CIMPA Research School on Combinatorial and Computational Algebraic Geometry, IBADAN 12 - 23 June 2017 - Nigeria

Groebner Bases Lectures

Damian Maingi - University of Nairobi

1. Basic Notions

We shall denote a field by k i.e. any field say $\mathbb{Z}_p \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

The cartesian product of n copies of Natural numbers, $\mathbb{N} \times \cdots \times \mathbb{N}$.

We shall denote by $R = k[x_1, x_2, \cdots, x_n]$, the polynomial ring in n variables with coefficients in k.
Our usual ring will be $\mathbb{Q}[x, y, z]$ since software (macaulay II, Cocoa, SAGE, etc) works in this ring.

By an ideal I of R we mean a linear combination of polynomials say $\{f_1, f_2, \cdots, f_t\}$ with coefficients polynomials we denote this by $I = \{\lambda_1 f_1 + \lambda_2 f_2 + \cdots + \lambda_t f_t : \lambda_i \in R\}$. We can write $I = \langle f_1, f_2, \cdots, f_t \rangle$ and say that I is generated by $f_1, f_2, \cdots f_t \in R$.
We shall formalize what happens in the Gaussian Elimination Method in linear algebra and Division Algorithm in 1 variable.

We notice that in both Gaussian Method and Division Algorithm we follow order i.e. the key is in reducing the systems at hand identifying pivot elements.

Definition 1.1. Monomial Order:
A monomial order on $R = k[\bar{x}]$ is a relation "$>$" on on natural numbers (nonnegative integers), $\mathbb{N}^n$ satisfying;

(a) $>$ is a total (linear) ordering i.e. for any $\alpha, \beta \in \mathbb{N}^n$ either $\alpha > \beta$ or $\alpha = \beta$ or $\alpha < \beta$.

(b) if $\alpha > \beta$ then for $\gamma \in \mathbb{N}^n$ we have $\alpha + \gamma > \beta + \gamma$ which is equivalent to $x^\alpha > x^\beta$.

(c) $>$ is a well ordering on $\mathbb{N}^n$.

Definition 1.2. LEXICOGRAPHIC Order(LEX)
Let $a = (a_1, \cdots, a_n)$ and $b = (b_1, \cdots, b_n)$ be in $\mathbb{N}^n$. Then $a >_{lex} b$ which is equivalent to $x^a >_{lex} x^b$ if the first nonzero element (pivot) in the vector $a - b$ is positive.

Definition 1.3. GRADED Lexicographic Order(GrLEX)
Let $a = (a_1, \cdots, a_n)$ and $b = (b_1, \cdots, b_n)$ be in $\mathbb{N}^n$. Then $a >_{grlex} b$ which is equivalent to $x^a >_{grlex} x^b$ if $|a| = \sum a_i > |b| = \sum b_i$ or $|a| = \sum a_i = |b| = \sum b_i$ and $a >_{lex} b$.

Definition 1.4. GRADED Reverse Lexicographic Order(GrevLEX)
Let $a = (a_1, \cdots, a_n)$ and $b = (b_1, \cdots, b_n)$ be in $\mathbb{N}^n$. Then $a >_{grevlex} b$ which is equivalent to $x^a >_{grevlex} x^b$ if $|a| = \sum a_i > |b| = \sum b_i$ or $|a| = \sum a_i = |b| = \sum b_i$ and the last nonzero entry in $a - b$ is negative.

Example 1.5.

---

(1) For the ring of polynomials in 1 variable, $k[x]$monomial order is $x^a > x^{a-1} \cdots > x > 1$.

(2) For polynomials in 2 variables, $k[x, y]$
LEX order: $x > y$, $x^3 > x^2y > xy^3 > x > y^3 > y^2 > y > 1$
GrLEX: $x > y$, $xy^3 > x^3 > x^2y > y^3 > y^2 > x > y > 1$ which is the same for GrevLEX.

