Geometry Theorem Proving Using Hilbert's Nullstellensatz

– Preliminary Version –

Deepak Kapur
Computer Science Branch
Corporate Research and Development
General Electric Company
Schenectady, NY

1. Introduction

The theory of elementary algebra and elementary geometry was shown to be decidable by Tarski using a quantifier elimination technique in the 1930's [26]. Subsequently, Tarski's decision algorithm was improved by others – notably among them Seidenberg [25], Monk [23], and Collins [12], and recently by Ben–Or et al [4]. These methods are algebraic and are based on translating geometry statements into first-order formulae using the operations 0, 1, −1, +, *, ≥, = of an ordered field with variables ranging over real numbers. Among these decision procedures, Collins's method based on cylinderical algebraic decomposition technique is, to our knowledge, the only decision procedure implemented so far; see [2, 3] for details.

Gelernter [13] investigated automating geometric reasoning using the synthetic approach to geometry. He characterized various geometric concepts including parallel line, vertical angle, collinear, congruence, equilateral triangle etc., by axioms and rules of inference. These axioms and rules of inference along with geometric construction techniques were used to prove some plane geometry theorems; see also [14].

Recently, Wu Wenjun [28] has revived interest in automated geometry theorem proving by showing how a subclass of geometry theorems can be proved using a fairly simple and elegant algebraic method. This method has been implemented by Wu in China and Chou at the University of Texas independently. Both Wu [28, 29] and Chou [9, 10] have extensively experimented with the method, and have been successful in proving many non–trivial theorems in geometry. Chou [9], in particular, has proved over 200 theorems in Euclidean and non–Euclidean geometries.

In Wu's approach, a geometry statement of the form – a finite set of hypotheses implying a conclusion, is considered. Hypotheses are polynomials expressing geometric relations with a subset of variables as parameters, and the conclusion is also a polynomial stating a geometric relation to be derived. Unlike Tarski, Seidenberg, Monk, Collins and Ben–Or et al's methods, the variables in Wu's method range over an algebraically closed field. So, Wu considered algebraic geometry instead of elementary geometry.

In Wu's formulation, proving a geometry formula is equivalent to the problem of checking whether the set of common zeros in an algebraically closed field of the hypothesis polynomials is contained in the set of zeros of the conclusion polynomial. However, if a given geometry formula is found to be not a theorem, Wu showed how to find a finite set of polynomial inequations (negations of polynomial equations) that rule out some common zeros of the hypothesis polynomials such that the remaining subset of common zeros of the hypothesis polynomials is indeed a subset of the zeros of the conclusion polynomial. Such polynomial inequations are called *non–degenerate conditions* by Wu and Chou; they are also called *subsidiary conditions* in this paper.

Even though for elementary geometry one is interested in ensuring that the set of *real common zeros* of the hypothesis polynomials is contained in the set of real zeros of a conclusion polynomial, Wu observed that for many geometry statements, it often suffices to consider the complex zeros instead of the real zeros. If a geometry formula is found to be a theorem by Wu's approach, then it is a theorem when interpreted over reals, but the converse does not hold. Wu's method is not complete in Tarski's sense even for a subclass of geometry theorems considered by Wu. It evidentally is a good heuristic for deciding geometry statements when interpreted over reals since Wu and Chou have been successful in automatically proving many non–trivial theorems.

In this paper, geometry statements in Wu's sense, henceforth called *Wu's geometry*, are considered and an alternative approach for proving such geometry theorems is proposed. This approach is based on Hilbert's Nullstellensatz and is complete in Wu's sense but is incomplete in Tarski's sense. Unlike Wu's approach, the proposed approach does not use factorization of polynomials over successive extension fields of a base field, which is generally considered a difficult problem (cf. [9], pp. 278–279). Further, we believe that subsidiary conditions, which are an integral part of a geometry statement, are handled in a natural way in the proposed approach. We think that subsidiary conditions can be stated a priori in Wu's approach also, but this, to our knowledge, has not be tried by Wu or Chou.

© 1986 ACM 0-89791-199-7/86/0700-0202 75¢

In the proposed approach, a geometry statement is translated to checking whether a finite set of polynomials does not have a common zero, or equivalently, has no common solution in an algebraically closed field. Since it follows from Hilbert's Nullstellensatz that a set of polynomials has a common zero if and only if their ideal is not the unit ideal, to prove a geometry statement it is sufficient to check whether an equivalent finite set of polynomials generates the unit ideal. The Gröbner basis method [5, 6, 7, 8, 18] is used for this check. Kutzler and Stifter at University of Linz [22] and Chou and Schelter at Univesity of Texas [11] have also independently investigated the use of the Gröbner basis method for proving geometry theorems; their works are discussed later in the paper.

This paper is a condensed version of [21]. An interested reader may consult [21] for further details and explanation, as well as for examples and precise statements of geometry theorems considered here.

