Automated Geometric Theorem Proving

Manish Patel

December 21, 2022

A Project on

Automated Geometric Theorem Proving

Submitted for partial fulfillment of award of

MASTER OF SCIENCE

University of Mumbai

Degree in MATHS

By
Manish Patel

Under the Guidance of
Dr. Selby Jose

Department of Mathematics
The Institute of Science
Mumbai - 400032

December, 2022

Declaration

I hereby declare that the project work entitled "**A**utomated Geometry Theorem Proving" carried out at the Department of Mathematics, The Institute of Science, Mumbai, is a record of an original work done by me under the guidance of **Dr. Selby Jose**, The Institute of Science, and this project work is submitted in the partial fulfillment of the requirements for the award of the degree of Master of Science in Mathematics, University of Mumbai. The results embodied in this report have not been submitted to any other University or Institute for the award of any degree or diploma.

Manish Patel (Candidate)

202117

Certificate

This is to certify that the project report entitled **Automated Geometry Theorem Proving**, carried out at the Department of Mathematics, The Institute of Science, Mumbai, in partial fulfillment for the award of the degree of Master of Science in Mathematics, University of Mumbai, is a record of bonafide work carried out by **Mr. Manish Patel**, Seat No. **202117**, under the supervision and guidance of **Dr. Selby Jose** during the academic year 2022-2023.

Dr. Selby Jose **External Examiner** **Head of Dept.** **Project Guide**
Mathematics

Place: Mumbai

Date:

Acknowledgment

I would like to start by extending my deep gratitude to my mentor, Dr. Selby Jose sir, for his unwavering support of my project study and related research, as well as for his patience, encouragement, and immense knowledge and experience. I was able to understand the subjects thanks to his guidance. Additionally, I thank him for giving me the chance to discover more and expand my knowledge.

Manish Patel

Abstract

Elementary geometry has been developed for more than 5000 years. Almost all the theorems and results were proved using geometric reasoning, which might require some more time. It was desirable to make the process of proving elementary geometric theorems mechanical. The advent of fast computers has revived interest in the algebraization of geometric reasoning. Grobner-bases theory was developed in the last century, which was a significant step forward, leading to the making of geometric proofs mechanical. The aim of this paper is to algebraize geometry so that most of the theorems in elementary geometry can now be proved or even rediscovered automatically on a computer.

Contents

1 Introduction

The earliest successful work on utilising computer programmes to prove geometry theorems was carried out by H. Gelernter and his associates. They used a strategy that was based on the conventional Euclidean proof strategy.

On the other hand, A. Tarski provided an algebraic method-based decision-making process for what he called elementary geometry. Even after A. Seidenberg, G. Collins, and others made advances along this line, Tarski's versions still didn't seem to be able to mechanically establish nontrivial geometry theorems in reality.

When Chinese mathematician Wu Wen-Tsün developed an algebraic technique in 1977 that may be used to prove a number of geometry theorems whose conventional proofs require a tremendous amount of human intelligence, it came as quite a surprise.

There is a variety of geometries. For example, we have heard about at least affine geometry and Euclidean geometry. Proving or disproving geometry statements in these two geometries is different since the field associated with Euclidean geometry is the field of real numbers, whereas almost any fields can be the fields associated with affine geometry; particularly, they can be algebraically closed fields. To understand this issue fully, we need to discuss the relationship between geometry and algebra.

§1.1 Affine Geometry

Our first example of geometry is the simplest one: affine geometry. This geometry can be illustrated as an example of how to introduce algebra or number systems to geometry. The only basic relation in this geometry is that of incidence, i.e., a point A is on a line l, or equivalently, a line l passes through (contains) a point A.

§1.2 Metric Geometry

The next example is metric geometry, introduced by Wu. Metric geometry is a class of affine geometry in which there are two new basic relations "perpendicularity" and "(segment) Congruence".

§1.3 Hilbert Geometry

Hilbert geometry is ordered metric geometry like $\mathbb{R}^2$.

§1.4 Tarski Geometry

An ordered field K for which no non-trivial algebraic extension (cf. Extension of a field) can be ordered. Each model of the theory of Tarski geometry can be represented as R^2, where R is a real closed field. Due to a fundamental contribution by Tarski, the theory of Tarski geometry is decidable. As we know, there are Non-Archimedean Tarski geometries.

The above four geometries are compatible with Euclidean geometry in the sense that Euclidean geometry is a model of the theories of the four geometries.

§1.5 algebra

Formulation **F1** Together with $h_1 = 0, \dots, h_n = 0$, all nondegenerate conditions necessary for the validity of the statement are specified in the polynomial equation forms $s_1 \neq 0, \dots, s_k \neq 0$. Then the algebraic formulation is: (2.1) $\forall y_i \in E\,[(h_1 = 0 \wedge \dots \wedge h_n = 0 \wedge s_1 \neq 0 \wedge \dots \wedge s_k \neq 0) \Rightarrow g = 0]$.

"All human knowledge begins with intuitions, thence passes to concepts and ends with ideas."

Theorem 1. Let D be a UFD, then the polynomial ring $D\,[y_1, \dots, y_m]$ is also a UFD. In particular, $K\,[y_1, \dots, y_m]$ is a UFD.

Theorem 2. Let D be a UFD and K be its quotient field. Let a be an element in any extension of K, algebraic over K; let x be an indeterminate. Suppose there is an algorithm for factorization in D, then

There is an algorithm for factorization in the polynomial rings $D[x]$ and $K[x]$.

There is an algorithm for factorization in the polynomial ring $K(a)[x]$.

Theorem 3. Let V be a nonempty algebraic set. V is irreducible if and only if $I(V)$ is a prime ideal.

Theorem 4. If P is a prime ideal of A not identical to (1), then $V(P)$ is irreducible and $I(V(P)) = P$.

2 polynomials

§2.1 Monomials

Definition 1 (Monomial)**.** A monomial in $x_1, \dots, x_n$ is a product of the form

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

where all of the exponents $\alpha_1, \dots, \alpha_n$ are nonnegative integers. The total degree of this monomial is the sum $\alpha_1 + \cdots + \alpha_n$.

We can simplify the notation for monomials as follows: let $\alpha = (\alpha_1, \dots, \alpha_n)$ and $x = (x_1, \dots, x_n)$ be an n-tuple of nonnegative integers. Then we set

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

When $\alpha = (0, \dots, 0)$, note that $x^\alpha = 1$. We also let $|\alpha| = \alpha_1 + \cdots + \alpha_n$ denote the total degree of the monomial x^α.

Definition 2 (Polynomial)**.** A polynomial f in $x_1, \dots, x_n$ with coefficients in a field k is a finite linear combination (with coefficients in k) of monomials. We will write a polynomial f in the form

$$f = \sum_\alpha a_\alpha x^\alpha, \quad a_\alpha \in k,$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \dots, \alpha_n)$.

The set of all polynomials in $x_1, \dots, x_n$ with coefficients in k is denoted $k[x_1, \dots, x_n]$.

Definition 3. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial in $k[x_1, \dots, x_n]$.

We call a_α the coefficient of the monomial x^α.

If $a_\alpha \neq 0$, then we call $a_\alpha x^\alpha$ a term of f.

The total degree of $f \neq 0$, denoted $\deg(f)$, is the maximum $|\alpha|$ such that the coefficient a_α is nonzero.

As an example, the polynomial $f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$ given above has four terms and total degree six.

§2.2 Variety

Definition 4 (Affine Space)**.** Given a field k and a positive integer n, we define the n-

dimensional affine space over k to be the set

$$k^n = \{(a_1, \dots, a_n) \mid a_1, \dots, a_n \in k\}$$

Definition 5 (Affine Varieties). Definition 1. Let k be a field, and let $f_1, \dots, f_s$ be polynomials in $k[x_1, \dots, x_n]$. Then we set

$$\mathbf{V}(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in k^n \mid f_i(a_1, \dots, a_n) = 0 \text{ for all } 1 \leq i \leq s\}.$$

We call $\mathbf{V}(f_1, \dots, f_s)$ the affine variety defined by $f_1, \dots, f_s$.

We begin in the plane $\mathbb{R}^2$ with the variety $\mathbf{V}\left(x^2 + y^2 - 1\right)$, which is the circle of radius 1 centered at the origin

Box Title

If $V, W \subseteq k^n$ are affine varieties, then so are $V \cup W$ and $V \cap W$.

Proof. Suppose that $V = \mathbf{V}(f_1, \dots, f_s)$ and $W = \mathbf{V}(g_1, \dots, g_t)$. Then we claim that

$$V \cap W = \mathbf{V}(f_1, \dots, f_s, g_1, \dots, g_t)$$
$$V \cup W = \mathbf{V}\left(f_i g_j \mid 1 \leq i \leq s, 1 \leq j \leq t\right)$$

§2.3 Ring Ideal

Definition 6 (Ideal). A subset $I \subseteq k[x_1, \dots, x_n]$ is an ideal if it satisfies:

$0 \in I$.

If $f, g \in I$, then $f + g \in I$.

If $f \in I$ and $h \in k[x_1, \dots, x_n]$, then $hf \in I$.

Definition 7 (Generated Ideal). Let $f_1, \dots, f_s$ be polynomials in $k[x_1, \dots, x_n]$. Then we set

$$\langle f_1, \dots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \mid h_1, \dots, h_s \in k[x_1, \dots, x_n] \right\}$$

is an ideal of $k[x_1, \dots, x_n]$ generated by polynomials $f_1, \dots, f_s$.

We say that an ideal I is finitely generated if there exist $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ such that $I = \langle f_1, \dots, f_s \rangle$, and we say that $f_1, \dots, f_s$, are a basis of I.

Every ideal of $k[x_1, \dots, x_n]$ is finitely generated (this is known as the Hilbert Basis Theorem).

§2.4 Ideal and Affine variety

Theorem 5. If $f_1, \dots, f_s$ and $g_1, \dots, g_t$ are bases of the same ideal in $k[x_1, \dots, x_n]$, so that $\langle f_1, \dots, f_s \rangle = \langle g_1, \dots, g_t \rangle$, then we have $\mathbf{V}(f_1, \dots, f_s) = \mathbf{V}(g_1, \dots, g_t)$.

