Gröbner Bases

Mini Project Report

Submitted in partial fulfilment of
the requirements for the award of the degree of

Bachelor of Technology
in
Computer Science and Engineering

Submitted by

Dhandeep M Lodaya
B080569CS

Ayush Sengupta
B080545CS

Anuj Tawari
B080511CS

Nitish Gupta
B080616CS

Project Guide: **Prof.Dr K Muralikrishnan.**

Department of Computer Science & Engineering
National Institute of Technology Calicut
Kerala - 673601

Winter 2010

ACKNOWLEDGEMENT

We are highly indebted to our guide Dr.K Muralikrishnan , Assistant Professor, National Institute of Technology, Calicut for his guidance and constant supervision throughout the project. We thank him for his valuable suggestions and guidelines.

We also like to thank Mr. Sreenu Naik Bhukya, Assistant Professor, National Institute of Technology, Calicut for his guidance and support.

ABSTRACT

The aim of the project would be to study the method of Gröbner bases, which will allow us to solve problems about polynomial ideals in an algorithmic or computational fashion. it is explicitly used in computing solutions of multivariate polynomial equations.We will also study and analyse algorithms for the construction of Gröbner bases from an arbitrary ideal bases, such as Buchburger's algorithm.

1 INTRODUCTION

Groebner bases allow us to solve problems about polynomial ideals in an algorithmic or computational fashion .

The main problems that we focus on are :

1. The existence of a finite generating set for polynomial ideals
2. Membership of a given polynomial f in a polynomial ideal

In this document, we refer to a polynomial ring in n variables as $k[x_1, x_2, x_3, ..., x_n]$.

2 IDEALS AND VARIETIES

Definition 1. A subset $I \subset k[x_1, x_2, x_3, ..., x_n]$ is an ideal if it satisfies:

1. $0 \in I$
2. If $f, g \in I$, then $f + g \in I$.
3. If $f \in I$ and $h \subset k[x_1, x_2, x_3, ..., x_n]$, then $hf \in I$.

Definition 2. Let k be a field, and let $f_1, ..., f_s$ be polynomials in $k[x_1, x_2, x_3, ..., x_n]$. Then we set
$V(f_1, ..., f_s) = \{(a_1, ..., a_s) \in k^n : f_i(a_1, ..., a_s) = 0 \text{ for all } 1 \leq i \leq s\}$.
We call $V(f_1, ..., f_s)$ the affine variety defined by $f_1, ..., f_s$.

3 MONOMIAL

Definition 1: A monomial in $x_1, ..., x_n$ is a product of the form $x_1^{\alpha_1}.x_2^{\alpha_2}...x_n^{\alpha_n}$, where all of $\alpha_1, \alpha_2, ..., \alpha_n$ are non-negative integers. The total degree of monomial is $\alpha_1 + \alpha_2 + ... + \alpha_n$.

Definition 2: A polynomial f in $x_1, ..., x_n$ with coefficients in k is a finite linear combination (with coefficients in k) of monomials. We will write a polynomial f in the form
$f = \Sigma_\alpha \ a_\alpha x^\alpha$ where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, ..., \alpha_n)$

4 ORDERING ON MONOMIALS

Ordering of monomials in $k[x_1, x_2, x_3, ..., x_n]$.
The ordering of terms in a polynomial is a key ingredient in various important algorithms like division algorithm in k[x] and row-reduction algorithm for a system of polynomial equations.

In this document , we focus on lexicographic ordering of terms in a polynomial.

Definition 3: Lexicographic ordering.
Let $\alpha = (\alpha_1, ..., \alpha_n)$ and $\beta = (\beta_1, ..., \beta_n) \in Z^n_{\geq 0}$
We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in Z^n$ the leftmost nonzero entry is positive.

5 MONOMIAL IDEAL

Definition 4: An ideal I $\subset k[x_1, x_2, x_3, ..., x_n]$ is a monomial ideal if there is a subset A $\subset Z^n$ (possibly infinite) such that I consists of all polynomials which are finite sums of the form $\Sigma_{a \in A} h_\alpha x^\alpha$ where $h_\alpha \in k[x_1, x_2, x_3, ..., x_n]$

Claim 1. Let I $= < x^\alpha : \alpha \in A >$ 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 $\alpha \in A$.
Proof:
If x^β is a multiple of x^α for some $\alpha \in A$, then $x^\beta \in I$ by the definition of ideal.
Conversely, if $x^\beta \in I$, then $x^\beta = h_i x^{\alpha(i)}$, where $h_i \in k[x_1, x_2, x_3, ..., x_n]$ and $\alpha(i) \in A$.
If we expand each h_i as a linear combination of monomials, we see that every term on the right side of the equation is divisible by some $x^{\alpha(i)}$. This is because the set A being a subset of $Z^n_{\geq 0}$ is well-ordered. Hence, well-ordering principle assures us of the existence of such a minimal element and we are done.

