AUTOMATED GEOMETRY THEOREM PROVING

İBRAHİM ESER

FEBRUARY 2011

AUTOMATED GEOMETRY THEOREM PROVING

by

İBRAHİM ESER

THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
THE ABANT İZZET BAYSAL UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE
OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF MATHEMATIC

FEBRUARY 2011

Approval of the Graduate School of Natural and Applied Sciences

Prof. Nihat Çelebi
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science

Assoc. Prof. Harun Karslı
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assis. Prof. Erol Yılmaz
Supervisor

Examining Committee Members

1. Assoc. Prof. Soner Durmuş ……
2. Assis. Prof. Ali Öztürk ……
3. Assis. Prof. Erol Yılmaz ……

ABSTRACT

AUTOMATED GEOMETRY THEOREM PROVING

Eser, İbrahim

Master of Science, Department of science

Supervisor: Assis. Prof. Erol Yılmaz

Feburary, 2011, 52 pages

The aim of this thesis is to show how the polynomial rings and computational methods designed for them can be help in proving plane geometry theorems. The Gröbner basis techniqes are used to do this. The automatic geometry theorem discovering are also covered. The both subject are illustrated with several examples.

ÖZET

OTOMATİK GEOMETRİK TEOREM

İSPATLAMA

Eser, İbrahim

Yüksek lisans, Matematik bölümü

Tez danışmanı: Yard. Doç. Dr. Erol Yılmaz

Şubat, 2011, 52 sayfa

Bu tezin amaçı polinom halkalarının ve onlar için dizan edilen hesaplama metodlarının düzlem geometrisi teoremlerinin ispatlanmasında nasıl yararlı olacağını göstermektir. Bu yapılırken Gröbner taban teknikleri kullanılmıştır. Geometri teoremlerinin otomatik keşfi de ayrıca tartışılmıştır. Her iki konuda örneklerle açıklanmaya çalışılmıştır.

To My Wife

ACKNOWLEDGMENTS

I express gratefullness to Assis. Prof. Erol Yılmaz for his guidance during my education life. Especially I would like to offer my sincere thanks to him for his guidance in preparing thesis process. To my Şehriban, I offer sincere thanks for her patiance while I was working on my thesies and my last speacial thanks to my little daughter Zehra for letting me work on computer.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

The automated proving of geometric theorems is a particularly successful area of computer algebra. Extensive and detailed studies (Chou.,1988 ; Dolzman., et al 1998; Kapur., 1986 ;Kutzler., and Stifter., 1988; Wu., 1984) have produced automatic proofs for a large number of classical and modern geometric theorems.

The general approach follows Descartes' idea of algebraization of geometry by introducing a Cartesian coordinate system the considered geometric configurations are described via polynomial equations. Then one try to prove the geometric statement by verifying its algebraic translation for all real values. In general this fails because in the algebraic translation of the geometric statements one forgets to enter non-degeneracy conditions in the hypothesis. Such conditions would, e.g., guarantee that certain points do not coincide or that a certain triangle does not collapse to a line. Adding non-degeneracy conditions by hand is extremly tedious. In automated proving therefore such conditions must be generated automatially. Because of these set of variables of the system split into two disjoint parts: parameters which can be chooen arbitrarly and remaining depented variables whose values are determined by the values of parameters and the geometric configuration.

The existing methods for geometric theorem proving can be divided into two clases : The Wu-Ritt method using characteristic sets, (Chou .,1988 ;Wu 1984) and Gröbner Basis Techniques (Kapur.,1986; Kutzler ., and Stifter.,

1986). In this thesis, we use Gröbner Basis Techniques. Gröbner Basis have been introduced by Buchberger in his dissertation for computing in linear spaces of polynomial rings modulo zero dimensional ideals. They have meanwhile turned out as an extremely powerful tool in algorithmic algebra.

Although there are several possible approaches to automated geometry theorem proving, the main steps are always similar. The first step is algebraic formulation of geometric statements. The second step is that using some decion procedure to determine the validity od the theorem. The final step is to search for extra conditions if the theorem, as it was formulated originally, is false.

The thesis is designed as follows: Chapter 2 involves main concepts and algorithms of computer algebra. In Chapter 3, automatic theorem proving with Gröbner bases in geometry is discussed. In Chapter 4, theorem discovering using minimal canonical comprehensive Gröbner bases is investigated. In all computations the computer algebra system SINGULAR is used (Gruel .et al 2010).

CHAPTER 2

FUNDAMENTAL CONCEPTS

2.1 Polynomial Ideals and Their Varieties

Definition 2.1 A polynomial in variables $x_1, x_2, \cdots, x_n$ with coeffients in a field k is a formal expression of the form

$f = \sum_{\propto \in S} a_\alpha x^\alpha,$ (2.1)

Where S is a finite subset of $\mathbb{N}_0^n$, $a_\alpha \in k$, and for $\alpha = (\alpha_1, \alpha_2, \cdots \alpha_n)$, x^α denotes the $monomial$ $x_1^{\alpha_1}, x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. In most cases of interest k will be $\mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$. The product $a_\alpha x^\alpha$ is called a $term$ of the polynomial f. The set of all polynomials in the variables $x_1, \cdots, x_n$ with coefficients in k is denoted by $k[x_1, \cdots, x_n]$. With the natural and well-known addition and Multiplication, $k[x_1, \cdots, x_n]$ is a commutative ring. The full degree of a monomial x^α is the number $|\alpha| = \alpha_1 + \cdots + \alpha_n$. The $full\ degree$ of a term $a_\alpha x^\alpha$ is the full degree of the monomial x^α. The $full\ degree$ of a polynomial f as in (2.1) denoted by deg(f), is the maximum of $|\alpha|$ among all monomials (with nonzero coefficients a_α), of course, of f

Definition 2.2 Let $f_1, \cdots, f_m$ be polynomials in a polynomial ring $k[x_1, \cdots, x_n]$. Set :

$$(f_1, \cdots, f_m) = \{h_1 f_1 + \cdots + h_m f_m | h_i \in k[x_1, \cdots, x_n]\}$$

Then $(f_1, \cdots, f_m)$ is an ideal, called the ideal generated by $f_1, \cdots, f_m$.

Lemma 2.3 The set $(f_1, \cdots, f_m)$ in $Definition\ 2.2$ is really is an $ideal$

Definition 2.4 Let k be a field and $n \in \mathbb{Z}_{>0}$. We define the $n - dimensional\ affine\ space\ over\ k$ to be the set:

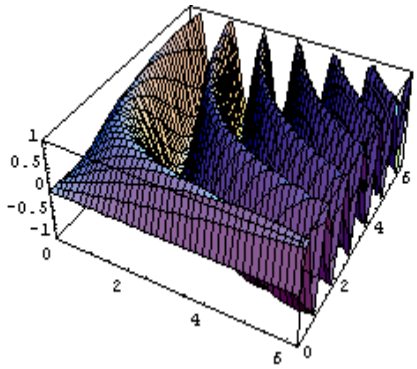
$$k^n = \{(a_1, \cdots, a_n) | a_i \in k\}$$

Remark 2.5 It is also to denote the affine space k^n by A_k^n (or simply A^n) . We call one – dimensional affine space $k^1 = k$ the $affine\ line$, and two – dimensional affine space k^2 the affine plane .

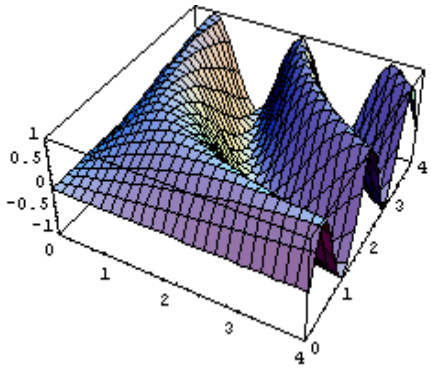
Definition 2.6 let k be a field , and let $f_1, \cdots, f_m \in k[x_1, \cdots, x_n]$ be a finite number of polynomials . Then

$V(f_1, \cdots, f_m)$: = $\{(a_1, \cdots, a_n) | \in k^n | f_i(a_1, \cdots, a_n) = 0$ for all $1 \leq i \leq m\}$

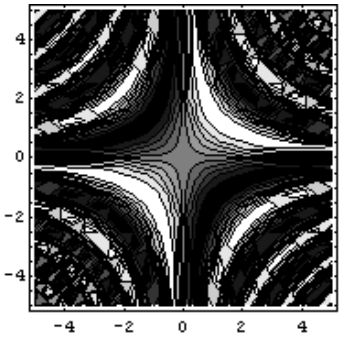
is called the $affine\ variety\ defined\ by\ f_1, \cdots, f_m$

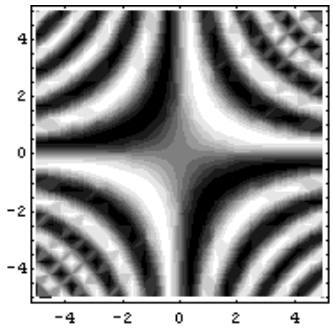


Graph of $\sin(xy)$



Graph of $\sin(xy)$





Proposition 2.7 Let $f_1, \cdots, f_s$ and $g_1, \cdots, g_m$ be $bases\ of\ an\ ideal\ I \subseteq k[x_1, \cdots, x_n]$, that is , $I = \langle f_1, \cdots, f_s \rangle = \langle g_1, \cdots, g_m \rangle$. Then

$V(f_1, \cdots, f_s) = V(g_1, \cdots, g_m)$

Definition 2.8 Let $V \subset k^n$ be an affine variety.The $ideal\ of\ the\ variety\ V$ is the set

$I(V) = \{ f \in k[x_1, \cdots, x_n] : \mathrm{f}(a_1, \cdots, a_n) = 0$ for all $(a_1, \cdots, a_n) \in V \}$

Proposition 2.9 Let $f_1, \cdots, f_s$ be elements of $k[x_1, \cdots, x_n]$. Then the set inclusion $\langle f_1, \cdots, f_s \rangle \subset I(V(f_1, \cdots, f_s))$ always holds , but could be strict.

Proof: Let $f \in \langle f_1, \cdots, f_s \rangle$. Then there exist $h_1, \cdots, h_s \in k[x_1, \cdots, x_n]$ such that $f = h_1 f_1 + \cdots + h_s f_s$. Since $f_1, \cdots, f_s$ all vanish on $V(f_1, \cdots, f_s)$, so does f , so $f \in I(V(f_1, \cdots, f_s))$. The demonstration that the inclusion can be strict is given by Example 2.10

Example 2.10 Let $V = \{(0,0)\} \subset \mathbb{R}^2$. Then $I(V)$ is the set all polynomials in two variables without constant term. We will express $V\ as\ V(f_1, f_2)$ in two different ways. Choosing $f_1 = x$ and $f_2 = y$, $V = V(f_1, f_2)$ and $I = \langle x, y \rangle$ is the same ideal as $I(V)$. Choosing $f_1 = x^2$ and $f_2 = y$, $V = V(f_1, f_2)$, but $J = \langle x^2, y \rangle$ is the set of elements of $\mathbb{R}[x, y]$, every term of which contains x^2 or

y ; hence $J \not\subset I(V)$. Note that both I and J have the property that V is precisely the set of common zeros of all their elements.

Proposition 2.11 Let V and W be affine varieties in k^n. Then

1. $V \subset W\ if\ and\ only\ if\ I(W) \subset I(V)$.