2. Wu's Geometry

Consider a field k of characteristic zero, for example, the field of rationals; let K be an algebraically closed field containing k [27]. Let +, *, 0, 1, -1 be the operations of K. Consider the set of all quantifier-free formulae constructed using these operations, the equality predicate and boolean connectives, in which the variables range over K. Let this language be W, after Wu, and such a geometry *Wu's geometry.*

2.1 Wu's Method

A geometry statement considered by Wu [28, 30] is of the following type:

Given a finite set of hypotheses expressed as polynomials, say $\{ h_1, \ldots, h_i \}$, over k, where indeterminates are coordinates of points in a geometry statement and some indeterminates are chosen to be *parameters* (also called *independent variables* whereas the remaining indeterminates are called *dependent variables*), determine subsidiary conditions, if any, in the form of negations of polynomial equations, under which a given conclusion polynomial c vanishes at the zeros in K of $\{ h_1, \ldots, h_i \}$.

Wu developed a method which can be used to derive these conditions for a geometry statement. Chou [9, 10] further developed Wu's method and, based on his extensive implementation experience with Wu's method, Chou has developed a way to interpret the subsidiary conditions geometrically.

Wu's method is reported to be complete for an algebraically closed field [30]. However, the major stumbling block in his method is the need to factorize polynomials over successive extension fields of a base field in obtaining irreducible triangular form(s) of hypothesis polynomials. Chou has developed an algorithm for factoring polynomials in which indeterminates have at most degree two [9, 10]; he has found his factoring algorithm to be quite adequate and efficient for proving plane geometry theorems. Factoring arbitrary polynomials over successive extension fields is generally considered a difficult problem (cf [9], pp. 278-279); as a result, theorems which need factorization of arbitrary polynomials over successive extenstion fields in Wu's method are likely to be not easily handled.

3. Method Based on Hilbert's Nullstellensatz

A geometry statement considered in the proposed approach is of the following kind:

$$\forall x_1, \ldots, x_n \in K, \ [[\ h_1 = 0 \textit{ and } \ldots \textit{ and } h_i = 0 \textit{ and } s_1 \neq 0 \textit{ and } \ldots \textit{ and } s_j \neq 0] \Rightarrow [\ c = 0\ ]\ ] \quad \text{(i)}$$

where h's are polynomials corresponding to geometry relations in the hypothesis of a geometry statement, s's are polynomials corresponding to degenerate cases, and c is a polynomial corresponding to a geometry relation stated as the conclusion of the geometry statement. Each of h's, s's, and c are in $k[x_1, \ldots, x_n]$.

The problem is to decide whether the formula (i) is a theorem or not. This problem is the same as checking whether the zeros in K of c include all the zeros of $\{h_1, \ldots, h_i\}$, on which s_1, ..., and s_j do not vanish.

Definitions: A polynomial equation $p = 0$, where $p \in k[x_1, \ldots, x_n]$, is *satisfiable* (or *consistent* or equivalently, *p has a solution*) iff there exist $v_1, \ldots, v_n$ in K such that $p(x_1 \leftarrow v_1, \ldots, x_n \leftarrow v_n)$, the result of substituting $v_1, \ldots, v_n$ for $x_1, \ldots, x_n$, respectively, in p, evaluates to 0. An equation $p = 0$ is *unsatisfiable* (or *inconsistent*) otherwise. Similarly, a polynomial inequation $p \neq 0$ is *satisfiable* if and only if there exist $v_1, \ldots, v_n$ in K such that $p(x_1 \leftarrow v_1, \ldots, x_n \leftarrow v_n)$ does not evaluate to 0; $p \neq 0$ is *unsatisfiable* otherwise. Given a set S of polynomial equations and inequations in $k[x_1, \ldots, x_n]$, S is *satisfiable* (or *consistent* or equivalently, *S has a common solution*) iff there exist $v_1, \ldots, v_n$ in K such that for every polynomial equation $p = 0$ in S, $p(x_1 \leftarrow v_1, \ldots, x_n \leftarrow v_n)$ evaluates to 0, and for every polynomial inequation $p \neq 0$, $p(x_1 \leftarrow v_1, \ldots, x_n \leftarrow v_n)$ does not evaluate to 0. The set S is *unsatisfiable* (or *inconsistent*) otherwise.

The proof-by-contradiction technique is employed for deciding whether the formula (i) is a theorem or not, much like the refutational approach used in resolution-based theorem proving and equational approaches to theorem proving in predicate calculus [16, 20]. It is checked whether the hypotheses including the subsidiary conditions and the negation of the conclusion together are unsatisfiable. Note that unlike Wu's formulation, there is no need to classify variables appearing in a geometry statement into independent variables and dependent variables.

In general, the problem is to decide whether a universally quantified formula in language W is a theorem or equivalently, whether an existentially quantified formula in W is unsatifiable.

Theorem 1: The satisfiability of any quantifier-free formula in the language W is equivalent to the satisfiability of a finite set of polynomial equations.