Theorem 1: Dicksons Lemma Let $I = \{x^\alpha : \alpha \in A \subseteq k[x_1, x_2, x_3, ..., x_n]\}$ be a monomial ideal. Then I can be written in the form I$=< x^{\alpha(1)}, x^{\alpha(2)}, ..., x^{\alpha(s)} >$,where $\alpha(1), \alpha(2), ..., \alpha(s) \in A$. In particular, I has a finite basis.
(Note that the set A can be an infinite subset of Zn)

Proof : We use the priciple of mathematical induction in this proof.
Base case: n=1
Here, I is generated by the monomials x_1^α,where $\alpha \in A \subset Z^n_{\geq 0}$. Let $\beta \leq \alpha$ be the smallest element of $A \subset Z^n_{\geq 0}$.
Again , well-ordering principle guarantees the existence of such an element.
Then $\beta \leq \alpha$ for all $\alpha \in A$, so that x_1^β, divides all other generators x_1^α. From here,

$I =< x_1^\beta >$ follows easily.
Assume that $n > 1$ and that the theorem holds for n-1.
Without loss of generality , we may rename the variables as $x_1, x_2, x_3, ..., x_n$ as $x_1, x_2, x_3, ..., x_{n-1}, y$ so that monomials in $k[x_1, x_2, x_3, ..., x_{n-1}, y]$ can be written as $x^\alpha y^m$,
where $\alpha = (\alpha_1, \alpha_2, ..., \alpha_{n-1}) \in Z^{n-1}_{\geq 0}$ and m $\in Z^1_{\geq 0}$.
Suppose that $I \in k[x_1, x_2, x_3, ..., x_{n-1}, y]$ is a monomial ideal A.
and let $J \in k[x_1, x_2, x_3, ..., x_{n-1}]$.
be the ideal generated by monomials x^α such that $x^\alpha y^m$ where $m \geq 0$.
Since J is a monomial ideal in $k[x_1, x_2, x_3, ..., x_{n-1}]$, our inductive hypothesis implies that finitely many of the x^αs generate J , let $J =< x^{\alpha(1)}, ..., x^{\alpha(s)} >$.
From this , it follows that for each i between 1 and s , $x^{\alpha(i)} y^{m_i} \in I$ for some $m_i \geq 0$. Let m be the largest of the m^i . Then, for each k between 0 and m 1, consider the ideal $J_k \in k[x_1, x_2, x_3, ..., x_{n-1}]$ generated by the monomials x^β such that $x^\beta y^k \in I$.
The inductive hypothesis tells us that J_k has a finite generating set of monomials, say
$J_k =< x^{\alpha_k(1)}, x^{\alpha_k(2)}, ..., x^{\alpha_k(s_k)} >$

Claim 2:

I is generated by the monomials in the following list:
from J : $x^{\alpha(1)}y^m, x^{\alpha(2)}y^m, ..., x^{\alpha(s)}y^m$.

from J_0 : $x^{\alpha_0(1)}y^0, x^{\alpha_0(2)}y^0, ..., x^{\alpha_0(s_0)}y^0$.
from J_1 : $x^{\alpha_1(1)}y^1, x^{\alpha_1(2)}y^1, ..., x^{\alpha_1(s_1)}y^1$.
$\vdots \qquad \vdots \qquad \vdots$
from J_{m-1} : $x^{\alpha_{m-1}(1)}y^{m-1}, x^{\alpha_{m-1}(2)}y^{m-1}, ..., x^{\alpha_{m-1}(s_{m-1})}y^{m-1}$.

Proof : It suffices to prove that every monomial in I is divisible by one on this list as then claim 1 gives us the desired result.
let $x^\alpha y^p \in I$. If $p \geq m$, then $x^\alpha y^p$ is divisible by some $x^{(i)}y^m$ by the construction of J . On the other hand, if $p \leq m-1$, then $x^\alpha y^p$ is divisible by some $x^{\alpha_p(j)}y^p$ by the construction of J_p .