2. $V = W\ if\ and\ only\ if\ I(W) = I(V)$

2.2 Division Algorithm and Gröbner Basis

In polynomial rings of several variables , we want to perform a division and examining a remainder. Matters are more complicated , however .In particular , ideals are not generated by just one polynomial , so we have to formulate a procedure for dividing a polynomial f by a set F of polynomials , and although there is a way to generalize the Division to do

this for elements of $k[x_1, \cdots, x_n]$, a complication aries in that the remainder under the division is not necessarily unique.

Definition 2.12: A monomial order $>$ on $k[x_1, \cdots, x_n]$ is total order on monomials satisfying the following:

1. **Multiplicative Property** if $x^\alpha > x^\beta$ then $x^\alpha x^\gamma > x^\beta x^\gamma$ (for any α, β, γ).

2. Well Ordering An arbitrary set of monomials

$$\{x^\alpha\}\ \alpha \in A$$

has least element .

The stipulation that $>$ be a total order means that any monomials $x^\alpha\ and\ x^\beta$ are comparable in the order , i.e. , either $x^\alpha > x^\beta$, $x^\alpha < x^\beta$ or $x^\alpha = x^\beta$.

Remark 2.13: The well-ordering condition is equivalent to the requirement that any decreasing sequence of monomials.

$$x^{\alpha(1)} > x^{\alpha(2)} > x^{\alpha(3)} > \cdots$$

eventually terminates.We give some basic example of monomial orders:

Example 2.14:(Pure Lexicographic Order):

This is basically the order on words in a dictionary .We have $x^\alpha >_{lex} x^\beta$ if the first nonzero entry of $(\alpha_1 - \beta_1, \alpha_2 - \beta_2, \cdots, \alpha_n - \beta_n)$ is positive.for example , we hav

$$x_1 >_{lex} x_2^3 >_{lex} x_2x_3 >_{lex} x_3^{100}$$

Definition 2.15 : *Fix a monomial order on $k[x_1, \cdots, x_n]$ and consider a nonzero polynomia*

$f = \sum_\alpha c_\alpha x^\alpha$.

The leading monomial of f (denoted LM(f)) is the largest monomial x^α such that $c_\alpha \neq 0$. The leading term of f (denoted LT(f)) is the corresponding term $c_\alpha x^\alpha$ For instance , in lexicographic order the polynomial

$$f = 5x_1x_2 + 7x_2^5 + 19x_3^{17}$$

has leading monomial $LM(f) = x_1x_2$ and leading term $LT(f) = 5x_1x_2$ .One nonintutive aspect of lexicographic order is that the degree of the terms is not paramount : the smallest degree term could be the leading one . We can remedy this easily :

Example 2.16:(Graded lexicographic order):

$$x^\alpha >_{grlex} x^\beta \text{ if } \deg(x^\alpha) > \deg(x^\beta)$$

or

$\deg(x^\alpha) = \deg(x^\beta)$ and $x^\alpha >_{lex} x^\beta$

Example 2.17:(Graded reverse lexicographic order):

$x^\alpha >_{grelex} x^\beta$ if $\deg(x^\alpha) > \deg(x^\beta)$ or $\deg(x^\alpha) = \deg(x^\beta)$ and the last nonzero

$\alpha_j - \beta_j < 0$. Note that $x_1x_2x_3 >_{grlex} x_1x_3^2$ but $x_1x_2x_5 <_{grlex} x_1x_3^2$. Generally ,this is more efficient than lexicographic order.

Proposition 2.18: *(Division Algorithm in $k[x_1, \cdots, x_n]$) .Let $>$ be a monomial order on $\mathbb{Z}_{\geq 0}^n$ and let $f_1 \cdots f_s \in k[x_1, \cdots, x_n]$. Then every $f \in k[x_1, \cdots, x_n]$ can be written in the form:*

$$f = a_1f_1 + \cdots + a_sf_s + r,$$

where $a_i, r \in k[x_1, \cdots, x_n]$ and either $r = 0$ or none of the monomials in r are divisible by any $LT(f_1), \cdots, LT(f_s)$. If $a_if_i \neq 0$ then $multideg(f) \geq multideg(a_if_i)$. We call r a remainder of f on division by $f_1, \ldots, f_s$.

Example 2.19 : In $\mathbb{Q}[x, y]$ with $x > y$ and the term order lex , we apply algorithm to divide $f = x^2y + xy^3 + xy^2$ by the polynomials $f_1 = xy + 1$ and $f_2 = y^2 + 1$,ordered f_1 then f_2.

First pass:

$LM(f_1) \mid LM(h)$ but $LM(f_2) \nmid LM(h)$

f_1 is leas

$$u_1 = 0 + \frac{x^2y}{xy} = x$$

$$h = (x^2y + xy^3 + xy^2) - x(xy + 1) = xy^3 + xy^2 - x$$

Second pass :

$LM(f_1) \mid LM(h)$ and $LM(f_2) \mid LM(h)$

f_1 is leas

$$u_1 = x + \frac{xy^3}{xy} = x + y^2$$

$$h = (xy^3 + xy^2 - x) - y^2(xy + 1) = xy^2 - x - y^2$$

Third pass:

$LM(f_1) \mid LM(h)$ and $LM(f_2) \mid LM(h)$

f_1 is leas

$$u_1 = x + y^2 + \frac{xy^2}{xy} = x + y^2 + y$$

$$h = (xy^2 - x - y^2) - y(xy + 1) = -x - y^2 - y$$

Fourth pass:

$LM(f_1) \nmid LM(h)$ and $LM(f_2) \nmid LM(h)$

$$r = 0 + (-x) = -x$$

$$h = -x - y^2 - y - (-x) = -y^2 - y$$

Fifth pass:

$LM(f_1) \nmid LM(h)$ and $LM(f_2) \mid LM(h)$

f_2 is leas

$$u_2 = 0 + \frac{-y^2}{y} = -1$$

$$h = (-y^2 - y) - (-1)(y^2 + 1) = -y + 1$$

Sixth pass :

$LM(f_1) \nmid LM(h)$ and $LM(f_2) \nmid LM(h)$

$r = -x + (-y) = -x - y$

$h = (-y + 1) - (-y) = 1$

Seventh pass:

$LM(f_1) \nmid LM(h)$ and $LM(f_2) \nmid LM(h)$

$r = -x - y + 1$

$h = 1 - 1 = 0$

If we change the order of the polynomials in Example 2.19 , dividing first by f_2 and then by f_1 then the quotient and remainder change to $\{xy + x, x - 1\}$ and $-2x + 1$, respectively .Thus we see that unlike the situation in the one-variable case , the quotient and remainder are not unique . They depend on the ordering of the polynomials in the set of divisors as well as on the term order chosen for the polynomial ring . But what is even worse from the point of wiev of solving the Ideal Membership problem is that , as the following examples show , it is even possible that , keeping the term order fixed , there exist an element of the ideal generated by the divisors whose remainder can be zero under one ordering of the divisors and different from zero under another or even different from zero no matter how the divisors are ordered.

Example 2.20: In the ring $\mathbb{R}[x, y]$, fix the lexicographic term with $x > y$ and consider the polynomial $f = x^2y + xy + 2x + 2$, when we use the multivariable Division Algorithm to reduce the polynomial f modulo the ordered set

$\{f_1 = x^2 - 1, f_2 = xy + 2\}$, we obtain

$$f = yf_1 + f_2 + (2x + y)$$

Since the corresponding remainder ,$2x + y$, is different from zero ,we might conclude that f is not the ideal $< f_1, f_2 >$. If , however we change the order of the divisors so that f_2 is first , we obtai

$$f = yf_1 + f_2 + (2x + y)$$

Since the corresponding remainder ,$2x + y$, is different from zero, we might conclude that f is not in the ideal $< f_1, f_2 >$. If ,however ,we change the order of the divisors so that f_2 is first, we obtai

$$f = 0f_1 + (x + 1)f_2 + 0 = (x + 1)f_2,$$

So that $f \in < f_1, f_2 >$. After all.

If , for any ideal I, we had a basis B with the special property that the leading term of every polynomial in I was divisible by the leading term of some element of B, then the Multivariable Division Algorithm would provide a answer to the Ideal Membership Problem:a polynomial f is in the ideal I if and only if the remainder of f upon division by elements of B, in any order ,is zero .This the idea behind the concept of a Gröbner basis of an ideal , and we use this special property as the defining characteristic of a Gröbner basis.

Definition 2.21: Let $I \subset k[x_1, \cdots, x_n]$ *be a non-zero ideal.By* $LT(I)$ *we mean the set of leading term of all polynomials in* I

$$LT(I) \coloneqq \{LT(f) \mid f \in I\}.$$

By $(LT(I))$ we mean the ideal generated by the set $LT(I)$.

Remark 2.22: Given a finitely generated ideal $I = (f_1, \cdots, f_n)$, it is tempting to believe that the ideal generated by the leading terms of the f_i is equal to $(LT(I))$; i.e. that $(LT(f_1), \cdots, LT(f_n)) = (LT(I))$. Rather crucially for what 's to follow , this is not generally the case.

For example , consider the ideal $I = (x + y, x) \subset k[x, y]$. Using lexicographic order , we have that $LT(x + y) = LT(x) = x$. Hence $(LT(x + y), LT(x)) = (x)$. Clearly $y \in I$, and so $y = LT(y) \in (LT(I)) \neq (x)$

Definition 2.23: Let $I \subset k[x_1, \cdots, x_n]$ *be an ideal ,and fix a monomial order .A finite subset* $\{g_1, \cdots, g_s\} \subset I$ *such taht* $(LT(g_1), \cdots, LT(g_s)) = (LT(I))$ *is said to be a Gröbner Basis of* I .

Theorem 2.24 : *(Hilbert Basis Theorem).Every ideal* $I \subset k[x_1, \cdots, x_n]$ *is finitely generated.*

Proposition 2.25: *Let* $G = \{g_1, \cdots, g_s\}$ *be a Gröbner basis for a non-zero ideal*

$I \subset k[x_1, \cdots, x_n]$ *. Let* $f \in k[x_1, \cdots, x_n]$ *. Then there exist a unique* $r \in k[x_1, \cdots, x_n]$ *such that:*

(1) No term of r *is divisible by one of* $LT(g_1, \cdots, LT(g_s))$;

(2) There exist a $g \in I$ *such that* $f = g + r$.

In particular , r is the remainder on division of f by G no matter the order in which we list the elements of G when running the division algorithm .

Corollary 2.26: Let $I \subset k[x_1, \cdots, x_n]$ be a on-zero ideal ,and G be a Gröbner basis for I .Let $f \in k[x_1, \cdots, x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero.

Definition 2.27: *Let* $x^\alpha, x^\beta \in k[x_1, \cdots, x_n]$ *be two monomials.If* $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$ *and* $\beta = (\beta_1, \cdots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$, $\gamma = (c_1, \cdots, c_n) \in \mathbb{Z}_{\geq 0}^n$ *be such that* $c_i = \max\{a_i, b_i\}$ *for* $i = 1, \cdots, n$ *. We call* x^γ *the least common multiple of* x^α *and* x^β, and write $x^\gamma = lcm\{x^\alpha, x^\beta\}$

Definition 2.28: *Let* $f, g \in k[x_1, \cdots, x_n]$ *be non-zero polynomials and fix a monomial order . The S-polynomial of* f *and* g *is*

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

Where $x^\gamma = lcm\{LM(f), LM(g)\}$.

