ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 19, Number 3, Summer 1989

A DECISION METHOD FOR CERTAIN ALGEBRAIC GEOMETRY PROBLEMS

HAI-PING KO AND SHANG-CHING CHOU

ABSTRACT. We present a mathematical theorem in algebraic geometry. The theorem implies a decision method for the membership of the set of all the polynomials which fix a certain type of algebraic variety denoted by V^* by WuWen-tsün. The theorem is a generalized form of similar theorems developed by Ritt, Wu, and the above authors. And the decision procedure is a natural extension of similar decision procedures introduced by Ritt, Wu, and the second author.

Wu Wen-tsün's method of mechanical theorem proving in geometry is complete for certain elementary geometry problems involving equality only. For the corresponding algebraic geometry problem, the method is complete for problems with an algebraically closed field as the associated field, but not complete for the above type of problems with the field of rational numbers ($\mathbf{Q}$) or the field of real numbers ($\mathbf{R}$) as the associated field. As suggested by Wu in 1982, the second author shows a condition for Wu's method to be complete for the above problems with R as associated field. We now show a more general condition for Wu's method to be complete for the above algebraic geometry problems with any field as the associated field.

Background. The algebraic problem to be presented here is extracted from a study of algebraic methods of automated geometry theorem proving.

Research in automated geometry theorem proving has been motivated by such visions as: (1) providing a mathematical tool for education in geometry, (2) studying the basic needs of an intelligent system, and (3) advancing the technology of robotics and computer vision. Proposed methods of automated geometry theorem proving can be classified as either logical or algebraic. For instance, the methods introduced by Tarski [**10**] and Wu Wen-tsün [**12, 13**] are considered as algebraic. The method introduced by Wu Wen-tsün has been considered as a breakthrough success since the time of Tarski. It

Supported by NSF Grant DCR-8503498.
Received by the editors on October 1, 1986 and in revised form on September 2, 1987.

has been demonstrated to be efficient and powerful in a wide range of geometry problems [**1** - **4**].

The algebraic part of Wu Wen-tsün's method of automated geometry theorem proving is a decision problem of the membership in algebraic geometry of the following type of sets:

$$I(V^*(h_1, h_2, \ldots h_s : u_1, u_2, \ldots u_d)).$$

We present a mathematical theorem to extend some theoretical property of Wu's method from algebraically closed fields to arbitrary fields. This extension to the field of real numbers is particularly significant, because Euclidean geometry is a geometry over $\mathbf{R}$ and a geometry which is mostly frequently used in physical sciences. One of this type of extensions is given in [**2**]. Our further extension to arbitrary fields here has significance in theory and an effect of unifying existing results for this type of problem.

The main theorem. Throughout this paper, suppose K is a field and $\overline{K}$ is an extended field of K. Let n be a positive integer and $KK = K[y_1, y_2, \ldots, y_n]$ be the polynomial ring of variables $y_1, y_2, \ldots, y_n$ over K.

DEFINITION 1. [**9**] For a nonempty ideal, say H, of KK, a generic zero of H is a zero of H, say $z = (z_1, z_2, \ldots, z_n)$, in an extended field of K such that, for any polynomial, say g, in KK, if $g(z) = 0$ then g is an element of H.

Let V be the function defined from the power set of KK to the power set of $\overline{K}^n$ by $V(J)$ = the set of all elements, say $(z_1, z_2, \ldots, z_n)$, of $\overline{K}^n$ such that, for all polynomials, say $f(y_1, y_2, \ldots, y_n)$, of J, $f(z_1, z_2, \ldots z_n) = 0$. Let I be the function defined from the power set of $\overline{K}^n$ to the power set of KK by $I(U)$ = the set of all polynomials, say $f(y_1, y_2, \ldots, y_n)$, of KK such that, for all elements, say $(z_1, z_2, \ldots, z_n$, of U, $f(z_1, z_2, \ldots, z_n) = 0$. Here, $V(J)$ is called the (affine) algebraic variety determined by J over $\overline{K}$ and $I(U)$ is called the set of all polynomials which fix U. It is known that all algebraic varieties can be decomposed into irreducible components in a unique manner. Let d

and r be positive integers and $u_1, u_2, \ldots u_d,\ \ x_1, x_2, \ldots x_r$ be variables such that $n = d + r$ and $\{u_1, u_2, \ldots, u_d\}$ and $\{x_1, x_2, \ldots, x_r\}$ together form $\{y_1, y_2, \cdots, y_n\}$. (We limit d and r to be positive integers mainly to simplify our discussion. It is very possible that, with some adjustment, d and r can be actually allowed to be nonnegative integers.) Let $V^*(\cdot; u_1, u_2, \ldots, u_d)$ be the function defined from the power set of KK to the power set of $\overline{K}^n$ by $V^*(J; u_1, u_2, \ldots, u_d) =$ the union of all the irreducible components, say V', of $V(J)$ so that $I(V')$ has a generic zero of form $(u_1, u_2, \ldots, u_d, \overline{x_1}, \overline{x_2}, \ldots, \overline{x_r})$ such that $u_1, u_2, \ldots, u_d$ are algebraically independent over K and $\overline{x_1}, \overline{x_2}, \ldots, \overline{x_r}$ are algebraic over $K(u_1, u_2, \ldots, u_d)$. For convenience, we also denote $V(\{f_1, f_2, \cdots, f_m\})$ simply by $V(f_1, f_2, \ldots, f_m)$, denote $V^*(\{f_1, f_2, \ldots f_m\}; u_1, u_2, \ldots, u_d)$ simply by $V^*(f_1, f_2, \ldots f_m; u_1, u_2, \ldots u_d)$, and denote $I(\{\sigma_1, \sigma_2, \ldots, \sigma_m\})$ simply by $I(\sigma_1, \sigma_2, \ldots \sigma_m)$. For the above types of algebraic varieties, the field K is called the base field and $\overline{K}$ is called the associated field. Given some special type of polynomials $h_1, h_2, \ldots, h_s$ in KK, the main theorem gives a characterization of members of $I(V^*(h_1, h_2, \ldots h_s : u_1, u_2, \ldots u_d))$.

