GRÖBNER BASES AND POLYNOMIAL EQUATIONS

J. K. VERMA

1. Introduction and preliminaries on Gróbner bases

Let $S = k[x_1, x_2, \ldots, x_n]$ denote a polynomial ring over a field k where $x_1, x_2, \ldots, x_n$ are indeterminates. A Gröbner basis is a set of polynomials in S which has several remarkable properties which enable us to carry out standard operations on ideals, rings and modules in an algorithmic way. Every set of polynomials in S can be transformed into a Gröbner basis. This process generalises three important algorithms:
(1) Gauss elimination method for solving a system of linear equations,
(2) Euclid's algorithm for finding the greatest common divisor and
(3) The simplex method of linear programming.
One of the goals of these two lectures is to explain how to reduce the problem of solving a system of polynomial equations to a problem of finding eigenvalues of commuting matrices. We will introduce term orders first on the set of monomials in S and define the concept of Gróbner basis of an ideal.

Term orders on monomials in $k[x_1, x_2, \ldots, x_n]$

The set of monomials in the polynomial ring $S = k[x_1, x_2, \ldots, x_n]$ is:

$$\text{Mon}(S) = \{x^a = x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} \mid (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n\}.$$

Definition 1.1. *By a* **term order** *on Mon(S) we mean a total order $<$ on Mon(S) which satisfies the following two conditions: (a) $1 < x^a$ for all nonzero $a \in \mathbb{N}^n$, (b) If $x^a < x^b$ then $x^c x^a < x^c x^b$ for all $a, b, c \in \mathbb{N}^n$.*

Remark 1.2. If m, n, p are monomials different from 1 and $m = np$ then $n < m$ for any monomial order. Indeed, $1 < p$ and hence $n < np = m$.

Examples of term orders

Lexicographic order : The lexicographic order on Mon(S) with $x_1 > x_2 > \cdots > x_n$ is defined as follows: Let $a, b \in \mathbb{N}^n$. Define $x^a < x^b$ if the first nonzero coordinate of $a - b$ from the left is negative. For example if $x < y$ then the total ordering on all monomials in x, y is

$$1 < x < x^2 < x^3 < \cdots < y < xy < x^2 y < \cdots < y^2 < \cdots .$$

Degree lexicographic order: We define $x^a < x^b$ in degree lexicographic order for $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n) \in \mathbb{N}^n$ if $\deg x^a < \deg x^b$ or if $\deg x^a = \deg x^b$ then $x^a < x^b$ in lexicographic order.

Degree reverse lexicographic order: Let $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ and $\beta = (\beta_1, \beta_2, \dots, \beta_n) \in \mathbb{N}^n$. We define $x^\alpha < x^\beta$ in degree reverse lexicographic if either $\deg x^\alpha < \deg x^\beta$ or if $\deg x^\alpha = \deg x^\beta$ then there the first nonzero coordinate in $\alpha - \beta$ from the right is positive. In this order, $x_1 > x_2 > \cdots > x_n$.

Remark 1.3. The deglex and degrevlex orders are same for monomials in two variables. But they differ for three variables. For example

$$x_1^2 x_2 x_3 >_{deglex} x_1 x_2^3 \text{ but } x_1^2 x_2 x_3 <_{degrevlex} x_1 x_2^3.$$

The support of a polynomial $f(x) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha$ is the set

$$\operatorname{supp}(f) = \{x^\alpha \mid a_\alpha \neq 0\}.$$

The initial monomial $in(f)$ **of a polynomial** f is

$$in(f) = x^\alpha \text{ if } x^\alpha > x^\beta \text{ for all } x^\beta \in \operatorname{supp}(f).$$

The leading term of f, denoted by $lt(f)$ is the term $a_\alpha x^\alpha$ where $in(f) = x^\alpha$.
The initial ideal of an ideal: Let I be a nonzero ideal of R. The **initial ideal** of I with respect to a given monomial order is defined by

$$in(I) = (in(f) \mid f \in I \setminus \{0\}).$$

Example 1.4. If $I = (f_1, f_2, \dots, f_s)$ is an ideal of S then the initial ideal of I may not be generated by $in(f_1), in(f_2), \dots, in(f_s)$. Consider the ideal
$I = (x_1^2 - x_2, x_1)$ in $k[x_1, x_2]$ under lexicographic order. Then $in(x_1^2 - x_2) = x_1^2$ and $in(x_1) = x_1$. Hence $(in(x_1^2 - x_2), in(x_1)) = (x_1)$. But $x_2 \in in(I) \setminus (in(x_1^2 - x_2), in(x_1))$.

