Automatic Geometric Theorem Proving

Samuel Nartey (samuel@aims.ac.za)
African Institute for Mathematical Sciences (AIMS)

Supervised by Barry Green
University of Stellenbosch

May 24, 2007

Abstract

We present an algorithmic method for proving geometric theorems in the Euclidean plane.

The geometric theorems considered in the automatic theorem proving assert that the configurations in question — for example points, lines, or circle in the Euclidean plane — intersect at a common point.

We use Algebraic translations to enable us to convert theorems of this kind into polynomials. We then calculate the Groebner basis and take into consideration any degenerate cases that may need to be excluded. These steps are necessary in order to employ the computer program Singular to prove the theorems.

We demonstrate the applicability of our method with Thales' Theorem, The Theorem of Apollonius and Pappus Theorem

The proofs produced by Automatic Theorem Proving describe the procedure for obtaining a given conclusion from its hypothesis.

Contents

1. Introduction

This essay will discuss algebraic methods in automatic geometric theorem proving, using Groebner basis and Singular. Proving geometric statements algorithmically is an area of research which has particular importance in the fields of robotics and artificial intelligence. While a computer implementing Singular can hardly be said to be "thinking" geometrically in the same sense as a human might, it can lend a computer the ability to interact with its physical environment in a fairly sophisticated and independent manner.

In general, we will follow the subject as presented in [DC96]. First, we will discuss some concepts from algebraic geometry and commutative algebra that will be needed throughout the essay. After examining rings, ideals and Groebner bases, we will discuss the translation of geometric statements to the realm of algebra. Next, we will discuss examples of geometric theorems and how these can be translated into polynomials. Lastly we will use Singular to prove three geometric theorems, of which two will require us to draw on radical membership to complete the proof.

A schematic overview of the Automatic Geometric Theorem Proving algorithm can be found in Figure 1.1.

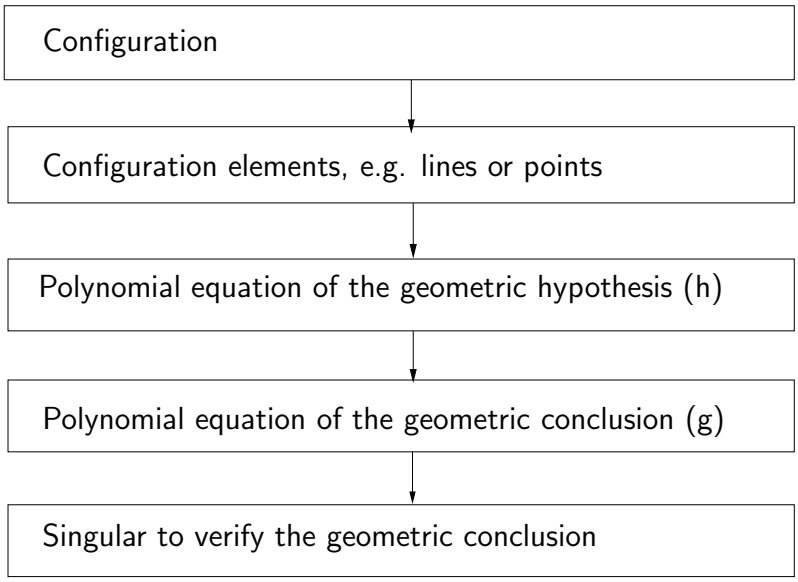

Figure 1.1: The process of Automatic Geometric Theorem Proving using Singular

To examine the same process in more detail, we can alternatively write out the procedure to prove a theorem geometrically in a maximum of 4 steps.

1. Translate the hypothesis of the theorem to the vanishing of a set of polynomials

$$h_1, \ldots, h_m \in K[u_1, \ldots, u_r, x_1, \ldots, x_s],$$

where the variables $u_1, \ldots, u_r$ are the parameters of the geometric configuration and the values of the variables $x_1, \ldots, x_s$ are determined by those of $u_1, \ldots, u_r$.

2. Translate the conclusion(s) of the theorem into the vanishing of a polynomial g.
3. We say that g follows strictly from $h_1, \ldots, h_m$ if $g \in \sqrt{\langle h_1, \ldots, h_m \rangle}$.
4. We say that g follows generically from $h_1, \ldots, h_m$ if $V(g)$ contain the irreducible components of $V(h_1, \ldots, h_m)$ on which $u_1, \ldots, u_r$ are algebraically independent.

The proof for any theorem will terminate at either step 3 or step 4, depending on the Groebner basis.

To complete step 3, we need to compute a Groebner basis for the ideal in the polynomial ring. If we can, in fact, not obtain the Groebner basis $\{1\}$, then the cause of our problem lies in the variety defined by the hypotheses $V(h_1, \ldots, h_m)$.

In cases such as these, we then apply step 4, where our goal will be to develop a general method for establishing the validity of our conclusion, using only those components of the configuration that do not correspond to degenerate cases of the theorem. In other words, we will be interested only in those components of the configuration on which the u_i are algebraically independent.

2. Basic Concepts from Algebraic Geometry and Commutative Algebra

In this chapter, we shall give a summary of the basic concepts from algebraic geometry and commutative algebra that will be encountered in this essay.

2.1 Polynomials Ideals

Let K be a field and denote by $K[X_1, \ldots, X_n] = K[X]$ the polynomial ring in n variables over K.

Definition 2.1. *A subset I of the polynomial ring in n variables $K[X]$ over the field K is an ideal if it satisfies*

1. $0 \in I$.
2. *If* $a, b \in I$, *then* $a + b \in I$.
3. *If* $a \in I$ *and* $b \in K[X_1, \ldots, X_n]$, *then* $a.b \in I$.

Definition 2.2. *The set of polynomials that vanish in a given set $S \subset K[X]$, i.e*

$$I(S) := \{f \in K[X] : f(a_1, \ldots, a_n) = 0 \ \forall (a_1, \ldots a_n) \in S\},$$

is an ideal, called the vanishing ideal of S.

Definition 2.3. *The ideal generated by a finite set of polynomials $f_1, \ldots, f_s$ is defined as,*

$$\langle f_1, \ldots, f_s \rangle := \{f | f = g_1 f_1 + \cdots + g_s f_s, \text{ for some } g_i \in K[X]\}.$$

An ideal is called principal if it can be generated by a single polynomial.

Observation 2.1. *A central result called the Hilbert Basis Theorem implies that every ideal I in $K[X_1, \ldots, X_n]$ is finitely generated. i.e.,there exist $g_i, \ldots, g_t \in I$ such that*

$$I = \left\{ \sum_{i=1}^{t} h_i g_i | h_1, \ldots, h_t \in K[X_1, \ldots, X_n] \right\}.$$

We write $I = \langle g_1, \ldots, g_t \rangle$.
We will mention this precisely in Section 2.7.

2.2 Algebraic Varieties

An (affine) algebraic variety is the zero set of a finite collection of polynomials.

Definition 2.4. *Let $f_1, \ldots, f_s$ be polynomials in $K[X]$.*
Let the set V be

$$V(f_1, \ldots, f_s) := \{(a_1, \ldots, a_n) \in K[X] : f_i(a_1, \ldots, a_n) = 0 \text{ for } 1 \leq i \leq s\}.$$

Then we call $V(f_1, \ldots, f_s)$ the affine variety defined by $f_1, \ldots, f_s$.

2.3 Monomial Orderings

To study bases for ideals, we need a way of ordering monomials. In the univariate case, this is straightforward, since we can define $X^a > X^b$ as being true if and only if $a > b$. But in the multivariate case it is different.

Definition 2.5. *A monomial in variables $X = (X_1, \ldots, X_n)$ is a product of the form*

$$X = X_1^{\alpha_1} \cdots X_n^{\alpha_n},$$

where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_+^n$.

