A Short Introduction to Gröbner Bases for Commutative Algebra

Soutrik Roy Chowdhury

Abstract

Gröbner bases, an important tool in both commutative and non-commutative algebra serve many purposes including it's main purpose to study the structure of A/I, where A is a K algebra and $I \subset A$ is an ideal. Gröbner bases can also think as an even more strong analogue to Euclidean algorithm for algebras with more than one generators. In this article, I will give a brief introduction to this theory in commutative case with examples.
Key words: Admissible ordering, Diamond lemma, Normal monomials, Buchberger's algorithm.

1 Introduction

Given a polynomial algebra $\mathbb{K}[x_1, x_2, \ldots, x_n]$ (where $\mathbb{K}$ is a field and $n \in \mathbb{N}$) and given an ideal I of our given polynomial algebra, we often face the question - given a polynomial $f \in \mathbb{K}[x_1, x_2, \ldots, x_n]$, whether it belong to I or not. For polynomials in one variable this is easy to compute as we can use our well known Euclidean algorithm but in case of a multivariable polynomial algebra, we face a big problem as our known division algorithm is not valid anymore. To deal with such problems and questions we are introduced to the concept of Gröbner bases.
We will begin this paper with some background materials require for our construction of Gróbner bases and then will define it and will state some terminologies regarding Gröbner bases. Later we will state the Diamond lemma and the computation of Gröbner basis for some algebras.

2 Background

Remark 2.0.1. We would like to point out that throughout this paper $a \cdot b = ab$ for any a, b belonging to either field, algebras etc. Sometime for our better understanding and to deal with some scenarios we use the multiplication symbol '$\cdot$'.

2.1 Algebras

Definition 2.1.1. An **algebra** is a vector space V (over a field $\mathbb{K}$) equipped with a multiplication $V \otimes V \to V$ with the following properties:

- $(x+y)z = xz + yz$ for $x, y, z \in V$
- $x(y+z) = xy + xz$ for $x, y, z \in V$
- $(ab)(xy) = (ax)(by)$ where $x, y \in V$ and $a, b \in \mathbb{K}$.

Example 2.1.1. Algebra of polynomials $\mathbb{K}[x_1, x_2, \ldots, x_n]$.

Definition 2.1.2. An algebra is **associative** if for the multiplication $\mu : V \otimes V \to V$ and for any $v_1, v_2, v_3 \in V$, we have the equality

$$\mu(\mu(v_1, v_2), v_3) = \mu(v_1, \mu(v_2, v_3)). \tag{1}$$

An associative algebra is called **commutative** if for any $v_1, v_2 \in V$ we have

$$\mu(v_1, v_2) = \mu(v_2, v_1). \tag{2}$$

Example 2.1.2. Algebra of commutative polynomials with either single or mutlivariables over a field $\mathbb{K}$ is an example of commutative associative algebra. We usually denote it by $\mathbb{K}[x_1, x_2, \ldots, x_n]$. However algebra of non-commutative polynomials are examples of non-commutative associative algebra and we usually denote it by $\mathbb{K}\langle x_1, x_2, \ldots, x_n\rangle$.

Definition 2.1.3. Let A be an algebra over a field $\mathbb{K}$. Then $I \subset A$ is a left ideal of A if:

1. $x - y \in I$ for any $x, y \in I$.
2. $ax \in I$ for any $a \in A$ and any $x \in I$.

Similarly $I \subset A$ is a right ideal of A if condition 1 holds and $xa \in I$ for any $a \in A$ and $x \in I$. I is a both-sided (more generally 'an ideal') ideal if it is left as well as right ideal.

