The Kinds of Truth of Geometry Theorems

Michael Bulmer[1], Desmond Fearnley-Sander[2], and Tim Stokes[3]

[1] University of Queensland, Queensland, Australia
mrb@maths.uq.edu.au
[2] University of Tasmania, Tasmania, Australia
Desmond.FearnleySander@utas.edu.au
[3] Murdoch University, Western Australia, Australia
stokes@prodigal.murdoch.edu.au

Abstract. Proof by refutation of a geometry theorem that is not universally true produces a Gröbner basis whose elements, called *side polynomials*, may be used to give inequations that can be added to the hypotheses to give a valid theorem. We show that (in a certain sense) all possible subsidiary conditions are implied by those obtained from the basis; that what we call the *kind of truth* of the theorem may be derived from the basis; and that the side polynomials may be classified in a useful way. We analyse the relationship between side polynomials and kinds of truth, and we give a unified algorithmic treatment of side polynomials, with examples generated by an implementation.

1 Algebraic Preliminaries

Throughout, let n be a positive integer and L a fixed field containing the field $\mathbb{Q}$ of rational numbers. Let $\mathbb{Q}[X_n]$ be the ring of polynomials with n-variable set $X_n = \{x_1, x_2, \ldots, x_n\}$ over $\mathbb{Q}$.

Let $F \subseteq \mathbb{Q}[X_n]$ and $f \in \mathbb{Q}[X_n]$. We call (F, f) a *possible theorem.* $(F)_{X_n}$ denotes the ideal generated by F in $\mathbb{Q}[X_n]$. For $a \in L^n$ we denote by $f(a)$ the result of substituting a for their corresponding variables in f and evaluating.

For $F \subseteq \mathbb{Q}[X_n]$, let

$$C_{X_n}(F) = \{f \in \mathbb{Q}[X_n] \mid \text{ for all } a \in L^n, h(a) = 0 \text{ for all } h \in F \text{ implies } f(a) = 0\},$$

an ideal of $\mathbb{Q}[X_n]$ as is easily checked. If the choice of polynomial ring is clear we often write just $C(F)$. If L is algebraically closed then by Hilbert's Nullstellensatz, $C_{X_n}(F) = \{f \in \mathbb{Q}[X_n] \mid f^k \in (F)_{X_n}\}$, the *radical ideal generated by* F in $\mathbb{Q}[X_n]$.

Dually, for $F \subseteq \mathbb{Q}[X_n]$, let

$$\mathcal{V}_{X_n}(F) = \{a \mid a \in L^n, f(a) = 0 \text{ for all } f \in F\},$$

the *variety* associated with $F \subseteq \mathbb{Q}[X_n]$. Again, we often write just $\mathcal{V}(F)$ if the context is clear, and if $F = \{f\}$, a singleton set, we shall often write $\mathcal{V}_{X_n}(f)$ (or just $\mathcal{V}(f)$) rather than $\mathcal{V}_{X_n}(\{f\})$. Varieties are closed under arbitrary intersections and finite unions.

There is a familiar dual isomorphism between the lattices of varieties of the form $\mathcal{V}_{X_n}(G)$ and ideals of the form $C_{X_n}(G)$, $G \subseteq \mathbb{Q}[X_n]$. Because the lattice of varieties is distributive and satisfies the descending chain condition, every variety $\mathcal{V}$ has a unique decomposition

$$\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2 \cup \cdots \cup \mathcal{V}_n$$

into distinct *irreducible components* (varieties which cannot themselves be expressed non-trivially as unions of two or more smaller varieties).

2 The Kind of Truth of a Possible Theorem

In geometrical theorem proving, the higher level statement of a valid geometry theorem naturally translates into an equational implication involving polynomials, with geometrical predicates such as "points A, B and C are collinear" becoming polynomial equations via coordinatisation. Further, one can require that certain variables be treated as independent, in the sense that no algebraic relations are assumed to hold amongst them. Chou has argued in [2] that the specification of the independent variables in a geometry theorem is an integral part of the algebraic formulation: such variables are chosen according to a notional "construction" that takes place when the geometry theorem hypotheses are read in order. It is this approach we adopt.

Formally, suppose the variables in $U \subseteq X_n$ are specified as being independent; view $\mathbb{Q}[U]$ as a subring of $\mathbb{Q}[X_n]$. We say that a variety $\mathcal{V}$ is *U-generic* (or simply *generic* if the choice of U is clear) if no polynomial in $\mathbb{Q}[U]$ is zero on all of $\mathcal{V}$. If L is algebraically closed, then $\mathcal{V}_{X_n}(F)$ is U-generic if and only if $(F)_{X_n} \cap \mathbb{Q}[U] = \{0\}$; this is called *$U$-independence* in [5]. Let $\mathcal{G}_{X_n}(F)$ denote the union of all U-generic irreducible components of $\mathcal{V}_{X_n}(F)$.

