Automatic Geometric Theorem Proving: An Application of Groebner Bases

Lois Olatayo (lois@aims.ac.za)
African Institute for Mathematical Sciences (AIMS)

Supervised by Barry Green
University of Stellenbosch

June 7, 2007

Abstract

The main goal of this work is the use of Groebner basis in proving geometric statements. It begins with a brief introduction, then basic definitions are given for necessary mathematical background. Next, a step by step process of translating some basic geometric statements to algebraic statements are elaborately explained. This is followed by the interpretation and translation of some elementary geometric theorems into algebraic statements. Finally, the concept of Groebner basis already introduced at the beginning of the work, is employed along with the computer package Singular and noting "degenerate cases", the already translated theorems are then verified.

Contents

1. Introduction and Basic Mathematical Concepts

1.1 Introduction

Groebner bases were first discovered by Bruno Buchberger in 1965, who named them after his supervisor Wolfgang Groebner. They have been applied successfully in algebraic geometry and commutative algebra. This work is based on Cox $et\ \ al$ [CLO92]. The method we employed translates geometric statements into algebraic statements, we illustrate this in chapter 2 and 3. In chapter 4 we verify our result by using the concept of Groebner bases and a computer package called Singular. First we begin with some basic concepts.

1.2 Polynomials

Let $k[x_1, x_2, \ldots, x_n]$ be a ring of n indeterminants $x_1, x_2, \ldots, x_n$. A polynomial f consists of a finite sum of the form:

$$\sum_{\alpha_1\alpha_2\ldots\alpha_n} a_{\alpha_1\alpha_2\ldots\alpha_n} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_3},$$

where k is a field, $\alpha_i \in \mathbf{Z}_{\geq 0}$, $a_{\alpha_1\alpha_2\ldots\alpha_n} \in k$ and $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_3}$ is known as a monomial.

Definition 1.1 *Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial in $k[x_1, x_2, \ldots, x_n]$,*

1. *a_α is the* $\mathbf{coefficient}$ *of the monomial x^α.*
2. *$a_\alpha x^\alpha$ is a* $\mathbf{term}$ *of f.*
3. *the maximum $|\alpha|$ such that $a_\alpha \neq 0$ is the* $\mathbf{total\ degree}$ *of f.*
   Where x^α is a shorthand $x_1^{\alpha_1}, x_2^{\alpha_2} \ldots, x_n^{\alpha_n}$, α is the tuple $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $|\alpha| = \alpha_1 + \alpha_2 + \ldots + \alpha_n$.

[Gre07]

1.3 Affine Space

Linking algebra and geometry is enabled using the affine space. We briefly recall the basic ideas and properties of the affine space.

Definition 1.2 *The set $k^n = \{(a_1, a_2, \ldots, a_n) | a_1, a_2, \ldots, a_n \in k\}$ is an affine space where k is a field and $n \in \mathbf{Z}$.*

Definition 1.3 *The set*

$$V(f_1, f_2, \ldots, f_s) = \{(a_1, a_2, \ldots, a_n) \in k^n | f_i(a_1, a_2, \ldots, a_n) = 0 \ \ for \ \ all \ \ 1 \leqslant i \leqslant s\}$$

is called an **affine variety** *defined by $f_1, f_2, \ldots, f_s$ over the field k.[CLO92]*

1.4 Ideals

Definition 1.4 *A nonempty subset I, of a ring R is called an ideal if*

1. $0 \in I$.
2. *for any* $a, b \in I$, $a + b \in I$.
3. *for any* $a \in I$ *and* $x \in R$, $ax \in I$.

[Gre07]

1.5 Monomial ideals

An ideal I is a monomial ideal if it has a basis consisting of a set of monomials,
$I = \langle x^\alpha | \alpha \in A \rangle$ and $A \subset \mathbf{Z}^n_{\geq 0}$.

Lemma 1.5 *Let I be a monomial ideal, then a monomial x^β is in I if and only if x^β is divisible by x^α for some $\alpha \in A$.[Gre07]*

Theorem 1.6 *Dickson's Lemma*

A monomial ideal $I = \langle x^\alpha | \alpha \in \mathbf{Z}^n_{\geq 0} \rangle \subset k[x_1, x_2, \ldots, x_n]$ can be written down in the form $I = \langle x^{\alpha(1)}, x^{\alpha(2)}, \ldots, x^{\alpha(s)} \rangle$, where $\alpha(1), \alpha(2), \ldots, \alpha(s) \in A \subset \mathbf{Z}^n_{\geq 0}$. In particular I has a finite basis.[CLO92]

1.6 Monomial Ordering

Definition 1.7 *A monomial ordering on $k[x_1, x_2, \ldots, x_n]$ is any relation $>$, on the set of monomials x^α, $\alpha \in \mathbf{Z}^n_{\geq 0}$, such that:*

1. *$>$ is a total (or linear) ordering on $\mathbf{Z}^n_{\geq 0}$. That is if $\alpha \neq \beta$, then $\alpha > \beta$ or $\beta > \alpha$ and if $\alpha > \gamma$ and $\gamma > \beta$ then $\alpha > \beta$.*

2. *if* $\alpha > \beta$ *and* $\gamma \in \mathbf{Z}^n_{\geq 0}$, *then* $\alpha + \gamma > \beta + \gamma$

3. $>$ *is a well-ordering on* $\mathbf{Z}^n_{\geq 0}$. *That is* $>$ *is an only decreasing sequence* $\alpha(1), \alpha(2), \ldots, \alpha(l), \ldots$. *of* $\mathbf{Z}^n_{\geq 0}$ *terminates.*

[Gre07]

1.7 Polynomials of Single Variables

Definition 1.8 *A polynomials of the form*

$$f(x) = a_0 x^m + a_1 x^{m-1} + \ldots + a_m$$

is a single variable polynomial with the degree of $f(x)$, *denoted by deg*$(\mathbf{f}(\mathbf{x}))$, *being* m. *The leading term of* $f(x)$, *denoted by LT*$(\mathbf{f}(\mathbf{x}))$, *being* $a_0 x^m$.

Theorem 1.9 *Every ideal* I *of* $k[x]$ *is of the form* $\langle g \rangle$ *for some* $g \in k[x]$.

Proof: Let g *be a polynomial of minimum degree in* I, *consider* $f \in I$. *Given a polynomial* f, *we can write* f *uniquely as* $f = qg + r$ *where* $r = 0$ *or deg(*r*)<deg(*g*). Furthermore* r *can be expressed as* $r = f - qg$ *but* g *is of minimum degree thus* r *cannot be less than* g. *Therefore* $r = 0$ *and* q *is called the quotient. In otherwords, every polynomial in the ideal can be generated from* g.

(See [Kar06] and [Gre07])

1.8 Polynomials of Multiple Variables

In polynomials of one variable the leading term was determined by the degree of the variable, but for a polynomial of multiple variables an ordering has to be defined on the variables.[Kar06]

Definition 1.10 *Lexicographic ordering:*

Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ *and* $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbf{Z}^n_{\geq 0}$. *We say* $\alpha >_{lex} \beta$, *if the left-most nonzero entry of the vector difference* $\alpha - \beta \in \mathbf{Z}^n$, *is positive. We will write* $x^\alpha >_{lex} x^\beta$ *if* $\alpha >_{lex} \beta$.

