2020

Gröbner Bases and Systems of Polynomial Equations

Rachel Holmes
Minnesota State University, Mankato

Gröbner Bases and Systems of Polynomial Equations

Rachel Holmes

An Alternative Plan Paper submitted in partial fulfillment of the requirements for the degree of Masters of Science in Mathematics and Statistics at Minnesota State University, Mankato

Mankato, Minnesota

December, 2020

This Alternative Plan Paper has been examined and approved by the following committee members:

Dr. Wook Kim, Advisor

Dr. Ruijun Zhao

Dr. Brandon Rowekamp

Acknowledgments

To my advisor, Dr. Wook Kim, for his unending guidance, knowledge, motivation, and invaluable talent as an educator. To my committee members, Dr. Brandon Rowekamp and Dr. Ruijun Zhao, for their time and evaluation.

To my dear friends, Sarah and Alex, whom I am eternally grateful.

To my family, for their continual support and encouragement.

Contents

Abstract

This paper will explore the use and construction of Gröbner bases through Buchberger's algorithm. Specifically, applications of such bases for solving systems of polynomial equations will be discussed. Furthermore, we relate many concepts in commutative algebra to ideas in computational algebraic geometry.

1 Introduction

In 1965, Bruno Buchberger's PhD thesis "An algorithm for finding the basis elements of the residue class ring of a zero-dimensional polynomial ideal" examined an algorithm provided to him by his advisor, Wolfgang Gröbner. In his thesis he discusses the termination and computer implementation of this algorithm. Shortly thereafter, he becomes the first person to implement it at the first computer laboratory [2]. This paper will seek to examine this algorithm as well, specifically its termination as well as some applications.

In section 2 we recall some important concepts from abstract algebra, specifically ring and field theory. We also discuss and define some important aspects of polynomials, discuss ordering of monomials, and recall the division algorithm for polynomials in $k[x]$.

Section 3 contains many important results and definitions which will be used frequently throughout our discussion of Gröbner bases and Buchberger's Algorithm in Section 5. Here we discuss Buchberger's Algorithm and Buchberger's Criterion and examine them in depth to verify their termination. We also consider the Hilbert Basis Theorem, and an equivalent theorem, the Ascending Chain Condition. Prior to this we discuss the division algorithm as it is extended to the polynomial ring $k[x_1, \ldots, x_n]$ in section 4. We conclude by considering a few applications of Gröbner bases. Many of the examples throughout this paper will make use of the Groebner package in Maple 2020.

2 Preliminary Information

2.1 Polynomials and Polynomial Rings

Polynomials are key in the study of Gröbner bases and while polynomials are familiar to most, some standard definitions need to be reconsidered to hold in the case of multiple variables. Ordering for example is not so clear. One may be familiar with the standard form of a polynomial in one variable, in which we order terms in descending order based on degree of the exponent. Ordering monomials in descending order becomes less obvious when dealing with multivariate polynomials. For example, determining the standard form of a polynomial such as $f = 2x^2yz^3 + x^6 + y^5z$ is not so clear. To determine such a form, a few definitions are in order.

Definition 2.1. A **monomial** in $x_1, \ldots, x_n$ is a product of the form

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \cdots \cdot x_n^{\alpha_n}$$

where $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$. Then we can write $x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \cdots \cdot x_n^{\alpha_n}$.

Definition 2.2. The **total degree** of a monomial $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \cdots \cdot x_n^{\alpha_n}$ is the sum $\alpha_1 + \cdots + \alpha_n$, and we can denote the total degree of x^α as $|\alpha| = \alpha_1 + \cdots + a_n$.

Furthermore, we see when $\alpha = (0, \ldots, 0)$, $x^\alpha = x_1^0 \cdot \cdots \cdot x_n^0 = 1$.