Let prem denote any pseudo remainder, such as that defined in [**6**] and used in [**1**]. A pseudo remainder, prem, here may be considered as a function from $KK \cdot (KK - \{0\}) \cdot \{y_1, y_2, \ldots, y_n\}$ to KK such that if rem=prem(g, f, y), then

$$\text{either rem} = 0 \quad \text{or} \quad \deg(\text{rem}, y) < \deg(f, y)$$

and there exists a polynomial q and a nonzero polynomial I in KK satisfying the following properties:

(1) $I \cdot g = q \cdot f + \text{rem}$;

(2) every prime factor of I is a factor of the leading coefficient of f w.r.t. y.

We extend the above prem to denote, for a pseudo remainder of successive pseudo divisions, as follows: for $m \geq 1, g$ in KK, $f_1, f_2, \ldots, f_m$ in $KK-\{0\}$, and $z_1, z_2, \ldots, z_m$ in $\{y_1, y_2, \ldots, y_n\}$; prem$(g, (f_1, f_2, \ldots f_m), (z_1, z_2, \ldots z_m))$ is defined as

prem(g, f_1, z_1) if $m = 1$, and

prem(prem$(g, (f_2, f_3, \ldots, f_m), (z_2, z_3, \ldots, z_m)), f_1, z_1)$ otherwise.

Given a pseudo remainder function prem, and following the notion of characteristic set introduced in [**9**], we define an R-characteristic set of any set of polynomials as below. (The format of the definition here is given in such a way so that we can have a dicussion without being involved in the notion of chains [**9**]. This does not suggest that the notion of chains can be eliminated in all related problems. The notion of chains has been used to prove theorems such as the Ritt-Wu Principle, which we use and state later in this paper.)

DEFINITION 2. For a set of polynomials, say S, in KK, an R-characteristic set of S is a pair of a finite sequence of polynomials and a finite sequence of variables of form $((p_1, p_2, \ldots, p_r), (x_1, x_2, \ldots, x_r))$ with ≥ 1 such that the p_i's are elements of the radical ideal generated by S, and, either ($r = 1$ and p_1 is a nonzero element of K) or all of the following conditions are satisfied:

(C1) (triangularity) $(p_1, p_2, \ldots, p_r)$ is strictly triangular with respect to
$(x_1, x_2, \ldots, x_r)$, i.e., for all i, p_i is an element of $K[u_1, u_2, \ldots, u_d, x_1, x_2, \ldots, x_i]$ but not an element of $K[u_1, u_2, \ldots, u_d, x_1, x_2, \ldots, x_{i-1}]$.

(C2) (nonzero initials) Let $I_1, I_2, \ldots I_r$ be leading coefficients of $p_1, p_2, \ldots, p_r$ w.r.t. $x_1, x_2, \ldots, x_r$ respectively. Then, for each $i = 2, 3, \ldots, r$, $\mathrm{prem}(I_i, (p_1, p_2, p_{i-1}), (x_1, x_2, \ldots, x_{i-1}))$ is nonzero in KK,

(C3) (zero remainders) For every element, say g, of S, we have prem $(g, (p_1, p_2, \ldots p_r), (x_1, x_2, \ldots, x_r)) = 0$. For convenience, we shall simply call $P = (p_1, p_2, \ldots, p_r)$ an R-characteristic set of S and $(x_1, x_2, \ldots, x_r)$ triangular variables of P. Furthermore, the R-characteristic set P, or $((p_1, p_2, \ldots, p_r), (x_1, x_2, \ldots, x_r))$, is said to be irreducible with $u_1, u_2, \ldots, u_d$ as independent variables if $d \geq 1$, $n = d + r$, $u_1, u_2, \ldots, u_d$ and $x_1, x_2, \ldots, x_r$ together form $y_1, y_2, \ldots, y_n$, and the following condition is satisfied:

(C4) [Ritt-irreducibility] If K_0 is the field $K(u_1, u_2, \ldots u_d)$, then p_1 is a nonzero irreducible polynomial of $K_0[x_1]$, and, for each $i = 2, \ldots, r$, if K_{i-1} is defined as the quotient field $K_{i-1}[x_{i-1}]/\mathrm{Ideal}(p_{i-1})$, then p_i is a nonzero irreducible polynomial of $K_{i-1}[x_i]$.

