AUTOMATED THEOREM PROVING IN NONLINEAR GEOMETRY

Franz Winkler

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 yet been solved satisfactorily. 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.

1980 Mathematics Subject Classification 13A15, 13F20, 51-04, 68C20, 68G15

Advances in Computing Research, Volume 6, pages 183–197.

ISBN: 1-55938-342-9

0. INTRODUCTION

The work of Wu Wen-tsün [WU1,WU2] 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 [HI]. Basically, Wu's geometry allows us to talk about incidence, parallelism, perpendicularity, cocircularity, congruence, and so forth, but not about "betweenness," because no order predicate is available.

Often a geometric statement is true only in a "generic" sense, that is, after certain degenerate situations have been ruled out. Such degenerate situations typically occur, for example, when triangles collapse to a line segment or circles to a point, 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, which means it has to be able automatically to find suitable subsidiary conditions that 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 [C1]. Many interesting theorems have been proved by these implementations, including Simson's Theorem, Pascal's Theorem, the Butterfly Theorem and Feuerbach's Theorems (see [C2]). Wu's algorithm is based on the computation of characteristic sets of polynomial ideals, as introduced by Ritt [RI].

Different approaches to geometry theorem proving, based on the computation of Gröbner bases [B1,B2] for polynomial ideals, have been reported. In [CS] Gröbner bases over the field generated by the independent variables of a geometric construction are employed. Kapur [KP1,KP2] describes a refutational theorem prover, based on Rabinowitsch's trick for proving Hilbert's Nullstellensatz. Kutzler and Stifter [KS1,KS2] 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 [KP2] 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 structure of this paper is as follows. In Section 1 we give a short introduction to the theory of Gröbner bases, reviewing definitions and basic facts as far as they will be necessary for the geometry theorem proving problem. In Section 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 Section 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 [B1,B2].

Let K be a field and $K[x_1,..., x_n]$ (or $K[X]$ for short) the polynomial ring over K in the indeterminates $x_1,..., x_n$. Let $[x_1,..., x_n] = [X]$ denote the monoid of power products in $x_1,..., x_n$. We start by choosing a *term ordering* $\prec$, that is, a linear ordering on $[X]$ that makes $[X]$ an ordered monoid and with $x_1^0 \cdots x_n^0$ 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 that results from f by subtracting the leading power product multiplied by the leading coefficient is called the *reduction* of f, that is, red(f) $= f - lc(f)$ 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 nonzero coefficient a in g_1, that is, $g_1 = au + h$ for some polynomial h that does not contain u, such that lpp(f) divides u, that is $u = \text{lpp}(f)u'$ for some u', and

$$g_2 = -\frac{a}{\text{lc}(f)}\, u' \,\text{red}(f) + h.$$

If F is a set of polynomials, the *reduction relation modulo F* is defined such 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, that is, 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 nonzero 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 $(G) = I$ (i.e., G generates I) and $f \in I \Leftrightarrow f \rightarrow_G 0$, for all $f \in K[X]$.

There are many equivalent definitions for Gröbner bases. The interested reader may consult [B2]. More importantly, however, every ideal I in $K[X]$ has a Gröbner basis, and a Gröbner basis for I can always he computed starting with some basis F of I.

Gröbner bases are an extremely powerful tool in commutative algebra. We mention some applications, insofar as we will need them in the subsequent chapters. For further applications we refer to [B2,WB,WI]. 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, that is, $f \in \text{radical}(I)$? can be solved by computing a Gröbner basis G for $(I, z(f-1))$, where z is a new variable, and checking whether G contains a constant (see [WI]).

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 [TR]. It means that the ith 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 $K[x_1, \ldots, x_i]$.

Given bases for the ideals I and J, bases for $(I \cup J)$ and IJ, the ideal generated by all products of elements of I and J, can easily be determined. In general, however, computing bases for $I \cap J$ and $I{:}J$ is a hard problem, which can be solved by the Gröbner basis algorithm.