2.2 Motivation

Suppose we have a commutative polynomial algebra in one variable, say $\mathbb{K}[x]$ where $\mathbb{K}$ is the ground field. Suppose we have an ideal I of that ring $\mathbb{K}[x]$. Our aim is to study the structure of $\mathbb{K}[x]/I$ in a constructive way. Later we will prove that the monomials not divisible by leading terms of the ideal I form a basis of $\mathbb{K}[x_1, x_2, \ldots, x_n]/I$. We will use such facts to get to know that given a polynomial $f \in \mathbb{K}[x]$, whether it belongs to the ideal I or not. Now for single variable case it's easy as single variable polynomial algebra $\mathbb{K}[x]$ is a Euclidean domain so we can perform Euclidean algorithm to know

whether f belongs to I or not. But in case of multivariable polynomial algebra $\mathbb{K}[x_1, x_2, \ldots, x_n]$. Suppose we have the same question: we have an ideal $I \subset \mathbb{K}[x_1, x_2, \ldots, x_n]$ and we are given a polynomial $f \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ and are asked whether f belongs to I or not. Now here the case is difficult as multivariable polynomial algebra $\mathbb{K}[x_1, x_2, \ldots, x_n]$ is neither a Euclidean domain nor a principal ideal domain.

Lemma 2.2.1. *The polynomial algebra $\mathbb{K}[x_1, x_2, \ldots, x_n]$ is not a principal ideal domain for $n > 1$.*

Proof. Take an ideal generated by $\{X_1, X_2\}$. If f generates this ideal, then f divides both X_1 and X_2, so f is a constant term. So our ideal must be the entire ring. But 1 is in the algebra, but not in the ideal. Contradiction. □

To solve this problem we have the concept of Gröbner basis which is a type of basis defined carefully which tells that if we replace our generators f_i of the ideal I with a Gröbner basis g_j of the same ideal then we have the property that the remainder of f on division by the polynomials g_j is 0 if and only if f is in the ideal.
So we understand that to study the structure of $\mathbb{K}[x_1, x_2, \ldots, x_n]/I$ in a constructive way we require the concept of Gröbner bases.The original definition was given in Bruno Buchberger's PhD thesis in 1965 [1]. Before moving to the definition of Gröbner bases we require some preliminary materials:

3 Gröbner Bases

3.1 Preliminary materials

Theorem 3.1.1 (Hilbert basis theorem)**.** *$I \subset \mathbb{K}[x_1, x_2, \ldots, x_n]$ is always finitely generated, so there exist $f_1, f_2, f_3, \ldots, f_m \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ such that $I = (f_1, f_2, \ldots, f_m)$.*

Definition 3.1.1. An **admissible ordering** " $<$ " of monomials is a total ordering of all monomials in $\mathbb{K}[x_1, x_2, \ldots, x_n]$ such that

- it is a well ordering which is equivalent as saying that there is no infinite decreasing sequences.
- $m_1 < m_2 \Rightarrow m_1 m_3 < m_2 m_3$ for any monomial m_3, where $m_1, m_2 \in \mathbb{K}[x_1, x_2, \ldots, x_n]$.

Lemma 3.1.1. *There is only one admissible ordering of monomials in $\mathbb{K}[x]$ i.e.*

$$x^k < x^l \text{ if and only if } k < l$$

Proof. Proof of this is easy. We will take an ordering like this,

$$1 < x \text{ implies } x < x^2 \text{ implies } x^2 < x^3 \text{ implies} \dots$$

so we get an well ordering as well as it satisfies the other condition require for admissible ordering and hence this is the admissible ordering. Now suppose we take $x < 1$ implies $x^2 < x$ implies $x^3 < x^2$ implies $\dots$, then this implies an infinite decreasing sequence, hence contradiction. □

Remark 3.1.1. For $n \geq 2$, there are infinitely many admissible orderings.

Definition 3.1.2 (**LEX**(lexicographic ordering))**.** It is an admissible ordering '$<$' which can be explained in this way, given two monomials $x_1^{i_1}x_2^{i_2}x_3^{i_3}\dots x_n^{i_n}$ and $x_1^{j_1}x_2^{j_2}x_3^{j_3}\dots x_n^{j_n}$ of our polynomial algebra, we compare

$$x_1^{i_1}x_2^{i_2}x_3^{i_3}\dots x_n^{i_n} < x_1^{j_1}x_2^{j_2}x_3^{j_3}\dots x_n^{j_n}$$

if

$$i_1 < j_1 \text{ or}$$

$$i_1 = j_1, i_2 < j_2 \text{ or}$$

$$i_1 = j_1, i_2 = j_2, i_3 < j_3 \text{ or}$$

$$\vdots$$

Definition 3.1.3 (**DEGLEX**(degree-lexicographic ordering))**.** It is an admissible ordering with little difference with **LEX** is that here first we consider the degree then the **LEX** ordering.