Definition 1.6. Let $f = \sum_a \lambda_a x^a$ be polynomial in $R = k[\bar{x}]$ and $>$ a monomial order on R then

(a) the multidegree of f denoted by multideg(f) is given by $\text{multideg}_>(f) = \max(a \in \mathbb{N}^n)\}$ (the largest degree with respect to $>$)

(b) the leading monomial of f denoted by $LM(f)$ is $x^{multideg(f)}$

(c) the leading coefficient of the leading monomial denoted by $LC(f)$ and is given by $\lambda_{multideg(f)}$

(d) the leading term of f, $LT(f) = LC(f).LM(f)$.

Exercise 1.7.

(1) Order the following polynomials using LEX, GrLEX, GrevLEX and weighted order for given weights:
   (a) $3x - 4y + 6z + 10x^3 - xz + y^3$

   (b) $2x^3y^5z^2 - 3x^4yz^5 + xyz^3 - xy^4$

   (c) $xyz^4 - 5yz^5 + x^3y^3 + y^2z^4$

   (d) $9x^3y - 7xy^2z + x^2yz$

(2) Determine the monomial order used for each of the following:
   (a) $7x^2y^4z - 2xy^6 + x^2y^2$

   (b) $xy^3z + xy^2z^2 + x^2z^3$

   (c) $x^4y^5z + 2x^3y^2z - 4xy^2z^4$

(3) Determine if $f \in I$ given
   (a) $f = x^3 - 1$, $I = \langle x^6 - 1, x^5 + x^3 - x^2 - 1\rangle$
   (b) $f = x^5 - 4x + 1$, $I = \langle x \rangle$

Theorem 1. *Division Algorithm in $R = k[x_1, x_2, \cdots, x_n]$*
Fix monomial order on $\mathbb{N}^n$, and let $F = (f_1, f_2, \cdots, f_t)$ be an ordered tuple of n polynomials in R then for any $f \in R$ there exists $a_1, a_2, \cdots, a_t, r \in R$ such that f can be expressed as $f = a_1f_1 + a_2f_2 + \cdots + a_tf_t + r$ where $r = 0$ or a polynomial none of whose terms is divisible by the leading term of any f_i for all i and furthermore the multideg(f) $\geq$multideg(a_if_i).

Proof. Cox et al - Ideals, Varieties and Algorithms. □

2. Groebner bases properties

Definition 2.1. Initial Ideal
The set of initial terms denoted by $in_>(f)$ or $LT(f)$ is generates an ideal called the initial ideal of I which we denote by $\langle LT(I)\rangle = \{LT(f) : \forall f \in I\}$.

Definition 2.2. Let $G = \{g_1, \cdots, g_t\} \subset I$ is called a Groebner basis(GB) of the ideal I with respect to some order if $\langle LT(I)\rangle = \langle LT(g_1), \cdots, LT(g_t)\rangle$.

Remark 2.3. *If $I = \langle g_1, \cdots, g_t\rangle$ then $\langle LT(g_1), \cdots, LT(g_t)\rangle \subseteq \langle LT(I)\rangle$.*

Example 2.4.

Let $I = \langle x^2, xy - y^2\rangle$, $f = x^2y$, setting $F = (x^2, xy - y^2)$ ordered (lex) we divide f by F.
In once case $f = y(x^2) + 0(xy - y^2) + 0$ i.e. zero remainder. In the other case we will get $x(x^2) + y(xy - y^2) - y^3$.
From we here we observe 2 things, one is that the remainder is not necessarily unique on division of f by F. Secondly we not that $y^3 \in I$ since it is a linear combination of generators of I. Also $y^3 \in LT(I)$ but $y^3 \notin \langle x^2, xy\rangle = \langle LT(x^2), LT(xy - y^2)\rangle$ and so we conclude that F is not a GB for I.

