# GRÖBNER BASES ON MULTIVARIABLE EQUATIONS AND PARABOLIC ENVELOPES

ANKITA PEDNEKAR

Abstract. Solving multivariable nonlinear equations is frequently very computationally complex to do so, of which Gröbner bases simplifies this computation significantly, along with its applications in other important fields. This paper will explore the necessary preliminaries to Gröbner bases, Buchberger's Algorithm, and envelopes as well as further directions interested readers can take.

## 1. Background

The usual technique for solving multivariable linear equations is row-reduction (also known as Gaussian elimination), using matrices to solve the linear equations as in the below example:

$$\begin{aligned} 2x+y+2z &= 0 \\ x+3y+z &= 0 \\ 2x+y+z &= 1 \end{aligned} \quad = \quad \begin{bmatrix} 2 & 1 & 2 & 0 \\ 1 & 3 & 1 & 0 \\ 2 & 1 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

$$= \boxed{(1,0,-1)}$$

However in the case of which one wants to solve multivariable nonlinear equations, such as $\{x^3+3y^2+z=4, x^5+x^3+6y^3=2, x^4+y^4+z^4=16\}$ in a strict method for as many variables, this cannot be solved through Row-Reduction, and can be through the means of Gröbner bases. Gröbner bases allows for a strict conversion of a multivariable nonlinear system of equations into a sequence of single variable equations, which makes it a lot more easier to solve. This is similar to how Row Reduction works, where a system of multivariable linear equations is converted into a matrix for the solution. Additionally, dealing with nonlinear equations leads to extremely large computation times, as well as being very tricky to solve by hand, especially with

*Date*: July 15, 2024.

large values and/or amount of variables. Computing generating sets in ideals, as discussed further in the Preliminaries section is additionally very complex, even by hand, which can be simplified with an algorithm. A standardized and quick computation method is needed when current methods are faulty.

Introduced in 1965 by Bruno Buchberger in his thesis along with Gröbner bases for an algorithmic method of solving polynomial equations, now known as Buchberger's Algorithm. Gröbner bases have now become a significant method in solving both linear and nonlinear equations. With the ability to additionally find the intersection of ideals, find the envelope of specific curves, and find degenerate solutions of geometric proofs, it can also be applied in fields ranging from graph theory to robotics and coding theory. This paper will investigate from Gröbner bases, to Buchberger's Algorithm, and to finally its usage in solving envelopes, and following from David Cox's Ideals, Varieties, and Algorithms.

## 2. Preliminaries

2.1. **Rings.** The ring $R$ is a set that is an abelian group under addition (meaning that it is associative, commutative, contains the additive identity and additive inverses of its elements), associative under multiplication, contains its multiplicative identity, and has its multiplication distributive over addition.

For example, the ring of integers is a ring because for any $a, b, c \in \mathbb{Z}$ :

- Abelian: $(a + b) + c = a + (b + c), a + b = b + a, 0$ is the additive identity, and $\mathbb{Z}$ contains the additive inverses, which are the opposites of the numbers.
- Associative under multiplication: $(a \times b) \times c = a \times (b \times c)$
- 1 is the multiplicative identity
- Multiplication follows both left and right distributivity because both $a \times (b + c) = (a \times b) + (a \times c)$ and $(a + b) \times c = (a \times c) + (b \times c)$ is true

Additionally, the polynomial ring, denoted as $R[x]$ and is composed entirely of polynomials, is also a ring because it also follows the same sets of rules, as described above. It is simple to replace $a, b, c \in \mathbb{Z}$ to $a, b, c \in \mathbb{Z}[x]$ or $\mathbb{C}[x]$ and to think of it as also as a ring.

2.2. **Ideals.** An ideal is a subring of a ring, but with a stronger condition such that for an ideal $I$ and a ring $R$, it follows that for all $r \in R$ and $m \in I$, $mr \in I$.

**Example 2.1.** For the ring of integers, a possible ideal containing $n$ will also contain its multiples of $n$, such that the set of multiples of $n$ in the ring of integers forms an ideal. All ideals of $\mathbb{Z}$ are in the form of the multiples of $n$ for some $n$. In the case of the polynomial ring, all multiples of the form 'the multiples of $f$' for some $f$ additionally form an ideal.

**Definition 2.2.** To generate an ideal means that every value of $f_n \in I$ can be expressed in terms of

$$f_n = h_1 f_1 + h_2 f_2 + ... + h_m f_m$$

where $h \in R$ and $f \in I$. In this case, if every ideal in the ring is generated by a single element, then it can be called the principal ideal domain.

**Definition 2.3.** A principal ideal domain is where every ideal is principal, or is generated by one element.

In the case earlier where all of the multiples of $n$ will form an ideal in $\mathbb{Z}$, this means that $n$ generates the ideal and therefore is $\mathbb{Z}$ a principal ideal domain. In the case of polynomial rings, if there is one polynomial that generates the ideal, then $\mathbb{Z}[x]$ will additionally be called the principal ideal domain. Then, because $\mathbb{Z}[x_1, x_2, ..., x_n]$ contains and is going to be generated by more than one element, it will not be a principal ideal domain.

This fact shows us why ideals in $\mathbb{Z}[x_1, \dots x_n]$ are hard to understand, compared with $\mathbb{Z}$ or $\mathbb{Z}[x]$, as Grobner bases are meant to be a tool for handling ideals in this case. Note that many of the rings studied later in this paper will be not be principal ideal domains, which Gröbner bases can be used to validate this.

2.2.1. *Euclidean's Algorithm.* As Euclidean's Algorithm is used to find the greatest common divisors of two integers, as the goal of an ideal essentially finds the generators in a polynomial ring. This can be used to find if two ideals are the same or for polynomial long division by comparing the generating sets.

## 2.3. **Noetheriananity and the Ascending Chain Condition.**

**Definition 2.4.** A ring satisfies the Ascending Chain Condition if an initial ideal can be broken into smaller ideals, of which will be expressed as

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq ...,$$

which will be finite, or where for such $N$ in

$$I_N = I_{N+1} = I_{N+2} = ...$$

will be true.

