

Gröbner Bases for Polynomial Ideals

Contents

1	Introduction	2
2	Polynomial Rings	2
2.1	Polynomials in One Variable	2
2.2	Multivariate Polynomials	3
2.3	Ordering	4
3	The Generalised Division Algorithm	5
4	Gröbner Bases	6
4.1	Ideals of a Polynomial Ring	6
4.2	The Gröbner Basis	6
4.3	Computing a Gröbner Basis	7
5	Applications of Gröbner Bases	8
5.1	Hilbert's Basis Theorem	8
5.2	Solving Non-Linear Systems	8

1 Introduction

The purpose of this essay is to investigate Gröbner bases and discover what uses people have found for them, which we will find is quite far reaching. The Gröbner base was invented as a tool by Bruno Buchberger circa 1966 to aid with the study of computational commutative algebras. They were simultaneously created by Heisuke Hironaka circa 1964 whilst working in the field of algebraic geometry where he gave them the name standard bases. Technically, a Gröbner base is defined as the generating set of a multivariate polynomial ideal. It then makes sense to start at the beginning refreshing our knowledge of rings.

2 Polynomial Rings

Before we can go on to study Gröbner bases, we should first remind ourselves what a polynomial ring is and generalise this to multiple variables.

2.1 Polynomials in One Variable

To define a polynomial in a sense that is useful to us we should start by defining a monomial.

Definition 1. A **monomial** in a variable X is a positive integer power of X multiplied by a coefficient a (generally we have $a \in R$ where R is a commutative ring). Monomials are generally expressed in the form aX^n .

Definition 2. A **polynomial** in variable X is a finite linear combination of monomials. A polynomial can be expressed as

$$\sum_{n \in \mathbb{N}} a_n X^n, \quad a_n = 0 \quad \forall n \gg 0$$

Each individual monomial in the polynomial is generally referred to as a **term**.

The condition that a_n is zero for all large n ensures that in this representation we have that the polynomial is finite. From now on, we assume that $n \in \mathbb{N}$ and that after some finite value of n , all a_n are zero. For this reason we can omit the lower limit from our summation as we can assume that $n \in \mathbb{N}$ and that the sum is always finite.

If we stipulate a_n is an element of a commutative ring R we can state the following lemma.

Lemma 1. *If a polynomial $\sum a_n X^n$ has coefficients $a_n \in R$ commutative, then the set of all polynomials of this kind form a ring and we denote this $R[X]$.*

Proof. If we define the binary operations of addition as

$$\sum a_n X^n + \sum b_n X^n = \sum (a_n + b_n) X^n$$

and multiplication as

$$\sum a_n X^n \cdot \sum b_n X^n = \sum \left(\sum_{i+j=n} a_i b_j \right) X^n$$

then we can show that the set of polynomials with coefficients in R satisfy the axioms of a ring.

Clearly, as $a_n, b_n \in R$, then $(a_n + b_n) \in R$, and similarly $a_i, b_j \in R$ then $a_i b_j \in R$. Therefore $R[X]$ is closed under these operations. Commutativity and associativity of addition is inherited from the commutativity and associativity of R . The additive identity is clearly the zero polynomial, which we can define as the polynomial $a_n = 0 \forall n$. Additive inverses are also inherited from R . Distributivity follows clearly from expansion and comparison of the polynomials. Hence $R[X]$ satisfies the axioms of a ring. \square

As we have proved that taking the set of polynomials with coefficients in a ring exhibits a ring, we should properly define a polynomial ring.

Definition 3. A **polynomial ring** is the set of all polynomials with coefficients in a commutative ring R equipped with the binary operations defined as above, such that:

$$R[X] = \left\{ \sum a_n X^n : a_n \in R, \quad a_n = 0 \quad \forall n \gg 0 \right\}$$

2.2 Multivariate Polynomials

We have reminded ourselves that if R is a commutative ring then $R[X]$ is also a commutative ring. It is surprisingly simple to show that the set of multivariate polynomials with coefficients in R also forms a commutative ring. If we take the ring $R[X]$ as the coefficients of a polynomial ring in variable Y then we have $(R[X])[Y]$. Clearly by our definition of a polynomial ring; given that $R[X]$ is a commutative ring, $(R[X])[Y]$ must be a commutative polynomial ring.