$$x_1^{i_1}x_2^{i_2}x_3^{i_3}\dots x_n^{i_n} < x_1^{j_1}x_2^{j_2}x_3^{j_3}\dots x_n^{j_n}$$

if

$$i_1 + i_2 + i_3 + \dots + i_n < j_1 + j_2 + j_3 + \dots + j_n \text{ or}$$

$$i_1 + i_2 + i_3 + \dots + i_n = j_1 + j_2 + j_3 + \dots + j_n \text{ and}$$

$$x_1^{i_1}x_2^{i_2}x_3^{i_3}\dots x_n^{i_n} <_{\mathbf{LEX}} x_1^{j_1}x_2^{j_2}x_3^{j_3}\dots x_n^{j_n}.$$

Definition 3.1.4. By $\mathrm{LT}(f)$ for $f \in I$ we will mean the leading term of the polynomial according to our fixed admissible ordering. Next by $\mathrm{LC}(f)$ we mean the co-efficient of leading term of f. We denote leading co-efficient by LC.

Example 3.1.1. For an example we fix an order $x > y$, let our f be x^2+y^2. Then $\mathrm{LT}(f)$ is x^2. Let us give another example, let us fix $y > x$ as our order then leading term of x^2+yx will be yx according to our **DEGLEX** ordering. For both cases leading co-efficients are 1.

Let us fix an admissible ordering. Let $I \subset \mathbb{K}[x_1, x_2, \ldots, x_n]$ be an ideal. From this I we can find $\mathrm{LT}(I)$ (leading terms of I) or we can say $\mathrm{LT}(I)$ = space of linear combinations of monomials m over $\mathbb{K}$ which are leading terms of elements of I. We say $m \in \mathrm{LT}(I)$ if there exists $f \in I$ such that $f = cm + \sum c_i m_i$, where m_i's are monomials with $m_i < m$ and $c_i \in \mathbb{K}$ and $c \neq 0$.

Lemma 3.1.2. $\mathrm{LT}(I)$ *is itself an ideal in* $\mathbb{K}[x_1, x_2, \ldots, x_n]$.

Proof. It is very easy to show. Let we take f with $f = cm + \sum c_i m_i$, we form $m' = m''m$, multiplying m'' with the equation of f we get $fm'' = cm''m + \sum c_i m''m_i$, so $cm''m$ is our leading term in fm'', as I is an ideal so $fm'' \in I$ implies $m' \in \mathrm{LT}(I)$. □

Lemma 3.1.3. *Cosets of monomials* $m \notin \mathrm{LT}(I)$ *form a basis in* $R = \mathbb{K}[x_1, x_2, \ldots, x_n]/I$.

Proof. Let us first prove the linear independence.
Let $m_1, m_2, \ldots, m_l \notin \mathrm{LT}(I)$, without loss of generality assume $m_1 < m_2 < \cdots < m_l$ (where $<$ is our fixed admissible ordering), then we have $c_1m_1 + c_2m_2 + \cdots + c_lm_l = 0$ in R, where $c_i's \in \mathbb{K}$. Let $f = c_1m_1 + c_2m_2 + \cdots + c_lm_l \in I$. Then $\mathrm{LT}(f) \in \mathrm{LT}(I)$, a contradiction unless $f = 0$ implies $c_1 = c_2 = \cdots = c_l = 0$.
Our next task is to show the spanning set property i.e. we need to show that if $m \in \mathrm{LT}(I)$, then m is a linear combination in R of cosets of monomials not present in $\mathrm{LT}(I)$. We will prove this with the help of contradiction. Let's take the smallest $m \in \mathrm{LT}(I)$ for which such a combination doesn't exist. Now by definition, $\exists f \in I$, such that $0 = f = cm + \sum c_i m_i$, with $m_i < m$, and each of $m_i's$ is not in $\mathrm{LT}(I)$. Then we have $m = -\sum(c_i/c)m_i$ which can be represented as a combination of cosets of elements outside $\mathrm{LT}(I)$. Contradiction. □

4 Definition and tools of Gröbner bases

4.1 Gröbner basis

Definition 4.1.1. $G \subset I$ is called a **Gröbner basis** of I if $\{\mathrm{LT}(g) |\ g \in G\}$ generate the ideal $\mathrm{LT}(I)$ i.e. for each $f \in I$, $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g)$ for some $g \in G$.