Definition 1.11 *Graded lex order:*

Let $\alpha,\ \beta \in \mathbf{Z}^n_{\geq} 0$ *and let us define* $|\alpha| = \Sigma^n_{i=1} \alpha_i$. *We say* $\alpha >_{grlex} \beta$ *if*

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

or

$$|\alpha| = |\beta|$$

and

$$\alpha >_{lex} \beta.$$

Definition 1.12 *Graded Reverse Lex Order:*

Let $\alpha, \beta \in \mathbf{Z}_{\geq}^{n} 0$. *We say* $\alpha >_{grevlex} \beta$ *if*

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

or

$$|\alpha| = |\beta|.$$

and in $\alpha - \beta \in \mathbf{Z}^n$, *the left-most non-zero entry is positive.*

Definition 1.13 *Let* $f = \Sigma_\alpha a_\alpha x^\alpha$ *be a non-zero polynomial in* $k[x_1, x_2, \ldots, x_n]$ *and let* $>$ *be a monomial order,*

1. *The multidegree of* f *is,*

$$multideg(f) = \max(\alpha \in \mathbf{Z}_{\geq 0}^{n} : a_\alpha \neq 0).$$

2. *The leading coefficient of* f *is*

$$LC(f) = a_{multideg(f)} \in k.$$

3. *The leading monomial of* f *is,*

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

4. *The leading term of* f *is,*

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

1.8.1 Division Algorithm

Theorem 1.14 *Let $>$ be a monomial order on $\mathbf{Z}^n_{\geq 0}$ and let $f = (f_1, f_2, \ldots, f_s)$ be an ordered s-tuple of polynomials in $k[x_1, x_2, \ldots, x_n]$. Then every $f \in k[x_1, x_2, \ldots, x_n]$, can be written as*

$$f = a_1 f_1 + a_2 f_2 + \ldots + a_s f_s + r,$$

where $a_i, r \in k[x_1, x_2, \ldots, x_n]$ and either $r = 0$ or r is a linear combination of monomials, with coefficients in k, none of which is divisible by any $LT(f_1), LT(f_2), \ldots, LT(f_s)$. We will call r a remainder of f.

Furthermore, if $a_i f_i \neq 0$, then we have

$$multideg(f) \neq multideg(a_i f_i).$$

Proof:

The existence of $a_1, a_2, \ldots, a_s$ and r is proved by the following constructive algorithm.

```
Input: f_1, f_2, ..., f_s, f

Output: a_1, a_2, ..., a_s, r

        a_i := 0  1 <= i <= s, r := 0; P := f

While P ≠0 Do
      i := 1
      dividing:=true
      While ((i ≤ s) AND (dividing)):=true Do
          IF LT(f_i) divides LT(P) THEN
               a_i := a_i + LT(P) / LT(f_i)
               P := P - (LT(P) / LT(f_i)) f_i
               dividing:= true
          ELSE:
              i := i + 1
      IF (dividing) THEN
          r := r + LT(P)
          P := P - LT(P)
```

The variable P represents the intermediate dividend at each step. As long as the leading term of the divisor divides the leading term of P, the algorithm proceeds as in the normal high school division algorithm for a one-variable. Otherwise, we remove the leading term of P and add it to the remainder. Now since the multideg(Lt(P)) decreases in each step, the algorithm is guaranteed

to terminate. Hence

$$f = a_1 f_1 + \ldots + a_s f_s + p + r \tag{1.1}$$

is the result obtained when it finally terminates. In general the result obtained depends on the order of f_i.

Theorem 1.15 *Hilbert Basis Theorem*

Every ideal $I \subset k[x_1, x_2, \ldots, x_n]$ *has a finite generating set. That is,* $I = \langle g_1, g_2, \ldots, g_s \rangle$ *for some* $g_1, g_2, \ldots, g_s \in I$.

Theorem 1.16 *The Ascending Chain Condition(ACC).*

Let $I_1 \subset I_2 \subset I_3 \subset \ldots.$ *be ascending chain of ideals in* $k[x_1, x_2, \ldots, x_n]$. *Then there exists an* $N \geq 1$ *such that*

$$I_N = I_{N+1} = I_{N+2} = \ldots.$$

Proposition 1.17 $V(I)$ *is an affine variety if* $I = \langle f_1, f_2, \ldots, f_s \rangle$, *then* $V(I) = V(f_1, f_2, \ldots, f_s)$.

1.9 Groebner Basis

Definition 1.18 *A Groebner basis* G *is formed once the following properties are satisfied, relative to some monomial order.*

1. *Multivariate division of any polynomial in the polynomial ring* $\mathbb{R}$ *by* G *gives a unique remainder.*
2. *Multivariate division of any polynomial in the ideal* I *by* G *gives* 0.

1.10 Properties of Groebner Basis

Proposition 1.19 *Let* $G = \{g_1, g_2, \ldots, g_s\}$ *be a Groebner basis for an ideal* $I \subset k[x_1, x_2, \ldots, x_n]$ *and let* $f \in k[x_1, x_2, \ldots, x_n]$. *Then there is a unique* $r \in k[x_1, x_2, \ldots, x_n]$ *with the two properties,*

1. *No term of* r *is divisible by any of* $LT(g_1), LT(g_2), \ldots, LT(g_s)$.
2. *There is* $g \in I$ *such that* $f = g + r$. *In particular,* r *is the remainder on division of* f *by* G *no matter how the elements of* G *are listed when using an algorithm.[CLO92]*

Corollary 1.20 *Let $G = \{g_1, g_2, \ldots, g_s\}$ be a Groebner basis for an ideal $I \subset k[x_1, x_2, \ldots, x_n]$ and let $f \in k[x_1, x_2, \ldots, x_n]$. Then $f \in I$ if and only if the remainder of f by G is zero.*

Proof:

If the remainder is zero, then we have already observed that $f \in I$.

Conversely, given $f \in I$, then $f = f + 0$ satisfies the two conditions in proposition 1.19. Hence 0 is the remainder of f on division by G.[CLO92]

Definition 1.21 *Let $f, g \in k[x_1, x_2, \ldots, x_n]$ be nonzero polynomials.*

1. *if multideg$(f) = \alpha$ and multideg$(g) = \beta$, then set $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n)$, where $\gamma_i = max(\alpha_i, \beta_i)$ for each i. We call x^γ the least common multiple of $LM(f)$ and $LM(g)$, written*

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

2. *The S-polynomial of f and g is the combination*

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

[Kar06]

Remark 1.22 *An S-polynomial is designed to produce cancellation of of leading terms.*

Theorem 1.23 *Let I be a polynomial ideal. Then a basis $G = \{g_1, g_2, \ldots, g_s\}$ for I is a Groebner basis for I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_i)$ by G is 0.[Gre07]*

1.11 Buchberger Algorithm

So far we have seen how to tell when an ideal is a Groebner basis, next we will see how to produce the Groebner basis of any given ideal I.

Theorem 1.24 *Let $I = \langle f_1, f_2, \ldots, f_s \rangle \neq 0$ be a polynomial ideal. Then a Groebner basis for I can be constructed in a finite number of steps by the following algorithm;*

```
Input: F = (f_1, f_2, ..., f_s)
Output: a Groebner basis G = (g_1, g_2, ..., g_t) for I, with F ⊂ G
G := F
REPEAT
```

```
      G := G'
      FOR each pair {p, q}, p ≠ q in G' DO
            S := S(p,q)^G'
            IF S ≠ 0
THEN G := G ∪ S
UNTIL G := G'
```

Proof:

We begin with some frequently used notation. If $G = \{g_1, g_2, \ldots, g_s\}$*, then* $\langle G \rangle$ *and* $\langle LT(G) \rangle$ *will denote the following ideals:*

$$\begin{aligned} \langle G \rangle &= \langle g_1, g_2, \ldots, g_t \rangle \\ \langle LT(G) \rangle &= \langle LT(g_1), LT(g_2), \ldots, LT(g_s) \rangle. \end{aligned}$$

By the algorithm in the theorem, if $G \subset I$*, then* p, q *and* $S(p,q)$ *are in* I *and since we are dividing by* $G' \subset I$*, we get* $G \subset S \subset I$*. Now* G *is actually a basis of* I*.*