Proof: This is done by showing how to simulate various boolean connectives by introducing new variables [25]. The satisfiability of $p \neq 0$ is equivalent to the satisfiability of $p\ z - 1 = 0$, where z is a new variable. This construction is similar to the one used in the proof of Hilbert's Nullstellensatz [27]. The satisfiability of $(p_1 = 0 \textit{ or } p_2 = 0)$ is equivalent to the satisfiability of $p_1\ p_2 = 0$, and the satisfiability of $(p_1 = 0 \textit{ and } p_2 = 0)$ is equivalent to the satisfiability of $\{ p_1 = 0,\ p_2 = 0 \}$. From these transformations, it is obvious that the satisfiability of any quantifier-free formula involving boolean connectives is equivalent to the satisfiability of a finite set of polynomial equations. (For instance, convert an arbitrary quantifier-free formula into a conjunctive normal form, and then use the above transformations to obtain a set of polynomial equations). □

3.1 A Decision Procedure for *W*

Using the above theorem, the problem of deciding the satisfiability of a quantifier-free formula in *W* is equivalent to finding whether an equivalent finite set of equations has a solution in *K*. This is a special case of the problem addressed by Hilbert's Nullstellensatz over *K* [27, vol. II, p. 157]. Using Hilbert's Nullstellensatz, it follows that

Theorem 2: The validity of a geometry statement of the form:

$$\forall x_1, \ldots, x_n \in K, \; [\; [\; h_1 = 0 \text{ and } \ldots \text{ and } h_i = 0 \text{ and } s_1 \neq 0 \text{ and } \ldots \text{ and } s_j \neq 0] \Rightarrow [\; c = 0 \;]]$$

is equivalent to whether the ideal

$(h_1, \ldots, h_i , s_1 \; z_1 - 1, \ldots, s_j \; z_j -1, c \; zz - 1)$ is the unit ideal, where $h_1, \ldots, h_i , s_1, \ldots, s_j , c \in k[x_1, \ldots, x_n]$, and $z_1, \ldots, z_j$, zz are distinct variables different from $x_1, \ldots, x_n$.

So, the validity of a formula in Wu's geometry reduces to checking whether the ideal generated by an equivalent finite set of polynomials is the unit ideal. The problem of checking whether an ideal generated by a finite set of polynomials is the unit ideal or equivalently whether a finite set of polynomials has a common zero in an algebraically closed field is known to be decidable and co-NP-hard [1]. This gives us a complete decision procedure for universally quantified formulae in Wu's geometry. Section 4 addresses the problem of checking whether a given basis generates the unit ideal.

3.2 Equivalence of Geometry Statements in Wu's Formulation and our Formulation

Let *Zeros*($\{ f_1, \ldots, f_i \}$) be the set of all common zeros in *K* of $f_1, \ldots, f_i$; this set is also called the *algebraic variety* or *algebraic manifold* defined by $\{ f_1, \ldots, f_i \}$.

A: *Given a finite set of hypothesis polynomials* $\{ h_1, \ldots, h_i \}$, *and a conclusion polynomial c, are Zeros(* $\{ h_1, \ldots, h_i \}$*)* $\subseteq$ *Zeros(* $\{ c \}$ *)?*

In our formulation, the same geometry statement is:

B: *Given a finite set of hypothesis polynomials* $\{ h_1, \ldots, h_i \}$, *and a conclusion polynomial c,* is *the following statement valid?*

$\forall x_1, \ldots, x_n \in K$, $[[\; h_1 = 0$ *and* ... *and* $h_i = 0] \Rightarrow [\; c = 0 \;]]$. *The validity of this formula is equivalent to the unsatisfiability of* $\{ h_1 = 0, \ldots, h_i = 0, c \; zz = 1 \}$, *where zz is a new variable not appearing in* $h_1, \ldots, h_i$ *and c, i.e., whether Zeros(*$\{ h_1, \ldots, h_i , c \; zz -1 \}$*) is empty.*

Theorem 3: Formulations **A** and **B** above are equivalent.

See [21] for a proof.

Wu and Chou have argued that a geometry statement is often valid only if certain degenerate conditions are ruled out; such conditions are often not clearly stated but are implicit in a problem statement such as certain points being distinct, certain points not being collinear, a triangle or a circle being non-trivial, etc. Deriving such subsidiary conditions under which a geometry statement is a theorem, is considered by them as a crucial feature of their methods. Consider a geometry problem formulation considered by Wu and Chou, which is a generalization of the formulation **A** above.

A': *Given a finite set of hypothesis polynomials* $\{h_1, \ldots, h_i \}$, *and a conclusion polynomial c, find* $s_1, \ldots, s_j$, *such that*

($Zeros(\{ h_1, \ldots, h_i \}) - Zeros(\{ s_1 , \ldots, s_j \}))$ $\subseteq$ *Zeros(* $\{ c \}$*).*

If a geometry statement under consideration is not a theorem and if formulation **B** is used, as is the case in the proposed method, the ideal generated by the polynomials corresponding to the geometry statement is not the unit ideal. Equivalently, the set of hypothesis polynomials of a given geometry statement has a common zero which is not a zero of the conclusion polynomial. In Section 5, a method for examining the structure of the ideal generated by the polynomials corresponding to the geometry statement is discussed. This method is used to obtain subsidiary conditions such that the original geometry statement with these subsidiary conditions is then a theorem.

3.3 Incompleteness of Wu's Method and the Proposed Method in Tarski's Sense

As the following example provided by Singer [private comm., Sept. 1984] illustrates, both Wu's method and the method discussed in this paper are incomplete in Tarski's sense as they consider complex zeros in contrast to Tarski's method which considers real zeros.

$$\forall x, y, x^2 + y^2 = 0 \Rightarrow [\; x = 0 \text{ and } y = 0 \;].$$

The above formula is a theorem if *x* and *y* are assumed to range over reals. However, the above is not a theorem if *x* and *y* are assumed to range over *K*. If Wu's method is used, the hypothesis polynomial is already in triangular form (assuming *x* > *y*), and the conclusion polynomials cannot be pseudo-divided. The above formula is not a theorem by the proposed method either, as the polynomials

$$x^2 + y^2 = 0 \;,\; (x \; z_1 - 1) \; (y \; z_2 - 1) = 0$$

do have a common complex zero. However, there is no common real zero.

