Mathematica Pannonica
1/1 (1990), 15 –32

GRÖBNER BASES IN GEOMETRY THEOREM PROVING AND SIMPLEST DEGENERACY CONDITIONS

Franz **Winkler**

Institut für Mathematik and Research Insitute for Symbolic Computation, Johannes Kepler Universität, A-4040 Linz, Österreich.

Received September 1988

AMS Subject Classification: 13 A 15, 13 F 20, 51-04, 68 C 20, 68 G 15

Keywords: geometry theorem proving, polynomial ideals, syzygies, Gröbner bases

Abstract: The method of Gröbner bases has been fruitfully applied to many problems in the theory of polynomial ideals. Recently Gröbner bases have been used in various ways for dealing with the problem of geometry theorem proving as posed by Wu. One approach is centered around the computation of a basis for the module of syzygies of the hypotheses and conclusion of a geometric statement. We elaborate this approach and extend it to a complete decision procedure.

In geometry theorem proving the problem of constructing subsidiary (or degeneracy) conditions arises. Such subsidiary conditions usually are not uniquely determined and obviously one wants to keep them as simple as possible. The question of constructing simplest subsidiary conditions has not been addressed yet. We show that our algorithm is able to construct the simplest subsidiary conditions with respect to certain predefined criteria, such as lowest degree or fewest variables.

0. Introduction

The work of Wu Wen-tsün [Wu 1978], [Wu 1984] has renewed the interest in automated geometry theorem proving. He has developed a decision algorithm for a certain class of geometry problems. The class of problems Wu considers (Wu's geometry, for short) consists, intuitively speaking, of those problems that can be translated into algebraic equations over some ground field K, the number system associated with the geometry. For the relationship between axiomatic geometries and number systems we refer to [Hilbert 1977]. Basically, Wu's geometry allows one to talk about incidence, parallelism, perpendicularity, cocircularity, congruence, etc., but not about "betweenness", because no order predicate is available.

Often a geometric statement is true only in a "generic" sense, i.e. after certain degenerate situations have been ruled out. Such degenerate situations typically occur when triangles collapse to a line segment, circles to a point, etc. and they are usually not explicitly mentioned. An automatic procedure for proving geometry statements has to be able to deal with the problem of such "degeneracy" or "subsidiary" conditions, that means it has to be able to automatically find suitable subsidiary conditions which make the statement a theorem, if such conditions exist at all.

Wu has given a decision procedure for solving the geometry theorem proving problem. His procedure also finds a subsidiary condition, if such a condition exists. Wu's decision algorithm has been partially implemented by himself and by Chou [Chou 1985]. Many interesting theorems have been proved by these implementations, including Simson's theorem, Pascal's theorem, the Butterfly theorem and Feuerbach's theorem. Wu's algorithm is based on the computation of characteristic sets of polynomial ideals, as introduced by Ritt [Ritt 1950].

Different approaches to geometry theorem proving, based on the computation of Gröbner bases [Buchberger 65], [Buchberger 85] for polynomial ideals, have been reported. In [Chou, Schelter 1986] Gröbner bases over the field generated by the independent variables of a geometric construction are employed. Kapur [Kapur 1986a,b] describes

a refutational theorem prover, based on Rabinowitsch's trick for proving Hilbert's Nullstellensatz. Kutzler and Stifter [Kutzler, Stifter 1986a,b] describe various ways of applying Gröbner bases to this problem, one of which is centered on the computation of a basis for the module of syzygies of the geometrical hypotheses and conclusion. This method is not complete. However, we are able to extend it to a complete decision procedure.

As we have mentioned above, an automatic procedure for geometry theorem proving must be able to find subsidiary conditions. Of course it would be of interest to keep the subsidiary condition as simple as possible. Referring to his approach Kapur [Kapur 1986b] claims that *"conditions found using this approach are often simpler and weaker than the ones reported using Wu's method or reported by an earlier version of Kutzler & Stifter's paper as well as Chou & Schelter based on the Gröbner basis method."* However, no algorithm for computing the "simplest" subsidiary condition has been reported up to now. Our algorithm is able to compute the "simplest" subsidiary condition by giving a complete overview of the possible subsidiary conditions. Reasonable criteria for "simplest" might be "of as low a degree as possible" or "involving only certain variables."

The stucture of this paper is as follows. In chapter 1 we give a short introduction to the theory of Gröbner bases, reviewing definitions and basic facts as far as they will be neccessary for the geometry theorem proving problem. In chapter 2 we define the geometry theorem proving problem. We derive a complete decision procedure *GEO*, which is also able to compute the simplest subsidiary condition for a given instance of the geometry theorem proving problem. Finally, in chapter 3 we demonstrate how *GEO* can be applied to concrete geometry problems.

1. The method of Gröbner bases

We define the notion of a Gröbner basis for a polynomial ideal as introduced by Buchberger [Buchberger 1965, 1985].