The algorithm terminates when $G = G'$*, which means* $\overline{S(p,q)^{G'}} = 0$ *for all* $p, q \in G$*. Hence* G *is a Groebner basis of* $\langle G \rangle = I$ *by theorem 1.23. Next the set* G *consists of* G' *together with the nonzero remainder of S-polynomials of elements of* G'*. Then*

$$\langle LT(G') \rangle \subset \langle LT(G) \rangle \tag{1.2}$$

since $G' \subset G$*. Also if* $G' \in G$*, we claim that* $\langle LT(G') \rangle$ *is strictly smaller than* $\langle LT(G) \rangle$*. Since for any remainder* r *on dividing by* G'*,* $LT(r) \in \langle G' \rangle$ *but* $LT(r) \in \langle LT(G) \rangle$*. By equation 1.2, the ideal* $\langle LT(G') \rangle$ *from successive iterations of the loop form an ascending chain of ideals in* $k[x_1, x_2, \ldots, x_n]$*. Thus by theorem 1.16, the ACC implies that after a finite number of iterations the chain will stabilize, so that* $\langle LT(G') \rangle = \langle LT(G) \rangle$ *must happen eventually. And so* $G' = G$ *so That the algorithm must terminate after a finite number of steps.[CLO92]*

Example 1.1 *Given* $I = \langle -x_1^3 + x_2, x_1^2 x_2 - x_3 \rangle$ *using a lex order, we claim that* $G = \{-x_1^3 + x_2, x_1^2 x_2 - x_3\}$*.*

Setting $F = (f_1, f_2)$*, then*

$$\begin{aligned}
f_1 &= -x_1^3 + x_2 \\
f_2 &= x_1^2 x_2 - x_3 \\
LT(f_1) &= -x_1^3 \\
LT(f_2) &= x_1^2 x_2 \\
LCM(LT(f_1), LT(f_2)) &= x_1^3 x_2 \\
S(f_1, f_2) &= \frac{x_1^3 x_2}{-x_1^3}(-x_1^3 + x_2) - \frac{x_1^3 x_2}{x_1^2 x_2}(x_1^2 x_2 - x_3) \\
&= -x_2(-x_1^3 + x_2) - x_1(x_1^2 x_2 - x_3) \\
&= x_1^3 x_2 - x_2^2 - x_1^3 x_2 + x_1 x_3 \\
&= -x_2^2 + x_1 x_3.
\end{aligned}$$

$\overline{S(p,q)^{G'}} \neq 0.$

Therefore $f_3 = -x_2^2 + x_1 x_3.$

Setting $F = \{(f_1, f_3), (f_2, f_3)\}$, *then*

$$\begin{aligned}
LT(f_3) &= -x_2^2 \\
LCM(LT(f_1), LT(f_3)) &= x_1^3 x_2^2 \\
S(f_1, f_3) &= \frac{x_1^3 x_2^2}{-x_1^3}(-x_1^3 + x_2) - \frac{x_1^3 x_2^2}{-x_2^2}(-x_2^2 + x_1 x_3) \\
&= -x_2^2(-x_1^3 + x_2) + x_1^3(-x_2^2 + x_1 x_3) \\
&= x_1^3 x_2^2 - x_2^3 - x_1^3 x_2^2 + x_1^4 x_3 \\
&= -x_2^3 + x_1^4 x_3.
\end{aligned}$$

Hence, from the multivariate division below $f_1, f_3 \in G.$

$$
\begin{array}{rl|l}
 & & x_1x_3 \\
 & & x_2 \\
\hline
-x_1^3+x_2 & & -x_2^3+x_1^4x_3 \\
-x_2^2+x_1x_3 & & -x_2^3+x_1x_2x_3 \\
\hline
 & & x_1^4x_3-x_1x_2x_3 \\
 & & -x_1^4x_3+x_1x_2x_3 \\
\hline
 & & 0
\end{array}
$$

$S(f_2, f_3) \Rightarrow$

$$
\begin{aligned}
LCM(LT(f_2), LT(f_3)) &= x_1^2x_2^2 \\
S(f_2, f_3) &= \frac{x_1^2x_2^2}{x_1^2x_2}(x_1^2x_2 - x_3) - \frac{x_1^2x_2^2}{-x_2^2}(-x_2^2 + x_1x_3) \\
&= y(x_1^2x_2 - x_3) + x_1^2(-x_2^2 + x_1x_3) \\
&= x_1^2x_2^2 - x_2x_3 - x_1^2x_2^2 + x_1^3x_3 \\
&= -x_2x_3 + x_1^3x_3 \\
&= x_3(-x_2 + x_1^3) \\
&= -x_3(-x_1^3 + x_2) \\
&= -x_3f_1.
\end{aligned}
$$

Hence $\overline{S(p,q)^{G'}} = 0$.

Thus

$$
\begin{aligned}
G &= \{-x_1^3 + x_2, x_1^2x_2 - x_3, -x_2^2 + x_1x_3\} \\
&= \{f_1, f_2, -x_2^2 + x_1x_3\}
\end{aligned}
$$

is a basis generated by $I = \langle -x_1^3 + x_2, x_1^2x_2 - x_3\rangle$.

1.12 Radical Ideals/Correspondence Between Ideals and Varieties

It is possible to identify ideals that consists of all polynomials which vanishes on some variety, and this is possible using the properties below.

Lemma 1.25 *Let V be a variety, if $f^m \in I(V)$, then $f \in I(V)$.*

Proof:

Let $x \in V$. If $f^m \in I(V)$, then $(f(x))^m = 0$. But this can happen only if $f(x) = 0$. Since $x \in V$ was arbitrary, we must have $f \in I(V)$.

Definition 1.26 *An ideal I is radical if $f^m \in I$ for any integer $m \geq 1$ implies that $f \in I$.*

(See [Kat06] and [CLO92])

Corollary 1.27 *$I(V)$ is a radical ideal.*

Proof:

This follows by rephrasing lemma 1.25 and using definition 1.26.

The concept of radical ideals shows that the one-to-one correspondence of the affine variety and the radical ideal, pointed out by the Hilbert Nullstellensatz theorem can be clearly represented by using the operation of taking the radical of an ideal. [AL94]

Definition 1.28 *Let $I \subset k[x_1, x_2, \ldots, x_n]$ be an ideal. The radical of I denoted $\sqrt{I}$, is the set*

$$\{f : f^m \in I \ \ for \ some \ integer \ \ m \geq 1\}.$$

[Kat06]

Theorem 1.29 *Radical Membership*

Let k be an arbitrary field and let $I = \langle f_1, f_2, \ldots, f_s \rangle \subset k[x_1, x_2, \ldots, x_n]$ be an ideal. Then $f \in \sqrt{I}$ if and only if the constant polynomial 1 belongs to the ideal

$$\overline{I} = \langle f_1, f_2, \ldots, f_s, 1 - yf \rangle \subset k[x_1, x_2, \ldots, x_n, y].$$

[CLO92]

Nullstellensatz

This is a theorem that identifies exactly which ideal correspond to varieties. It gives the required properties between geometry and Algebra.

Using the Hilbert basis Theorem, several algebraic and geometric concepts can be obtained and explained.

The Hilbert basis theorem proves that $V(I)$ is actually an affine variety, since there exists a finite set of polynomials $f_1, f_2, \ldots, f_s \in I$ such that $I = \langle f_1, f_2, \ldots, f_s \rangle$ and from proposition 1.17, $V(I)$ is the set of common roots of these polynomials. Thus there is a map $I \to V(I)$ and these two maps gives a correspondence between ideals and varieties.

The nature of this correspondence can be described using the following properties.[CLO92]

Definition 1.30 *A field F is said to be algebraically closed if every polynomial in one variable of degree at least 1, with coefficients in F, has a zero (root) in F.*

Theorem 1.31 *The strong Nullstellensatz*

Let k be an algebraically closed field. If I is an ideal in $k[x_1, x_2, \ldots, x_n]$, then

$$I(V(I)) = \sqrt{I}.$$

Theorem 1.32 *Hilbert's Nullstellensatz*

Let k be an algebraically closed field. If $f_1, f_2, \ldots, f_s \in k[x_1, x_2, \ldots, x_n]$ are such that $f \in I(V(f_1, f_2, \ldots, f_s))$, then there exists an integer $m \geq 1$ such that $f^m \in \langle f_1, f_2, \ldots, f_s \rangle$ and conversely.