Definition 2.6. *A monomial order on $K[X_1, \ldots, X_n]$ is any relation $>$ on $\mathbb{Z}_+^n$, or equivalently, any relation on the set of monomials $X^\alpha, \alpha \in \mathbb{Z}_+^n$, satisfying:*

1. *$>$ is a total order on $\mathbb{Z}_+^n$.*
2. *If $\alpha > \beta$ and $\gamma \in \mathbb{Z}_+^n$, then $\alpha + \gamma > \beta + \gamma$.*
3. *Any nonempty subset of $\mathbb{Z}_+^n$ has a smallest element under $>$.*

Examples of monomial orders include:

1. The lexicographic order:
   For every $\alpha, \beta \in \mathbb{Z}_+^n$, we say $\alpha >_{\text{lex}} \beta$ (or $X^\alpha >_{\text{lex}} X^\beta$) if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the leftmost nonzero entry is positive.
   For example $\alpha = (1, 2, 0) >_{\text{lex}} (1, 1, 3) = \beta$, since $\alpha - \beta = (0, 1, -3)$.
2. The graded lex order:
   For every $\alpha, \beta \in \mathbb{Z}_+^n$, we say $\alpha >_{\text{grlex}} \beta$ (or $X^\alpha >_{\text{grlex}} X^\beta$)
   if,

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|,$$

or

$$|\alpha| = |\beta| \text{ and } \alpha >_{\text{lex}} \beta.$$

In other words, grlex orders by total degree first and breaks ties using the lex order. For example, $\alpha = (1, 2, 3) >_{\text{grlex}} (3, 2, 0) = \beta$, since $|\alpha| = 6 > 5 = |\beta|$.

3. The graded reverse lex order:
For every $\alpha, \beta \in \mathbb{Z}_+^n$, we say $\alpha >_{\text{grevlex}} \beta$ (or $X^\alpha >_{\text{grevlex}} X^\beta$) if,

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|,$$

or

$$|\alpha| = |\beta| \text{ and } \alpha - \beta \in \mathbb{Z}^n.$$

the rightmost nonzero entry is negative.
For example, $\alpha = (1, 5, 2) >_{\text{grevlex}} (2, 3, 3) = \beta$, since $|\alpha| = |\beta| = 8$ and $\alpha - \beta = (-1, 2, -1)$.

Definition 2.7. *Given a monomial order $>$ and a polynomial $f(X) = \sum_{\alpha \in S} f_\alpha X^\alpha$ we define*

1. *The multidegree of f is*

$$\textit{multideg}(f) = \max_{\alpha \in S} \alpha,$$

where the maximum is taken over the given order $>$.

2. *The leading coefficient of f is*

$$LC(f) = f_{multideg(f)}.$$

3. *The leading monomial of f is*

$$LM(f) = X^{multideg(f)}.$$

4. *The leading term of f*

$$LT(f) = LC(f).LM(f).$$

2.4 Division Algorithm

This is taken from [Gre07a]

Review in $K[X_1, \ldots, X_n]$: $g(X) = g(X)f(X) + r(X)$. Remainder $r(X) = 0$ or deg $r(X) <$ deg $f(X)$.
Induction step:

$$g(X) := g(X) - \tfrac{LT(g)}{LT(f)} f,$$

and

$$q(X) := q(X) + \tfrac{LT(g)}{LT(f)},$$

finally $g(X)$ is the remainder.

Let $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$. We fix a monomial ordering $>$ on $\mathbb{Z}^n_{\geqslant 0}$. Let $g \in K[X_1, \ldots, X_n]$, we want to find

$$g = q_1 f_1 + \cdots + q_s f_s + r,$$

where r is the remainder with certain properties.
Algorithm:
If $LT(g)$ is divisible by $LT(f_1)$, then

$$g := g - \tfrac{LT(g)}{LT(f_1)} f_1,$$

$$q_1 := q_1 + \tfrac{LT(g)}{LT(f_1)}.$$

else if $LT(g)$ is divisible by $LT(f_2)$, then

$$g := g - \tfrac{LT(g)}{LT(f_2)} f_2,$$

$$q_2 := q_2 + \tfrac{LT(g)}{LT(f_1)}.$$

else if...
Otherwise $LT(g)$ is not divisible by any $LT(f_i)$, then put $LT(g)$ to the remainder:

$$g := g - LT(g),$$

$$r := r + LT(g).$$

Start with the new g.
Result

$$g = q_1 f_1 + \cdots + q_s f_s + r,$$

with $r = 0$ or r is a sum of monomials (with coefficients) which are all not divisible by any $LT(f_1), \ldots, LT(f_s)$.

2.5 S-Polynomial

Definition 2.8. *This is taken from [Gre07a]*

Let $f, g \in K[X_1, \ldots, X_n]$.
Suppose α=multideg(f), β=multideg(g) and γ=($\gamma_1, \ldots, \gamma_n$) where γ_i=max(α_i, β_i) $\forall i$,

Use X^γ to denote the least common multiple of $LM(f) = X^\alpha$, and $LM(g) = X^\beta$, such that

$$LCM(LM(f), LM(g)) := X^\gamma.$$

Then the S-Polynomial of f and g is defined to be

$$S(f, g) = \frac{X^\gamma}{LT(f)} f - \frac{X^\gamma}{LT(g)} g.$$

2.6 Groebner Bases

Definition 2.9. *A monomial ideal is a polynomial ideal that can be generated by monomials.*

2.7 Remark

A polynomial belongs to a monomial ideal I if and only if all its terms are in I.

Theorem 2.10 (Dickson's lemma). *Every monomial ideal is finitely generated. [MIT]*
By Observation 2.1

Definition 2.11. *Let $G = \{g_1, \ldots, g_t\}$ be a set of polynomials and $I = \langle g_1, \ldots, g_t \rangle$. G is called Groebner basis for the ideal I if $f \in I$ if and only if the remainder of the division of f by the polynomials in G is always zero, independent of the order in which we perform the division. [MIT]*

Theorem 2.12. *Every ideal I has a Groebner basis G.*
Furthermore, $I = \langle g_1, \ldots, g_s \rangle$. [MIT]

2.8 Buchberger's Algorithm

The traditional algorithm to effectively compute Groebner bases is the Buchberger's algorithm, and was developed by Bruno Buchberger in 1965.

Proposition 2.13. *Let G be a Groebner basis for the ideal $I \subset k[X_1, \ldots, X_n]$ and let $f \in k[X_1, \ldots, X_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero. [MIT]*

Definition 2.14. *A minimal Groebner basis for a polynomial ideal I is a Groebner basis G for I such that*

1. *$LC(p) = 1$ for all $p \in G$.*
2. *For all $p \in G, LT(p) \notin \langle LT(G \backslash \{p\})\rangle$.[MIT]*

Definition 2.15. *A reduced Groebner basis for a polynomial ideal I is a Groebner basis G for I such that*

1. *$LC(p) = 1$ for all $p \in G$.*
2. *For all $p \in G$, no monomial of p lies in $\langle LT(G \backslash \{p\})\rangle$.[MIT]*

Theorem 2.16. *For a given monomial order, a polynomial ideal has a unique reduced Groebner basis.[MIT]*

Corollary 2.17. *Two ideals are equal if and only if they have the same reduced Groebner basis.[MIT]*

Definition 2.18. *Let $f, g \in k[X_1, \ldots, X_n]$, with multidegrees a and b, respectively.*

$$S(f, g) = \frac{X^c}{LT(f)} f - \frac{X^c}{LT(g)} g,$$

where c=(max(a_1, b_1),...,max(a_n, b_n)), so X^c is the least common multiple of $LT(f)$ and $LT(g)$.[MIT]

Theorem 2.19. *A basis $G = \{g_1, \ldots, g_n\}$ for nonzero ideal I is a Greobner basis for I if and only if the division of $S(g_i, g_j)$ by G is zero for all $i \neq j$.[Gre07a]*

The Buchberger Algorithm

This algorithm is taken from [Gre07a]

Input: A set $F = \{f_1, \ldots, f_s\}$ of polynomials in $K[X_1, \ldots, X_n]$ and a monomial order.
Output: A Greobner basis $G = \{g_1, \ldots, g_t\}$ for $I = \langle f_1, \ldots, f_s\rangle$.
Algorithm:

1. (Initialization) Let $G := (f_1, \ldots, f_s)$ be the ordered tuple obtained from F.

