Hilbert Basis Theorem and Grobner Basis for Polynomial Ideals

Lwin Mar Htun[1] and Sandar[2]

Abstract

This paper is an exposition of Hilbert Basis Theorem and Grobner Basis. We first recall some basis concepts of the ideal theory and Hilbert Basis theorem for Polynomial ideals.

Hilbert Basis Theorem states that every polynomial ideal is finitely generated. Then we discuss the Grobner Basis for polynomial ideals which is an essential tool for computational Algebraic Geometry.

1. Ring and Ideals

In this paper, rings will be commutative rings with unit element. N will denote the set of non-negative integers.

1.1 Definition. A nonempty subset I of a ring R is called an **ideal** of R if

(i) I is a subgroup of R under addition,

(ii) $RI \subset I$ (i.e., for any $r \in R$ and for any $a \in I$, we have $ra \in I$).

1.2 Definition. Let R be a ring and B a subset of R. The **ideal generated by B**, denoted by $< B >$ is the smallest ideal containing B. Equivalently $< B >$ is the intersection of all ideals that contain B. $< B >$ has the form

$$RB = \{r_1b_1 + \ldots + r_nb_n : r_i \in R \text{ and } b_i \in B, n \in N \text{ for all } i = 1, 2, \ldots, n\}.$$

An ideal I in a ring R is said to be **finitely generated** if there exists a finite set $\{b_1, b_2, \ldots, b_n\}$ such that $< b_1, b_2, \ldots, b_n > = I$.

2. Multivariate polynomials

2.1 Definition. A multi index α is an n tuple $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are nonnegative integers.

Let $x_1, x_2, \ldots, x_n$ be n variables and let $x = (x_1, x_2, \ldots, x_n)$. Then

$$x^{\alpha} = (x_1, x_2, \ldots, x_n)^{(\alpha_1, \alpha_2, \ldots, \alpha_n)}$$

$$= x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$ is called a **monomial** in $x_1, x_2, \ldots, x_n$.

2.2 Definition. A **multivariate polynomial** f in n variables $x_1, x_2, \ldots, x_n$ with coefficients in a field K is a linear combination of the form

$$f(x_1, x_2, \ldots, x_n) = \sum_{\alpha} a_{\alpha} x^{\alpha}$$

of monomials x^{α} with coefficients a_{α} in K.

2.3 Definition. The set of all multivariate polynomials in $x_1, x_2, \ldots, x_n$ with coefficients in a field K is denoted by $K[x_1, x_2, \ldots, x_n]$. It can be easily verified that $K[x_1, x_2, \ldots, x_n]$ is a ring with respect to the usual addition and multiplication of polynomials. It is called a **polynomial ring.**

1. Professor /Head, Dr., Department of Mathematics, Yangon University of Education
2. Assistant Lecturer, Dr., Department of Mathematics, Yangon University of Education

2.4 Definition. Let $F = \{f_1, f_2, \dots , f_n\}$ be a finite set of polynomials in $K[x_1, x_2, \dots , x_n]$. Then F is called a **basis** for the ideal $< F > = < f_1, f_2, \dots , f_n>$ and the polynomials

$f_1, f_2, \dots , f_n$ are called **basis polynomials**. The ideal $< F >$ is said to be **finitely generated**.

2.5 Theorem (The Hilbert Basis Theorem). Every ideal in $K[x_1, x_2, \dots , x_n]$ is finitely generated [1].

3. Monomial ordering in $K[x_1, x_2, \dots , x_n]$

3.1 Definition. A **monomial ordering** in $K[x_1, x_2, \dots , x_n]$ is an order relation '< 'such that

(i) for any monomials m, n exactly one of the followings is true

$$m < n,\ n < m \text{ or } m = n,$$

(ii) for any monomials m_1, m_2 and m_3, if $m_1< m_2$ and $m_2< m_3$, then $m_1< m_3$,

(iii)for any monomials $m\neq 1$, $1< m$,

(iv)for any monomials m_1 and m_2, if $m_1< m_2$, then $nm_1< nm_2$ for any monomial.

3.2 Definition(Lexicographic order). Let α and β be two multi indices. We define the **Lexicographic order ($>_{Lex}$)**

$$\alpha >_{Lex} \beta \text{ if and only if the first nonzero component in } \alpha - \beta \text{ is positive.}$$

For example,

$$\alpha = (2, 1) >_{Lex} (1, 7) = \beta$$

$$\alpha = (2, 3, 1) >_{Lex} (2, 1, 7) = \beta.$$

Before defining an ordering among the monomials in $K[x_1, x_2, \dots , x_n]$, we agree that

$$x_1< x_2< \dots < x_n.$$

3.3 Definition. Let $m_1 = x^{\alpha} = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ and $m_2 = x^{\beta} = x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n}$ be two monomials in $K[x_1, x_2, \dots , x_n]$. We define **Lexicographic order ($>_{Lex}$)**

$$m_1 >_{Lex} m_2 \text{ if and only if } \alpha > \beta.$$

For example, $m_1 = x^2y^3z^5 >_{Lex} x^1y^4z^6 = m_2$

$$m_1 = x > yz = x^0y^1z^1 = m_2.$$

3.4 Definition. The **multidegree** of a monomial $x^{\alpha} = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ is defined to be the multiindex $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$.

The **total degree** of x^{α} is defined to be the **length** $|\alpha| = \alpha_1 + \alpha_2 + \dots + \alpha_n$ of the multiindex $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$.