Claim 3: Let $>$ be a relation on Z^n satisfying:

1. $>$ is a total ordering on Z^n.
2. if $\alpha > \beta$ and $\gamma \in Z^n$, then $\alpha + \gamma > \beta + \gamma$.

Then $>$ is well-ordering if and only if $\alpha \geq 0$ for all $\alpha \in Z^n$.

Proof : Assume that $>$ forms a well-ordering and let α_0 be the smallest element of Z^n. It clearly suffices to show that $\alpha_0 \geq 0$. if $0 > \alpha_0$, then by hypothesis (2), we can add α_0 to both sides to obtain $\alpha_0 > 2\alpha_0$, a contradiction
Converse : Assuming that $\alpha_0 \geq 0$ for all αinn , let $A \subset Z^n$ be nonempty It suffices to prove that A has a smallest element
Since I $= < x^\alpha : \alpha \in A >$ is a monomial ideal, Dicksons Lemma gives us $\alpha(1), \alpha(2), ..., \alpha(s) \in A$ so that I$=< x^{\alpha(1)}, x^{\alpha(2)}, ..., x^{\alpha(s)} >$
Without loss of generality , we may assume that $\alpha(1) < \alpha(2) < ... < \alpha(s)$.

Claim 4: $\alpha(1)$ is the smalllest element of A

Proof : take $\alpha \in A$. Then $x^\alpha \in I =< x^{\alpha(1)}, x^{\alpha(2)}, ..., x^{\alpha(s)} >$,
so that by Claim 1, x^α is divisible by some $x^{\alpha(i)}$. Let $\alpha = \alpha(i) + \gamma$ for some $\gamma \in n$. Then $\gamma \geq 0$ and hypothesis (2) imply that
$\alpha = \alpha(i) + \gamma \geq \alpha(i) + 0 = \alpha(i) \geq \alpha(1)$.
Thus, $\alpha(1)$ is the smalllest element of A and we are done.

6 HILBERT BASIS THEOREM

Definition : Let I be an ideal of the polynomial ring in n variables.

1. Denote by LT(I) the set of leading terms of elements of I. Thus, LT(I) = $\{cx^\alpha$: there exists $f \in I$ with $LT(f) = cx^\alpha\}$.
2. Denote by $< LT(I) >$ the ideal generated by the elements of LT(I).

Claim 1 : Let $I \subset k[x_1, x_2, x_3, ..., x_n]$ be an ideal.

1. LT(I) is a monomial ideal.
2. There exist $g_1, ..., g_t \in I$ such that $< LT(I) >=< LT(g_1), ..., LT(g_t) >$.

Proof :
(i)The leading monomials LM(g) of elements $g \in I - \{0\}$ generate the monomial ideal $LM(g) : g \in I - \{0\}$ Since LM(g) and LT(g) differ by a nonzero constant,
this ideal equals $LT(g) : g \in I - \{0\}$= LT(I). Hence LT(I) is a monomial ideal.
(ii) Since LT(I) is generated by the monomials LM(g) for $g \in I - \{0\}$, Dicksons Lemma tells us that $LT(I) = < LM(g_1), ..., LM(g_t) >$ for finitely many $g_1, ..., g_t \in I$. Since $LM(g_i)$ differs from $LT(g_i)$ by a nonzero constant, it follows that $LT(I) = < LT(g_1), ..., LT(g_t) >$. and the claim is established.

Theorem (Hilbert Basis Theorem) : Every ideal I $\subset k[x_1, x_2, x_3, ..., x_n]$ has a finite generating set. That is, $I =< g_1, ..., g_t >$ for some $g_1, ..., g_t \in I$

Proof : If $I = \{0\}$, Take generating set to be $\{0\}$ .Otherwise I contains some non-zero polynomial.
By claim 1, there exist $g_1, ..., g_t \in I$ such that $LT(I) = < LT(g_1), ..., LT(g_t) >$.

Claim : $I =< g_1, ..., g_t >$.

