

$x = r.t$

$y = r.t^2$

$z = r^2$

Roughly, this surface has the shape of a ship hull whose keel is the y-axis and whose bug is the z-axis. Applying algorithm GB to $\{x - r.t, y - r.t^2, z - r^2\}$ with respect to the ordering $z \prec y \prec x \prec t \prec r$ yields the following Gröbner basis:

(Gröbner Basis)

$x^4 - y^2.z$

$t.x - y$

$t.y.z - x^3$

$t^2.z - x^2$

$r.y - x^2$

$r.x - t.z$

$r.t - x$

$r^2 - z$

The polynomial depending only on x, y, z is an implicit equation for the surface defined by (Parameter Representation).

By close inspection one will detect that, actually, the implicit equation occurring in the above (Gröbner Basis) does not strictly meet the specification of the (Implicitization Problem). The y-axis is a solution to the implicit equation whereas it does not appear in the surface defined by the (Parameter Representation). This is not a deficiency of the Gröbner basis method but has to do with the particular (Parameter Representation) which, in some sense, is not "general enough" or, stated differently, in the (Continuation of Partial Solutions) property, solutions at infinity have to be taken into account. This question deserves some further detailed study. (Sturmfels 1987) has already sketched some analysis of this phenomenon. He proposes the following parameter presentation, which includes the y-axis and whose implicit equation is again $x^4 - y^2.z$.

(Parametric Representation)

$x = u.v$

$y = v^2$

$z = u^4$

This example was computed in 4 sec on an IBM AT in the author's research implementation of the Gröbner basis method in the muMATH system. Other examples with more complicated coefficients and similar degree characteristics had computing times in the range of several seconds. I guess that the examples occuring in practice should be well tractible by the method.

Example: The method can also be used for rational parametric representations. We consider the example of a circle in the plane.

(Rational Parametric Representation)

$x = \frac{1-s^2}{1+s^2}$

$y = \frac{2.s}{1+s^2}$

In the case of rational parametric representations, we first clear denominators. In the example, the input to GB should therefore be $\{x+x.s^2-1+s^2, y+y.s^2-2.s\}$. The result is, of course, x^2+y^2-1.

6 Application: Inversion of Parametric Representations

The inversion problem for parametric representations is defined as follows:

(Inversion Problem for Parametric Representations)

Given: $p_1, \ldots, p_m \in K[x_1, \ldots, x_n]$ and
a point $(a_1, \ldots, a_m)$ on the hypersurface
parametrically defined by $p_1, \ldots, p_m$.

Find: $\{(b_1, \ldots, b_n) \mid a_1 = p_1(b_1, \ldots, b_n), \ldots, a_m = p_m(b_1, \ldots, b_n)\}$.

This problem is closely connected with the (Implicitization Problem). In fact, the (Inversion Problem) is just a special case of the general problem of solving systems of polynomial equations, which is completely solved by the Gröbner basis method based on the (Elimination Ideals) property or based on the (Minimal Polynomial) property. For solving the (Inversion Problem), the general Gröbner bases solution method can be applied to the system $\{y_1 - p_1(x_1, \ldots, x_n), \ldots, y_m - p_m(x_1, \ldots, x_n)\}$, i. e. we have the following algorithm.

(Inversion Algorithm for Parametric Representations)

$G := \mathrm{GB}(\{y_1 - p_1(x_1, \ldots, x_n), \ldots, y_m - p_m(x_1, \ldots, x_n)\}$,
where GB has to be computed using the lexical ordering determined by
$y_1 \prec \cdots \prec y_m \prec x_1 \prec \cdots \prec x_n$.

$\{f_1, \ldots, f_k\} := G \cap K[y_1, \ldots, y_m]$.

(If, for some $1 \leq i \leq k$, $f_i(a_1, \ldots, a_m) \neq 0$, then "Input Error".)

Substitute a_i for y_i in G and solve the system G, which is "triangularized".

In fact, the steps necessary in this algorithm include the steps of the (Implicitization Algorithm). Therefore, when we apply the Gröbner bases method to the (Implicitization Problem), we automatically get also a solution for the (Inversion Problem) and vice versa.

Example: We use again the example of Section 5.