It is known from the Ritt-Wu Principle [**13**] that, for any nonempty set, say S, of nonzero polynomials, R-characteristic sets exist. Furthermore, if S is a finite set and prem can be evaluated in an algorithmic manner, then there is an algorithmic method to obtain an R-characteristic set of S. This method merely uses a finite sequence of prem operations. We give a statement of the Ritt-Wu Principle as follows:

RITT-WU PRINCIPLE. *Suppose $h_1, h_2, \ldots, h_s$ are nonzero polynomials in KK, $(s \geq 1)$. Then, for any linear ordering on $\{y_1, y_2, \ldots, y_n\}$, say $<$, there exists an algorithm to find an R-characteristic set of form $((f_1, f_2, \ldots, f_r), (x_1, x_2, \ldots, x_r))$ with $x_1 < x_2 < \cdots < x_r$.*

In the above case, if f_1 is an element of K, then $V(h_1, h_2, \ldots, h_s) = V(f_1, f_2, \ldots, f_r)$ is empty. If f_1 is not an element of K and we let I_i be the leading coefficient of f_i w.r.t. x_i, for each $i = 1, 2, \ldots, r$, and $I = I_1 \cdot I_2 \cdot \cdots \cdot I_r$, then $V(h_1, h_2, \ldots, h_s)$ is the disjoint union of $V(f_1, f_2, \ldots, f_r) - V(I)$ and $V(f_1, f_2, \ldots, f_r, I)$. Multiple R-characteristic sets exist. For instance, if $S = \{x + y, x - y\}$ and prem is any pseudo remainder function, then each of the following sequences is an irreducible R-characteristic set of S with (x, y) as its triangular variables: $(x, y), (x, x + y), (x, (x + 1)(x + y))$.

Our main theorem is

THEOREM 1. *Suppose in KK, $S = \{h_1, h_2, \ldots, h_s\}$ $(s \geq 1)$ has an irreducible R-characteristic set, say $((p_1, p_2, \ldots, p_r), (x_1, x_2, \ldots, x_r))$ with $u_1, u_2, \ldots, u_d$ as independent variables. Let H be the ideal generated by $h_1, h_2, \ldots, h_s$ in KK, and $H_1 = \{g : g$ is an element of KK, and $\mathrm{prem}(g, (p_1, p_2, \ldots p_r), (x_1, x_2, \ldots x_r)) = 0\}$. Suppose d is a positive integer and $u_1, u_2, \ldots, u_d$ are variables such that $u_1, u_2, \ldots, u_d$ and $x_1, x_2, \ldots, x_r$ together form $y_1, y_2, \ldots, y_n$. Then H_1 is a prime ideal containing H. Furthermore, if the condition:*

(S1) *$V^* = V^*(h_1, h_2, \ldots h_s; u_1, u_2, \ldots u_d)$ is nonempty is satisfied, then*

(D1) *V^* is an irreducible algebraic variety, $V^* = V(H_1)$ and $H_1 = I(V^*) = I(V(H_1))$, and*

(D2) *for any prime ideal H' in KK, if $H \subseteq H' \subseteq I(V^*)$, then $H' = H_1$.*

This theorem is a generalized form of similar theorems in [**9**, **13**, **8**, **2**, and **7**]. If $\overline{K}$ is algebraically closed, then condition (S1) follows from conditions (C1)-(C4). But in case $\overline{K}$ is not algebraically closed, then (S1) does not necessarily follow.

DEFINITION 3. [**13**] If polynomials $p_1, p_2, \ldots, p_r$, and variables $u_1, u_2, \ldots, u_d$, $x_1, x_2, \ldots, x_r$ satisfy conditions (C1), (C2) and (C4), then a generic point of $P = (p_1, p_2, \ldots, p_r)$ is defined as zero, say $(u_1, u_2, \ldots, u_d, x_1, x_2, \ldots, x_r)$, of $p_1, p_2, \ldots, p_r$ in an extended field of K with $u_1, u_2, \ldots, u_d$ algebraically independent over K.

Also noted in [**7**], a generic point defined here is different from a generic zero defined for ideals in general. It can be proved that if $P = (p_1, p_2, \ldots, p_r)$ satisfies conditions (C1), (C2) and (C4), then any generic point of P is a generic zero of ideal H_1 as defined in the following Lemma.

LEMMA 1. *Suppose in* KK, $\{h_1, h_2, \ldots, h_s\}$ $(s \geq 1)$ *has an irreducible R-characteristic set* $((p_1, p_2, \ldots, p_r), (x_1, x_2, \ldots, x_r))$ *with* $u_1, u_2, \ldots, u_d$ *as independent variables, and condition* (S1) *is satisfied. Let point* $\sigma = (u_1, u_2, \ldots, u_d, x_1, x_2, \ldots, x_r)$ *in* K_r *be a generic point of* $P, H = \mathrm{Ideal}(h_1, h_2, \ldots h_s)$ *in* KK, *and* $H_1 = \{g : g$ *is an element of* KK, and $\mathrm{prem}(g, (p_1, p_2, \ldots, p_r), (x_1, x_2, \ldots, x_r)) = 0\}$. *Then* H_1 *is a prime ideal containing* H, *and* σ *is a generic zero of* H_1. *Furthermore,* g *is an element of* H_1 *if and only if one of the following conditions is satisfied:*

(1) σ *is a zero of* g, *and*

(2) *there exists a polynomial, say* q, *in* $K[u_1, u_2, \ldots u_d]$ *such that* $q \cdot g$ *is an element of* H.