We can now define the four basic *kinds of truth* of a possible theorem: for $F \cup \{f\} \subseteq \mathbb{Q}[X_n]$, we say the possible theorem (F, f) is

1. *universally true* if f is zero on all of $\mathcal{V}_{X_n}(F)$, that is, $f(a) = 0$ for all $a \in \mathcal{V}_{X_n}(F)$;
2. *generically true* if f is zero on $\mathcal{G}_{X_n}(F)$;
3. *generically conditionally true* if there exists an irreducible component of $\mathcal{G}_{X_n}(F)$ on which f is zero but f is not zero on all of $\mathcal{G}_{X_n}(F)$;
4. *generically false* there is no irreducible component of $\mathcal{G}_{X_n}(F)$ on which f is zero.

We are further able to separate the final category into two subcategories. A generically false possible theorem is:

- *degenerately true* if there is no irreducible component of $\mathcal{G}_{X_n}(F)$ on which f is zero, yet there is at least one irreducible component of $\mathcal{V}_{X_n}(F)$ on which f is zero;

- *rarely true* if there is no irreducible component of $\mathcal{V}_{X_n}(F)$ on which f is zero.

We call these kinds of truth 1 to 4 respectively, with kind 4 split into 4(a) and 4(b) as above. Note that a possible theorem is of at least one of these five types, and exactly one of types 2 to 4 (b). We shall show how to determine the kind of truth of a possible theorem using Gröbner bases for the case where L is algebraically closed.

Generic truth reflects the idea that the conclusion holding on the generic irreducible components of the hypotheses is what is "really intended" by the author of a theorem. Generically conditional truth occurs when there is some ambiguity in the hypotheses of the theorem and the conclusion will not hold on all generic irreducible components; this is in practice a rare situation but can occur as illustrated in [2] and elsewhere. Generic falsity occurs when the conclusion is valid on no generic irreducible components. In contrast to rare truth, degenerate truth is at least a form of conditional truth, and the fact that it can be algorithmically distinguished from rare truth has led us to define it separately.

Most of these kinds of truth have in essence been considered elsewhere along with algorithmic ways of determining the kind of truth of a possible theorem (see [2], [1] and more recently [7] and [6] for instance). However, so far as we know, no unified algorithmic treatment of the kind presented here, applying to all the kinds of truth discussed here and providing a complete set of side polynomials for each, has appeared previously.

3 Side Polynomials and Kinds of Truth

For the remainder of the article, F and f will be an arbitrary subset and an element of $\mathbb{Q}[X_n]$ respectively.

In Kapur [4], a method described as refutational theorem proving was considered for proving geometry theorems translated into polynomial equations in this way. Kapur's approach was based on the idea of considering the conjunction of the hypotheses of the theorem with the negation of the conclusion (in a certain sense), forming a Gröbner basis and determining if it was $\{1\}$; if so, then the theorem was validated and if not the polynomials in the basis could be used to give side conditions in the form of inequations which could be added to the hypotheses in order to give a valid theorem.

Such side conditions prove necessary because most standard Euclidean geometry "theorems", as normally stated, are not universally true, owing to the absence from the hypotheses of certain additional non-degeneracy conditions that may be represented algebraically as inequations. These may correspond to hypotheses of the form "points A, B and C are *not* collinear", and so forth. Often, such extra hypotheses are not easy to guess, as is discussed at length in [2], although synthetic proofs of geometry theorems make at least tacit use of them. Note that any finite number of inequations may be expressed as a single inequation.

We show that all possible side conditions (in a certain natural sense) are implied by those obtained from the Gröbner basis used in Kapur's method, and that the kind of truth of the theorem may be derived from this basis; moreover, the side polynomials may be classified in a useful way.

Formally, we say that $g \in \mathbb{Q}[X_n]$ is a *side polynomial* for (F, f) if $f(a) = 0$ for all $a \in \mathcal{V}(F)$ for which $g(a) \neq 0$. Let the set of all side polynomials for (F, f) be denoted $side(F, f)$.

Theorem 1 *For the possible theorem (F, f), $C(side(F, f)) = side(F, f)$.*

Proof. Now of course $side(F, f) \subseteq C(side(F, f))$. Suppose $h \in C(side(F, f))$ and that $h(a) \neq 0$ for some $a \in \mathcal{V}(F)$. Then because $h \in C(side(F, f))$, by definition there exists $g \in side(F, f)$ such that $g(a) \neq 0$, so $f(a) = 0$. Hence $h \in side(F, f)$ by definition, and so $C(side(F, f)) \subseteq side(F, f)$. Hence the two sets are equal. □

There are various kinds of side polynomial, corresponding to the various kinds of truth as we shall show. Thus a side polynomial g for (F, f) is

1. *generic* if $g \in \mathbb{Q}[U]$;
2. *generically resolving* if $g \notin \mathbb{Q}[U]$ and (F, g) is not generically true;
3. *degenerate* if $g \notin \mathbb{Q}[U]$ and (F, g) is generically true;
4. *extraneous* if $g \notin \mathbb{Q}[U]$ and (F, g) is universally true.