Proof : Clearly , $g_1, ..., g_t \subset I$ since each $g_i \in I$.
Conversely, let $f \in I$ be any polynomial. If we apply the division algorithm to divide f by $g_1, ..., g_t$
then we get an expression of the form
$f = a_1g_1 + a_2g_2 + ... + a_tg_t + r$ where no term of r is divisible by any of $LT(g_1), ..., LT(g_t)$.

Claim : r = 0

Proof : $r = f - a_1g_1 - a_2g_2 - ... - a_tg_t \in I$. If $r \neq 0$, then LT(r) $\in LT(I) =< LT(g_1), ...LT(g_t) >$.
Hence , LT(r) must be divisible by some $LT(g_i)$. , a contradiction.
Hence , r=0 and the claim is established.
This gives $f = a_1g_1 + a_2g_2 + ... + a_tg_t$ hence $f \in < g_1, ..., g_t >$
Hence $I \subset < g_1, ..., g_t >$. And the proof is complete.
The set $\{g_1, ..., g_t\} \subset I$ is called a Groebner basis of I.

Claim : Let $I_1 \subset I_2 \subset I_3 \subset ....$
be an ascending chain of ideals in $k[x_1, x_2, x_3, ..., x_n]$. Then there exists a maximal ideal I_n.
ie. No I_k exists such that $I_n \subset I_k$

Proof :
consider the set $I = \bigcup_{i=1}^{\infty} I_i$.

Claim : I is an ideal in $k[x_1, x_2, x_3, ..., x_n]$.

Proof : First, $0 \in I$ since $0 \in I_i$for every i.
Next, if f, g ∈ I, then by definition, f $\in I_i$, and $g \in I_j$ for some i and j (possibly different). However, since the ideals I_i form an ascending chain, without loss of generality, we may assume that $i \leq j$, then both f and g are in I_j . Since I_j is an ideal, the sum $f + g \in I_j$, hence, $\in I$. Similarly, if $f \in I$ and $r \in k[x_1, x_2, x_3, ..., x_n]$, then $f \in I_i$ for some i, and $r.f \in I_i \subset I$. Hence, I is an ideal and we are done.
By Theorem , the ideal I must have a finite generating set: $I =< f_1, ..., f_s >$
Clearly , ∃ n : $f_i \in I_n \forall$ i. and we have established the existence of a maximal ideal.

7 An unique property of Gröbner Bases

Every non-zero ideal $I \subset k[x_1, x_2, x_3, ..., x_n]$ has a Gröbner basis. In this section properties of Gröbner bases will be introduced.
Property 1 :
Let $G = \{g_1, ..., g_n\}$ will be a Gröbner basis for $I \subset k[x_1, x_2, x_3, ..., x_n]$ and let $f \in k[x_1, x_2, x_3, ..., x_n]$ then $\exists r \in k[x_1, x_2, x_3, ..., x_n]$, S.T

1. No term of r is divisible by any of $LT(g_1), ..., LT(g_t)$.
2. $\exists g \in I : f = g + r$
3. r is unique

Proof : Dividing by $(g_1, ..., g_n)$ we get $f = a_1g_1 + ... + a_ng_n + r$, where r satisfies (1). Also $a_1g_1 + ... + a_ng_n \in I$, and thus satisfies (2).
Let $f = g + r = g' + r'$
$g - g' = r' - r \in I$
$\Rightarrow LT(r' - r) \in < LT(I) >=< LT(g_1), ..., LT(g_n) >$
This is impossible since no term of r and r' is divisible by $(LT(g_1), ..., LT(g_n))$. This satisfies (3).

There is an important implication of this property. Its is that for any ideal $I \subset k[x_1, x_2, x_3, ..., x_n]$, $f \in I$ iff the remainder when f is divided by the Groebner bases of I, is zero.

Also this property tells us that anfy $f \subset k[x_1, x_2, x_3, ..., x_n]$ when divided by a Groebner bases G of an ideal I, gives remainder zero, irrespective of the order of division.

Some Definitions

Definition 5 :- multideg(f) : Let $f = \Sigma_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, x_2, x_3, ..., x_n]$ and let $>$ be a monomial order.

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

Definition 6 :- We will write $\overline{f}^F$ for the remainder of f by the ordered s-tuple $F = (f_1, f_2, ..., f_s)$.

Definition 7 :- Let $f, g \in k[x_1, x_2, x_3, ..., x_n]$ be two non zero polynomials.