3.5 Definition. Let '<' be amonomial ordering on $K[x_1, x_2, \dots , x_n]$. Let f be a nonzero polynomial in $K[x_1, x_2, \dots , x_n]$ of the form

$$f = c_1m_1 + c_2m_2 + \dots + c_km_k$$

where $c_i \in K$, $c_i \neq 0$ for $i = 1, 2, \dots, k$ and $m_1, m_2, \dots, m_k$ are monomials such that $m_1 > m_2 > \dots > m_k$. Then we define

(i) the **leading coefficient** $LC(f) = c_1$,

(ii) the **leading monomials** $LM(f) = m_1$,

(iii) the **leading term** $LT(f) = LC(f).LM(f) = c_1m_1$.

3.6 Definition. If I is an ideal in $K[x_1, x_2, \dots, x_n]$, we define LM(I)-**the leading monomial** of I to be the ideal generated by LM(f), $f \in I$, i.e., $LM(I) = < LM(f) : f \in I >$.

3.7 Theorem(Division Algorithm). Let $F = \{f_1, f_2, \dots, f_m\}$ be a given ordered m-tuple of polynomials in $K[x_1, x_2, \dots, x_n]$. Then for every $f \in K[x_1, x_2, \dots, x_n]$ we have

$$f = a_1f_1 + a_2f_2 + \dots + a_mf_m + r$$

where $a_1, a_2, \dots, a_m, r \in K[x_1, x_2, \dots, x_n]$ and no term of r is divisible by $LT(f_1), \dots, LT(f_m)$. r is called the remainder of f when divided by F.

We will illustrate this theorem by the following example.

3.8 Example. Let $f(x, y) = xy^3 + x + y^2 + 3$ and let $F = (f_1, f_2)$, $f_1(x, y) = xy + 1$, $f_2(x, y) = -x+1$.

First we divide f by f_1:

$$\begin{array}{r|l} & \quad y^2 \\ \hline xy+1 & xy^3 + x + y^2 + 3 \\ & xy^3 + y^2 \\ \hline & \qquad x + 3 \end{array}$$

Now we divide the remainder x + 3 by f_2

$$\begin{array}{r|l} & \ -1 \\ \hline -x+1 & x + 3 \\ & x - 1 \\ \hline & \quad 4 \end{array}$$

So, we have

$$xy^3 + x + y^2 + 3 = y^2(xy+1) + (-1)(-x+1) + 4$$

$$f = a_1f_1 + a_2f_2 + r$$

4. Grobner Basis

Let $I = < f_1, f_2, \dots, f_n >$. Then LM(I) contains the leading monomials $LM(f_1), LM(f_2), \dots, LM(f_m)$, of the generators $f_1, f_2, \dots, f_m$ of I. So by Definition 3.6

we have

$$< LM(f_1), LM(f_2), \dots ,LM(f_m) > \subset LM(I).$$

This inclusion can be strict.

4.1 Example. Consider $f_1 = x^3y–xy^2+1$, $f_2 = x^2y^2– y^3+ 1$ with respect to the lexicographic ordering.

Let $I = < f_1, f_2>$. Then we have

$LM(f_1) = x^3y$, $LM(f_2) = x^2y^2$

and

$<LM(f_1), LM(f_2) > = <x^3y, x^2y^2> \subset LM(I)$.

Since $g = yf_1 – xf_2 = y(x^3y–xy^2+1)– x(x^2y^2– y^3+ 1) = x + y \in I$.

$LM(g) = x \in LM(I)$

But $x \notin < LM(f_1), LM(f_2) > = <x^3y, x^2y^2>$,

since any element in $<x^3y, x^2y^2>$ has total degree at least 4.

Thus

$< LM(f_1), LM(f_2) > \neq LM(I)$.

4.2 Definition. Let I be an ideal in $K[x_1, x_2, \dots , x_n]$. A **Grobner basis** for I is a set of generators for I whose leading monomials generate the ideal of all leading monomials LM(I).

That is

$I = < g_1, g_2, \dots , g_m> \Rightarrow < LM(g_1), LM(g_2), \dots ,LM(g_n)> =LM(I)$.

4.3 Theorem. If $\{g_1, g_2, \dots , g_m\}$ is a Grobner basis for an ideal I, then $<g_1, g_2, \dots , g_m>=I$.

Proof: Clearly $< g_1, g_2, \dots , g_m> \subset I$ since $g_i \in I$ for $i = 1, 2, \dots , m$.

Let $f \in I$. Then we have by the division algorithm

$f = a_1g_1+ a_2g_2+ \dots + a_mg_m+ r$

where no term in r is divisible by $LM(g_i)$ for any $i = 1, 2, \dots , m$.

If $r \neq 0$, $LM(r) \in LM(I) = < LM(g_1), LM(g_2), \dots ,LM(g_n) >$.

Then LM(r) must be divisible by some $LM(g_i)$.

This is a contradiction.

Hence $r = 0$ and $f = a_1g_1+ a_2g_2+ \dots + a_mg_m \in < g_1, g_2, \dots , g_m>$. □

Acknowledgements

We would like to express our deep and sincere gratitude to U Kyin Ko, Professor and Head (Rtd. Department of Mathematics, Yangon University) for giving us the opportunity to do research and providing invaluable guidance through this paper.

We also would like to express our sincere thanks which go to Pro-rectors, Dr. Pyone Pyone Aung and Dr. Kay Thwe Hlaing, Yangon University of Education for their permission to write this research paper.

References

1. A Cox, J, Little and D. O'Shes: Using Algebraic Geometry, 2^{nd} Ed, 2004.

2. D. S. Dummit and R.M. Foote, Abstract Algebras, Third Ed. John Wiley and Sons, 2004.

3. K. Moran, Grobner Bases and their Application Online Notes.