(Parametric Representation)

$x = r.t$

$y = r.t^2$

$z = r^2$

Suppose we want to determine the parameter values defining the point $(2, 2, 4)$ on the surface. Application of GB yields

(Gröbner Basis)

$x^4 - y^2.z$

$t.x - y$

$t.y.z - x^3$

$t^2.z - x^2$

$r.y - x^2$

$r.x - t.z$

$rt - x$

$r^2 - z$

The first polynomial is the implicit equation, which can be used to check whether $(2, 2, 4)$ is, in fact, on the surface: $2^4 - 2^2.4 = 0$. Substituting $(2, 2, 4)$ in the second, third, and fourth polynomial of the Gröbner basis (and making all polynomials monic) yields the system

(Gröbner Basis After First Substitution)

$t - 1$

$t - 1$

$t^2 - 1$

This system of univariate polynomials, by the property (Continuation of Partial Solutions) must always have a common zero that can be determined by forming the greatest common divisor, $g := t - 1$, of the three polynomials and solving for t. This leads to $t = 1$.

Substituting $(2, 2, 4, 1)$ in the fifth, ...,eights polynomial of the Gröbner basis (and making all polynomials monic) yields the system

$r - 2$

$r - 2$

$r - 2$

$r^2 - 4$

Again, this system of univariate polynomials, by the property (Continuation of Partial Solutions) must have a common zero that can be determined by forming the greatest common divisor, $h := r - 2$, of the four polynomials and solving for r. This leads to $r = 2$.

Actually, it has been shown recently in (Kalkbrener 1987) and, independently, in (Gianni 1987) that the computation of greatest common divisors is not necessary in the above procedure. Rather, as can be verified in the above example, for each of the univariate systems the first non-zero polynomial will always be the greatest common divisor of the system. This is a drastic simplification of the general procedure for solving arbitrary systems of polynomial equations by the Gröbner bases method.

7 Application: Detection of Singularities

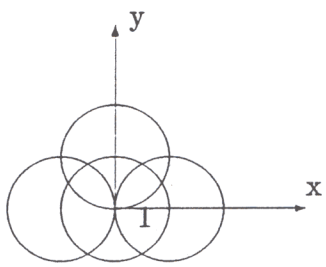
In tracing implicitly given planar curves, numerical methods work well except when tracing curves through singular points, see (Hofmann 1987). (Hofmann 1987a) has pointed out that Göbner bases yield an immediate approach to detect all singular

points of implicitly given planar curves. The singular points of a planar curve given by $f(x,y) = 0$ are exactly the points (a,b) that are common zeros of f, f_x, and f_y. Hence, the problem of determining the set S of singular points of a planar curve f can be treated by the following algorithm.

(Algorithm for Detection of Singularities)

> $G :=$ GB$(\{f, f_x, f_y\})$, where f_x, f_y are the partial derivatives of f w. r. t. x and y respectively and GB has to be computed w. r. t. a lexical ordering of x, y.
>
> $S :=$ set of common zeros of G determined by the successive substitution method.

Example: Let us consider the following planar curve



This curve has 9 singular points. We detect them by applying GB to $\{f, f_x, f_y\}$, where

(Four Circle Curve)

$f := (x^2 + y^2 - 1).((x-1)^2 + y^2 - 1)((x+1)^2 + y^2 - 1)(x^2 + (y-1)^2 - 1).$

Application of GB, using the lexical ordering determined by $x \succ y$, yields

(Gröbner Basis for Four Circle Curve)

$y^5.p(y)$,
$x.y.p(y)$,
$x^2 - y^4.q(y)$,
where $p(y) := y^4 - \frac{3}{2}y^3 - \frac{1}{4}y^2 - \frac{9}{8}y - \frac{3}{8}$,
$q(y) := \frac{2558}{27}y^4 - \frac{823}{9}y^3 - \frac{3895}{54}y^2 + \frac{823}{12}y + \frac{5}{4}$.