Definition 8. Let $V \subseteq k^n$ be an affine variety. Then we set

$$\mathbf{I}(V) = \{f \in k[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in V\}.$$

The crucial observation is that $\mathbf{I}(V)$ is an ideal.

Theorem 6. If $V \subseteq k^n$ is an affine variety, then $\mathbf{I}(V) \subseteq k[x_1, \dots, x_n]$ is an ideal. We will call $\mathbf{I}(V)$ the ideal of V.

$$\mathbf{I}(\{(0,0)\}) = \langle x, y \rangle.$$

$\mathbf{I}(k^n) = \{0\}$ when k is infinite. A more interesting example is given by the twisted cubic $V = \mathbf{V}\left(y - x^2, z - x^3\right)$ in $\mathbb{R}^3$. We claim that

$$\mathbf{I}(V) = \left\langle y - x^2, z - x^3 \right\rangle.$$

The example of the twisted cubic is very suggestive. We started with the polynomials $y - x^2$ and $z - x^3$, used them to define an affine variety, took all functions vanishing on the variety, and got back the ideal generated by the two polynomials. It is natural to wonder if this happens in general. So take $f_1, \dots, f_s \in k[x_1, \dots, x_n]$. This gives us

$$\underset{f_1, \cdots f_s}{\overset{polynomials}{}} \rightarrow \overset{variety}{V(f_1, \cdots f_s)} \rightarrow \overset{Ideal}{I(V(f_1, \cdots f_s))}$$

and the natural question to ask is whether $\mathbf{I}(\mathbf{V}(f_1, \dots, f_s)) = \langle f_1, \dots, f_s \rangle$?

The answer, unfortunately, is not always yes.

Theorem 7. Let $f_1, \dots, f_s \in k[x_1, \dots, x_n]$. Then $\langle f_1, \dots, f_s \rangle \subseteq \mathbf{I}(\mathbf{V}(f_1, \dots, f_s))$, although equality need not occur.

For arbitrary fields, the relationship between $\langle f_1, \dots, f_s \rangle$ and $\mathbf{I}(\mathbf{V}(f_1, \dots, f_s))$ can be rather subtle. However, over an algebraically closed field like $\mathbb{C}$, there is a straightforward relation between these ideals. This will be explained when we prove the Nullstellensatz in Chapter 4.

Although for a general field, $\mathbf{I}(\mathbf{V}(f_1, \dots, f_s))$ may not equal $\langle f_1, \dots, f_s \rangle$, the ideal of a variety always contains enough information to determine the variety uniquely.

Theorem 8. Let V and W be affine varieties in k^n. Then:

$V \subseteq W$ if and only if $\mathbf{I}(V) \supseteq \mathbf{I}(W)$.

$V = W$ if and only if $\mathbf{I}(V) = \mathbf{I}(W)$.

§2.5 Polynomial of One variable

Definition 9. Given a nonzero polynomial $f \in k[x]$, let

$$f = c_0 x^m + c_1 x^{m-1} + \cdots + c_m,$$

where $c_i \in k$ and $c_0 \neq 0$ thus, $m = \deg(f)$. Then we say that $c_0 x^m$ is the leading term of f, written $\mathrm{LT}(f) = c_0 x^m$.

Theorem 9 (The Division Algorithm). Let k be a field and let g be a nonzero polynomial in $k[x]$. Then every $f \in k[x]$ can be written as

$$f = qg + r$$

where $q, r \in k[x]$, and either $r = 0$ or $\deg(r) < \deg(g)$. Furthermore, q and r are unique, and there is an algorithm for finding q and r.

```
Input : g, f
Output : q, r
q := 0
r := f
while r != 0 and LT(g) divides LT(r):
    q := q + LT(r)/LT(g)
    r := r - (LT(r)/LT(g)) g
return q,r
```

Definition 10 (principle ideal). an ideal generated by one element is called a principal ideal. We say that $k[x]$ is a principal ideal domain, PID in short.

Definition 11 (Greatest Common Divisor). A greatest common divisor of polynomials $f, g \in k[x]$ is a polynomial h such that:

h divides f and g.

If p is another polynomial which divides f and g, then p divides h. When h has these properties, we write $h = \gcd(f, g)$.

```
Input : f , g
Output : h = gcd(f , g)
h := f
s := g
while s != 0:
    rem := remainder(h,s)
```

```
    h := s
    s := rem
RETURN h
```

§2.6 Monomial Ordering

we note that we can reconstruct the monomial $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ from the n-tuple of exponents $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{>0}^n$.

This observation establishes a one to one correspondence between the monomials in $k[x_1, \ldots, x_n]$ and $\mathbb{Z}_{\geq 0}^n$.

Furthermore, any ordering $>$ we establish on the space $\mathbb{Z}_{\geq 0}^n$ will give us an ordering on monomials: if $\alpha > \beta$ according to this ordering, we will also say that $x^\alpha > x^\beta$.

To begin, since a polynomial is a sum of monomials, we would like to be able to arrange the terms in a polynomial unambiguously in descending (or ascending) order.

This means that for every pair of monomials x^α and x^β, exactly one of the three statements

$$x^\alpha > x^\beta, \quad x^\alpha = x^\beta, \quad x^\beta > x^\alpha$$

should be true. A total order is also required to be transitive, so that $x^\alpha > x^\beta$ and $x^\beta > x^\gamma$ always imply $x^\alpha > x^\gamma$

Definition 12 (Monomial Ordering)**.** A monomial ordering $>$ on $k[x_1, \ldots, x_n]$ is a relation $>$ on $\mathbb{Z}_{\geq 0}^n$, or equivalently, a relation on the set of monomials $x^\alpha, \alpha \in \mathbb{Z}_{\geq 0}^n$, satisfying:

$\geq$ is a total (or linear) ordering on $\mathbb{Z}_{\geq 0}^n$.

If $\alpha > \beta$ and $\gamma \in \mathbb{Z}_{\geq 0}^n$, then $\alpha + \gamma > \beta + \gamma$.

$>$ is a well-ordering on $\mathbb{Z}_{\geq 0}^n$.

Definition 13 (Lexicographic Order)**.** Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ be in $\mathbb{Z}_{\geq 0}^n$. We say $\alpha >_{\text{lex}} \beta$ if the leftmost nonzero entry of the vector difference $\alpha - \beta \in \mathbb{Z}^n$ is positive. We will write $x^\alpha >_{\text{lex}} x^\beta$ if $\alpha >_{\text{lex}} \beta$.

The lex ordering on $\mathbb{Z}_{\geq 0}^n$ is a monomial ordering.

Definition 14 (Graded Lex Order)**.** Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. We say $\alpha >_{\text{grlex}} \beta$ if

$$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i, \quad \text{or} \quad |\alpha| = |\beta| \text{ and } \alpha >_{\text{lex}} \beta$$

Definition 15. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, \dots, x_n]$ and let $>$ be a monomial order.

The multidegree of f is

$$\text{multideg}(f) = \max\left(\alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0\right)$$

(the maximum is taken with respect to $>$).

The leading coefficient of f is

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

The leading monomial of f is

$$\text{LM}(f) = x^{\text{multideg}\,(f)}$$

The leading term of f is

$$\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f).$$

Example 1. To illustrate, let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ as before and let $>$ denote lex order. Then

$$\begin{aligned} \text{multideg}\,(f) &= (3, 0, 0) \\ \text{LC}(f) &= -5 \\ \text{LM}(f) &= x^3 \\ \text{LT}(f) &= -5x^3 \end{aligned}$$

§2.7 Generalized Division Algorithm

Theorem 10 (Division Algorithm Multinomials). Let $>$ be a monomial order on $\mathbb{Z}^n_{\geq 0}$, and let $F = (f_1, \dots, f_s)$ be an ordered s-tuple of polynomials in $k[x_1, \dots, x_n]$. Then every $f \in k[x_1, \dots, x_n]$ can be written as

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

where $q_i, r \in k[x_1, \dots, x_n]$, and either $r = 0$ or r is a linear combination, with coefficients in k, of monomials, none of which is divisible by any of $\text{LT}(f_1), \dots, \text{LT}(f_s)$. We call r a remainder of f on division by F. Furthermore, if $q_i f_i \neq 0$, then

$$\text{multideg}(f) \geq \text{multideg}\,(q_i f_i)$$

```
Input: f1, f2,..., fs, f
Output: q1, q2,..., qs, r

q1 := 0
q2 := 0 ...
qs := 0
r := 0
p := f

while p != 0 Do
    i := 1
    divisionoccured := false
    while i<= s and divisionoccured = false Do
        If LT(fi) divides LT(p):
            qi := qi + LT(p)/LT(fi)
            p := p - (LT(p)/LT(fi))fi
            divisionoccured := true
        else
            i := i + 1
        if divisionoccured = false:
            r := r + LT(p)
            p := p - LT(p)
return q1, q2, ..., qs, r
```

Example 2. We will first divide $f = xy^2 + 1$ by $f_1 = xy + 1$ and $f_2 = y + 1$, using lex order with $x > y$.

$$\begin{array}{rll} & a_1: & y \\ & a_2: & -1 \\ xy+1 & & \sqrt{xy^2+1} \\ y+1 & & \underline{xy^2 + y} \\ & & -y+1 \\ & & \underline{-y-1} \\ & & 2 \end{array}$$

Since $\mathrm{LT}(f_1)$ and $\mathrm{LT}(f_2)$ do not divide 2 , the remainder is $r = 2$ and we are done. Thus, we have written $f = xy^2 + 1$ in the form

$$xy^2 + 1 = y \cdot (xy + 1) + (-1) \cdot (y + 1) + 2.$$

§2.8 Monomial Ideals

Definition 16 (Monomial Ideals). An ideal $I \subseteq k[x_1, \ldots, x_n]$ is a monomial ideal if there

is a subset $A \subseteq \mathbb{Z}_{>0}^n$ (possibly infinite) such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha\in\Lambda} h_\alpha x^\alpha$, where $h_\alpha \in k[x_1, \dots, x_n]$. In this case, we write $I = \langle x^\alpha \mid \alpha \in A\rangle$

An example of a monomial ideal is given by $I = \left\langle x^4y^2, x^3y^4, x^2y^5\right\rangle \subseteq k[x, y]$.