2. For $p, q \in G$,
   (a) Let $\alpha = multideg(p), \beta = multideg(q), \gamma_i = max(\alpha_i, \beta_i)$, and $\gamma = (\gamma_1, \ldots, \gamma_n)$
   (b) Compute the polynomial

$$S(p,q) = \frac{X^\alpha}{LT(p)}.p - \frac{X^\gamma}{LT(q)}.q.$$

   (c) Compute the remainder r of the division of $S(p,q)$ with the ordered set G, denoted as $R(S(p,q), G)$ using the given monomial order.
   (d) If $r \neq 0$, then $G := (G, r)$; goto Step 2; If $r = 0$ for all $p, q \in G$, then goto Step 3.

3. Output G.

Theorem 2.20. *The Buchberger algorithm terminates in finite time. It computes a Groebner basis for the ideal $I = \langle f_1, \ldots, f_s \rangle$ with respect to the given monomial order.[MIT]*

2.9 Radical Membership

Definition 2.21. *A radical of an ideal $I \subset K[X_1, \ldots, X_m]$, denoted $\sqrt{I}$, is defined by*

$$\sqrt{I} = \{f \in K[X_1, \ldots, X_m] | f^m \in I \text{ for some } m\}.$$

An ideal I is radical if $I = \sqrt{I}$.

Consider an ideal $I = \langle f_1, \ldots, f_s \rangle \subset K[X_1, \ldots, X_n]$, and a polynomial f, for which we want to check whether $f \in \sqrt{I}$. Since $\sqrt{I}$ is also an ideal, we could compute a Groebner basis for it, and then reduce the problem to ideal membership. However, it is often more efficient to instead use the following result (Rabinowitch's trick): $f \in \sqrt{I}$ if and only if $1 \in \langle f_1, \ldots, f_s, 1 - yf \rangle$, where y is a new additional variable.

Proposition 2.22. *Let K be an arbitrary field and $I = \langle f_1, \ldots, f_s \rangle \subset K[X_1, \ldots, X_n]$ be an ideal. Then $f \in \sqrt{I}$ if and only if the constant polynomial 1 belongs to the ideal $\tilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset K[X_1, \ldots, X_n, y]$ (in which case $\tilde{I} = K[X_1, \ldots, X_s, y]$). [Gre07a]*

Proof. This proof is taken from [Gre07a]

Suppose $1 \in \tilde{I}$. We want to show $f^m \in I$ for some m so that $f \in \sqrt{I}$.

As $1 \in \tilde{I}$, we have a writing

$$1 = \sum_{i=1}^{s} p_i(X_1, \ldots, X_n, y) f_i + q(X_1, \ldots, X_n, y)(1 - yf)$$

for some polynomials $p_i, q \in K[X_1, \ldots, X_n, y]$.

As y is a variable we set $y = \frac{1}{f}$ in the equation above and obtain

$$1 = \sum_{i=1}^{s} p_i(X_1, \ldots, X_n, \frac{1}{f}) f_i + q(X_1, \ldots, X_n, \frac{1}{f})(1 - \frac{1}{f} f)$$

$$1 = \sum_{i=1}^{s} p_i(X_1, \ldots, X_n, \frac{1}{f}) f_i$$

Multiply both sides by a large enough power f^m, we clear all denominators and obtain

$$f^m = \sum_{i=1}^{s} A_i f_i \in I$$

where $A_i \in K[X_1, \ldots, X_n]$.

Suppose $f \in \sqrt{I}$. Then for some m we have

$$f^m \in I \subset \tilde{I}$$

We also have $1 - yf \in \tilde{I}$ and consequently

$$1 = y^m f^m + (1 - y^m f^m) = y^m f^m + (1 - yf)(1 + yf + y^2 f^2 + \ldots + y^{m-1} f^{m-1} \in \tilde{I}$$

as desired. □

The proposition above immediately leads to the radical membership algorithm:

That is to determine if $f \in \sqrt{(f_1, \ldots, f_s)} \subset K[X_1, \ldots, X_n]$ we compute a reduced Groebner basis for the ideal $\langle f_1, \ldots f_s, 1 - yf \rangle \subset K[X_1, \ldots, X_n, y]$, with respect to some ordering. If the result is $\{1\}$, then $f \in \sqrt{I}$, otherwise $f \notin \sqrt{I}$.

3. Algebraic Formulation of Geometric Theorems

This chapter explains the basic ideas underlying the methods we use to express the hypothesis and the conclusion as polynomials. We suppose there are two sets of polynomials, one describing the hypothesis and the other describing the conclusion. In this chapter, we consider the class of theorems whose algebraic formulations involves polynomial equations and inequalities of the form,

$$\mathrm{hypothesis} : \mathrm{h_1(X)} = 0, \ldots, \mathrm{h_s(X)} = 0,$$

and

$$\mathrm{conclusion} : \mathrm{g(X)} = 0,$$

where $X = (X_1, \ldots, X_n)$ are geometric entities. The polynomials are all in X with coefficents in the geometry-associated field R. Proving a theorem in geometry implies that

$$\text{for all } X, [h_1(X) = 0 \ldots = h_s(x) = 0],$$
$$\text{it implies that } g(X) = 0.$$

3.1 Steps in Translation of Geometric Statements into Polynomials

1. Introduce a coordinate system
2. Use the geometry properties of the configuration to write the polynomial.

Remark 3.1. *Translating the hypotheses of a theorem into a system of polynomial equations can be accomplished most readily if we think of constructing a figure illustrating the configuration in question point by point.*

3.2 Translation

We suppose that there are two sets of polynomials, where one describes the hypothesis and the other describes the conclusion. This can be done as follows.

We suppose that the hypothesis of the configuration(e.g points, circles or lines) is given by polynomial equations in $X_1, \ldots X_l$. For example, two points (say (X_1, X_2) and (X_3, X_4)) on the same line (say $y = Ax + B$) are given by the following two equations:

$$X_2 - AX_1 - B = 0.$$

$$X_4 - AX_3 - B = 0.$$

We will say the hypothesis is given by $h_1 = X_2 - AX_1 - B$ and $h_2 = X_4 - AX_3 - B$. In general, the hypothesis is given by polynomial equations $h_1(\underline{X}) = \ldots = h_n(\underline{X}) = 0$.