1. $\exists \gamma \in Z^n_{\geq 0}$, ST $\gamma_i = max(\alpha_i, \beta_i)$, where α=multideg(f) and β = multideg(g). here x^γ is called LCM of LCM(f) and LCM(g).
2. we define s-polynomial as $s(f, g) = \frac{x^\gamma}{LT(f)}.f - \frac{x^\gamma}{LT(g)}.g$

8 SCHWARTZ-ZIPPEL LEMMA

Schwartz-Zippel Lemma is a tool commonly used for polynomial identity testing, i.e. In the problem of determining whether a given multivariate polynomial is the zero polynomial (or identically equal to zero).
Theorem:- (Schwartz, Zippel). Let

$$p \in k[x_1, x_2, x_3, ..., x_n]$$

be a non-zero polynomial of degree $d \geq 0$ over a field F. Let $s \subset F$ and —S— is finite. Let $r_1, r_2, ...r_n$ be selected randomly from S. Then

$$Pr[P(r_1, r_2, ...r_n) = 0] \leq \frac{d}{|S|} \qquad -(1)$$

Proof : When n=1, P can have atmost d roots.
Thus (1) holds.
Let us assume the theorem holds for n-1 variables.
Now, $P(x_1, ..., x_n) = \Sigma^d_{i=0} x_1^i P_i(x_2, ..., x_n)$.
let us take the largest i for which $p_i \neq 0$ identically
By inductive Hypothesis,
$Pr[P_i(r_2, r_3, ...r_n) = 0] \leq \frac{d-1}{|S|}$, where $(r_2, ...r_n) \in S^n$
Also $Pr[P(r_1, r_2, ...r_n)|P_i(r_2, r_3, ...r_n) \neq 0] \leq \frac{i}{|S|}$.
Let A $\equiv P(r_1, r_2, ...r_n) = 0$
Let B $\equiv P_i(r_2, r_3, ...r_n) = 0$

$$\begin{aligned} Pr[A] &= Pr[A \cap B] + Pr[A \cap B'] \\ &= Pr[A].Pr[A|B] + Pr[B'].Pr[A|B'] \\ &\leq Pr[B] + Pr[A|B'] \\ &\leq \frac{d-i}{|S|} + \frac{i}{|S|} = \frac{d}{|S|} \end{aligned}$$

9 BUCHBERGER'S ALGORITHM

Here we discuss an algorithm (due to Buchberger), which constructs a Groebner bases for an ideal $I =< f_1, f_2, ..., f_s >$, in a finite number of steps. It proves an important fact, that the problem of comstructing Groebner bases is decidable.
The Algorithm

BUCHBERGER(F=$f_1, f_2, ..., f_s$)
{
G=F
do
{
G'=G
FOR each pair $\{p, q\}, p \neq q$ in G'
do
{
$S = \overline{S(p,q)}^{G'}$
if S≠0 then G=G $\bigcup\{S\}$
}
}while(G ≠ G')
return G
}

Proof : We first prove the invariant that $g \in I$ holds after each step of the algorithm. This is because $p, q \in I$ at each step and so does $\overline{S(p,q)}^{G'}$. We also note that G contains the given basic F of I so that G is also a basis of I.
The algorithm terminates when for all (p,q) pairs in G, $\overline{S(p,q)}^{G'} = 0$. Thus we have to prove that when this condition is true, G is a Groebner basis. This condition is also known as Buchberger's criterion. We will prove it in the next section.
It remains to prove that the algorithm terminates. We will see that after each pass,$G' \subset G$ and thus $< LT(G') > \subset < LT(G) >$.
Furthermore, if G ≠ G', we claim that $< LT(G') >$ is strictly smaller than $< LT(G) >$. To see this, we notice that $r = \overline{S(p,q)}^{G'} \notin < LT(G') >$ for LT(r) is not divisible by elements of $< LT(G') >$. But $r \in < LT(G) >$.
Thus, the size of the ideal $< LT(G) >$ strictly increases at each step. Now , we know that the size of the Groebner basis is finite (say m). Also, size of F is also finite and less than that of the Groebner bases. Also at each step, we strictly increase the size of the ideal. Thus after a finite number of steps, the size of the ideal will be equal to the size of the Groebner basis (ascending chain condition). Thus the algorithm terminates.