Theorem 2 *The possible theorem (F, f) is*

1. *universally true if and only if every polynomial is a side polynomial;*
2. *generically true if and only if there exists a generic side polynomial;*
3. *generically conditionally true if and only if there exist no generic side polynomials, but there does exist a generically resolving side polynomial;*
4. *degenerately true if and only if there exist no generic or generically resolving side polynomials, but there does exist a degenerate side polynomial;*
5. *rarely true if and only if all side polynomials are extraneous.*

Proof. The first part is immediate. The second is proved in [2].

Now suppose (F, f) has no generic or generically resolving side polynomials. If $g \in side(F, f)$ then (F, g) is generically true, so if $h(a) = 0$ for all $h \in F$ and $g(a) \neq 0$ then $a \notin \mathcal{G}(F)$. Suppose h is a non-degenerate side polynomial for (F, f); hence fh is zero on $\mathcal{V}(F)$, so certainly fh is zero on $\mathcal{V}(G)$, so $\mathcal{V}(G) \subseteq \mathcal{V}(fh) = \mathcal{V}(f) \cup \mathcal{V}(h)$. Hence $\mathcal{V}(G) = [\mathcal{V}(G) \cap \mathcal{V}(f)] \cup [\mathcal{V}(G) \cap \mathcal{V}(h)]$. But h is non-degenerate, so h is not zero on all of $\mathcal{V}(G)$, so $\mathcal{V}(G) \not\subseteq \mathcal{V}(h)$, so $\mathcal{V}(G) \cap \mathcal{V}(h) \subset \mathcal{V}(G)$, and so $\mathcal{V}(G) \cap \mathcal{V}(f)$ is a finite non-empty union of irreducible components of $\mathcal{V}(G)$: let $\mathcal{V}(G')$ be one of these irreducible components. Then $\mathcal{V}(G')$ is a generic irreducible component of $\mathcal{V}(F)$ also, and because $\mathcal{V}(G') \subseteq \mathcal{V}(G) \cap \mathcal{V}(f) \subseteq \mathcal{V}(f)$, it follows that f is zero on $\mathcal{V}(G')$. Hence (F, f) is neither degenerately true nor rarely true.

Conversely, suppose (F, f) is neither degenerately true nor rarely true. Now $\mathcal{V}(F) \neq \emptyset$, so $C(F) \neq \mathbb{Q}[X_n]$. Suppose f is zero on the generic irreducible component $\mathcal{V}(F')$ of $\mathcal{V}(F)$; then $\mathcal{V}(F') \subseteq \mathcal{V}(f)$. If $\mathcal{V}(F)$ has only one irreducible component (namely itself), then $\mathcal{V}(F) = \mathcal{V}(F')$ and then f is zero on $\mathcal{V}(F)$ and so any polynomial $h \notin C(F)$ is a non-degenerate side polynomial for (F, f); these exist because $C(F) \neq \mathbb{Q}[X_n]$. On the other hand, if $\mathcal{V}(F)$ has more than one irreducible component, let $\mathcal{V}(H)$ be the union of the irreducible components of $\mathcal{V}(F)$ other than $\mathcal{V}(F')$. Let $h \in C(H) \backslash C(F')$; such a non-zero h exists since $\mathcal{V}(F') \nsubseteq \mathcal{V}(H)$, so $C(H)$ is not a subset of $C(F')$, and $C(H)$ is non-empty. Further, if $F(a) = 0$ yet $h(a) \neq 0$ then $a \in \mathcal{V}(F) \backslash \mathcal{V}(H) \subseteq \mathcal{V}(F') \subseteq \mathcal{V}(f)$. So $h \in \mathit{side}(F, f)$. But $h \notin C(F')$ and $\mathcal{V}(F') \subseteq \mathcal{V}(G)$, so $h \notin C(G)$, so h is a non-degenerate side polynomial for (F, f). Thus every side polynomial for (F, f) is degenerate if and only if (F, f) is degenerately true or rarely true.

Let $U' = \emptyset$. Then all irreducible components of $\mathcal{V}(F)$ are U'-generic, (F, g) is U'-generically true if and only if (F, g) is universally true, and a side polynomial is U'-degenerate if and only if it is extraneous. Then (F, f) is rarely true if and only if (F, f) is U'-degenerately or rarely true if and only if every side polynomial for (F, f) is U'-degenerate, that is to say, extraneous.

Finally, there is at least one generically resolving side polynomial for (F, f) yet no generic side polynomials for (F, f) if and only if (F, f) is not generically true and (by the above) neither degenerately nor rarely true, that is, if and only if (F, f) is generically conditionally true. □

4 Proof by Refutation and the Kind of Truth

Because of Hilbert's Nullstellensatz, algebraically closed fields are algorithmically convenient to work with, and we frequently assume algebraic closure of L in what follows; moreover all fields have characteristic zero since we work with polynomials over the rational numbers. When L is the field of real numbers, a geometry theorem being true in any of the senses just defined means that it is *true in the theory of Euclidean geometry*. Of course, if a possible theorem is universally true over an algebraically closed field of characteristic zero, then it is true over the complex numbers and hence over the reals also. Although the converse fails, it seems to do so rarely, a fact which apparently generalises to the other kinds of truth as we see in examples to follow. Certainly any side polynomial over algebraically closed L is a side polynomial over the reals also. Thus the assumption that L is algebraically closed is not totally artificial and corresponds to a certain well-defined level of geometrical reasoning which in practice seems only a little weaker than full Euclidean geometry, namely *metric geometry*. We recommend the book [2] to the reader interested in a more detailed account of some of these matters, which have been discussed by many authors.