Theorem 11. Let $I = \langle x^\alpha \mid \alpha \in A\rangle$ be a monomial ideal. Then a monomial x^β lies in I if and only if x^β is divisible by x^α for some $\alpha \in A$.

Theorem 12 (Dickson's Lemma). Let $I = \langle x^\alpha \mid \alpha \in A\rangle \subseteq k[x_1, \dots, x_n]$ be a monomial ideal. Then I can be written in the form $I = \left\langle x^{\alpha(1)}, \dots, x^{\alpha(s)}\right\rangle$, where $\alpha(1), \dots, \alpha(s) \in A$. In particular, I has a finite basis.

Definition 17. Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal other than $\{0\}$, and fix a monomial ordering on $k[x_1, \dots, x_n]$. Then:

We denote by $\mathrm{LT}(I)$ the set of leading terms of nonzero elements of I. Thus,

$$\mathrm{LT}(I) = \{cx^\alpha \mid \text{ there exists } f \in I\backslash\{0\} \text{ with } \mathrm{LT}(f) = cx^\alpha\}.$$

We denote by $\langle \mathrm{LT}(I)\rangle$ the ideal generated by the elements of $\mathrm{LT}(I)$.

Theorem 13. Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal different from $\{0\}$.

$\langle \mathrm{LT}(I)\rangle$ is a monomial ideal.

There are $g_1, \dots, g_t \in I$ such that $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t)\rangle$.

§2.9 Grobner Basis

Theorem 14 (The Hilbert Basis Theorem). Every ideal $I \subseteq k[x_1, \dots, x_n]$ has a finite generating set. In other words, $I = \langle g_1, \dots, g_t\rangle$ for some $g_1, \dots, g_t \in I$.

Definition 18. Let $f, g \in k[x_1, \dots, x_n]$ be nonzero polynomials. (i) If $\mathrm{multideg}(f) = \alpha$ and $\mathrm{multideg}(g) = \beta$, then let $\gamma = (\gamma_1, \dots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i. We call x^γ the least common multiple of $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$, written $x^\gamma = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$. (ii) The S-polynomial of f and g is the combination

$$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g$$

Example 3. let $f = x^3y^2 - x^2y^3 + x$ and $g = 3x^4y + y^2$ in $\mathbb{R}[x, y]$ with the grlex order.

Then $\gamma = (4, 2)$ and

$$\begin{aligned} S(f,g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ &= x \cdot f - (1/3) \cdot y \cdot g \\ &= -x^3y^3 + x^2 - (1/3)y^3 \end{aligned}$$

Theorem 15 (Buchberger's Criterion). Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ of I is a Gröbner basis of I if and only if for all pairs $i \neq j$, the remainder on division of $S\left(g_i, g_j\right)$ by G (listed in some order) is zero.

```
# Input: F = (f1, f2,... ,fs)
# Output: G = (g1, g2, ..., gt) # for I with F subset of G

G := F
REPEAT
    G_ := G
    For each pair {p, q}, p != q in G_ Do
        r := S(p,q)^(G_)
        If r != 0 Then G := G U {r}
Until G = G_
Return G
```

Theorem 16. Let G be a Gröbner basis of $I \subseteq k[x_1, \ldots, x_n]$. Let $p \in G$ be a polynomial such that $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \backslash \{p\}) \rangle$. Then $G \backslash \{p\}$ is also a Gröbner basis for I.

Definition 19. A reduced Gröbner basis for a polynomial ideal I is a Gröbner basis G for I such that:

$\mathrm{LC}(p) = 1$ for all $p \in G$.

For all $p \in G$, no monomial of p lies in $\langle \mathrm{LT}(G \backslash \{p\}) \rangle$.

Theorem 17. Let $I \neq \{0\}$ be a polynomial ideal. Then, for a given monomial ordering, I has a reduced Gröbner basis, and the reduced Gröbner basis is unique.

Theorem 18 (Ideal Membership Problem).

$$f \in I \text{ if and only if } \bar{f}^G = 0.$$

Example 4. Let $I = \langle f_1, f_2 \rangle = \left\langle xz - y^2, x^3 - z^2 \right\rangle \in \mathbb{C}[x, y, z]$, let $f = -4x^2y^2z^2 + y^6 + 3z^5$. We want to know if $f \in I$.

Using a computer algebra system, we find a Gröbner basis

$$G = \{f_1, f_2, f_3, f_4, f_5\} = \left\{xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5\right\}$$

Note that this is a reduced Gröbner basis. We may now test polynomials for membership in I. For example, dividing f above by G, we find

$$f = \left(-4xy^2z - 4y^4\right) \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 0 \cdot f_4 + (-3) \cdot f_5 + 0$$

Since the remainder is zero, we have $f \in I$.

3 Pseudodivision

To describe the first step in the process, we consider two polynomials in the ring $k[x_1, \ldots, x_n, y]$, written in the form where the coefficients c_i, d_j are polynomials in $x_1, \ldots, x_n$. Assume that $m \leq p$. Proceeding as in the one-variable division algorithm for polynomials in y, we can attempt to remove the leading term $c_p y^p$ in f by subtracting a multiple of g. However, this is not possible directly unless d_m divides c_p in $k[x_1, \ldots, x_n]$. In pseudodivision, we first multiply f by d_m to ensure that the leading coefficient is divisible by d_m, then proceed as in one-variable division. We can state the algorithm formally as follows.

Theorem 19. Let $f, g \in k[x_1, \ldots, x_n, y]$ and assume $m \leq p$ and $d_m \neq 0$.

$$f = c_p y^p + \cdots + c_1 y + c_0,$$
$$g = d_m y^m + \cdots + d_1 y + d_0,$$

There is an equation

$$d_m^s f = qg + r,$$

where $q, r \in k[x_1, \ldots, x_n, y]$, $s \geq 0$, and either $r = 0$ or the degree of r in y is less than m.

$r \in \langle f, g \rangle$ in the ring $k[x_1, \ldots, x_n, y]$.

```
# Input : f, g
# Output : q, r
m = deg(g, y)
d = LC(g, y)
r = f
q = 0
while r != 0 and deg(r, y) >= m:
    r := dr-LC(r, y)g y^(deg(r, y)-m)
    q := dq+LC(r, y)y^(deg(r, y)-m)
return q , r
```

Note that if we follow this procedure, the body of the WHILE loop will be executed at most $p - m + 1$ times. Thus, the power s in $d^s f = qg + r$ can be chosen so that $s \leq p - m + 1$.

From $d^s f = qg + r$, it follows that $r = d^s f - qg \in \langle f, g \rangle$. Since $d = d_m$, we also have $d_m^s f = qg + r$

The polynomials q, r are known as a pseudoquotient and a pseudoremainder of f on pseudodivision by g, with respect to the variable y.

We will use the notation $\mathrm{Rem}(f, g, y)$ for the pseudoremainder produced by the algorithm.

For example, if we pseudodivide $f = x^2 y^3 - y$ by $g = x^3 y - 2$ with respect to y by the algorithm above, we obtain the equation

$$\left(x^3\right)^3 f = \left(x^8y^2 + 2x^5y + 4x^2 - x^6\right) g + 8x^2 - 2x^6.$$

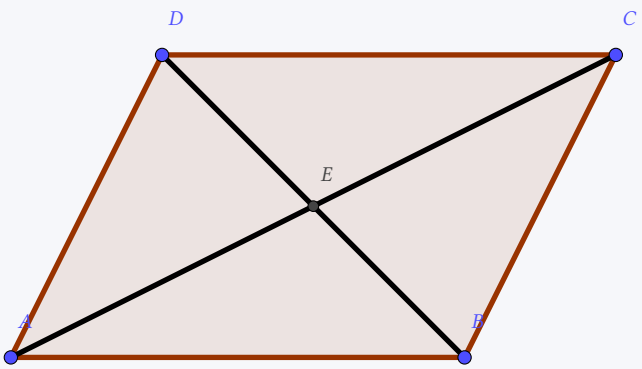
In particular, the pseudoremainder is $\mathrm{Rem}(f, g, y) = 8x^2 - 2x^6$.

4 Different Theorem Proving Methods

§4.1 The Defects in Traditional Proofs

§4.1.i Euclidean Proof

Example 5. Diagonal of parallelogram bisect each other.



Let $ABCD$ be a parallelogram (i.e, $AB \| CD, BC \| AD$), E be the intersection of the diagonals AC and BD. Show $AE \equiv CE$

We have to Prove that $EA = EC$ and $EB = ED$.

first to prove $\triangle ACB \cong \triangle CAD$ (hence $AB \equiv CD$), then to prove $\triangle AEB \cong \triangle CED$ (hence $AE \equiv CE$). In proving the congruence of these triangles, we have repeatedly used the fact $\angle CAB \equiv \angle ACD$. This fact is quite evident because the two angles are the alternative angles with respect to parallels AB and CD. However, here we have implicitly assumed the "trivial fact" that point D and B are on either sides of line AC. The last fact is harder to prove than the original statement.

Therefore, diagonals of a parallelogram bisect each other.

However, here we have implicitly assumed the "trivial fact" that point D and B are on either sides of line AC. The last fact is harder to prove than the original statement.

This extremely simple example reveals difficulty in implementing a powerful and sound geometry theorem prover based on traditional proofs. Of course, one can develop an interactive prover so that the user can input some trivial facts such as the one in the previous paragraph. These facts can be stored in a data base by programs. Then one would face a much more severe problem of the consistency of proofs.

§4.1.ii Analytic Proof

We place the vertex A at the origin and align the side $\overline{AB}$ with the horizontal coordinate axis.

We can let $A = (0,0), B = (u_1, 0), C = (u_2, u_3), D = (x_2, x_1)$, and $E = (x_4, x_3)$. Then we want to prove $g = 2u_2x_4 + 2u_3x_3 - u_3^2 - u_2^2 = 0$, i.e., $AE \equiv CE$.