10 PROOF OF BUCHBERGER'S CRITERION

Buchberger's criterion states that for a polynomial ideal I, a basis $G = \{g_1, g_2..., g_t\}$ is a Gröebner basis for I iff for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G (listed in some order) is zero.

Proof

$\Rightarrow$: Since $S(g_i, g_j) \in I$ amd G is a Groebner basis, the remainder on division by G is zero, due to the inherent property of G.

$\Leftarrow$: Let $f \in I$ be a non-zero polynomial.

As $f \in I$, $f = \Sigma_{i=1}^{t} h_i g_i$ ——(1)

Let m(i) = $multideg(h_i g_i)$

Also, let δ = max(m(1),m(2) . . . .m(t))

It is apparent that multideg(f) $leq\delta$.

now if multideg(f) = δ, then multideg(f)= max(multideg($h_i g_i$) and thus

$LT(f) \in < LT(g_1), LT(g_2, ...LT(g_t)) >$. Thus G is a Groebner basis.

Now we have to prove the case if multideg(f) $< \delta$.

Let us assume it is true.

Let us write

$f = \Sigma_{m(i)=\delta} h_i g_i + \Sigma_{m(i)<\delta} h_i g_i$.

$f = \Sigma_{m(i)=\delta} LT(h_i) g_i + \Sigma_{m(i)=\delta} (h_i - LT(h_i)) g_i + \Sigma_{m(i)<\delta} h_i g_i$.

The multidegree of the second and third terms in the RHS is $< \delta$. Thus if multideg(f)$< \delta$, then some cancellation occurs in the first term to produce the following result.

Now, $\Sigma_{m(i)=\delta} LT(h_i) g_i = \Sigma_{m(i)=\delta} c_i x^{\alpha(i)} g_i$

now, let $\alpha_i = LC(x^{\alpha(i)} g_i)$.

and $P_i = \frac{x^{\alpha(i)} g_i}{d_i}$

$\Sigma_1^s c_i x^{\alpha(i)} g_i = \Sigma_1^s c_i P_i d_i$

$= c_1 d_1 (P_1 - P_2) + (c_1 d_1 + c_2 d_2)(P_2 - P_3) + ... + (c_1 d_1 + ... + c_{s-1} d_{s-1})(P_{s-1} - P_s)$.——(2)

Now, as the multideg of the first term is $< \delta, \Sigma_{i=1}^{s} (c_i d_i) = 0$.

thus the last term of the equation (2) cancels out.

Again. $S(x^{\alpha(i)} g_i, x^{\alpha(j)} g_j) = \frac{x^\delta}{LT(x^{\alpha(i)} g_i)} . x^{\alpha(i)} g_i - \frac{x^\delta}{LT(x^{\alpha(j)} g_j)} . x^{\alpha(j)} g_j$

$= P_i - P_j$———————————————- (3)

this is also equal to

$\frac{x^\delta}{x^{\alpha(i)} LT(g_i)} . x^{\alpha(i)} g_i - \frac{x^\delta}{x^{\alpha(j)} LT(g_j)} . x^{\alpha(j)} g_j$

$= x^{\delta - \gamma_{ij}} S(g_j, g_k)$———————————————(4)

Now, $\Sigma c_i x^{\alpha(i)} g_i = \Sigma c_{jk} S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k)$

from (2) and (3), as $P_i - P_j$ is essentially a particular s-polynomial.

$\Sigma_{m(i)=\delta} LT(h_i)g_i = \Sigma c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k)$

Now, as the remainder of $S(g_j, g_k)$ when divided by G is zero.(our assumptions).

$S(g_j, g_k) = \Sigma_{i=1}^{t} a_{ijk} g_i$.

Also $multideg(a_{ijk}.g_i) \leq multideg(S(g_j, g_k))$ by divition algorithm.

Also $multideg(x^{\delta-\gamma_{jk}} S(g_j, g_k)) < \delta$

$\Sigma_{m(i)=\delta} LT(h_i)g_i = \Sigma c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k)$

$= \Sigma c_{jk}(\Sigma b_{ijk} g_i) = \Sigma_i \tilde{h}_i g_i$——(5)

where $multideg(\tilde{h}_i g_i) < \delta$

Subtituting (4) in (5), we get a new expression of f with a lesser value of δ. This is because all the multideg(f) is less than δ. Thus for any δ , if multideg(f) is less than δ, we can use S-polynomial to get a lesser value than δ. Now as the multideg(f) if finite, we can use this method iteratively to to reach a particular δ_{min}, such that multideg(f) = δ_{min}. As proved earlier, in this case G is a Groebner basis. Thus we have completely proved the Buchberger's algorithm. Even though this algorithm proved the computability of Groebner bases, it amy take a long time to terminate. The time complexity of the algorithm is doubly exponential in the input data, which implies that its worst case behavior may be very slow. As the size of the Groebner basis can be very large, the algorithm has large storage requirements.