Gröbner basis of an ideal: Let I be an ideal of $S = k[x_1, x_2, \dots, x_n]$. Let $<$ be a monomial order on S. A set of polynomials $g_1, g_2, \dots, g_m \in I$ is called a Gröbner basis of I with respect to the monomial order $<$ if

$$in(I) = (in(g_1), in(g_2), \dots, in(g_m)).$$

Proposition 1.5. *Every ideal I has a Gröbner basis.*

Proof. By the Hilbert basis theorem, the ideal $in(I)$ is finitely generated. Let for some $g_1, g_2, \dots, g_m \in I$, the initial ideal of I be given by $in(I) = (in(g_1), in(g_2), \dots, in(g_m))$. Then $g_1, g_2, \dots, g_m$ is a Gröbner basis of I. □

Definition 1.6 (Reduced Gröbner basis of an ideal:). *A Gröbner basis G of I is called* **reduced** *if the coefficients of initial monomials of polynomials in G are* 1 *and $in(I)$ cannot be generated by a proper subset of $\{in(g_1), \dots, in(g_m)\}$.*

Reduced Gröbner Basis of an ideal

Lemma 1.7. (1) *There is no infinite descending chain of monomials in S with respect to any term order.*
(2) *Any nonempty subset of monomials in S has a minimal element.*

Proof. Let $m_1 > m_2 > \cdots$ be an infinite descending chain of monomials. By Hilbert basis theorem the ideal generated by these monomials is finitely generated. Therefore there a j such that $m_j \in (m_1, m_2 \ldots, m_{j-1})$. Hence $m_j = nm_i$ for some monomial n and $i = 1, 2, \ldots, j-1$. Therefore $m_i < m_j$ which is a contradiction. □

Theorem 1.8. *Let I be a nonzero ideal of R with a monomial order $<$. Then*
(1) *I has a reduced Gröbner basis.*
(2) *Reduced Gröbner basis of I is unique.*
(3) *If G is a Gröbner basis of I, then $I = (G)$.*

Proof. Existence of reduced Gröbner basis is clear. Let G be a Gröbner basis of I. If $I \neq (G)$ then the set of initial monomials of $f \in I \setminus (G)$ has a minimal element, say $in(h)$. But $in(h) \in in(I)$. Hence there is a $g \in G$ such that $in(g) \mid in(h)$. Write $in(h) = in(g)m$ for some monomial m. Consider $f = h - mg$ Then $f \in I \setminus (G)$ and $in(f) < in(h)$. Therefore $in(h) > in(g)$. This is a contradiction. Hence $I = (G)$. □

Gröbner basis and division algorithm

Theorem 1.9 (Euclid's Division Algorithm). *For a polynomial $f(x) \in k[x]$ and a nonzero polynomial $g(x)$ we have a unique remainder $r(x)$ such that*

$$f(x) = q(x)g(x) + r(x).$$

The remainder $r(x)$ is either zero or $\deg r(x) < \deg g(x)$.

We may restate the condition $\deg r < \deg g$, as: no term in $r(x)$ is divisible by $in(g(x))$.

Theorem 1.10 (Multivariate Division Algorithm:). *Let $G = \{g_1, g_2, \ldots, g_m\}$ be a Gröbner basis of the ideal they generate. Then $f \in S$ can be written as*

$$f = q_1 g_1 + q_2 g_2 + \cdots + q_m g_m + r$$

for some $q_1, q_2, \ldots, q_m \in S$ and $r = 0$ or no term in r is divisible by any $in(g_i)$ for all $i = 1, 2, \ldots, m$. The remainder r, which is unique, is called the **normal form of f with respect to** G *and we write it as $r = N_G(f)$.*

Buchberger's Algorithm for Gröbner basis

Definition 1.11 (The S-polynomial). *Let f, g be nonzero polynomials in $S = k[x_1, x_2, \ldots, x_n]$. The S*-**polynomial of** f **and** g *is the polynomial*

$$S(f,g) = \frac{lcm\ (in(f), in(g))}{lt(f)} f - \frac{lcm\ (in(f), in(g))}{lt(g)} g.$$

Theorem 1.12 (Buchberger's Theorem). *Let $G = \{g_1, g_2, \ldots, g_t\}$ be a set of nonzero polynomials in S.*