**Definition 2.5.** A Noetherian ring is a ring that satisfies the Ascending Chain Condition.

Examples of a Noetherian ring is the ring of integers, as in the example of where the ideal can contain the multiples of 8, which can be contained in the multiples of 4, which can ultimately be contained in the ideal containing multiples of 2, as below:

$$\{\text{multiples of } 8\} \subseteq \{\text{multiples of } 4\} \subseteq \{\text{multiples of } 2\} \subseteq \mathbb{Z},$$

or otherwise written as

$$(8) \subseteq (4) \subseteq (2) \subseteq \mathbb{Z}.$$

Because there is no larger ideal the ring itself, the maximal ideal in $\mathbb{Z}$ are the ideals generated by the prime numbers $(p)$.

**Definition 2.6.** The Ascending Chain Condition is additionally true for multivariable polynomials because of Hilbert's Basis Theorem, which states that if $R$ is a Noetherian ring, then the $R[x]$ and $R[x_1, x_2, ..., x_n]$ will additionally be Noetherian rings.

From this, since $\mathbb{Z}$ is a Noetherian ring, then this would mean the rings we will be studying, $\mathbb{Z}[x]$ and $\mathbb{Z}[x_1, x_2, ..., x_n]$ will additionally be Noetherian, such that the Ascending Chain Condition can follow through our later calculations. Additionally, there is a further point about Noetherian Rings such that:

**Definition 2.7.** Every ideal in a Noetherian Ring is finitely generated.

**Example 2.8.** An example of a non-Noetherian ring is the ring $\mathbb{Z}[x_1, \dots]$, because the ideal $(x_1)$ will be contained in an infinite ordering of ideals, as below

$$(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \dots.$$

On the contrary, $\mathbb{Z}[x_1, \dots x_n]$ is a Noetherian ring as the below is true:

$$(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \cdots \subseteq (x_1, \dots x_n).$$

2.4. **Admissible Ordering.** An admissible order, or otherwise called a monomial order, orders the terms in the polynomial. This is central in Gröbner bases as it is used in the calculation of the polynomials in the Gröbner basis and that the monomial order is relative to the Gröbner basis.

In the case of a single variable ordering, the degrees are often compared to find the greater polynomial, such as how when $n < m$, $x^n < x^m$.

However in the cases of compare multivariable polynomials, such comparison by degree becomes confusing. There are many types of orderings that are involved with Gröbner bases, but a majority of the examples discussed in this paper will revolve around **lexicographic ordering**.

Lexicographic ordering on monomials can be defined as if $x > y$ and $n < n'$ then $x^n y^m < x^{n'} y^{m'}$, essentially ignoring the other variable $y$ with the focused variable being $x$ because $x$ will be greater than $y$. It's very similar to arranging terms by ordering single variable polynomials but the other variables in multiplication will be ignored if they are less than the greatest variable. However in the case that $n = n'$ and $m < m'$, then $x^n y^m < x^{n'} y^{m'}$, where if the exponents of $x$ are equal, then the next greatest variable is then taken into consideration.

**Example 2.9.** In the example that we have $x > y > z$, and we wish to order the polynomials in the set $\{x^4, x^3, x^3y^3, x^3z^3, y^3z^3\}$, we will achieve that

$$x^4 > x^3y^3 > x^3z^3 > x^3 > y^3z^3.$$

The leading monomial is the largest monomial found from the ordering. In the previous example, the leading monomial would then be $x^4$. The leading monomial of a function $f$ is denoted as $LM(f)$. The leading monomial term will be the highest term of the leading monomial.

## 3. Gröbner Bases

**Definition 3.1.** A Gröbner basis can be defined as a set of polynomials when for all $g_i \in G$ and all $f_j \in I$, $G$ denoting the Gröbner basis and $I$ denoting the ideal,

$$LM(g_i)|LM(f_j).$$

It could additionally be phrased that the leading monomials generate the ideal.

Alternatively, a generating set will be called a Gröbner basis if all of the highest power product (leading power product or the leading monomial term) in the polynomials of the linear combinations are a multiple of at least one of the highest power products.

The second definition essentially checks that the leading power product, found by linear combinations, will be a multiple of the power products in the ideal. It follows that if the ideal is generated by the Gröbner basis then the polynomials will be linear combinations of the one or more of the highest power products, meaning that both definitions are two perspectives that are essentially the same. Comparing the highest power product of the polynomials from linear combinations will also be generating the ideal as a whole.

**Definition 3.2.** A Gröbner basis is called reduced if all of the elements are not multiples of the other elements, or if the elements are irreducible by the elements of the basis, and if the leading coefficient is 1.

It is important to note that a reduced Gröbner basis is typically used as a labeling term, which the later discussed Buchberger's Algorithm will sometimes output reduced Gröbner bases, but there is no current algorithm to find the reduced Gröbner bases. Next, we will show that the reduced Gröbner basis is unique if $I \neq 0$, and two ideals are equal if and only if they have the same reduced Gröbner basis.

**Theorem 3.3.** Every ideal has a unique reduced Gröbner basis.

*Proof.* We will prove by contradiction and begin by assuming that $G$ and $H$ are both the same reduced Gröbner bases. From this, for all $g_i \in G$ and $h_i \in H$,

$$LM(g_i) = LM(h_i)$$

after properly arranging each of the polynomials in the Gröbner bases. Since the Gröbner bases generate the ideal and ideals are closed under addition, then $g_i - h_i \in I$.

Additionally, for some values $g_k \in R$ and $f_j \in I$, $LM(g_k)|LM(f_k)$ as per the definition of a Gröbner basis. Then if $g_i - h_i = f_j$, this can be rewritten to be that

$$LM(g_k)|LM(g_i - h_i).$$

Because we had initially stated that $G$ and $H$ were the same reduced Gröbner basis, and we had initally found that $LM(g_i) = LM(h_i)$, this would mean that the terms would cancel each other out because then $LM(g_i - h_i) = 0$. We had found that for some $g_k \in G$ then $LM(g_k)|LM(g_i - h_i)$ but since $LM(g_i - h_i)$ has been reduced, then it would not be possible since $G$ and $H$ are both reduced. Therefore this contradiction proves that $g_i$ must equal $h_i$ when both of the Gröbner bases are reduced, so then $G$ must additionally equal $H$, meaning that every ideal will have exactly one reduced Gröbner basis.

The calculation of Gröbner bases, and that is repeated used in Buchberger's Algorithm, is based on finding the S-polynomial of two polynomials $f, g \in R$ at a time, as below:

$$S(f,g) = f \cdot \frac{\text{LCM(LM(f),LM(g))}}{\text{LT(f)}} - g \cdot \frac{\text{LCM(LM(f),LM(g))}}{\text{LT(g)}},$$

where $LT$ denotes the leading term and $LM$ denotes the leading monomial. The calculation of the S-Polynomial follows that if $f, g \in I$, then $S(f,g) \in I$.