Example2.29: The purpose of the S-polynomial is to cancel out the leading terms of the two polynomials f *and* g . For example if $f = z - x^2 z$ and $g = xy - 1$ then using lexicographic order we have $LT(f) = -x^2 z$ and $LT(g) = xy$. We obtain $lcm\{LM(f), LM(g)\} = x^2 yz$,

And so:

$$S(f,g) = \frac{x^2yz}{-x^2z}f - \frac{x^2yz}{xy}g$$

$$= (-y)(z - x^2z) - (xz)(xy - 1)$$

$$= -yz + x^2yz - x^2yz + xz$$

$$= xz - yz$$

Theorem 2.30 : (**Buchberger's Criterion**) *Fix a monomial order and polynomials* $f_1, \cdots, f_r$ *in* $k[x_1, \cdots, x_n]$. *The following are equivalent:*

1. $f_1, \cdots, f_r$ *form a Gröbner Basis for* $< f_1, \cdots, f_r >$.

2. *Each S-polynomial* $S(f_i, f_j)$ *gives remainder zero an application of the the division algorithm .*

Corollary 2.31: (Buchberger's Algorithm) Fix a monomial order and polynomials $f_1, \cdots, f_r \in k[x_1, \cdots, x_n]$. *A Gröbner basis for* $< f_1, \cdots, f_r >$ *is obtained by iterating the following procedure :*

For each i, j apply the division algorithm to the S-polynomials to get expressions

$$S(f_i, f_j) = \sum_{l=1}^{r} h(ij)_l f_1 + r(ij), \quad LM(S(f_i, f_j)) \geq LM(h(ij)_l f_1)$$

Where each $LM(r(ij))$ is not divisible by any of the $LM(f_1)$. If all the remainders $r(ij) = 0$ then $f_1, \cdots, f_r$ are already a Gröbner basis . Otherwise let $f_{r+1}, \cdots, f_{r+s}$ denote the nonzero $r(ij)$ and adjoin these to get a new set generators

$$\{f_1, \cdots, f_r, f_{r+1}, \cdots, f_{r+s}\} .$$

Continue these process until the Buchberger's criterion is satisfied .

Example.2.32:

We compute a Gröbner basis of

$$I =< f_1, f_2 >=< x_1^2 - x_2, x_1^3 - x_3 >$$

With respect to lexicographic order .

The first S-polynomial is

$$S(f_1, f_2) = x_1 f_1 - f_2 = x_1(x_1^2 - x_2) - (x_1^3 - x_3) = -x_1 x_2 + x_3 \text{ ;}$$

Its leading term is not contained in

$$< LM(f_1), LM(f_2) >=< x_1^2 >.$$

Therefore, we must add

$$f_3 = x_1 x_2 - x_3$$

to the Gröbner Basis .

The next step S-polynomial is

$$S(f_1, f_3) = x_2 f_1 - x_1 f_3 = x_1 x_3 - x_2^2 \text{ ;}$$

Its leading term is not contained in

$$< LM(f_1), LM(f_2), LM(f_3) >=< x_1^2, x_1 x_2 > .$$

Therefore we must add

$$f_4 = x_1 x_3 - x_2^2$$

to the Gröbner basis.

We have :

$$S(f_2, f_3) = x_2 f_2 - x_1^2 f_3 = x_1^2 x_3 - x_2 x_3 = x_3 f_1,$$

$$S(f_1, f_4) = x_3 f_1 - x_1 f_4 = x_1 x_2^2 - x_2 x_3 = x_2 f_3,$$

$$S(f_2, f_4) = x_3 f_2 - x_1^2 f_4 = x_1^2 x_2^2 - x_3^2 = (x_1 x_2 + x_3) f_3,$$

$$S(f_3, f_4) = x_3 f_3 - x_2 f_4 = x_2^3 - x_3^2.$$

The last has leading term not contained in

$$< LM(f_1), \cdots LM(f_4) >=< x_1^2, x_1x_2, x_1x_3 >$$

Therefore ,we must ad

$$f_5 = x_2^3 - x_3^2.$$

To the Gröbner basis

Adding this new generator necessitates computing the S-polynomials involving (f_5):

$$S(f_1, f_5) = x_2^3 f_1 - x_1^2 f_5 = -x_2^4 + x_1^2 x_3^2 = (x_1x_3 + x_2^2)f_4,$$

$$S(f_2, f_5) = x_2^3 f_2 - x_1^3 f_5 = -x_2^3 x_3 + x_1^3 x_3^2 = x_1^2 x_3 f_3 + x_2 x_3 f_1$$

$$S(f_3, f_5) = x_2^2 f_3 - x_1 f_5 = -x_2^2 x_3 + x_1 x_3^2 = x_3 f_4$$

$$S(f_4, f_5) = x_2^3 f_4 - x_1 x_3 f_5 = x_1 x_3^3 + x_2^5 = x_3^2 f_4 - x_2^2 f_5$$

Buchberger's criterion implies $\{f_1, f_2, f_3, f_4, f_5\}$ is a Gröbner basis.

Remark 2.33: Note tha

$$LM(f_2) \in < LM(f_1), LM(f_3), LM(f_4), LM(f_5) >$$

So that f_2 is redundent and can be removed from the minimal Gröbner basis . The division algorithm applied to the S-polynomials for f_1, f_3, f_4, f_5 gives the following relations.

$$0 = S(f_1, f_3) - f_4 = x_2 f_1 - x_1 f_3 - f_4,$$

$$0 = S(f_1, f_4) - x_2 f_3 = x_3 f_1 - x_1 f_4 - x_2 f_3,$$

$$0 = S(f_1, f_5) - (x_1x_3 + x_2^2)f_4 = x_2^3 f_1 - x_1^2 f_5 - (x_1x_3 + x_2^2)f_4,$$

$$0 = S(f_3, f_4) - x_3 f_4 = x_2^2 f_3 - x_1 f_5 - x_3 f_4,$$

$$0 = S(f_4, f_5) - x_3^2 f_4 + x_2^2 f_5 = (x_2^3 - x_3^2)f_4 - (x_1x_3 - x_2^2)f_5,$$

2.3 The Nullstellensatz

For an arbitrary ideal $\mathrm{I} \subset \mathrm{k}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$. We have an inclusion $\mathrm{I} \subset \mathrm{I}(\mathrm{V}(\mathrm{I}))$, but not necessarily equality.(as illustrated by taking $\mathrm{I} = (\mathrm{x}^2)$). In this section we shall see when $\mathrm{I} = \mathrm{I}(\mathrm{V}(\mathrm{I}))$. We shall introduce the notion of a *radical ideal* from Commutative Algebra and understand the connection with Algebraic Geometry . Before we can proceed , we need another result due to Hilbert : the Nullstellensatz .

Theorem2.34 :(The Weak* Nullstellensatz*).Let $I \subset \mathbb{C}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$ *bean ideal such that* $V(I) = \emptyset$. *Then* $I \subset \mathbb{C}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$.

Theorem2.35: (The Nullstellensatz). *Let* $I \subset \mathbb{C}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$ *be an ideal. A polynomial* $f \in \mathrm{I}(\mathrm{V}(\mathrm{I}))$ *if and only if there exists an integer* $m \geq 1$ *suc that* $f^m \in I$.

Example2.36: Let $\mathrm{I} = (\mathrm{x}^2 + \mathrm{y}^2 - 1, \mathrm{x} - 1) \subset \mathbb{C}[\mathrm{x}, \mathrm{y}]$. A Gröbner basis for I is $\{\mathrm{y}^2, \mathrm{x} - 1\}$,

Hence $\mathrm{V}(\mathrm{x}^2 + \mathrm{y}^2 - 1, \mathrm{x} - 1) = \mathrm{V}(\mathrm{y}^2, \mathrm{x} - 1)$.we proved eailier $\mathrm{y} \in \mathrm{I}(\mathrm{V}(\mathrm{I}))$ even though $y \notin I$. In fact it is easy to see that $\mathrm{I}(\mathrm{V}(\mathrm{I})) = (\mathrm{y}, \mathrm{x} - 1)$.

Definition 2.37: Let $I \subset k[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$ be an ideal.We call I radical if $f^m \in I$ for some integer $m \geq 1$ implies that $f \in I$.

Definition2.38: $I \subset k[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$ be an ideal.The *radical of* I is given by:

$$\sqrt{I} := \{f \in k[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}] f^m \in \mathrm{I} \text{ for some integer } m \geq 1\}$$

Example 2.40: The ideal $(x^2 - y^2, x)$ is not radical,since it contains y^2 but not

y . We have that $\sqrt{(x^2 - y^2, x)} = (x, y)$.

Thereom2.41 : (***The Strong*** **Nullstellensatz)**. Let $I \subset \mathbb{C}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$ be an ideal . Then $\mathrm{I}(\mathrm{V}(\mathrm{I})) = \sqrt{\mathrm{I}}$

Remark 2.42: Affine varieties and radical ideals are in one-to-one correspondence . We can think of $V(I)$ as a map from the set of radical ideals to the set of affine varieties , and $I(V)$ as a map in the opposite direction.In other words ,

$$V: \{radical\ ideals\ in\ \mathbb{C}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]\} \to \{affine\ varieties\ in\ \mathbb{C}^n\},$$

$$I: \{affine\ varieties\ in\ \mathbb{C}^n\} \to \{radical\ ideals\ in\ \mathbb{C}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]\}.$$

If I is a radical ideal,then $\mathrm{I}(\mathrm{V}(\mathrm{I})) = \sqrt{\mathrm{I}} = \mathrm{I}$. If V is an afine variety then $\mathrm{V}(\mathrm{I}(\mathrm{V}))$. Hence I and V are inverses of each other . It is a difficult computational problem to compute the radical of a given ideal . The following theorem gives a method for checking whether or not a given polynomial belongs to the radical of a given ideal .

Theorem 2.43 : Let k be an arbitrary field and $I = < f_1, \cdots f_s >$ be an ideal in $k[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$. Then $f \in \sqrt{I}$ if and only if

$$1 \in < f_1, \cdots f_s, 1 - wf > \subset k[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}, \mathrm{w}].$$

2.4 Elimination theory

Definition2.44 : Let I be an ideal in $k[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$ (with the implict ordering variables $x_1 > \cdots > x_n$) and fix $\ell \in \{0,1, \cdots, n-1\}$.The ℓth Elimination ideal of I is the ideal $I_\ell = I \cap k[x_{\ell+1}, \cdots, x_n]$. Any point $(a_{\ell+1}, \cdots, a_n) \in V(I_\ell)$ is called a partial solution of the system$\{f = 0 : f \in I\}$ The following theorem is most helpful in investigating solutions of systems of polynomial equations . We will use it several times in later sections .

Theorem2.45: (Elimination theorem) Fix the lexicographic term order on the ring $k[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$ with $x_1 > \cdots > x_n$ and let G be a Gröbner basis for an ideal I of $k[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$ with respect to this order.Then for every

ℓ, $0 \leq \ell \leq n-1$, the set

$$G_\ell := G \cap k[x_{\ell+1}, \cdots, x_n].$$

is a Gröbner Basis for the ℓth elimination ideal of I_ℓ

The next theorem gives a sufficient condition for the possibility of extending a partial solution of a polynomial system to the complete solution.