4. Automated Geometry Theorem Proving

The validity of a geometry statement in Wu's geometry is equivalent to checking whether the ideal generated by a finite set of polynomials is the unit ideal.

4.1. Checking for the Unit Ideal

There are many methods for deciding whether a finite set of polynomials generates the unit ideal; this is called the *triviality problem of polynomial ideals* in [1]. In this paper, the use of the Gröbner basis method [5, 6, 7, 8, 18] is investigated for this problem. Other methods worth investigating are (i) Hermann's method [15], (ii) a method based on combining elimination, resultants and S-polynomials ala Gröbner basis [24], (iii) Wu's method based on triangulation.

4.1.1 Factoring is Essential in Wu's method

If Wu's method is to be used for deciding whether an ideal generated by a set of polynomials is the unit ideal, factorization of polynomials over successive extension fields of a base field is essential in the triangulation procedure. The need for factorization in Wu's method is illustrated by a following simple example due to Narendran [Private communication, Oct. 1985]:

$p_1 = x^2 + 2x + 1, \; p_2 = (x+1)y^2 + x$

It is easy to see that the ideal generated by p_1 and p_2 is the unit ideal; this can be tested also using the Gröbner basis method. However, the two polynomials are in triangular form under the ordering $x < y$. This shows that it is not just sufficient to bring the polynomials in triangular form to check whether a set of polynomials generate the unit ideal. The polynomial p_1 is factorizable, i.e., $p_1 = (x+1)^2$. So, if the problem is decomposed considering each of the factors (in this case, the two factors are identical), one gets $p_1' = (x+1)$. The polynomial p_1' simplifies p_2, giving 1 as the triangular form.

4.2 Gröbner Basis of a Polynomial ideal

The concept of a Gröbner basis was introduced by Buchberger [5, 6] for deciding the ideal membership problem for polynomial ideals over a field, and other related problems. A polynomial is viewed as a rule for simplifying other polynomials. Since then, this concept has been extensively studied and extended to other algebraic structures; see [8, 18] for details.

Theorem *(Buchberger)*: A Gröbner basis of the unit ideal must include 1.

4.3 Using the Gröbner Basis Method for Geometry Theorem Proving

The proposed method is illustrated on a simple example due to Mundy which can be done by hand. For more examples, the reader may consult [21].

Example: Given three lines such that *AB* is perpendicular to *AC* and *CD* is perpendicular to *AC*, prove that *AB* is parallel to *CD*; see Figure 1 below.

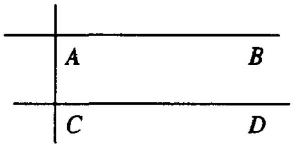

Figure 1.

Set $A = (0, 0)$, $B = (x1, y1)$, $C = (x3, y3)$, $D = (x2, y2)$. The hypothesis polynomial equations are:

1. $y1\, y3 = -x1\, x3$;;; *AB is perpendicular to AC*
2. $y3(y2 - y3) = -(x2 - x3)x3$;;; *CD is perpendicular to AC*

The subsidiary condition is that points *A* and *C* be distinct, i.e., $x3 \neq 0$ *or* $y3 \neq 0$. By introducing new variables *z1* and *z2*, the above transforms to

3. $(x3\, z1 - 1)\,(y3\, z2 - 1) = 0.$

Polynomial equation for the conclusion is

4. $y1\,(x2 - x3) = x1\,(y2 - y3)$;;; *AB and CD are parallel.*

And, its negation translates, after introducing a new variable *zz1*, to

5. $(y1\,(x2 - x3) - x1\,(y2 - y3))\, zz1 - 1 = 0.$

The Gröbner basis of the above polynomials is 1, which implies that under the condition that *A* and *C* are distinct points, the theorem holds. In [21], some of the steps in the computation are illustrated.

The method used for proving geometry theorems is:

Method 1: Given hypotheses $h_1, \ldots, h_i$, degenerate cases $s_1, \ldots, s_j$, and a conclusion c :

$$1 \in Gr\ddot{o}bner(\{h_1, \ldots, h_i, s_1\ z_1 - 1, \ldots, s_j\ \ z_j - 1, c\, zz - 1\},$$
$$Q[x_1, \ldots, x_n, z_1, \ldots, z_j, zz])?$$

yes: return *theorem*
no: return *falsifiable*

end.

The function *Gröbner* above takes a finite set of polynomials and a polynomial ring from which these polynomials are taken as arguments, and computes a Gröbner basis of the ideal specified by the input basis. The reader may consult [7, 8, 18] for algorithms for computing a Gröbner basis.