**Theorem 3.4.** Buchberger's Criterion: If for all $f_i$ and $f_j$ in the set $f$ has that $f|S(f_i, f_j)$, then $f$ will be a Gröbner Basis for all pairs in the set.

*Proof.* We begin by letting $f$ be a nonzero polynomial in $I$, and can be expressed as

$$f = \sum_{i=1}^{k} a_i g_i$$

where $a_i \in Z[x_1, x_2 \ldots, x_n]$ and $g_i \in G$ with $k$ polynomials. Now because $g_i$ is the Gröbner basis polynomials, it follows that the multidegree of $f$ will be at most the maximum possible multidegree of $a_i g_i$ as a result of monomial ordering and it thus being at a greater degree.

This leads to two possible cases: where the multidegrees are equivalent and when the mutlidegree of $f$ is less than the maximum mutlidegree of $a_i g_i$. In the case that these multidegrees are equivalent, then this means that the leading term of $f$ will thus be divisible by the leading term of $g_i$, or will be generated by the leading term of $g_i$. As such, then this can get that

$$\text{LT}(f) \in \langle \text{LT}(g_1), \ldots \text{LT}(g_k) \rangle.$$

However in the case that the multidegree of $f$ is less than $a_i g_i$, then we can use a different value for $g$ in $G$ such that for $g_j$, $a_i g_j$ will have a greater multidegree, which also gets the same result as in the previous case.

If we then denote

$$\gamma = \max(\text{multideg}(a_i g_i)) \text{ when minimal,}$$

we can further express this as

$$\begin{aligned}\gamma &= \sum_{\text{multideg}(a_i g_i)=\gamma} a_i g_i + \sum_{\text{multideg}(a_i g_i)<\gamma} a_i g_i \\ &= \sum_{\text{multideg}(a_i g_i)=\gamma} \text{LT}(a_i) g_i + \sum_{\text{multideg}(a_i g_i)=\gamma} (h_i - \text{LT}(a_i)) g_i + \sum_{\text{multideg}(a_i g_i)<\gamma} a_i g_i,\end{aligned}$$

when $\gamma$ is reduced from the calculations of finding the S-Polynomial. The second and third terms have a multidegree less than $\gamma$ as the second term subtracts this case and the third term states it.

The first term, $\sum_{\text{multideg}(a_i g_i)=\gamma} \text{LT}(a_i) g_i$, can be set such that $\text{LT}(a_i) g_i = k_i$. From this, it will be a linear combination of $S(p_i, p_j)$ can be expressed in terms of $S(g_i, g_j)$ where

$$S(p_i, p_j) = \frac{\text{LT}(g_i, g_j) S(g_i, g_j)}{\text{lcm}(\text{LM}(g_i)), \text{LM}(g_j))}.$$

Furthermore, because each of the polynomials in the Gröbner basis can be expressed in terms of the values in the original ring, as we donate $b \in R[x_1, \ldots, x_n]$, we get that

$$S(g_i, g_j) = \sum_{p=1}^{k} b_p g_p,$$

to get that the multidegree of $b_p g_p$ would be at most the multidegree of $S(g_i, g_j)$. We now aim to obtain this in terms of the earlier term such that $\sum_{\text{multideg}(a_i g_i)=\gamma} \text{LT}(a_i) g_i$.

As such, we find that if $d_p = \frac{\text{LT}(g_i, g_j)}{\text{lcm}(\text{LM}(g_i)), \text{LM}(g_j))} b_p$, then our ealier expression of $\frac{\text{LT}(g_i, g_j) S(g_i, g_j)}{\text{lcm}(\text{LM}(g_i)), \text{LM}(g_j))}$ can then be rewritten to

$$\frac{\text{LT}(g_i, g_j) S(g_i, g_j)}{\text{lcm}(\text{LM}(g_i)), \text{LM}(g_j))} = \sum_{p=1}^{k} d_p g_p.$$

This means that the multidegree of $d_p g_p$ would be then at most the multidegree of $\frac{\text{LT}(g_i, g_j) S(g_i, g_j)}{\text{lcm}(\text{LM}(g_i)), \text{LM}(g_j))}$, which will still be less than $\gamma$ because the leading term of $S(g_i, g_j)$ is less than $\text{lcm}(\text{LM}(g_i)), \text{LM}(g_j))$.

Becauuse we had initially stated that $\gamma$ was minimal, this contradicts this fact as

$$\sum_{\text{multideg}(a_i g_i)=\gamma} \text{LT}(a_i) g_i = \sum_{p=1}^{k} d_p g_p,$$

and shows that the remainder will thus be zero.

3.1. **Buchberger's Algorithm.** Buchberger's Algorithm follows that:
Input: I = $(f_1, \ldots, f_s)$
Output: $G = (g_1, \ldots, g_t)$ for $I$, with $G \subseteq I$
Repeat: $G := I$
$G' := G$
For every unique pair $\{f_1, f_2\} \in G'$
$g := S(f_1, f_2)$
If g $\neq 0$, then $G := G \cup \{g\}$
Until G = G';
Return G;

The algorithm begins by taking a finite set of polynomials, or by taking a generating set for the ideal, and initializes the Gröbner basis $G$ to the ideal $I$, so that $G$ contains all of the polynomials in $I$. The repeat function allows the Gröbner basis $G$ to stabilize such that no more polynomials are added. From this, the current $G$ is copied into a new Gröbner basis $G'$ to make changes to this basis by repeated calculating for the S-polynomial. Each of the polynomial pairs in $G'$ was used to calculate an S-polynomial and then was altered dependent on the following two results from the next two lines. If the S-polynomial found from this calculation is not zero, then it would be added in the Gröbner basis $G$. Finally when all the calculations are completed, it will repeat until $G$ does not change, essentially until $G$ becomes the Gröbner basis. From this, it will return the Gröbner basis $G$ for the given ideal.