Let K be a field and $K[x_1, \ldots, x_n]$ (or $K[X]$ for short) the polynomial ring over K in the indeterminates $x_1, \ldots, x_n$. Let $[x_1, \ldots, x_n] = [X]$ denote the monoid of power products in $x_1, \ldots, x_n$. We start by choosing a *term ordering* $\prec$, i.e. a linear ordering on $[X]$ which makes $[X]$ an ordered monoid with $x_1^0 \ldots x_n^0$ as the least element. With respect to $\prec$ every nonzero polynomial $f \in K[X]$ contains a highest power product, which is called the *leading power product of* $f, lpp(f)$. The coefficient of $lpp(f)$ in f is called the *leading coefficient* of $f, lc(f)$. The polynomial which results from f by subtracting the leading power product multiplied by the leading coefficient is called the *reductum* of f, i.e. $red(f) = f - lc(f) \cdot lpp(f)$.

Every nonzero polynomial f gives rise to a *reduction relation* $\rightarrow_f$ on $K[X]$ in the following way: $g_1 \rightarrow_f g_2$ if and only if there is a power product u with a nozero coefficient a in g_1, i.e. $g_1 = au + h$ for some polynomial h which does not contain u, such that $lpp(f)$ divides u, i.e. $u = lpp(f)u'$ for some u', and $g_2 = -\frac{a}{lc(f)}u'red(f) + h$. If F is a set of polynomials, the *reduction relation* modulo F is defined so that $g_1 \rightarrow_F g_2$ if and only if $g_1 \rightarrow_f g_2$ for some $f \in F$. In this case g_1 is *reducible to* g_2 *modulo* F. If there is no such g_2, g_1 is *irreducible modulo* F. For every set of polynomials F the reduction relation $\rightarrow_F$ is Noetherian, i.e. every chain $f_1 \rightarrow_F f_2 \rightarrow_F \cdots$ terminates. We say that g is a *normal form of* f *modulo* F, if f can be reduced to g by a finite number of applications of $\rightarrow_F$, and g is irreducible modulo F. Normal forms are usually not unique.

If F is the basis of a polynomial ideal I, then obviously $f \rightarrow_F 0$ implies $f \in I$. In general, however, the implication in the reverse direction does not hold. A non-zero polynomial f might be irreducible modulo F and still $f \in I$.

Definition 1.1. Let I be an ideal in $K[X]$. A finite set of polynomials G is a *Gröbner basis* for I iff $(G) = I$ (G generates I) and $f \in I \Leftrightarrow f \rightarrow_F 0$, for all $f \in K[X]$. $\Diamond$

There are many equivalent definitions for Gröbner bases. The interested reader may confer [Buchberger 1985]. More importantly, however, every ideal I in $K[X]$ has a Gröbner basis and a Gröbner basis for I can always be computed starting with some basis F of I.

Göbner bases are an extremely powerful tools in commutative algebra. We mention some applications, as far as we will need them in the subsequent chapters. For further applications we refer to [Buchberger 1985], [Winkler et al. 1985], [Winkler 1986]. The "main problem" of polynomial ideal theory, namely the question whether $f \in I$ for a polynomial f and a polynomial ideal I, can easily be solved once a Gröbner basis G for I has been computed: reduce f to its unique normal form modulo G and check whether this normal form is 0. The identity $I = J$ for two ideals I and J can be checked algorithmically by computing Gröbner bases G_I and G_J for I and J, respectively, and then checking whether every basis element in G_I is in J and vice versa. The membership problem for the radical of an ideal I (i.e. wheter $f \in \mathit{radical}(I)$) can be solved by computing a Gröbner basis G for $(I, z \cdot f - 1)$, where z is a new variable, and checking whether G contains a constant.

The computation of a Gröbner basis is an important step in solving a system of algebraic equations. The following elimination property of a Gröbner basis with respect to a lexicographic ordering of the variables has been observed by Trinks [Trinks 1978]. It means that the i-th elimination ideal of an ideal I with Gröbner basis G is generated by the basis elements in G that depend only on the first i variables.

Lemma 1.2. *Let I be an ideal in $K[X]$ and G a Gröbner basis for I with respect to the lexicographic ordering $\prec$ with $x_1 \prec x_2 \prec \cdots \prec x_n$. Then, for $1 \leq i \leq n$,*

$$I \cap K[x_1, \ldots, x_i] = (G \cap K[x_1, \ldots, x_i]),$$

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

Proof. Obviously the right hand side is contained in the left hand side. On the other hand, assume that $f \in I \cap K[x_1, \ldots, x_i]$. Then f can be reduced to 0 modulo G with respect to the lexicographic ordering $\prec$. All the polynomials occurring in this reduction process depend only on the variables $x_1, \ldots, x_i$, and we get a representation of f as a linear combination of polynomials in G, where all the summands in this representation depend only on $x_1, \ldots, x_i$. $\Diamond$

Given bases for the ideals I and J, bases for $(I \cup J)$ and $I \cdot J$ can easily be determined. In general, however, computing bases for $I \cap J$ and $I : J$ is a hard problem.

Lemma 1.3. *Given bases for the ideals I and J in $K[X]$, bases for the following can be computed:*
(a) $I \cap J$,
(b) $I : J$,
(c) *radical*(I).

Proof. (a) For a new variable z we have

$$I \cap J = ((z-1)I \cup zJ) \cap K[X].$$

From bases for I and J we immediately get a basis for $((z-1)I \cup zJ)$. The intersection with $K[X]$ can be computed by Lemma 1.2.