In the same manner we can describe one or more conclusion by the polynomial equations in $X_1, \ldots, X_l$. For example, we might want to test to see whether a certain point is on the line above, say $(\frac{X_1+X_3}{2}, \frac{X_2+X_4}{2})$. This is express by the following equation:

$$\frac{X_2 + X_4}{2} - A(\frac{X_1 + X_3}{2}) - B = 0,$$

or

$$(X_2 + X_4) - A(X_1 + X_3) - 2B = 0.$$

In general, the conclusion holds when $g_1(\underline{X}) = \ldots = g_k(\underline{X}) = 0$ for all $\underline{X}$ that characterize the configuration. So, the conclusion holds if and only if

$$\forall\,(\underline{X} : h_1(\underline{X}) = \ldots = h_n(\underline{X}) = 0) \Longrightarrow (g_1(\underline{X}) = \ldots = g_k(\underline{X}) = 0)\,.$$

Now we use the algebra we developed in Chapter two. We will work in the ring $K[X_1, \ldots, X_l]$. The 'hypothesis ideal' $I \subset R$ is defined as follows:

$$I = (h_1, \ldots, h_n)$$

Suppose g_i is in I, then

$$g_i = f_1 h_1 + \ldots + f_n h_n \text{ for some } \; f_1, \ldots, f_n.$$

So, if g_i is in I and $h_i(\underline{X}) = 0$, then $g_i(\underline{X}) = 0$. In practice, this means that the conclusion holds if the hypothesis is such as described by the h_i. Now the only thing we need is a way to determine whether $g_i \in I$.

We then calculate a Groebner basis G of I. For each g_i determine the remainder on division of g_i by G. If this remainder is zero for every $i = 1, \ldots, k$, then every g_i is in I.

Definition 3.2 (Admissibility). *A geometry theorem is said to be admissible if both its hypothesis and its conclusion admit translations into polynomials.*

3.3 Admissible Geometric Theorem

Let $U_1, \ldots, U_m$ be the independent variables of a geometric theorem.

Let $X_1, \ldots, X_m$ be the dependent variables of a geometric theorem.

The hypotheses of the theorem will be represented by the collection of the polynomial equations in the U_i, X_j.

The conclusions of the theorem will also be expressed as polynomials in the U_i, X_j.

It is reasonable to consider the case of one conclusion since, if there are more, we can simply treat them one at a time.

Let the conclusion be

$$g(U_1, \ldots, U_m, X_1, \ldots, X_n) = 0.$$

We want to deduce that g follows from $h_1, \ldots, h_n$ algebraically. We need g to vanish whenever $h_1, \ldots, h_n$ do, and this leads to the application of algebraic varieties.

Let the variety be

$$V = V(h_1, \ldots, h_n) = \{\underline{a} \in K^{m+n} | h_i(\underline{a}) = 0 \quad for \quad 1 \leq i \leq n\}.$$

And, let the ideal be

$$I(V) = \{f \in K[U_1, \ldots, U_m, X_1, \ldots, X_n] | f(\underline{a}) = 0 \quad for \quad all \quad \underline{a} \in V\}.$$

• For degenerate cases the configuration is distorted. A typical example is that of a parallelogram, with one vertex which is dependent. If we set this vertex to zero, the parallelogram collapses.

Remark 3.3. *It is not absolutely necessary to distinguish between the independent variables and the dependent variables for confirming theorems, but it is very helpful to do so for determining non-degeneracy conditions.*

Definition 3.4. *The conclusion g follows strictly from the hypotheses $h_1, \ldots, h_n$ if $g \in I(V) \subset K[U_1, \ldots, U_m, X_1, \ldots, X_n]$ where $V = V(h_1, \ldots, h_n)$.*

Proposition 3.5. *If $g \in \sqrt{\langle h_1, \ldots, h_n \rangle} = \{f \in K | f^s \in \langle h_1, \ldots, h_n \rangle \quad for \quad some \quad s\}$, then g follows strictly from $h_1, \ldots, h_n$. [DC96]*

Proof. This proof is taken from [DC96].

Suppose that

$$g \in \sqrt{\langle h_1, \ldots, h_n \rangle}$$

then for suitable s

$$g^s = \sum_{i=1}^{n} A_i h_i, \ A_i \in K$$

Now for each $\underline{a} \in V$

$$g^s(\underline{a}) = \sum_{i=1}^{n} A_i(\underline{a}) h_i(\underline{a}) = \sum_{i=1}^{n} A_i(\underline{a}).0 = 0$$

Therefore $g(\underline{a}) = 0$, i.e. $g \in I(V)$. □

3.4 Examples of Translation of Geometric Statements into Polynomials

To illustrate the translation of geometric statements into a suitable system of algebraic equations, we consider a few examples.

3.4.1 Parallel lines

Two lines that are parallel can be translated into polynomials as follows. Let A, B, C, D be points in the plane.

Let $\overline{AB}$ be parallel to $\overline{CD}$, as shown in figure 3.1.

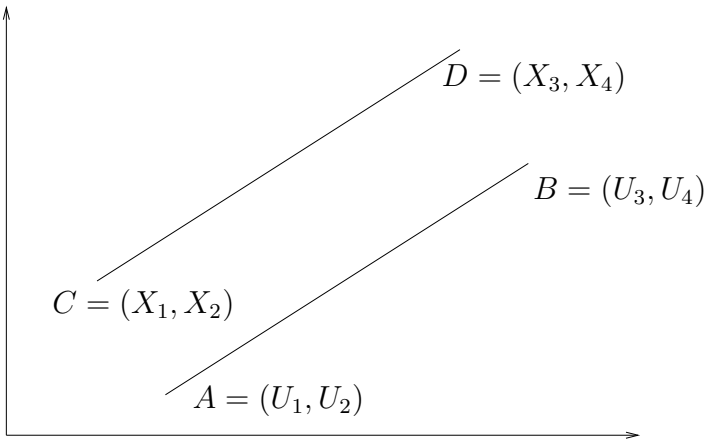

Figure 3.1: Parallel lines

Since two lines that are parallel have the same slope, the geometric hypotheses (h) of the $\overline{AB} \| \overline{CD}$ may be translated into polynomial relations as:

$$\overline{AB} \| \overline{CD}$$

$$\frac{U_4 - U_2}{U_3 - U_1} = \frac{X_4 - X_2}{X_3 - X_1}$$

$$h = (U_4 - U_2)(X_3 - X_1) - (U_3 - U_1)(X_4 - X_2) = 0.$$

3.4.2 Perpendicular Lines

Let $\overline{AB}$ be perpendicular to $\overline{CD}$, as shown in figure 3.2.

Since $\overline{AB}$ is perpendicular to $\overline{CD}$, then we have

$$\overline{AB} \perp \overline{CD}$$

$$\frac{X_4 - X_2}{X_3 - X_1} = -\left(\frac{U_4 - U_2}{U_3 - U_1}\right)^{-1}$$

$$\frac{X_4 - X_2}{X_3 - X_1} = \frac{U_1 - U_3}{U_4 - U_2}$$

$$h = (U_4 - U_2)(X_4 - X_2) - (U_1 - U_3)(X_3 - X_1) = 0.$$

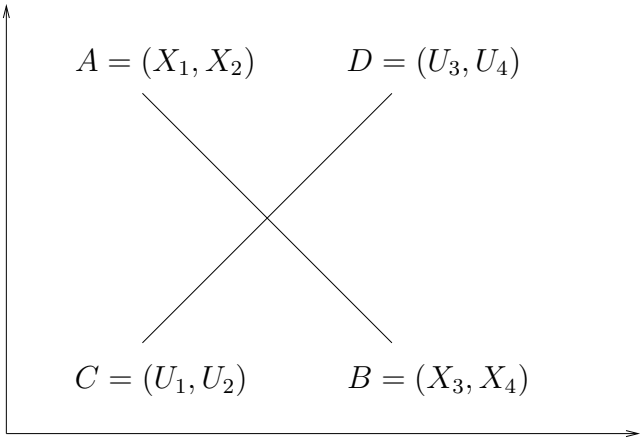

Figure 3.2: Perpendicular Lines

3.4.3 Collinear

Let A, B, C be collinear in the plane, as shown in figure 3.3.