**Example 3.5.** We can begin with the input ideal such that

$$I = \langle x^2 - y^2, xy^2 - z^3 \rangle,$$

and we expect an output Gröbner basis. First, the Gröbner basis initializes $I$ and creates a Gröbner basis include the polynomials of the ideal. From this, repeated S-Polynomial calculations with pairs in the ideal until there are no further polynomials that can be abstracted. This calculation is shown below:

$$S(f_1, f_2) = LCM(LT(x^2 - y^2), LT(xy^2 - z^3))(\frac{x^2 - y^2}{x^2} - \frac{xy^2 - z^3}{z^3}) = \boxed{xz^3 - y^4} = f_3$$
$$S(f_1, f_3) = LCM(LT(x^2 - y^2), LT(xz^3 - y^4))(\frac{x^2 - y^2}{x^2} - \frac{xz^3 - y^4}{xz^3}) = y^2(xy^2 - z^3)$$
$$S(f_2, f_3) = LCM(LT(xy^2 - z^3), LT(xz^3 - y^4))(\frac{xy^2 - z^3}{xy^2} - \frac{xz^3 - y^4}{xz^3}) = \boxed{y^6 - z^6}.$$

If there are any polynomials that can be written in terms of the other polynomials, it will not be added into the Gröbner basis such that the remainder will be 0. As such, the output will be the Gröbner basis

$$G = \{x^2 - y^2, xy^2 - z^3, xz^3 - y^4, y^6 - z^6\}$$

*Proof.* To begin this proof, we can begin with the fact that the Gröbner basis will be a subset of the ideal, otherwise shown as $G \subseteq I$. Polynomials in $G$ can be also found by calculating the S-polynomial of two polynomials in $I$, which can be expressed in terms of two random polynomials in $I$, $f_1$ and $f_2$. The remainder, or the S-polynomial where $S(f_1, f_2) \in I$, would additionally be in the ideal. This new Gröbner basis including $S(f_1, f_2)$ can then be written as $G'$.

Buchberger's Algorithm will not add additional polynomials into the Gröbner basis when there are repetitions of the polynomials. This is can be proven by that the leading terms of $G'$ would then be a subset of the leading terms of $G$ because $G'$ itself is a subset of $G$. However, $G'$ must be equal to $G$. By the Ascending Chain Condition, where $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$, then $I_N = I_{N+1} = I_{N+2} = ...$ for some $n$, meaning that our current chain will stabilize such that the leading term set of $G'$ and $G$ will equate after a finite set of steps meaning that Buchberger's algorithm will not output any values in the Gröbner basis where there are repetitions of the polynomials.

3.2. **Elimination and Extension Theorems.** To solve actual equations, we use some technical facts about Gröbner bases, called the Elimination and Extension Theorems.

**Definition 3.6. Elimination Theorem:** If $I \subseteq R[x_1, ..., x_n]$, then the Gröbner basis of the $k$-th elimination ideal $I_k$ is

$$G_k = G \subseteq R[x_{k+1}, ..., x_n].$$

The elimination ideal reduces the variables in the ring such that the if the given ideal could be expressed as $I = \langle f_1, \dots f_n \rangle = R[x_1, \dots, x_n]$, the $k$th elimination ideal will then become

$$I_k = I \cap R[x_{k+1}, \dots, x_n] \subseteq R[x_{k+1}, \dots, x_n].$$

This is then similarly seen with the Gröbner bases, as it is a subset of the ideal.

We can begin with the fact that the Gröbner basis $G$ is a subset of the ideal $I$, meaning that for a $k$-th elimination ideal, $G_k \subseteq I_k$. Additionally, if this is true, because the leading terms in the ideal are a subset of the leading terms in the Gröbner basis, then

$$\langle LT(I_k)\rangle \subseteq \langle LT(G_k)\rangle$$

will additionally be true.

We then assume that there are some $f \in I_k$ and $g \in G_k$. Since $LT(g)|LT(f)$, then $LT(g)$ will only be consisting of $x_{k+1}, ..., x_n$, which otherwise can be expressed as

$$LT(g) \in R[x_{k+1}, \ldots, x_n].$$

As such, then $g \in R[x_{k+1}, \ldots, x_n]$. As such, then

Since we are in lexicographic order, $LT(g) \in m[x_{k+1}, ...x_n]$ so $g \in m[x_{k+1}, ...x_n]$, so $g \in G_k$. From this, it then becomes apparent that $G_k$ would then be equal to when $G$ is a subset of the eliminated ring.

**Definition 3.7. Extension Theorem:** If $I = \langle f_1, ..., f_n\rangle \subseteq \mathbb{C}[x_1, ..., x_n]$, each $f$ can be expressed as $f_i = c_i(x_2, ..., x_n)x_1^{N_i}$ such that $c_i \in \mathbb{C}x_1, ..., x_n]$ and $I_1$ is the first elimination ideal of $I$. If we have the partial solution $(a_2, ..., a_n) \in \mathbf{V}(I_1)$ but $(a_2, ..., a_n) \notin \mathbf{V}(c_1, ..., c_n)$, then there exists such $a_1 \in R$ where $(a_1, ..., a_n) \in \mathbf{V}(I)$.

Additionally, if extended to the $k$-th elimination ideal, the definition can then be written as:

**Definition 3.8. Extension Theorem (with the $k$-th elimination ideal):** If $I = \langle f_1, ..., f_n\rangle \subseteq \mathbb{C}[x_1, ..., x_n]$, each $f$ can be expressed as $f_i = c_i(x_{k+1}, ..., x_n)x_1^{N_i}$ such that $c_i \in \mathbb{C}[x_1, ..., x_n]$ and $I_1$ is the first elimination ideal of $I$. If we have the partial solution $(a_{k+1}, ..., a_n) \in \mathbf{V}(I_k)$ but $(a_{k+1}, ..., a_n) \notin \mathbf{V}(c_1, ..., c_n)$, then there exists such $a_k \in R$ where $(a_1, ..., a_n) \in \mathbf{V}(I)$.

Simply phrased, the Extension Theorem allows for a solution, such as the solution $(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$, to be extended into the larger ideal (or sometimes the original equations), which the previous example solution would then become $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$.

It should additionally be stated that the extension theorem only works for $\mathbb{C}$ because it reaches solutions that are not possible to be solved under the field of $\mathbb{R}$, and would thus be false.

*Proof.* We begin this proof by noting that $c_i$ must be nonzero because all of the coefficients of the polynomials are nonzero. From this, since $c_i \neq 0$, then this means that

$$\mathbf{V}(c_1, \ldots, c_n) = 0$$

because it is a vanishing solution, meaning that all such values must equate to zero.