Table I. Time Needed to Prove Theorems

Theorem	Time (seconds)
Centroid	.7
Ceva's	20.9
Secants	9.6
Equidistant Secants	.2
Simson	13.7
Pappus	3.0
Square	.3
Tangent Circle	1.5
Peripheral Angle	6.5
Altitudes	.4
Desargues	1.2
Nine Point Circle	12
Isosceles Midpoint	6.4
Pentagon	.05
Tetraeder	5.2
Pappus's Dual	6.9
Quadrangle in R^2	.45
Quadrangle in R^3	.7
Gauss	.2
Pascal	640
Brahmagupta	1.1
Wang	19.6
Butterfly	25.1

The above method was used to prove a number of geometry theorems including Simson's theorem, Pascal's theorem, Pappus's theorem, Desargues's theorem, nine-point circle theorem, butterfly theorem, and Gauss's theorem; see [21] for precise statements of these theorems. An implementation of the Gröbner basis algorithm for the polynomial rings over the integers [18] and rationals [8] developed by Richard Harris at General Electric Corporate Research and Development, was used for this purpose. This implementation incorporates optimizations for not considering certain critical pairs proposed by Buchberger [7] and Kapur et al. [19], and it supports both lexicographic and degree ordering on terms. The implementation runs on a Symbolics 3640 Lisp machine. The above table gives computation times on some representative geometry theorems taken from [9, 10, 11, 22]. The Gröbner basis computation for these theorems was performed using the degree ordering as that was found to be generally much faster than the pure lexicographic ordering.

Based on timings given for some of these theorems in [11], it appears that Chou's implementation of Wu's method is much faster than the proposed method.

4.4 Related Work on the Use of the Gröbner Bases for Geometry Theorem Proving

Kutzler and Stifter [22] have independently investigated the use of the Gröbner basis method for geometry theorem proving. Their method is based on checking whether the conclusion polynomial is in the ideal generated by the hypothesis polynomials; they compute the Gröbner basis of polynomials over $Q(u_1, ..., u_d)$, where $u_1, ..., u_d$ are parameters in Wu's sense. Polynomials in $u_1, ..., u_d$, that are needed to be non-zero in checking whether the conclusion polynomial is in the ideal of hypothesis polynomials are produced as the subsidiary conditions by their method.

Chou and Schelter [private communication, July 1985] studied the use of the Gröbner basis method for checking whether a conclusion polynomial is in the ideal generated by hypothesis polynomials in triangular form and subsidiary conditions obtained from the triangulation method. Recently, Chou and Schelter [11] have also been using a Gröbner basis of polynomial ideals over $Q(u_1, ..., u_d)$ for checking whether the conclusion polynomial is in the ideal of hypothesis polynomials under certain conditions. Their method also produces subsidiary conditions which are polynomials required to be non-zero in generating a Gröbner basis and simplifying a conclusion polynomial. They compared the Gröbner basis approach with Wu's method on 80 examples and found Wu's method to be faster than the Gröbner basis approach.

The approaches pursued by Kutzler and Stifter as well as Chou and Schelter are based on checking whether a conclusion polynomial is in the ideal generated by hypothesis polynomials under subsidiary conditions. This is a first approximation to checking whether the conclusion polynomial is in the radical of the hypothesis polynomials; however, as shown by their results, even this first approximation works on many examples. These approaches are incomplete. For completeness, if the conclusion polynomial is not in the ideal generated by the hypothesis polynomials, one needs to successively examine powers of the conclusion polynomial for membership. Chou and Schelter have also reported results based on an approach very similar to ours, but they have not investigated it in detail.

The check for the triviality of an ideal is a special case of the check for the ideal membership problem. The theoretical complexity of the ideal membership problem is obviously at least as much as the theoretical complexity of the triviality problem. Further, if a polynomial p simplifies to 0 using a basis, then using the same basis and using at most one more reduction, the polynomial $p\ z - 1$, where z does not appear in p, reduces to -1. Thus, a suitable implementation of the triviality check should be at least as fast as the membership check for ideals. This along with the fact that the method based on Hilbert's Nullstellensatz is complete for Wu's geometry are our reasons for investigating the proposed approach.

5. Deducing Subsidiary Conditions

In case a geometry statement is not a theorem, it is possible, just like in Wu's approach, to derive using the proposed approach, the subsidiary conditions such that if they are included as part of the original geometry statement, it becomes a theorem. Although the proposed approach is quite inefficient as compared to Wu's approach, subsidiary conditions found using it are often simpler and weaker than the ones reported using Wu's method [9] or those reported in [11] and [22] using the Gröbner basis approach.

For instance, for the example discussed in Section 4, if a Gröbner basis of the hypothesis polynomials and the polynomial corresponding to the negation of the conclusion is computed without the subsidiary condition, the result does not include 1. Instead, there appear $x3$, $y3$, and other polynomials in the Gröbner basis. This implies that the hypothesis polynomials indeed have common zeros which are not zeros of the conclusion polynomial; these zeros are $x3 = 0$, $y3 = 0$, and suitably chosen values of the remaining varibles. Further, these zeros are real zeros, suggesting that the above is a theorem only when such zeros are ruled out, i.e., when $x3 \neq 0$ *or* $y3 \neq 0$, which is the condition that A and C are distinct points thus making AC indeed determine a line.

In contrast, if Wu's method is used for this example, we obtain stronger conditions. If we partition the variables such that $y1$ and $y2$ are dependent variables, then the hypothesis polynomials are already in triangular form. The conclusion polynomial can be pseudo-divided to 0 under the condition that $y3 \neq 0$. This condition is sufficient as imposing this condition would make points A and C distinct. However it is too strong. If instead, we choose $x1$ and $x2$ as dependent variables, then again, the hypothesis polynomials are still in triangular form with respect to this choice of variables. The conclusion polynomial can be pseudo-divided to 0 under the condition that $x3 \neq 0$, which is still too strong.