Lemma 4.1.1. $\langle G \rangle = I$.

Proof. We know that $(G) \subset I$, suppose assume that $(G) \neq I$. Let $f \in I \backslash (G)$ with smallest possible leading term. Then $\mathrm{LT}(f) = m\,\mathrm{LT}(g)$ for some $g \in G$, $m \in I$. Let $F = f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} mg$, where LC is the leading coefficient of leading term, then we have $\mathrm{LT}(F) < \mathrm{LT}(f)$, it implies $F \in I \Rightarrow F \in (G)$, then $f = F + \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} mg \in (G)$, which is a contradiction. □

Remark 4.1.1. We have already proved that monomials not divisible by $\mathrm{LT}(G)$ form a basis of $\mathbb{K}[x_1, x_2, \ldots, x_n]/I$.

We are now going to define *reduction* and *S-polynomial* for the commutative case, these two definitions play an important role for computation of Gröbner bases. For all these definitions we have $\mathbb{K}[x_1, x_2, \ldots, x_n]$ as the commutative algebra.

Definition 4.1.2. Suppose f_1,f_2 are two polynomials belong to our defined algebra, such that there exists a monomial m with

$$\mathrm{LT}(f_1) = m\,\mathrm{LT}(f_2).$$

Then

$$R_{f_2}(f_1) = f_1 - \frac{\mathrm{LC}(f_1)}{\mathrm{LC}(f_2)} m f_2 \tag{3}$$

is called **reduction** of f_1 with respect to f_2.

Definition 4.1.3. We have two polynomials f_1 and f_2 in the algebra, suppose there exist monomials m_1,m_2 such that

$$m_1\,\mathrm{LT}(f_2) = m_2\,\mathrm{LT}(f_1) \text{ and } \deg(m_1) < \deg \mathrm{LT}(f_1) \tag{4}$$

then

$$S(f_1, f_2) = \frac{1}{\mathrm{LC}(f_1)} m_2 f_1 - \frac{1}{\mathrm{LC}(f_2)} m_1 f_2 \tag{5}$$

is called **S-polynomial** with respect to a small common multiple (4).

Example 4.1.1. Let us give an example to show how reduction and S-polynomial work, suppose we have a commutative polynomial algebra in 2 variable i.e. $\mathbb{K}[x, y]$. We will pick **DEGLEX** ordering. Now let $f_1 = x^3 - y^2$ and $f_2 = x^3 - x + 1$. Then one can see for both f_1 and f_2, LT is x^3. So $\mathrm{LT}(f_1) = \mathrm{LT}(f_2) = x^3$ implies $m = 1$ so that $x^3 = 1 \cdot x^3$, our reduction of f_1 w.r.t f_2 will be then $x^3 - y^2 - (x^3 - x + 1) = x - y^2 - 1$.
And while computing S-polynomial with respect to a small common multiple we have 3 choices,

$$1 \cdot x^3 = 1 \cdot x^3$$

$$x \cdot x^3 = x \cdot x^3$$

$$x^2 \cdot x^3 = x^2 \cdot x^3$$

hence for each cases we can compute the S-polynomial using our formula (5). For an example if we consider $x \cdot x^3 = x \cdot x^3$ then our S-polynomial will be $x^2(x^3 - y^2) - x^2(x^3 - x + 1) = x^3 - x^2y^2 - x^2$.

5 Terminology for Gröbner bases

Before moving towards the computation of Gröbner bases for commutative case, we will first give some terminology regarding Gröbner bases.

Definition 5.0.4. Normal monomial:
Given a Gröbner basis $G \subset I$, normal monomials with respect to G are those monomials which are not divisible by $\mathrm{LT}(g)$, for $g \in G$.
We sometime call normal monomials as normal words.

Lemma 5.0.2. *Cosets of normal monomials form a basis of* $\mathbb{K}[x_1, x_2, \ldots, x_n]/I$.