There are methods which allow one to test whether a given guess is a side polynomial for a possible theorem (and these are considered in detail in [4]), but guessing side polynomials is generally difficult. Furthermore, the existence of (say) a resolving side polynomial for (F, f) does not preclude the existence of generic side polynomials, so the kind of truth is not necessarily established by a correctly guessed side polynomial. Moreover, one can never be sure of having a complete set of side polynomials (so that the disjunction of the associated inequations covers all possibilities for side conditions) using such an approach. A method which is able both to produce a complete set of side polynomials and then to read off the kind of truth of the possible theorem is desirable. It turns out that the set obtained using Kapur's method in [4], based on constructing the Gröbner basis of $F \cup \{fz - 1\}$, does this job.

Recall from Theorem 1 that $C(side(F, f)) = side(F, f)$. We shall call any set of polynomials $G \subseteq \mathbb{Q}[X_n]$ for which $C(G) = side(F, f)$ a *complete set* of side polynomials for (F, f). Then certainly, for any $a \in L^n$, $h(a) = 0$ for all $h \in F$ and $g_1(a) \neq 0 \vee g_2(a) \neq 0 \vee \cdots \vee g_k(a) \neq 0$ imply $f(a) = 0$, and moreover any side polynomial p is such that $p(a) \neq 0$ implies $g_1(a) \neq 0 \vee g_2(a) \neq 0 \vee \cdots \vee g_k(a) \neq 0$. So the disjunction of the side conditions of the form $g_i \neq 0$ is the weakest possible such disjunction. We similarly define a complete set of generic side polynomials for (F, f) to be any finite $G \subseteq \mathbb{Q}[U]$ for which $C(G) \cap \mathbb{Q}[U] = side(F, f) \cap \mathbb{Q}[U]$.

For $F \cup \{f\} \subseteq \mathbb{Q}[X_n]$ and U a non-empty subset of X_n, let $(F : f)_U$ be the ideal $(F \cup \{fz - 1\})_{X_n \cup \{z\}} \cap \mathbb{Q}[U]$. (If $U = X_n$, this is the *saturation* of f with respect to the ideal $(F)_{X_n}$.)

Results similar to the following have already appeared in the literature.

Theorem 3 *For the possible theorem (F, f), $side(F, f) = C_{X_n \cup \{z\}}(F \cup \{fz - 1\}) \cap \mathbb{Q}[X_n]$.*

Proof. Let $B(F, f) = C_{X_n \cup \{z\}}(F \cup \{fz - 1\}) \cap \mathbb{Q}[X_n]$. The following are equivalent.

- $g \in B(F, f)$;
- $g \in \mathbb{Q}[X_n]$, and if $a \in \mathcal{V}_{X_n}(F)$ and $f(a)b = 1$ for some $b \in L$, then $g(a) = 0$;
- $g \in \mathbb{Q}[X_n]$ and if $a \in \mathcal{V}_{X_n}(F)$ and $f(a) \neq 0$, then $g(a) = 0$;
- $g \in \mathbb{Q}[X_n]$ and if $a \in \mathcal{V}_{X_n}(F)$ and $g(a) \neq 0$, then $f(a) = 0$;
- $g \in side(F, f)$.

Hence $side(F, f) = B(F, f)$. □

Theorem 4 *Suppose L is algebraically closed. Then $side(F, f) = C((F : f)_{X_n})$, and if a lexicographic order is used in which z is the biggest variable and the variables in U are all ordered below those in $X_n \backslash U$, then $GB(F \cup \{fz - 1\}) \cap \mathbb{Q}[U]$ is a complete set of generic side polynomials for (F, f).*

Proof.

$$\begin{aligned} C_U((F : f)_U) &= C_U((F \cup \{fz - 1\})_{X_n \cup \{z\}} \cap \mathbb{Q}[U]) \\ &\subseteq C_{X_n \cup \{z\}}((F \cup \{fz - 1\})_{X_n \cup \{z\}} \cap \mathbb{Q}[U]) \cap \mathbb{Q}[U] \\ &\subseteq C_{X_n \cup \{z\}}((F \cup \{fz - 1\})_{X_n \cup \{z\}}) \cap \mathbb{Q}[U] \\ &= C_{X_n \cup \{z\}}(F \cup \{fz - 1\}) \cap \mathbb{Q}[U] \\ &= side(F, f) \end{aligned}$$

from Theorem 3. (Note this part of the argument works even if L is not algebraically closed.)