(b) If $J = (f)$, then compute a basis $\{g_1, \ldots, g_k\}$ of $I \cap (f)$ by (a). $\{g_1/f, \ldots, g_k/f\}$ is a basis for $I : (f)$. In the general case $J = (f_1, \ldots, f_m)$ we have

$$I : J = \bigcap_{i=1}^{m} (I : (f_i)).$$

(c) The zero-dimensional case is treated in [Kalkbrener 1987], [Kobayashi et al. 1988] and the general case in [Kandri-Rody 1984], [Gianni et al. 1988].

$\Diamond$

Definition 1.4. Let $< f_1, \ldots, f_m > \in K[X]^m$. $< g_1, \ldots, g_m > \in \in K[X]^m$ is a *syzygy* of $< f_1, \ldots, f_m >$ iff $\sum_{i=1}^{m} f_i g_i = 0$. For a subset M of $K[X]^m$, $< g_1, \ldots, g_m >$ is a *syzygy* of M iff it is a syzygy of every element of M.

$\Diamond$

For a finite set $M \subset K[X]$, the syzygies of M are the solutions of a homogeneous system of linear equations with coefficients in M. A (finite) set $M \subset K[X]^m$ generates a module over $K[X]$, and on the other hand, as a consequence of Hilbert's basis theorem, every submodule of $K[X]^m$ has a finite basis. The set of syzygies of a subset M of $K[X]^m$ is equal to the set of syzygies of the module generated by M over $K[X]$, and it forms again a module over $K[X]$. The Gröbner bases algorithm can be used to compute a basis for the module of syzygies of M.

Lemma 1.5. *For every finite subset M of $K[X]^m$ a basis for the module of syzygies of M can be computed.*

Proof. see [Buchberger 1985] for the case $|M| = 1$ and [Winkler 1986] for the general case. An alternative approach via extending the notion of a Gröbner basis to modules is taken in [Galligo 1979] and [Möller, Mora 1986]. ◇

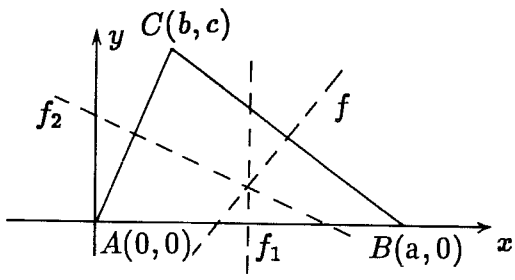
2. Geometry theorem proving: a decision procedure

We consider a geometry whose associated number system is the algebraic closure $\bar{K}$ of a field K, i.e. the geometric objects lie in $\bar{K}^n$ for some $n \in \mathbb{N}$. The statements we allow have to be expressible in the form

$$(2.1) \qquad (\forall x \in \bar{K}^n)[f_1(x) = 0 \wedge \ldots \wedge f_m(x) = 0 \Rightarrow f(x) = 0]$$

for some polynomials $f_1, \ldots, f_m, f$ in $K[x_1, \ldots, x_n] = K[X]$. The $f_1, \ldots, f_m$ are called the *hypothesis polynomials* or *hypotheses* for short, and f is called the *conclusion polynomial* or just the *conclusion.* Basically, this enables us to talk about incidence, parallelism, perpendicularity, cocircularity, congruence, etc., but not about "betweenness", because no order predicate is available.

As an example let us consider the geometric theorem (in $\mathbb{R}^2$) that "*for every triangle ABC the lines orthogonal to the sides of the triangle and passing through the midpoints of the associated sides have a common point of intersection*". Before we can express this theorem algebraically, we have to place the triangle in a two dimensional coordinate system. Without loss of generality we can assume that A is placed at the origin, $A = (0, 0)$, and that the side AB is parallel to the x-axis, $B = (a, 0)$. No restriction is put on $C = (b, c)$.



The equations for f_1, f_2 and f are

$$f_1(x,y) = x - \frac{1}{2}a,$$

$$f_2(x,y) = b(x - \frac{1}{2}b) + c(y - \frac{1}{2}c),$$

$$f(x,y) = (a-b)(x - \frac{1}{2}(a-b)) + c(y - \frac{1}{2}c).$$

In order to prove the theorem, it suffices to show that f vanishes on the variety of $(f_1, f_2) \subset \mathbb{R}(a,b,c)[x,y]$, or in other words that $f \in$ $\in$ *radical*(f_1, f_2). By the method described in Chapter 1 this problem can be decided by computing a Gröbner basis for $(f_1, f_2, z \cdot f - 1)$ in $\mathbb{R}(a,b,c)[x,y]$. The computation can be carried out completely over the field $\mathbb{Q}(a,b,c)$, yielding the Gröbner basis $\{1\}$. So f is indeed in the radical of (f_1, f_2) and the theorem is proved. A geometry theorem prover along these lines is described in [Chou,Schelter 1986].