Definition 2.3. A **polynomial** f in $x_1, \ldots x_n$ with coefficients in a field k is a finite

linear combination of monomials whose coefficients are in k. That is, we can write

$$f = \sum_{\alpha} a_\alpha x^\alpha$$

where $a_\alpha \in k$ and the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n)$.

Before discussing polynomial rings, it may first be useful to recall some basic axioms and definitions of rings and fields. Since polynomials have the commutative property, we will be concerned only with commutative rings.

Definition 2.4. A **commutative ring** consists of a set R and two binary operations " $+$ " and " $\cdot$ " for which the following axioms are satisfied for all $a, b, c \in R$:

i. (Associativity) $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

ii. (Commutativity) $a + b = b + a$ and $a \cdot b = b \cdot a$.

iii. (Distributivity) $a \cdot (b + c) = a \cdot b + a \cdot c$.

iv. (Existence of identities) There exists $0, 1 \in R$ such that $a + 0 = a$ and $a \cdot 1 = a$.

v. (Additive inverses) For every a there exists $-a$ such that $a + (-a) = 0$.

Notice the last axiom fails to require the existence of a multiplicative inverse; if a commutative ring also has multiplicative inverses for all nonzero elements, then it is called a field.

Definition 2.5. A **field** k is a commutative ring with the property that for all nonzero $a \in k$, there exists $a^{-1} \in k$ such that $a \cdot a^{-1} = 1$.

Definition 2.6. A **polynomial ring** $k[x_1, \ldots, x_n]$ is a commutative ring whose elements consist of the collection of polynomials whose coefficients belong to a field k and which has indeterminants $x_1, \ldots, x_n$.

The sum and products of any two polynomials will also result in a polynomial and it can be shown further that $k[x_1, \ldots, x_n]$ satisfies the axioms of a commutative ring. We will often make use of the general commutative ring $k[x_1, \ldots, x_n]$, but occasionally we may specify a specific ring such as $\mathbb{R}[x, y]$, which is the ring of polynomials with indeterminants x and y with coefficients coming from the field of real numbers.

Note that $x_1, \ldots, x_n$ in many texts are referred to as variables; here instead we refer to them as **indeterminants**. This is to distinguish that in general we are treating $x_1, \ldots, x_n$ as characters or symbols, and not always as variables for polynomial functions. Consider also the following definitions regarding polynomials.

Definition 2.7. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial in $k[x_1, \ldots, x_n]$. Then:

i. a_α is called the **coefficient** of the monomial x^α.

ii. If $a_\alpha \neq 0$ then we call $a_\alpha x^\alpha$ a **term** of f.

iii. The **total degree** of $f \neq 0$, which we denote $\deg(f)$, is the maximum $|\alpha|$ such that the coefficient a_α is nonzero.

As a note, the total degree of the zero polynomial is undefined or in some texts it is considered to have a degree of $-\infty$.

Example 2.8. Consider the polynomial $f = -2y^3z^5 + 13x^2 \in k[x, y, z]$; f has two terms: $-2y^3z^5$ and $13x^2$, which have total degrees of 8 and 2, and coefficients -2 and 13, respectively.

Alternative notation for the two monomials in the above example would be $(0, 3, 5)$ and $(2, 0, 0)$, respectively. These ordered triples $(x, y, z) \in \mathbb{Z}^3_{\geq 0}$ represent the degree of the individual indeterminants in a monomial and disregards any coefficients. This type of notation is convenient for ordering monomials which will be discussed further in section 2.5.

We next define affine spaces to allow us to communicate ideas about polynomials both algebraically and geometrically.