Definition 2.5. Monomial Ideal
An ideal $I \lhd R$ is called a monomial ideal if there exists a subset A of $\mathbb{N}^n$ such that $I = \langle x^\alpha : \alpha \in A\rangle$.

Example 2.6.

$I = \langle x^4y^2, x^3y^4, x^2y^5\rangle \lhd k[x, y]$.

Lemma 2.7. *Let $I = \langle x^\alpha : \alpha \in A\rangle$ then $x^\beta \in I \iff x^\alpha$ divides x^α.*

Lemma 2.8. *Dickson's Lemma*
Let $I = \langle x^\alpha : \alpha \in A \subset \mathbb{N}^n\rangle \lhd R$ be a monomial ideal then I can be writen in the form $I = \langle x^{\alpha_1}, \cdots, x^{alpha_s}\rangle$ where $\alpha_i \in A$ for all i. That is every monomial ideal I has a finite generating set.

Exercise 2.9. *Draw the ideal $I = \langle x^4y^2, x^3y^4, x^2y^5\rangle \lhd k[x, y]$ on the graph of $\mathbb{N}^2$ where (m, n) corresponds to the monomial x^my^n and determine a generating set for I.*

Proposition 2.10. *If $G = \{g_1, g_2, \cdots, g_t\} \in I \lhd R$ is groebner basis then it generates I i.e. $\langle G\rangle = I$.*

Proof. Since $\{g_1, g_2, \cdots, g_t\} \in I$ then $\langle g_1, g_2, \cdots, g_t\rangle \subseteq I$.
Now suppose $f \in I$ then by division algorithm in R we can express f as
$f = a_1g_1 + a_2g_2 + \cdots + a_tg_t + r$ where $r = 0$ or is a polynomial none of whose terms is divisible by any $LT(g_i)$ for all i and $a_i \in R$.
Now if $r = 0$ then $f = \sum a_ig_i \in \langle G\rangle$ and we are done. If $r \neq 0$ then we have $r = f - a_1g_1 - a_2g_2 - \cdots - a_tg_t$ and so $LT(r) \in \langle LT(I)\rangle = \langle G\rangle$ i.e. $LT(r)$ is divisible by some $LT(g_i)$ which is a contradiction and so $r = 0$. Hence $I = \langle G\rangle$. □

Theorem 2. *Every Ideal $I \lhd R = k[x_1, x_2, \cdots, x_n]$ has a groebner basis.*

Proof. The initial ideal $\langle I\rangle$ is a monomial ideal i.e. generated by monomial, $LT(f)$, $f \in I$ and Dickson's lemma it is finitely generated i.e. there exists $g_1, g_2, \cdots, g_t \in I$ such that $\langle I\rangle = \langle LT(g_1), \cdots, LT(g_t)\rangle$ and this is the definition of a groebner basis and by the proposition above it generates I □

Theorem 3. *Hilbert Basis Theorem*
Every Ideal $I \lhd R = k[x_1, x_2, \cdots, x_n]$ is finitely generated.

Proof. Choose a monomial order on R and determine a groebner basis G for an ideal I then G finitely generates I. □

Proposition 2.11. *Let $G = \{g_1, g_2, \cdots, g_t\}$ be a groebner basis for an ideal I of R and let $f \in I$. Then there is a unique $r \in R$ satisfying*

(a) *No term of r is divisible by any $LT(g_i)$ for all i and*
(b) *there exists $g \in I$ such that $f = g + r$*

Proof. Division algorithm gives $f = \sum a_i g_i + r$ so r is the remainder with $r = 0$ or satifies (i) and now set $g = \sum a_i g_i \in I$.
Now for uniqeness of r, suppose $f = g+r$ and $f = g+r'$ from which we have $r-r' = g'-g \in I$ if $r \neq r'$ then $LT(r - r') \in \langle LT(I)\rangle = \langle LT(g_1), \cdots, LT(g_t))\rangle$
which implies that $LT(r - r')$ is divisible by some $LT(g_i)$ which is a contradiction. □

3. How to determine a groebner basis

Given a set $F = \{f_1, \cdots, f_s\} \subset I \lhd R$ and $f \in R$ we shall denote by $\bar{f}^F$ the remainder on division of f by F.