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) IJ,
(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) For two ideals I and J, the set $I{:}J$ is defined as $\{h \in K[X] \mid hg \in I \text{ for every } g \in J\}$. $I{:}J$ is again an ideal, and it can be computed as follows: 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) For an ideal I, the set radical(I) is defined as $\{h \in K[X] \mid h^m \in I \text{ for some } m \in \mathbb{N}\}$. radical$(I)$ is again an ideal, and it is called the *radical* of I. The zero-dimensional case of computing radical(I) is treated in [KL,KR,KMH] and the general case in [KA,GI]. Basically, it amounts to a primary decomposition of the ideal I and collecting the associated prime ideals. ■

DEFINITION 1.4: Let $<f_1,\ldots,f_m> \in K[X]^m$. $<g_1,\ldots,g_m> \in K[X]^m$ *is a syzygy* of $<f_1,\ldots,f_m>$ iff $\Sigma_{i=1}^{m} f_i g_i = 0$. 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.

For a finite set $M \subset K[X]^m$, the syzygies of M are the solutions of a homogeneous system of linear equations with the components of M as coefficients. 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 basis 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 [B2] for the case $|M| = 1$ and [WI] for the general case. An alternative approach via extending the notion of a Gröbner basis to modules is taken in [GA] and [MM]. ■

2. GEOMETRY THEOREM PROVING: A DECISION PROCEDURE

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

$$(\forall x \in \overline{K}^n) \qquad [f_1(x) = 0 \wedge \cdots \wedge f_m(x) = 0 \Rightarrow f(x) = 0], \tag{2.1}$$

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, and so forth, but not about "betweenness," because no order predicate is available.

As an example let us consider the geometric theorem (in $\mathbb{R}^2$): 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 (Figure 1). 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, $C = (b,c)$.

The equations for f_1, f_2, and f are

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

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

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

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 $f \in \text{radical}(f_1,f_2)$. By the method described in Section 1, this problem can be decided by computing a Gröbner basis for $(f_1,f_2,z(f-1))$ 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 [CS].

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

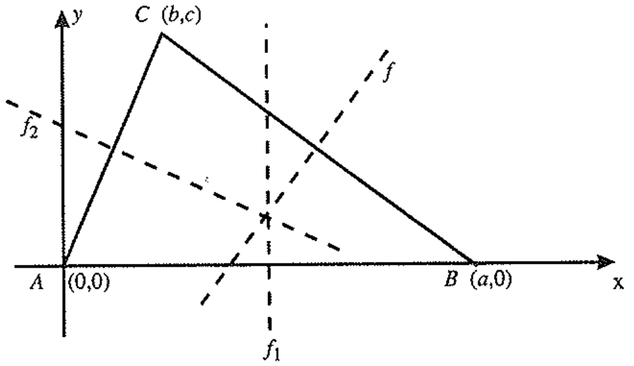

Figure 1.

[TA] and has become known as Tarski algebra. Tarski's decision procedure has recently been improved in [CO], [BKR], and [GR].

Often a geometric theorem is true only after certain degenerate situations have been ruled out by a nondegeneracy or subsidiary condition.

EXAMPLE. As an example we take the following geometric statement: 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 (Figure 2).

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

$$f_1\colon\ x_1^2 + y_1^2 - x_2^2 - y_2^2$$

(P_1 and P_2 are points on a circle with center (0,0)), and

$$f_2\colon\ a(x_2 - x_1) + b(y_2 - y_1)$$

($\begin{pmatrix} a \\ b \end{pmatrix}$ is perpendicular to P_1P_2), and the conclusion is

$$f\colon\ a(y_1 + y_2) - b(x_1 + x_2)$$

[the line $y = {}^b\!/\!_a x$ contains M, the midpoint of P_1 and P_2].

By a Gröbner basis computation, it turns out that $f \notin \text{radical}(f_1, f_2)$. And indeed, if $P_1 = P_2$, the perpendicular line is not uniquely determined. So the statement is not a theorem, although we have the strong "feeling" that by excluding a few degenerate cases (like $P_1 = P_2$) it might become a theorem. ■

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 $K[X]$,

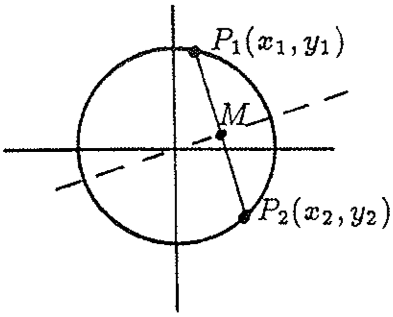

Figure 2.

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

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 problem posed in [W2]. Let K be a field, $\overline{K}$ the algebraic closure of K.