Conversely, if L is algebraically closed and $g \in \mathit{side}(F,f) \cap \mathbb{Q}[U]$, then by Theorem 3, $g \in C_{X_n \cup \{z\}}(F \cup \{fz-1\}) \cap \mathbb{Q}[U]$, so by Hilbert's Nulltellensatz, there exists $n > 0$ for which $g^n \in (F \cup \{fz-1\})_{X_n \cup \{z\}}$ and hence $g^n \in C_U((F:f)_U)$, so by Hilbert's Nullstellensatz, $g \in C_U((F:f)_U)$. Hence $\mathit{side}(F,f) \cap \mathbb{Q}[U] \subseteq C_U((F:f)_U)$ and so $\mathit{side}(F,f) = C_U((F:f)_U)$.

From the theory of Gröbner bases, if a lexicographic order is used in which the variables in U are all ordered below those in $X_n \cup \{z\} \backslash U$, then $GB((F \cup \{fz-1\}) \cap \mathbb{Q}[U]) = GB(F \cup \{fz-1\}) \cap \mathbb{Q}[U]$, which is therefore a generating set for the ideal $(F:f)_U$ and hence is a complete set of side polynomials for (F,f), since if an ideal I is a complete set of side polynomials for (F,f) then so is any generating set for I. □

The following is immediate if one lets $U = X_n$.

Corollary 5 *Suppose L is algebraically closed. If a lexicographic order is used in which z is the biggest variable, then $GB(F \cup \{fz-1\}) \cap \mathbb{Q}[X_n]$ is a complete set of side polynomials for (F,f).*

This generalises a result in [4], where it was shown that if a side polynomial h consistent with the hypotheses (in other words a non-extraneous side polynomial) exists, then there will be one in $GB(F \cup \{fz-1\}) \cap \mathbb{Q}[X_n]$. Our result shows that $GB(F \cup \{fz-1\}) \cap \mathbb{Q}[X_n]$ spans all possible side conditions in the natural sense described earlier, and moreover this extends to generic side polynomials.

Suppose L is algebraically closed. Let $G(\mathit{side}(F,f)) = GB(F \cup \{fz-1\}) \cap \mathbb{Q}[X_n]$, computed with respect to a fixed lexicographic order in which z is the biggest variable and the variables in U are all ordered below those in $X_n \backslash U$.

Let

$$G_1 = G(\mathit{side}(F,f)) \cap \mathbb{Q}[U],$$

$$G_2 = \{g \mid g \in G(\mathit{side}(F,f)), g \notin \mathbb{Q}[U], G(\mathit{side}(F,g)) \cap \mathbb{Q}[U] = \emptyset\},$$

$$G_3 = \{g \mid g \in G(\mathit{side}(F,f)), G(\mathit{side}(F,g)) \cap \mathbb{Q}[U] \neq \emptyset, G(\mathit{side}(F,g)) \neq \{1\}\},$$

$$G_4 = \{g \mid g \in G(\mathit{side}(F,f)), G(\mathit{side}(F,g)) = \{1\}\}.$$

G_1 consists of a complete set of generic side polynomials as we have just shown, G_2 consists of generically resolving side polynomials, G_3 consists of non-extraneous degenerate side polynomials and G_4 consists of extraneous side polynomials. Thus the G_i partition $G(\mathit{side}(F,f))$: $G = \cup_{i=1}^4 G_i$ and $G_i \cap G_j = \emptyset$ for $i \neq j$.

Theorem 6 *The possible theorem (F,f) is*

1. *universally true if and only if $G_1 = \{1\}$;*
2. *generically true if and only if $G_1 \neq \emptyset$;*
3. *generically conditionally true if and only if $G_1 = \emptyset$, $G_2 \neq \emptyset$;*
4. *degenerately true if and only if $G_1 = G_2 = \emptyset$, $G_3 \neq \emptyset$;*
5. *rarely true if and only if $G_1 = G_2 = G_3 = \emptyset$, $G_4 \neq \emptyset$.*

Proof. Since it generates the ideal $side(F, f)$, $G(side(F, f))$ is a complete set of side polynomials for (F, f). Consequently, for any side polynomial for (F, f), there exists $k \in G(side(F, f))$ such that $h(a) \neq 0$ implies $k(a) \neq 0$, $a \in L^n$. Hence k is zero on no more irreducible components of $\mathcal{V}_{X_n}(F)$ than is h.

If (F, f) is generically true, then by Theorem 4, $G_1 \neq \emptyset$; the converse is obvious.

Suppose (F, f) is generically conditionally true. Then $G_1 = \emptyset$ as otherwise there would be a generic side polynomial for (F, f). Furthermore, there exists a side polynomial h for (F, f) which is generically resolving. Hence by the above, there exists $k \in G(side(F, f))$ which vanishes on no more irreducible components of $\mathcal{V}(F)$ than does h. Hence k is either generically resolving or generic. It cannot be generic since $G_1 = \emptyset$, so $k \in G_2$ and so $G_2 \neq \emptyset$.

Conversely, suppose $G_1 = \emptyset$, $G_2 \neq \emptyset$. Then (F, f) is not generically true since G_1 is a complete set of generic side polynomials, but there is a generically resolving side polynomial, so (F, f) is generically conditionally true.