The proof is an obvious extension of the proofs of [**2**; Appendix 2, Theorems 1 & 2] and [**3**, Theorem(9.3)]. □

LEMMA 2. *For a proper prime ideal* H *in* KK, *if* σ *is a zero of* H *of transcendence degree* d *and the transcendence degree of the quotient* *field of KK/H over K is d, then σ is a generic zero of H.*

The proof of this Lemma follows almost directly from [**11**, p. 155]. □

Now we prove Theorem 1. Suppose, in KK, $S = \{h_1, h_2, \ldots, h_s\}$ has an irreducible R-characteristic set, say $((p_1, p_2, \ldots, p_r),\ (x_1, x_2, \ldots, x_r))$ with $u_1, u_2, \ldots, u_d$ as independent variables. Then H_1 is a prime ideal containing H in KK, by Lemma 1. Suppose V^* is nonempty. Let V' be an irreducible component of V^* and $\sigma_0 = (u_1, u_2, \ldots, u_d, \overline{x_1}, \overline{x_2}, \ldots, \overline{x_r})$ be a generic zero of $I(V')$ such that $u_1, u_2, \ldots, u_d$ are algebraically independent over K and $\overline{x_1}, \overline{x_2}, \ldots, \overline{x_r}$ are algebraic over $K(u_1, u_2, \ldots, u_d)$. Since $H \subseteq I(V(H)) \subseteq I(V^*(H)) \subseteq I(V')$, σ_0 is also a zero of H. Because of Lemma 1(2), for every element, say h, of H_1, there exists q in $K[u_1, u_2, \ldots, u_d]$ such that $q{\cdot}h$ is an element of H, thus $q(\sigma_0){\cdot}h(\sigma_0) = 0$. Since the u_i's in σ_0 are algebraically independent, $q(\sigma_0)$ is nonzero, so σ_0 is a zero of h and thus a zero of H_1. But $I(V') = \{g : g \text{ is an element of } KK \text{ and } g(\sigma_0) = 0\}$, and thus $H_1 \subseteq I(V')$. The transcendence degree of the quotient field of $KK/I(V')$ is d and thus the transcendence degree of the quotient field of KK/H_1 over K is greater than or equal to d. But $H \subseteq H_1$ and, in H, $x_1, x_2, \ldots x_r$ are algebraically dependent on $\{u_1, u_2, \ldots, u_d\}$, and thus the transcendence degree of the quotient field of KK/H_1 is less than or equal to d. Therefore, the transcendental degree of KK/H_1 is equal to d. By Lemma 2, σ_0 is also a generic zero of H_1 and $H_1 = I(V')$. This implies $V(H_1) = V'$, $I(V(H_1)) = H_1$, and $V^* = V' = V(H_1)$ is irreducible. This proves (D1). The proof for (D2) becomes obvious by using Lemma 2 again for H' between H and $I(V^*)$. □

Corresponding decision method. Suppose that K is a field for which both subraction and nonzero division for elements in K can be evaluated in an algorithmic manner. An example of such a field is **Q**, or any finite field. Then the pseudo remainder defined in [**6**] and [**1**] can be evaluated in an algorithmic manner for polynomials in KK. In this case, the previous theorem implies a decision procedure for the membership of $I(V^*(S; u_1 u_2, \ldots, u_d))$ for a special type of S. We state a theorem in terms of decision procedures as follows:

THEOREM 2. *Suppose* $S = \{h_1, h_2, \ldots, h_s\}$ $(s \geq 1)$ *has an irreducible R-characteristic set, say* $((p_1, p_2, \ldots, p_r),\ (x_1, x_2, \ldots, x_r))$, *in* KK *with* $u_1, u_2, \ldots, u_d$ *as independent variables such that condition* (S1) *is satisfied. Then a necessary and sufficient condition for any polynomial* g *in* KK *to be a member of* $I(V^*(p_1, p_2, \ldots, p_r; u_1, u_2, \ldots, u_d))$ *is* $\mathrm{prem}(g(p_1, p_2, \ldots, p_r),\ (x_1, x_2, \ldots, x_r)) = 0$. *Therefore, as long as the pseudo remainder function* prem *can be evaluated in an algorithmic manner, there is an algorithm to determine the membership of* $I(V^*(S; u_1, u_2, \ldots, u_d))$.

Condition (S1) can be proved as a consequence of conditions (C1)-(C4) if one of the following conditions is satisfied:

(1) $\overline{K}$ is algebraically closed,

(2) $K = \overline{K} = \mathbf{R}$ =the field of real numbers, and there exist nonempty open intervals $O_1, O_2, \cdots, O_d$ in R such that if $u_i \in O_i$ for all i, then $p_1 = 0$, $p_2 = 0, \ldots$ and $p_r = 0$ has a common solution for $(x_1, x_2, \ldots, x_r)$ in R.