PROBLEM P_{Wu}. For given: polynomials $f_1,\ldots,f_m, f$ in $K[X]$, decide whether there exists a polynomial $s \in K[X]$ such that

(1) $(\forall x \in \overline{K}^n) \quad (f_1(x) = \cdots = f_m(x) = 0 \ \wedge \ s(x) \neq 0 \Rightarrow f(x) = 0)$,

(2) $(\exists x \in \overline{K}^n) \quad (f_1(x) = \cdots = f_m(x) = 0 \ \wedge \ s(x) \neq 0)$.

If so, find such an s.

Part (2) in P_{Wu} guarantees that the subsidiary condition does not exclude all points on 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 $s_1(x) \neq 0 \wedge \cdots \wedge s_n(x) \neq 0$, 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 $s_1 \ldots s_n$ satisfies P_{Wu}.

In [W2] Wu describes a decision algorithm for P_{Wu}, which has been partially implemented by himself and by Chou [C1]. Wu's algorithm is based on the computation of characteristic sets of polynomial ideals, as introduced by Ritt [RI]. In [KP2] it is shown (Theorem 2) that by a Gröbner basis computation a subsidiary condition can be computed if one exists. In this paper we solve P_{Wu} by computing a basis for the ideal containing all the solutions of part (1), thus also getting a method for computing the simplest subsidiary condition.

THEOREM 2.1: Let $f_1,...,f_m, f$ 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) $N_P = \text{radical}(f_1,...,f_m):(f)$.

(iii) $N_P = \text{radical}(S_P):(f)$, where

$$S_P = \{s | <s_1,...,s_m, s> \text{ is a syzygy of } <f_1,...,f_m,f> \text{ for some } s_1,...,s_m\}.$$

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 $x \in \overline{K}^n$ be such that $f_1(x) = \cdots = f_m(x) = 0$ and $(t_1s_1 + t_2s_2)(x) = t_1(x)s_1(x) + t_2(x)s_2(x) \neq 0$. Then either $s_1(x) \neq 0$ or $s_2(x) \neq 0$. Without loss of generality, assume that $s_1(x) \neq 0$. But then $f(x) = 0$, since s_1 is a solution of part (1) of P. So also $t_1s_1 + t_2s_2$ is a solution of part (1) of P.

(ii) If $s \in N_P$, then sf vanishes on every common root of $f_1,...,f_m$ in $\overline{K}$. That, however, means that $sf \in \text{radical}(f_1,...,f_m)$ and therefore $s \in \text{radical}(f_1,...,f_m):(f)$.

On the other hand, if $s \in \text{radical}(f_1,...,f_m):(f)$, then $sf \in \text{radical}(f_1,...,f_m)$. So f vanishes on every common root of $f_1,...,f_m$ on which s does not vanish, that is, $s \in N_P$.

(iii) If $s \in N_P$, we know from (ii) that $sf \in \text{radical}(f_1,..., f_m)$, that is, for some $k \in \mathbb{N}$, and for some $s_1,...,s_m \in K[X]$,

$$s_1f_1 + \cdots + s_mf_m + s^kf^k = 0,$$

that is, $s^kf^{k-1} \in S_P$ and also $s^kf^k \in S_P$. So $sf \in \text{radical}(S_p)$ and therefore $s \in \text{radical}(S_P):(f)$.

On the other hand, let $s \in \text{radical}(S_p):(f)$, that is, $sf \in \text{radical}(S_p)$. Then $s^kf^k \in S_P$ for some $k \geq 1$. Also $s^{k+1}f^k \in S_P$, that is,

$$s_1f_1 + \cdots + s_mf_m + s^{k+1}f^{k+1} = 0.$$

So $sf \in \text{radical}(f_1,..., f_m)$ and $s \in \text{radical}(f_1,..., f_m):(f) = N_P$. ■

Theorem 2.1 gives two methods for computing the set of solutions of part (1) of P_{Wu}. By Lemma 1.3 a basis for the radical can be computed, and by Lemma 1.5 a basis for the module of syzygies can be computed. Characterization (ii) is very similar to the one developed in [KP2], Theorem 2. Characterization (iii) is the complete version of the heuristic approach of [KS1,KS2].

Since a radical has to be computed anyway, one might argue that the characterization (ii) is definitely better than the characterization (iii), because it does not involve the computation of syzygies. However, in the examples we considered we found that usually S_P is simpler than the ideal generated by the hypotheses, so the radical computation for S_P is less costly. In any case 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) that also satisfies (2). If possible, we want to compute a simplest such condition.