An important step in this approach is the transition from the question whether a polynomial f vanishes on the variety of an ideal I to the problem whether f is in the radical of I. That is only possible if the varieties are defined over an algebraically closed ground field. So, for instance, one cannot decide geometric statements in real space but only in complex space. Theorems in real geometry can only be confirmed, but not disproved. For actually deciding statements in real geometry one has to consider the theory of elementary algebra and elementary geometry, based on real closed fields.This theory has been

shown to be decidable by Tarski [Tarski 1951] and has become known as Tarski algebra. Tarski's decision procedure has recently been improved in [Collins 1975], [Ben-Or et al. 1984] and [Grigor'ev 1988].

Often a geometric theorem is true only after certain degenerate situations have been ruled out by a nondegeneracy or subsidiary condition. As for the hypotheses and the conclusion, we require that the subsidiary condition be expressible by a polynomial, this time by a polynomial inequation of the form $s(x_1, \ldots, x_n) \neq 0$. So the problem becomes to decide whether for given $f_1, \ldots, f_m, f$ and s in $K[X]$

$$(2.2) \quad (\forall x \in \bar{K}^n)[f_1(x) = \cdots = f_m(x) = 0 \wedge s(x) \neq 0 \Rightarrow f(x) = 0].$$

Moreover, as we have mentioned above, in a geometry theorem proving setting it is reasonable to require that a subsidiary condition be determined algorithmically.

So we arrive at the following formal specification of the geometry theorem proving problems posed in [Wu 1984]. Let K be a field, $\bar{K}$ the algebraic closure of K.

P_{Wu}:
given: polynomials $f_1, \ldots, f_m, f$ in $K[X]$
decide: does there exist a polynomial $s \in K[X]$ such that
(1) $(\forall x \in \bar{K}^n)(f_1(x) = \ldots = f_m(x) = 0 \wedge s(x) \neq 0 \Rightarrow f(x) = 0)$
and
(2) $(\exists x \in \bar{K}^n)(f_1(x) = \ldots = f_m(x) = 0 \wedge s(x) \neq 0)$?
If so, find such an s.

Part (2) in P_{Wu} guarantees that the subsidiary condition does not exclude all points in the variety of $f_1, \ldots, f_m$. Sometimes it seems natural to use a finite number $s_1, \ldots, s_n$ of subsidiary conditions, replacing $s(x)$ in P_{Wu} by $s_1(x) \neq 0 \wedge \ldots \wedge s_n(x) \neq 0$, thus getting a modified problem. However, it can easily be seen that a single subsidiary condition s is sufficient. The factors of s satisfy the modified problem, and if $s_1, \ldots, s_n$ satisfy the modified problem, then their product $s_1 \cdot \ldots \cdot s_n$ satisfies P_{Wu}.

In [Wu 1984] Wu describes a decision algorithm for P_{Wu}, which has been partially implemented by himself and by Chou [Chou 1985].

Wu's algorithm is based on the computation of characteristic sets of polynomial ideals, as introduced by Ritt [Ritt 1950]. In this paper we solve P_{Wu} by computing a basis for the module of syzygies of the geometrical hypotheses and conclusion, thus getting also a method for computing the simplest subsidiary condition.

Theorem 2.1. *Let $f_1, \ldots, f_m, f$ be the parameters of an instance P of P_{Wu}.*

(i) *Those polynomials $s \in K[X]$, which satisfy part (1) of P, constitute an ideal N_P.*

(ii) *For every $s \in N_P$ there exist $s_1, \ldots, s_m \in K[X]$ and $k \in \mathbb{N}$, such that $< s_1, \ldots, s_m, s^k \cdot f^{k-1} >$ is a syzygy of $< f_1, \ldots, f_m, f >$, i.e. $s_1 \cdot f_1 + \cdots + s_m \cdot f_m + s^k \cdot f^{k-1} \cdot f = 0$.*

(iii) *If $< s_1, \ldots, s_m, s^k \cdot f^{k-1} >$, $k \in \mathbb{N}$, is a syzygy of $< f_1, \ldots, f_m, f >$, then $s \in N_P$.*

(iv) *Set*
$S_P = \{s | < s_1, \ldots, s_m, s >$ *is a syzygy of* $< f_1, \ldots, f_m, f >$ *for some* $s_1, \ldots, s_m\}$. *Then* $N_P = radical(S_P) : (f)$.

Proof. (i) Suppose both s_1 and s_2 solve part (1) of P. Now let t_1, t_2 be arbitrary polynomials, and let $x \in \bar{K}^n$ be such that $f_1(x) = \ldots = f_m(x) = 0$ and $(t_1 s_1 + t_2 s_2)(x) = t_1(x) \cdot s_1(x) + t_2(x) \cdot s_2(x) \neq 0$. Then either $s_1(x) \neq 0$ or $s_2(x) \neq 0$. W.l.o.g. assume that $s_1(x) \neq 0$. But then $f(x) = 0$, since s_1 is a solution of part (1) of P. So $t_1 s_1 + t_2 s_2$ is also a solution of part (1) of P.