Suppose (F, f) is degenerately true. Then as above, $G_1 = G_2 = \emptyset$. Also as above, because there is a degenerate side polynomial for (F, f), there must be one in $G(side(F, f))$, and so $G_3 \neq \emptyset$. Conversely, if $G_1 = G_2 = \emptyset$ and $G_3 \neq \emptyset$, then (F, f) is certainly not generically true since $G_1 = \emptyset$, but neither is it generically conditionally true, as if it were, $G_2 \neq \emptyset$ from earlier in the proof. Thus (F, f) is degenerately true since there are no generic or generically resolving side polynomials, but there is at least one degenerate side polynomial.

Suppose (F, f) is rarely true. Then, again, $G_1 = G_2 = G_3 = \emptyset$ yet $G_4 \neq \emptyset$. Conversely, if $G_1 = G_2 = G_3 = \emptyset$, $G_4 \neq \emptyset$, then, as above, (F, f) is not generically true, nor generically conditionally true, nor degenerately true, and hence is rarely true. □

Thus $G(side(F, f))$ provides a complete set of side polynomials for (F, f) from which the kind of truth may be determined along with the relevant side polynomials and, with luck, a geometrical interpretation of each such side polynomial, leading to a geometrical side condition for each.

5 Implementation and Examples

The classification procedure given by Theorem 6 can be attached to a standard implementation of a refutational prover for algebraic geometry theorems. This has been coded in Mathematica using the following algorithm:

1. Translate geometric predicates in the hypotheses and conclusion to algebraic polynomials, giving $F \subseteq \mathbb{Q}[X]$ and $f \in \mathbb{Q}[X]$, respectively. For example, `Collinear[`*a*`,`*b*`,`*c*`]` (meaning that the points a, b, and c are collinear) translates to the coordinate polynomial

   $$(x[a] - x[b])(y[b] - y[c]) - (y[a] - y[b])(x[b] - x[c]).$$

   Additionally, the construction sequence is used to determine which variables are independent, the elements of $U \subseteq X$, as described in [2].

2. Compute the Gröbner basis $G(side(F,f)) = GB(F \cup \{fz - 1\}) \cap \mathbb{Q}[X]$, removing the polynomials involving z.
3. Split $Gside(F,f))$ into the four sets G_1, G_2, G_3, G_4, as defined in the preamble to Theorem 6. This involves additional Gröbner basis computations.
4. If $G_1 = \{1\}$ then return `True`. Otherwise, attempt to translate the polynomials back into geometric predicates using pattern matching. (If no predicate can be determined then the polynomial is returned for inspection by the user.)

The Mathematica code for our implementation can be downloaded from

```
http://www.maths.utas.edu.au/People/dfs/dfs.html
```

We now give some simple examples to show the kinds of truth of geometry theorems and the results of this algorithm.

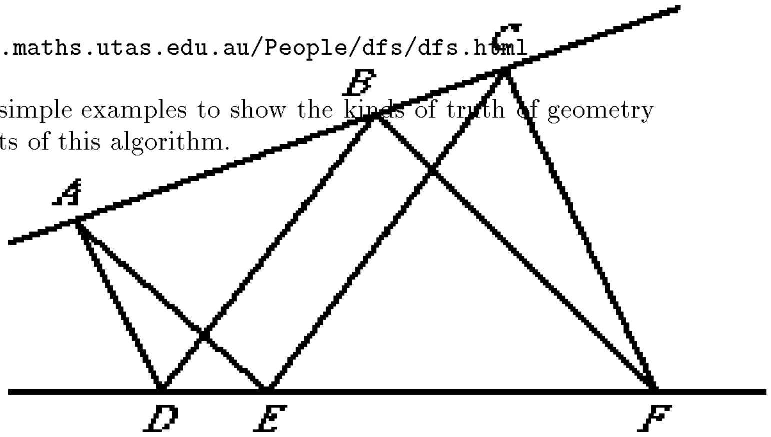

Fig. 1. The Parallel Pappus Theorem.

Parallel Pappus. The following is a famous theorem of Pappus:

```
Hyps[Pappus] = { Collinear[A,B,C], Collinear[D,E,F],
                 Parallel[A,E,B,F], Parallel[B,D,C,E] };
Conc[Pappus] = Parallel[A,D,C,F];
```

The function `Prove[`F`,`f`]` returns the kind of truth of the possible theorem (F,f) as a 4-tuple $\{generic, conditional, degenerate, extraneous\}$ of sets of equations. In the case where the first of these equals $\{1\}$ with all others empty, the output is rendered as `True`.

```
Prove[Hyps[Pappus],Conc[Pappus]]
```

```
True
```

Thus this possible theorem is universally true. Any instance of the hypotheses is an instance of the conclusion, without restriction.

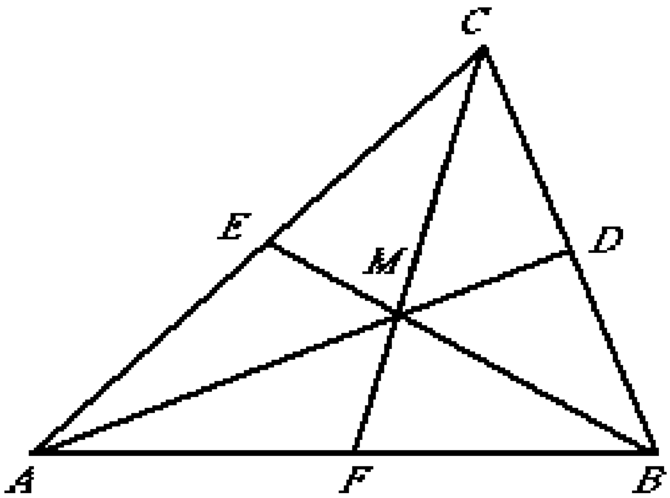

Fig. 2. The Centroid Theorem.