Definition 1.33 *An affine variety $V \subset k^n$ is irreducible if whenever V is written in the form $V = V_1 \cup V_2$, where V_1 and V_2 are affine varieties, then either $V_1 = V$ or $V_2 = V$.[CLO92]*

Definition 1.34 *An ideal $I \subset k[x_1, x_2, \ldots, x_n]$ is a prime if whenever $f, g \in k[x_1, x_2, \ldots, x_n]$ and $f, g \in I$, then $f \in I$ or $g \in I$.(See [Kat06] and [CLO92])*

Proposition 1.35 *Let $V \subset k^n$ be an affine variety. Then V is irreducible if $I(V)$ is a prime ideal.(See [Kat06] and [CLO92])*

2. Translation of Geometric Statements

The purpose of this chapter is to show the basic steps of translating geometric statements to algebraic statements. First, some notations used are illustrated and then the application to translating geometrical statements is explained.

2.1 Notations

Let A, B, C, D, M be points in the plane, then

- $\mathrm{int}(A, B, C, D, W)$, means the lines $\overline{AB}$ and $\overline{CD}$ intersect at W.
- $\mathrm{col}(A, B, W)$, means the points A, B, W are collinear.
- $\mathrm{midp}(A, B, W)$, means W is the midpoint of the line $\overline{AB}$.
- $\mathrm{pall}(A, B, C, D)$, means the lines $\overline{AB}$ and $\overline{CD}$ are parallel.
- $\mathrm{perp}(A, B, C, D)$, means the lines $\overline{AB}$ and $\overline{CD}$ are perpendicular.

Next we illustrate some translations as we have below:

2.2 Intersection and Collinearity

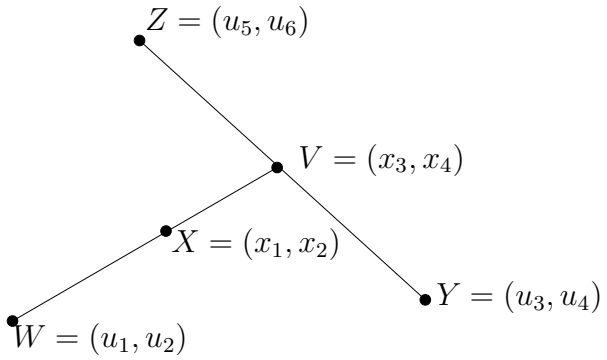


Figure 2.1: Lines $\overline{WX}$ and $\overline{YZ}$ intersect at V

From figure 2.1 we have $\mathrm{int}(W, X, Y, Z, V)$ which we using the steps below:

- W, X, V are collinear i.e $\mathrm{col}(W, X, V)$.
- Y, Z, V are collinear i.e $\mathrm{col}(Y, Z, V)$.

Slope of $WX = \dfrac{x_2 - u_2}{x_1 - u_1}$, provided $x_1 \neq u_1$.

Therefore V along $\overline{WX}$:

$$x_4 - u_2 = \frac{x_2 - u_2}{x_1 - u_1}(x_3 - u_1).$$

Simplifying,

$$x_1x_4 - u_1x_4 - u_2x_1 + u_1u_2 - x_2x_3 + u_1x_2 + u_2x_3 + u_1u_2 = 0.$$

Applying the same method for $\mathrm{col}(Y, Z, V)$ we obtain the translation:

$\mathrm{int}(W, X, Y, Z, V) \Leftrightarrow$

$$x_1x_4 - u_1x_4 - u_2x_1 + u_1u_2 - x_2x_3 + u_1x_2 + u_2x_3 + u_1u_2 = 0$$

$$u_3x_4 - u_5x_4 - u_3u_6 + u_5u_6 - u_4x_3 + u_4u_5 + u_6x_3 - u_5u_6 = 0.$$

2.3 Midpoint of A Line

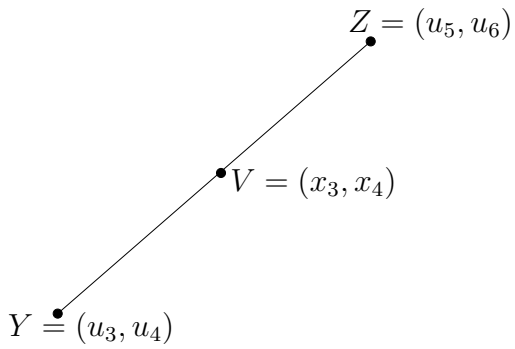


Figure 2.2: V is the midpoint of $\overline{ZY}$

From figure 2.2 we have $\mathrm{midp}(Z, Y, V)$, which we translate using the steps below:

$$\begin{aligned} V = (x_3, x_4) &= \left(\frac{Z_x + Y_x}{2}, \frac{Z_y + Y_y}{2}\right) \\ &= \left(\frac{u_5 + u_3}{2}, \frac{u_6 + u_4}{2}\right) \end{aligned}$$

$$\begin{aligned} x_3 = \frac{u_5 + u_3}{2} \Rightarrow 2x_3 - u_5 - u_3 &= 0 \\ x_4 = \frac{u_6 + u_4}{2} \Rightarrow 2x_4 - u_6 - u_4 &= 0. \end{aligned}$$

Hence

$$\mathrm{midp}(Z, Y, V) \Leftrightarrow 2x_3 - u_5 - u_3 = 0, 2x_4 - u_6 - u_4 = 0.$$

2.4 Parallel Lines

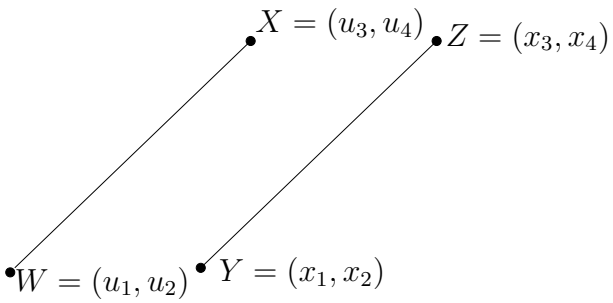


Figure 2.3: The lines $\overline{WX}$ and $\overline{YZ}$ are parallel.

From figure 2.3, $\mathrm{pall}(W, X, Y, Z)$ is translated as below:

$$\frac{u_4 - u_2}{u_3 - u_1} = \frac{x_4 - x_2}{x_3 - x_1}$$

Simplifying,

$$u_4x_3 - u_4x_1 - u_2x_3 + u_2x_1 - u_3x_4 + u_1x_4 + u_3x_2 - u_1x_2 = 0.$$

Hence

$$\mathrm{pall}(W, X, Y, Z) \Leftrightarrow u_4x_3 - u_4x_1 - u_2x_3 + u_2x_1 - u_3x_4 + u_1x_4 + u_3x_2 - u_1x_2 = 0.$$

2.5 Perpendicular Lines

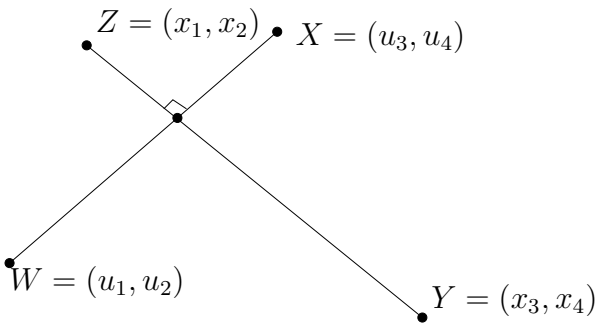


Figure 2.4: $\overline{WX}$ and $\overline{YZ}$ are perpendicular.

From figure 2.4, $\mathrm{perp}(W, X, Y, Z)$ is translated as below:

$$\frac{x_4 - x_2}{x_3 - x_1} = -\left(\frac{u_4 - u_2}{u_3 - u_1}\right)^{-1}.$$

Simplifying, we have

$$(x_4 - x_2)(u_4 - u_2) - (x_3 - x_1)(u_3 - u_1) = 0.$$

Hence $\mathrm{perp}(W, X, Y, Z) \Leftrightarrow u_4x_4 - u_2x_4 - u_4x_2 + u_2x_2 - u_1x_3 + u_3x_3 + u_1x_1 - u_3x_1 = 0$.