However, because the $c_i$s are the leading coefficients, this would mean that $(a_2, ..., a_n) \notin \mathbf{V}(c_1, ..., c_n)$. If the leading coefficients do disappear, then the Extension Theorem would fail when calculating with equations. However, because $(a_2, ..., a_n) \notin \mathbf{V}(c_1, ..., c_n)$, then the Extension Theorem will not fail.

### 3.3. **Examples.**

3.3.1. *Multivariable Linear Equation.* We begin by finding the solutions for a multivariable linear equations using Gröbner bases. We have the equations

$$\begin{aligned} 2x + y + 2z &= 0 \\ x + 3y + z &= 0 \\ 2x + y + z &= 1, \end{aligned}$$

which then can be used to form the ideal

$$I = \langle 2x + y + 2z, x + 3y + z, 2x + y + z - 1 \rangle.$$

From this ideal, we then calculate the Gröbner basis of each of the pairs, as below:

$$\begin{aligned} S(f_1, f_2) &= (2x + y + 2z) \cdot \frac{2x}{2x} - (x + 3y + z) \cdot \frac{2x}{x} = -5y \\ S(f_1, f_3) &= (2x + y + 2z) \cdot \frac{2x}{2x} - (2x + y + z - 1) \cdot \frac{2x}{2x} = z + 1 \\ S(f_2, f_3) &= (x + 3y + z) \cdot \frac{2x}{x} - (2x + y + z - 1) \cdot \frac{2x}{2x} = 5y + z + 1 \end{aligned}$$

Notice that the $x$ variable has been removed from the Gröbner bases as a result of the Elimination Theorem, making the final Gröbner basis as:

$$\langle -5y, z + 1, 5y + z + 1 \rangle.$$

We can check for further for extra polynomials to be added in the Gröbner basis, but this equation can be easily solved. We solve the zeros of the Gröbner basis as below (note that $S_3$ was removed from the calculations because they would get for the same values),

$$\begin{aligned} -5y &= 0 \\ z + 1 &= 0 \end{aligned}$$

meaning that $y = 0$ and $z = -1$. This is allowed because of the Extension Theorem where the solutions found in the Gröbner basis will also be solutions

of the ideal and the original equations. Going back to our original equations, it can easily be solved that $x = 1$, meaning that we get the point $(1, 0, -1)$ as the final answer. Our earlier example at the beginning through solving through Row Reduction also produces a similar result, and when graphing, we produce the same result.

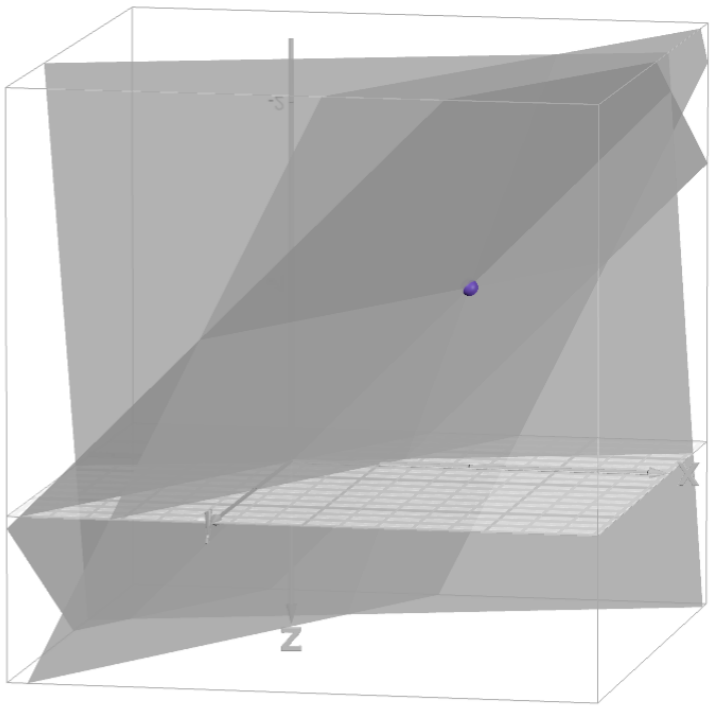


FIGURE 1. The purple point is the point of intersection.

3.3.2. *Multivariable Nonlinear Equation.* We now present an example for solving nonlinear multivariable equations. We have the system of equations with the following equations: $x^2 + y - z = 1, x + zy = 5$, and $xyz = 3$. From this, the ideal will become

$$I = \langle x^2 + y - z - 1, x + zy - 5, xyz - 3 \rangle$$

and the Gröbner bases of this will then be:

$$g_1 = z^4 - 17z^3 - 14z^2 + 75z + 3$$
$$g_2 = 104y + 25z^3 - 420z^2 - 434z + 1809$$
$$g_3 = 104x - 5z^3 + 84z^2 + 66z - 445.$$

From this, $g_1$ can be factored to the following values: $-2.3471, -0.0397, 1.8332,$ and $17.5536$. These values can then be substituted into $g_2$ and $g_3$ to get the following points: $(0.6972, -1.8332, -2.3471)$, $(4.3028, -17.5536, -0.0397)$, $(0.6972, 2.3471, 1.833)$, and $(4.3028, 0.0397, 17.5536)$.

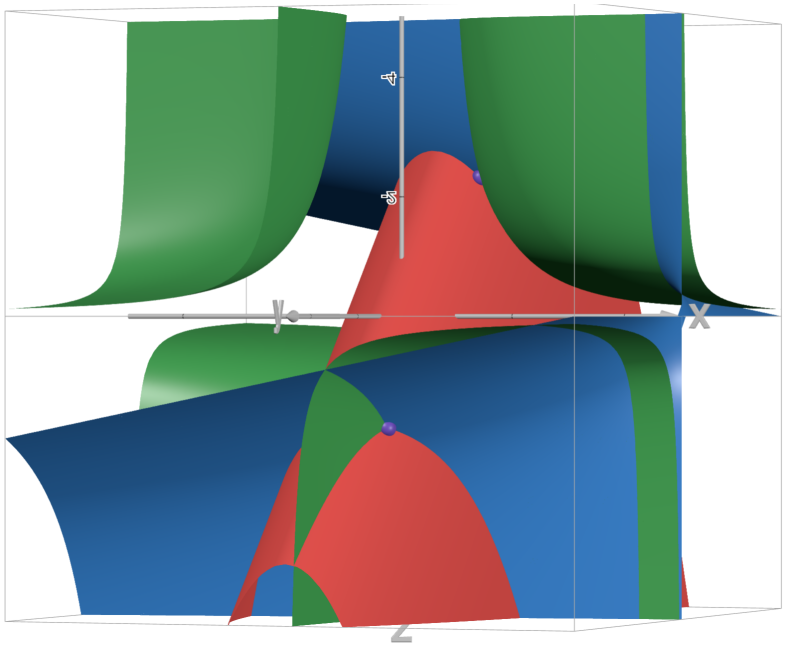


FIGURE 2. The purple points shown are the points of connection from all three curves.