Definition 2.9. Given a field k and a positive integer n, then define the n-dimensional **affine space** over k to be the set

$$k^n = \{(a_1, \ldots a_n) : a_1, \ldots, a_n \in k\}.$$

Now we discuss the evaluation map of a polynomial f. That is, for a polynomial $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ and $\mathbf{a} = (a_1, \ldots, a_n) \in k^n$ we have the evaluation map $\mathrm{ev}_\mathbf{a} : k[x_1, \ldots, x_n] \to k$ defined by the homomorphism

$$f(x_1, \ldots, x_n) \to f(a_1, \ldots, a_n).$$

For $(a_1, \ldots, a_n) \in k^n$, each x_i is replaced with a_i in the given expression for f. Here $f(x_1, \ldots, x_n)$ is the function corresponding to the polynomial f. Since the coefficients

of f are in k, then $f(a_1, \ldots, a_n)$ also lies in k. This function takes in some ordered n-tuple from k^n and will output some constant belonging to k, i.e.,

$$f : k^n \to k.$$

A special case of this is when $f(a_1, \ldots, a_n) = 0$. This has two implications: either f is the zero *polynomial* or f is the zero *function*. If f is the zero polynomial, then all of its coefficients are zero and thus $f = 0$. If f is the zero function, then $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in k^n$. Fortunately, the latter is only a possibility when k is a *finite* field.

Proposition 2.10. *Let k be a infinite field and $f \in k[x_1, \ldots, x_n]$. Then $f = 0$ if and only if $f : k^n \to k$ is the zero function.*

The zero polynomial will certainly give the zero function, but to see why k must be an infinite field for this proposition to hold, consider the following example.

Example 2.11. Let $\mathbb{F}_2 = \{0, 1\}$ be the finite field with two elements and consider the polynomial

$$f = x^3 - x \in \mathbb{F}_2[x].$$

This is clearly not the zero polynomial, but it is the zero function since

$$f(0) = f(1) = 0.$$

We will only be concerned with polynomials rings over *infinite* fields such as $\mathbb{R}$ or $\mathbb{C}$, and as such the only polynomial in which $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in k^n$

is the zero polynomial $f = 0$. When $f(a_1, \ldots, a_n) = 0$, we refer to $(a_1, \ldots, a_n)$ as a **zero** or a **root** of f.

Theorem 2.12 (The Fundamental Theorem of Algebra)**.** *Every nonconstant polynomial $f \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.*

Many proofs for this theorem exist and can be found in many texts; while the statement may seem simple, the proof is often not and thus is omitted. Instead, to illustrate how we may fail to have a zero for a polynomial in $\mathbb{R}$, consider the following example.

Example 2.13. Let $f = x^2 + 1 \in \mathbb{R}[x]$. To find the zeros of f,

$$x^2 + 1 = 0$$

$$x^2 = -1$$

$$x = \pm\sqrt{-1}.$$

Clearly neither zero is a real number, and thus f has no zeros in $\mathbb{R}$. If instead we take $f \in \mathbb{C}[x]$, then f has two zeros $x = \pm\sqrt{-1} = \pm i$.

Furthermore, we can equate two polynomials if we consider their corresponding functions.

Corollary 2.14. *Let k be an infinite field, then $f = g$ for $f, g \in k[x_1, \ldots, x_n]$ if and only if $f : k^n \to k$ and $g : k^n \to k$ are the same function.*

Proof. The forward direction follows directly from the definition of the function of a polynomial. For the backward direction, we assume f, $g \in k[x_1, \ldots, x_n]$ are the same function. Then, for all $(a_1, \ldots, a_n) \in k^n$, this implies

$$f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n).$$

It follows that the function $f - g = 0$ for all $(a_1, \ldots, a_n) \in k^n$, therefore $f - g$ must be the zero function. Hence $f - g$ is the zero polynomial by proposition 2.10, and thus $f = g$. □

2.2 Domains

Domains, which are special types of rings, are a important topic in the study of ring theory. We define a few here and and discuss their relationship to polynomial rings. One may also recall that these domains are nested proper subsets of each other as follows:

$$\text{Fields} \subset \text{Euclidean Domains} \subset \text{PID's} \subset \text{UFD's} \subset \text{Integral Domains}.$$

An **integral domain** is a ring R such that R contains no zero divisors. A zero divisor is a nonzero element $a \in R$ such that $a \cdot b = 0$ for some $b \in R$. For example, the ring $\mathbb{Z}/5\mathbb{Z}$ is an integral domain, but $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain as it contains zero divisors. For example, in $\mathbb{Z}/6\mathbb{Z}$

$$4 \cdot 3 \equiv 0 \mod 6$$

so 4 is a zero divisor. Since $k[x_1, \ldots, x_n]$ has no zero divisors, it is a integral domain. To discuss unique factorization domains, we first recall the following definitions.