If any of the approaches in [11, 22] based on computing Gröbner basis on $Q(u_1, ..., u_d)$ is used, the conditions obtained are too strong then also. For instance, the two hypothesis polynomials of the example above constitute a Gröbner basis over $Q(x3, y3, x1, x2)$; the conclusion polynomial simplifies to 0 under the condition that $y3 \neq 0$, which is stronger than the condition that points A and C be distinct. Similarly, the two hypothesis polynomials of the example above constitute a Gröbner basis over $Q(x3, y3, y1, y2)$; the conclusion polynomial simplifies to 0 under the condition that $x3 \neq 0$.

For Pappus's theorem (example 3 in [9]), when a Gröbner basis is computed of the hypothesis polynomials along with the polynomial corresponding to the negation of the conclusion without the subsidiary conditions, the result includes

$$x1\ x4,\ x2\ x5,\ x3\ x6,\ x1\ x2\ x3,\ x4\ x5\ x6$$

as polynomials, among others. The subsidiary condition under which the theorem holds is a disjunction of the following conditions: (i) $x1\ x4 \neq 0$, i.e., points $A1$ and $B1$ are distinct, (ii) $x2\ x5 \neq 0$, i.e., $A2$ and $B2$ are distinct, (iii) $x3\ x6 \neq 0$, i.e., $A3$ and $B3$ are distinct, (iv) $x1\ x2\ x3 \neq 0$, i.e., neither of $A1$, $A2$, and $A3$ is the point of intersection of lines $A1A2A3$ and $B1B2B3$, (v) $x4\ x5\ x6 \neq 0$, i.e., neither of $B1$, $B2$ and $B3$ is the point of intersection of lines $A1A2A3$ and $B1B2B3$. For the square example, (example 4 in [9]), the condition found by this method is simply that the square have a non-zero side. For the triangle altitudes theorem (example 5 in [9]), the subsidiary condition found is $x3 \neq 0$.

Geometry problems considered in this case have the following structure:

Given a consistent set of hypotheses $\{h_1 = 0, ..., h_i = 0\}$, and a conclusion $c = 0$ such that $c \notin k$, find s's, if any, such that

(i) $\forall\, x_1, \ldots, x_n \in K$, $[\,[\, h_1 = 0$ *and* ... *and* $h_i = 0] \Rightarrow$ $[\, s_1 = 0$ *or* ... *or* $s_j = 0\,]\,]$, is not a theorem, and

(ii) $\forall\, x_1, \ldots, x_n \in K$, $[[\, h_1 = 0$ *and* ... *and* $h_i = 0$ *and* $s_1 \neq 0$ *and* ... *and* $s_j \neq 0] \Rightarrow [c = 0]]$, is a theorem or equivalently, *Zeros*($\{ h_1, \ldots, h_i, s_1\ z_1 - 1, \ldots, s_j\ z_j - 1, c\ zz - 1 \}$) is empty.

If for a given geometry problem, a Gröbner basis of the ideal $(h_1, \ldots, h_i, c\ zz - 1)$ does not include 1, which implies that $c \notin \text{Radical}(h_1, \ldots, h_i)$, the radical ideal of $(h_1, \ldots, h_i)$, then any polynomial $p \in k[x_1, \ldots, x_n]$ from the Gröbner basis such that p is not a consequence of the hypotheses (i.e., $p \notin \text{Radical}(h_1, \ldots, h_i)$), is a candidate for stating degenerate cases which must be avoided for the theorem to hold. One can pick a 'simplest' such candidate (in fact, a set of polynomials) from the Gröbner basis for this purpose.

The following theorem serves as the basis of this approach (Method 2 below) for deducing degenerate cases.

Theorem 4: Let $\{ h_1 = 0, \ldots, h_i = 0 \}$ be a consistent set of hypotheses, and $c = 0$ where $c \notin k$, be a conclusion, such that there is a polynomial $p \in k[x_1, \ldots, x_n]$ and $p \notin \text{Radical}(h_1, \ldots, h_i)$ but $p\ c \in \text{Radical}(h_1, \ldots, h_i)$. Let *GB* be a Gröbner basis of $(h_1, \ldots, h_i, c\ zz - 1)$ under a lexicographic ordering on terms in which $zz >$ other variables, where zz is an indeterminate different from $x_1, \ldots, x_n$. Then there exists a polynomial $q \in GB$ not involving zz such that

(i) $q \notin \text{Radical}(h_1, \ldots, h_i)$,

(ii) $s_1, \ldots, s_j$ are the irreducible factors of q, and

(iii) $q\ c \in \text{Radical}(h_1, \ldots, h_i)$, thus implying

$\forall\, x_1, \ldots, x_n \in K$, $[[\, h_1 = 0$ *and* ... *and* $h_i = 0$ *and* $s_1 \neq 0$ *and* ... *and* $s_j \neq 0] \Rightarrow [c = 0]]$.

Theorem 4 holds even if p in its statement is restricted to be in $k[x_1, \ldots, x_m]$, where $\{ x_1, \ldots, x_m \}$ is a subset of $\{ x_1, \ldots, x_n \}$.