One sees that, for any solution y of the first polynomial in the Gröbner basis, the second polynomial vanishes identically whereas the third equation yields at most two different values for x. Proceeding by the general substitution method for Gröbner bases, we obtain the following singular points:

$(-1,1),(1,1)$,
$(-1/2,\sqrt{3}/2),(1/2,\sqrt{3}/2)$,
$(-\sqrt{3}/2,1/2),(\sqrt{3}/2,1/2)$,
$(0,0)$,
$(-1/2,-\sqrt{3}/2),(1/2,-\sqrt{3}/2)$,

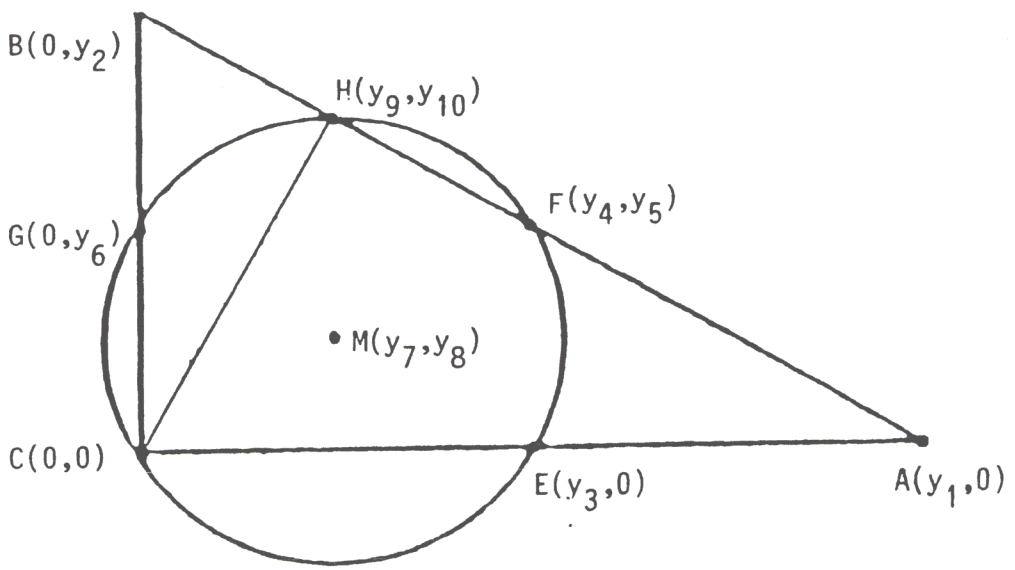
In accordance with the picture, we obtained five different values for y and, altogether, nine singular points. The computation took 78 sec in the author's muMATH Gröbner bases package on an Apollo workstation emulation of an IBM AT.

8 Application: Geometrical Theorem Proving

Automated Geometrical Theorem Proving is intriguing in two ways. First, it is a playground for developing and studying new algorithmic techniques for automated mathematics and, second, it becomes more and more important for advanced geometric modeling, which requires to check plausibility and consistency of inaccurate and numerically distorted geometrical objects and to derive and restore their consistent shape, see for example (Kapur 1987). Apart from older approaches to geometrical theorem proving based on heuristics, recently there have been developed three systematic approaches based on three different algorithmic methods in computer algebra, namely Collins' cylindrical algebraic decomposition method (Collins 1975), Wu's method of characteristic sets (Wu 1978) and the Gröbner basis method. (Kutzler 1987) compares the three methods. The use of Gröbner bases for automated geometrical theorem proving has been independently introduced by B. Kutzler and D. Kapur, see for example (Kutzler, Stifter 1986) and (Kapur 1986). In this section we give an outline of the main idea how Gröbner bases can be used for proving geometrical theorems. We start with an example of a geometrical theorem. For simplicity, we present Kapur's approach, Kutzler's approach is slightly different.

Example: Apollonios' Circle Theorem.

The altitude pedal of the hypotenuse of a right-angled triangle and the midpoints of the three sides of the triangle lie on a circle.



After introducing coordinates, a possible algebraic formulation of this problem is as follows:

(Hypotheses)

$h_1 :=$	$2y_3 - y_1 = 0$	(E is midpoint of CA),
$h_2 :=$	$2y_4 - y_1 = 0$	(F is midpoint of AB, 1st coordinate),
$h_3 :=$	$2y_5 - y_2 = 0$	(F is midpoint of AB, 2nd coordinate),
$h_4 :=$	$2y_6 - y_2$	(G is midpoint of BC),
$h_5 :=$	$(y_7 - y_3)^2 + y_8^2 - (y_7 - y_4)^2 -$ $-(y_8 - y_5)^2 = 0$	(length EM = length FM),
$h_6 :=$	$(y_7 - y_3)^2 + y_8^2 - (y_8 - y_6)^2 -$ $-y_7^2 = 0$	(length EM = length GM),
$h_7 :=$	$(y_9 - y_1)y_2 + y_1 y_{10} = 0$	(H lies on AB),
$h_8 :=$	$-y_1 y_9 + y_2 y_{10} = 0$	(CH is perpendicular to AB).