Definition 2.15. In a commutative ring R, and for $p, x, y \in R$ we call p **prime** if when $p|xy$, then $p|x$ or $p|y$.

Definition 2.16. In a commutative ring R, and for $a, b, c \in R$, we call a **irreducible** if when $a = bc$, b is a unit or c is a unit.

In general, a prime element is also irreducible, though the converse is not always true. In a unique factorization domain, we find that irreducible elements are also prime elements. A **unique factorization domain** (UFD) is a integral domain in which every element can be written uniquely as a product of prime powers.

To see that irreducible elements are also prime elements, let $a \in R$ be a irreducible element. Then, we can write $a|bc$ for some $b, c \in R$. If we can show $a|b$ or $a|c$, then a is also prime. Since $a|bc$, by the division algorithm, we can write $ad = bc$ for some $d \in R$. Since $b, c, d \in R$, we can write them as a product prime powers. Denote these unique factorizations by

$$b = b_1^{\alpha_1} \cdot \cdots \cdot b_r^{\alpha_r},$$

$$c = c_1^{\beta_1} \cdot \cdots \cdot c_s^{\beta_s},$$

$$d = d_1^{\gamma_1} \cdot \cdots \cdot d_t^{\gamma_t},$$

where $b_i^{\alpha_i}, c_j^{\beta_j}, d_k^{\gamma_k} \in R$ are prime powers. Since $ad = bc$, this implies

$$a(d_1^{\gamma_1} \cdot \cdots \cdot d_t^{\gamma_t}) = (b_1^{\alpha_1} \cdot \cdots \cdot b_r^{\alpha_r})(c_1^{\beta_1} \cdot \cdots \cdot c_s^{\beta_s}).$$

It follows that since these factorizations are unique, then a must be some b_i or c_j, or equivalently, $a|b$ or $a|c$.

Clearly $k[x_1, \ldots, x_n]$ is a UFD, where an irreducible element is defined as follows.

Definition 2.17. A non-constant polynomial $f \in k[x_1, \ldots, x_n]$ is said to be **irreducible** if when

$$f = h \cdot g$$

for $h, g \in k[x_1, \ldots, x_n]$, then either h or g is a constant.

A **principal ideal domain** (PID) is defined as an integral domain in which every ideal can be generated by a single element. In general $k[x_1, \ldots, x_n]$ is not a PID, but if $n = 1$, as we will see in Theorem 2.23, every ideal $I \subseteq k[x]$ can be generated by a single polynomial, and therefore $k[x]$ is PID. We will investigate PID's further after defining ideals and generators. Lastly, we have **Euclidean domains**. A integral domain R is a Euclidean domain if we have some sort of measure $\nu : R \to \mathbb{Z}_{\geq 0}$ and for $a, b \in R$ and $b \neq 0$, then there exists unique $q, r \in R$ such that

$$a = b \cdot q + r$$

where $r = 0$ or $\nu(r) < \nu(b)$.

We find $k[x]$ is also a Euclidean domain with the usual polynomial division, the result of which we define in the following section. In this case the measure in question is degree.

2.3 Division in $k[x]$

One may recall the usual single indeterminant polynomial division. In $k[x]$ we can define a polynomial simply as follows.

Definition 2.18. A polynomial $f \in k[x]$ is of the form

$$f = c_0x^m + c_1x^{m-1} + \cdots + c_{m-1}x + c_m$$

where $c_i \in k$ and $c_0 \neq 0$. We call c_0x^m the **leading term** of f, and denote this by $\mathrm{LT}(f) = c_0x^m$. We say f is of degree m and denote this by $\deg(f) = m$.