Proof. This is proved earlier in lemma 3.1.3. □

Definition 5.0.5. Reduced Gröbner basis:
G, a Gröbner basis of I is reduced if for each $g \in G$,

- $\mathrm{LC}(g) = 1$.
- $g - \mathrm{LT}(g)$ is a linear combination of normal monomials.

Theorem 5.0.1. *Let us fix an admissible ordering. Then every I has a unique reduced Gröbner basis.*

Proof. Let us take some Gröbner basis $G \subset I$.
First condition of reduced Gröbner basis is easy to satisfy as we just divide each g by it's LC, i.e. $g \to g/\mathrm{LC}(g)$.
The reduction and S-polynomial suggests that remaining terms of g is not divisible by the leading term of any terms in G which implies that $g - \mathrm{LT}(g)$ is a linear combination of normal monomials. Now we will prove the uniqueness.
Let $\{f_1, f_2, \ldots, f_s\}$ and $\{g_1, g_2, \ldots, g_s\}$ be two reduced and ordered Gröbner bases so that $\mathrm{LT}(f_i) = \mathrm{LT}(g_i)$ for each i. Consider $f_i - g_i \in I$, if it's not 0, then its leading term must be a term that appeared either in f_i or in g_i. In either case, this contradicts the fact that the bases being reduced, so in fact we get our required $f_i = g_i$. □

6 Computation of Gröbner bases

In this section we will show how to compute Gröbner basis for an ideal I of a polynomial algebra $\mathbb{K}[x_1, x_2, \ldots, x_n]$. But at first let us construct the general algorithm to compute the Gröbner basis in case of commutative algebras.

Definition 6.0.6. f can be reduced to 0 modulo G, if there exists $g_1, g_2, \ldots, g_n \in G$ such that

$$R_{g_m}(\ldots\ldots R_{g_2}(R_{g_1}(f))\ldots) = 0$$

Lemma 6.0.3. ***Diamond lemma:***
For an ideal I of a commutative algebra A, $G \subset I$ forms a Gröbner basis if and only if for each $g_1, g_2 \in G$
$R_{g_2}(g_1)$ (if defined) can be reduced to 0 modulo G.
And also for each $g_1, g_2 \in G$ and each small common multiple of $\mathrm{LT}(g_1), \mathrm{LT}(g_2)$; the corresponding S-polynomial can be reduced to 0 modulo G.

We will write another lemma which is equivalent to the *diamond lemma* and it is easy to prove:

Lemma 6.0.4. *Assume $\langle G \rangle = I$, then the following statements are equivalent:*
(i) G is a Gröbner basis of I.
(ii) All reductions and all S-polynomials of pair of elements of G can be reduced to 0 modulo G.
(iii) For every $f \in I$, f admits a representation

$$f = h_1 g_1 + h_2 g_2 + \cdots + h_n g_n \ ; \ g_i \in G$$

with

$$\mathrm{LT}(f) = \max(\mathrm{LT}(h_i g_i))$$

Proof. Readers may find it interesting to prove the lemma. □

6.1 Buchberger's algorithm

We start with an ideal I generated by a set G. The Buchberger's algorithm, which is a simple consequence of lemma 6.0.3, is the following:
Step 1: If the leading term of any element u of G occurs inside the leading term of another element v of G, then we reduce v by subtracting off the required multiple of u. In general we will perform the reduction mentioned in definition 4.1.2.
Step 2: For each pair of distinct elements of G we compute the S-polynomial and a remainder of it.
Step 3: If the remainder can be reduced further then we will follow step 1 or we will add that term in our set G. If all S-polynomials reduce to 0, then the algorithm ends and G is the Gröbner basis of I. If not then we will continue further with our 3 steps.
For commutative cases the algorithm ends in a finite number of stages.