Proposition 1. $(R[X])[Y]$ is equivalent to $(R[Y])[X]$.

Proof. From our definition of a polynomial ring we have that:

$$(R[X])[Y] = \{a_0 + a_1Y + a_2Y^2 + \cdots + a_nY^n : a_i \in R[X]\}$$

However because $a_i \in R[X]$ we can rewrite this by replacing each a_i by elements from $R[X]$. This gives us the following:

$$(R[X])[Y] = \{b_0 + b_1X + b_2Y + b_3X^2 + b_4XY + b_5Y^2 + \cdots : b_i \in R\}$$

It then follows by the same logic applied to some $b_i \in R$ that we can write this in the form:

$$(R[X])[Y] = \{c_0 + c_1X + c_2X^2 + \cdots + c_nX^n : c_i \in R[Y]\}$$

However, if we inspect the last line, it is exactly the definition of $(R[Y])[X]$ and so we have shown that $(R[X])[Y] = (R[Y])[X]$, hence the claim is true. \square

A consequence of this claim is that we can write the ring $(R[X])[Y]$ as $R[X, Y]$ with no ambiguity. It is clear that this generalises to any finite number of variables. For example we can apply the method in the proof to show the following. Clearly $(R[X, Y])[Z]$ is a ring; but this is equivalent to $(R[X, Z])[Y]$ and $(R[Y, Z])[X]$. Therefore we can write this as $R[X, Y, Z]$. A similar argument shows that any finite number of variables satisfies this. Therefore a general ring of polynomials with n variables is just $R[X_1, \dots, X_n]$.

To define a multivariate polynomial ring in a similar way to that of a single variable polynomial ring we must generalise our definition of a monomial. An extended definition follows.

Definition 4. A monomial in several variables is the product of variables $X_i \in (X_1, X_2, \dots, X_n)$ to positive integer powers multiplied by a coefficient in R .

We can now see a monomial as an element $a \cdot X_1^{m_1} \cdot X_2^{m_2} \cdot \dots \cdot X_n^{m_n}$ with $a \in R$ and each $m_i \in \mathbb{N}$. However, we can define a much less cumbersome notation.

Definition 5. A **multi-index** $\alpha \in \mathbb{N}^n, \alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ allows us to write a monomial in several variables such that:

$$X^\alpha = X^{(\alpha_1, \dots, \alpha_n)} = X_1^{\alpha_1} \cdot X_2^{\alpha_2} \cdot \dots \cdot X_n^{\alpha_n}$$

Using this notation allows us to concisely define a polynomial ring in several variables which is analogous to the single variable definition.

Definition 6. A **multivariate polynomial ring** is a finite linear combination of monomials of several variables with coefficients in R .

$$R[X_1, \dots, X_n] = \left\{ \sum a_\alpha X^\alpha : \alpha \in \mathbb{N}^n, a_\alpha \in R, a_\alpha = 0 \quad \forall \alpha_i \gg 0 \right\}$$

2.3 Ordering

We shall now make a slight detour from rings, and look at how we order the terms of the polynomials. We shall see later that one of the caveats of Gröbner bases is that they are not unique up to the ordering of the polynomial. But what does it mean to order a multivariate polynomial? It is clear when working in one variable that, say $X^7 > X^2$, and it is trivial to order any given polynomial. This is because the notion of the degree is a well defined ordering.

Definition 7. The **degree** of a monomial is just $|\alpha| = \sum_i \alpha_i$. The degree of a polynomial is defined as the maximum degree of all monomials that compose the polynomial.

It is clear that the degree of each monomial in a single variable polynomial is enough to determine a well defined ordering. If the degree of two monomials is equal, then they only differ by coefficient. This means that the monomials can be combined so that we have a new monomial with coefficient $a_3 = a_1 + a_2$.

However, when we look at monomials with several variables then the degree of the monomial is not a well defined notion. For example, the degree of X_1^3 is clearly three, but $X_1^2 \cdot X_2$ and $X_1 \cdot X_2 \cdot X_3$ also have degree equal to three. So if we have a polynomial $X_1 \cdot X_2 \cdot X_3 + X_1^2 \cdot X_2 + X_1^3$ how can we give the monomials a well defined order?