Theorem 2.19. *Let k be a field, and $f, g \in k[x]$ such that $g \neq 0$. Then there exists unique $q, r \in k[x]$ such that $f = gq + r$ where* $\deg(r) < \deg(g)$.

The proof of this theorem is omitted, not as to dismiss the importance and power of it as its result is used frequently, but to focus on the division algorithm in multiple indeterminants. Proofs for this theorem can be found in many algebra texts. Though instead we will consider the algorithm in pseudo-code, as it relates closely to that of the algorithm in $k[x_1, \ldots, x_n]$. When performing division in $k[x]$ we work with a single divisor and produce a single quotient. An important result of the division algorithm in $k[x]$ is the quotient and remainder are *unique*. This may not be the case when we extend this processes to $k[x_1, \ldots, x_n]$.

Consider the pseudo-code below, presented as it is in [4], of the division of a polynomial f by g to produce unique remainder r and quotient q.

Algorithm 1: Division in $k[x]$

Input : f, g
Output: q, r

```
1 q := 0
2 r := f
3 while r ≠ 0 AND LT(g)|LT(r) do
4 |   q := q+LT(r)/LT(g)
5 |   r := r − (LT(r)/LT(g))g
6 end
7 RETURN q, r;
```

An important piece of this algorithm is the redefinition of q and r for each iteration. This gives us a useful identity:

$$f = q \cdot g + r = \left(q + \left(\frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}\right)\right) \cdot g + \left(r - \left(\frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}\right) \cdot g\right).$$

Consider the following example, which demonstrates how this identity is useful in writing the iterations of division concisely.

Example 2.20. Let $f = 2x^3 + 8x^2 - 3$ and $g = x + 3$, then by the division algorithm

$$\begin{aligned} 2x^3 + 8x^2 - 3 &= (0)(x+3) + (2x^3 + 8x^2 - 3) \\ &= (2x^2)(x+3) + (2x^2 - 3) \\ &= (2x^2 + 2x)(x+3) + (-6x - 3) \\ &= (2x^2 + 2x - 6)(x+3) + (15). \end{aligned}$$

A typical proof of the termination of the division algorithm follows closely to the above example, as note the degree of the remainder is strictly decreasing at

each iteration. Instead of verifying it's termination formally, we will explore the termination of the division algorithm in $k[x_1, \ldots, x_n]$ in depth in section 4.

2.4 Generators and Ideals

We recall the definition of an ideal, as ideals are central in the discussion of Gröbner bases.

Definition 2.21. Let R be a commutative ring. Then $I \subseteq R$ is an **ideal** if the following conditions hold:

i. $0 \in I$.

ii. $a + b \in I$ for all $a, b \in I$.

iii. $r \cdot a \in I$ for all $a \in I$, $r \in R$.

Polynomial rings also contain ideals, and like any ring $k[x_1, \ldots, x_n]$ has the trivial ideals: the zero ideal $\{0\}$ and the ring $k[x_1, \ldots, x_n]$ itself. The most common ideals we will encounter are those generated by a collection of polynomials. When we say "generate" this is analogous to "spanning" in the linear algebra sense. In order for a collection of polynomials to generate an ideal I they must span the entirety of I. Often we will begin with a set of polynomials $f_1, \ldots, f_s$ and we will generate an ideal I with those polynomials.

To follow with this linear algebra concept, recall the unit vectors $\vec{e}_1 = (1, 0)$, $\vec{e}_2 = (0, 1) \in \mathbb{R}^2$, which are linearly independent and span all of $\mathbb{R}^2$. We say $\vec{e}_1$ and

$\vec{e}_2$ *generate* all of $\mathbb{R}^2$ and we often call $\{\vec{e}_1, \vec{e}_2\}$ a *basis* for $\mathbb{R}^2$. Since these vectors form a basis for $\mathbb{R}^2$, then we can represent any vector $(x, y) \in \mathbb{R}^2$ by a unique linear combination

$$(x, y) = c_1\vec{e}_1 + c_2\vec{e}_2$$

with coefficients $c_1, c_2 \in \mathbb{R}$.