2.6 Points On A Circle

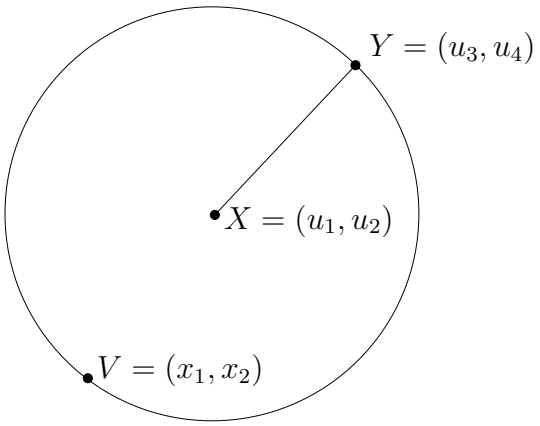


Figure 2.5: V lies on a circle of radius $\overline{XY}$ and centre X.

From figure 2.5, V lies on a circle of radius $\overline{XY}$ and centre X is translated as:

$$|VX| = |VY|$$

$$(x_2 - u_2)^2 + (x_1 - u_1)^2 = (x_2 - u_4)^2 - (x_1 - u_3)^2$$

$$(x_2 - u_2)^2 + (x_1 - u_1)^2 - (x_2 - u_4)^2 - (x_1 - u_3)^2 = 0.$$

For futher details see [Gre07].

3. Relating Theorems To Automatic Geometric Theorem Proving

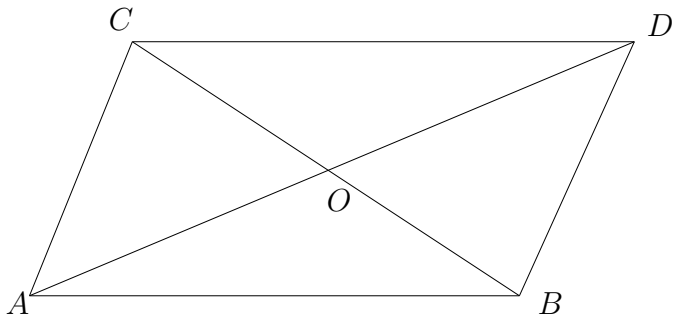
In this chapter we will begin with algebraic proofs of various theorems in Euclidean geometry by relating them to questions in commutative algebra. This is done by assigning coordinates in such a way that the naming convention used allows the determination of other points from arbitrary ones.

It must be noted here that against the fact that automatic theorem proving is outstanding in proving without the direct use of human intelligence, we will at this stage have to use the expertise of the human intelligence to translate these coordinates. The main idea is to obtain polynomials from the placed coordinates based on the theorem. The coordinates placing is chosen arbitrarily. There is no fixed approach to determining how the coordinates should be selected.

We begin with a very simple theorem and follow with other basic ones for which we shall just give their translations. The notations defined in chapter 2 will be employed here. The next chapter will give the final proof of the theorems.

3.1 First Automatic Theorem Translation

Theorem 3.1 *The intersection of the diagonals of a parallelogram in the plane bisects the diagonals.[Eli]*



Translating:

Placing the coordinate system such that $A = (0, 0),\ B = (u_1, 0),\ C = (u_2, u_3)$ *while* $D = (x_1, x_2)$ *and* $O = (x_3, x_4)$ *are completely determined by the choice of* A, B, C.

It should be noted here that the naming convention h_i *and* g_j*, used below denotes translated hypothesis and conclusions respectively.*

Therefore the coordinates (x_1, x_2) *of* D *are determined by:*

1. $\mathrm{pall}(C, D, A, B) \Rightarrow$

$$\frac{x_2 - u_3}{x_1 - u_2} = \frac{0 - 0}{u_1 - 0},$$

and we may define,

$$h_1 \equiv x_2 - u_3 = 0.$$

2. $\mathrm{pall}(A, C, B, D) \Rightarrow$

$$\frac{u_3 - 0}{u_2 - 0} = \frac{x_2 - 0}{x_1 - u_1}$$

and we may define,

$$h_2 \equiv (x_1 - u_1)u_3 - x_2 u_2 = 0.$$

While the coordinates (x_3, x_4) *of* O *are determined by:*

$\mathrm{int}(A, D, B, C)$

which gives:

1. $\mathrm{col}(A, D, O) \Rightarrow$

$$\begin{aligned} \textit{slope of } \overline{AD} &= \frac{x_2}{x_1} \\ \mathrm{col}(A, D, O) \Rightarrow x_4 - 0 &= \frac{x_2}{x_1}(x_3 - 0) \end{aligned}$$

and we may define,

$$h_3 \equiv x_1 x_4 - x_2 x_3 = 0.$$

2. $\mathrm{col}(B, C, O) \Rightarrow$

$$\begin{aligned} \textit{slope of } \overline{BC} &= \frac{u_3 - 0}{u_2 - u_1} \\ \mathrm{col}(A, D, O) \Rightarrow x_4 - 0 &= \frac{u_3 - 0}{u_2 - u_1}(x_3 - u_1) \end{aligned}$$

which we may also define,

$$h_4 \equiv x_4(u_2 - u_1) - u_3(x_3 - u_1) = 0.$$

Now the theorem states that the diagonals $\underline{bisect}$ *each other, meaning we are to show that*

1. $\overline{AO} = \overline{OD}$.
2. $\overline{CO} = \overline{OB}$.

This we can translate as:

$$\begin{aligned} \overline{AO} &= (x_3 - 0)^2 + (x_4 - 0)^2 \\ \overline{OD} &= (x_3 - x_1)^2 + (x_4 - x_2)^2 \\ \overline{CO} &= (x_3 - u_2)^2 + (x_4 - u_3)^2 \\ \overline{OB} &= (x_3 - u_1)^2 + (x_4 - 0)^2. \end{aligned}$$

Therefore,

$$\begin{aligned} x_3^2 + x_4^2 &= (x_3 - x_1)^2 + (x_4 - x_2)^2 \\ x_3^2 + x_4^2 &= x_3^2 - 2x_3x_1 + x_1^2 + x_4^2 - 2x_4x_2 + x_2^2 \\ g_1 \equiv x_1^2 - 2x_3x_1 - 2x_4x_2 + x_2^2 &= 0, \end{aligned}$$

and

$$\begin{aligned} (x_3 - u_2)^2 + (x_4 - u_3)^2 &= (x_3 - u_1)^2 + (x_4 - 0)^2 \\ x_3^2 - 2x_3u_2 + u_2^2 + x_4^2 - 2x_4u_3 + u_3^2 &= x_3^2 - 2x_3u_1 + u_1^2 + x_4^2 \\ g_2 \equiv 2x_3u_2 + 2x_4u_3 - 2x_3u_1 + u_1^2 - u_2^2 - u_3^2 &= 0. \end{aligned}$$

Where the polynomials g_1, g_2 *can only be determined by the polynomials* h_1, h_2, h_3, h_4. *Hence it will be enough to show that each set of values* $x_1, x_2, x_3, x_4, u_1, u_2, u_3$ *which makes* $h_1 = h_2 = h_3 = h_4 = 0$ *also makes* $g_1 = g_2 = 0$.

3.2 Second Automatic Theorem Translation

Theorem 3.2 *Let* A, B, C *be any three points in the plane,* D *the midpoint of* $\overline{AB}$ *and* E *the midpoint of* $\overline{CD}$. *Extend* AE *to intersect* $\overline{BC}$ *at point* F. *Show that* $|\overline{FB}| = 2|\overline{FC}|$.*[Wan98]*

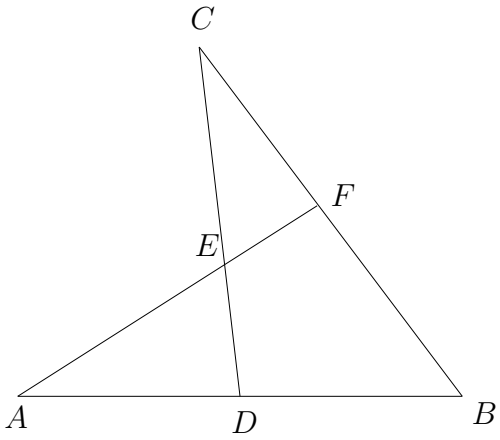
Translating:

Placing coordinates $D = (0, 0), B = (u_1, 0), A = (-u_1, 0), C = (u_2, u_3)$ *where* $E = (x_1, x_2)$ *and* $F = (x_3, x_4)$ *are to be determined as before from* A, B, C.