Definition 8. The **lexicographical order** \leq_{lex} on a Cartesian product of the natural numbers is defined as follows. Take $v, w \in \mathbb{N}^n$ where $v = (v_1, v_2, \dots, v_n)$ and $w = (w_1, w_2, \dots, w_n)$. Then we have that $v <_{\text{lex}} w$ if and only if one of the following conditions is satisfied:

$$\begin{aligned} &v_1 < w_1 \\ \text{or } &v_1 = w_1 \text{ and } v_2 < w_2 \\ \text{or } &v_1 = w_1 \text{ and } v_2 = w_2 \text{ and } v_3 < w_3 \\ &\vdots \\ \text{or } &v_1 = w_1 \text{ and } v_2 = w_2 \text{ and } \dots \text{ and } v_{n-1} = w_{n-1} \text{ and } v_n < w_n \end{aligned}$$

Example. If we take the vectors $v, w \in \mathbb{N}^3$ where $v = (1, 2, 3)$, $w = (2, 3, 1)$ then $v <_{\text{lex}} w$ because $1 < 2$, and no other components are significant.

Now if we express our polynomial in multi-index notation, we have $X^{(1,1,1)} + X^{(2,1,0)} + X^{(3,0,0)}$. If we supply an order with the polynomial then the polynomial can be written in **normal form**. So for this example we can use the lexicographical order that we have just defined. It is obvious that the polynomial has been written in the reverse order, and with respect to the lexicographical order the polynomial in normal form should read: $X^{(3,0,0)} + X^{(2,1,0)} + X^{(1,1,1)}$. To demonstrate the wide array of notations that can be used, this is equivalent to $X^3 + X^2Y + XYZ$ which is a notation often used when the number of variables is small.

Now that we have expressed a way of ordering a given polynomial in a normal form, we can introduce a notion that will allow us to extend the well known Euclidean division algorithm.

Definition 9. The **initial term** of a polynomial $f \in R[X_1, \dots, X_n]$ with respect to the ordering $<_{\text{lex}}$ is denoted $\text{in}_{<_{\text{lex}}}(f)$, and $\text{in}_{\leq_{\text{lex}}}(f) = a_\beta X^\beta$ such that $\beta = \max \{\alpha \in \mathbb{N}^n : a_\alpha \neq 0\}$.

β is well defined because the ordering that we have supplied is well defined. The initial term is always the first term of the polynomial if it is in normal form with respect to the given ordering. From this point on, any polynomial will be given with respect to the lexicographical ordering, therefore all orderings can be denoted \leq without confusion. Then it follows that the initial term will always be found with respect to \leq , and it is unnecessary to include this in the subscript; hence the initial term of f will always be denoted as $\text{in}(f)$.

Example. The initial term of our previous polynomial is X^3 .

3 The Generalised Division Algorithm

The Euclidean division algorithm has many uses, one of which is closely linked to polynomial rings. Given two polynomials f and g such that $\deg(f) \geq \deg(g)$ with $f, g \in R[X]$, then there exists $q, r \in R[X]$ such that we can find a unique representation $f(x) = q(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg(r) < \deg(g)$. We are required to constrain our choice of base ring here however, as the polynomial ring must be a Euclidean domain. This is satisfied if R is a field. This becomes even more important when we try to generalise the algorithm for multiple variables. Therefore from this point forward, to make it clear that the ring R is a field, we shall denote our polynomial rings as $k[X_1, \dots, X_n]$: the polynomial ring over the field k .

Now that we are working with several variables, one extension that we can make is to find a form for our polynomial f that is a linear combination of a sequence of smaller polynomials. This clearly can not be the case when we are in one variable. As long as the degree of each polynomial in our sequence (f_1, f_2, \dots, f_m) is less than the degree of f , which is an equivalent condition to the one required for multiple variables, then f can be written as $f(x) = q(x)f_i(x) + r(x)$ for any f_i . Therefore having a sequence of polynomials is meaningless in this case.

On the other hand, it is quite useful to be able to write a polynomial of multiple variables as a linear combination of a sequence of polynomials. This will become apparent when we look at ideals of polynomial rings.