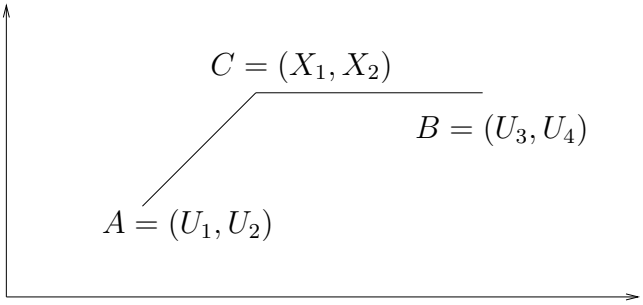

Figure 3.3: Collinear

Using the slope formula, we have

$$\overline{AC} = \overline{BC}$$
$$\frac{X_2 - U_2}{X_1 - U_1} = \frac{X_2 - U_4}{X_1 - U_3}$$
$$h_1 = (X_2 - U_2)(X_1 - U_3) - (X_2 - U_4)(X_1 - U_1) = 0.$$

3.4.4 Circle

Let C lie on a circle of radius $\overline{AB}$ and centre A, as shown in figure 3.4.

We can then write

$$|AC|^2 = |AB|^2$$
$$(X_2 - U_2)^2 + (X_1 - U_1)^2 = (U_4 - U_2)^2 + (U_3 - U_1)^2$$
$$h = (X_2 - U_2)^2 + (X_1 - U_1)^2 - (U_4 - U_2)^2 - (U_3 - U_1)^2 = 0.$$

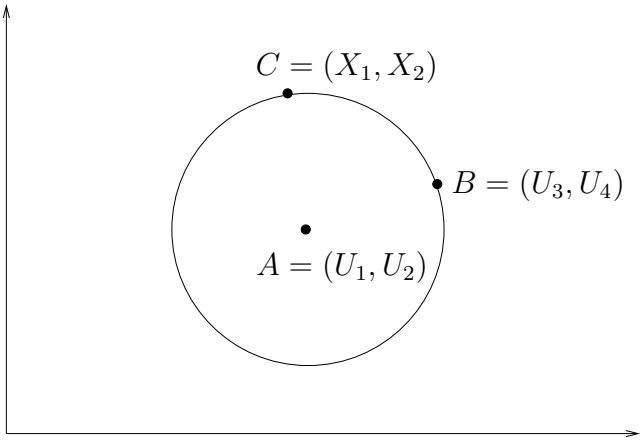

Figure 3.4: Circle

3.4.5 Midpoint

Let C be the mid-point of $\overline{AB}$, as shown in figure 3.5.

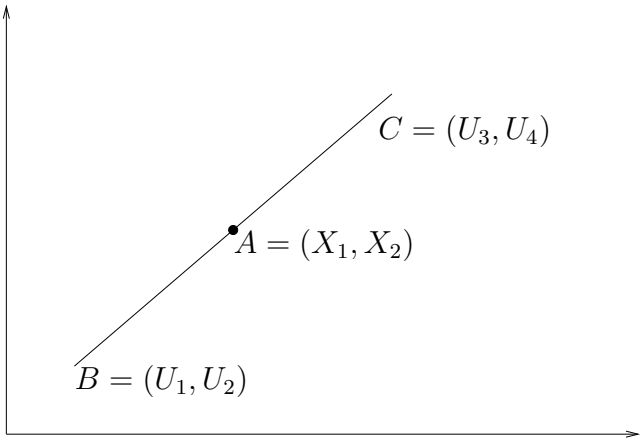

Figure 3.5: Midpoint

Since C is the mid-point of $\overline{AB}$, it implies that

$$\overline{AB} = \overline{AC}$$

We use Pythagoras' theorem to find $\overline{AB}$, $\overline{AC}$. This yields

$$(X_1 - U_1)^2 + (X_2 - U_2)^2 = (X_1 - U_3)^2 + (X_2 - U_4)^2$$

$$h_1 = (X_1 - U_1)^2 + (X_2 - U_2)^2 - (X_1 - U_3)^2 - (X_2 - U_4)^2 = 0.$$

Also, C is the mid-point of $\overline{AB}$, which implies that ABC are collinear, i.e., they lie in the same straight line.
Then

$$\frac{X_2 - U_2}{X_1 - U_1} = \frac{X_2 - U_4}{X_1 - U_3}$$

$$h_2 = (X_2 - U_2)(X_1 - U_3) - (X_2 - U_4)(X_1 - U_1) = 0.$$

4. Proving Translated Theorems

We have seen that we can translate geometric statements into systems of algebraic equations in the ring $K[u_1, \ldots, u_r, x_1, \ldots x_s]$: $h_1, \ldots, h_m$ (the hypotheses) and $g_1, \ldots, g_s$ (the conclusions).

4.1 Thales' Theorem

Thales' theorem (named after Thales of Miletus) states that if A, B and C are points on a circle where the line AC is a diameter of the circle, then the angle ABC is a right angle. The geometry of this situation is shown below in figure 4.1

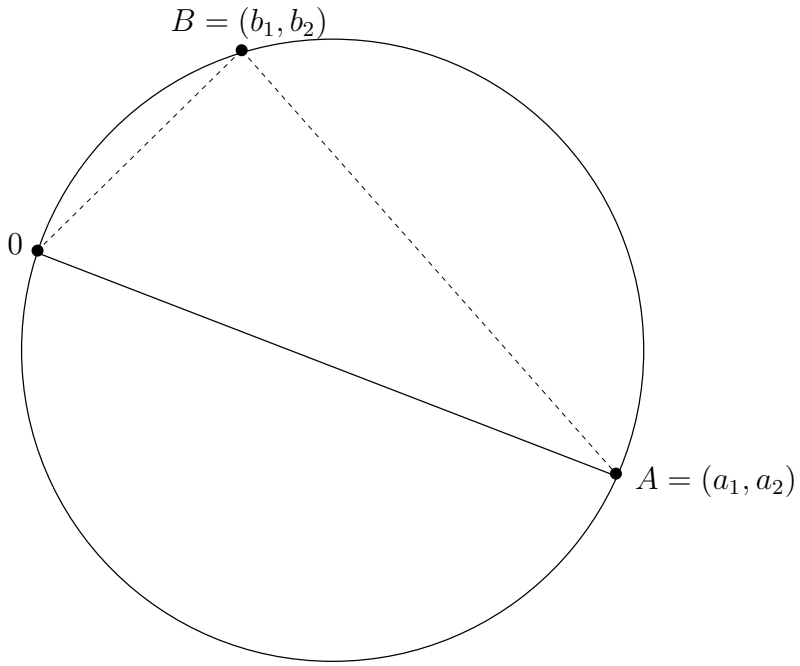

Figure 4.1: Thales' Theorem

The line OA is the diameter. The point B is a point on the circle.

We have to prove that $OB \perp BA$.

Let the origin be at the point O. The line segment OA is the diameter of the circle.

Let s be the raduis of the circle. Then

$$OA = 2 * \text{radius}$$

The coordinates of O, A and B are, as in the figure, set to $(0, 0)$, (a_1, a_2) and (b_1, b_2).

Then

$$OA^2 = a_1^2 + a_2^2$$

giving

$$OA^2 = (2s)^2$$

This implies that

$$a_1^2 + a_2^2 = (2s)^2$$

And so

$$h_1 = a_1^2 + a_2^2 - (2s)^2 = 0.$$

Let the coordinates of point B be

$$B = (b_1, b_2)$$

Point B is on the circle, so

$$(b_1 - \frac{1}{2}a_1)^2 + (b_2 - \frac{1}{2}a_2)^2 = s^2$$

This implies that

$$h_2 = (2b_1 - a_1)^2 + (2b_2 - a_2)^2 - (2s)^2 = 0.$$

The hypotheses of the theorem are:

$$\begin{cases} h_1 = a_1^2 + a_2^2 - (2s)^2 = 0, \\ h_2 = (2b_1 - a_1)^2 + (2b_2 - a_2)^2 - (2s)^2 = 0. \end{cases}$$

The conclusion of the theorem is

$$OB \perp BA$$

$$g = b_1(b_1 - a_1) + b_2(b_2 - a_2) = 0$$

The hypothesis is characterized by the ideal

$$I = (h_1, h_2) \subset Q(a_1, a_2, b_1, b_2, s)$$

We want to show that $g \in I$.