(Conclusion)

$c :=$	$(y_7 - y_3)^2 + y_8^2 - (y_7 - y_9)^2 -$ $-(y_8 - y_{10})^2 = 0$	(length EM = length HM).

To prove the theorem means to show that

for all $a_1, \ldots, a_{10} \in \mathbf{R}$:
if $h_1(a_1, \ldots, a_{10}) = 0, \ldots, h_8(a_1, \ldots, a_{10}) = 0$,
then $c(a_1, \ldots, a_{10}) = 0$.

All expressions h_i and c occurring in this proposition are polynomial expressions. If one replaces $\mathbf{R}$ by $\mathbf{C}$, the proposition, by definition, is just the proposition "$c \in$ Radical($\{h_1, \ldots, h_8\}$)". However, by (Radical Membership), arbitrary radical membership questions "$c \in$ Radical($\{h_1, \ldots, h_m\}$)?" can be decided by deciding "$1 \in$ GB($\{h_1, \ldots, h_m, z.c - 1\}$)?", where z must be a new indeterminate.

This method is totally general and automatic for all geometrical theorems whose hypothesis and conclusions are polynomial equations. In fact, it is also efficient. Hundreds of non-trivial theorems have been proven by this approach, most of them in only several seconds of computing time, see (Kutzler, Stifter 1986), (Kapur 1986) and (Kutzler 1987) for extensive statistics.

Two remarks are appropriate. First, replacing $\mathbf{R}$ by $\mathbf{C}$ slightly distorts the problem. Of course, if a geometrical theorem holds over $\mathbf{C}$ then it also holds over $\mathbf{R}$. The reverse is not true in general. It turns out, however, that the geometrical theorems occuring in the mathematical literature are generally true over $\mathbf{C}$. Still, one must bear in mind that, if a negative answer is produced by this method for a given proposition, this does not necessarily mean that the proposition is false over $\mathbf{R}$. It is false over $\mathbf{C}$, it could be still true over $\mathbf{R}$.

Second, most geometrical theorems are only true for the "general" case. It may well happen that they are false for "degenerate" situations, for examples, when circles have zero radius, angles become zero, lines become parallel etc. Geometric theorem proving based on the Gröbner bases method can handle degenerate situations automatically in a very strong sense.

1. In situations where the degenerate situations can be described in the form $d(x_1, \ldots, x_n) \neq 0$, d a polynomial, one can again use a new indeterminate to transform the question into an ideal (and, hence, Gröbner basis) membership question. Namely,

$$\forall z((h(z) = 0 \wedge s(z) \neq 0) \Longrightarrow c(z) = 0)$$

is equivalent to

$$\exists z, u, v((h(z) = 0 \wedge u.s(z) = 1 \wedge v.c(z) = 1)$$

is equivalent to

$$1 \in \mathrm{GB}(h, u.s - 1, v.c - 1).$$

Using this wellknown transformation technique one can actually show that the Gröbner basis method yields a decision algorithm for the following general class of formulae:

(quantifiers)(arbitrary boolean combination of polynomial equations)

where either all the quantifiers must be existential or they must be universal, and the formulae must be closed, i. e. no free variables may occur.

2. The Gröbner bases approach to geometrical theorem proving can also be modified in such a way that, in case a proposition does not hold in general, the method automatically produces a set of polynomials describing the degenerate cases in which the proposition may be false. Roughly, this can be done, for example, by analyzing the denominators of the coefficients that are produced when Gröbner bases are computed over rational function coefficient fields. Quite some research has been devoted to this question, see (Kutzler 1986) and (Kapur 1986).