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 that satisfies (2), then there is a polynomial in the basis B that satisfies (2).

(ii) If B is a Gröbner basis for N_P with respect to the term ordering $\prec$, B' is the set of those $b \in B$ satisfying part (2) of P, and $t = \min\{\mathrm{lpp}(b) | b \in B'\}$, then for every solution s of P, $t \preceq \mathrm{lpp}(s)$.

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

$$(\forall x \in \overline{K}^n) \quad (f_1(x) = \cdots = f_m(x) = 0 \Rightarrow b_i(x) = 0) \quad \text{for all } 1 \le i \le r.$$

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

$$(\forall x \in \overline{K}^n) \quad (f_1(x) = \cdots = f_m(x) = 0 \Rightarrow s(x) = 0),$$

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 $\mathrm{lpp}(b) \preceq \mathrm{lpp}(s)$ 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, such that s_1 is simpler than s_2 if and only if $\mathrm{lpp}(s_1) \prec \mathrm{lpp}(s_2)$. For instance, a Gröbner basis for N_P with respect to a graduated ordering contains a solution of lowest degree of P, if any such solution exists. A Gröbner basis for N_P with respect to a lexicographic ordering $x_1 \prec \cdots \prec x_m \cdots \prec x_n$ contains a solution depending only on $x_1,...,x_m$, if such a solution exists. The variables $x_1,...,x_m$ could be the "independent" variables (see [KS2]) 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 $x_1,...,x_m$ by some ordering $\prec_1$, for example, according to the degree, and also the power products in $x_{m+1},...,x_n$ by some ordering $\prec_2$. Then a term ordering $\prec$ can be constructed by

$$u_1u_2 \prec t_1t_2 :\Leftrightarrow u_2 \prec_2 t_2 \vee (u_2 = t_2 \wedge u_1 \prec_1 t_1),$$

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

In their report [CY] 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 Section 3.