3.3.3. *Multivariable Nonlinear Equation with More Variables.* To find the Gröbner Basis of the ideal $I = \langle x^2 - y, x^3 - z \rangle$ with lexicographic order $x > y > z$ through the Buchberger Algorithm, we can begin by computing for the S-polynomial

$$S(x^2 - y, x^3 - z) = LCM(x^2 - y, x^3 - z)(\frac{x^2 - y}{x^2} - \frac{x^3 - z}{x^3}) = \boxed{-xy + z}.$$

Our Gröbner basis will then contain $-xy + z$ because it cannot be reduced further with $x^2 - y$ and $x^3 - z$. This can be labeled as the value for $S(f_1, f_2)$, and then be continued to find the values of $S(f_1, f_3)$ and $S(f_2, f_3)$ to find more Gröbner bases. Furthermore, if any more polynomials are found and added to the Gröbner basis, this can then be further used to calculate the values of $S(f_1, f_4), S(f_2, f_4)$, and further as shown below:

$$S(f_1, f_3) = LCM(LT(x^2 - y), LT(-xy + z))(\frac{x^2 - y}{x^2} - \frac{-xy + z}{-xy}) = \boxed{xz - y^2}$$

$$S(f_2, f_3) = LCM(LT(x^3 - z), LT(-xy + z))(\frac{x^3 - z}{x^3} - \frac{-xy + z}{-xy}) = z(x^2 - y)$$

$$S(f_1, f_4) = LCM(LT(x^2 - y), LT(xz - y^2))(\frac{x^2 - y}{x^2} - \frac{xz - y^2}{xz}) = y(-xy + z)$$

$$S(f_2, f_4) = LCM(LT(x^3 - z), LT(xz - y^2))(\frac{x^3 - z}{x^3} - \frac{xz - y^2}{xz}) = (xy + z)(-xy + z)$$

$$S(f_3, f_4) = LCM(LT(-xy + z), LT(xz - y^2))(\frac{-xy + z}{-xy} - \frac{xz - y^2}{xz}) = \boxed{y^3 - z^3}$$

Checking with $f_5 = y^3 - z^3$, we will find that there will be no more polynomials that can be added to the basis. This situation appears when there are no values of $x$ left to create pairs with in the Gröbner basis, and as such this calculation can terminate. The Gröbner basis will then contain the set $\{x^2 - y, x^3 - z, -xy + z, xz - y^2, y^3 - z^3\}$.

To know that we have finished the calculations, we can compute further with $f_5$ to test if there any more polynomials that can be added to the basis.

$$S(f_1, f_5) = LCM(LT(x^2 - y), LT(y^3 - z^3))(\frac{x^2 - y}{x^2} - \frac{y^3 - z^3}{y^3})$$

$$S(f_2, f_5) = LCM(LT(x^3 - z), LT(y^3 - z^3))(\frac{x^2 - y}{x^2} - \frac{y^3 - z^3}{y^3})$$

$$S(f_3, f_5) = LCM(LT(-xy + z), LT(y^3 - z^3))(\frac{x^2 - y}{x^2} - \frac{y^3 - z^3}{y^3})$$

$$S(f_4, f_5) = LCM(LT(xz - y^2), LT(y^3 - z^3))(\frac{x^2 - y}{x^2} - \frac{y^3 - z^3}{y^3})$$

It then becomes unnecessary to continue because there are no further polynomials that can be added to the Gröbner basis as they can all be expressed in terms of the other polynomials in the Gröbner basis.

We find that because $f_5$ does not contain any values of $x$, the $LCM$ of the leading terms become undefined, as such, it means that there will be no further solutions to be added to the Gröbner basis. Finally, the final Gröbner basis is

$$G = \langle x^2 - y, x^3 - z, -xy + z, xz - y^2, y^3 - z^3 \rangle.$$

If we find the solution set, by solving with the original equations. Note that the Gröbner basis can be useful in more complex situations. The solution set

can then be expressed as

$$x = \pm\sqrt{y} = \sqrt[3]{z},$$

or as $(x, x^2, x^3)$. Graphing, we find that the final solution set matches along the curve of intersection, as shown below in the graph.

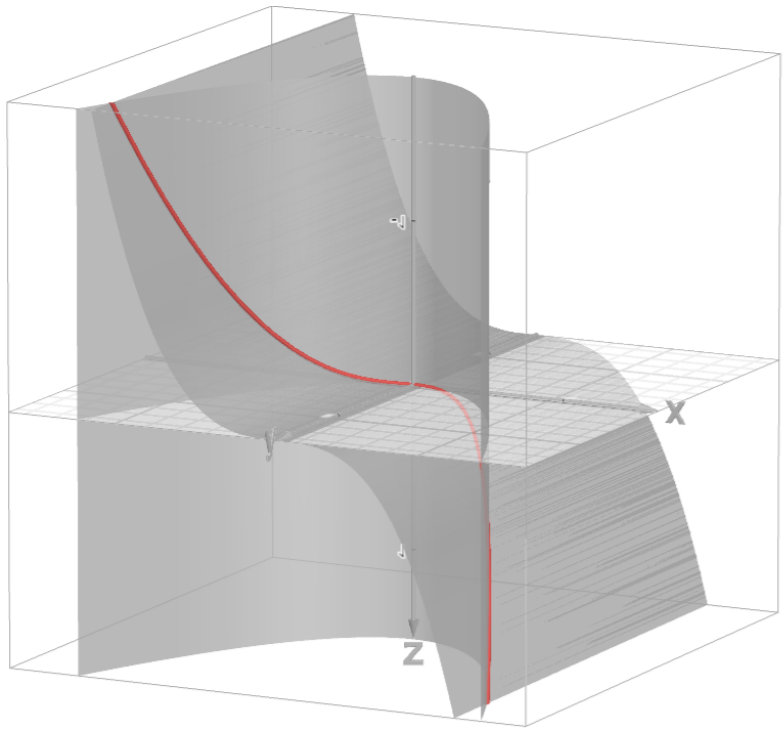


FIGURE 3. Curve of intersection labeled in red with the original equations.