Proof: Let $J = (h_1, \ldots, h_i, c\ zz - 1)$ and $J' = J \cap k[x_1, \ldots, x_n\}$. Since there is a polynomial $p \in k[x_1, \ldots, x_n]$ such that $p\ c \in \text{Radical}(h_1, \ldots, h_i)$, for some m, $(p\ c)^m \in (h_1, \ldots, h_i)$. It is easy to see that $p^m \in J'$ since $p^m = (\ p\ c\ zz)^m - p^m\ ((c\ zz)^m - 1)$. So, p^m reduces to 0 using polynomials not involving zz in *GB*. There is at least one polynomial among them which is not in $\text{Radical}(h_1, \ldots, h_i)$, as otherwise $p \in \text{Radical}(h_1, \ldots, h_i)$ leading to a contradiction. Call that q. The rest of the proof follows. □

The proposed method is thus complete for deriving subsidiary conditions also in case a given geometry statement is not a theorem.

Method 2: Given hypotheses $h_1, \ldots, h_i$, and a conclusion c satisfying conditions of Theorem 4:

```
{ $g_1, \ldots, g_m$ } := Gröbner({ $h_1, \ldots, h_i$ , $c\ zz - 1$},
                          $Q[x_1, \ldots, x_n, zz]$);
if $g_1 = 1$ then return theorem: no condition needed
   else repeat from $v = 1$ to $m$
        if $g_v \in Q[x_1, \ldots, x_n]$ and $g_v \notin \{ h_1, \ldots, h_i \}$ then
            if $1 \notin$ Gröbner({ $h_1, \ldots, h_i$ , $g_v\ zz - 1$},
                          $Q[x_1, \ldots, x_n, zz]$)
                then theorem under condition $g_v \neq 0$;
        end repeat;
end;
```

The function *Gröbner* above is assumed to return polynomials in a Gröbner basis in ascending order using the lexicographic ordering on terms.

A polynomial selected from a Gröbner basis to state a degenerate case gives a disjunction of polynomial equations, each corresponding to an irreducible factor of the polynomial g_v above. The above method can be easily modified to select in general a set of polynomials from a Gröbner basis instead of a single polynomial; then the conjunction of the formulae corresponding to the polynomials in this set is the degenerate case. Thus in general, this method gives a conjunction of disjunctions of polynomial equations as a degenerate case. In general, there are two types of degenerate cases found: (i) those corresponding to geometrically degenerate cases, and (ii) those expressing common complex zeros of the hypotheses which are not zeros of the conclusion. Developing a good method to distinguish between these two types of degenerate cases is an interesting open research problem.

Conditions thus obtained are usually simpler and weaker than those obtained using Wu's method because for a fixed classification of variables into independent and dependent variables, there exist many triangulation forms and different triangulation forms give rise to different subsidiary conditions. Further, variables can be classified into independent and dependent variables in more than one way. As discussed above about the example, different choice led to different subsidiary condition. In contrast to this, a reduced (minimal) Gröbner basis of an ideal is unique once an ordering on polynomial terms is fixed [8]; all the information about the degenerate cases is available from the Gröbner basis. Conditions derived by the proposed method are also simpler and weaker than those obtained using approaches discussed in [11, 22] because if a conclusion polynomial or its power is a member of an ideal generated by the hypothesis polynomials, there is usually more than one way to simplify that polynomial to zero with respect to its Gröbner basis. One sequence of simplifications of a polynomial with respect to its Gröbner basis may lead to simpler conditions as compared to another sequence of simplifications with respect to the same Gröbner basis. The weakest condition in this way is the disjunction of conditions obtained for every simplification sequence.

In [21], a table is given with computation times for deducing subsidiary conditions for most geometry problems of Table I above, along with an English description of the subsidiary conditions. The table is not reproduced here because of lack of space.

It was observed in practice that computing a Gröbner basis without subsidiary conditions is highly time-consuming on big examples. For all examples, deducing subsidiary conditions took more time than proving a geometry theorem when subsidiary conditions were stated as part of the input. For examples such as the butterfly theorem, Pascal Theorem, their Gröbner bases could not be computed without subsidiary conditions in a reasonable amount of time.

Acknowledgements

I am thankful to Rick Harris, Paliath Narendran, David Cyrluk, Shang-Ching Chou, Hai-Ping Ko, David Musser, and Joe Mundy for their help in this research. I also thank the referees for their suggestions.

References

1. Agnarsson, S., Kandri-Rody, A., Kapur, D., Narendran, P., and Saunders, B. D., "Complexity of Testing whether a Polynomial Ideal is Non-trivial," *Proc. of the 1984 MACSYMA Users' Conf.*, Schenectady, NY, pp. 452-458, July 1984.

2. Arnon, D.S., Collins, G.E., and McCallum, S., "Cylinderical Algebraic Decomposition I: the Basic Algorithm," *SIAM J. of Computing*, Vol. 13 No. 4, pp. 865-877, Nov. 1984.

3. Arnon, D.S., Collins, G.E., and McCallum, S., "Cylinderical Algebraic Decomposition II: An Adjacency Algorithm for the Plane," *SIAM J. of Computing*, Vol. 13 No. 4, pp. 878-889, Nov. 1984.

4. Ben-Or, M., Kozen, D., Reif, J.,"The Complexity of Elementary Algebra and Geometry," *Proc. 16th ACM Symp. on Theory of Computing*, May 1984, pp. 457-464.