The former condition is assumed in [**9**] and [**13**]. The latter condition is suggested by Wu in 1982 and introduced by the second author in [**2**].

Suppose that there is an algorithm to evaluate prem. In the above, we have an algorithmic method to determine the membership of an ideal of form $I(V^*(h_1, h_2, \ldots, h_s; u_1, u_2, \ldots, u_d))$ with $h_1, h_2, \ldots, h_s$ and $u_1, u_2, \ldots, u_d$ satisfying conditions (C1), (C2), (C3), (C4) and (S1). From an application point of view, such as to introduce a totally mechanical method in the area of automated geometry theorem proving based on Wu Wen-tsün's method, it is important to investigate whether all the above conditions can be checked in an algorithmic manner. Note that checking of conditions (C1), (C2) and (C3) can be easily performed in an algorithmic manner. However, checking conditions (C4) and (S1) do not seem to be easy to do. We know that, in case $\deg(p_i, x_i) \leq 2$ for all i, condition (C4) can be easily checked in an algorithmic manner as demonstrated in [**2**]. In general, Hermann [**5**] and others have introduced algorithmic methods to check condition (C4), and we believe that Tarski's [**10**] and related methods can be used to check condition (S1) for the case when $\overline{K} = \mathbf{R}$. All the general methods seem not to be easy to use at this time.

An application in automated geometry theorem proving. The very first step in automated geometry theorem proving by algebraic methods is to convert a given geometry problem to an algebraic problem. It is emphasized by Wu Wen-tsün and now generally recognized that this first step is, in fact, extremely hard to accomplish in a precise manner. This is because almost all known geometry statements are true subject to some unstated conditions, called nondegenerate conditions, which can often be poorly-defined and very hard to identify. For this reason, it is proposed by Wu Wen-tsün that to determine the truth value of such poorly-defined statements, what one should actually determine is the "generically truth value." We consider such an approach realistic and valuable. Further studies and development have been planned by many researchers and are expected to grow in time. Our algebraic geometry problem is extracted from this type of automated geometry theorem proving. We use two examples in Euclidean plane geometry to give a descripton of the above type of automated geometry theorem proving and to explain the role of our main theorem. The readers are referred to [**4**] for a rich collection of other examples.

EXAMPLE 1. [**3**, Example (2.1) (Parallelogram Theorem)] Let points A, B, C, D form a parallelogram so that AB, CD are parallel and AD, BC are parallel. Let lines AC and BD intersect at point E. Then E is the midpoint of diagonal AC and diagonal BD, but E does not necessarily have equal distance from points A and D.

EXAMPLE 2. [**3**] (Simson Theorem) From a point D on the circumscribed circle of a triangle ABC, perpendiculars are drawn to the sides of the triangle. Then the feet of the perpendiculars are collinear.

To convert the above problems to algebraic problems, note that, for any coordinate system of a Euclidean plane geometry, if points A_1, A_2, A_3, A_4, A_5 have the coordinates

$$\begin{aligned} &A_1 = (X1, Y1), \qquad A_2 = (X2, Y2), \qquad A_3 = (X3, Y3),\\ &A_4 = (X4, Y4), \qquad A_5 = (X5, Y5), \end{aligned}$$

then the following geometric relations can be represented by the following corresponding sets of polynomials in $\overline{K} = \mathbf{R}$, meaning that the given geometric relation holds if and only if the corresponding coordinates are common zeros of the given set of polynomials in $\mathbf{R}$:

(1) points A_1, A_2, A_3 are collinear -

$$X2Y3 \ - X1\,Y3 - X3\,Y2 + X1\,Y2 + X3\,Y1 - X2\,Y1,$$

(2) point A_3 is the midpoint of points A_1, A_2 -

$$\begin{aligned} &X1 + X2 - 2 \cdot X3, \\ &Y1 + Y2 - 2 \cdot Y3, \end{aligned}$$

(3) lines A_1A_2 and A_3A_4 are parallel -

$$(X2 - X1)(Y4 - Y3) - (X4 - X3)(Y2 - Y1),$$

(assume: points A_1, A_2, A_3 are noncollinear and points A_3, A_4 are distinct);

(4) lines A_1A_4, A_2A_3 are perpendicular -

$$(Y3 - Y2)(Y4 - Y1) + (X3 - X2)(X4 - X1),$$

(assume: points A_1, A_4 are distinct and points A_2, A_3 are distinct);

(5) the distance from A_1 to A_2 is equal to the distance from A_3 to A_4 -

$$(X1 - X2)^2 + (Y1 - Y2)^2 - (X3 - X4)^2 - (Y3 - Y4)^2.$$

The above type of polynomials are not uniquely determined; but we shall assume that the notion of "generically true" will be defined w.r.t. a specific set of algebraic formulations for elementary geometric relationships such as the above. In the notion of "generically true", it is also assumed that, for each statement in a large class of geometric problems, there are points, called arbitrary points, whose positions can be arbitrarily chosen and all the positions of other points in the given statements are then determined in a "dependent manner", i.e., the number of their solutions will then be finite. Let K be the field that characterizes all the possible coefficients of the basic algebraic formulas, $\overline{K}$ be the field that characterizes possible values of the coordinates of points $u_1, u_2, \ldots, u_d$ be variables representing "free coordinates" of the arbitrary points, and $x_1, x_2, \ldots, x_r$ be variables representing the remaining coordinates of all the points. Then it is possible to use variables $u_1, u_2, \ldots, u_d,\ \ x_1, x_2, \ldots, x_r$ and polynomials $h_1, h_2, \ldots, h_s,\ \ g$ in $KK = K[u_1, u_2, \ldots, u_d,\ \ x_1, x_2, \ldots, x_r]$ to characterize the given geometry statement in the following form:

The given geometry statement is true if and only if the following condition is satisfied.