3.3.4. *Equivalent Ideals.* As we had shown before, every ideal has a unique reduced Gröbner basis. If there exists two reduced Gröbner bases such that $G_1 = G_2$, then the ideals must be equal. Otherwise, $I_1 \neq I_2$.

## 4. Envelopes

If we have a family of curves, Gröbner bases can be used to formulate an equation that would depict the enveloping curve. However to begin, it is important to show how finding tangential lines from a single point can be found without using calculus.

**Example 4.1.** To begin, we can start with the fact that the tangent line will contain the point it will touch the original equation. Meaning that for some

$x$ and $y$ in the equation of the tangent containing point $(p, q)$, the following equations can be derived:

$$x = p + am$$
$$y = q + bm$$

We can then use these equations to solve for the tangential line on a curve. If we are looking for the tangent line on the parabola $y = x^3$ at the point $(1, 1)$, we would additionally express this as

$$1 + bm = (1 + am)^3,$$

which then can become

$$1 + bm = 1 + 3at + 3(at)^2 + (at)^3,$$

which will finally be simplified into

$$b = 3a + 3a^2m + a^3m^2.$$

The multiplicative zeros from this equation will thus be where the tangential line intersects $y = x^3$. To determine the multiplicity, it is found by the degree of the lowest non-zero term, which will thus be the term $a^3m^2$.

Since the term has $m^2$, it means that it that the multiplicity at the point $(1, 1)$ will be two, which will then mean that it is tangent to the curve since the multiplicity is greater than one.

To find the tangent line, we find the derivative of $y = x^3$ in respect to $x$ and substitute $(1, 1)$ now we know that a tangent line exists at that point. The derivative will thus be

$$\frac{dy}{dx} = 3x^2,$$

which can then be substituted to have the final tangent line of $y = 3x - 2$.

Doing these steps is important for the cases that there does not exist a tangent line to a curve, through checking the multiplicity at the intersection. Such curve is shown in Figure 4.

4.1. **Envelopes Example with a Family of Circles.** For envelopes, we can begin with an example polynomial that describes a family of circles:

$$(x - t)^2 + y^2 = t,$$

meaning that each circle has center of $(t, 0)$ and radii of $\sqrt{t}$.

**Lemma 4.2.** To find the equation for the envelope of the curves can be found when both the polynomial and the partial derivative in respect to $t$ must be both equal to zero.

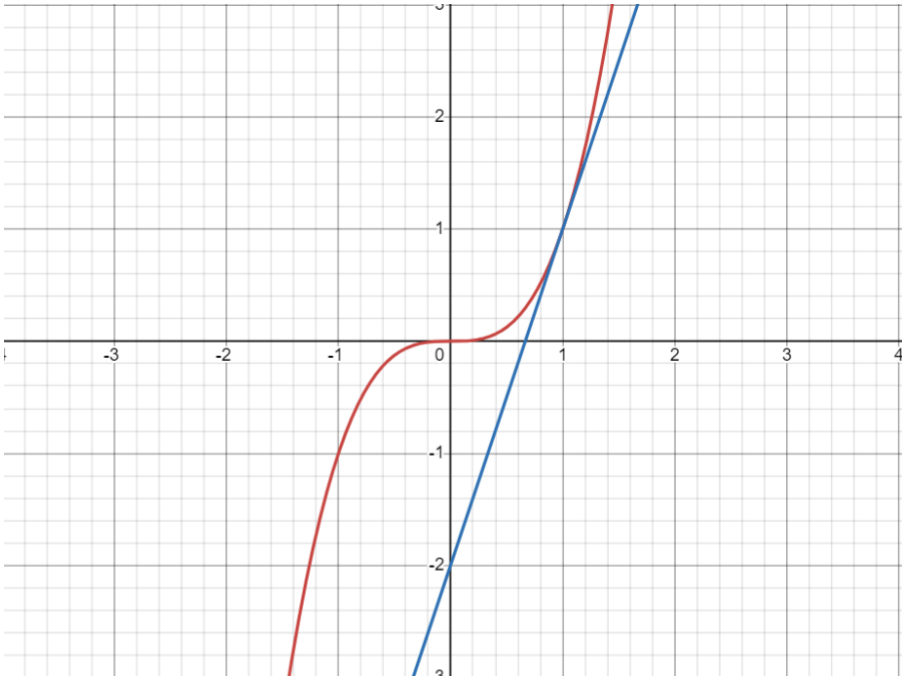


FIGURE 4. Original equation ($y = x^3$) and the tangent line ($y = 3x - 2$) at point $(1, 1)$.

From this,

$$f(x) = (x-t)^2 + y^2 - t = 0$$
$$\frac{\partial f(x)}{\partial t} = -2(x-t) - 1 = 0$$

This can then form the ideal

$$\{(x-t)^2 + y^2 - t, -2(x-t) - 1\},$$

which can then be turned into the Gröbner basis

$$\{4y^2 - 4x - 1, -2x - 1.\}$$

It can then be found from this that the equation $4y^2 - 4x - 1 = 0$ is the envelope for the family of circles of when $(x-t)^2 + y^2 = t$, as graphed in Figure 5.

4.2. **Envelopes Example with a Family of Spheres.** This additional application can be furthered with spheres. If we have the family of spheres that follows such rule that the equation to model this is