(1) *The set G is a Gröbner basis of the ideal $I = (g_1, g_2, \ldots, g_t)$ if and only if for all $i \neq j$, the normal forms of $S(g_i, g_j)$ with respect to G are zero.*
(2) *Let $I = (f_1, f_2, \ldots, f_s)$ be an ideal of S. Add to $F = \{f_1, f_2, \ldots, f_s\}$ the normal forms of all the S-polynomials of pairs of polynomials in F with respect to F. Repeat this until a Gröbner basis is produced.*
(3) *Every nonzero ideal of S has a unique reduced Gröbner basis of I with respect to the given term order on S.*

Construction of a basis of $k[x_1, x_2, \ldots, x_n]/I$

Definition 1.13. *A polynomial $f \in S$ is called* **reduced with respect to a Gröbner basis** G *if no term in f is divisible by $in(g)$ for all $g \in G$. A monomial $m \in S$ is called* **standard with respect to** G *if $m \notin in(I)$.*

Proposition 1.14. *Let I be an ideal of S. Then*

(1) *$S/I = \{N_G(f) + I \mid f \in S\}$. Moreover $f + I = h + I$ if and only if $N_G(f) = N_G(h)$.*
(2) *In particular the residue classes of standard monomials are a basis of the k-vector space S/I.*

Proof. (1) Let $f \in S$. Then by division algorithm $f = q + N_G(f)$ where $q \in I$ and $N_G(f)$ is reduced with respect to G. Hence $f + I = N_G(f) + I$.
(2) Let $f + I = h + I$. Write $f = q + N_G(f)$ and $h = r + N_G(h)$. for some $q, r \in I$. Then $f - h = q - r + N_G(f) - N_G(h) \in I$. Hence $N_G(f) - N_G(h) \in I$. But $N_G(f), N_G(h)$ are reduced with respect to G. Hence $N_G(f) = N_G(h)$.
(3) Since $N_G(f)$ is a k-linear combination of the standard monomials with respect to G, the residue classes of these form a basis of the vector space S/I. □

2. Solving systems of polynomial equations

Consider a system $\mathcal{S}$ of polynomial equations with complex coefficients:

$$
\begin{aligned}
f_1(x_1, x_2, \ldots, x_n) &= 0 \\
f_2(x_1, x_2, \ldots, x_n) &= 0 \\
&. \\
f_s(x_1, x_2, \ldots, x_n) &= 0
\end{aligned}
$$

It is natural to ask (1) if $\mathcal{S}$ has a solution? (2) How to find if $\mathcal{S}$ has finite or infinite number of solutions? (3) If $\mathcal{S}$ has finitely many solutions, how to find them efficiently?

Gauss Elimination and Gröbner Bases: Consider a system of linear equations:

$$\begin{aligned} 3x - 6y - 2z &= 0 \\ 2x - 4y + 4w &= \\ x - 2y - z - w &= 0 \end{aligned}$$

The row echelon form of the coefficient matrix is:

$$\begin{bmatrix} 1 & -2 & -1 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

If we use the lex order with $x > y > z > w$, then the linear forms $x - 2y - z - w, z + 3w$ corresponding to the rows of the echelon form matrix above constitute a Gröbner basis of the ideal $(3x - 6y - 2z, 2x - 4y + 4w, x - 2y - z - w)$.

Ideals and Varieties

Let $R = \mathbb{C}[x_1, x_2, \ldots, x_n]$ be the polynomial ring. Let $\mathcal{F} = \{f_1, f_2, \ldots, f_s\}$ be a subset of polynomials in R. The **variety** defined by $\mathcal{F}$ is

$$\mathscr{V}(\mathcal{F}) = \{z \in \mathbb{C}^n \mid f_1(z) = f_2(z) = \cdots = f_s(z) = 0\}.$$

The **ideal** of R generated by $\mathcal{F}$ is the set of polynomials

$$(\mathcal{F}) = \{f_1 g_1 + f_2 g_2 + \cdots + f_s g_s \mid g_1, g_2, \ldots, g_s \in R\}.$$

Note that $\mathscr{V}(\mathcal{F}) = \mathscr{V}((\mathcal{F}))$. If $V \subseteq \mathbb{C}^n$ then the ideal of V is defined as

$$\mathscr{I}(\mathscr{V}) = \{f \in \mathbb{C}[x_1, x_2, \ldots, x_n] \mid f(p) = 0 \text{ for all } p \in V\}.$$

It is easy to see that $\mathscr{I}((a_1, a_2, \ldots, a_n)) = \mathfrak{m}_a = (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$.