9 Application: Primary Decomposition

A polynomial ideal is "decomposable" iff it can be represented as the non-trivial intersection of two other polynomial ideals. Geometrically, this corresponds to a representation of the algebraic manifold (set of zeros) of the ideal as the non-trival union of two algebraic manifolds. It is well known in polynomial ideal theory that every polynomial ideal can be decomposed into finitely many ideals that can not be decomposed further ("irreducible components") and that this decomposition is essentially unique. This is the content of the famous Lasker-Noether decomposition theorem, see for example (Van der Waerden 1953). However, the proof of this theorem is non-constructive, i. e. no general algorithmic method is provided that would find, for a polynomial ideal given by a finite basis F, the finite bases for its irreducible components.

In more detail, the primary decomposition of a polynomial ideal (algebraic manifold) I (algebraic manifold) not only gives its irreducible parts (the corresponding "prime ideals") P_i but also information about the "multiplicity" of these irreducible

parts. This information is contained in the "primary ideals" Q_i corresponding to the prime ideals. Each prime ideal and its corresponding primary ideal implicitly describe the same irreducible algebraic manifold. However, the prime ideal and a corresponding primary ideal may be different. In this case, the primary ideal tells us "how often" the irreducible manifold defined by the prime ideal occurs in the algebraic manifold defined by the given ideal I. Summarizing, the algorithmic version of the primary decomposition problem has the following specification (where we use Z(F) for "set of common zeros of F"):

(Primary Decomposition Problem)

Given: F.
Find: G_i, H_i such that
the Ideal(G_i) are primary,
the Ideal(H_i) are the prime ideals corresponding to Ideal(G_i),
Ideal(F) = $\bigcap_i$ Ideal(G_i),
(i. e. Z(F) = $\bigcup_i$ Z(G_i)), and
some minimality conditions are satisfied.

Note that the problem depends on the underlying coefficient field. For example, $x^2 + 1$ is irreducible over $\mathbf{R}$ but reducible over $\mathbf{C}$.

Recently the problem of algorithmic primary decomposition has been completely solved using Gröbner bases. Still, the algorithm for the most general case is not yet implemented in a software system. Complete implementations may be expected for the very near future. A number of papers, of different generality and level of detail, contributed to the recent progress in this area: (Kandri-Rody 1984), (Lazard 1985), (Gianni, Trager, Zacharias 1985), (Kredel 1987).

An exact formulation of the problem and a detailed description of the algorithms, which are quite involved, is beyond the scope of this paper. It should be clear that automatic decomposition of algebraic manifolds (e. g. intersection curves of 3D objects) should be of utmost importance for geometrical modeling where the global analysis of finitely represented objects, as opposed to a mere local numerical evaluation, is more and more desirable in advanced applications. All the algorithms invented for the solution of the primary decomposition problem heavily rely on the basic properties of Gröbner bases as compiled in Theorem 2.5.1 and Theorem 2.5.2, notably on the properties (Elimination Ideals), (Ideal Membership) and properties derived from these properties as, for example, (Intersection Ideal).

For bringing this important research to the attention of the geometric modeling community we present a simple example showing the kind of information obtainable from a primary decomposition.

Example: Primary Decomposition of Cylinder/Sphere Intersection.

Let us consider the intersection of a cylinder with radius r_1 whose axis coincides with the x_3-axis and a sphere with radius r_2 and midpoint at the origin. The intersection curve consists of the common zeros of the following two polynomials:

$$F := \{x_1^2 + x_2^2 - r_1^2, x_1^2 + x_2^2 + x_3^2 - r_2^2\}.$$

Depending on whether $r_1 < r_2$, $r_1 = r_2$, or $r_1 > r_2$, the primary decomposition algorithm, over $\mathbf{R}$, yields the following representation of Ideal(F) as the intersection of primary ideals:

Case $r_1 < r_2$:

Ideal(F) = Ideal$(x_3 + r, x_2^2 + x_1^2 - r_1^2) \cap$ Ideal$(x_3 - r, x_2^2 + x_1^2 - r_1^2)$,
where $r := \sqrt{r_2^2 - r_1^2}$.

The two primary components are, in fact, prime.

Case $r_1 = r_2$:

Ideal(F) = Ideal$(x_3^2, x_2^2 + x_1^2 - r_1^2)$.

The ideal is already primary with corresponding prime ideal
Ideal$(x_3, x_2^2 + x_1^2 - r_1^2)$.

Case $r_1 > r_2$:

Ideal(F) = Ideal$(x_3^2 - r_2^2 + r_1^2, x_2^2 + x_1^2 - r_1^2)$.