Let us fix points A, B and C. We can use the line equations for AD and CD to solve the coordinates of point D, and the line equations for BD and AC to solve the coordinates of point E. Then we can substitute the solutions in the conclusion polynomial g to see whether the result is zero. Thus we have two line equations for x_1 and x_2 :

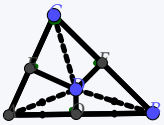
$$h_1 = u_1x_1 - u_1u_3 = 0$$
$$h_2 = u_3x_2 - (u_2 - u_1)\,x_1 = 0$$

AB is parallel to DC DA is parallel to CB. Also we have two line equations for x_3 and x_4

$$\begin{aligned} h_3 &= x_1x_4 - (x_2 - u_1)\,x_3 - u_1x_1 = 0 && E \text{ is on } BD \\ h_4 &= u_3x_4 - u_2x_3 = 0 && E \text{ is on } AC. \end{aligned}$$

Solving the first two equations, we have $x_1 = u_3, x_2 = u_2 - u_1$. Solving the last two equations and using the solutions for x_1 and x_2, we have $x_3 = u_3/2, x_4 = u_2/2$. Now substituting the solutions in g, we have $g = 0$. Thus, we prove the theorem.

Theorem 20. Every triangle is isosceles. Let ABC be a triangle as shown in Figure. We want to prove $CA \equiv CB$.



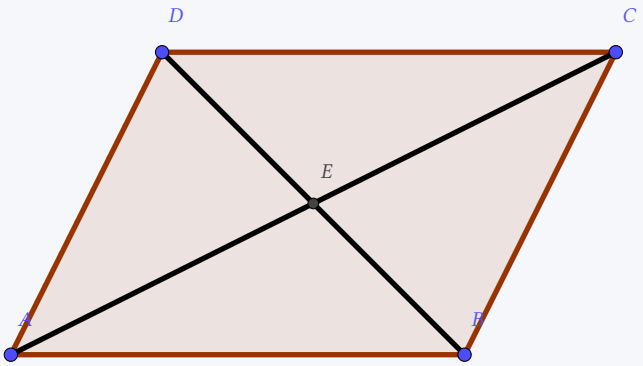
Proof. Let D be the intersection of the perpendicular bisector of AB and the internal bisector of angle ACB. Let $DE \perp AC$ and $DF \perp CB$. It is easy to see that $\triangle CDE \cong \triangle CDF$ and $\triangle ADE \cong \triangle BDF$. Hence $CE + EA = CF + FB$, i.e., $CA \equiv CB$

5 Grobner Basis Method

The basic idea underlying the methods is seeing points as Cartesian coordinates. Every simple hypotheses conclusions of geometric theorems can be expressed as polynomial equations.

§5.1 Geometric Configuration

Example 6. Let A, B, C, D be the vertices of a parallelogram in the plane. The two diagonals $\overline{AD}$ and $\overline{BC}$ of any parallelogram intersect at a point which bisects both diagonals.



Let $ABCD$ be a parallelogram (i.e, $AB \| CD, BC \| AD$), E be the intersection of the diagonals AC and BD. Show $AE \equiv CE$

We have to Prove that $EA = EC$ and $EB = ED$.

$A = (0, 0)$ $B = (u_1, 0)$ for some $u_1 \neq 0 \in \mathbb{R}$. $C = (u_2, u_3)$, where u_2, u_3 are new indeterminates independent of u_1, and $u_3 \neq 0$. The remaining vertex D is now completely determined by the choice of A, B, C.

While constructing the geometric configuration described by a theorem, some of the coordinates of some points will be arbitrary, whereas the remaining coordinates of points will be determined (possibly up to a finite number of choices) by the arbitrary ones.

To indicate arbitrary coordinates, we will consistently use variables u_i, whereas the other coordinates will be denoted x_j.

It is important to note that this division of coordinates into two subsets is in no way uniquely specified by the hypotheses of the theorem. Different constructions of a figure, for example, may lead to different sets of arbitrary variables and to different translations of the hypotheses into polynomial equations. eg. Parallelogram opposite points first

Since D is determined by A, B, and C, we will write $D = (x_1, x_2)$. One hypothesis of our theorem is that the quadrilateral $ABDC$ is a parallelogram or, equivalently, that the opposite pairs of sides are parallel and, hence, have the same slope. Using the slope formula for a line segment, we see that one translation of these statements is as follows:

$$\overline{AB} \parallel \overline{CD} \,:\, 0 = \frac{x_2 - u_3}{x_1 - u_2},$$
$$\overline{AC} \parallel \overline{BD} \,:\, \frac{u_3}{u_2} = \frac{x_2}{x_1 - u_1}.$$

Clearing denominators, we obtain the polynomial equations

$$h_1 = x_2 - u_3 = 0$$
$$h_2 = (x_1 - u_1)\, u_3 - x_2 u_2 = 0.$$

Is this unique way to represent? Below, we will discuss another way to get equations for x_1 and x_2.

Next, we construct the intersection point of the diagonals of the parallelogram. Since the coordinates of the intersection point E are determined by the other data, we write $E = (x_3, x_4)$. Saying that E is the intersection of the diagonals is equivalent to saying that E lies on both of the lines $\overline{AD}$ and $\overline{BC}$, or to saying that the triples A, E, D and B, E, C are collinear.

$$A, E, D \text{ collinear} : \frac{x_4}{x_3} = \frac{x_2}{x_1},$$
$$B, E, C \text{ collinear} : \frac{x_4}{x_3 - u_1} = \frac{u_3}{u_2 - u_1}.$$

Clearing denominators again, we have the polynomial equations

$$h_3 = x_4 x_1 - x_3 x_2 = 0$$
$$h_4 = x_4 (u_2 - u_1) - (x_3 - u_1)\, u_3 = 0.$$

The system of four equations formed from eq1 and eq2 gives one translation of the hypotheses of our theorem.

$$AE = ED \,:\, x_3^2 + x_4^2 = (x_3 - x_1)^2 + (x_4 - x_2)^2$$
$$BE = EC \,:\, (x_3 - u_1)^2 + x_4^2 = (x_3 - u_2)^2 + (x_4 - u_3)^2.$$

Canceling like terms, the conclusions can be written as

$$g_1 = x_1^2 - 2x_1 x_3 - 2x_4 x_2 + x_2^2 = 0,$$
$$g_2 = 2x_3 u_1 - 2x_3 u_2 - 2x_4 u_3 - u_1^2 + u_2^2 + u_3^2 = 0.$$

Our translation of the theorem states that the two equations in eq3 should hold when the hypotheses in eq1 and eq2 hold.

As we noted earlier, different translations of the hypotheses and conclusions of a theorem are possible. For instance, There is also a great deal of freedom in the way that hypotheses can be translated. $B = (u_1, 0)$ and $C = (u_2, u_3)$. Writing $D = (x_1, x_2)$, this alternate translation would be

$$h_1' = x_1 - u_1 - u_2 = 0,$$
$$h_2' = x_2 - u_3 = 0.$$

The following proposition lists some of the most common geometric statements that can be translated into polynomial equations.

Theorem 21. Let A, B, C, D, E, F be points in the plane. Each of the following geometric statements can be expressed by one or more polynomial equations:

$\overline{AB}$ is parallel to $\overline{CD}$.

$\overline{AB}$ is perpendicular to $\overline{CD}$.

A, B, C are collinear.

The distance from A to B is equal to the distance from C to D : $AB = CD$.

C lies on the circle with center A and radius AB.

C is the midpoint of $\overline{AB}$.

The acute angle $\angle ABC$ is equal to the acute angle $\angle DEF$

$\overline{BD}$ bisects the angle $\angle ABC$.

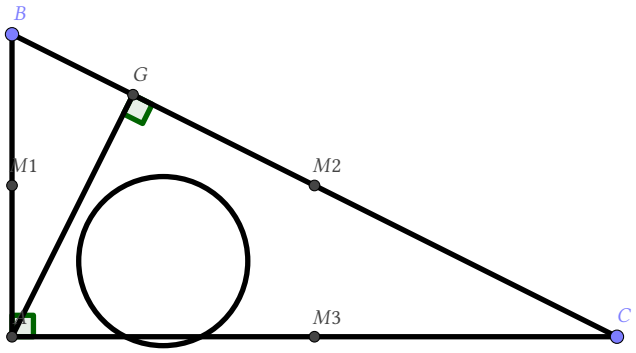
Let's translate the following beautiful result into polynomial equations.

Theorem 22 (The Circle Theorem of Apollonius)**.** Let $\triangle ABC$ be a right triangle in the plane, with right angle at A. The midpoints of the three sides and the foot of the altitude drawn from A to $\overline{BC}$ all lie on one circle.

The theorem is illustrated in the following figure:

We begin by constructing the triangle.

A at $(0, 0)$ B at $(u_1, 0)$, the hypothesis that $\angle CAB$ is a right angle says $C = (0, u_2)$.



=info= Of course, we are taking a shortcut here; we could also make C a general point and add the hypothesis $CA \perp AB$, but that would lead to more variables and more equations. =info=

$M_1 = (x_1, 0)$, $M_2 = (0, x_2)$, and $M_3 = (x_3, x_4)$.

Proposition 2 , we obtain the equations

$$\begin{aligned} h_1 &= 2x_1 - u_1 = 0, \\ h_2 &= 2x_2 - u_2 = 0, \\ h_3 &= 2x_3 - u_1 = 0, \\ h_4 &= 2x_4 - u_2 = 0. \end{aligned}$$

The next step is to construct the point $H = (x_5, x_6)$, the foot of the altitude drawn from A. We have two hypotheses here:

$$\begin{aligned} B, H, C \text{ collinear} : h_5 &= u_2 x_5 + u_1 x_6 - u_1 u_2 = 0, \\ AH \perp BC \ : h_6 &= u_1 x_5 - u_2 x_6 = 0. \end{aligned}$$

Finally, we must consider the statement that M_1, M_2, M_3, H lie on a circle.

Thus, our conclusion can be restated as follows: if we construct the circle containing the noncollinear triple M_1, M_2, M_3, then H must lie on this circle also. To apply part (v) of Proposition 2, we must know the center of the circle, so this is an additional point that must be constructed. We call the center $O = (x_7, x_8)$ and derive two additional hypotheses:

$$\begin{aligned} M_1O = M_2O \ : h_7 &= (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0 \\ M_1O = M_3O \ : h_8 &= (x_1 - x_7)^2 + (0 - x_8)^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0. \end{aligned}$$

Our conclusion is $HO = M_1O$, which takes the form

$$g = (x_5 - x_7)^2 + (x_6 - x_8)^2 - (x_1 - x_7)^2 - x_8^2 = 0.$$

=remark= Remark Both here and in Example 1, the number of hypotheses and the number of dependent variables x_j are the same. This is typical of properly posed geometric hypotheses. =remark=

=info= We expect that given values for the u_i, there should be at most finitely many different combinations of x_j satisfying the equations. =info=

§5.2 Generalization

We now consider the typical form of an admissible geometric theorem. We will have some number of arbitrary coordinates, or independent variables in our construction, denoted by $u_1, \ldots, u_m$. In addition, there will be some collection of dependent variables $x_1, \ldots, x_n$.