> If σ is a solution for $(u_1, u_2, \ldots, u_d, x_1, x_2, \ldots, x_r)$ to the following system of equations in $\overline{K}^n$ and σ does not correspond to any degenerate case of the given geometry statement:
>
> $$\begin{aligned} &h_1(u_1, u_2, \ldots, u_d, x_1, x_2, \ldots, x_r) = 0, \\ &h_2(u_1, u_2, \ldots, u_d, x_1, x_2, \ldots, x_r) = 0, \\ &\ldots \\ &h_s(u_1, u_2, \ldots, u_d, x_1, x_2, \ldots, x_r) = 0, \end{aligned}$$
>
> then σ is also a solution to $g(u_1, u_2, \ldots u_d, x_1, x_2, \ldots x_r) = 0$.

Here, the hypothetical conditions of the given geometry statement are represented by polynomials $h_1, h_2, \ldots, h_s$, and the conclusion is represented by g. Then the given geometric statement, or the conclusion g, is said to be generically true if and only if

(G1) g is a member of $I(V^*(h_1, h_2, \ldots h_s;\ u_1, u_2, \ldots u_d))$.

With some precise adjustment of the above notions, it can be proved that if a geometry statement is generically true then the given geometry statement is true subject to some algebraic condition of form

$$I(u_1, u_2, \ldots u_d, x_1, x_2, \ldots x_r) \neq 0.$$

This is easy to see in the case when $\{h_1, h_2, \ldots, h_s\}$ has an irreducible R-characteristic set, say $((p_1, p_2, \ldots, p_r), (x_1, x_2, \ldots, x_r))$, with $u_1, u_2, \ldots, u_d$ as independent variables and $V^*(h_1, h_2, \ldots h_s;\ u_1, u_2, \ldots u_d)$ nonempty. For in this case, if the given geometric statement is generically true, then condition (G1) is satisfied and so, by Theorem 2, the following condition is satisfied:

(G2) $\text{prem}(g, (p_1, p_2, \ldots, p_r), (x_1, x_2, \ldots, x_r)) = 0$.

If polynomial I is the product of all the leading coefficients of p_i's w.r.t. x_i's, then, for some nonnegative integer t, the following remainder formula holds:

$$I^t \cdot g = q_1 \cdot p_1 + q_2 \cdot p_2 + \cdots + q_r \cdot p_r.$$

So, the given geometry statement is true as long as $I \neq 0$.

We now prove Examples 1 and 2 by using the above notions and prove the "generically truth value" of each of the given conclusions. (An elementary part of Wu's method can be used as an heuristic method to determine the truth value of many geometry statements, provided degenerate cases are well understood in an either explicit or implicit manner. However, a discussion in this direction does not seem to be appropriate to be introduced in this paper and thus is not provided.) The definition of prem can be the one introduced in either [**6**] or [**1**]. In either example, we have $K = \mathbf{Q}$, $\overline{K} = \mathbf{R}$, and the given $\{h_1, h_2, \ldots, h_s\}$ has an irreducible R-characteristic set $((p_1, p_2, \ldots, p_r), (x_1, x_2, \ldots, x_r))$ with $u_1, u_2, \ldots, u_d$ as independent variables and $V^*(h_1, h_2, \ldots, h_s; u_1, u_2, \ldots, u_d)$ is nonempty. So, for any conclusion, say characterized by $g = 0$, to be generically true, it is necessary and sufficient that condition (G2) is satisfied.

PROOF OF EXAMPLE 1. Let

$$A = (0,0), \qquad B = (U1, 0), \qquad C = (U2, U3),$$
$$D = (X1, X2), \qquad E = (X3, X4),$$

$$(u_1, u_2, \ldots, u_d) = (U1, U2, U3, U4, U5, U6),$$
$$(x_1, x_2, \ldots, x_r) = (X1, X2, X3, X4).$$

Let

$h_1 = U1\ (X2 - U3)$ (AB, CD are parallel),
$h_2 = (U2 - U1)\ X2 - U3\ X1$ (AD, BC are parallel),
$h_3 = U3\ X3 - U2\ X4$ (A, E, C are collinear),
$h_4 = -X1\ X4 + U1\ X4 + X2\ X3 - U1\ X2$ (B, E, D are collinear),

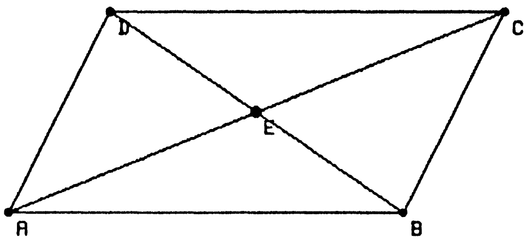

FIGURE 1.