Example 2.22. Similarly, consider the ring $\mathbb{C}[x]$. If f is some polynomial in $\mathbb{C}[x]$, we denote the set of polynomials generated by f as $\langle f \rangle$. This set has the form

$$\langle f \rangle = \{h \cdot f : h \in \mathbb{C}[x]\}.$$

Take, for example, $f = 1$; the set of polynomials generated by f is

$$\langle f \rangle = \langle 1 \rangle = \{h \cdot 1 : h \in \mathbb{C}[x]\}$$

which is clearly the entire ring $\mathbb{C}[x]$. As another example, take instead $f = x - 1$; then the set of polynomials generated by f is

$$\langle f \rangle = \langle x - 1 \rangle = \{h \cdot (x - 1) : h \in \mathbb{C}[x]\}.$$

This set can be also thought of as the collection of polynomials which attain a zero at 1.

Theorem 2.23. *If k is a field, then every ideal $I \subseteq k[x]$ can be written as $\langle f \rangle$ for some $f \in k[x]$. Furthermore, f is unique up to multiplication by a nonzero constant in k.*

Proof. Assume $I \subseteq k[x]$ is a nonzero ideal, otherwise we are done. We will show $I = \langle f \rangle$ by choosing nonzero $f \in I$ such that f is of minimum degree of the elements of I. By the division algorithm, for $f \in I$ we can write any element $g \in I$ as

$$g = q \cdot f + r$$

for unique $q, r \in I$, and $\deg r < \deg f$. Then, we write

$$r = g - q \cdot f.$$

If $r \neq 0$ we arrive at a contradiction, as clearly $r \in I$ and $\deg r < \deg f$, but we chose f to be of minimal degree. Therefore r must be zero, i.e., any element $g \in I$ can be generated by f. Uniqueness can be shown similarly by assuming I can be generated by $\langle f \rangle$ and $\langle g \rangle$. One can then write $f = q \cdot g$ since $f \in \langle g \rangle$ and likewise $g = \tilde{q} \cdot f$. Performing appropriate substitution, we obtain

$$f = q \cdot \tilde{q} \cdot f$$

which implies $\deg(q) = \deg(\tilde{q}) = 0$, and thus f and g differ only by some constant. □

If we are given some ideal $I \subseteq k[x]$ which is generated by more than one polynomial, say $I = \langle f_1, \ldots, f_s \rangle$, how can we find a unique f such that $\langle f \rangle = \langle f_1, \ldots, f_s \rangle$? This problem is easily answered by use of the greatest common divisor (gcd).

Definition 2.24. A polynomial $h \in k[x]$ is said the be the **greatest common divisor** of the polynomials $f, g \in k[x]$ when:

i. $h|f$ and $h|g$.

ii. If p is another polynomial such that $p|f$ and $p|g$, then $p|h$.

When h satisfies the above conditions, we denote $h = \gcd(f, g)$.

The gcd of two polynomials has the following properties.

Proposition 2.25. *Let $f, g \in k[x]$. Then:*

i. $\gcd(f, g)$ *exists and is unique up to multiplication by a nonzero constant in* k.

ii. $\langle \gcd(f, g) \rangle = \langle f, g \rangle$.

iii. There is an algorithm for finding $\gcd(f, g)$.