$$(x-t)^2 + y^2 + z^2 - t = 0,$$

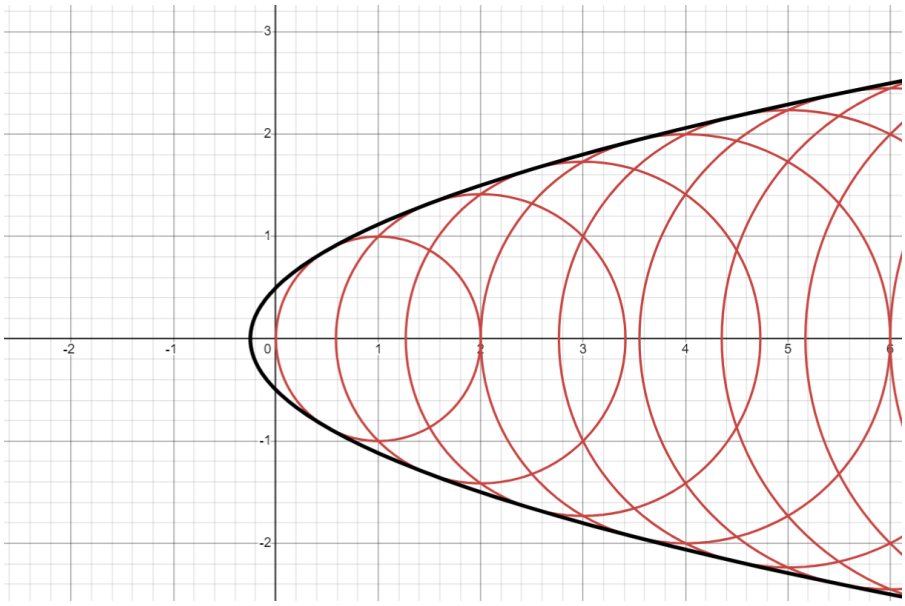


FIGURE 5. As shown, the parabola $4y^2 - 4x - 1 = 0$ is the envelope for the family of circles.

we can again follow the earlier steps in finding the envelope for this case. Note that in the 3rd dimension does not all necessarily have an envelope.

We then can find the partial derivative in respect to $t$ and find the Gröbner basis of these two equations, as follows:

$$f(x) = (x-t)^2 + y^2 + z^2 - t = 0$$
$$\frac{\partial f(x)}{\partial t} = -2(x-t) - 1 = 0.$$

The ideal with these equations becomes the following:

$$I = \langle (x-t)^2 + y^2 + z^2 - t, -2(x-t) - 1.$$

Solving for the Gröbner basis leads to the following:

$$G = \{-t + y^2 + z^2 + 0.25, -t + x + 0.5.\}$$

If we want to form an equation that will model the values of the Gröbner basis, it can thus be expressed by substituting the values of $t$, becoming $x + 0.5 = y^2 + z^2$, or

$$x - y^2 - z^2 + 0.5 = 0$$

as our solution for the parabola that models it. Graphing this shows that this parabola is therefore the envelope of the family of curves.

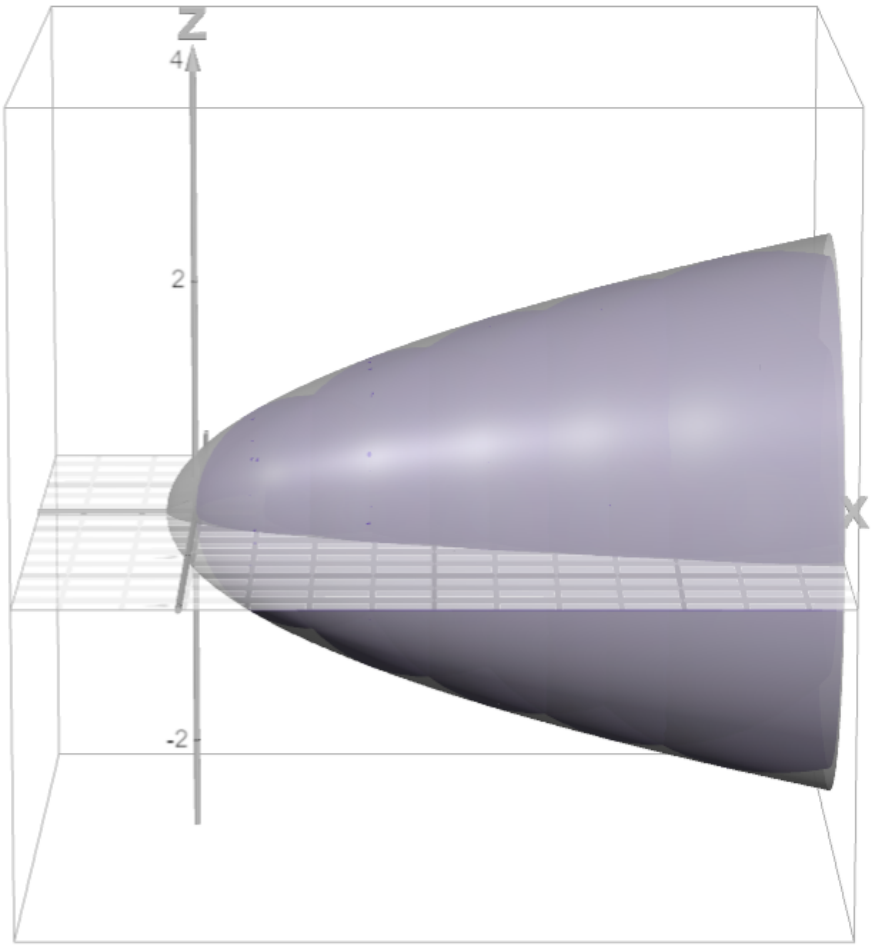


FIGURE 6. As shown, the parabola $x - y^2 - z^2 + 0.5 = 0$ is the envelope for the family of spheres in purple.

## 5. Conclusion

Overall, this paper explores the background of Gröbner bases and its application in solving multivariable nonlinear equations as well as finding envelopes for a family of curves. The Buchberger Algorithm relies heavily on the Buchberger Criterion such that the S-Polynomial can be used in calculated the Gröbner basis. To use Gröbner bases in solving equations, it is important to additionally understand the Elimination and Extension Theorems, of which allow for such computation and the usage of Gröbner bases in calculations, furthered even more through finding the envelopes of families of curves.

There are many further directions that an interested reader could explore. For example, the more intricate Hilbert Driven Buchberger Algorithm, having

homogeneous polynomials in it's ideal and Gröbner basis, has a faster run time than the Buchberger Algorithm, provided you start with extra information about the original ideal. Additionally, faster algorithms like the $F_4$ Algorithm directly uses Row Reduction for finding the remainders of the S-polynomials for the remainders and has termination.

Gröbner bases can also be used in geometric proofs, directly solving complex multivariable equations in coordinate geometry and even further in the plane $\mathbb{P}^2(\mathbb{R})$, such as Pappus's Theorem. Gröbner bases can also find the dimension of the algebraic variety and additionally find the images of these varieties under projections. Gröbner bases can also additionally be applied in graph theory, robotics (via the joint mechanics), and software engineering.

## 6. Acknowledgements

The author would like to thank Simon Rubinstein-Salzedo for the opportunity to participate in this program. The author would also like to thank Dora Woodruff for her constant encouragement and support, as well as her invaluable advice and feedback throughout this program.