Theorem2.46: (Extension Theorem) *Let* $I =< f_1, \cdots, f_s >$ *be a nonzero ideal*

in the ring $\mathbb{C}[x_1, \cdots, x_n]$ *and let* I_1 *be the first elimination ideal for* I*. Write the generators of* I *in the form* $f_j = g_j(x_2, \cdots, x_n){x_1}^{N_j} + \tilde{g}_i$*, where* $N_j \in \mathbb{N}_0, g_j \in \mathbb{C}[x_2, \cdots, x_n]$ *are nonzero polynomials and* $\tilde{g}_i$ *are the sum of terms of* f_j *of degree less than* N_j *in* x_1*. Consider a partial solution* $(a_2, \cdots, a_n) \in V(I_1)$*. If* $(a_2, \cdots, a_n) \notin V(g_1, \cdots, g_s)$*, then there exists* a_1 *such that* $(a_1, a_2, \cdots, a_n) \in V(I_1)$

Theorem2.47: (Closure theorem) *Let* $V = V(f_1, \cdots, f_s)$ *be an affine variety in* $\mathbb{C}^n$ *and let* I_ℓ *be the* ℓth *elimination ideal fort he ideal* $I =< f_1, \cdots, f_s >$*. Then*

1. *V(*I_ℓ*) is the smallest affine variety containing* $\pi_\ell(V) \subset \mathbb{C}^{n-\ell}$*, and*
2. *If* $V \neq \emptyset$*, then there is an affine variety* $W \subsetneq V(I_\ell)$ *such that* $V(I_\ell) \backslash W \subset \pi_\ell(V)$.

2.5 Operations in ideals and varieties

Now we turn to question of the relationship between operations on ideals and the corresponding effects on the affine varieties that they define, and between properties of ideals and properties of the corresponding varieties.Hence let I and J be two ideals in $\mathrm{k}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$. The intersection of I and J is their set-theoretic intersectio

$$I \cap J = \{f \in \mathrm{k}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}] : f \in I \text{ and } f \in J\},$$

And the sum of I and J is

$$I + J := \{f + g : f \in I \text{ and } g \in J\},$$

Definition2.48: Let I and J be ideals in $\mathrm{k}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$. Their ideal quotient $I:J$ is the idea

$$I:J = \{f \in \mathrm{k}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}] : fg \in I \text{ for all } g \in J\}.$$

Theorem 2.49: *if I and J are ideals in $\mathrm{k}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$, then*

1. $V(I + J) = V(I) \cap V(J)$ *and*
2. $V(I \cap J) = V(I) \cup V(J)$.

Suppose $I \text{ and } J$ are ideals in $\mathrm{k}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$ for which we have explicit finite bases ,say $I =< f_1, \cdots, f_u >$ and $J =< g_1, \cdots, g_v >$. We wish to use these bases to obtain bases for $I + J$, $I \cap J$, and $I:J$. For $I + J$ the answer is simple , $I + J =< f_1, \cdots, f_u, g_1, \cdots, g_v >$. To solve the problem for $I \cap J$ we need the expression for $I \cap J$ in terms of an ideal in a polynomial ring with one additional indeterminate as given by the following proposition . The equality in the proposition is proved by treating its constitutents only assets .

Proposition 2.50 : If $I =< f_1, \cdots, f_u >$ and $J =< g_1, \cdots, g_v >$ are ideals in $\mathrm{k}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$ then ,

$$I \cap J =< tf_1, \cdots, tf_u, (1-t)g_1, \cdots, (1-t)g_v > \cap \mathrm{k}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}] .$$

If we order the variables $t > x_1 > \cdots > x_n$, then in the language of definition elimination ideal , the proposition 2.44 says that $I \cap J$ is the first elimination ideal of the ideal in $\mathrm{k}[\mathrm{t}, \mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$ given by

$$K =< tf_1, \cdots, tf_u, (1-t)g_1, \cdots, (1-t)g_v >$$

The proposition and the Elimination theorem together thus yield the following algorithm : The polynomials involving only x_i's in the Gröbner basis

of K with respect to lex order $t > x_1 > \cdots > x_n$ gives a generating set for $I \cap J$. To obtain a basis for ideal $I{:}J$ from bases for I and J we will need two more results.

Proposition 2.51: Suppose I is an ideal in $\mathrm{k}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$ and g is a nonzero element of $\mathrm{k}[\mathrm{x}_1, \cdots, \mathrm{x}_\mathrm{n}]$ .If $\{h_1, \cdots, h_s\}$ is a basis for $I \cap < g >$, then $\{{}^{h_1}/_{g}, \cdots, {}^{h_s}/_{g}\}$ is a basis for $I{:} < g >$.

Proposition 2.52: *Suppose that* I *and* $J_1, \cdots, J_m$ *are ideals in* $k[x_1, \cdots, x_n]$. *Then*

$$I{:}(\sum_{s=1}^{m} J_s) = \bigcap_{s=1}^{m} (I{:}J_s).$$

Using the fact that any ideal $J = < g_1, \cdots, g_s >$ can be represented as the sum of the principal ideals of its generators , $J = < g_1 > + \cdots < g_s >$, using proposition 2.50 , and the algorithm for intersection of ideals ,we obtain a method for computing generators of the ideal quotient. We can compute $I{:}J$ by computing , for $i = 1, \cdots, s$ $I \cap < g_i >$, divide generators by g_i getting $I{:} < g_i >$ and compute the intersection

$$\cap_i \, (I{:} < g_i >)$$

Definition 2.53: Let $I_1 , I_2 \subset k[x_1, \cdots, x_n]$. We consider the quotient of I, by powers of I_2

$$I_1{:}\, I_2^0 \subset I_1 : I_2^1 \subset I_1 : I_2^2 \subset I_1 : I_2^3 \subset \cdots \subset k[x_1, \cdots, x_n]$$

Since $k[x_1, \cdots, x_n]$ is Neotherion , there exist an s such that $I_1{:}\, I_2^s = I_1 : I_2^{s+i}$ for all $i \geq 0$. Such an s satisfies.

$$I_1 : I_2^\infty \coloneqq \bigcup_{i \geq 0} I_1 : I_2^s = I_1 : I_2^s,$$

and $I_1 : I_2^s$ is called the saturation of I_1 with respect to I_2 . The minimal such s is called the saturation exponent.

Given ideals I_1 , $I_2 \subset k[x_1, \cdots, x_n]$ generators for $I_1 : I_2^{\infty}$ can be computed as Follows .

Set ideals $I^{(0)} = I_1$ and compute succesively $I^{(j+1)} = I^{(j)} : I_2$, $j \geq 0$. In each step check whether $I^{(j+1)} \subset I^{(j)}$.

If s is the first j when this happens , then $I^{(s)} = I_1 : I_2^{\infty}$ and s is the saturation exponent .

CHAPTER 3

Automated Geometric Theorem Proving

3.1 Introduction

Theorems of elementary geometry have always been considered an important test case for the scope of methods in automatic theorem proving. Such problems have stimulated a variety of algebraic techniques for their solution, in particular the Wu-Ritt method and Gröbner Basis techniques have proved to be quite successful. Such methods are of interest to reseachers both in artificial intelegence and in geometric modelling because they have been used in the design of programs that can prove or disprove conjectured relationships or theorems about plane geometric objects . Their common basis can be characterized as follows:

1. A translation of the geometrical assertion ***G*** via a suitably positioned coordinate system into an algebraic statement ***A*** involving multivariate polynomial equations.

2. The use of the corresponding algebraic method itself in an attempt to prove ***A*** as a statement about complex numbers . Since ***A*** is generally a universally quantfied assertion , the validity of ***A*** over the complex numbers entails the validity of A over the reals and thus an automatic proof of the

original geometrical assertion. If, in contrast, ***A*** turns out to be false over the complex numbers, no decision on the validity of ***G*** can be made. Hence first of all we consider the translate geometric statements into polynomials

3.2 Geometric Statements and Polynomials

Both Wu's method and the method of Gröbner bases depend on the construction of a particular type of polynomial to represent a given geometric figure. As an example, consider the following figure of parallel lines. Suppose that the distance between point $\boldsymbol{A}$ and point $\boldsymbol{C}$, and the distance between point $\boldsymbol{B}$ and point $\boldsymbol{D}$ is given. A traditional analytic approach might be to start by assigning variable Cartesian coordinates to each of the points $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$ and $\boldsymbol{D}$, and this is what Wu's method and the Gröbner bases method require.

For our proofs to be correct in a general case, the coordinates must not be directly specified; however, the coordinates given cannot be too general. Start with the point $\boldsymbol{A}$. Since $\boldsymbol{A}$ is the first point chosen, any coordinates will do. Next, choose coordinates for $\boldsymbol{B}$. We have the freedom to choose any point other than (u_1, u_2). Then the coordinates of point $\boldsymbol{C}$ and point D are depens on u_1, u_2, u_3 and u_4. We will show them ith x_i's.

In general, allow for dependencies amongst the points we will denote variables for which we are free to choose any value as u_j , $j = 1, \cdots, n$ and those variables which are dependent on others as x_i, $i = 1, \cdots, m$.

Example 3.1:(Parellel lines)

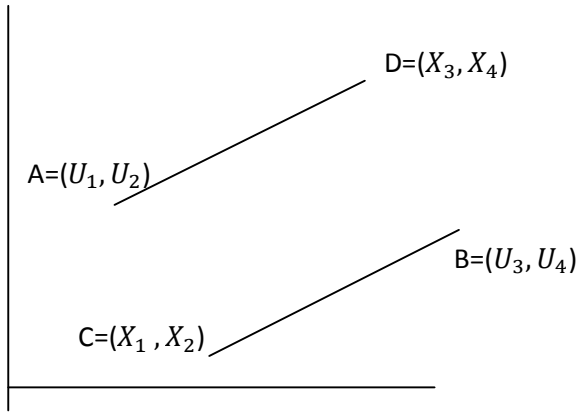


Figure 3.1 Parellel lines

Example 3.2:(Perpendicular lines)

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

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

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

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

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

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

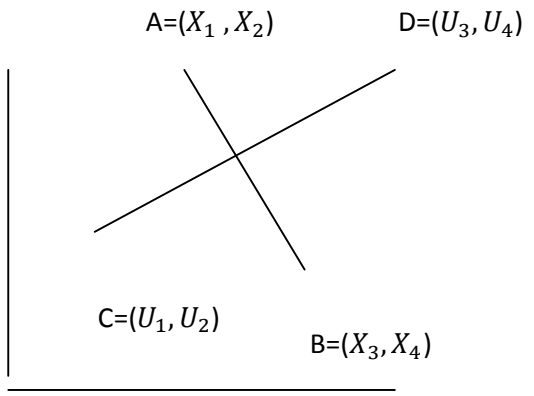


Figure 3.2 Perpendicular Line

Example 3.3:(Collinear)

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

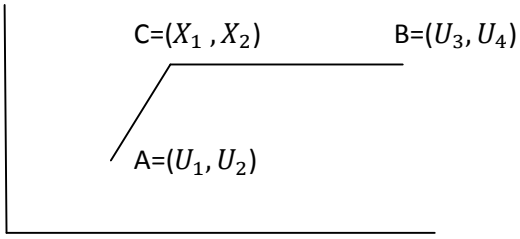


Figure 3.3 Collinear

Using the slope Formula , we hav

$$\overline{AC} = \overline{BC}$$

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

h=($X_2 - U_2)(X_1 - U_3) - (X_1 - U_3)(X_1 - U_1) = 0$

Example 3.4:(Circle)

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

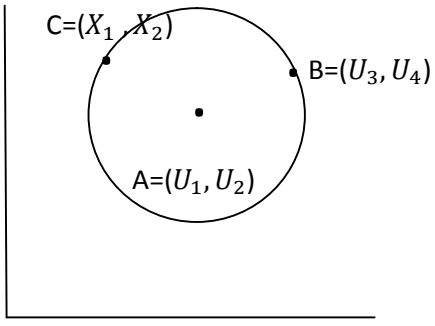


Figure 3.4

We can write

$$|AC|^2 = |AB|^2$$

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

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

Example 3.5:(Midpoint)