The hypotheses of the theorem will be represented by a collection of polynomial equations in the u_i, x_j.

As we noted in Example 3 , it is typical of a properly posed theorem that the number of hypotheses is equal to the number of dependent variables, so we will write the hypotheses as

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

The conclusions of the theorem will also be expressed as polynomials in the u_i, x_j. It suffices to consider the case of one conclusion since if there are more, we can simply treat them one at a time. Hence, we will write the conclusion as

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

=question= The question to be addressed is: how can the fact that g follows from $h_1, \ldots, h_n$ be deduced algebraically? The basic idea is that we want g to vanish whenever $h_1, \ldots, h_n$ do. We observe that the hypotheses (9) are equations that define a variety

$$V = \mathbf{V}(h_1, \ldots, h_n) \subseteq \mathbb{R}^{m+n}$$

=question=

> **Definition 20.** The conclusion g follows strictly from the hypotheses $h_1, \ldots, h_n$ if $g \in \mathbf{I}(V) \subseteq \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$, where $V = \mathbf{V}(h_1, \ldots, h_n)$

=warning= Although this definition seems reasonable, we will see later that it is too strict. Most geometric theorems have some "degenerate" cases that Definition 4 does not take into account. But for the time being, we will use the above notion of "follows strictly." =warning=

One drawback of Definition 4 is that because we are working over $\mathbb{R}$, we do not have an effective method for determining $\mathbf{I}(V)$. But we still have the following useful criterion.

Theorem 23. If $g \in \sqrt{\langle h_1, \dots, h_n \rangle}$, then g follows strictly from $h_1, \dots, h_n$.

Proof. The hypothesis $g \in \sqrt{\langle h_1, \dots, h_n \rangle}$ implies that $g^s \in \langle h_1, \dots, h_n \rangle$ for some s. Thus, $g^s = \sum_{i=1}^{n} A_i h_i$, where $A_i \in \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$. Then g^s, and, hence, g itself, must vanish whenever $h_1, \dots, h_n$ do. integraldomain ■

=note= Note that the converse of this proposition fails whenever $\sqrt{\langle h_1, \dots, h_n \rangle} \subsetneq \mathbf{I}(V)$, which can easily happen when working over $\mathbb{R}$. Nevertheless, Proposition 5 is still useful because we can test whether $g \in \sqrt{\langle h_1, \dots, h_n \rangle}$ using the radical membership algorithm. =note=

Theorem 24. Let $\bar{I} = \langle h_1, \dots, h_n, 1 - yg \rangle$ in the ring $\mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n, y]$. Then Proposition 8 of Chapter 4, §2 implies that

$$g \in \sqrt{\langle h_1, \dots, h_n \rangle} \iff \{1\} \text{ is the reduced Gröbner basis of } \bar{I}.$$

If this condition is satisfied, then g follows strictly from $h_1, \dots, h_n$.

Theorem 25. R to C Theorem If we work over $\mathbb{C}$, we can get a better sense of what $g \in \sqrt{\langle h_1, \dots, h_n \rangle}$ means. By allowing solutions in $\mathbb{C}$, the hypotheses $h_1, \dots, h_n$ define a variety $V_{\mathbb{C}} \subseteq \mathbb{C}^{m+n}$. Then, in Exercise 9, you will use the Strong Nullstellensatz to show that

$$g \in \sqrt{\langle h_1, \dots, h_n \rangle} \subseteq \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n] \iff g \in \mathbf{I}(V_{\mathbb{C}}) \subseteq \mathbb{C}[u_1, \dots, u_m, x_1, \dots, x_n].$$

Thus, $g \in \sqrt{\langle h_1, \dots, h_n \rangle}$ means that g "follows strictly over $\mathbb{C}$ " from $h_1, \dots, h_n$.

Let us apply these concepts to an example. This will reveal why Definition 4 is too strong.

Example 1 (continued). To see what can go wrong if we proceed as above, consider the theorem on the diagonals of a parallelogram from Example 1, taking as hypotheses the four polynomials from (1) and (2):

$$\begin{aligned} h_1 &= x_2 - u_3 \\ h_2 &= (x_1 - u_1)\, u_3 - u_2 x_2 \\ h_3 &= x_4 x_1 - x_3 x_2 \\ h_4 &= x_4 (u_2 - u_1) - (x_3 - u_1)\, u_3. \end{aligned}$$

We will take as conclusion the first polynomial from (3):

$$g = x_1^2 - 2x_1 x_3 - 2x_4 x_2 + x_2^2.$$

To apply Proposition 5, we must compute a Gröbner basis for

$$\bar{I} = \langle h_1, h_2, h_3, h_4, 1 - yg \rangle \subseteq \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4, y].$$

Surprisingly enough, we do not find $\{1\}$. (You will use a computer algebra system in Exercise 10 to verify this.) Since the statement is a true geometric theorem, we must try to understand why our proposed method failed in this case.

§5.3 Degenerate Cases

The reason can be seen by computing a Gröbner basis for $I = \langle h_1, h_2, h_3, h_4 \rangle$ in $\mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4]$, using lex order with $x_1 > x_2 > x_3 > x_4 > u_1 > u_2 > u_3$. The result is

$$\begin{aligned}
f_1 &= x_1x_4 + x_4u_1 - x_4u_2 - u_1u_3, \\
f_2 &= x_1u_3 - u_1u_3 - u_2u_3, \\
f_3 &= x_2 - u_3, \\
f_4 &= x_3u_3 + x_4u_1 + x_4u_2 - u_1u_3, \\
f_5 &= x_4u_1^2 - x_4u_1u_2 - \frac{1}{2}u_1^2u_3 + \frac{1}{2}u_1u_2u_3, \\
f_6 &= x_4u_1u_3 - \frac{1}{2}u_1u_3^2.
\end{aligned}$$

The variety $V = \mathbf{V}(h_1, h_2, h_3, h_4) = \mathbf{V}(f_1, \dots, f_6)$ in $\mathbb{R}^7$ defined by the hypotheses is actually reducible. To see this, note that f_2 factors as $(x_1 - u_1 - u_2)\,u_3$, which implies that

$$V = \mathbf{V}(f_1, x_1 - u_1 - u_2, f_3, f_4, f_5, f_6) \cup \mathbf{V}(f_1, u_3, f_3, f_4, f_5, f_6)$$

Since f_5 and f_6 also factor, we can continue this decomposition process. Things simplify dramatically if we recompute the Gröbner basis at each stage, and, in the exercises, you will show that this leads to the decomposition

$$V = V' \cup U_1 \cup U_2 \cup U_3$$

into irreducible varieties, where

$$\begin{aligned}
V' &= \mathbf{V}\left(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1 + u_2}{2}, x_4 - \frac{u_3}{2}\right), \\
U_1 &= \mathbf{V}(x_2, x_4, u_3) \\
U_2 &= \mathbf{V}(x_1, x_2, u_1 - u_2, u_3) \\
U_3 &= \mathbf{V}(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1)
\end{aligned}$$

You will also show that none of these varieties are contained in the others, so that V', U_1, U_2, U_3 are the irreducible components of V.

The problem becomes apparent when we interpret the components $U_1, U_2, U_3 \subseteq V$ in terms of the parallelogram $ABDC$. On U_1 and U_2, we have $u_3 = 0$. This is troubling since u_3 was supposed to be arbitrary. Further, when $u_3 = 0$, the vertex C of our parallelogram lies on $\overline{AB}$ and, hence we do not have a parallelogram at all. This is a degenerate case of our configuration, which we intended to rule out by the hypothesis that $ABDC$ was an honest parallelogram in the plane. Similarly, we have $u_1 = 0$ on U_3, which again is a degenerate configuration.

You can also check that on $U_1 = \mathbf{V}(x_2, x_4, u_3)$, our conclusion g becomes $g = x_1^2 - 2x_1x_3$, which is not zero since x_1 and x_3 are arbitrary on U_1. This explains why our first attempt failed to prove the theorem.

=question= Once we exclude the degenerate cases U_1, U_2, U_3, the above method easily shows that g vanishes on V'. We leave the details as an exercise. =question=

=solution= Our goal is to develop a general method that can be used to decide the validity of a theorem, taking into account any degenerate special cases that may need to be excluded. To begin, we use Theorem 2 of Chapter 4, §6 to write $V = \mathbf{V}(h_1, \dots, h_n) \subseteq \mathbb{R}^{m+n}$ as a finite union of irreducible varieties, =solution=

$$V = V_1 \cup \cdots \cup V_k.$$

As we saw in the continuation of Example 1, it may be the case that some polynomial equation involving only the u_i holds on one or more of these irreducible components of V. Since our intent is that the u_i should be essentially independent, we want to exclude these components from consideration if they are present. We introduce the following terminology.

Definition 21. Let W be an irreducible variety in the affine space $\mathbb{R}^{m+n}$ with coordinates $u_1, \dots, u_m, x_1, \dots, x_n$. We say that the functions $u_1, \dots, u_m$ are algebraically independent on W if no nonzero polynomial in the u_i alone vanishes identically on W.

Equivalently, Definition 6 states that $u_1, \dots, u_m$ are algebraically independent on W if $\mathbf{I}(W) \cap \mathbb{R}[u_1, \dots, u_m] = \{0\}$.

Thus, in the decomposition of the variety V given in (10), we can regroup the irreducible components in the following way:

$$V = W_1 \cup \cdots \cup W_p \cup U_1 \cup \cdots \cup U_q,$$

where $u_1, \dots, u_m$ are algebraically independent on the components W_i and are not algebraically independent on the components U_j. Thus, the U_j, represent "degenerate" cases of the hypotheses of our theorem.