The coordinate (x_1, x_2) *of* E *can be determined from:*

$\mathrm{midp}(C, D, E) \Rightarrow$

$$(x_1, x_2) = \left(\frac{u_2 + 0}{2}, \frac{u_3 + 0}{2} \right).$$



Therefore,

$$\begin{aligned} h_1 \equiv 2x_1 - u_2 &= 0 \\ h_2 \equiv 2x_2 - u_3 &= 0. \end{aligned}$$

While the coordinate (x_3, x_4) *of* F *from:*

$\mathrm{int}(A, E, C, B, F) \Rightarrow$

1. $\mathrm{col}(A, E, F)$

$$\begin{aligned} \textit{slope of } \overline{AE} &= \frac{x_2 - 0}{x_1 + u_1} \\ x_4 - 0 &= \frac{x_2}{x_1 + u_1}(x_3 + u_1) \\ h_3 \equiv (x_1 + u_1)x_4 - (x_3 + u_1)x_2 &= 0. \end{aligned}$$

2. $\mathrm{col}(C, B, F)$

$$\begin{aligned} \textit{slope of } \overline{CB} &= \frac{u_3 - 0}{u_2 - u_1} \\ x_4 - 0 &= \frac{u_3 - 0}{u_2 - u_1}(x_3 - u_1) \\ h_4 \equiv (u_2 - u_1)x_4 - (x_3 - u_1)u_3 &= 0. \end{aligned}$$

Having gotten the polynomials that determine the other coordinates, we as before find the polynomials for the actual problem in the theorem, which in this case is showing that $|\overline{FB}| = 2|\overline{FC}|$.

Translating:

$|\overline{FB}| \Rightarrow$

$x_3 - u_1 \longrightarrow$ *along x-axis*

$x_4 - 0 \longrightarrow$ *along y-axis*

and

$2|\overline{FC}| \Rightarrow$

$u_2 - x_3 \longrightarrow$ *along x-axis*

$u_3 - x_4 \longrightarrow$ *along y-axis.*

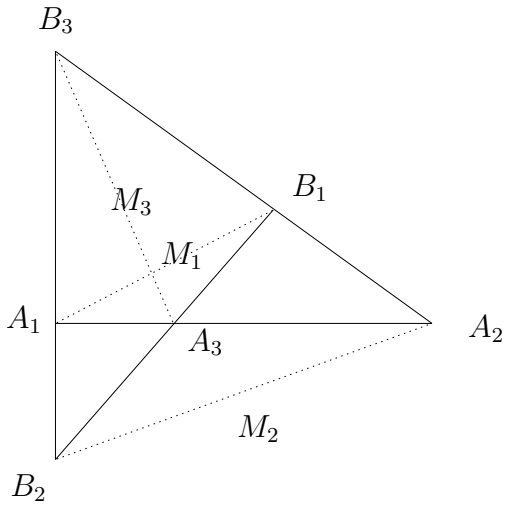
Therefore we have the following polynomials using the hypothesis $|\overline{FB}| = 2|\overline{FC}|$*:*

$$\begin{aligned} x_3 - u_1 &= u_2 - x_3 \\ \Rightarrow g_1 \equiv 3x_3 - 2u_2 - u_1 &= 0 \\ x_4 - 0 &= u_3 - x_4 \\ \Rightarrow g_2 \equiv 3x_4 - 2u_3 &= 0. \end{aligned}$$

3.3 Third Automatic Theorem Translation

Theorem 3.3 *(Gauss' Line.)*

The midpoints M_1, M_2, M_3 *of the three diagonals* $\overline{A_1B_1}, \overline{A_2B_2}, \overline{A_3B_3}$ *of any complete quadrilateral are collinear.[Wan98]*



placing coordinates:

$$\begin{aligned} A_1 &= (0,0) \\ A_2 &= (u_1,0) \\ B_2 &= (0,u_3) \\ B_1 &= (x_1,x_2) \\ B_3 &= (0,u_4) \\ A_3 &= (u_2,0) \\ M_1 &= (x_3,x_4) \\ M_2 &= (x_5,x_6) \\ M_3 &= (x_7,x_8), \end{aligned}$$

we obtain the following:

$$\begin{aligned} h_1 \equiv u_2x_2 - u_2u_3 + u_3x_1 &= 0 \\ h_2 \equiv u_1x_2 + u_4x_1 - u_1u_4 &= 0 \\ h_3 \equiv 2x_3 - x_1 &= 0 \\ h_4 \equiv 2x_4 - x_2 &= 0 \\ h_5 \equiv 2x_5 - u_1 &= 0 \\ h_6 \equiv 2x_6 - u_3 &= 0 \\ h_7 \equiv 2x_7 - u_2 &= 0 \\ h_8 \equiv 2x_8 - u_4 &= 0. \end{aligned}$$

We are to show:

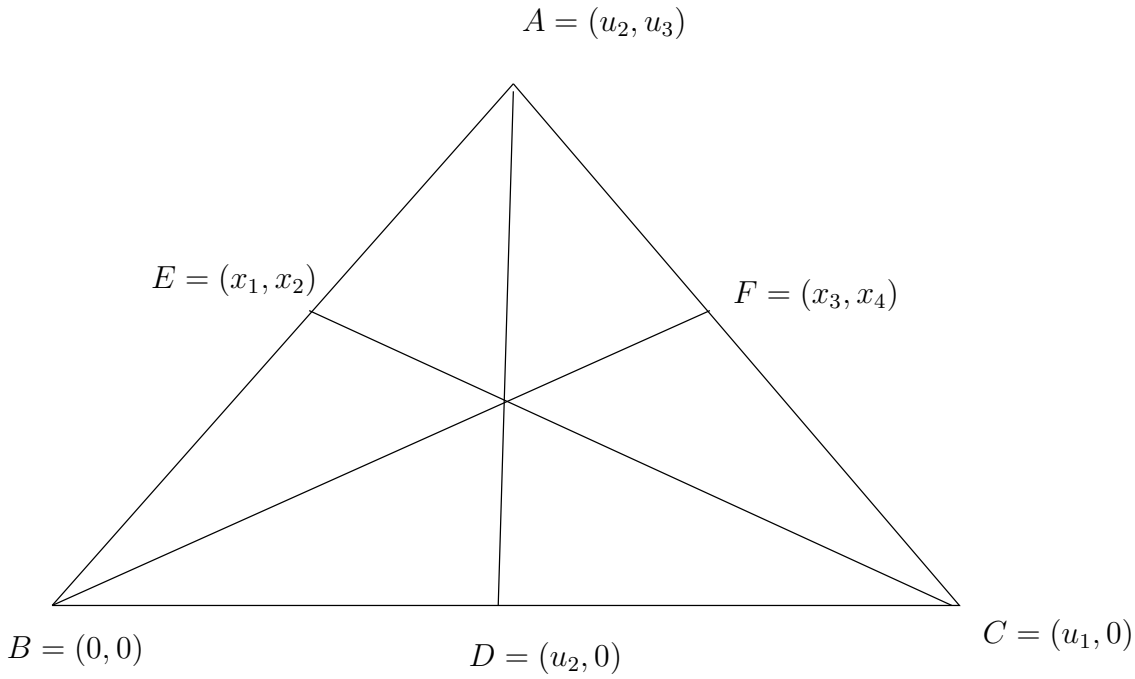
$$g \equiv x_3x_8 - x_5x_8 - x_3x_6 - x_4x_7 + x_4x_5 + x_6x_7 = 0.$$

3.4 Fourth Automatic Theorem Translation

Theorem 3.4 *(Ceva's theorem) The altitudes of a triangle $\triangle ABC$ all meet in a single point, O, called the orthocenter.[Eli]*