Theorem 1. *Take any polynomial $f \in k[X_1, \dots, X_n] \setminus \{0\}$ and fix an ordering \leq . Then for any sequence $(f_1, \dots, f_m) \in k[X_1, \dots, X_n] \setminus \{0\}$ there exists $a_1, \dots, a_m, r \in k[X_1, \dots, X_n]$ such that*

$$f = a_1 f_1 + a_2 f_2 + \dots + a_m f_m + r$$

where $r = 0$ or no terms in r are divisible by any $\text{in}(f_i)$.

Proof. The proof of this theorem is basically a statement of the algorithm. It is clear that for any sequence of polynomials, the algorithm terminates and hence it is sufficient to prove that the theorem is true.

Begin by setting $a_1, \dots, a_m = 0, r = 0$ and introduce $s = f$. Now we have

$$f = a_1 f_1 + \dots + a_m f_m + r + s.$$

The aim is to reduce s until it is the zero polynomial, then it is clear that we have the required result. Clearly the algorithm is going to revolve around this polynomial s , and the first step is to compare $\text{in}(s)$ with all $\text{in}(f_i)$. Now if any $\text{in}(f_i)$ divide $\text{in}(s)$ then we choose the smallest i such that $\text{in}(f_i) | \text{in}(s)$. Now we replace the following:

$$s := s - \frac{\text{in}(s)}{\text{in}(f_i)} f_i$$

$$a_i := a_i + \frac{\text{in}(s)}{\text{in}(f_i)}$$

It is clear that if we look at our initial equation, we have added and subtracted the same thing and the equation is still true. If no $\text{in}(f_i)$ that divides $\text{in}(s)$ is found then we simply add $\text{in}(s)$ to the remainder. $r := r + \text{in}(s), s := s - \text{in}(s)$. Again, our equation remains unchanged. It is clear that if we iterate this process, then eventually it will terminate. This is a consequence of f , and hence s , being finite. Each time the algorithm is applied, if $\text{in}(s)$ is not divisible by any $\text{in}(f_i)$ then it is simply removed. If the converse is true, then by consequence of our well ordered polynomial, $\frac{\text{in}(s)}{\text{in}(f_i)} f_i$ is equal to $\text{in}(s)$ plus a polynomial $g = g_1 + \dots + g_k$ where each g_i is smaller than $\text{in}(s)$ with respect to our ordering. Therefore it is the case that the algorithm will eventually terminate and s is reduced to zero. We have then achieved the form

$$f = a_1 f_1 + \dots + a_m f_m + r$$

as required. □

Example. We shall use the polynomial $f = X^3 + X^2Y + Y$ throughout our following examples. We shall also use the polynomial sequence $f_1 = X^2 + Y, f_2 = XY$. To illustrate the algorithm we shall perform the division of f by the sequence. To begin we have $\text{in}(s) = X^3$. Now it is clear that $\text{in}(f_1) = X^2 | X^3$ so we subtract $X \cdot (X^2 + Y)$ from s and add X to a_1 . Now $s = X^2Y - XY + Y$ and again $\text{in}(f_1) | \text{in}(s)$

and so we subtract $Y \cdot (X^2 + Y)$ from s and add Y to a_1 . $s = -XY - Y^2 + Y$ and so only $\text{in}(f_2)$ divides $\text{in}(s)$ and gives -1 . Therefore, applying the algorithm gives $s = -Y^2 + Y$ and it is clear that neither initial terms of f_1 or f_2 will divide either term of s . This means we can transfer both terms to r and we are done. In this case we have $a_1 = X + Y, a_2 = -1$ and $r = -Y^2 + Y$, or

$$f = (X + Y)(X^2 + Y) + (-1)(XY) + (-Y^2 + Y)$$

4 Gröbner Bases

At this point, we have covered enough ground to begin to define a Gröbner basis. The generalisation of the division algorithm is further refined by the definition of Gröbner bases, and the algorithm used to compute them.

4.1 Ideals of a Polynomial Ring

Initially, we defined a Gröbner basis as a set of polynomials that generates an ideal. It would be a good idea then to define what it is to be a polynomial ideal.

Definition 10. An **ideal** of a ring R is a subset I that satisfies the following:

1. $\forall a, b \in I$ we have $a + b \in I$
2. $\forall a \in I$ and $\forall r \in R$ we have $a \cdot r \in I$

Note that if we have a subset $S \subset R$ such that $S = \{r_1 s_1 + \dots + r_n s_n : s_i \in S, r_i \in R\}$ then this set of finite linear combinations forms an ideal generated by S . If S is finite, then this ideal can be denoted $\langle s_1, \dots, s_n \rangle$.