To ensure that the variables u_i are actually arbitrary in the geometric configurations we study, we should consider only the subvariety

$$V' = W_1 \cup \cdots \cup W_p \subseteq V.$$

Given a conclusion $g \in \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$ we want to prove, we are not interested in how g behaves on the degenerate cases. This leads to the following definition.

Definition 22. The conclusion g follows generically from the hypotheses $h_1, \dots, h_n$ if $g \in \mathbf{I}(V') \subseteq \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$, where, as above, $V' \subseteq \mathbb{R}^{m+n}$ is the union of the components of the variety $V = \mathbf{V}(h_1, \dots, h_n)$ on which the u_i are algebraically independent.

=question= Saying a geometric theorem is "true" in the usual sense means precisely that its conclusion(s) follow generically from its hypotheses. The question becomes, given a conclusion g : can we determine when $g \in \mathbf{I}(V')$? =question=

In other words, can we develop a criterion that determines whether g vanishes on every component of V on which the u_i are algebraically independent, ignoring what happens on the possible "degenerate" components?

Determining the decomposition of a variety into irreducible components is not always easy, so we would like a method to determine whether a conclusion follows generically from a set of hypotheses that does not require knowledge of the decomposition eq11. Further, even if we could find V', we would still have the problem of computing $\mathbf{I}(V')$.

Fortunately, it is possible to show that g follows generically from $h_1, \ldots, h_n$ without knowing the decomposition of V given in eq11. We have the following result.

Example 7. Proposition 8 In the above situation, g follows generically from $h_1, \ldots, h_n$ whenever there is some nonzero polynomial $c(u_1, \ldots, u_m) \in \mathbb{R}[u_1, \ldots, u_m]$ such that

$$c \cdot g \in \sqrt{H},$$

where H is the ideal generated by the hypotheses h_i in $\mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$.

Proof. Let V_j be one of the irreducible components of V'. Since $c \cdot g \in \sqrt{H}$, we see that $c \cdot g$ vanishes on V and, hence, on V_j. Thus, the product $c \cdot g$ is in $\mathbf{I}(V_j)$. But V_j is irreducible, so that $\mathbf{I}(V_j)$ is a prime ideal by Proposition 3 of Chapter 4, §5. Thus, $c \cdot g \in \mathbf{I}(V_j)$ implies either c or g is in $\mathbf{I}(V_j)$. We know $c \notin \mathbf{I}(V_j)$ since no nonzero polynomial in the u_i alone vanishes on this component. Hence, $g \in \mathbf{I}(V_j)$, and since this is true for each component of V', it follows that $g \in \mathbf{I}(V')$. ■

For Proposition 8 to give a practical way of determining whether a conclusion follows generically from a set of hypotheses, we need a criterion for deciding when there is a nonzero polynomial c with $c \cdot g \in \sqrt{H}$. This is actually quite easy to do. By the definition of the radical, we know that $c \cdot g \in \sqrt{H}$ if and only if

$$(c \cdot g)^s = \sum_{j=1}^{n} A_j h_j$$

for some $A_j \in \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$ and $s \geq 1$. If we divide both sides of this equation by c^s, we obtain

$$g^s = \sum_{j=1}^{n} \frac{A_j}{c^s} h_j$$

$K(y)[x]$, i.e., the coefficients are rational functions in y

which shows that g is in the radical of the ideal $\tilde{H}$ generated by $h_1, \ldots, h_n$ over the ring $\mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n]$ (in which we allow denominators depending only on the u_i). Conversely, if $g \in \sqrt{\widetilde{H}}$, then

$$g^s = \sum_{j=1}^{n} B_j h_j$$

where the $B_j \in \mathbb{R}(u_1, \dots, u_m)[x_1, \dots, x_n]$. If we find a least common denominator c for all terms in all the B_j and multiply both sides by c^s (clearing denominators in the process), we obtain

$$(c \cdot g)^s = \sum_{j=1}^{n} B_j' h_j,$$

where $B_j' \in \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$ and c depends only on the u_i. As a result, $c \cdot g \in \sqrt{H}$. These calculations and the radical membership algorithm from §2 of Chapter 4 establish the following corollary of Proposition 8.

Corollary. Corollary 9. In the situation of Proposition 8, the following are equivalent: (i) There is a nonzero polynomial $c \in \mathbb{R}[u_1, \dots, u_m]$ such that $c \cdot g \in \sqrt{H}$. (ii) $g \in \sqrt{\widetilde{H}}$, where $\widetilde{H}$ is the ideal generated by the h_j in $\mathbb{R}(u_1, \dots, u_m)[x_1, \dots, x_n]$. (iii) $\{1\}$ is the reduced Gröbner basis of the ideal

$$\langle h_1, \dots, h_n, 1 - yg \rangle \subseteq \mathbb{R}(u_1, \dots, u_m)[x_1, \dots, x_n, y]$$

If we combine part (iii) of this corollary with Proposition 8, we get an algorithmic method for proving that a conclusion follows generically from a set of hypotheses. We will call this the Gröbner basis method in geometric theorem proving.

To illustrate the use of this method, we will consider the theorem on parallelograms from Example 1 once more.

We first compute a Gröbner basis of the ideal $\langle h_1, h_2, h_3, h_4, 1 - yg \rangle$ in the ring $\mathbb{R}(u_1, u_2, u_3)[x_1, x_2, x_3, x_4, y]$. This computation does yield $\{1\}$ as we expect.

Making u_1, u_2, u_3 invertible by passing to $\mathbb{R}(u_1, u_2, u_3)$ as our field of coefficients in effect removes the degenerate cases encountered above, and the conclusion does follow generically from the hypotheses.

Moreover, in Exercise 12, you will see that g itself (and not some higher power) actually lies in $\langle h_1, h_2, h_3, h_4 \rangle \subseteq \mathbb{R}(u_1, u_2, u_3)[x_1, x_2, x_3, x_4]$

=task= Note that the Gröbner basis method does not tell us what the degenerate cases are. The information about these cases is contained in the polynomial $c \in \mathbb{R}[u_1, \dots, u_m]$, for $c \cdot g \in \sqrt{H}$ tells us that g follows from $h_1, \dots, h_n$ whenever c does not vanish (this is because $c \cdot g$ vanishes on V). In Exercise 14, we will give an algorithm for finding c.

=task2= Over $\mathbb{C}$, we can think of Corollary 9 in terms of the variety $V_{\mathbb{C}} = \mathbf{V}(h_1, \dots, h_n) \subseteq \mathbb{C}^{m+n}$ as follows. Decomposing $V_{\mathbb{C}}$ as in (11), let $V_{\mathbb{C}}' \subseteq V_{\mathbb{C}}$ be the union of those components where the u_i are algebraically independent. Then Exercise 15 will use the Nullstellensatz to prove that

$$\exists c \neq 0 \text{ in } \mathbb{R}[u_1, \ldots, u_m] \text{ with } c \cdot g \in \sqrt{\langle h_1, \ldots, h_n \rangle} \subseteq \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_u]$$
$$\iff g \in \mathbf{I}\left(V'_{\mathbb{C}}\right) \subseteq \mathbb{C}[u_1, \ldots, u_m, x_1, \ldots, x_n].$$

Thus, the conditions of Corollary 9 mean that g "follows generically over $\mathbb{C}$ " from the hypotheses $h_1, \ldots, h_n$.

=task3= This interpretation points out what is perhaps the main limitation of the Gröbner basis method in geometric theorem proving: it can only prove theorems where the conclusions follow generically over $\mathbb{C}$, even though we are only interested in what happens over $\mathbb{R}$. In particular, there are theorems which are true over $\mathbb{R}$ but not over $\mathbb{C}$. Our methods will fail for such theorems.

When using Corollary 9 , it is often unnecessary to consider the radical of $\widetilde{H}$. In many cases, the first power of the conclusion is in $\widetilde{H}$ already. So most theorem proving programs in effect use an ideal membership algorithm first to test if $g \in \widetilde{H}$, and only go on to the radical membership test if that initial step fails.

=method 3= To illustrate this, we continue with the Circle Theorem of Apollonius from Example 3 . Our hypotheses are the eight polynomials h_i from (5)-(7). We begin by computing a Gröbner basis (using lex order) for the ideal $\widetilde{H}$, which yields

$$\begin{aligned}
f_1 &= x_1 - u_1/2 \\
f_2 &= x_2 - u_2/2 \\
f_3 &= x_3 - u_1/2 \\
f_4 &= x_4 - u_2/2 \\
f_5 &= x_5 - \frac{u_1 u_2^2}{u_1^2 + u_2^2} \\
f_6 &= x_6 - \frac{u_1^2 u_2}{u_1^2 + u_2^2} \\
f_7 &= x_7 - u_1/4 \\
f_8 &= x_8 - u_2/4
\end{aligned}$$

We leave it as an exercise to show that the conclusion (8) reduces to zero on division by this Gröbner basis. Thus, g itself is in $\widetilde{H}$, which shows that g follows generically from $h_1, \ldots, h_8$. Note that we must have either $u_1 \neq 0$ or $u_2 \neq 0$ in order to solve for x_5 and x_6.

=dcases=

The equations $u_1 = 0$ and $u_2 = 0$ describe degenerate right "triangles" in which the three vertices are not distinct, so we certainly wish to rule these cases out.

It is interesting to note, however, that if either u_1 or u_2 is nonzero, the conclusion is still true. For instance, if $u_1 \neq 0$ but $u_2 = 0$, then the vertices C and A coincide. From (5) and (6), the midpoints M_1 and M_3 coincide, M_2 coincides with A, and H coincides with A as well. As a result, there *is* a circle (infinitely many of them in fact) containing M_1, M_2, M_3, and H in this degenerate case.

6 Wu's Method

This method, introduced by the Chinese mathematician Wu Wen-Tsün, was developed before the Gröbner basis method. It is also more commonly used than the Gröbner basis method in practice because it is usually more efficient.

The idea here is to follow the one-variable polynomial division algorithm as closely as possible, and we obtain a result known as the pseudodivision algorithm.

§6.1 A Summary of Wu's Method

Step 1. Conversion of a geometry statement into the corresponding polynomial equations.