Determining $E = (x_1, x_2)$ and $F = (x_3, x_4)$ and from the obtained polynomials, we place coordinates $G = (u_2, x_5)$ and $H = (u_2, x_6)$ to obtain the system of polynomials below:

$$\begin{aligned} h_1 \equiv u_2x_2 - u_3x_1 &= 0 \\ h_2 \equiv u_2x_4 - u_1x_4 - u_3x_3 + u_1u_3 &= 0 \\ h_3 \equiv x_2u_3 + u_2x_1 - u_1u_2 &= 0 \\ h_4 \equiv x_4u_3 + u_2x_3 - u_1x_3 &= 0 \\ h_5 \equiv x_2x_1 - x_5x_1 - u_1x_2 + u_1x_5 - x_2x_1 + u_2x_2 &= 0 \\ h_6 \equiv x_6x_3 - u_2x_4 &= 0. \end{aligned}$$



We are to show that:

$$g \equiv x_5 - x_6 \quad = \quad 0.$$

4. Application of Groebner Basis

Considering a typical geometric theorem, we will have some number of arbitrary coordinates, or independent variables, denoted by $u_1, u_2, \ldots, u_m$ and also dependent variables $x_1, x_2, \ldots, x_n$, as seen in chapter 3.[CLO92] The hypotheses of the theorem will be represented by a collection of polynomial equations in the u_i, x_j. So we suppose there are two sets of polynomials, one describing the configuration assumptions, which we denote h_i.The other one describing the assumption being made, denoted g_j:

$$\begin{aligned} h_1(u_1, u_2, \ldots, u_m, x_1, x_2, \ldots, x_n) &= 0 \\ &\vdots \\ h_n(u_1, u_2, \ldots, u_m, x_1, x_2, \ldots, x_n) &= 0. \end{aligned}$$

The conclusion of the theorem will also be expressed as polynomials in the u_i, x_j. Now if there are more than one conclusion, we will have to solve the theorem one polynomial at a time. Thus considering one polynomial, we write

$$g(u_1, u_2, \ldots, u_m, x_1, x_2, \ldots, x_n) = 0.$$

We seek to know how g can be arrived at from $h_1, h_2, \ldots, h_n$, that is we want g to vanish whenever $h_1, h_2, \ldots, h_n$ does. Now 4.1 are equations that define a variety, that is

$$V = V(h_1, h_2, \ldots, h_n) \subset \mathbb{R}^{m+n}.$$

4.1 A Generic Conclusion of g

Definition 4.1 *The conclusion g follows strictly from the hypotheses $h_1, h_2, \ldots, h_n$ if $g \in I(V) \subset \mathbb{R}[u_1, u_2, \ldots, u_m, x_1, x_2, \ldots, x_n]$, where $V = V(h_1, h_2, \ldots, h_n)$,[CLO92]*

Definition 4.1 proves reasonable only for theorems without "degenerate" cases. By "degenerate" cases we mean situations where the x_j variables obtained from u_i which were arbitrary chosen, vanishes.

Therefore to prove that a theorem is true we would also need to show that its conclusion follows generically from its hypotheses.

Definition 4.2 *The conclusion g follows generically from hypotheses $h_1, h_2, \ldots, h_n$ if $g \in I(V') \subset \mathbb{R}[u_1, u_2, \ldots, u_m, x_1, x_2, \ldots, x_n]$, where $V' \subset R^{m+n}$ is the union of the components of the variety $V = V(h_1, h_2, \ldots, h_n)$ on which the u_i are algebraically independent. (See [Kat06] and [CLO92]).*

Proposition 4.3 *g follows generically from $h_1, h_2, \ldots, h_n$ whenever there is some nonzero polynomial $c(u_1, u_2, \ldots, u_m) \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ such that $c.g \in \sqrt{H}$ where H is the ideal generated by the hypothesis h_i in $\mathbb{R}[u_1, u_2, \ldots, u_m, x_1, x_2, \ldots, x_n]$.*

Proof:

Let V_j be one of the irreducible components of V'. Since $c.g \in \sqrt{H}$, we see that $c.g$ vanishes on V and, hence on V_j. Thus the product $c.g$ is in $I(V_j)$. But V_j is irreducible, so that $I(V_j)$ is a prime ideal by proposition 1.35. Thus $c.g \in I(V_j)$ implies either c or g is in $I(V_j)$. We know $c \notin I(V_j)$ since no nonzero polynomial in the u_i alone vanishes on this component. Hence $g \in I(V_j)$ and the same is true for components of V_j it follows that $g \in V'$.[CLO92]

Corollary 4.4 *In the situation of proposition 4.3, the following are equivalent*

1. *There is a nonzero polynomial $c \in \mathbb{R}[u_1, u_2, \ldots, u_m]$ such that $c.g \in \sqrt{H}$.*
2. *$g \in \sqrt{\overline{H}}$, where $\overline{H}$ is the ideal generated by the h_j in $\mathbb{R}(u_1, u_2, \ldots, u_m)[x_1, x_2, \ldots, x_n]$.*
3. *$\{1\}$ is the reduced Groebner basis of the ideal $\langle h_1, h_2, \ldots, h_n, 1 - yg\rangle \subset \mathbb{R}(u_1, u_2, \ldots, u_m)[x_1, x_2, \ldots, x_n]$.[CLO92]*

Combining proposition 4.3 and 3 of corollary 4.4 gives the Groebner basis method in geometric theorem proving.[Sog]

Now in chapters 2 and 3 we saw how to translate and also determine polynomials from arbitrary placed coordinates. Next we will here use the theorem stated above to show for the first three theorems, that g follows generically from $h_1, h_2, \ldots, h_n$. This is made easier using the package Singular.(See [Cen94], [Kat06] and [Wan98])

4.2 First Automatic Theorem Proof

From chapter 3 the first case considered was a very simple theorem of parallelograms. The verification is as stated below. (See [AL94])

```
> ring r=(0,x1,x2,x3,x4),(u1,u2,u3),lp;
> ideal i=u2-x4,u1*x4-x2*x4-u2*x3,x4*u3-u1*x1,x1*x3-x1*x2-x4*u3-x2*x4;
> groebner(i);
_[1]=1
```

Now by definition 4.1, theorem 1.29 in Chapter 1, proposition 1.35 and corollary 4.4, we can say g and f follows generically from $h_1, h_2, \ldots, h_n$ if $\{1\}$ is the Groebner basis of the ideal generated by $\{h_1, h_2, h_3, h_4, 1 - yg\}$ and $\{h_1, h_2, h_3, h_4, 1 - yf\}$ respectively, where y is a variable. Now the result above gotten using the package Singular, shows that $\{1\}$ is a Groebner basis of the

ideal generated by $\{h_1, h_2, h_3, h_4, 1-yg\}$ or $\{h_1, h_2, h_3, h_4, 1-yf\}$. We would next check if that condition is truly satisfied.[Sog] Therefore we will verify the membership of $1-yg$ and $1-yf$ in i by checking if it is a Groebner basis. Solving, we have:

```
> ring r=(0,x1,x2,x3,x4),(u1,u2,u3,y),lp;
> poly g=u1^2-2*u1*u3+u2^2-2*u2*x1;
> poly g1=1-y*g;
> ideal i=u2-x4,u1*x4-x2*x4-u2*x3,x4*u3-u1*x1,x1*x3-x1*x2-x4*u3-x2*x4,g1;
> groebner(i);
_[1]=1
//
> ring r=(0,x1,x2,x3,x4),(u1,u2,u3,y),lp;
> poly f=2*x2*u3-2*x3*u3-2*x1*x4+x3^2+x4^2-x2^2;
> poly f1=1-y*f;
> ideal i=u2-x4,u1*x4-x2*x4-u2*x3,x4*u3-u1*x1,
x1*x3-x1*x2-x4*u3-x2*x4,f1;
> groebner(i);
_[1]=1
>
```

And as expected the results above satisfies the already stated conditions, in particular, proposition 1.35 and corollary 4.4. Hence the theorem is verified.