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

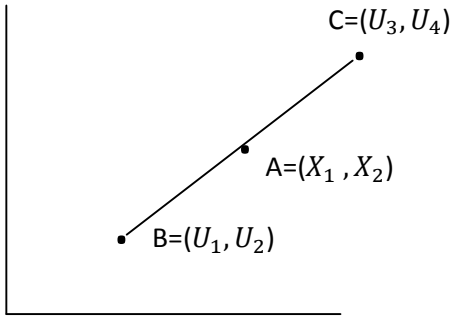


Figure 3.5 Mid-poin

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

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

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

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

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

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

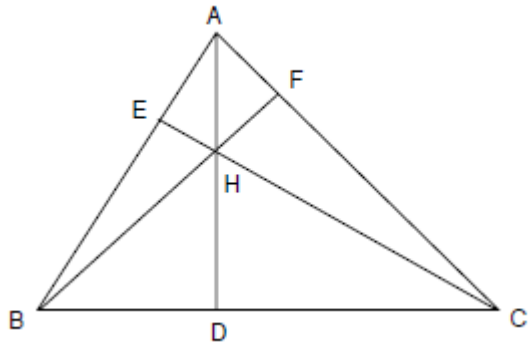
Then

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

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

3.3 Algebraic Formulation of Geometric Theorems

A Standard geometry theorem states that the altitudes of a triangle ABC all meet in a single point, *H*, called the orthocente



The basic idea is to place the figure above in the coordinate plane and then to interpret the hypotheses of the theorem as statements in coordinate, rather than Euclidean, geometry. So we begin by coordinatizing the parallelogram by placing the point *B* at the origin, so $B = (0,0)$. Now we can say that the point C corresponds to $(u_1, 0)$. Next we construct the altitudes. For example, if we let D be the point given by $(u_2, 0)$ then the line segment AD is the altitude from *A*(u_2, u_3) . The other two altitudes require more work.

Let $E = (x_1, x_2)$ and $F = (x_3, x_4)$ be points such that BF, CE are the altitudes from B, C respectively. We must have *B, E,A* and *C,F,A* collinear. Algebraic translation of these hypotheses are

$$x_2u_2 - x_1u_3 = 0$$

$$x_4(u_2 - u_1) - u_3(x_3 - u_1) = 0$$

CE must be perpendecilar to AB and BF must also be perpendecular to AC. Hence

$$x_2u_3 + u_2(x_1 - u_1) = 0$$

$$x_4u_3 + x_3(u_2 - u_1) = 0$$

Labeling the polynomials as h_1,h_2,h_3 and h_4.Now,we want to conclude that all three altitudes meet at a single point. Hence we construct the following two additional points: G*:(* u_2 *,*x_5 *)* and H*=(*u_2 *,*x_6*)* .We intend that G should be the intersection of $\overline{AD}$ and $\overline{CE}$ while H should be the intersection of the line segments $\overline{AD}$ and $\overline{BF}$.Hence we need the additional hypotheses that $G, E, C,$ and H, B, F are collinear yielding the following two equations:

$(x_2 - x_5)(x_1 - u_1) - x_2(x_1 - u_2) = 0$

$$x_6x_3 - x_4u_2 = 0$$

which we call h_5 and h_6.Finally, our conclusion becomes the assertion that the points *G* and *H* are in fact identical.Hence , we get the equation.

$$x_5 - x_6 = 0$$

Call this polynomial

We have seen that we can translate a geometric theorem into a system of algebraic equations in the ring *k*[$u_1, \ldots, u_d, x_1, \ldots, x_r$]: $h_1, \ldots, h_r$ (the hypotheses) and *g* (the conclusion). In what sense then does our conclusion, *g*, follow from the hypotheses , $h_1, \ldots, h_r$? The basic idea is that we want *g* to be satisfied by every point that satisfies $h_1, \ldots, h_r$. In other words, we

want every point in the variety defined by the hypotheses to satisfy *g*. Hence we start with the following definition.

Definition 3.6: The conclusion *g* follows strictly from the hypotheses $h_1,\cdots,h_r$ if $g \in I(V) \subset k[u_1,\ldots,u_d,x_1,\ldots,x_r]$ where $V=V(h_1,\ldots,h_r)$

We will briefly investigate a straightforward attempt to use this definition. In general, the field *k* may not be algebraically closed, so we cannot rely on computing $I(V)$ directly using Hilbert's Nullstellensatz . We can, however, use the following test.

Proposition 3.7 : if $g \in \sqrt{(h_1,\ldots,h_r)}$ *then g follows strictly from* $h_1,\ldots,h_r$.

Proof : the hypothesis $g \in \sqrt{(h_1,\ldots,h_r)}$, means that $g^\infty \in < h_1,\ldots,h_r >$ for some *s*. Hence $g^\infty = \sum_{t=1}^{n} A_t h_t$ where $A_t \in k[u_1,\ldots,u_d,x_1,\ldots,x_r]$ .Then g^∞ must vanish whenever the h_1 vanish , and hence *g* does as well. This test is useful because we have an algorithm for determining if $g \in \sqrt{(h_1,\ldots,h_r)}$

Let us recall our example. We are attempting to show that the conclusion follows from our hypotheses . Hence we have the following hypotheses:

$h_1 : x_2u_2 - x_1u_3$

$h_2 : x_4(u_2 - u_1) - u_3(x_3 - u_1)$

$h_3 : x_2u_3 + u_2(x_1 - u_1)$

$h_4 : x_4u_3 + x_3(u_2 - u_1)$

$h_5 : (x_2 - x_5)(x_1 - u_1) - x_2(x_1 - u_2)$

$h_6 : x_6x_3 - x_4u_2$

The conclusion we are interested in is

$g : x_5 - x_6$

We try to develop a method that can be used to check the trueness of the theorem , excluding the degeneracy cases. Since our to intent is that u_i should be essantially independent, we introduce the following terminolog

Definition 3.8: Let W be an irreducible affine variety in the affine space $\mathbb{R}^{m+n}$ with coordinates $u_1, \cdots, u_m, x_1, \cdots x_n$.We say $u_1, \cdots, u_m$ are algebraically independent on W if I(W)∩ $\mathbb{R}[u_1, \cdots, u_n]$={0}, it is well known that any affine variety V can be written as a finite union of irreducible varieties .Afte regrouping the irreducible decomposition, the affine variety can be written a V=$W_1 \cup \cdots \cup W_p \cup U_1 \cup \cdots \cup U_q$,

Where $u_1, \cdots, u_m$ are algebraically independent on the components W_i and are not algebraically independent on the compenents U_j .To ensure that the variables $u_1, \cdots, u_m$ are in fact arbitrary ,we should consider only the subvariety

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

Definition 3.9:*The conclusion g follows generically from hypothesis* $h_1, \cdots, h_n$

if $g \in I(V') \subset \mathbb{R}[u_1, \cdots, u_m, x_1, \cdots x_n]$ *where* $V' \subseteq \mathbb{R}^{n+m}$ *is the union of the compenents of the variety* $V = V(h_1, \cdots, h_n)$ *on which* $u_1, \cdots, u_m$ *are algebraically independent* Finding the decomposition of a variety into irreducible components is not always easy, so we would like to determine whether or not a conclusion follow generically from the hypotheses without knowing irreducible decomposition of the variety of hypotheses.

Proposition 3.10 : *A conclusion g follows generically from the hypothese* $h_1, \cdots, h_n$ *whenever there is some nonzero polynomial. c(* $u_1, \cdots, u_m$*)*∈ $\mathbb{R}[u_1, \cdots, u_m]$ *such tha*

c.g $\epsilon\sqrt{< h_1, \cdots, h_n >} \subseteq \mathbb{R}[u_1, \cdots, u_m, x_1, \cdots x_n]$

Proof : *Let* V_j *be one of the irreducible components of* V'*. Since*

c.g $\epsilon \sqrt{< h_1, \cdots, h_n >}$ *c.g vanishes on* $V(h_1, \cdots, h_n)$ *and so on* V_j*. Thus ,*

c.g $\epsilon I(V_j)$*. But* V_j *being irreducible implies that* $I(V_j)$ *is a prime ideal*

$I(V_j) \cap \mathbb{R}[u_1, \cdots, u_m]$*={0} implies that* $c \notin I(V_j)$*.Therefore* $g \in I(V_j)$ *. Since* V_j *is*

an arbitrary component of V'*,* $g \in I(V')$*.*

Proposition 3.11:*There is a nonzero polynomial* $c \in \mathbb{R}[u_1, \cdots, u_m]$*. Such that* $c.g \in \sqrt{< h_1, \cdots, h_n >}$ *if and only if* $g \in \sqrt{\tilde{I}}$ *where*

$$\tilde{I} =< h_1, \cdots, h_n > \subseteq R(u_1, \cdots, u_m)[x_1, \cdots x_n]$$

Proof: We know that $c.g\, \epsilon\sqrt{< h_1, \cdots, h_n >}$ if and only if

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

for some $A_j \in \mathbb{R}[u_1, \cdots, u_m, x_1, \cdots x_n]$ and for some positive integer k . Hence

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

Hence $g\epsilon\sqrt{< h_1, \cdots, h_n >} \subseteq \mathbb{R}(u_1, \cdots, u_m)[x_1, \cdots x_n]$

Conversely, if $g \in \sqrt{\tilde{I}}$, then

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

Where $B_j \epsilon \mathbb{R}(u_1, \cdots, u_m)[x_1, \cdots x_n]$ if we find a least common denominotor c for all terms in all the B_j

And multiply both sides by c^k ,we obtain

$$(c.g)^k = \sum_{j=1}^{n} B_j' h_j$$

Where $B_j^{'} \epsilon \mathbb{R}[u_1, \cdots, u_m, x_1, \cdots x_n]$ and c depends only on the $u_1, \cdots, u_m$,and $c.g\ \epsilon\sqrt{< h_1, \cdots, h_n >}$ As a result of above proposition ,we get the method for proving a geometric statement.

Corollary 3.12:*Let $h_1, \cdots, h_n$ be hypotheses and g be the conclusion of a geometric statement .The conclusion g follows generically from the hypotheses $h_1, \cdots, h_n$ if and only if {1} is the reduced Grobner* Basis of the ideal

$$< h_1, \cdots, h_n, 1 - yg > \subseteq R(u_1, \cdots, u_m, y)$$

Note that the Grobner Basis method does not tell us what the degenerate cases are .The information about these cases is cases is contained in the polynomial $c \epsilon \mathbb{R}[u_1, \cdots, u_m]$.In the next section,we develop a method finding such polynomials.

3.4 A Method to Find Degenareted Case

Proposition 3.13 :*Let $g, h_1, \cdots, h_n$ be non-zero polynomials in $\mathbb{R}[u_1, \cdots, u_m, x_1, \cdots x_n]$ and let c be a non-zero polynomial in $\mathbb{R}[u_1, \cdots, u_m]$ then*

$c.g\ \epsilon\sqrt{< h_1, \cdots, h_n >}$ *if and only if* $g\epsilon\sqrt{< h_1, \cdots, h_n >: c^{\infty}}$

Proof: Let $c.g\ \epsilon\sqrt{< h_1, \cdots, h_n >}$ then $(cg)^k \in < h_1, \cdots, h_n >$ for some positive integer k therefore $g^k \in < h_1, \cdots, h_n >: c^k \subseteq < h_1, \cdots, h_n >: c^{\infty}$ and this that $g \in \sqrt{< h_1, \cdots, h_n >: c^{\infty}}$

Conversely , let $g \in \sqrt{< h_1, \cdots, h_n >: c^{\infty}}$ .So $g^k \in < h_1, \cdots, h_n >: c^{\infty}$ for some positive integer k,and then $g^k c^t \in < h_1, \cdots, h_n >$ for some positive integer t.Let $s = \max\{k, t\}$.So $(gc)^s \in < h_1, \cdots, h_n >$ and it follows that

$gc \in \sqrt{< h_1, \cdots, h_n >}$.