Step 2. Triangulation of the hypothesis polynomials using pseudo division. In the complete method, decomposition or check of the irreducibility is needed in this step

Step 3. Successive pseudo division to compute the final remainder R_0. If $R_0 = 0$, then by the remainder formula we can infer the conclusion by adding the subsidiary or nondegenerate conditions available after triangulation. If the final remainder is not zero, then the decomposition or check of irreducibility is needed to make further conclusions. Wu's method is complete for geometric statements involving equality only in metric geometry, not in Euclidean geometry. However, under certain natural conditions, it is also a decision procedure for Euclidean geometry.

Step 4. Analysis of nondegenerate conditions $I_1 \neq 0, \dots, I_r \neq 0$. Some of the conditions $I_i = 0$ can be considered degenerate cases and can be translated back into their geometric forms by the program for at least a large class of geometry statements. The other conditions $I_i \neq 0$ are not necessarily connected with nondegeneracy and have been proved unnecessary for $g = 0$ to be valid if the triangular form $f_1, \dots, f_r$ is irreducible.

We recall the situation studied in §4, in which the hypotheses and conclusion of a theorem in Euclidean plane geometry are translated into a system of polynomials in variables $u_1, \dots, u_m, x_1, \dots, x_n$, with $h_1, \dots, h_n$ representing the hypotheses and g giving the conclusion.

As in equation (11) of §4, we can group the irreducible components of the variety $V = \mathbf{V}(h_1, \dots, h_n) \subseteq \mathbb{R}^{m+n}$ as

$$V = V' \cup U,$$

where V' is the union of the components on which the u_i are algebraically independent. Our goal is to prove that g vanishes on V'.

The elementary version of Wu's method that we will discuss is tailored for the case where V' is irreducible. We note, however, that Wu's method can be extended to the more general reducible case also.

The main algebraic tool needed (Ritt's decomposition algorithm based on characteristic sets for prime ideals) would lead us too far afield, though, so we will not discuss it.

Note that, in practice, we usually do not know in advance whether V' is irreducible or not. Thus, reliable "theoremprovers" based on Wu's method should include these more general techniques too.

Our simplified version of Wu's method uses the pseudodivision algorithm in two ways in the process of determining whether the equation $g = 0$ follows from $h_j = 0$.

Step 1 of Wu's method uses pseudodivision to reduce the hypotheses to a system of polynomials f_j that are in triangular form in the variables $x_1, \ldots, x_n$. In other words, we seek

$$\begin{aligned} f_1 &= f_1(u_1, \ldots, u_m, x_1) \\ f_2 &= f_2(u_1, \ldots, u_m, x_1, x_2) \\ &\vdots \\ f_n &= f_n(u_1, \ldots, u_m, x_1, \ldots, x_n) \end{aligned}$$

such that $\mathbf{V}(f_1, \ldots, f_n)$ again contains the irreducible variety V', on which the u_i are algebraically independent.

Step 2 of Wu's method uses successive pseudodivision of the conclusion g with respect to each of the variables x_j to determine whether $g \in \mathbf{I}(V')$. We compute

$$\begin{aligned} R_{n-1} &= \mathrm{Rem}(g, f_n, x_n), \\ R_{n-2} &= \mathrm{Rem}(R_{n-1}, f_{n-1}, x_{n-1}), \\ &\vdots \\ R_1 &= \mathrm{Rem}(R_2, f_2, x_2), \\ R_0 &= \mathrm{Rem}(R_1, f_1, x_1). \end{aligned}$$

Then $R_0 = 0$ implies that g follows from the hypotheses h_j under an additional condition, to be made precise in Theorem 4.

To explain how Wu's method works, we need to explain each of these steps, beginning with the reduction to triangular form.

In practice, this reduction can almost always be accomplished using a procedure very similar to Gaussian elimination for systems of linear equations. We will not state any general theorems concerning our procedure, however, because there are some exceptional cases in which it might fail.

A completely general procedure for accomplishing this kind of reduction may be found in CHOU (1988).

The elementary version is performed as follows. We work one variable at a time, beginning with x_n.

1.1. Among the h_j, find all the polynomials containing the variable x_n. Call the set of such polynomials S. (If there are no such polynomials, the translation of our geometric theorem is most likely incorrect since it would allow x_n to be arbitrary.)

1.2. If there is only one polynomial in S, then we can rename the polynomials, making that one polynomial f_n', and our system of polynomials will have the form

$$f_1' = f_1'(u_1, \ldots, u_m, x_1, \ldots, x_{n-1}),$$

(4)

$$f'_{n-1} = f'_{n-1}(u_1, \dots, u_m, x_1, \dots, x_{n-1}),$$
$$f'_n = f'_n(u_1, \dots, u_m, x_1, \dots, x_n).$$

1.3. If there is more than one polynomial in S, but some element of S has degree 1 in x_n, then we can take f'_n as that polynomial and replace all the other hypotheses in S by their pseudoremainders on division by f'_n with respect to x_n.

One of these pseudoremainders could conceivably be zero, but this would mean that f'_n would divide $d^s h$, where h is one of the other hypothesis polynomials and $d = LC(f'_n, x_n)$. This is unlikely since V' is assumed to be irreducible. We obtain a system in the form (4) again. By part (ii) of Proposition 1 , all the f'_j are in the ideal generated by the h_j.

1.4. If there are several polynomials in S, but none has degree 1 in x_n, then pick $a, b \in S$ where $0 < \deg(b, x_n) \leq \deg(a, x_n)$ and compute the pseudoremainder $r = \mathrm{Rem}(a, b, x_n)$. Then:

a. If $\deg(r, x_n) \geq 1$, then replace S by $(S \backslash \{a\}) \cup \{r\}$ (leaving the hypotheses not in S unchanged) and repeat either 1.4 (if $\deg(r, x_n) \geq 2$) or 1.3 (if $\deg(r, x_n) = 1$)

b. If $\deg(r, x_n) = 0$, then replace S by $S \backslash \{a\}$ (adding r to the hypotheses not in S) and repeat either 1.4 (if the new S has ≥ 2 elements) or 1.2 (if the new S has only one element).

Eventually we are reduced to a system of polynomials of the form (4) again. Since the degree in x_n are reduced each time we compute a pseudoremainder, we will eventually remove the x_n terms from all but one of our polynomials. Moreover, by part (ii) of Proposition 1 , each of the resulting polynomials is contained in the ideal generated by the h_j. Again, it is conceivable that we could obtain a zero pseudoremainder at some stage here. This would usually, but not always, imply reducibility, so it is unlikely. We then apply the same process to the polynomials $f'_1, \dots, f'_{n-1}$ in (4) to remove the x_{n-1} terms from all but one polynomial. Continuing in this way, we will eventually arrive at a system of equations in triangular form as in (2) above.

Once we have the triangular equations, we can relate them to the original hypotheses as follows.

Proposition 2. Suppose that $f_1 = \cdots = f_n = 0$ are the triangular equations obtained from $h_1 = \cdots = h_n = 0$ by the above reduction algorithm. Then

$$V' \subseteq V = \mathbf{V}(h_1, \dots, h_n) \subseteq \mathbf{V}(f_1, \dots, f_n)$$

Proof. As we noted above, all the f_j are contained in the ideal generated by the h_j. Thus, $\langle f_1, \dots, f_n \rangle \subseteq \langle h_1, \dots, h_n \rangle$ and hence, $V = \mathbf{V}(h_1, \dots, h_n) \subseteq \mathbf{V}(f_1, \dots, f_n)$ follows immediately. Since $V' \subseteq V$, we are done.

Example 3. To illustrate the operation of this triangulation procedure, we will apply it to the hypotheses of the Circle Theorem of Apollonius from §4. Referring back to (5)-(7) of §4, we have

$$
\begin{aligned}
h_1 &= 2x_1 - u_1 \\
h_2 &= 2x_2 - u_2 \\
h_3 &= 2x_3 - u_1 \\
h_4 &= 2x_4 - u_2 \\
h_5 &= u_2x_5 + u_1x_6 - u_1u_2, \\
h_6 &= u_1x_5 - u_2x_6 \\
h_7 &= x_1^2 - x_2^2 - 2x_1x_7 + 2x_2x_8 \\
h_8 &= x_1^2 - 2x_1x_7 - x_3^2 + 2x_3x_7 - x_4^2 + 2x_4x_8.
\end{aligned}
$$

Note that this system is very nearly in triangular form in the x_j. In fact, this is often true, especially in the cases where each step of constructing the geometric configuration involves adding one new point.

In Step 1 of the triangulation procedure, we see that h_7, h_8 are the only polynomials in our set containing x_8. Even better, h_8 has degree 1 in x_8. Hence, we proceed as in 1.3 of the triangulation procedure, making $f_8 = h_8$, and replacing h_7 by

$$
\begin{aligned}
f_7 &= \operatorname{Rem}(h_7, h_8, x_8) \\
&= (2x_1x_2 - 2x_2x_3 - 2x_1x_4)\, x_7 - x_1^2x_2 + x_2x_3^2 + x_1^2x_4 - x_2^2x_4 + x_2x_4^2.
\end{aligned}
$$

As this example indicates, we often ignore numerical constants when computing remainders. Only f_7 contains x_7, so nothing further needs to be done there. Both h_6 and h_5 contain x_6, but we are in the situation of 1.3 in the procedure again. We make $f_6 = h_6$ and replace h_5 by

$$
f_5 = \operatorname{Rem}(h_5, h_6, x_6) = \left(u_1^2 + u_2^2\right) x_5 - u_1u_2^2.
$$

The remaining four polynomials are in triangular form already, so we take $f_i = h_i$ for $i = 1, 2, 3, 4$.

The key step in Wu's method is the successive pseudodivision operation given in equation (3) computing the final remainder R_0. The usefulness of this operation is indicated by the following theorem.