4.3 Second Automatic Theorem Proof

The second translation has the result below:

```
> ring r=(0,x1,x2,x3,x4),(u1,u2,u3),lp;
> ideal i=2*u1-x3,2*u2-x4,u1*x1+x1*x2-u2*u3-u2*x2,x1*x3-x1*x2
-x4*u3+x4*x2;
> groebner(i);
_[1]=1
```

From the first verification, we have seen that all we need show is that g and f follows generically from $h_1, h_2, \ldots, h_n$ if $\{1\}$ is the Groebner basis of the ideal generated by $\{h_1, h_2, h_3, h_4, 1-yg\}$ or $\{h_1, h_2, h_3, h_4, 1-yf\}$. The result above satisfies one of the conditions, next we check if $1-yg$ and $1-yf$ are both in i.

```
> ring r=(0,x1,x2,x3,x4),(u1,u2,u3,y),lp;
> poly g=3*u3-2*x3-x2;
> poly g1=1-y*g;
```

```
> ideal i=2*u1-x3,2*u2-x4,u1*x1+x1*x2-u2*u3-u2*x2,
x1*x3-x1*x2-x4*u3+x4*x2,g1;
> groebner(i);
_[1]=1
//
>  poly f=3*x1-2*x4;
> poly f1=1-y*f;
> i=2*u1-x3,2*u2-x4,u1*x1+x1*x2-u2*u3-u2*x2,
x1*x3-x1*x2-x4*u3+x4*x2,f1;
> groebner(i);
_[1]=1
```

And from the already stated conditions, they are both in i. Hence, proving the theorem.

4.4 Third Automatic Theorem Proof

We are now conversant with the steps so we will prove directly as below:

```
 ring r=(0,u1,u2,u3,u4),(x1,x2,x3,x4,x5,x6,x7,x8),lp;
> ideal i=u2*x2-u2*u3+u3*x1,u1*x2+u4*x1-u1*u4,2*x3-x1,2*x4-x2,
. 2*x5-u1,2*x6-u3,2*x7-u2,2*x8-u4;
> poly g=x3*x8-x5*x8-x3*x6-x4*x7+x4*x5+x6*x7;
> groebner(i);
_[1]=2*x8+(-u4)
_[2]=2*x7+(-u2)
_[3]=2*x6+(-u3)
_[4]=2*x5+(-u1)
_[5]=(-2*u1*u3+2*u2*u4)*x4+(u1*u3*u4-u2*u3*u4)
_[6]=(2*u4)*x3+(2*u1)*x4+(-u1*u4)
_[7]=x2-2*x4
_[8]=x1-2*x3
> reduce(g,std(i));
0
```

We will note here that, the Groebner basis generated here is not $\{1\}$, but it satisfies the proposition 1.19, corollary 1.20 and corollary 4.4 thus proving the theorem.

Remark 4.5 *It will be noted here that it is possible to obtain a generated Groebner basis that is neither* $\{1\}$ *nor its remainder on division equal to* 0. *In such cases, we make use of the steps of the Division Algorithm, theorem 1.14 and the Buchberger Algorithm, theorem 1.24. That is we replace the remainder obtained, in the ideal* i *and repeat the multivariate division again.*

In general when performing automatic theorem proving, one has to be careful not to include 'degenerate" cases. This can be done simply by defining the variables x_j in r (r is the ring in the code above) different from zero. This turns out to be a limitation in Groebner basis Method, because it does not tell us what the "degenerate" cases are. Consequently, when using Groebner basis Method, we can verify theorems directly without knowing what the "degenerate" cases actually are.

4.5 Singular Package

The Singular package, its manual and libraries can be obtained at http://www.singular.uni-kl.de/Manual/latest/.

5. Conclusion

This work began with basic definitions, a brief overview of Groebner bases and also a detailed step by step presentation of the translation of Euclidean geometry to algebraic geometry. The work continued with the applications of the already built background in different geometric theorems. As the topic of the essay implies, the results of these translations were finally verified using the computer software Singular. In the course of proving, a limitation was observed and that is the fact that Groebner basis does not tell us what the degenerated cases are. However for such cases we were able to subject the dependent variables to a nonzero condition, eventually proving the theorems.

Interestingly the aspect of translating to algebraic geometry opens a door for further research as there is a possibility of developing an automatic process of translating the given theorem without directly involving the human intelligence.

Furthermore the degenerate cases of the Groebner basis method can be looked into using other methods like the Wu's method which is outside the scope of this work.

Acknowledgements

I give all honour and praise to Him who owns all lives and by whom I have my being. I am who I am because of Him, I acknowledge His sovereign majesty and declare that He is indeed God.

I acknowledge the great wisdom and supervision of my supervisor Professor Barry Green of the University of Stellenbosch. Your words and directions will remain guiding principles to me. I am grateful to the management of AIMS for this opportunity granted me to study here at AIMS. I am most honoured.

I will also like to acknowledge the support of my Dean of Faculty, Prof M. S. Audu, my Head of Department Prof W. Sirisena, the director of Carnegie, Jos, Prof L. S. O. Liverpool, Prof S. U. Momoh and all my senior colleagues all of the University of Jos, who saw to it that I had all I needed to study here at AIMS. I have great leaders in you, thank you very much.

The joy of having a family cannot be over emphasised as I acknowledge the great support of a woman of honour, a woman of rare gem, one who stands by me continually, my Mother, Mrs Louise Ramotu Olatayo and my loving father Mr Martin Adebayo Olatayo. With me on this walk is a very humble man and one of great countenance my fiance Engr Adewoye Peter Ademola, thank you for your support and practically staying awake through the nights as I studied. I will also like to acknowledge the great support of my wonderful sister Modupe Olatayo and all my siblings Mr and Mrs Ocholi, Mr Oludare Olatayo, Stephen Olatayo, Rotimi Olatayo, and my blessed little nephew Ephraim Ocholi.

I will also like to acknowledge the great team spirit of our Tutors Henry, Laure, Sam, Christian, Jean Marie, Eman, Ambrose and my Tutor Paul, who have patiently seen to it that as a student the best of my work was carefully written and presented.

What is study without the determined spirit of unique students from all countries within Africa! Especially my great Nigerian colleagues, to you I owe the determination to excel and I say thank you all.

Bibliography

[AL94] W. Adams and P. Loustaunau. An introduction to groebner bases, 1994. AMS Graduate Studies in Mathematics 3.

[Cen94] The Geometry Center. Groebner bases and elimination of variables, 1994. "Available from http://www.geom.uiuc.edu/ fjw/calc-init/nephroid/grobner.html".

[CLO92] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms an introduction to computational algebraic geometry and commutative algebra*. Undergraduate texts in mathematics. Springer-Verlag New York-Berlin-Paris, 1992.

[Eli] Joran Elias. Automatic geometric theorem proving: Wu's method. "Available from http://www.montanamath.org/TMME/v3n1/TMMEv3n1a2.pdf".

[GMG06] H. Schoenemann G. M. Greuel, G. Pfister. Singular manual, 2006. "Available from http://www.singular.uni-kl.de/Manual/latest/index.htm".

[Gre07] Barry Green. Topics in computational algebra and applications 2007, 2007. Unpublished manuscript.

[Kar06] Richard Karp. Great algorithms, 2006. "Available from http://www.eecs.berkeley.edu/ karp/greatalgo/".

[Kat06] Moty Katzman. Automatic geometric theorem proving; or a good excuse to tell you what i do for a living, 2006. "Available from http://www.katzman.staff.shef.ac.uk/Talks/VTgroupJuly2006.pdf".

[Sch03] Hall Schenck. Computational algebraic geometry, 2003. London Mathematical Society Student Text 58.

[Sog] Aksel Sogstad. The algebraic geometry notebooks for non-experts. "Available from http://www.sogstad.net/algnotes/".

[Wan98] Dongming Wang. Groebner bases applied to geometric theorem proving and discovering, 1998. Groebner Bases and Applications (Proceedings of the International Conference "33 Years of Groebner Bases", B. Buchberger and F. Winkler, eds.).