Centroid Theorem. We denote by `Midpoint[`a`,`b`,`c`]` that the midpoint of the line segment between a and b is the point c, and by `Centroid[`a`,`b`,`c`,`d`]` that the centroid of the points a, b, and c is the point d.

```
Hyps[CentroidThm] = { Centroid[A,B,C,M], Midpoint[B,C,D] };
Conc[CentroidThm] = Collinear[A,D,M];
```

```
Prove[Hyps[CentroidThm],Conc[CentroidThm]]
```

```
True
```

Again, this theorem happens to be universally true.

Universal truth is an uncommonly strong property of possible theorems. It means that the entailment holds for arbitrary choices of the points. For example, the Centroid theorem holds even when all the points are collinear.

Collinearity Theorem. Consider the following statement carefully:

```
Hyps[CollinearityThm] = { Collinear[A,B,C], Collinear[A,B,D] };
Conc[CollinearityThm] = Collinear[B,C,D];
```

Again we invoke `Prove` to establish truth:

```
Prove[Hyps[CollinearityThm],Conc[CollinearityThm]]
```

```
{{!Identical[A, B]}, {}, {}, {}}
```

In this case we obtain a generic side polynomial for the possible theorem. The theorem is generically true, and the associated side condition asserts that points `A` and `B` are not identical. The prover has established that `!Identical[A, B]` is a weakest possible (generic) side condition: any other side condition is at least as strong. (Readers should draw a diagram for the case where `A` and `B` coincide to see the problem.)

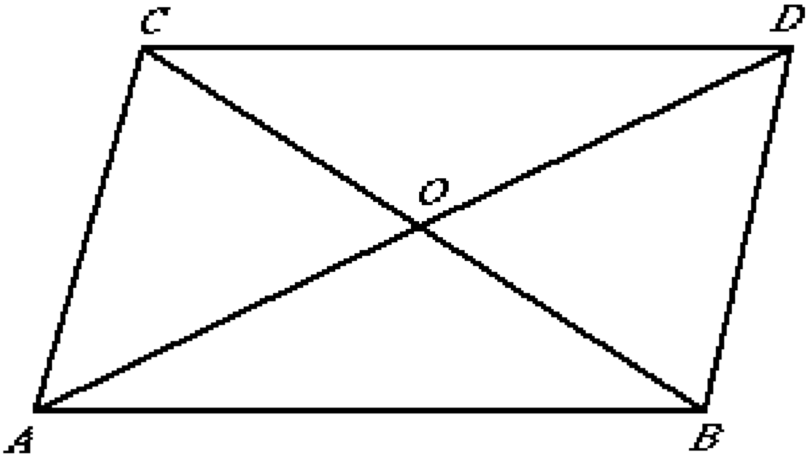

Fig. 3. The Parallelogram Theorem.

Parallelogram Theorem. The following possible theorem says that the diagonals of a parallelogram bisect each other.

```
Hyps[ParallelogramThm] = { Parallel[A,B,D,C],
  Parallel[D,A,C,B], Collinear[O,B,D], Collinear[O,A,C] };
Conc[ParallelogramThm] = EqualLength[A,O,O,C];
```

Here the predicate EqualLength[a,b,c,d] says that the line segments ab and cd are of equal length.

```
Prove[Hyps[ParallelogramThm],Conc[ParallelogramThm]]

{{!Collinear[A,B,C]},
 {!Collinear[A,C,D],!Collinear[B,C,D],!Collinear[B,C,O],
 !Collinear[C,D,O]},
 {},
 {!Collinear[A,C,O]}}
```

This theorem is generically true: the associated side condition states that the points A, B, and C are not collinear, and again, any other generic side condition is at least as strong as this one. We also have five non-generic side conditions. One of these, the side condition Collinear[A, C, O] is a consequence of the hypotheses and hence is *extraneous.* The remaining four side conditions are generically resolving.

Isosceles Theorem. In this example, EqualAngle[a, b, c, d, e, f] says that the angle $\angle abc$ is equal to the angle $\angle def$.

```
Hyps[IsoscelesThm] = {EqualAngle[A,B,C,C,A,B]};
Conc[IsoscelesThm] = EqualLength[A,C,B,C];
```

We obtain

```
Prove[Hyps[IsoscelesThm],Conc[IsoscelesThm]]

{{}, {!Collinear[A, B, C]}, {}, {}}
```

So the possible theorem is generically conditionally true. The conditional predicate `!Collinear[A, B, C]` identifies which of the two generic components gives a theorem.