Proof. The proof of existence and uniqueness is common and trivial, and the existence will be examined using the Euclidean algorithm. We instead focus on the equivalence of ideals and the algorithm for finding $\gcd(f, g)$. To see $\langle \gcd(f, g) \rangle = \langle f, g \rangle$, suppose $\gcd(f, g)$ exists and denote it by $h = \gcd(f, g)$. It follows from the definition of $\gcd(f, g)$ that $h|f$ and $h|g$. Therefore, for some $\tilde{f}, \tilde{g} \in k[x]$, we can write

$$\begin{cases} f &= h \cdot \tilde{f} \\ g &= h \cdot \tilde{g} \end{cases} \implies \begin{cases} f &\in \langle h \rangle \\ g &\in \langle h \rangle \end{cases}$$

Therefore $\langle f, g \rangle = \langle h \rangle = \langle \gcd(f, g) \rangle$.

The algorithm mentioned in (iii) is the usual Euclidean algorithm for finding the $\gcd(f, g)$, and is stated below [4].

Algorithm 2: Euclidean Algorithm

Input : $f, g \in k[x]$
Output: $h = \gcd(f, g)$

```
h := f
s := g
while s ≠ 0 do
    r := remainder(h, s)
    h := s
    s := r
end
RETURN h;
```

To see that this algorithm does produce the $\gcd(f, g)$, for $f = qg + r \in k[x]$, we claim that $\gcd(f, g) = \gcd(f - qg, g) = \gcd(r, g)$. It suffices to show that $\langle f, g\rangle = \langle f - qg, g\rangle$.

Consider an element $\tilde{f} \in \langle f - qg, g\rangle$. We can write

$$\begin{aligned}\tilde{f} &= (f - qg) \cdot h_1 + g \cdot h_2 \\ &= fh_1 - qgh_1 + gh_2 \\ &= fh_1 - g(qh_1 + h_2),\end{aligned}$$

and denoting $\tilde{h}_2 = qh_1 + h_2 \in k[x]$, then $\tilde{f}$ is of the form $\tilde{f} = fh_1 - g\tilde{h}_2 \in \langle f, g\rangle$. Therefore $\langle f, g\rangle = \langle f - qg, g\rangle = \langle r, g\rangle$. This shows that the first iteration of the Euclidean algorithm holds. To see that it holds at every iteration and that it will eventually terminate, consider that after the first iteration $\deg(g) > \deg(r)$ or $r = 0$. Assuming $r \neq 0$, this algorithm continues through another iteration. By the division algorithm we have $g = q'r + r'$ and therefore $\gcd(g, r) = gcd(r, r')$, where again

$\deg(r) > \deg(r')$, or $r = 0$ and the algorithm terminates. Assuming it does not terminate, then at each step we continue to have the strict set of inequalities

$$\deg(g) > \deg(r) > \deg(r') > \deg(r'') > \dots$$

which clearly must terminate since $\deg(g)$ is finite. Therefore at some iteration we will achieve $r = 0$ which gives $s = 0$, and thus $h = \gcd(h, 0) = \gcd(f, g)$. □

Consider the following example, which makes use of both the division and Euclidean algorithms.

Example 2.26. Let $I = \langle f_1, f_2 \rangle \subseteq \mathbb{R}[x]$, where $f_1 = x^3 - 2x^2 + x - 2$ and $f_2 = x^5 - 2x^4 - 10$. Since $\mathbb{R}[x]$ is a PID, we must be able to generate this ideal with a single polynomial. Furthermore, this implies $\mathbb{R}[x]$ is UFD, and therefore by the division and Euclidean algorithms we can write

$$f_1 = x^3 - 2x^2 + x - 2 = (x - 2)(x^2 + 1)$$

and

$$f_2 = x^5 - 2x^4 - 10 = (x - 2)(x^4 + 5).$$

We see that the $\gcd(f_1, f_2) = x - 2$, implying the ideal can instead be generated by the single polynomial $x - 2$.

Fortunately, we can extend these properties and definitions of $\gcd(f, g)$ to ideals which are generated by more than two polynomials. First we define the greatest

common divisor for more than two polynomials.