The ideal is already primary and identical to the corresponding prime ideal.

In geometrical terms, the above outcome of the primary decomposition algorithm gives us the following information:

Case $r_1 < r_2$: The manifold decomposes in two irreducible components, namely, two horizontal circles of radius r_1 with midpoints $(0, 0, \pm r)$. The multiplicity of these circles is one (the primary ideals are identical to their corresponding prime ideals).

Case $r_1 = r_2$: The manifold does not decompose. It consists of the horizontal circle with radius r_1 with midpoint $(0, 0, 0)$. However, this circle has to be "counted twice" because, in the primary ideal, there appears the term x_3^2 whereas in the prime ideal, which defines the "shape" (i. e. point set) of the manifold, x_3 appears only linearly. This corresponds to the geometrical intuition that the intersection curve results from merging, in the limit, the two horizontal circles of case $r_1 < r_2$.

Case $r_1 > r_2$: The manifold does not decompose (over $\mathbf{R}$!). In fact it has no real points. In contrast to the case $r_1 = r_2$, the manifold has multiplicity one because the primary ideal coincides with the prime ideal.

10 Conclusions

The Gröbner bases method provides an algorithmic approach to many problems in polynomial ideal theory. We tried to provide some first evidence that the method could be a valuable tool for the progressing needs of geometrical engineering (geometric modeling, image processing, robotics, CAD etc.).

Further research should concentrate on two areas:

- The theoretical problems (for example, solutions at infinity in paremtric representations) occuring in the application of the method to geometrical problems must be completely studied.

parts. This information is contained in the "primary ideals" Q_i corresponding to the prime ideals. Each prime ideal and its corresponding primary ideal implicitly describe the same irreducible algebraic manifold. However, the prime ideal and a corresponding primary ideal may be different. In this case, the primary ideal tells us "how often" the irreducible manifold defined by the prime ideal occurs in the algebraic manifold defined by the given ideal I. Summarizing, the algorithmic version of the primary decomposition problem has the following specification (where we use Z(F) for "set of common zeros of F"):

(Primary Decomposition Problem)

Given: F.
Find: G_i, H_i such that
the Ideal(G_i) are primary,
the Ideal(H_i) are the prime ideals corresponding to Ideal(G_i),
Ideal(F) = $\bigcap_i$ Ideal(G_i),
(i. e. Z(F) = $\bigcup_i$ Z(G_i)), and
some minimality conditions are satisfied.

Note that the problem depends on the underlying coefficient field. For example, $x^2 + 1$ is irreducible over $\mathbf{R}$ but reducible over $\mathbf{C}$.

Recently the problem of algorithmic primary decomposition has been completely solved using Gröbner bases. Still, the algorithm for the most general case is not yet implemented in a software system. Complete implementations may be expected for the very near future. A number of papers, of different generality and level of detail, contributed to the recent progress in this area: (Kandri-Rody 1984), (Lazard 1985), (Gianni, Trager, Zacharias 1985), (Kredel 1987).

An exact formulation of the problem and a detailed description of the algorithms, which are quite involved, is beyond the scope of this paper. It should be clear that automatic decomposition of algebraic manifolds (e. g. intersection curves of 3D objects) should be of utmost importance for geometrical modeling where the global analysis of finitely represented objects, as opposed to a mere local numerical evaluation, is more and more desirable in advanced applications. All the algorithms invented for the solution of the primary decomposition problem heavily rely on the basic properties of Gröbner bases as compiled in Theorem 2.5.1 and Theorem 2.5.2, notably on the properties (Elimination Ideals), (Ideal Membership) and properties derived from these properties as, for example, (Intersection Ideal).

For bringing this important research to the attention of the geometric modeling community we present a simple example showing the kind of information obtainable from a primary decomposition.

Example: Primary Decomposition of Cylinder/Sphere Intersection.