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

Algorithm *GEO*

```
in: polynomials $f_1,...,f_m, f \in K[X]$,
out: $s$, a solution of the instance $P = <f_1,...,f_m, f> P_{Wu}$,
    if such a solution exists, or "no";
(1)  Compute a finite basis $B$ for $N_P$ using either one of the characterizations
     of Theorem 2.1.
(2)  Check the polynomials $b$ in $B$ for $b \notin$ radical($I$), where $I = (f_1,...,f_m)$. 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

First let us consider the example of Section 2. We use the decision algorithm *GEO* to prove the following:

If P_1andP_2 are two points on a circle and M is the midpoint of P_1andP_2 then the line through M and perpendicular to P_1P_2 contains the center of the circle (Figure 3).

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

$$f_1\colon\ x_1^2 + y_1^2 - x_2^2 - y_2^2$$

(P_1 and P_2 are points on a circle with center (0,0)),

$$f_2\colon\ a(x_2 - x_1) + b(y_2 - y_1)$$

($\begin{pmatrix} a \\ b \end{pmatrix}$ is perpendicular to P_1P_2) and the conclusion is

$$f\colon\ a(y_1 + y_2) - b(x_1 + x_2)$$

[the line $y = {}^{b}\!/_{a}x$ contains M, the midpoint of P_1andP_2].

First we compute a basis for the ideal S_P, that is, the third component of the module

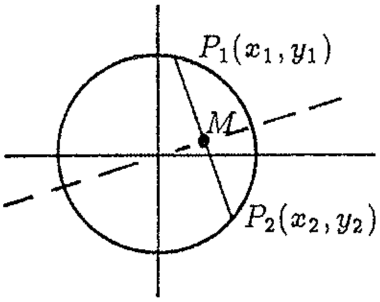

Figure 3.

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 $a \prec \mathrm{b} \prec x_1 \prec x_2 \prec y_1 \prec y_2 \prec$ is

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

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 [B2] this syzygy basis can be transformed to a basis of the syzygies of $<f_1,f_2f>$:

$$(-b,y_2 + y_1,x_1 - x_2), \quad (-a,x_2 + x_1,y_2 - y_1),$$

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

$$(2aby_1 - b^2x_2 - a^2x_2 - b^2x_1 + a^2x_1, ay_2^2 - ay_1^2 + ax_2^2 - ax_1^2, - by_2^2 + by_1^2 - bx_2^2 + bx_1^2).$$

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

S_P is radical. For computing S_P:radical(f), we apply Lemma 1.3 and first compute a basis for $S_P \bigcap ideal(f)$. A Gröbner basis for $((z - 1)S_P \bigcup \{zf\})$is

$$x_2z - x_1z - x_2 + x_1, \quad y_2z - y_1z - y_2 + y_1,$$

$$ay_2z + ay_1z - bx_2z - bx_1z, \quad ay_1z - bx_1z + \tfrac{1}{2}ay_2 - \tfrac{1}{2}ay_1 - \tfrac{1}{2}bx_2 + \tfrac{1}{2}bx_1,$$

$$ax_2y_2 - ax_1y_2 + ax_2y_1 - ax_1y_1 - bx_2^2 + bx_1^2 = (x_2 - x_1)f,$$

$$ay_2^2 - bx_2y_2 - bx_1y_2 - ay_1^2 + bx_2y_1 + bx_1y_1 = (y_2 - y_1)f.$$

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, that is, P_1 and P_2 do not collapse to a single point.

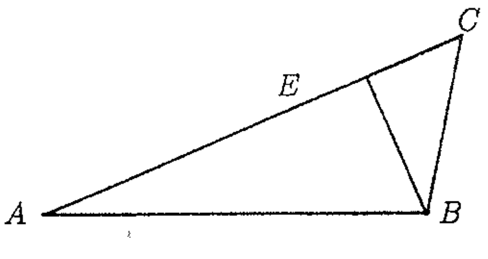

Figure 4.

For further demonstrating the usefulness of computing a simplest subsidiary condition, we consider an example used in [CY] 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: every triangle is isosceles, which, of course, is not a theorem in complex geometry. Chou and Yang observe, however, that there is a formulation of this problem as an instance of P_{Wu} that admits a subsidiary condition s.

The algebraic formulation they use is the following: Let ABC be a triangle, and BE the altitude from B (Figure 4). 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

$$h_1 = y_3y_5 + (y_2 - y_1)y_4 = 0, \quad BE \perp AC,$$

$$h_2 = -y_2y_5 + y_3y_4 = 0, \quad E \text{ is on } AC,$$

and the conclusion into the equation

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

$s = y_3^2 + y_2^2 - y_1y_2$ satisfies both conditions in P_{Wu}. In fact, Kapur's theorem prover confirms the "theorem" under the subsidiary condition s. Chou and Yang now state, "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 opinion, 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, for example, a lexicographic ordering based on

$$\underbrace{y_1 < y_4 < y_5}_{\text{independent variables}} < \underbrace{y_2 < y_3}_{\text{dependent variables}}$$

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 [KP2] 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

$$\{b_1 = y_4y_3 - y_5y_2,\ b_2 = y_5^2y_2 + y_4^2y_2 - y_1y_4^2,$$

$$b_3 = y_3^2 + y_2^2 - y_1y_2,\ b_4 = y_5y_3 + y_4y_2 - y_1y_4\}$$

as a basis for N_P.

In step (2) we detect that $b_3 \notin \text{radical}(h_1,h_2)$, but there exists no possible subsidiary condition involving only the independent variables y_1,y_4,y_5.

Note added in proof. In his recent Ph.D. thesis [KU] B. Kutzler has reformulated the geometry theorem proving problem. In his formulation one does not have to search for subsidiary conditions and the problem is a pure decision problem. Nevertheless, for certain applications (as, for example, incorrectly stated theorems) the "finding" problem is still of importance.