Definition 3.1. S-polynomials
Let $\alpha = (\alpha_1, \cdots, \alpha_n)$ and $\beta = (\beta_1, \cdots, \beta_n) \in \mathbb{N}^n$, and $\gamma = (\gamma_1, \cdots, \gamma_n)$ where $\gamma_i = \max(\alpha_i, \beta_i)$ and also $\{f_1, f_2, \cdots, f_t\} \in I$, an ideal then the $S-$polynomial of f_i and f_j denoted by $S(f_i, f_j)$ for all $i \neq j$ is defined as $S(f_i, f_j) = \frac{x^\gamma}{LT(f_i)} f_i - \frac{x^\gamma}{LT(f_j)} f_j$.

Theorem 4. *BUCHBERGER'S CRITERION*
A subset $G = \{g_1, \cdots, g_t\}$ of an ideal $I \lhd R$ is a groebner basis for $I \iff$ the remainder on divison of $S(g_i, g_j$ by G is zero for all $i \neq j$.

Proof. Cox. □

Theorem 5. *BUCHBERGER'S ALGORITHM*
Let $I = \langle f_1, f_2, \cdots, f_s\rangle \neq 0 \lhd k[\bar{x}]$, then a groebner basis for I can be constructed in a finite number of stepsby the following algorithm:
ALGORITHM:
INPUT: $F = (f_1, \cdots, f_s)$
OUTPUT: groebner basis $G = (g_1, \cdots, g_t)$ for I
Let $G := F$
Repeat
Let $G' := G$
For each pair $\{p, q\}$, $p \neq q$ in G'
Do let $S := \bar{S(p,q)}^{G'}$, the remainder of division of $S(p, q)$ by G'
if $S \neq 0$
then $G := G \cup \{S\}$
UNTIL $G = G'$

Remark 3.2.

We basically compute the S-polynomials then check for each nonzero remainder, add it to the starting generating set and keep repeating the process until there are no more nonzero remainders, the set obtained is a groebner basis which may be unnecessarily large. We can therefore apply the lemma below to reduce it.

Lemma 3.3. *Let $G = \{g_1, \cdots, g_s\}$ be a groebner basis for an ideal I and $p \in G$ such that $LT(p) \in \langle LT(G - \{p\}) \rangle$ then $G - \{p\}$ is a groebner basis.*

Proof. left as an exercise. □

Exercise 3.4. *Groebner Basis construction*

(1) *Given the ideal $I = \langle x^2 - y, x^3 - z \rangle$ with lex order, determine a groebner basis for I.*

(2) *Given the ideal $I = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$, w.r.t grlex order determine a groebner basis for I.*

(3) *Is the set $\{xy + 1, y^2 - 1\}$ a groebner basis for $I = \langle xy + 1, y^2 - 1 \rangle \lhd k[x, y]$?*

Lemma 3.5. *A groebner basis $G = \{g_1, \cdots, g_t\}$ is said to be minimial if*

(a) *Each g_i is monic and*

(b) *There is no $p \in G$ such that $LT(p) \in \langle LT(G - \{p\}) \rangle$*

Remark 3.6.

(a) A minimial groebner basis is not unique.

(b) Two minimal groebner bases must have the same cardinality.

(c) Every ideal $I \lhd R = k[x_1, \cdots, x_n]$ has a unique reduce groebner basis. The next lemma aids us in that.

Lemma 3.7. *A groebner basis $G = \{g_1, \cdots, g_t\}$ is said to be reduced if*

(a) *Each g_i is monic and*

(b) *There is no term of $p \in G$ is divisible by any $LT(g_i)$.*