Corollary 3.14*: A conclusion g follows generically from the hypotheses $h_1, \cdots, h_n$.if there is some non-zero polynomial $c(u_1, \cdots, u_m) \in \mathbb{R}[u_1, \cdots, u_m]$ such that*.

$$g \in \sqrt{< h_1, \cdots, h_n >: c^\infty}$$

The following result will be useful for finding degeneracy cases.

Lemma 3.15: *Let R be a Noetherian ring , let $I$and J be ideals in $\mathbb{R}$, and let $f, g \epsilon \mathbb{R}\{0\}$. Then the followings are equivalent.*

i. $g\epsilon\sqrt{I: f^\infty}$

ii. $f\epsilon\sqrt{I: g^\infty}$

iii. $1 \in I :< fg >^\infty$

iv. Proof: (i)→(ii). $g\epsilon\sqrt{I: f^\infty}$ implies that $g^k \in I: f^\infty$ for some power k.Then $g^k f^t \in I$

again for some power t. It follows that $g^k \in I: f^t \subseteq I: f^\infty$ and $g\epsilon\sqrt{I: f^\infty}$

(ii)→(iii) since $f\epsilon\sqrt{I: g^\infty}$,there exist a positive integer k , $f^k \in I: g^\infty$.therefore there exists a positive integer t , $f^k g^t \in I$. Let $s = \max\{k, t\}$. So $(fg)^s \in I$

It follows that $1 \in I:< fg >^s \subseteq I:< fg >^\infty$

(iii)→ (i) Let k be a positive integer such that $1 \in I:< fg >^k$ so $(fg)^k \in I$ then

$g^k \in I: f^t \subseteq I: f^\infty$ it is easily follows that $g \in \sqrt{I:< f >^\infty}$

We can conclude the following

Theorem 3.16 :*A conclusion g follows generically from the hypotheses $h_1, \cdots, h_n$ whenever there is non-zero polynomial $c(u_1, \cdots, u_m) \in \mathbb{R}[u_1, \cdots, u_m]$ in $\sqrt{< h_1, \cdots, h_n >: g^\infty}$*

Proof: By above lemma, $g \in \sqrt{< h_1, \cdots, h_n >: C^\infty}$ if and only if $C \in \sqrt{< h_1, \cdots, h_n >: g^\infty}$. $c \in \sqrt{< h_1, \cdots, h_n >: g^\infty}$ implies g follows generically

from the hypotheses $h_1, \cdots, h_n$

We can prove the converse of the above the theorem can also hold . To do this we need some preparatio

Definition 3.17:*An ideal* I *in a ring R is primary if* $fg \in I$ *implies* $f \in I$ *or* $g^m \in I$ *for some power* m

Theorem3.18 (Existence of Primary Decomposition): *For any* I *in a noetherion ring* $\mathbb{R}$ *,we can write*

$$I = Q_1 \cap Q_2 \cap \cdots Q_r$$

Where each Q_j*is primary in* $\mathbb{R}$*.this is called a primary decomposition of* I

Definition 3.19: *A primary decomposition*

$$I = Q_1 \cap Q_2 \cap \cdots Q_r$$

İs weakly irreduntunt if none of the Q_j *is superflous, i.e*

$$\bigcap_{j \neq i} Q_j \nsubseteq Q_i$$

Theorem3.20(Uniqueness Theorem) :*Let* $\mathbb{R}$ *be Noetherion and* $I \subset \mathbb{R}$ *an ideal with weakly irredundunt primary decomposition*.

$$I = Q_1 \cap Q_2 \cap \cdots Q_r$$

The associated primes $P_1, \cdots, P_L$ where $q_i = \sqrt{Q_i}$ are uniquely determined by I The relation between primary ideals and struction is given by the following theorem.

Theorem 3.21: *Let* R *be a ring in* $\mathbb{R}$ *.Let* Q *be primary ideal with* $q = \sqrt{Q}$ *and let* $f \in \mathbb{R}$

$$Q{:}< f >^{\infty} \begin{cases} Q & f \notin q \\ R & f \in q \end{cases}$$

Proof:Let $f \notin q$ by definition $Q \subseteq Q{:}< f >^{\infty}$.if $g \in Q{:}< f >^{\infty}, gf^t \in Q$ for some power t

$f^t \notin q$ and Q is primary implies $g \in Q$

Let $f \in q$ so $f^k \in$ Hence for any $g \in \mathbb{R}, g f^k \in Q$ which implies $g \in Q:< f >^{\infty}$

A consequence of this theorem is

Corollary 3.22: Let R be Noetherion and $I \subset R$ an ideal with primary decomposition

$$I = Q_1 \cap Q_2 \cap \cdots Q_r$$

For any $f \in R$

$$I:< f >= \bigcap_{f \notin q_i} Q_i$$

Theorem 3.23: If a conclusion g follows generically from hypotheses $h_1, \cdots, h_n$ then there exists non-zero polynomial $c \in \sqrt{< h_1, \cdots, h_n >: g^{\infty}} \cap \mathbb{R}[u_1, \cdots, u_n]$

Proof: let $I =< h_1, \cdots, h_n >$ and let

$$I = Q_1 \cap Q_2 \cap \cdots Q_r$$

Be its primary decomposition,

Hence,

$V(I) = V(Q_1), \cup \cdots, \cup V(Q_r)$

This is irreducible decomposition of $V(I)$ since $I\big(V(Q_i)\big) = \sqrt{Q_1}$ by Hilbert's nullstellensatz and $\sqrt{Q_i}$ is a prime ideal . After reordering we can write

$$V(I) = W_1 \cup \cdots \cup W_t U U_1 \cup \cdots \cup U_l$$

Where $I(W_i) \cap \mathbb{R}[u_1, \cdots, u_n]$={0} for each $i = 1, \cdots, t$ and

$$I\big(U_j\big) \cap \mathbb{R}[u_1, \cdots, u_n] \neq \{0\}$$

Since g follows generically from hypotheses $h_1, \cdots, h_n$, for $j = 1, \cdots l$

$g \in I(W_1 \cup \cdots \cup W_t) = I(W_1) \cap \cdots \cap I(W_t)$

So $I:< g >^{\infty} = Q_{L_1} \cap Q_{L_2} \cdots \cap Q_{i_l}$ where $V\left(Q_{i_j}\right) = U_j$

Since $I\left(V\left(Q_{i_j}\right)\right) \cap \mathbb{R}[u_1, \cdots, u_n] = I\big(U_j\big) \cap \mathbb{R}[u_1, \cdots, u_n] \neq \{0\}$,

$$\sqrt{I:< g >^{\infty}} \cap \mathbb{R}[u_1, \cdots, u_n] = \sqrt{Q_{i_1} \cap Q_{i_2} \cdots \cap Q_{i_l}} \cap \mathbb{R}[u_1, \cdots, u_n]$$

$$= \sqrt{Q_{i_1}} \cap \sqrt{Q_{i_2}} \cap \cdots \cap \sqrt{Q_{i_l}} \cap \mathbb{R}[u_1, \cdots, u_n]$$

$$= [I(V(\left(Q_{i_j}\right)) \cap \cdots \cap I(V\left(Q_{i_l}\right))] \cap$$

$\mathbb{R}[u_1, \cdots, u_n]$

$$\neq \{0\}$$

Hence we can say that $\sqrt{< h_1, \cdots, h_n >: g^{\infty}}$ contains all conditions under which the geometric statement is true. To decide whether a conclusion g follows generically from the hypotheses $h_1, \cdots, h_n$,all we have to do is check whether or not $< h_1, \cdots, h_n >: g^{\infty} \cap \mathbb{R}[u_1, \cdots, u_n]$ is zero or not .

If we go back to our example , the below Singular Computation shows that $< h_1, \cdots, h_6 >: g^{\infty} \cap \mathbb{R}[u_1, u_2, u_3] = < u_1 u_3^2, u_1 u_2 u_3 (u_1 - u_2) >$. Hence our conclusion follows from hypotheses . Moreover $u_1 u_3 = 0$, $u_1 = u_2$ and $u_1 u_2 u_3 = 0$ are only degenerate cases.

```
> ring r=0,(x1,x2,x3,x4,x5,x6,u1,u2,u3),dp ;
> LIB "elim.lib";
// ** loaded /usr /share/Singular/LIB/elim.lib (12231,2009-11-02)
// ** loaded /usr /share/Singular/LIB/ring.lib (12231,2009-11-02)
// ** loaded /usr/share/Singular/LIB/primdec.lib (12508,2010-02-03)
// ** loaded /usr/share/Singular/LIB/absfact.lib (12231,2009-11-02)
// ** loaded /usr/share/Singular/LIB/triang.lib (12231,2009-11-02)
// ** loaded /usr/share/Singular/LIB/matrix.lib (12231,2009-11-02)
// ** loaded /usr/share/Singular/LIB/nctools.lib (12231,2009-11-02)
// ** loaded /usr/share/Singular/LIB/random.lib (12231,2009-11-02)
// ** loaded /usr/share/Singular/LIB/poly.lib (12443,2010-01-19)
// ** loaded /usr/share/Singular/LIB/general.lib (12231,2009-11-02)
```

```
// ** loaded /usr/share/Singular/LIB/inout.lib (12541,2010-02-09)'



> ideal  i=x2*u2-x1*u3,x4*(u2-u1)-u3*(x3-u1),x2*u3+u2*(x1-u1),x4*u3+x3*(u2-u1),(x2-
x5)*(x1-u1)-x2*(x1-u2),x6*x3-x4*u2;

> poly  g=x5-x6;

> sat(i,g);

[1]:

  [1]=x2*u2-x1*u3

  [2]=x1*u2-u1*u2+x2*u3

  [3]=x4*u1-x4*u2+x3*u3-u1*u3

  [4]=x3*u1-x3*u2-x4*u3

  [5]=x3*x6-x4*u2

  [6]=x1*x5+x2*u1-x5*u1-x1*u3

  [7]=x1*x3-x3*u2-x4*u3

  [8]=u1*u3^2

  [9]=x4*x6*u3+x3*u2*u3-u1*u2*u3

  [10]=x2*x5*u3-x1*u1*u3+u1*u2*u3-x2*u3^2

  [11]=x2*x4*u3

  [12]=x1*x4*u3-x4*u2*u3+x3*u3^2-u1*u3^2

  [13]=x3^2*u3+x4^2*u3-x3*u2*u3-x4*u3^2

  [14]=x2*x3*u3

  [15]=x1^2*u3+x2^2*u3-x1*u1*u3

  [16]=x4*u2*u3^2-x3*u3^3

  [17]=x3*u2*u3^2+x4*u3^3

  [18]=u1^2*u2*u3-u1*u2^2*u3

[2]:

  1
```

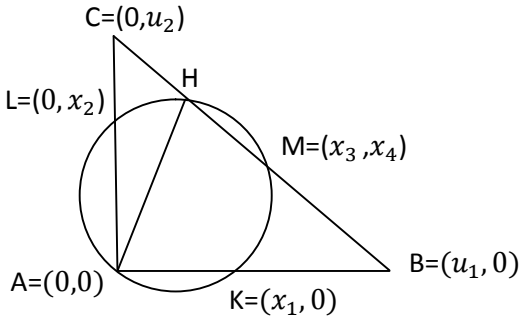
> eliminate(sat(i,g)[1],x1*x2*x3*x4*x5*x6);