Let us consider the intersection of a cylinder with radius r_1 whose axis coincides with the x_3-axis and a sphere with radius r_2 and midpoint at the origin. The intersection curve consists of the common zeros of the following two polynomials:

$$F := \{x_1^2 + x_2^2 - r_1^2, x_1^2 + x_2^2 + x_3^2 - r_2^2\}.$$

Depending on whether $r_1 < r_2$, $r_1 = r_2$, or $r_1 > r_2$, the primary decomposition algorithm, over $\mathbf{R}$, yields the following representation of Ideal(F) as the intersection of primary ideals:

Case $r_1 < r_2$:

$$\text{Ideal}(F) = \text{Ideal}(x_3 + r, x_2^2 + x_1^2 - r_1^2) \cap \text{Ideal}(x_3 - r, x_2^2 + x_1^2 - r_1^2),$$

where $r := \sqrt{r_2^2 - r_1^2}$.

The two primary components are, in fact, prime.

Case $r_1 = r_2$:

$$\text{Ideal}(F) = \text{Ideal}(x_3^2, x_2^2 + x_1^2 - r_1^2).$$

The ideal is already primary with corresponding prime ideal

$$\text{Ideal}(x_3, x_2^2 + x_1^2 - r_1^2).$$

Case $r_1 > r_2$:

$$\text{Ideal}(F) = \text{Ideal}(x_3^2 - r_2^2 + r_1^2, x_2^2 + x_1^2 - r_1^2).$$

The ideal is already primary and identical to the corresponding prime ideal.

In geometrical terms, the above outcome of the primary decomposition algorithm gives us the following information:

Case $r_1 < r_2$: The manifold decomposes in two irreducible components, namely, two horizontal circles of radius r_1 with midpoints $(0, 0, \pm r)$. The multiplicity of these circles is one (the primary ideals are identical to their corresponding prime ideals).

Case $r_1 = r_2$: The manifold does not decompose. It consists of the horizontal circle with radius r_1 with midpoint $(0, 0, 0)$. However, this circle has to be "counted twice" because, in the primary ideal, there appears the term x_3^2 whereas in the prime ideal, which defines the "shape" (i. e. point set) of the manifold, x_3 appears only linearly. This corresponds to the geometrical intuition that the intersection curve results from merging, in the limit, the two horizontal circles of case $r_1 < r_2$.

Case $r_1 > r_2$: The manifold does not decompose (over $\mathbf{R}$!). In fact it has no real points. In contrast to the case $r_1 = r_2$, the manifold has multiplicity one because the primary ideal coincides with the prime ideal.

10 Conclusions

The Gröbner bases method provides an algorithmic approach to many problems in polynomial ideal theory. We tried to provide some first evidence that the method could be a valuable tool for the progressing needs of geometrical engineering (geometric modeling, image processing, robotics, CAD etc.).

Further research should concentrate on two areas:

- The theoretical problems (for example, solutions at infinity in paremtric representations) occuring in the application of the method to geometrical problems must be completely studied.

- The computational behavior of the method must be improved by obtaining new mathematical results that could hold in the special situations (e. g. kinematics of certain robot classes) in which the method is applied.

Research on efficiency aspects and on geometrical applications of the Gröbner basis method is only at the beginning.

Acknowledgement. I am indebted to C. Hofmann, and B. Sturmfels for personal communications I used in this paper. Thanks also to B. Kutzler, R. Michelic-Birgmayr, and S. Stifter for helping in the preparation of some of the examples.

REFERENCES

D. S. ARNON, T. W. SEDERBERG, 1984. *Implicit Equation for a Parametric Surface by Gröbner Bases.* In: Proceedings of the 1984 MACSYMA User's Conference (V. E. Golden ed.), General Electric, Schenectady, New York, 431–436.

A. H. BARR, 1981. *Superquadrics and Angle-Preserving Transformations.* IEEE Computer Graphics and Applications, **1**/1, 11–23.

B. BUCHBERGER, 1965. *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal (German).* Ph. D. Thesis, Univ. of Innsbruck (Austria), Dept. of Mathematics.

B. BUCHBERGER, 1970. *An Algorithmic Criterion for the Solvability of Algebraic Systems of Equations (German).* Aequationes Mathematicae **4**/3, 374–383.

B. BUCHBERGER, G. E. COLLINS, R. LOOS, 1982. "Computer Algebra: Symbolic and Algebraic Computation". Springer-Verlag, Vienna - New York.

B. BUCHBERGER, 1985. *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory.* In: Multidimensional Systems Theory (N. K. Bose ed.), D. Reidel Publishing Company, Dordrecht - Boston - Lancaster, 184–232.