It follows then that a polynomial ideal is the set of linear combinations of that polynomial.

Example. If we take our sequence of polynomials $f_1 = X^2 + Y, f_2 = XY$ then the ideal $I = \langle X^2 + Y, XY \rangle$ is the set of linear combinations of f_1 and f_2 with elements from $k[X, Y]$.

$$I = \{g(X, Y)(X^2 + Y) + h(X, Y)(XY) : g, h \in k[X, Y]\}$$

If we take the polynomial $f = X^3 - XY^2 + XY$, then clearly $f \in I$ (as we have just taken $g = X$ and $h = -Y$ in the previous example). However, if we take our polynomial from the previous section then we have no methodical way of testing whether it is in the ideal or not. This is where Gröbner bases come in useful.

4.2 The Gröbner Basis

Now we have recalled the definition of an ideal in terms of polynomial rings, we can properly define a Gröbner basis.

Definition 11. For an ideal $I \subset k[X_1, \dots, X_n]$, a sequence $(f_1, \dots, f_m) \subseteq k[X_1, \dots, X_n] \setminus \{0\}$ of polynomials is called a **Gröbner basis** of the ideal with respect to the ordering \leq if $f_1, \dots, f_m \subseteq I$ and $\forall f \in I \setminus \{0\}$ then we have $\text{in}(f_i) | \text{in}(f)$ for at least one $i \in 1, \dots, m$.

This definition seems quite cumbersome initially. We find that it is very neat, however, since at once it allows us to state the following result.

Proposition 2. Let $G = (f_1, \dots, f_m)$ be a Gröbner basis with respect to the ordering \leq . Now if we take the ideal $I = \langle f_1, \dots, f_m \rangle$ then we have $f \in I \iff \text{rem}(f, G) = 0$.

Here we have introduced the notation $\text{rem}(f, F)$ to mean the remainder term of f when divided by the sequence of polynomials $F = (f_1, \dots, f_m)$. This proposition gives us the ability to decide whether a polynomial is in an ideal, with the constraint that the generator of our ideal is a known Gröbner basis. We shall prove the proposition.

Proof. Assuming we have for our chosen f , $\text{rem}(f, G) = 0$. This means that we have found elements $a_1, \dots, a_m \in k[X_1, \dots, X_n]$ such that $f = a_1f_1 + \dots + a_mf_m$. Hence f must be in our ideal.

Now if we assume that f is in the ideal I , where $I = \langle f_1, \dots, f_m \rangle$. Now if we let $f = a_1f_1 + \dots + a_mf_m + \text{rem}(f, G)$, we can see that $\text{rem}(f, G) = f - a_1f_1 - \dots - a_mf_m$. It is clear that $\text{rem}(f, G) \in I$. Assuming that $\text{rem}(f, G) \neq 0$ then there exists $f_i \in G$ such that $\text{in}(f_i) | \text{in}(\text{rem}(f, G))$ by the stipulation that G is a Gröbner basis. However this implies that $\text{rem}(f, G)$ is not the remainder after division by G . This contradiction implies that $\text{rem}(f, G) = 0$ as required. \square

4.3 Computing a Gröbner Basis

We have shown that having the Gröbner basis for an ideal is a very useful tool. But, unless we already know that we have a Gröbner basis we are still unable to do any of the useful tricks that the basis allows. We need to devise a way to find a basis for any given polynomial ideal.

Definition 12. The **S-polynomial** for a pair of polynomials $f, g \in k[X_1, \dots, X_n] \setminus \{0\}$ with respect to a term ordering \leq , is defined as

$$S(f, g) := \frac{\text{lcm}(\text{in}(f), \text{in}(g))}{\text{in}(f)}f - \frac{\text{lcm}(\text{in}(f), \text{in}(g))}{\text{in}(g)}g$$

The S-polynomial is a vital tool for determining whether the generators of our ideal are in fact a Gröbner basis. The following theorem is a key result that allows us to form an algorithm to compute the basis.