Existence of Solutions: Hilbert's Nullstellensatz

Theorem 2.1. (1) **The Weak Nullstellensatz:** *The system of equations*

$$f_1(z) = f_2(z) = \cdots = f_s(z) = 0$$

has no solution $\Leftrightarrow 1 = f_1 g_1 + f_2 g_2 + \cdots + f_s g_s$ *for some* $g_1, g_2, \ldots g_s \in R$.
(2) **The Strong Nullstellensatz:** *If* J *be an ideal of* $R = \mathbb{C}[x_1, x_2, \ldots, x_n]$ *then*

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

(3) **Constructive Hilbert's Nullstellensatz:** *Let* I *be an ideal of* $\mathbb{C}[x_1, x_2, \ldots, x_n]$ *with reduced Gröbner basis* G. *Then* $\mathscr{V}(I) = \emptyset$ *if and only if* $G = \{1\}$.

Finiteness Theorem for Polynomial Equations

Theorem 2.2 (**The Finiteness Theorem:**). *Let I be a proper ideal of the ring $S = \mathbb{C}[x_1, x_2, \dots, x_n]$. Then the following are equivalent:*
(1) *$\mathscr{V}(I)$ is a finite set.*
(2) *S/I is a finite dimensional complex vector space.*
(3) *I has a Gröbner basis G having $g_1, g_2, \dots, g_n \in G$ such that $in(g_i) = x_i^{d_i}$ for $i = 1, 2, \dots, n$.*

Proof. (1) $\Rightarrow$ (2): Suppose $\mathscr{V}(I)$ is finite. Let $a_1, a_2, \dots, a_k$ be the i^{th} coordinates of all the points in $\mathscr{V}(I)$. Then $f(x_i) = (x_i - a_1)(x_i - a_2)\cdots(x_i - a_k)$ vanishes at every point of $\mathscr{V}(I)$. By Hilbert's Nullstellensatz, there is a d_i so that $f(x_i)^{d_i} \in I$. Let $d = \max\{kd_1, kd_2, \dots, kd_n\}$. Then $[x_i^d] \in S/I$ for each variable x_i can be expressed in terms of residue classes of lower powers of x_i. Hence S/I has a basis of residue classes of monomials in which powers of all variables are bounded. Therefore S/I is finite dimensional.
(2) $\Rightarrow$ (3): Now let S/I be a finite dimensional complex vector space. Consider the residue classes

$$[1], [x_1], [x_1^2], \dots .$$

Since S/I is finite dimensional, these must be linearly dependent. Hence there are complex numbers $\alpha_0, \alpha_1, \alpha_2, \dots \alpha_t$, not all zero, such that

$$\alpha_0[1] + \alpha_1[x_1] + \alpha_2[x_1^2] + \ldots + \alpha_t[x_1^t] = 0.$$

Hence $f_1(x_1) = \alpha_0 + \alpha_1 x_1 + \alpha_2 x_1^2 + \cdots + \alpha_t x_1^t \in I$. Therefore, $x_1^t \in in(I)$. Similarly some power of each variable is in $in(I)$.
(3) $\Rightarrow$ (1): Let G be a Gröbner basis of I containing g_i so that $in(g_i) = x_i^{d_i}$ for $i = 1, 2, \dots, n$. Hence $g_i \in \mathbb{C}[x_i, x_{i-1}, \dots, x_1]$. This shows that $\mathscr{V}(I)$ is finite. □

The Number of solutions

Definition 2.3 (**The Interpolation polynomials**). *Let $p_1, p_2, \dots, p_m \in \mathbb{C}^n$. Then there exist $g_1, g_2, \dots, g_m$ called the* **interpolation polynomials** *so that*

$$g_i(p_j) = 0 \ \text{ for } j \neq i \text{ and } g_i(p_i) = 1 \text{ for all } i = 1, 2, \dots, n.$$

Theorem 2.4. *Let I be an ideal of $R = \mathbb{C}[x_1, x_2, \dots, x_n]$. If $\mathscr{V}(I)$ is finite then*

$$|\mathscr{V}(I)| \leq \dim_{\mathbb{C}} R/I$$

and equality holds if and only if $I = \sqrt{I}$.