11 Applications of Gröbner basis

One can view Gröbner basis as a multivariate, non-linear generalization of:

1. The Euclidean algorithm for computation of univariate greatest common divisors,
2. Gaussian elimination for linear systems, and
3. integer programming problems.

11.1 Solving Multivariate Polynomial Equations

Gröbner basis can be used to solve a set of multivariate polynomial equations.
In particular, this gives us a method for solving simultaneous polynomial equations. If there are only finitely many solutions (over an algebraic closure of the field in which the coefficients lie) to the system of equations.
$\{(f_1[x_1, ..., x_n] = a_1), (f_2[x_1, ..., x_n] = a_2), ..., (f_m[x_1, ..., x_n] = a_m)\}$ We should be able to manipulate these equations to get something of the form
$g(x_n) = b$.
The elimination property says that if we compute a Gröbner basis for the ideal generated by $f_1 a_1, ..., f_m a_m$ relative to the right ordering, then we can find the polynomial g as one of the elements of our basis. Furthermore, (taking k = n - 1) there will be another polynomial in the basis involving only x_{n-1} and x_n, so we can take our possible solutions for x_n and find corresponding values for x_{n-1}. This lifting continues all the way up until we've found the values of all the variables.

11.2 Applications of grobner basis to mathematical chemistry

Consider the special case of the compound cyclohexane (C_6H_{12})
let $a_1, a_2, ..., a_6$ denote the bond vectors in a given conformation of cyclohexane .
the fixed bond length and angles give us
$||ai|| = a_{i,1}^2 + a_{i,2}^2 + a_{i,3}^2 = 1$ for i = 1,2.....6
Also, $< a_i.a_j >= a_{i,1}a_{j,1} + a_{i,2}a_{j,2} + a_{i,3}a_{j,3} = \cos\alpha = -1/3$
Furthermore , we have
$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 = 0$
they can be expanded to three co-ordinates.
Also, following equations fix the position of structure in space :
$a_{1,1} = 0$, $a_{1,2} = 0$ and $a_{2,1} = 0$
Certainly these equations can be solved by using Grobner bases . From these solutions we can analyze the chair form and twisted form of cyclohexane.
The idea can be extended to higher classes of chemical compounds as well .

12 CONCLUSION AND FUTURE WORK

In our project, we have studied about ideals, varieties and affine space. We have defined monomial ideals and lexical ordering. We have written proofs for Dickson's lemma and Hilbert Basis theorem. We have defined Gröbner basis and mentioned some of its unique properties. We have also studied Buchberger's algorithm. We have endeavoured to write the proofs for some of the theorems in a better and more lucid manner.

We note that the Buchberger's algorithm has a time complexity which is doubly exponential in the input data, which implies that its worst case behavior may be very slow. Various new algorithms have been proposed, such as Faugere's F-4 and F-5 , which computes the Gröbner basis of an ideal. These algorithms use the same mathematical principles as the Buchberger's algorithm, but are faster.

In the future, we will try to implement and analyse Faugere's F-4 and F-5 algorithms and compare it to Buchberger's algorithm. This will give us a deeper insight and we can then look to find further improvements for the same.

References

[1] David Cox, John Little, and Donal OShea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra.* (Undergraduate Texts in Mathematics). Springer, July 2005.

[2] Stanislav Bulygin and Ruud Pellikaan. *Decoding error-correcting codes with Gröbner bases, Proceedings of 28th Symposium on Information Theory in the Benelux, Enschede,* May 24-25, pp. 3-10, 2007

[3] Martin Kreuzer. *Solving polynomial equations using Gröbner basis.*

[4] Lorenzo Robbiano. *Solving Polynomial Equations.*

[5] *Gröbner Bases and Applications, London Mathematical Society Lecture Note Series.*

[6] Mario de Boer and Ruud Pellikaan..*Gröbner bases for error-correcting codes and their decoding.*