Theorem 2. Let $I = \langle f_1, \dots, f_m \rangle \subset k[X_1, \dots, X_n]$. Then $G = (f_1, \dots, f_m)$ is a Gröbner basis of I if and only if $\text{rem}(S(f_i, f_j), G) = 0$ for all $i, j \in 1, \dots, m$.

To prove this theorem, we will need to first prove some intermediate steps that should together show that indeed the theorem is true.

Lemma 2. For a sequence $(f_1, \dots, f_m) \in k[X_1, \dots, X_n]$ with an ideal $I = \langle f_1, \dots, f_m \rangle$ if we have that, $\forall f \in I$, $\text{rem}(f, (f_1, \dots, f_m)) = 0$ then the sequence (f_1, \dots, f_m) gives us a Gröbner basis.

Proof. This follows trivially from Proposition 2. If we apply the proposition to every $f \in I$ then we can see that (f_1, \dots, f_m) must be a Gröbner basis for I . \square

Lemma 3. For a sequence $(f_1, \dots, f_m) \in k[X_1, \dots, X_n]$ with an ideal $I = \langle f_1, \dots, f_m \rangle$ if we have $\text{rem}(S(f_i, f_j), (f_1, \dots, f_m)) = 0$ for all $i, j \in 1, \dots, m$ then $\text{rem}(f, (f_1, \dots, f_m)) = 0$ for all $f \in I$.

Proof. Adapted from [4, p. 207]. Let $F = (f_1, \dots, f_m)$. Then let $f \in I$ so that f is a linear combination of f_i 's. Then since $\text{rem}(S(f_i, f_j), F) = 0$ we have

$$S(f_i, f_j) = e_1f_1 + \dots + e_mf_m$$

with $e_i \in k[X_1, \dots, X_n]$ and $\text{in}(e_l f_l) \leq \text{in}(S(f_i, f_j))$, $l \in 1, \dots, m$. Now we can define $C = \text{in}(a_1)f_1 + \dots + \text{in}(a_r)f_r$, then

$$f = C + (a_1 - \text{in}(a_1))f_1 + \dots + (a_r - \text{in}(a_r))f_r + a_{r+1}f_{r+1} + \dots + a_mf_m$$

Now we can say that the expression for $S(f_i, f_j)$ can be written in the form $f = h_1f_1 + \dots + f_mh_m$ with $\max\{\text{in}(h_i f_i) : h_i f_i \neq 0, i \in 1, \dots, m\} < \delta$. This means that if the maximal terms of $f = a_1f_1 + \dots + a_mf_m$ cancel and $\text{rem}(S(f_i, f_j), F) = 0$, then there is an expression $f = h_1f_1 + \dots + h_mf_m$ such that the maximal initial terms are strictly less than the maximal initial terms in the first expression. Then eventually we end up with an expression

$$f = b_1f_1 + \dots + b_mf_m$$

where the maximal term is $\text{in}(f)$, hence $\text{rem}(f, F) = 0$. \square

With the statement and proofs of the preceding lemmas, we now have enough information such that we can prove the theorem.

Proof. (Theorem 2) It is clear that by Lemma 3 that if $\text{rem}(S(f_i, f_j), (f_1, \dots, f_m)) = 0$, then the remainder of the division of f by the sequence (f_1, \dots, f_m) is 0 for any f in the ideal. Now if we apply Lemma 2, we can see that if for any $f \in I$ we have $\text{rem}(f, (f_1, \dots, f_m)) = 0$ then it is true that (f_1, \dots, f_m) is a Gröbner basis for I . \square

With Theorem 2 we now have a base to implement an algorithm to find a Gröbner basis for any polynomial ideal I . Basically, if we apply the S-polynomial to all pairs f_i, f_j in the sequence and have $\text{rem}(S(f_i, f_j), G) = 0$, where G is the sequence (f_1, \dots, f_m) , for all pairs, then we are done. If we have that $\text{rem}(S(f_i, f_j), G) \neq 0$, then call this value f_{m+1} and add it to G and retest. It can be shown that this process always terminates.

Using our ideal from an earlier section, $\langle X^2 + Y, XY \rangle$, we shall give an example of this process in action.