ACKNOWLEDGMENTS

Work reported herein has been supported by the Österreichische Forschungsgemeinschaft and by the Austrian Fonds zur Förderung der wissenschaftlichen Forschung, Projekt Nr. P6763.

REFERENCES

[BKR] M. Ben-Or, D. Kozen, and J. Reif, "The complexity of elementary algebra and geometry" *Proceedings of the 16th ACM Symposium on Theory of Computing*, 457–464 (1984).

[B1] B. Buchberger, "Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal." Ph.D. dissertation, University of Innsbruck, Austria (1965).

[B2] B. Buchberger, "Gröbner bases: An algorithmic method in polynomial ideal theory", in: *Multidimensional Systems Theory*, (N.K. Bose, ed.), pp. 184–232. D. Reidel, Dordrecht, 1985.

[C1] S.-C. Chou, "Proving and discovering theorems in elementary geometry using Wu's method," Ph.D. Thesis, Dept. of Mathematics, University of Texas, Austin (1985).

[C2] S.-C. Chou, *Mechanical Geometry Theorem Proving*. D. Reidel, Dordrecht, 1988.

[CS] S.-C. Chou and W.F. Schelter, "Proving geometry theorems with rewrite rules," *Journal of Automated Reasoning* 2:253–273 (1986).

[CY] S.-C. Chou and J.-G. Yang, "On the algebraic formulation of certain geometry statements and mechanical geometry theorem proving", *Algorithmica*, 4:237–262 (1989).

[CO] G.E. Collins, "Quantifier elimination for real closed fields by cylindrical algebraic decomposition", *Proceedings of the 2nd GI Conference on Automata Theory and Formal Languages*, LNCS 35, 134–183. Springer-Verlag, Berlin, 1975.

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

[GI] P. Gianni, B. Trager, and G. Zacharias, "Gröbner bases and primary decomposition of polynomial ideals", *Journal of Symbolic Computation* 6(2–3):149–167 (1988)

[GR] D.Yu. Grigor'ev, "Complexity of deciding Tarski algebra", *Journal of Symbolic Computation* 5(1–2):65–108 (1988).

[HI] D. Hilbert, *Grundlagen der Geometrie*. Teubner Verlag, Stuttgart, 1977.

[KL] M. Kalkbrener, "Application of Gröbner bases: Solution of algebraic equations and decomposition of radicals," Diplomarbeit, RISC-Linz, J. Kepler Univ. Linz, (1987).

[KA] A. Kandri-Rody, "Effective methods in the theory of polynomial ideals," Ph.D. thesis, Rensselaer Polytechnic Institute, Troy, NY (1984).

[KP1] D. Kapur, "Geometry theorem proving using Hilbert's Nullstellensatz," *Proceedings of SYMSAC'86*, 202–208 (B.W. Char, ed.). ACM, New York, 1986.

[KP2] D. Kapur, "Using Gröbner bases to reason about geometry problems," *Journal of Symbolic Computation* 2(4):399–408 (1986).

[KMH] H. Kobayashi, S. Moritsugu, and R.W. Hogan, "On radical zero-dimensional ideals," *Journal of Symbolic Computation* 8(6):545–552 (1988).

[KR] H. Kredel, "Primary ideal decomposition," *Proceedings EUROCAL'87, Leipzig* (1987).

[KU] B. Kutzler, "Algebraic approaches to automated geometry theorem proving," Ph.D. thesis, Institut für Mathematik, J. Kepler Univ., Linz, Austria (1988).

[KS1] B. Kutzler and S. Stifter, "Automated geometry theorem proving using Buchberger's algorithm," *Proceedings of the 1986 Symposium on Symbolic and Algebraic Computation (SYMSAC'86)*, 209–214 (B.W. Char, (ed.)), ACM, New York, 1986.

[KS2] B. Kutzler and S. Stifter, "On the application of Buchberger's algorithm to automated geometry theorem proving", *Journal of Symbolic Computation* 2(4):389–397 (1986).

[MM] H.M. Möller and F. Mora, "New constructive methods in classical ideal theory", *Journal of Algebra* 100(1):138–178 (1986).

[RI] J.F. Ritt, *Differential Algebra*, AMS Colloquium Publications, New York, 1950.

[TA] A. Tarski, *A Decision Method for Elementary Algebra and Geometry*. University of California Press, Berkeley (1948) [2nd ed. (1951)].

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

[WI] F. Winkler, "Solution of equations I: Polynomial ideals and Gröbner bases," in: *Computers in Mathematics* (D.V. Chudnovsky and R.D. Jenks, eds.), 383–407. Marcel Dekker, New York, 1990.

[WB] F. Winkler, B. Buchberger, F. Lichtenberger, and H. Rolletschek, "An algorithm for constructing canonical bases of polynomial ideals," *ACM Transactions on Mathematical Software* 11(1):66–78 (1985).

[WU1] Wu Wen-tsün, "On the decision problem and the mechanization of theorem proving in elementary geometry," *Scientia Sinica* 21:157–179 (1978).

[WU2] Wu Wen-tsün, "Basic principles of mechanical theorem-proving in elementary geometry", *Journal of Systems Science and Mathematical Sciences* 4(3):207–235 (1984).