Testing to see if $g \in I$ is done in Singular as follows:

```
  SINGULAR                                 /
 A Computer Algebra System for Polynomial Computations   /   version 3-0-2
                                                        0<
     by: G.-M. Greuel, G. Pfister, H. Schoenemann         \   July 2006
FB Mathematik der Universitaet, D-67653 Kaiserslautern     \
> // ** The ring we use is **;
. ring r=0,(a1,a2,b1,b2,s),lp;
>
. // ** The hypotheses are **;
. poly h1=a1^2+a2^2-(2*s)^2;
> poly h2=(2*b1-a1)^2+(2*b2-a2)^2-(2*s)^2;
>
. // ** The conclusion is **;
. poly g=b1*(b1-a1)+b2*(b2-a2);
```

```
>
. // ** The verification of the conclusion is **;
. ideal i=h1,h2;
> groebner(i);
_[1]=a2^2*b1^2+a2^2*b2^2-2*a2*b1^2*b2-2*a2*b2^3+b1^4+2*b1^2*b2^2-4*b1^2*s^2+b2^4
_[2]=a1*b1+a2*b2-b1^2-b2^2
_[3]=a1*a2*b2+3*a1*b1^2-a1*b2^2-a2^2*b1+4*a2*b1*b2-4*b1^3-4*b1*b2^2+4*b1*s^2
_[4]=a1^2-4*a1*b1+a2^2-4*a2*b2+4*b1^2+4*b2^2-4*s^2
> reduce(g,groebner(i));
0
```

This shows that $g \in \langle h_1, h_2 \rangle$, so the theorem described by conclusion g holds in the hypotheses described by h_1, h_2.

4.2 The Theorem of Apollonius

Let ABC be a right triangle in the plane, with a right angle at A. The midpoint of the three sides and the foot of the altitude drawn from A to the line BC lie on a circle.

The diagram is shown in figure 4.2

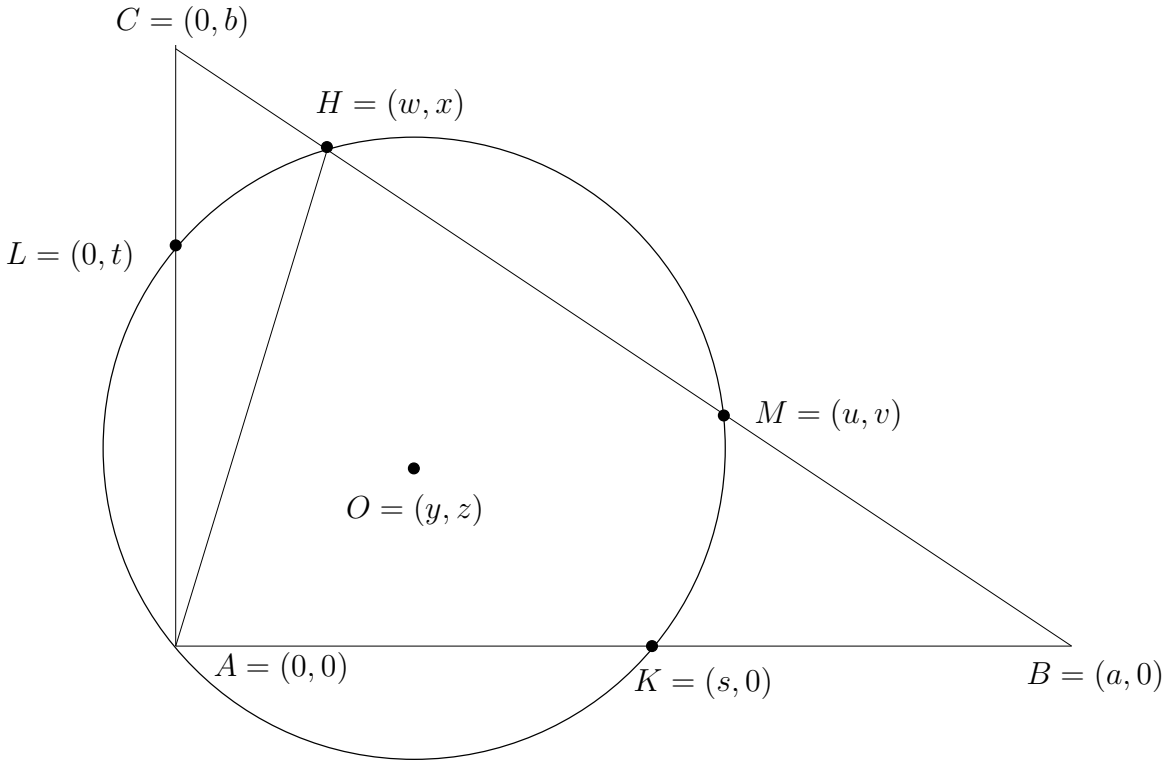

Figure 4.2: Theorem of Apollonius

Place A at $(0, 0), B(a, 0)$. Since the angle at A is a right angle, we have $C = (0, b)$.

Let the three midpoints have coordinates $K = (s, 0)$, $L = (0, t)$, and $M = (u, v)$.

We use the naming convention so that a, b are arbitrary, whereas $s, \ldots, z$ are determined by the values of a, b.

K is a midpoint if the segments $2AK = AB$, that is $2s = a$, which gives us

$$h_1 = 2s - a = 0.$$

L as a midpoint gives us

$$h_2 = 2t - b = 0.$$

and M is a midpoint if $BM = BC$. This means that,

$$2[(u, v) - (a, 0)] = (0, b) - (a, 0).$$

This gives us that

$$h_3 = 2u - a = 0,$$

$$h_4 = 2v - b = 0.$$

We shall construct the point $H = (w, x)$ as follows.

AH is at right angles to BC if the inner product of these is zero.

The inner product between two arbitrary vectors is

$$(d, g) \circ (f, e) = df + ge,$$

where "$\circ$" denotes the inner product.

Using our points from the theorem, we get

$$AH \circ BC = (w, x) \circ (-a, b) = -wa + xb,$$

which gives us

$$h_5 = wa - xb = 0.$$

Also

$$wb(a, 0) - ab(w, x) + xa(0, b) = (0, 0).$$

Points B, H and C are on the same line if

$$wb + xa - ab = 0,$$

and this gives us the sixth equation

$$h_6 = wb + xa - ab = 0.$$

We must consider the statement that K, L, M and H lie on a circle. A general collection of four points do not lie on a circle, but a collection of three points does. Thus, our conclusion can be restated as follows:

If we construct the circle through K, L, and M, then H must lie on this circle also.

To check this, we need to construct the centre of the circle $O = (y, z)$. K, L, and M are on the same circle if $KO = LO$ and $KO = MO$.