[1]=u1*u3^2

[2]=u1^2*u2*u3-u1*u2^2*u3

3.5 Examples

Example 3.24 : The Theorem of apollonius :



Let ABC be a right triangle in the plane with a right angle at A. The midpoint of the three sides and the foot of the altitude drawn from A to the BC lie on a circle. Place A at (0,0) B(u_1, 0) . Since the angle at A is right angle, we have

C= (0,u_2) Let the three midpoints have coordinates K=(x_1, 0) , L=(0,x_2) and M= (x_3, x_4) K is a midpoint if the segments $2AK = AB$, that is $2x_1 = u_1$, which gives

$$h_1 = 2x_1 - u_1 = 0$$

L as a midpoint

$$h_2 = 2x_2 - u_2 = 0$$

and M is a midpoint if $BM = 2BC$ this means tha

$$h_3 = u_1^2 + u_2^2 - 4[(x_3 - u_1)^2 + x_4^2] = 0$$

We shall construct the point H=(x_5, x_6) as follows:

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

Hence

$$h_4 = (x_5, x_6).(u_1, -u_2) = x_5u_1 - x_6u_2 = 0$$

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

$$h_5 = x_5u_2 + x_6u_1 - u_1u_2 = 0$$

We must consider the statement that K, L, M and H lie on a circle. A general collection of four points do not lie on a circle , but a collection of three points

does .Thus , our conclusion can be restated as follows:

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

also . To check this , we need to construct the center of the circle

$O = (x_7, x_8)$ K, L and M are on the same circle if $KO = LO$ and

$KO = MO$

Equality of KO and LO gives

$$h_6 = (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0$$

Equality of KO and MO gives

$$h_7 = (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0$$

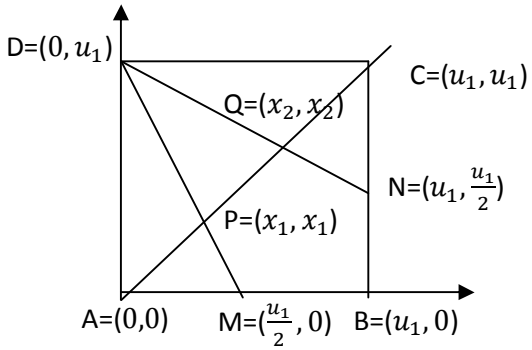
Our conclusion is $HO = KO$ gives

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

A Singular Computation shows that $< h_1, \cdots, h_7 >: g^{\infty} \cap k[u_1, u_2] =$

$< u_1, u_2 >$ so conclusion follows from hypotheses .

Example . 3.25 : Diagonal Trisection Theorem



The two lines passing through a vertex of a square and the midpoints of the opposite sides cut the opposite diagonal into three equal parts. D , P and M being colinear giv

$$(x_1 - u_1)\left(x_1 - \frac{u_1}{2}\right) - x_1^2 = 0$$

Implies

$$h_1 = u_1^2 - 3x_1u_1 = 0$$

D , Q and N being colinear give

$$(x_2 - u_1)(x_2 - u_1) - (x_2 - \frac{u_1}{2})x_2$$

Implies

$$h_2 = 2u_1^2 - 3x_2u_1 = 0$$

$AP = PQ$

$$(x_1 - 0)^2 + (x_1 - 0)^2 = (x_2 - x_1)^2 + (x_2 - x_1)^2$$

$$h_3 = x_1^2 = (x_2 - x_1)^2$$

Conclusion

$$PQ = QC$$

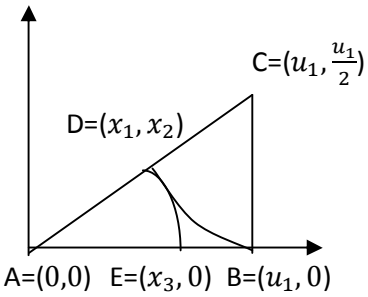
$$g = (x_2 - u_1)^2 = (x_2 - x_1)^2$$

A Singular Computation shows that $< h_1 , h_2 , h_3 >: g^{\infty} =< u_1 >$. When $u_1 = 0$ the square is collapse which is degenerate cases . The conclusion follows from hypotheses except $u_1 = 0$

Example 3.26 : The Golden Mean Theorem

Let AB a line segment , let BC be perpendicular to AB and have half its length , let D be the intersection of AC with circle centered on C passing through B and let E be the intersection of AB with the circle centered on A and passing through D . Then the point E is the golden mean of AB , that is,

$$\frac{AB}{AE} = \frac{1}{2}(1+\sqrt{5})$$



We have to Express the hypotheses that D is contained in the line AC

$$h_1 = u_1x_1 - 2u_1x_2 = 0$$

The other two hypotheses $BC = CD$ and $AD = AE$,which give us

$$h_2 = u_1^2 - 2u_1x_1 + x_1^2 - u_1x_2 + x_2^2 = 0$$

$$h_3 = x_1^2 + x_2^2 - x_3^2 = 0$$

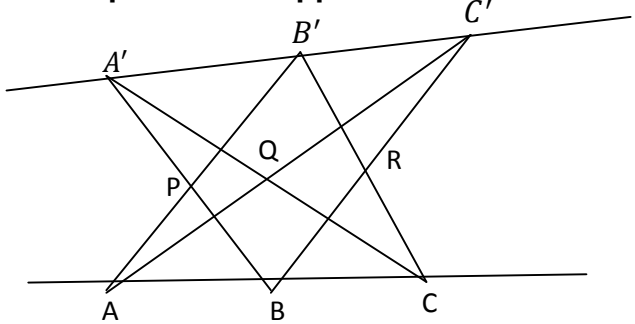
The conclusion polynomial is

$$g = 2u_1 - (1+\sqrt{5})\, x_3$$

Again , a Singular Computation shows that $< h_1 , h_2 , h_3 > : g^{\infty} = < u_1 >$.

So g follows from h_1 , h_2 , h_3 except $u_1 = 0$ which is degenerate case .

Example 3.27 : Poppus theorem



Let A, B, C and A', B', C' be two set of collinear points.Let $P = \overline{AB'} \cap \overline{A'B}$,

$Q = \overline{AC'} \cap \overline{A'C}$, $R = \overline{BC'} \cap \overline{B'C}$

Theorem states that P, Q and R are collinear

Let A = (0,0) , B = $(u_1, 0)$, C = $(u_2, 0)$, A'= (u_3, u_1) , B'=(u_5, u_6) , C' = (u_7, x_1) ,

P = (x_2, x_3) ,

Q = (x_4, x_5) ,R = (x_6, x_7)

Hypotheses;

The points A', B', C' are collinear

$$h_1 = (u_6 - u_1)(u_7 - u_3) - (x_1 - u_1)(u_5 - u_3) = 0$$

The points A, P, B' are collinear

$$h_2 = x_3 u_5 - u_6 x_2 = 0$$

The points B, P, A' are collinear

$$h_3 = u_1(x_2 - u_1) - x_3(u_3 - u_1) = 0$$

The points A, Q, C' are collinear

$$h_4 = x_5 u_7 - x_1 x_4 = 0$$

The points C, Q, A' are collinear

$$h_5 = x_5(u_3 - u_2) - u_1(x_4 - u_2) = 0$$

The points B, R, C' are collinear

$$h_6 = x_7(u_7 - u_1) - x_1(x_6 - u_1) = 0$$

The points C, R, B' are collinear

$$h_7 = u_6(x_6 - u_2) - x_7(u_5 - u_2) = 0$$

The conclusion is that P, Q and R are collinaer

$$g = (x_5 - x_3)(x_6 - x_2) - (x_7 - x_3)(x_1 - x_2) = 0$$

The following Singular Computation shows we have several degenerate cases , and the conclusion follows from the hypotheses except these cases .

```
> ring r=0,(x1,x2,x3,x4,x5,x6,x7,u1,u2,u3,u4,u5,u6,u7),dp ;
> poly h1=(u6-u4)*(u7-u3)-(x1-u4)*(u5-u3);
> poly h2=x3*u5-u6*x2;
> poly h3=u4*(x2-u1)-x3*(u3-u1);
> poly h4=x5*u7-x1*x4;
> poly h5=x5*(u3-u2)-u4*(x4-u2);
> poly h6=x7*(u7-u1)-x1*(x6-u1);
> poly h7=u6*(x6-u2)-x7*(u5-u2);
> poly g=(x5-x3)*(x6-x2)-(x7-x3)*(x4-x2);
> ideal i=h1,h2,h3,h4,h5,h6,h7;
> LIB "elim.lib";
// ** loaded /usr/share/Singular/LIB/elim.lib (12231,2009-11-02)
// ** loaded /usr/share/Singular/LIB/ring.lib (12231,2009-11-02)
// ** loaded /usr/share/Singular/LIB/primdec.lib (12508,2010-02-03)
// ** loaded /usr/share/Singular/LIB/absfact.lib (12231,2009-11-02)
// ** loaded /usr/share/Singular/LIB/triang.lib (12231,2009-11-02)
// ** loaded /usr/share/Singular/LIB/matrix.lib (12231,2009-11-02)
// ** loaded /usr/share/Singular/LIB/nctools.lib (12231,2009-11-02)
// ** loaded /usr/share/Singular/LIB/random.lib (12231,2009-11-02)
// ** loaded /usr/share/Singular/LIB/poly.lib (12443,2010-01-19)
// ** loaded /usr/share/Singular/LIB/general.lib (12231,2009-11-02)
// ** loaded /usr/share/Singular/LIB/inout.lib (12541,2010-02-09)
> eliminate(sat(i,g)[1],x1*x2*x3*x4*x5*x6*x7);
[1]=u4*u5+u1*u6-u3*u6
[2]=u4*u6*u7
[3]=u1*u6*u7-u3*u6*u7
```

[4]=u2*u4*u7

[5]=u1*u2*u7-u2*u3*u7-u1*u5*u7+u3*u5*u7

[6]=u1*u4*u6

[7]=u1*u2*u6-u1*u3*u6+u2*u4*u7+u1*u6*u7-u2*u6*u7

[8]=u1^2*u6-u1*u3*u6

[9]=u1*u2*u5-u1*u3*u5-u2*u5*u7+u3*u5*u7

[10]=u2*u3*u6*u7-u3^2*u6*u7-u2*u6*u7^2+u3*u6*u7^2

[11]=u1*u3*u5*u7-u2*u3*u5*u7-u1*u5^2*u7+u3*u5^2*u7+u2*u5*u7^2-u3*u5*u7^2

[12]=u2^2*u3*u5*u7-u2*u3^2*u5*u7-u2*u3*u5^2*u7+u3^2*u5^2*u7-
u2^2*u5*u7^2+u2*u3*u5*u7^2+u2*u5^2*u7^2-u3*u5^2*u7^2

CHAPTER 4

AUTOMATED GEOMETRIC THEOREM DISCOVERING

4.1 The Minimal Comprehensive Canonical Gröbner Basis

This chapher involves an application of Minimal Canonical Comprehensive Gröbner System (MCCGS) to the problem of discovering the correct hypotheses that give an interesting theorem in geometry. The discussion was inspired by ?.

The goals and output of the MCCGS algorithm, procedure for computing the minimal canonical comprehensive Gröbner system of a given parametric ideal is briefly described as follows: Given a parametric polynomial system of equations over some computable field, such as the rational numbers, our interest focuses on discussing the type of solutions over some algebraically closed extension, such as the complex numbers, depending on the values of the parameters. A concrete example might be helpful.