A Rarely True Theorem. Rarely true theorems are not of great interest, but here is an example:

```
Hyps[NonThm] = {Midpoint[A,B,C]};
Conc[NonThm] = Midpoint[A,C,B];
```

```
Prove[{Midpoint[A,B,C]},Midpoint[A,C,B]]
```

```
{{}, {}, {}, {!Midpoint[A,B,C]}}
```

Thus any side conditions for the possible theorem are at least as strong as the negation of the hypothesis! That is, there is no component of the hypothesis on which the conclusion holds. The theorem fails to hold in a most comprehensive way.

6 Conclusion

Universal truth was considered in [2] and [3], as was the Gröbner basis characterisation given above. The definitions of generic truth and non-degeneracy conditions originate with Wu, [8] and [9], and have been considered also by Chou in [2], where a variant on the Gröbner basis method using fields of rational functions is featured. Conditional truth in general (meaning neither universal truth nor rare truth) was considered in [3] along with the Gröbner basis method of proof. Generically conditional truth was considered in [2] though no Gröbner basis method was given. In [1], two strengths of generic truth were defined in terms of the highest dimension irreducible components of the hypothesis variety, an approach often giving a different notion of generic truth to the one used here and one which Chou argues in [2] is not always the one intended by the user. The notion of a complete set of side polynomials, though hinted at in [3], seems not to have been explicitly considered elsewhere.

More recently, the article [7] takes a similar approach to ours, in that a possible theorem (F, f) is classifiable as universally true (called "geometrically true" in [7]), generically true, neither generically true nor generically false (generically conditionally true in our terms), and generically false. However, this is done by computing with both (elimination ideals generated by) $F \cup \{fz - 1\}$ and $F \cup \{f\}$, whereas our approach considers only Gröbner bases of the former kind of set (that is, side polynomial calculations). The approach in [7] does not seem to be able to provide information in the generically conditionally true case (other than to flag the need for a decomposition), whereas our approach is able to provide side polynomials which eliminate the generic irreducible components on which the conclusion fails to hold. An advantage of the approach in [7] is the possibility of generating additional hypotheses of equational type (rather than just inequations) in the generically false case, although the approach is not guaranteed to do this. Nonetheless, it would be possible to use a combination of the approach in [7] and our approach in such cases: first, that a theorem is generically false could be established using our approach, and then $F \cup \{f\}$ could be considered in an attempt to obtain sufficient additional equational hypotheses.

The main contribution of the current work is to bring together facts which show that a single Gröbner basis calculation for $F \cup \{fz - 1\}$ yields a complete set of side polynomials $\{g_1, g_2, \ldots, g_k\}$ for the possible theorem (F, f), and moreover that this (plus perhaps similar calculations of Gröbner bases for some of the $F \cup \{g_i z - 1\})$ is all that is needed to classify the kind of truth of the theorem and to provide the appropriate complete set of side conditions.

Obtaining the prover. A *Mathematica* Notebook **GeometryExamples.nb** containing the above examples along with the associated *Mathematica* package **GeometryProver.m** are available for downloading from

`http : //www.maths.utas.edu.au/People/dfs/dfs.html`

Acknowledgements. We thank the anonymous referees of the first draft of this paper for their helpful suggestions. The work reported here was partially supported by Australian Research Council Large Grants A49132001 and A49331346.

References

1. Carra Ferro, G. and Gallo, G.: A procedure to prove geometrical statements, in L. Huguet, A. Poli (eds.), *AAECC-5*, Applied algebra, algebraic algorithms, and error-correcting codes : 5th International Conference, AAECC-5, Menorca, Spain, June 15-19, 1987 : proceedings, Lecture notes in computer science 356, Springer-Verlag, Berlin, New York (1989), 141-150.
2. Chou, S.-C.: *Mechanical Geometry Theorem Proving*, D. Reidel (1988).
3. Kapur, D.: Geometry Theorem Proving Using Hilbert's Nullstellensatz, in *Proceedings of the 1986 Symposium on Symbolic and Algebraic Computation* (1986), 202–208.
4. Kapur, D.: A Refutational Approach to Theorem Proving in Geometry, *Artificial Intelligence* 37 (1988), 61-93.
5. Kutzler, B. and Stifter, S.: Automated Geometry Theorem Proving Using Buchberger's Algorithm, in *Proceedings of the 1986 Symposium on Symbolic and Algebraic Computation* (1986), 209-214.
6. Recio, T., Sterk, H. and Velez, M.: Automatic Geometry Theorem Proving, in A.M. Cohen, H. Cuipers and H. Sterk (eds.), *Some Tapas of Computer Algebra*, Algorithms and Computation in Mathematics vol.4, Springer Verlag, (1998).
7. Recio, T., and Velez, M.: "Automatic Discovery of Theorems in Elementary Geometry," *J. Automated Reasoning* 23 (1999), 63-82.
8. Wu, W.-t.: On the Decision Problem and the Mechanization of Theorem Proving in Elementary Geometry, *Scientia Sinica* **21** (1978), 157-179.
9. Wu, W.-t.: *Mechanical Theorem Proving in Geometries: Basic Principles*, Springer, New York, 1994.