(ii) Since $s \in N_P$, we know that $s \cdot f$ vanishes on every common zero of $f_1, \ldots, f_m$ in $\bar{K}$. That, however, means that $s \cdot f$ is in the radical of $(f_1, \ldots, f_m)$, and a power of $s \cdot f$, say $s^k \cdot f^k$, $k \in \mathbb{N}$, is in $(f_1, \ldots, f_m)$. Therefore, for some $s_1, \ldots, s_m \in K[X]$,

$$s_1 \cdot f_1 + \cdots + s_m \cdot f_m + s^k \cdot f^k = 0,$$

i.e. $< s_1, \ldots, s_m, s^k \cdot f^{k-1} >$ is a syzygy of $< f_1, \ldots, f_m, f >$.

(iii) $s_1 \cdot f_1 + \cdots + s_m \cdot f_m + s^k \cdot f^k = 0$, so for every $x \in \bar{K}^n$

$$f_1(x) = \ldots = f_m(x) = 0 \wedge s(x) \neq 0 \Rightarrow f(x) = 0.$$

(iv) Clearly S_P is an ideal in $K[X]$. By (ii) and (iii)

$$N_P = \{s \in K[X] | s^k \cdot f^{k-1} \in S_P \text{ for some } k \geq 1\}$$

If $s \in N_P$, then $s^k f^{k-1} \in S_P$ for some $k \geq 1$. Thus $s^k f^k \in S_P$. This, however, implies $sf \in radical(S_P)$ and therefore $s \in radical(S_P) : (f)$. On the other hand, let $s \in radical(S_P) : (f)$, i.e. $sf \in radical(S_P)$. Then $s^k f^k \in S_P$ for some $k \geq 1$. So $s^{k+1} f^k \in S_P$ and therefore $s \in N_P$. ◇

By Lemma 1.5 a finite basis for the module of syzygies of a sequence of polynomials can be computed. So for every instance P of P_{Wu} one can compute a finite basis for the ideal S_P. From the basis for S_P a basis for N_P can be computed by Lemma 1.3. Hence we have a complete overview of the solutions of part (1) of P_{Wu}. The remaining question is, whether there is a solution of (1), which also satisifies (2).

Theorem 2.2. *Let P be an instance of P_{Wu}, B a finite basis for N_P.*
(i) *If there is a polynomial in N_P which satisfies (2), then there is a polynomial in the basis B which satisfies (2).*
(ii) *If B is a Gröbner basis for N_P with respect to the term ordering $\prec$, B' is the set of $b \in B$ which satisfy part (2) of P, and $t = \min\{lpp(b) | b \in B'\}$, then for every solution s of P, $lpp(s) \geq t$.*

Proof. (i) Let $f_1, \ldots, f_m, f$ be the parameters of the instance P of P_{Wu} and $B = \{b_1, \ldots, b_r\}$. Assume that no basis polynomial b_i, $1 \leq i \leq r$, satisfies (2), i.e.

$$(\forall x \in \bar{K}^n)(f_1(x) = \ldots = f_m(x) = 0 \Rightarrow b_i(x) = 0) \text{ for all } 1 \leq i \leq r.$$

Then also for every linear combination $s = \sum_{i=1}^{r} h_i b_i$ we have

$$(\forall x \in \bar{K}^n)(f_1(x) = \ldots = f_m(x) = 0 \Rightarrow s(x) = 0),$$

so no $s \in N_P$ satisfies (2).

(ii) Let s be a solution of part (1) of P. $s \in N_P$, so s is reducible to 0 w.r.t. B. Let $C \subseteq B$ be the set of elements of B used in this reduction. Then $lpp(b) \leq lpp(s)$ for every $b \in C$. If no $b \in C$ satisfies part (2) of P, then neither does s. ◇

Theorem 2.2 (ii) establishes that "simplest" subsidiary conditions can be computed by choosing the term ordering $\prec$ appropriately, namely so that s_1 is simpler than s_2 if and only if $lpp(s_1 \prec lpp(s_2)$.

For instance, a Gröbner basis for N_P with respect to a graded ordering contains a solution of lowest degree of P, if any solution exists. A Gröbner basis for N_P with respect to a lexicographic ordering $x_1 \prec \ldots \prec x_m \prec \ldots \prec x_n$ contains a solution depending only on $x_1, \ldots, x_m$, if such a solution exists. The variables $x_1, \ldots, x_m$ could be the "independent" variables (see [Kutzler, Stifter 1986b]) of the geometric construction. So one can ask the question whether there is a nondegeneracy condition depending only on the independent variables. The two orderings can, of course, be combined by ordering the power products in $x_1, \ldots, x_m$ by some ordering $\prec_1$, e.g. according to the degree, and also the power products in $x_{m+1}, \ldots, x_n$ by some ordering $\prec_2$. Then a term ordering $\prec$ can be constructed by

$$u_1 u_2 \prec t_1 t_2 :\Leftrightarrow u_2 \prec_2 t_2 \vee (u_2 = t_2 \wedge u_1 \prec_1 t_1),$$

where u_1, t_1 are power products over $x_1, \ldots, x_m$ and u_2, t_2 power products over $x_{m+1}, \ldots, x_n$. This ordering will lead to a subsidiary condition of lowest degree involving only the independent variables $x_1, \ldots, x_m$.