Theorem 4. Consider the set of hypotheses and the conclusion for a geometric theorem. Let R_0 be the final remainder computed by the successive pseudodivision of g as in (3), using the system of polynomials $f_1, \dots, f_n$ in triangular form (2). Let d_j be the leading coefficient of f_j as a polynomial in x_j (so d_j is a polynomial in $u_1, \dots, u_m$ and $x_1, \dots, x_{j-1}$). Then:

(i) There are nonnegative integers $s_1, \dots, s_n$ and polynomials $A_1, \dots, A_n$ in the ring $\mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$ such that

$$
d_1^{s_1} \cdots d_n^{s_n} g = A_1f_1 + \cdots + A_nf_n + R_0.
$$

(ii) If R_0 is the zero polynomial, then g is zero at every point of $V' \setminus \mathbf{V}(d_1d_2 \cdots d_n) \subseteq \mathbb{R}^{m+n}$

Proof. Part (i) follows by applying Proposition 1 repeatedly. Pseudodividing g by f_n with respect to x_n, we have

$$R_{n-1} = d_n^{s_n} g - q_n f_n.$$

Hence, when we pseudodivide again with respect to x_{n-1} :

$$\begin{aligned} R_{n-2} &= d_{n-1}^{s_{n-1}} \left(d_n^{s_n} g - q_n f_n \right) - q_{n-1} f_{n-1} \\ &= d_{n-1}^{s_{n-1}} d_n^{s_n} g - q_{n-1} f_{n-1} - d_{n-1}^{s_{n-1}} q_n f_n. \end{aligned}$$

Continuing in the same way, we will eventually obtain an expression of the form

$$R_0 = d_1^{s_1} \cdots d_n^{s_n} g - (A_1 f_1 + \cdots + A_n f_n),$$

which is what we wanted to show.

(ii) By the result of part (i), if $R_0 = 0$, then at every point of the variety $W = \mathbf{V}(f_1, \ldots, f_n)$, either g or one of the $d_j^{s_j}$ is zero. By Proposition 2 , the variety V' is contained in W, so the same is true on V'. The assertion follows.

Even though they are not always polynomial relations in the u_i alone, the equations $d_j = 0$, where d_j is the leading coefficient of f_j, can often be interpreted as loci defining degenerate special cases of our geometric configuration.

Example 3 (continued). For instance, let us complete the application of Wu's method to the Circle Theorem of Apollonius. Our goal is to show that

$$g = (x_5 - x_7)^2 + (x_6 - x_8)^2 - (x_1 - x_7)^2 - x_8^2 = 0$$

By Theorem 4, Wu's method confirms that the Circle Theorem is valid when none of the leading coefficients of the f_j is zero. The nontrivial conditions here are

$$\begin{aligned} d_5 &= u_1^2 + u_2^2 \neq 0, \\ d_6 &= u_2 \neq 0, \\ d_7 &= 2x_1x_2 - 2x_2x_3 - 2x_1x_4 \neq 0, \\ d_8 &= 2x_4 \neq 0. \end{aligned}$$

The second condition in this list is $u_2 \neq 0$, which says that the vertices A and C of the right triangle $\triangle ABC$ are distinct recall we chose coordinates so that $A = (0, 0)$ and $C = (0, u_2)$ in Example 3 of §4]. This also implies the first condition since u_1 and u_2 are real. The condition $2x_4 \neq 0$ is equivalent to $u_2 \neq 0$ by the hypothesis $h_4 = 0$. Finally, $d_7 \neq 0$ says that the vertices of the triangle are distinct (see Exercise 5). From this analysis, we see that the Circle Theorem actually follows generically from its hypotheses as in §4.

The elementary version of Wu's method only gives $g = 0$ under the side conditions $d_j \neq 0$. In particular, note that in a case where V' is reducible, it is entirely conceivable that one of the d_j could vanish on an entire component of V'. If this happened, there would be no conclusion concerning the validity of the theorem for geometric configurations corresponding to points in that component.

Indeed, a much stronger version of Theorem 4 is known when the subvariety V' for a given set of hypotheses is irreducible. With the extra algebraic tools we have omitted (Ritt's decomposition algorithm), it can be proved that there are special triangular form sets of f_j (called characteristic sets) with the property that $R_0 = 0$ is a necessary and sufficient condition for g to lie in $\mathbf{I}(V')$. In particular, it is never the case that one of the leading coefficients of the f_j is identically zero on V' so that $R_0 = 0$ implies that g must vanish on all of V'.

We refer the interested reader to CHOU (1988) for the details. Other treatments of characteristic sets and the Wu-Ritt algorithm can be found in MISHRA (1993) and WANG (2001).

Finally, we will briefly compare Wu's method with the method based on Gröbner bases introduced in §4. These two methods apply to exactly the same class of geometric theorems and they usually yield equivalent results. Both make essential use of a division algorithm to determine whether a polynomial is in a given ideal or not. However, as we can guess from the triangulation procedure described above, the basic version of Wu's method at least is likely to be much quicker on a given problem. The reason is that simply triangulating a set of polynomials usually requires much less effort than computing a Gröbner basis for the ideal they generate, or for the ideal $\widetilde{H} = \langle h_1, \ldots, h_n, 1 - yg \rangle$. This pattern is especially pronounced when the original polynomials themselves are nearly in triangular form, which is often the case for the hypotheses of a geometric theorem. In a sense, this superiority of Wu's method is only natural since Gröbner bases contain much more information than triangular form sets. Note that we have not claimed anywhere that the triangular form set of polynomials even generates the same ideal as the hypotheses in either $\mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$ or $\mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n]$. In fact, this is not true in general (Exercise 4). Wu's method is an example of a technique tailored to solve a particular problem. Such techniques can often outperform general techniques (such as computing Gröbner bases) that do many other things besides.

§6.2 Triangulation of hypothesis

§6.3 Succesive Pseudodivision

==========example==========

The next step is to triangulate h_1, h_2, h_3, h_4 so that each polynomial introduces only one new (dependent) variable x_i. Thus h_1, h_2, h_3, h_4 are not in triangular form because h_3 introduces two new variables, x_3 and x_4, at the same time. We can use a simple elimination procedure to obtain a triangular form: let $f_1 = h_1, f_2 = h_2$, $f_3 = \operatorname{prem}(h_4, h_3, x_4), {}^3 f_4 = h_4$. Then we have a triangular form:

$$
\begin{aligned}
f_1 &= u_1 x_1 - u_1 u_3 = 0 \\
f_2 &= u_3 x_2 - (u_2 - u_1)\, x_1 = 0 \\
f_3 &= (u_3 x_2 - u_2 x_1 - u_1 u_3)\, x_3 + u_1 u_3 x_1 = 0 \\
f_4 &= u_3 x_4 - u_2 x_3 = 0
\end{aligned}
$$

Now we do successive pseudo divisions:

$$
\begin{aligned}
R_3 &= \operatorname{prem}(g, f_4, x_4) = \left(2u_3^2 + 2u_2^2\right) x_3 - u_3^3 - u_2^2 u_3 \\
R_2 &= \operatorname{prem}(R_3, f_3, x_3) = \left(-u_3^4 - u_2^2 u_3^2\right) x_2 + \left(\left(u_2 - 2u_1\right) u_3^3 + \left(u_2^3 - 2u_1 u_2^2\right) u_3\right) x_1 + \\
& u_1 u_3^4 + u_1 u_2^2 u_3^2 \\
R_1 &= \operatorname{prem}(R_2, f_2, x_2) = \left(-u_1 u_3^4 - u_1 u_2^2 u_3^2\right) x_1 + u_1 u_3^5 + u_1 u_2^2 u_3^3 \\
R_0 &= \operatorname{prem}(R_1, f_1, x_1) = 0.
\end{aligned}
$$

Because the final remainder R_0 is zero, the theorem follows from appropriate subsidiary conditions. To see this, let us recall the simple and important remainder formula (see Section 4) for successive pscudo divisions of g with respect to a triangular form $f_1, \ldots, f_r$:

$$
I_1^{s_1} \cdots I_r^{s_r} g = Q_1 f_1 + \ldots + Q_r f_r + R_0
$$

where I_k are the leading coefficients of f_k in x_k. Since $R_0 = 0, g = 0$ under $I_k \neq 0 (k = 1, \ldots, r)$. The subsidiary conditions $I_k \neq 0$ are usually connected with nondegeneracy and are also called nondegenerate conditions.

$$
\begin{aligned}
I_1 &= u_1 \neq 0 \\
I_2 &= u_3 \neq 0 \\
I_3 &= u_3 x_2 - u_2 x_1 - u_1 u_3 \neq 0 \\
I_4 &= u_3 \neq 0.
\end{aligned}
$$

The conditions $u_1 \neq 0$ and $u_3 \neq 0$ mean that A, B, and C are not collinear. The condition $u_3 x_2 - u_2 x_1 - u_1 u_3 \neq 0$ means that line AC and line BD should have a normal intersection.

7 Bibliography

Summary

```
@book{book:{91131740},
    title =     {Ideals, varieties, and algorithms: an introduction to computational a
    author =    {David A. Cox, John Little, Donal O'Shea},
    publisher = {Springer},
    isbn =      {9780387356518; 0387356517; 0387356509; 9780387356501},
    year =      {2007},
    series =    {Undergraduate texts in mathematics},
    edition =   {3rd ed},
    url =       {libgen.li/file.php?md5=fe87b6a947782875c3cbfa6daeb5d2f6}}

    @book{book:{92003093},
    title =     {Elimination Methods},
    author =    {Dr. Dongming Wang (auth.)},
    publisher = {Springer},
    isbn =      {9783211832417; 3211832416; 9783709162026; 3709162025},
    year =      {2001},
    series =    {Texts & Monographs in Symbolic Computation  },
    edition =   {1},
    url =       {libgen.li/file.php?md5=103632b3805fb1f73fa841471f6855f5}}

    @book{book:{92021850},
    title =     {Mechanical Theorem Proving in Geometries: Basic Principles},
    author =    {Dr. Wen-tsün Wu (auth.)},
    publisher = {Springer},
    isbn =      {9783211825068; 3211825061; 9783709166390; 370916639X},
    year =      {1994},
    series =    {Texts & Monographs in Symbolic Computation  },
    edition =   {1},
    url =       {libgen.li/file.php?md5=859b35b11a26233491e6a222f420e32c}}

    @book{book:{92208942},
    title =     {Mechanical Geometry Theorem Proving},
    author =    {Shang-Ching Chou},
    publisher = {Springer},
    isbn =      {9027726507; 9789027726506},
    year =      {1987},
    series =    {Mathematics and Its Applications (closed)},
    edition =   {1987},
    url =       {libgen.li/file.php?md5=ace7869b74008b2924dde9081dbfb836}}
```