$g_1 = 2\ X3 - U2 \quad (g_1, g_2 : E \text{ is the midpoint of } A, C),$
$g_2 = 2\ X4 - U3,$
$g_3 = 2\ X3 - X1 - U1 \ (g_3, g_4 : E \text{ is the midpoint of } B, D),$
$g_4 = 2\ X4 - X2,$
$g_w = -(X4 - X2)^2 + X4^2 - (X3 - X1)^2 + X3^2 \quad (AE = DE).$

We have at least two irreducible R-characteristic sets for $\{h_1, h_2, \ldots, h_s\}$, namely the list of following polynomials:

$p_1 = U1\ U3\ (X1 - U2 + U1),$
$p_2 = U1\ (X2 - U3),$
$p_3 = U1\ U3\ (2\ X3 - U2),$
$p_4 = U1\ U2\ U3\ (2\ X4 - U3),$

and the list
$p_1 = -U1\ U3\ (X1 - U2 + U1),$
$p_2 = U1\ (X2 - U3),$
$p_3 = -(U2\ X2\ X3 - U3\ X1\ X3 + U1\ U3\ X3 - U1\ U2\ X2),$
$p_4 = -(U2\ X4 - U3\ X3).$

For either one of them, g_i satisfies condition (G2) for all $i = 1, 2, 3, 4$, but g_w does not. So, g_i's are generically true conclusions for all $i = 1, 2, 3, 4$, but g_w is not. □

PROOF OF EXAMPLE 2. Let point O be the center of the circumscribed circle and

$$O = (0,0), \qquad A = (U1, 0), \qquad B = (U2, X1), \qquad C = (U3, X2),$$

$$D = (U4, X3), \qquad E = (X4, X5), \qquad F = (X6, X7), \qquad G = (X8, X9),$$

$$(u_1, u_2, \ldots, u_d) = (U1, U2, U3, U4),$$
$$(x_1, x_2, \ldots, x_r) = (X1, X2, X3, X4, X5, X6, X7, X8, X9),$$

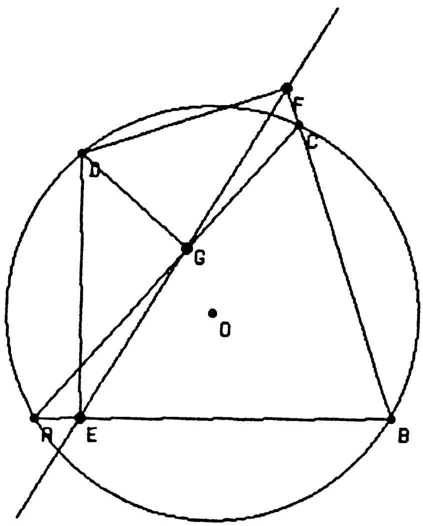

FIGURE 2.

Let

$$\begin{aligned} h_1 &= -X1^2 - U2^2 + U1^2 \quad (OA = OB), \\ h_2 &= -X2^2 - U3^2 + U1^2 \quad (OA = OC), \\ h_3 &= -X3^2 - U4^2 + U1^2 \quad (OA = OD), \end{aligned}$$

(h_4, h_5 : E is the perpendicular foot from D to AB)

$$\begin{aligned} h_4 &= U2\ X5 - U1\ X5 - X1\ X4 + U1\ X1, \\ h_5 &= X1\ (X5 - X3) + (U2 - U1)\ (X4 - U4), \end{aligned}$$

(h_6, h_7 : F is the perpendicular foot from D to AC)

$$h_6 = U3\ X7 - U2\ X7 - X2\ X6 + X1\ X6 + U2\ X2 - U3\ X1,$$

$h_7 = (X2 - X1)\ (X7 - X3) + (U3 - U2)\ (X6 - U4)$,

(h_8, h_9 : G is the perpendicular foot from D to BC)

$h_8 = -U3\ X9 + U1\ X9 + X2\ X8 - U1\ X2$,
$h_9 = (U1 - U3)\ (X8 - U4) - X2\ (X9 - X3)$,
$g = X6\,X9 - X4\,X9 - X7\,X8 + X5\,X8 + X4\,X7 - X5\,X6$, ($D, E, F$ are collinear).

We have at least two irreducible R-characteristic sets for $\{h_1, h_2, \dots, h_s\}$, namely, the list of the following polynomials:

$p_1 = -X1^2 - U2^2 + U1^2$,
$p_2 = -X2^2 - U3^2 + U1^2$,
$p_3 = -X3^2 - U4^2 + U1^2$,
$p_4 = (U2 - U1)\ (2\,U1\ X4 + X1\ X3 + U2\ U4 - U1\ U4 - U1\ U2 - U1^2)$,
$p_5 = (U2 - U1)\ (2\,U1\ X5 - U2\ X3 - U1\ X3 + U4\ X1 - U1\ X1)$,
$p_6 = 2\ X1\ X2\ X6 + 2\ U2\ U3\ X6 - 2\ U1^2\ X6 + U3\ X2\ X3 - U2\ X2\ X3 - U3\ X1\ X3 + U2\ X1\ X3 - U3\ X1\ X2 - U2\ X1\ X2 + U3^2 U4 - 2\,U2\,U3\,U4 + U2^2\ U4 - U2\,U3^2 - U2^2 U3 + U1^2\ U3 + U1^2\ U2$,
$p_7 = (U3 - U2)\ (2\ X1\ X2\ X7 + 2\ U2\ U3\ X7 - 2U1^2 X7 - 2\,X1\,X2\,X3 - U3^2 X3 - U2^2 X3 + 2U1^2 X3 + U3\,U4\,X2 - U2\,U4\,X2 - U2\,U3\,X2 + U2^2 X2 - U3\,U4\,X1 + U2\,U4\,X1 + U3^2 X1 - U2\,U3\,X1)$,
$p_8 = (U3 - U1)\ (2\,U1\ X8 + X2\ X3 + U3\ U4 - U1\ U4 - U1\ U3 - U1^2)$,
$p_9 = (U3 - U1)\ (2\,U1\ X9 - U3\ X3 - U1\ X3 + U4\ X2 - U1\ X2)$,

and the list of the following polynomials:

$p_1 = -X1^2 - U2^2 + U1^2$,
$p_2 = -X2^2 - U3^2 + U1^2$,
$p_3 = -X3^2 - U4^2 + U1^2$,
$p_4 = (X1^2 + U2^2 - 2\,U1\,U2 + U1^2)\ X4 + (U1 - U2)\ X1\ X3 - U1\ X1^2 + (-U2^2 + 2\ U1\ U2 - U1^2) U4$,
$p_5 = (U2 - U1)\ X5 - X1\ X4 + U1\ X1$,
$p_6 = (X2^2 - 2\,X1\,X2 + X1^2 + U3^2 - 2\,U2\,U3 + U2^2) X6 + ((U2 - U3)\ X2 + (U3 - U2)\ X1)\ X3 - U2\ X2^2 + (U3 + U2)\ X1\ X2 - U3\ X1^2 + (-U3^2 + 2\ U2\ U3 - U2^2)\ U4$,
$p_7 = (U3 - U2)\ X7 + (X1 - X2)\ X6 + U2\ X2 - U3\ X1$,
$p_8 = (X2^2 + U3^2 - 2\,U1\,U3 + U1^2)\ X8 + (U1 - U3)\ X2\ X3 - U1\ X2^2 + (-U3^2 + 2\ U1\ U3 - U1^2) U4$,
$p_9 = (U1 - U3)\ X9 + X2\ X8 - U1\ X2$.

For either one of them, g satisfies condition (G2) and thus is a generically true conclusion. □

REFERENCES

1. Shang-ching Chou, "Proving Elementary Geometry Theorems Using Wu's Algorithm," *Automated Theorem Proving: after* 25 *years*, Contemporary Mathematics **29** (1984), 243-286.

2. ———, *Proving and Discovering Theorems in Elementary Geometries Using Wu's Method*, Ph.D. Thesis, Department of Mathematics, University of Texas, Austin, 1985.

3. ———, *An Introduction to Wu's Method for Mechanical Theorem Proving in Geometry*, preprint, 1986.

4. ———, *Proving Geometry Theorems Using Wu's Method, A Collection of Geometry Theorems Proved Mechanically*, Technical Report 50, July 1986, Institute for Computing Science, The University of Texas at Austin, Austin, 78712.

5. G. Hermann, *Die Frage der endlich vielen Schritt in der Theorie der Polynomideale*, Math. Ann. **95** (1926), 736-788.

6. Donald E. Knuth, *The Art of Computer Programming*, Vol. 2, Addision-Wesley Publishing Company, Massachusetts, 1981.

7. Hai-Ping Ko and Shang-ching Chou, *Decision Procedure for Certain Triangular Algebraic Varieties*, preprint, 1986.

8. ——— and Moayyed A. Hussain, *A Study of Wu's Method - a Method to Prove Certain Theorems in Elementary Geometry*, Congr. Numer. **48** (1985), 225-242.

9. Joseph Fels Ritt, *Differential Algebra*, AMS, New York City, 1950.

10. A. Tarski, *A Decision Method for Elementary Algebra and Geometry*, Berkeley and Los Angeles, 1951.

11. B.L. van der Waerden, *Algebra*, Translated by John R. Schulenberger, Vol. 2, Frederick Ungar Publishing Co., New York, 1970.

12. Wu Wen-tsün, *On Decision Problem and Mechanization of Theorem Proving in Elementary Geometry*, Sci. Sinica **21** (1978), 159-172.

13. *Basic Principles of Mechanical Theorem Proving in Elementary Geometries*, J. Systems Sci. Math. Sci. **4** (1984), 207-235.

14. *On Zeros of Algebraic Equations - an application of Ritt Principle*, Kexue Tongbao, Vol. **31**, No. 1, January 1986.

CORPORATE RESEARCH AND DEVELOPMENT, GENERAL ELECTRIC COMPANY, SCHENECTADY, NY 12301

INSTITUTE FOR COMPUTING SCIENCE, THE UNIVERSITY OF TEXAS AT AUSTIN, AUSTIN, TX 78712