In their report [Chou,Yang 1986] Chou and Yang consider the problem statement P_{Wu} and claim: "*The algebraic problem in this formulation is well defined. However, the polynomial s sometimes has nothing to do with nondegenerate conditions in geometry. To make things worse, this formulation is unsound from the geometric point of view.*" They go on to stress their point by an example. We will deal with this example and the criticism of P_{Wu} in Chapter 3.

Combining Theorems 2.1 and 2.2 we get the following decision algorithm for P_{Wu}.

Algorithm *GEO* (**in:** polynomials $f_1, \ldots, f_m$, $f \in K[X]$,
out: s, a solution of the instance
$P =< f_1, \ldots, f_m, f >$ of P_{Wu},
if such a solution exists,
or "no");

(1) *Compute a finite basis C for S_P, the ideal generated by the last component of the syzygies of $< f_1, \ldots, f_m, f >$.*

(2) *Compute a basis C' for radical(S_P).*

(3) *Compute a Gröbner basis C'' for $((z-1)C' \cup \{z \cdot f\})$ in $K[X][z]$ with respect to a lexicographic term ordering $x_1 \prec \cdots \prec x_n \prec z$.*

(4) *Set $C''' = C'' \cap K[X]$. C''' is a basis for radical$(S_P) \cap (f)$.*

(5) *Set $B = \{h/f | h \in C'''\}$. B is a basis for radical$(S_P) : (f) = N_P$.*

(6) *Check the polynomials b in B for $b \notin$ radical(I), where $I = (f_1, \ldots, f_m)$. If B is a Gröbner basis with respect to the term ordering $\prec$ and b is the element of B with the least leading power product satisfying $b \notin$ radical(I), then b is the simplest subsidiary condition. Set $s = b$ and stop. Otherwise output "no".* ♢

3. Examples

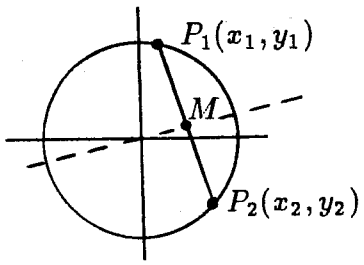
We use the decision algorithm *GEO* to prove that

"if P_1 and P_2 are two points on a circle and M is the midpoint of P_1 and P_2 then the line through M and perpendicular to P_1P_2 contains the center of the circle".

The hypotheses of the given instance P of P_{Wu} are

$f_1 : x_1^2 + y_1^2 - x_2^2 - y_2^2$
(P_1 and P_2 are points on a circle with center (0,0))

$f_2 : a(x_2 - x_1) + b(y_2 - y_1)$
($\binom{a}{b}$ is perpendicular to P_1P_2)



and the conclusion is

$f : a(y_1 + y_2) - b(x_1 + x_2)$
(the line $y = \frac{b}{a}x$ contains M, the midpoint of P_1 and P_2).

First we compute a basis for the ideal S_P, i.e. the third component of the module of syzygies of (f_1, f_2, f). A Gröbner basis for *ideal*(f_1, f_2, f) in $\mathbb{Q}[a, b, x_1, x_2, y_1, y_2]$ w.r.t. the lexicographic ordering with $a \prec b \prec x_1 \prec x_2 \prec y_1 \prec y_2$ is

$$\{f_1, f_2, f, f_3 = aby_1 - \frac{1}{2}b^2x_2 - \frac{1}{2}a^2x_2 - \frac{1}{2}b^2x_1 + \frac{1}{2}a^2x_1\}.$$

From the Gröbner basis we immediately get a basis for the module of syzygies of $< f_1, f_2, f_3, f >$. By an algorithm described in [Buchberger 1985] this syzygy basis can be transformed to a basis of the syzygies of $< f_1, f_2, f >$:

$$(-b, y_2 + y_1, x_1 - x_2),$$

$$(-a, x_2 + x_1, y_2 - y_1),$$

$$(0, ay_2 + ay_1 - bx_2 - bx_1, -by_2 + by_1 - ax_2 + ax_1),$$

$$(2aby_1 - b^2x_2 - a^2x_2 - b^2x_1 + a^2x_1, ay_2^2 - ay_1^2 + ax_2^2 - ax_1^2,$$

$$-by_2^2 + by_1^2 - bx_2^2 + bx_1^2).$$

Thus $S_P = (x_2 - x_1, y_2 - y_1)$ and $C = \{x_2 - x_1, y_2 - y_1\}$.

S_P is radical, so $C' = C$. Next we determine a Gröbner basis C'' for $((z-1)C' \cup \{zf\})$ in $\mathbb{Q}[a, b, x_1, x_2, y_1, y_2, z]$, getting

$$\begin{aligned}
&x_2z - x_1z - x_2 + x_1,\\
&y_2z - y_1z - y_2 + y_1,\\
&ay_2z + ay_1z - bx_2z - bx_1z,\\
&ay_1z - bx_1z + \frac{1}{2}ay_2 - \frac{1}{2}ay_1 - \frac{1}{2}bx_2 + \frac{1}{2}bx_1,\\
&ax_2y_2 - ax_1y_2 + ax_2y_1 - ax_1y_1 - bx_2^2 + bx_1^2 = (x_2 - x_1) \cdot f,\\
&ay_2^2 - bx_2y_2 - bx_1y_2 - ay_1^2 + bx_2y_1 + bx_1y_1 = (y_2 - y_1) \cdot f.
\end{aligned}$$

Intersecting this basis with $\mathbb{Q}[a, b, x_1, x_2, y_1, y_2]$ and dividing by f we finally get the basis $B = \{x_2 - x_1, y_2 - y_1\}$ for $radical(S_P) : (f) = N_P$.