6.2 An example of computation in case of a commutative algebra

Example 6.2.1. We have previously defined what is meant by a commutative polynomial algebra. Let us take $\mathbb{K}[x_1, x_2]$ as our commutative polynomial ring with two variables x_1, x_2. Suppose there are two polynomials

$$h_1(x_1, x_2) = x_1^2 + x_2^2$$

$$h_2(x_1, x_2) = x_1^3 + x_2^3$$

belonging to our polynomial ring $\mathbb{K}[x_1, x_2]$. We will compute the Gröbner basis for $I = (h_1, h_2) \subset \mathbb{K}[x_1, x_2]$.
Let us fix an admissible ordering. Usually we take **DEGLEX** ordering. So here we consider $x_1 > x_2$. So we get $\mathrm{LT}(h_1) = x_1^2$ and $\mathrm{LT}(h_2) = x_1^3$. So initially our set is $G = \{h_1, h_2\}$. But we see that h_2 can be reduced further. So we have $x_1^3 = x_1 \cdot x_1^2$,

$$R_{h_1}(h_2) = (x_1^3 + x_2^3) - x_1(x_1^2 + x_2^2)$$

$$= x_2^3 - x_1x_2^2.$$

So we have obtained a new term $x_2^3 - x_1x_2^2$ which cannot be reduced further, we add this to our set G which is now $\{h_1, R_{h_1}(h_2)\}$. We call $R_{h_1}(h_2)$ as h_3. We see that the leading term of h_3 is $x_1x_2^2$. We have also found that $x_1 \cdot x_1x_2^2 = x_1^2 \cdot x_2^2$. So we will compute the S-polynomial between h_1, h_3.

$$S(h_1, h_3) = -x_1(x_2^3 - x_1x_2^2) - (x_1^2 + x_2^2)x_2^2$$

$$= -x_1x_2^3 - x_2^4.$$

The term $-x_1x_2^3 - x_2^4$ has $x_1x_2^3$ as the leading term which can be reduced further through $\mathrm{LT}(h_3)$. We get $x_1x_2^3 = (x_1x_2^2) \cdot x_2$. hence the reduction yields

$$-x_1x_2^3 - x_2^4 - (x_2^3 - x_1x_2^2)x_2$$

$$= -2x_2^4$$

which cannot be reduced further and also one cannot compute more S-polynomial. Hence we add $-2x_2^4$ in our set G and the final set G is our Gröbner basis for I, the set is precisely as follows

$$\{x_1^2 + x_2^2,\ x_2^3 - x_1x_2^2,\ -2x_2^4\}.$$

Remark 6.2.1. The reduced Gröbner basis of I of our previous example is given by $\{x_1^2 + x_2^2,\ x_1x_2^2 - x_2^3,\ x_2^4\}$. It is not very difficult to obtain this reduced Gröbner basis from our computed Gröbner basis. If we recall the definition of reduced Gröbner basis we will see that all leading co-efficients of the reduced basis should be 1. So we just divide terms $-2x_2^4, x_2^3 - x_1x_2^2$ of $\{x_1^2 + x_2^2,\ x_2^3 - x_1x_2^2,\ -2x_2^4\}$ by -2 and -1 respectively to obtain $\{x_1^2 + x_2^2,\ x_1x_2^2 - x_2^3,\ x_2^4\}$. Indeed x_2^2 and x_2^3 are normal monomials. So we have obtained the reduced Gröbner basis of I.

7 Conclusion

Similarly for a non-commutative algebra we can similarly define Gröbner bases, reduction, S-polynomial and Diamond lemma for the computation of Gröbner bases. But the interesting fact is that Buchberger's algorithm in non-commutative case doesn't guarantee to be terminated. In that case we get an infinite set of Gröbner basis. Gröbner bases has many major applications. One of the interesting application is to compute Hilbert series of an algebra from chains[3]. Readers may also find it interesting to learn more applications of Gröbner bases in commutative algebra in [2].

References

[1] Bruno Buchberger, An Algorithm for Finding the Basis Elements of the Residue Class Ring of a Zero Dimensional Polynomial Ideal, Ph.D. Dissertation,1965. *Journal of Symbolic Computation*, **41**, 2006 (Translation).

[2] Viviana Ene - Jürgen Herzog, *Gröbner Bases in Commutative Algebra*, Graduate Studies in Mathematics, Volume 130, AMS.

[3] V.A.Ulfarovskij, *Combinatorial and Asymptotic Methods in Algebra*. pp.- 42-58. Algebra VI, Springer, 1995.