G. E. COLLINS, 1975. *Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition.* 2nd GI Conference on Automata Theory and Formal Languages, Lecture Notes in Computer Science **33**, 134–183.

P. GIANNI, 1987. *Properties of Gröbner Bases Under Specialization.* Proc. of the EUROCAL '87 Conference, Leipzig, 2–5 June 1987, to appear.

P. GIANNI, B. TRAGER, G. ZACHARIAS, 1985. *Gröbner Bases and Primary Decomposition of Polynomial Ideals.* Submitted to J. of Symbolic Computation. Available as manuscript, IBM T. J. Watson Research Center, Yorktown Heights, New York.

C. HOFMANN, 1987. *Algebraic Curves.* This Volume. Institute for Mathematics and its Applications, U of Minneapolis.

C. HOFMANN, 1987a. Personal Communication. Purdue University, West Lafayette, IN 47907, Computer Science Dept.

M. KALKBRENER, 1987. *Solving Systems of Algebraic Equations by Using Gröbner Bases.* Proc. of the EUROCAL '87 Conference, Leipzig, 2–5 June 1987, to appear.

D. KAPUR, 1986. *A Refutational Approach to Geometry Theorem Proving.* In: Proceedings of the Workshop on Geometric Reasoning, Oxford University, June 30 - July 3, 1986, to appear in *Artificial Intelligence.*

D. KAPUR, 1987. *Algebraic Reasoning for Object Construction from Ideal Images.* Lecture Notes, Summer Program on Robotics: Computational Issues in Geometry, August 24–28, Institute for Mathematics and its Applications, Univ. of Minneapolis.

A. KANDRI-RODY, 1984. *Effective Methods in the Theory of Polynomial Ideals.* Ph. D. Thesis, Rensselaer Polytechnic Institute, Troy, New York, Dept. of Computer Science.

H. KREDEL, 1987. *Primary Ideal Decomposition.* Proc of the EUROCAL '87 Conference, Leipzig, 2–5 June 1987, to appear.

B. KUTZLER, 1987. *Implementation of a Geometry Proving Package in SCRATCHPAD II.* Proceedings of the EUROCAL '87 Conferenc, Leipzig, 2–5 June, 1987, to appear.

B. KUTZLER, S. STIFTER, 1986. *On the Application of Buchberger's Algorithm to Automated Geometry Theorem Proving.* J. of Symbolic Computation, **2**/4, 389–398.

D. LAZARD, 1985. *Ideal Bases and Primary Decomposition: Case of Two Variables.* J. of Symbolic Computation **1**/3, 261–270.

R. P. PAUL, 1981. " Robot Manipulators: Mathematics, Programming, and Control". The MIT Press, Cambridge (Mass.), London.

F. P. PREPARATA, M. I. SHAMOS, 1985. "Computational Geometry". Springer-Verlag, New York, Berlin, Heidelberg.

T. W. SEDERBERG, D. C. ANDERSON, 1984. *Implicit Representation of Parametric Curves and Surfaces.* Computer Vision, Graphics, and Image Processing **28**, 72–84.

D. SPEAR, 1977. *A Constructive Approach to Ring Theory.* Proc. of the MACSYMA Users' Conference, Berkeley, July 1977 (R. J. Fateman ed.), The MIT Press, 369–376.

B. STURMFELS, 1987. Private Communication. Institute for Mathematics and its Applications.

W. TRINKS, 1978. *On B. Buchberger's Method for Solving Systems of Algebraic Equations (German).* J. of Number Theory **10**/4, 475–488.

A. VAN DEN ESSEN, 1986. *A Criterion to Decide if a Polynomial Map is Invertible and to Compute the Inverse.* Report 8653, Catholic University Nijmegen (The Netherlands), Dept. of Mathematics.

B. L. VAN DER WAERDEN, 1953. "Modern Algebra I, II", Frederick Ungar Publ. Comp., New York.

F. WINKLER, 1986. *Solution of Equations I: Polynomial Ideals and Gröbner Bases.* Proc. of the Conference on Computers and Mathematics, Stanford University, July 30 - August 1, 1986, to appear.

W. T. WU , 1978. *On the Decision Problem and the Mechanization of Theorem Proving in Elementary Geometry.* Scientia Sinica **21**, 150-172.