Example. Let $f_1 = X^2 + Y, f_2 = XY$. As we only have 2 polynomials in our sequence, then we only need to find $\text{rem}(S(f_1, f_2), (f_1, f_2))$. Let $F = (f_1, f_2)$. Plugging into the definition of the S-polynomial, we get that $\text{rem}(S(f_1, f_2), F) = Y^2 \neq 0$. Straight away, we know that F is not a Gröbner basis for the ideal $I = \langle X^2 + Y, XY \rangle$. However, if we now define $F := F \cup \{\text{rem}(S(f_i, f_j), F)\}$ then we can repeat the check until we obtain a Gröbner basis. So now $F = (X^2 + Y, XY, Y^2)$. We need to check that $\text{rem}(S(f_i, f_j), F) = 0$ for all pairs in the sequence. It is obvious that $\text{rem}(S(f_1, f_2), F) = 0$ because we have just added the previous remainder to F . Now, $S(f_1, f_3) = Y^3$. This is just $Y \cdot Y^2$, so the remainder in this case is also 0. Now it remains to check $S(f_2, f_3)$. In this case, $S(f_2, f_3) = 0$, hence the remainder must be 0. Therefore we have now exhibited a finite basis for our ideal, $G = (X^2 + Y, XY, Y^2)$.

As we can see, we now finally have our method for formulating a Gröbner basis. This algorithm is known as **Buchberger's Algorithm**. This method is not always easy, and the number of divisions needed to compute this can become extremely large. The computation of bases is normally left to a computer, as the algorithmic approach transfers well. This is also due to how difficult the basis can become. Even a simple looking ideal may admit a basis with a large number of elements and each element having many multiple terms. There are refinements that can be made at the algorithmic stage that make this process easier, however, but it is still best left to computer algebra systems if we want to actually compute a basis.

5 Applications of Gröbner Bases

The Gröbner basis of an ideal lends itself to many applications outside of its initial use. Initially, it was a construction to help with proofs in Algebraic Geometry, where we study vanishing sets of systems of polynomials. This clearly is aided by the study of polynomial rings, and more specifically ideals of these rings. Therefore if there exists an easy way to show whether f belongs to an ideal, then this greatly improves our ability to study such things.

5.1 Hilbert's Basis Theorem

In the late 19th Century, David Hilbert made the claim that all ideals of polynomial rings are finitely generated. This was seen as very controversial at the time, however he offered a proof which was nevertheless accepted. His theorem and proof however, gave no insight in to how one would calculate a basis for a given ideal. This is where Buchberger's work in the 1960's that has given us the preceding algorithm comes in. It admits a finite basis for any polynomial ideal, and gives us a way of finding the basis. This also simplifies the proof of the theorem.

Theorem 3. *Let $I \subset k[X_1, \dots, X_n]$. Then there is a finite sequence of polynomials such that for all $f \in I$*

$$f = a_1 f_1 + \dots + a_m f_m.$$

Proof. This follows easily from our previous results on Gröbner bases. □

5.2 Solving Non-Linear Systems

One very useful application of Gröbner bases is for solving non-linear systems of simultaneous equations, in a similar manner to Gaussian elimination. We shall show this by example.

Example. Take the system of polynomials,

$$\begin{aligned} X^2 + Y &= 0 \\ X + Y &= 0 \end{aligned}$$

One can compute the Gröbner basis, and finds that $G = (Y^2 + Y, X + Y)$. We can see that the Gröbner basis has reduced at least one element to just a combination of one variable. This is always true of a Gröbner basis. Now we have methods to solve an equation in one variable, and then with back substitution it is easy to find the solutions for each variable. Clearly in our case, $Y^2 + Y = 0 \iff Y \cdot (Y + 1) = 0 \iff Y = 0$ or $Y = -1$, and then this implies that $X = 0$ or $X = 1$. Geometrically, the intersection of the curves $Y = -X^2$ and $Y = -X$ is at $(0, 0)$ and $(1, -1)$. A more difficult example is given in [4, p. 216].

References

- [1] William W. Adams and Philippe Loustau. *An Introduction to Gröbner Bases*. American Mathematical Society, 1994.
- [2] Ralf Fröberg. *An Introduction to Gröbner Bases*. John Wiley & Sons, 1997.
- [3] Derek Holt. Algebra II lecture notes.
- [4] Niels Lauritzen. *Concrete Abstract Algebra: From Numbers to Gröbner Bases*. Cambridge University Press, 2003.