A general circle is given by

$$(X - a)^2 + (Y - b)^2 = R^2,$$

where (X, Y) is some point on the curve, (a, b) is the centre of the circle, and R is the radius. Equating the radii KO and LO gives

$$(s - y)^2 + (0 - z)^2 = (-y)^2 + (t - z)^2,$$

and so

$$h_7 = (s - y)^2 + z^2 - y^2 - (t - z)^2 = 0.$$

Equating KO and MO gives

$$h_8 = (s - y)^2 + z^2 - (u - y)^2 - (v - z)^2 = 0.$$

Our conclusion is $KO = HO$, which similarly results in the final equation:

$$g = (s - y)^2 + z^2 - (w - y)^2 - (x - z)^2 = 0.$$

We have now translated the theorem of Apollonius into the statement that g follows from $h_1 - h_8$. We complete the proof in Singular.

```
                     SINGULAR                                 /
 A Computer Algebra System for Polynomial Computations   /   version 3-0-2
                                                        0<
     by: G.-M. Greuel, G. Pfister, H. Schoenemann         \   July 2006
FB Mathematik der Universitaet, D-67653 Kaiserslautern    \
> // ** The ring we use is **;
. ring r=(0,a,b),(p,s,t,u,v,w,x,y,z),lp;
>
. // ** The hypotheses are **;
. poly h1=2*s-a;
> poly h2=2*t-b;
> poly h3=2*u-a;
> poly h4=2*v-b;
> poly h5=2*v-b;
> poly h6=b*w+a*x-a*b;
> poly h7=(s-y)^2+z^2-y^2-(z-t)^2;
> poly h8=(s-y)^2+z^2-(w-y)^2-(v-z)^2;
>
. // ** The conclusion is **;
. poly g=(w-y)^2+(x-z)^2-(s-y)^2-(s-y)^2-z^2;
>
. // ** The verification of the concluion is **;
. ideal i=h1,h2,h3,h4,h5,h6,h7,h8;
```

```
> groebner(i);
_[1]=(a)*w+(-b)*x
_[2]=(a2+b2)*x+(-a2b)
_[3]=2*v+(-b)
_[4]=2*u+(-a)
_[5]=2*t+(-b)
_[6]=2*s+(-a)
_[7]=(-4a)*y+(4b)*z+(a2-b2)
_[8]=(4a2b+4b3)*z+(a4-2a2b2-b4)
> reduce(g,groebner(i));
(-a2b4)/(4a4+8a2b2+4b4)
```

```
This is not the result we want. Maybe there are some problems with degeneration.
We should, for example make, sure that a and b are not equal to zero.
The fact that a and b are not equal to zero can be guaranteed by adding the
hypothesis g2=1-p*g.
We proceed in Singular as
```

```
> poly g2=1-p*g;
> ideal i=h1,h2,h3,h4,h5,h6,h7,h8,g2;
// ** redefining i **
> groebner(i);
_[1]=1
```

This shows that $g \in \sqrt{\langle h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8, g_2\rangle}$ so the theorem described by the conclusion g holds in the hypothesis described by $h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8$.

4.3 Pappus Theorem

Theorem 4.1. *Let A, B, C and A', B', C' be two sets of collinear points. Then let $P = \overline{AB'} \cap \overline{A'B}$, $Q = \overline{AC'} \cap \overline{A'C}$ and $R = \overline{BC'} \cap \overline{B'C}$. Then the points P, Q and R are collinear.*

This is shown in figure 4.3,

For our translation, let $A = (0,0), B = (u_1, 0), C = (u_2, 0), A' = (u_3, u_4), B' = (u_5, u_6), C' = (u_7, x_1), P = (x_2, x_3), Q = (x_4, x_5), R = (x_6, x_7)$. Point C' is partially dependent on our choices of A, B, A', B', so one of its coordinates is x_1.

We translate the hypotheses of the theorem as follows,

The points A', B' and C' are collinear, and using the slope formula, we have

$$A'B' = A'C'$$

$$\frac{u_6 - u_4}{u_5 - u_3} = \frac{x_1 - u_4}{u_7 - u_3}$$

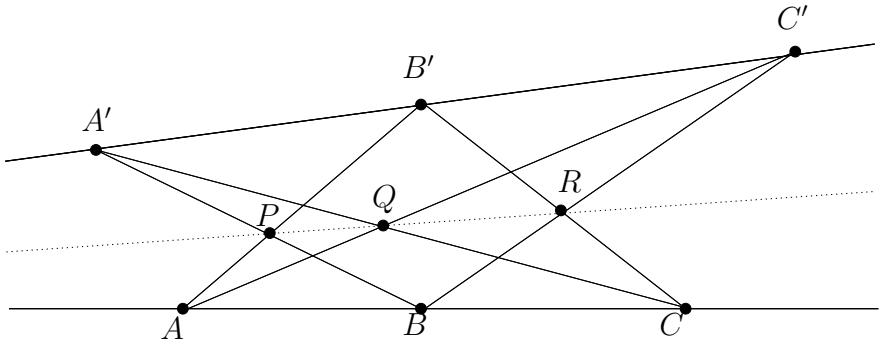

Figure 4.3: Pappus Theorem

$$(u_6 - u_4)(u_7 - u_3) = (x_1 - u_4)(u_5 - u_3)$$
$$h_1 = (u_6 - u_4)(u_7 - u_3) - (x_1 - u_4)(u_5 - u_3) = 0.$$

The points A, P and B' are collinear, so using the slope formula, we find

$$AP = AB'$$
$$\frac{x_3 - 0}{x_2 - 0} = \frac{u_6 - 0}{u_5 - 0}$$
$$\frac{x_3}{x_2} = \frac{u_6}{u_5}$$
$$x_3 u_5 = u_6 x_2$$
$$h_2 = x_3 u_5 - u_6 x_2 = 0.$$

The points B, P and A' are collinear, and using the slope formula, we obtain

$$BA' = BP$$
$$\frac{u_4 - 0}{u_3 - u_1} = \frac{x_3 - 0}{x_2 - u_1}$$
$$u_4(x_2 - u_1) = x_3(u_3 - u_1)$$
$$h_3 = u_4(x_2 - u_1) - x_3(u_3 - u_4) = 0.$$

The points A, Q and C' are collinear. Again using the slope formula, we have

$$AQ = AC'$$
$$\frac{x_5 - 0}{x_4 - 0} = \frac{x_1 - 0}{u_7 - 0}$$
$$\frac{x_5}{x_4} = \frac{x_1}{u_7}$$
$$x_5 u_7 = x_1 x_4$$
$$h_4 = x_5 u_7 - x_1 x_4 = 0.$$

The points C, Q and A' are collinear, and using the slope formula,

$$CQ = CA'$$
$$\frac{x_5 - 0}{x_4 - u_2} = \frac{u_4 - 0}{u_3 - u_2}$$
$$x_5(u_3 - u_2) = u_4(x_4 - u_2)$$
$$h_5 = x_5(u_3 - u_2) - u_4(x_4 - u_2) = 0.$$

The points B, R and C' are collinear, and using the slope formula,

$$BR = BC'$$
$$\frac{x_7 - 0}{x_6 - u_1} = \frac{x_1 - 0}{u_7 - u_1}$$
$$x_7(u_7 - u_1) = x_1(x_6 - u_1)$$
$$h_6 = x_7(u_7 - u_1) - x_1(x_6 - u_1) = 0.$$

The points C, R and B' are collinear, and using the slope formula,

$$CR = CB'$$
$$\frac{x_7 - 0}{x_6 - u_2} = \frac{u_6 - 0}{u_5 - u_2}$$
$$u_6(x_6 - u_2) - x_7(u_5 - u_2) = 0$$
$$h_7 = u_6(x_6 - u_2) - x_7(u_5 - u_2) = 0.$$

Our conclusion is that the points P, Q and R are collinear, so that using the slope formula, we have

$$PQ = PR$$
$$\frac{x_5 - x_3}{x_4 - x_2} = \frac{x_7 - x_3}{x_6 - x_2}$$
$$(x_5 - x_3)(x_6 - x_2) - (x_7 - x_3)(x_4 - x_2) = 0$$
$$g = (x_5 - x_3)(x_6 - x_2) - (x_7 - x_3)(x_4 - x_2) = 0.$$