5. Buchberger, B., *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal.* (in German) Ph.D. Thesis, Univ. of Innsbruck, Austria, Math., Inst., 1965.

6. Buchberger, B., "An Algorithmic Criterion for the Solvability of an Algebraic System of Equations," *Aequations Mathematical* 4/3, pp. 374-383, 1970.

7. Buchberger, B., "A Criterion for Detecting Unnecessary Reductions in the Construction of Groebner bases," Proc. *EUROSAM 79*, Marseille, June 1979, (W. Ng. ed), LNCS 72, pp. 3-21, 1979.

8. Buchberger, B., "Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory," in *Multidimensional Systems Theory* (ed.N.K.Bose), Reidel, pp. 184-232, 1985.

9. Chou, S.-C., "Proving Elementry Geometry Theorems Using Wu's Algorithm," *Theorem Proving: After 25 years* (eds. Bledsoe & Loveland). *Contemporary Mathematics* Vol. 29, pp. 243-286, 1984.

10. 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.

11. Chou, S.-C. and Schelter, W. F., "Proving Geometry Theorems with Rewrite Rules," Unpublished Manuscript, University of Texas, Austin, Dec. 1985.

12. Collins, G.E., "Quantifier Elimination for Real Closed Fields by Cylinderic Algebraic Decomposition," *Proc. 2nd GI Conf. on Automata Theory and Formal Languages*, Springer-Verlag, LNCS 35, Berlin, pp. 134-183, 1975.

13. Gelernter, H.,"Realization of a Geometry Theorem Proving Machine," in *Computers and Thought* (eds. Feigenbaum & Feldman), pp.134-152, McGraw Hill, 1963.

14. Gilmore, P.C.,"An Examination of the Geometry Theorem Proving Machine," *Artificial Intelligence* Vol. 1, pp. 171-187, 1970.

15. Hermann, G., "Die Frage der endlich vielen Schritte in der Theorie der Polynomideale," *Mathematische Annalen* 95, 736-788, 1926.

16. Hsiang, J., "Refutational Theorem Proving using Term-Rewriting Systems," *Artificial Intelligence*, Vol. 25, No. 3, pp. 255-300, March 1985.

17. Kandri-Rody, A., *Effective Methods in the Theory of Polynomial Ideals.* Ph.D. Thesis, Dept. of Mathematics, Rensselaer Polytechnic Institute, Troy, NY, May 1984.

18. Kandri-Rody, A., and Kapur, D., "Algorithms for Computing the Gröbner Bases of Polynomial Ideals over Various Euclidean Rings," *Proc. of the EUROSAM, '84*, Springer Verlag LNCS 174 (ed. Fitch), Cambridge, England, July 1984.

19. Kapur, D., Musser, D.R., and Narendran, P., *Only Prime Superpositions need be considered for the Knuth-Bendix Completion Procedure.* Unpublished Manuscript, General Electric R&D Center, Schenectady, NY, December 1984.

20. Kapur, D., and Narendran, P., "An Equational Approach to Theorem Proving in First-Order Predicate Calculus," *9th International Joint Conference on Artificial Intelligence*, Los Angeles, Calif., August 1985.

21. Kapur, D., *Geometry Theorem Proving Using Hilbert's Nullstellensatz.* Unpublished Manuscript, General Electric R&D Center, Schenectady, NY, May 1986. (An expanded version of this paper.)

22. Kutzler, B., Stifter, S., "On the Application of Buchberger's Algorithm to Automated Geometry Theorem Proving," to appear in *Journal of Symbolic Computation*.

23. Monk, L.G., *Elementary-Recursive Decision Procedures*, Ph.D. Thesis, Dept. of Mathematics, University of California, Berkeley, 1975.

24. Pohst, M. E., and Yun, D. Y. Y., "On Solving Systems of Algebraic Equations via Ideal Bases and Elimination Theory," *Proc. 1981 ACM Symp. on Symbolic and Algebraic Computation*, pp. 206-211, 1981.

25. Seidenberg, A., "A New Decision Method for Elementary Algebra," *Annals of Mathematics*, Vol. 60 No. 2, pp. 365-374, Sept. 1954.

26. Tarski, A., *A Decision Method for Elementray Algebra and Geometry.* U. of Calif. Press, 1948; 2nd edition, 1951.

27. van der Waerden, B.L., *Modern Algebra*, Vol. I and II, Fredrick Ungar Publishing Co., New York, 1966.

28. Wu, W., "On the Decision Problem and the Mechanization of Theorem Proving in Elementary Geometry," *Scientia Sinica* 21, pp. 150-172, 1978. Also in *Theorem Proving: After 25 years* (eds. Bledsoe & Loveland). *Contemporary Mathematics* Vol. 29, pp. 213-234, 1984.

29. Wu, W., "Some Recent Advances in Mechanical Theorem Proving of Geometries," in *Theorem Proving: After 25 years* (eds. Bledsoe & Loveland). *Contemporary Mathematics* Vol. 29, pp. 235-241, 1984.

30. Wu, W., "Basic Principles of Mechanical Theorem Proving in Geometries," *J. of System Sciences and Mathematical Sciences*, Vol. 4 No. 3, pp. 207-23, 1984.