Neither $x_2 - x_1$ nor $y_2 - y_1$ is in the radical of $ideal(f_1, f_2)$, so both are solutions of the geometric problem instance P, and they are solutions of lowest degree.

That means the theorem holds in $\mathbb{C}^2$ (and therefore also in $\mathbb{R}^2$) if either the x-coordinates or the y-coordinates of the two points P_1 and P_2 differ from one another, i.e. P_1 and P_2 do not collapse to a single point.

For further demonstrating the usefulness of computing a simplest subsidiary condition, we consider an example used in [Chou,Yang 1986]

to support the claim that the polynomial s computed as a solution of P_{Wu} may have nothing to do with a subsidiary condition for the geometric problem.

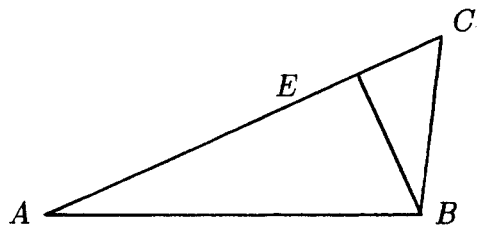
The goal is to prove that *"every triangles is isosceles"*, which of course, is not a theorem in complex geometry. Chou & Yang observe, however, that there is a formulation of this problem as an instance of P_{Wu}, which admits a subsidiary condition s.

The algebraic formulation they use is the following: let ABC be a triangle, and BE the altitude from B. Show that $AB \equiv CB$. As coordinates for the points they choose $A = (0,0)$, $B = (y_1,0)$, $C = (y_4,y_5)$, and $E = (y_2,y_3)$. Now the hypotheses can be translated into the algebraic equations

$$h_1 = y_3y_5 + (y_2 - y_1)y_4 = 0 \qquad BE \perp AC$$
$$h_2 = -y_2y_5 + y_3y_4 = 0 \qquad E \text{ is on } AC$$

and the conclusion into the equation

$$g = -y_5^2 - y_4^2 + 2y_1y_4 = 0 \qquad AB \equiv CB.$$



$s = y_3^2 + y_2^2 - y_1y_2$ satisfies both conditions in P_{Wu}. In fact, Kapur's theorem prover confirms the "theorem" under the subsidiary condition s. Chou & Yang now state that *"Thus under this formulation we can prove that "every" triangle is isosceles"* and they take this as evidence of their claim that P_{Wu} is *"unsound"*.

In our oppinion, the controversy stems from the fact that the dependent variables y_2, y_3 are not explicitly excluded from the subsidiary condition. If one wants to consider only such subsidiary conditions, which do not involve the dependent variables (which is reasonable from a geometric point of view), then this can be achieved by a suitable

ordering of the power products, e.g. a lexicographic ordering based on

$$\underbrace{y_1 < y_4 < y_5}_{\text{indep. var.}} < \underbrace{y_2 < y_3}_{\text{dep. var.}}.$$

Now the algorithm *GEO* is able to detect that there exists no subsidiary condition involving only the independent variables y_1, y_4, y_5. Actually also Kapur [Kapur 1986b] mentions the possibility of recognizing that there is no such subsidiary condition in a remark following Theorem 2.

Let us apply the algorithm *GEO* to the geometric problem in the formulation above, where h_1, h_2 are the hypotheses and g is the conclusion. We get

$$\begin{aligned}\{b_1 &= y_4y_3 - y_5y_2,\\ b_2 &= y_5^2y_2 + y_4^2y_2 - y_1y_4^2,\\ b_3 &= y_3^2 + y_2^2 - y_1y_2,\\ b_4 &= y_5y_3 + y_4y_2 - y_1y_4\}\end{aligned}$$

as a basis for S_P, the ideal generated by the last component of the syzygies of (h_1, h_2, g). S_P is radical, so we just have to compute the intersection $S_P \cap \mathit{ideal}(g)$ and divide by g. This leads to the basis $\{b_1, b_2, b_3, b_4\}$ for N_P.

Finally in step (6) we detect that $b_3 \notin \mathit{radical}(h_1, h_2)$, but there exists no possible subsidiary condition involving only the independent variables y_1, y_4, y_5.

Acknowledgement. Work reported herein has been supported by the *Österreichische Forschungsgemeinschaft* and by the Austrian *Fonds zur Förderung der wissenschaftlichen Forschung* under Project Nr. P.6763.

References

[Ben-Or et al. 1984] BEN-OR, M; KOZEN, D.; REIF, J. : "The Complexity of Elementary Algebra and Geometry", *Proc. 16th ACM Symp. on Theory of Computing*, 457 – 464 (1984).