We have now translated the theorem of Pappus into the statement that g follows from $h_1 - h_7$. We complete the proof in Singular.

```
                     SINGULAR                                 /
 A Computer Algebra System for Polynomial Computations   /   version 3-0-2
                                                       0<
     by: G.-M. Greuel, G. Pfister, H. Schoenemann        \   July 2006
FB Mathematik der Universitaet, D-67653 Kaiserslautern    \
> // ** The ring we use is **;
```

```
. ring r=(0,x1,x2,x3,x4,x5,x6,x7),(y,u1,u2,u3,u4,u5,u6,u7),lp;
>
. // ** The hypotheses are **;
. poly h1=(u6-u4)*(u7-u3)-(x1-u4)*(u5-u3);
> poly h2=x3*u5-u6*x2;
> poly h3=u4*(x2-u1)-x3*(u3-u1);
> poly h4=x5*u7-x1*x4;
> poly h5=x5*(u3-u2)-u4*(x4-u2);
> poly h6=x7*(u7-u1)-x1*(x6-u1);
> poly h7=u6*(x6-u2)-x7*(u5-u2);
>
. // ** The conclusion is **;
. poly g=(x5-x3)*(x6-x2)-(x7-x3)*(x4-x2);
>
. // ** The verification of the conclusion is **;
. ideal i=h1,h2,h3,h4,h5,h6,h7;
> groebner(i);
_[1]=(x5)*u7+(-x1*x4)
_[2]=(x3)*u5+(-x2)*u6
_[3]=(x1-x7)*u1+(x7)*u7+(-x1*x6)
_[4]=(x1*x3-x3*x7)*u3+(-x7)*u4*u7+(-x1*x2+x1*x6+x2*x7)*u4+(x3*x7)*u7+(-x1*x3*x6)
_[5]=(-x1*x2*x5+x1*x3*x4-x1*x4*x7+x1*x5*x6+x2*x5*x7-x3*x4*x7)*u4+(x1*x3*x5-x3*x5 *x7)
_[6]=(-x1*x2*x5+x1*x3*x4+x2*x5*x7-x3*x5*x6)*u6^2+(-x3*x5*x7)*u6*u7+(x1*x3*x5*x6) *u6
_[7]=(x1*x2*x5^2-x1*x2*x5*x7-x1*x3*x4*x5+x1*x3*x5*x6+x1*x4*x5*x7-x1*x5^2*x6-x2*x 5^2*
> reduce(g,groebner(i));
(-x2*x5+x2*x7+x3*x4-x3*x6-x4*x7+x5*x6)
```

This is not the result we want. Maybe there are some problems with degeneration. We should, for example, make sure that x1,x2,x3,x4,x5,x6 and x7 are not equal to zero. The fact that x1,x2,x3,x4,x5,x6 and x7 are not equal to zero can be guaranteed by adding the hypothesis g2=1-y*g.
We proceed in Singular as

```
> poly g2=1-y*g;
> ideal i=h1,h2,h3,h4,h5,h6,h7,g2;
// ** redefining i **
> groebner(i);
_[1]=1
```

This shows that $g \in \sqrt{\langle h_1, h_2, h_3, h_4, h_5, h_6, h_7, g_2 \rangle}$ so the theorem described by the conclusion g holds in the hypotheses described by $h_1, h_2, h_3, h_4, h_5, h_6, h_7$.

5. Conclusion

Let us summarize the ideas from commutative algebra, algebraic geometry and Singular that we have explored in this essay concerning automatic geometric theorem proving.

We have shown that we can prove geometric theorems by means of Groebner basis and Singular by translating the hypothesis of these theorems to the vanishing of a set of polynomials. We have also translated the conclusion(s) of the geometric theorem into the vanishing of a set of polynomials. The basic idea is that we want our proof to be satisfied by every point that fulfills the criteria of the hypothesis. We then use Singular to verify our conclusion. To provide verification using Singular, we defined the ring, the ideal and calculated the Groebner basis of the ideal. For each conclusion of these theorems, we calculated the remainder on division of the conclusion of these theorems by the Groebner basis. The theorem was found to be true if and only if the remainder is zero. However, if the remainder is not zero, we would then define the degenerate condition and recalculate the Groebner bases accordingly. If the result is $\{1\}$, then the conclusion of the theorem must be true.

An interesting problem arose when we encountered degenerations. An example of this was when we considered the Theorem of Apollonius. We had variables $s, \ldots, z$ and our ring was the real numbers with a and b as parameters. By setting the characteristic of the ring to zero, the parameters a and b are forced to be invertible, and a degenerate triangle was prevented. Once the issue of degeneration had been bypassed, the implementation of an easy-to-use Singular program was straightforward.

In the limited time frame available for this essay, we have been able to review basic concepts in the area, applying them to explain theorems, culminating in the automatic proof of Thales' theorem, The Apollonus theorem of a circle and Pappus theorem.

Possible directions for a further investigation might include the search for

1. The translation of polynomials into geometric configurations such as lines and points.
2. Methods for automatically fixing degenerations.
3. Manipulation of given polynomials, prior to calculating the Groebner basis, so the Groebner basis calculation can be executed more rapidly.
4. Exploration of the treatment of conclusions in the radical ideal.

Acknowledgements

First and foremost, I thank Professor Barry W. Green for this interesting and fruitful topic and his continuous help and advice.

I want to express my special gratitude to Anahita New for her valuable comments on a draft version of this essay, and her support throughout the year which has guided my work and made it more enjoyable.

Jan, Andy and the tutors have helped me in many ways, and I wish to thank all of them.

I am grateful for the scholarship I received from AIMS during my studies.

Bibliography

[DAV96] Sturm T. Dolzmann A. and Weispfenning V., *A New Approach for Automatic Theorem Proving in Real Geometry*, University of Passau (1996).

[DC96] John Little & Donal O'Shea David Cox, *Ideals, varieties, and algorithms (2nd edition)*, Contemporary Mathematics, no. 133, Springer, Providence, RI, 1996.

[DL06] W. Decker and C. Lossen, *Computing in Algebraic Geometry- A Quick Start using Singular*, ACM 16, Springer-Verlag, 2006.

[Don] W. Dongming, *Groebner Bases Applied to Geometric Theorem Proving and Discovering*.

[Eli06] J. Elias, *Automated Geometric Theorem Proving: Wu's Method*, T.M.M.E **3** (2006), no. 1, 3–50.

[Gre07a] Barry W. Green, *From topics in computational algebra and application 2007*, 2006/2007, Unpublished manuscript.

[Gre07b] ———, *Topics in computational algebra and application 2007*, 2006/2007.

[htt] http://www.sogstad.net/algnotes/apollonius.html.

[Kat] Katzman M., *Automatic Geometric Theorem Proving*, The University of Sheffield.

[MIT] *Algebraic geometry and integer optimization*, http://ocw.mit.edu/NR/rdonlyres/Sloan-School-of-Management/15-083jFall-2004/1FD5CA8D-F9C9-4858-A309-B23EE1EBD3A1/0/lecture13_14.pdf.

[Par] P. A. Parrilo, *Algebraic techniques and semidefinite optimization*, 4 April.

[Roo06] Dan Roozemond, *Automatic geometric theorem proving*, Bachelorproject, Eindhoven University of Technology, 9th July 2006.

[SG] Shang-Ching C. and Xiao-Shan G., *A Class of Geometry Statements of Constructive Type and Geometry Theorem Proving*, The Wichita State University, Wichita.