Given ideal $I =< (u-1)x + y^2, uy + u >\subseteq k[x, y, u]$. A lexicographic Gröbner basis $x > y > u$ is

$$\{ux - x + y^2, uy + u, xy + x - y^3 - y^2\}.$$

Set $V = V(I) \subseteq k^3$. The Elimination Theorem implies that $I_2 = \{\}$ and The Closure Theorem says that projection of V onto the last coordinate has Zariski closure set. A more careful analysis reveals that $\pi_2(V) = k^1 \backslash \{1\}$.

If u is considered as a parameter, then the question is that does

$$G = \{ux - x + y^2, uy + u, xy + x - y^3 - y^2\}$$

remain Gröbner basis (for lex with $x > y$) when the parameter u is given a numeric value b ?

Setting $u = 1$ gives $\overline{G_1} = \{y^2, y + 1, xy + x - y^3 - y^2\}$ which generates $< 1 >= k[x, y]$. Since $1 \notin < y^2, y, x\, y >$, $\overline{G_1}$ is not a Gröbner basis. In fact, after rewriting G as

$$\{(\boldsymbol{u} - \mathbf{1})x + y^2, \boldsymbol{u}\, y + u, \mathbf{1}\, xy + x - y^3 - y^2\},$$

by the Closure Theorem one can conclude that if $u = b \neq 0,1$, then $\overline{G_b}$ is a Gröbner basis.

Since $\pi_2(V) = k^1 \backslash \{1\}$, the equations

$$\{(\boldsymbol{u} - \mathbf{1})x + y^2 = \boldsymbol{u}\, y + u = 0\}$$

have a unique solution if $u = b \neq 0,1$ and infinitely many solution if $u = b = 0$.

Consider the following pairs:

$(S_1, G_1) = (k \backslash \{0,1\}, \{(u - 1)x + y^2, uy - u\})$

$(S_2, G_2) = (\{0\}, \{x - y^2\})$

$(S_3, G_3) = (\{1\}, \{1\})$

Note that $S_1 \cup S_2 \cup S_2 = k^1$ is a constructible partition. For $b \in S_i$, $\overline{G_i}$ is a reduced Gröbner basis up to a constant and $< LT(\overline{G_{i_b}}) >$ is independent of b. This is in fact minimal comprehensive cononical Gröbner system (MCCGS). The following is the formal definition of MCCGS is due to ?.

Definition 4.1 *Let* $I \subseteq k[\mathbf{x}, \mathbf{u}]$ *be an ideal with variables* $\mathbf{x} = (x_1, x_2, \dots, x_n)$ *and parameters* $\mathbf{u} = (u_1, u_2, \dots, u_m)$. *Fix an order* > *on* $k[\mathbf{x}]$. *A minimal canonical comprehensive Gröbner system for* I *and* > *consists of pairs* (S_i, G_i) *satisfying*

(i) *The* S_i*'s give a contructible partition of* k^m.

(ii) *For* $\mathbf{b} \in S_i$, *setting* $\mathbf{u}=\mathbf{b}$ *gives reduced Gröbner basis* $\bar{G}_{i_b}$ *up to constant.*

(iii) *For* $\mathbf{b} \in S_i$, $< LT(\bar{G}_{i_b}) >$ *is indepent of* $\mathbf{b}$ **.**

(iv) *No smaller partition exists with these properties.*

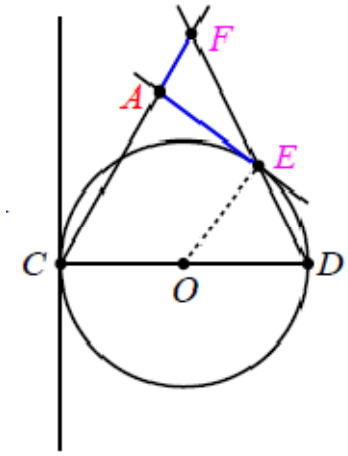
There are several algorithms that allow one to build both Comprehensive Gröbner Systems, but they are oriented differently. The main objective is to have disjoint and reduced Gröbner bases. The algorithm BUILDTREE (introduced in Montes (2002) as DISPGB and improved in Manubens and Montes (2006)) already builds a disjoint, reduced comprehensive Gröbner system. The algorithm BUILDTREE has already implemented to the computer algebra system SINGULAR. In Montes (2007) the interest is focused on the improvement of BUILDTREE to obtain a simpler and canonical CGS. The method consisted of grouping together all the segments with the same leading terms that allow a same basis specializing well on all the grouped segments.

4.2 An Application of MCCGB to Geometric Theorem Discovering

Let $H =< f_1, \dots, f_t >$ be the set of hypothesis ideal and g be the polynomial that correspondences to theorem we want to be true under some extra conditions. To find degeneracy conditions $T = H: g^{\infty}$. Therefore the ideal we

will consider is $I = H{:}T^{\infty}$. Then computing MCCGB for the ideal $I+< g >$ and examining every segment, one can find extra conditions which makes theorem true.

Example 4.2



Let CD be the diameter of a circle of radius 1. Fix A. Then the line AE is tangent to the circle at E. The lines AC and ED meet at F. The theorem AE = AF is generally false. The goal is to discover reasonable hypotheses on A to make the theorem true.

Set $C = (0,0), O = (1,0), D = (2,0), A = (u_1, u_2), E = (x_1, x_2)$ and $F = (x_3, x_4)$.

AE being perpendicular to OE gives

$h_1 = (x_1 - u_1)(x_1 - 1) + (x_2 - u_2)x_2$.

The length of segment OE being 1 gives

$$h_2 = (x_1 - 1)^3 + {x_2}^2 - 1$$

F being intersection of AC and ED gives

$$h_3 = u_1 x_4 - u_2 x_3,$$

$$h_4 = x_4(x_1 - 1) - x_2(x_3 - 2).$$

We also have to assume that $A \neq C$ that is $u_1 \neq 0, u_2 \neq 0$ and $E \neq D$ that is $x_2 \neq 2$.

Therefore the ideal that describes this problem is the saturation

$I =< h_1, h_2, h_3, h_4 >: < (x_2 - 2)u_1, (x_2 - 2)u_2 >$.

Our false assertation AE=AF gives

$$g = (u_1 - x_1)^2 + (u_2 - x_2)^2 - (u_3 - x_3)^2 - (u_4 - x_4)^2$$

Now, we should compute a MCCGS for the ideal

$$I+< g >\subseteq k[x_1, x_2, x_3, x_4, u_1, u_2]$$

with variables u_1 and u_2 .

A MCCGS with respect to lex order for the above ideal is:

i	Segment S_i:	$LT(\bar{G}_{i_b})$
1	$k^2 \backslash (V({u_1}^2 + {u_2}^2 - 2u_1) \cup V(u_1))$	1
2	$V({u_1}^2 + {u_2}^2 - 2u_1) \backslash \{(0,0), (2,0)\}$	$x_1, x_2, x_3, {x_4}^2$
3	$V(u_1) \backslash \{(0,0), (0, \pm i)\}$	$x_1, x_2, x_3, {x_4}^2$
4	$\{(0, \pm i)\}$	$x_1, x_2, x_3, {x_4}^2$
5	$\{(2,0)\}$	$x_1, x_2, x_3, {x_4}^2$
6	$\{(0,0)\}$	$x_1, x_2, x_3, {x_4}^2$

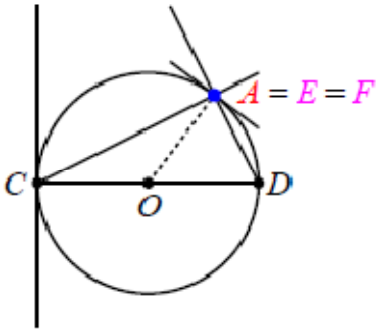
We can disregard the segments S_4, S_5 and S_6 since they are contains only the points.

$G_1 = \{1\}$ and $S_1 = k^2 \backslash (V({u_1}^2 + {u_2}^2 - 2u_1) \cup V(u_1))$ implies that $V(I+< g > = \emptyset$ if $b \notin V({u_1}^2 + {u_2}^2 - 2u_1) \cup V(u_1)$. Hence the result $AE = AF$ can not be followed our hypothesis unless A comes from $V({u_1}^2 + {u_2}^2 - 2u_1) \cup V(u_1)$.

That means A is on the circle or in the y-axis. Hence A is on the circle or in the y-axis is a necessary condition for $AE = EF$.

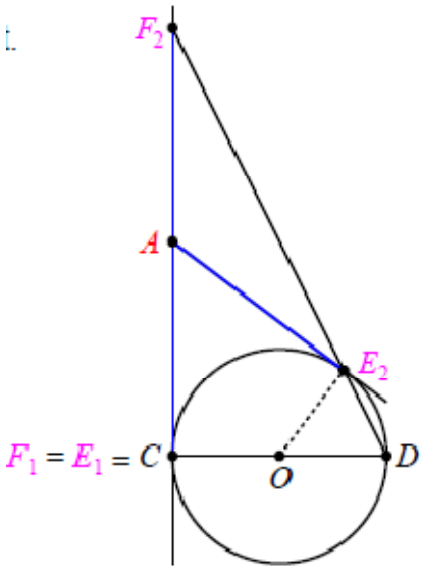
To study whether the condition is sufficient, we use S_2 and S_3. Notice that S_2 corresponds to A being on the circle and S_3 corresponds to A being in the y-axis.

When A is on the circle, we get



Here, AE = AF is true (both sides are zero!). Hence the theorem is true but not interesting.

When A is in the y- axis, we get



we get the picture to the right.

There are two choices for E: For E_1, we get $E_1 = F_1$, so $AE = AF$ is true but uninteresting. For E_2, we get an interesting theorem!

REFERENCES

Adams, W., Loustaunau, P., 1994. "*An Introduction to Grobner Bases*", Graduate Studies in Mathematics, Vol. 3, AMS, New York.

Cox, D., Little, J., O'Shea, D.,1997. *" Ideals, varieties, and algorithms*", Texts in Mathematics, Springer-Verlag, New York.

Chou, S-C., 1988. "*Mechanical Geometry Theorem Proving*", K. Reidel, Dordrecht.

Dolzmann, A., Sturm, T., Weispfenning, V., 1998. "*A new approach for Automatic theorem proving in real geometry*", Journal of Automated Reasoning 21, 357-380.

Greuel, G-M., Pfister, G., Schönemann, H., 2010. "*SINGULAR 3.1: A Computer Algebra System for Polynomial Computations"*, Centre for Computer Algebra,University of Kaiserslautern, http://www.singular.uni-kl.de.

Kapur, D., 1986. "*Using Gröbner Bases to reason about geometry problems*", Journal of Symbolic Comput. 2(4), 399-408;

Kutzler, B., Stifter, S., 1986. "*On the application of Buchberger's algorithm to automated geometry theorem proving*", Journal of Symbolic Computation 2, 389-397.

Manubens, M., Montes, A., 2006. " *Minimal canonical comprehensive Groebner systems*.", Journal of Symbolic Computation 44, 463-478.

Montes, A., 2002., "*New algorithm for discussing Gröbner bases with parameters*.", Journal of Symbolic. Comput. 33, 183-208.

Montes, A., 2007., "*On the canonical discussion of polynomial systems with parameter*", Preprint arXiv: AC/0601674.

Montes, A., Recio, T., 2007. "*Automatic discovery of geometry theorems using minimal canonical comprehensive Groebner systems.*", Lecture Notes in Artificial Engineering 4869, 113-138.

Wu, W-T., 1984. "*Basic principles of mechanical theorem proving in elementary geometry*", Journal of Systems Sci. and Math Sci. 4, 207-235.