[Buchberger 1965] BUCHBERGER, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Ph.D. dissertation Univ. Innsbruck, Austria (1965).

[Buchberger 1985] BUCHBERGER, B.: "Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory", in: *Multidimensional Systems Theory*, N.K. Bose, ed., 184 – 232, D. Reidel Publ. Comp. (1985).

[Chou 1985] CHOU, S.-C.: Proving and Discovering Theorems in Elementary Geometry Using Wu's Method, Ph.D. Thesis, Dept. of Mathematics, University of Texas, Austin (1985).

[Chou, Schelter 1986] CHOU, S.-C.; SCHELTER, W.F.: "Proving Geometry Theorems with Rewrite Rules", *J. Automated Reasoning* **2**, 253 – 273 (1986).

[Chou, Yang 1986] CHOU, S.-C.; YANG, J.-G.: "On the Algebraic Formulation of Geometry Theorems", Techn. Rep., Inst. for Computer Science, Univ. of Texas, Austin (1986).

[Collins 1975] COLLINS, G.E.: "Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition", *Proc. 2nd GI Conf. on Automata Theory and Formal Languages*, Springer-Verlag, LNCS 35, 134 – 183, Berlin (1975).

[Galligo 1979] GALLIGO, A.: "Théorème de division et stabilité en géometrie analytique locale", *Ann. Inst. Fourier* **29**, 107 – 184 (1979).

[Gianni et al. 1988] GIANNI, P; TRAGER, B.; ZACHARIAS, G.: "Gröbner Bases and Primary Decomposition of Polynomial Ideals", to appear in *J. of symbolic Computation* (1988).

[Grigor'ev 1988] GRIGOR'EV, D.Yu.: "Complexity of Deciding Tarski Algebra", *J. of Symbolic Computation* **5/1& 2**, 65 – 108 (1988).

[Hilbert 1977] HILBERT, D.: Grundlagen der Geometrie, Teubner Verlag, Stuttgart (1977).

[Kalkbrener 1987] KALKBRENER, M.: Application of Gröbner Bases: Solution of Algebraic Equations and Decomposition of Radicals, Diplomarbeit, RISC-Linz, J. Kepler Univ. Linz (1987).

[Kandri-Rody 1984] KANDRI-RODY, A.: Effective Methods in the Theory of Polynomial Ideals, Ph. D. thesis, Rensselaer Polytechnic Institute, Troy, NY (1984).

[Kapur 1986a] KAPUR, D.: "Geometry Theorem Proving Using Hilbert's Nullstellensatz", *Proc. SYMSAC'86*, 202 – 208. B.W. Char, ed., ACM (1986).

[Kapur 1986b] KAPUR, D.: "Using Gröbner Bases to Reason About Geometry Problems", *J. of Symbolic Computation* **2/4**, 399 – 408 (1986).

[Kobayashi et al. 1988] KOBAYASHI, H.; MORITSUGU, S. and HOGAN, R.W.: "On Solving Systems of Algebraic Equations", to appear in *J. of Symbolic Computation* (1988).

[Kutzler, Stifter 1986a] KUTZLER, B.; STIFTER, S.: "Automated Geometry Theorem Proving Using Buchberger's Algorithm", *Proc. 1986 Symp. on Symbolic and Algebraic Computation (SYMSAC'86)*, 209 – 214, B.W. Char (ed.), ACM, New York (1986).

[Kutzler, Stifter 1986b] KUTZLER, B.; STIFTER, S.: "On the Application of Buchberger's Algorithm to Automated Geometry Theorem Proving", *J. of Symbolic Computation* **2/4**, 389 – 397 (1986).

[Möller, Mora 1986] MÖLLER, H.M.; MORA, F.: "New Constructive Methods in Classical Ideal Theory", *J. of Algebra* **100/1**, 138 – 178 (1986).

[Ritt 1950] RITT, J.F.: Differential Algebra, AMS Colloquium Publications, New York (1950).

[Tarski 1951] TARSKI, A.: A Decision Method for Elementary Algebra and Geometry, Univ. of California Press (194), 2nd ed. (1951).

[Trinks 1978] TRINKS, W.: Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen", *J. of Number Theory* **10/4**, 475 – 488 (1978).

[Winkler 1986] WINKLER, F.: Solution of Equations I: Polynomial Ideals and Gröbner Bases; lecture notes of the short course on "Symbolic and Algebraic Computation", Conf. "Computers & Mathematics", Stanford Univ. (1986).

[Winkler et al. 1985] WINKLER, F.; BUCHBERGER, B.; LICHTENBERGER, F.; ROLLETSCHEK, H.: "An Algorithm for Constructing Canonical Bases of Polynomial Ideals", *ACM Trans. on Mathematical Software* **11/1**, 66 – 78 (1985).

[Wu 1978] WU, Wen-tsün: "On the Decision Problem and the Mechanization of Theorem Proving in Elementary Geometry", *Scientia Sinica* **21**, 157 – 179 (1978).

[Wu 1984] WU, Wen-tsün: "Basis Principles of Mechanical Theorem-Proving in Elementary Geometry", *J. Syst. Sci.* & Math. Sci. **4/3**, 207 – 235 (1984).