Proof. Let $\mathscr{V}(I) = \{p_1, p_2, \dots, p_m\} \subset \mathbb{C}^n$. Define the linear transformation

$$\phi : R/I \to \mathbb{C}^m, \ \ \phi([f]) = (f(p_1), f(p_2), \dots, f(p_m)).$$

Then the Kernel $\phi = \{[f] \mid f(p_i) = 0 \text{ for all } i = 1, 2, \dots, m\} = \sqrt{I}/I$. Hence $m = |\mathscr{V}(I)| \leq \dim_{\mathbb{C}} R/I$. Therefore equality holds if and only if $I = \sqrt{I}$. □

Theorem 2.5 (**Stickelberger**). *Let I be an ideal of $R = \mathbb{C}[x_1, x_2, \ldots, x_n]$ with $\mathscr{V}(I)$ finite. Then*

$$\mathscr{V}(I) = \{(a_1, a_2, \ldots, a_n) \mid m_{x_i}([g]) = a_i[g] \text{ for all } i \text{ and } [g] \neq 0\}.$$

Proof. Let $\mathscr{V}(I) = \{P_1, P_2, \ldots, P_m\}$ and $(a_1, a_2, \ldots, a_n) = P_1$. Let $g_1, g_2, \ldots, g_m$ be the interpolation polynomials for the points $P_1, P_2, \ldots, P_m$ Then

$$(x_i g_1 - a_i g_1)(P_1) = 0 \text{ and } (x_i g_1 - a_i g_1)(P_j) = 0 \text{ for } j \neq 1$$

Hence $x_i g_1 - a_i g_1 \in I$ for all $i = 1, 2, \ldots, n$. Therefore $m_{x_i}([g_1]) = a_i[g_1]$ for all i. Conversely, let $a = (a_1, a_2, \ldots, a_n)$ and $m_{x_i}([g]) = a_i[g]$ for $[g] \neq 0$.
Let $f \in I$. We wish to prove that $f(a_1, a_2, \ldots, a_n) = 0$. Since

$$f(m_{x_1}, m_{x_2}, \ldots, m_{x_n})([g]) = f(a_1, a_2, \ldots, a_n)[g]$$

and $[f] = 0$, it follows that $f(a) = 0$. □

Theorem 2.6 (**The Eigenvector Theorem**). *Let I be a radical ideal with $V(I) = \{p_1, p_2, \ldots, p_m\}$. Let $g_1, g_2, \ldots, g_m$ be interpolation polynomials for $V(I)$. For $g \in R$ define $m_g : R/I \to R/I$ by $m_g([f]) = [fg]$ for all $f \in R$. Then $\{[g_1], [g_2], \ldots, [g_m]\}$ is a basis of eigenvectors for m_g with eigenvalues $\{g(p_1), g(p_2), \ldots, g(p_m)\}$.*

Proof. Let $V(I) = \{P_1, P_2, \ldots, P_m\}$. Let $g \in R$. We show that $[g_i]$ is an eigenvector of the linear map $m_g : R/I \to R/I$ with eigenvalue $g(P_i)$ for $i = 1, 2, \ldots, m$. Observe that for all j,

$$(gg_i - g(P_i)g_i)(P_j) = g(P_j)g_i(P_j) - g(P_i)g_i(P_j) = 0$$

Hence the polynomial $f = gg_i - g(P_i)g_i$ vanishes at each point of $V(I)$. Therefore by Nullstellensatz, $f \in I$ as I is a radical ideal. So $[gg_i - g(P_i)g_i] = 0$. Hence $[gg_i] = [g(P_i)g_i]$. Therefore $m_g[g_i] = g(P_i)[g_i]$ for all i.

□

References

[1] David A. Cox, John Little and Donald O'Shea, *Using Algebraic Geometry,* Springer(2005).

[2] David A. Cox, *Introduction to Gröbner bases,* Applications of computational algebraic geometry (San Diego, CA, 1997), 1–24, Proc. Sympos. Appl. Math., 53.

[3] P. Pedersen, M.-F. Roy and A. Sziprglas, *Counting real zeros in the multivariate case,* Computational Algebraic Geometry, F. Eyssette and A. Galligo, editors, Birkhäuser, Boston (1993), 203-224.

[4] Bernd Sturmfels, *Polynomial equations and convex polytopes,* American Mathematical Monthly 105 (1998) 907-922.

[5] Bernd Sturmfels, *Solving Systems of Polynomial Equations,* American Mathematical Society (2002).

Dept. of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400 076
E-mail address: jkv@math.iitb.ac.in