Definition 2.27. A polynomial $h \in k[x]$ is said the be the **greatest common divisor** of the polynomials $S = \{f_1, \dots f_s\} \subseteq k[x]$ when:

i. $h|f$ for all $f \in S$.

ii. If p is another polynomial such that $p|f$ for all $f \in S$, then $p|h$.

When h satisfies these conditions, we denote $h = \gcd(f_1, \dots, f_s)$.

Proposition 2.28. *Let $f_1, \dots f_s \in k[x]$,where $s \geq 2$. Then:*

i. $\gcd(f_1, ..., f_s)$ *exists and is unique up to multiplication by a nonzero constant.*

ii. $\gcd(f_1, ..., f_s)$ *is a generator of the ideal $\langle f_1, \dots, f_s \rangle$.*

iii. If $s \geq 3$, then $\gcd(f, \dots, f_s) = \gcd(f_1, \gcd(f_2, \dots, f_s))$.

iv. There is an algorithm for finding $\gcd(f_1, \dots, f_s)$.

The proof of this proposition is omitted as it follows similarly to that of proposition 2.25. The algorithm mentioned in (iv) is the same Euclidean algorithm as before, where the gcd is found in pairs, as mentioned in (iii). Note the $\gcd(f_1, \dots, f_s)$ may be 1 (or some other nonzero constant), in which this would imply the ideal is the entire ring $k[x]$.

More often a generating set is made up of polynomials of multiple indeterminants. Before we formally define a generating set, we consider two examples of ideals in $k[x, y]$.

Example 2.29. Let $f_1 = x - 3y$ and $f_2 = 2y^2$ be polynomials in $\mathbb{C}[x, y]$. Then all $f \in I = \langle f_1, f_2 \rangle$ are of the form

$$\begin{aligned} f &= h_1 \cdot f_1 + h_2 \cdot f_2 \\ &= h_1 \cdot (x - 3y) + h_2 \cdot (2y^2), \end{aligned}$$

where $h_1, h_2 \in \mathbb{C}[x, y]$. Furthermore, the polynomial $3xy^2 - 3y^3 - 2y^2 \in I$, since

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

Example 2.30. Let $I = \langle x + y^2, x^3 \rangle$ and $J = \langle x + y^2, x^2y^2 \rangle$ be two ideals in $k[x, y]$. Notice we can write the second generating polynomial of J in terms of the polynomials from I; that is,

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

This means $J \subseteq I$. Furthermore, we can represent x^3 as a linear combination of the polynomials in J.

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

This shows $I \subseteq J$. Because both ideals are subsets of one another, this implies $I = J$.

In general, we can have a generating set of any number of polynomial in the ring $k[x_1, \ldots, x_n]$. We now formally define such a generating set.

Definition 2.31. If $S \subseteq k[x_1, \ldots, x_n]$, then we define

$$\langle S\rangle = \left\{ \sum_{\alpha} h_\alpha f_\alpha : f_\alpha \in S \text{ and } h_\alpha \in k[x_1, \ldots, x_n] \right\},$$

for $1 \leq \alpha \leq s$ for some finite s. We call $\langle S\rangle$ the ideal generated by S where $S = \{f_1, \ldots, f_s\}$. Occasionally, for $f \in \langle S\rangle = \langle f_1, \ldots, f_s\rangle$, we may write f explicitly as

$$f = h_1 \cdot f_1 + \cdots + h_s \cdot f_s.$$

We occasionally use T to represent some other collection of polynomials.

Lemma 2.32. *If $S \subseteq k[x_1, \ldots, x_n]$, then $\langle S\rangle$ is an ideal of $k[x_1, \ldots, x_n]$.*

Clearly by the definition of $\langle S\rangle$, the axioms of an ideal are satisfied. Our main concern lies with ideals which can be *finitely* generated.

Definition 2.33. An ideal $I \subseteq k[x_1, \ldots, x_n]$ is said to be **finitely generated** if there exists $S \subseteq k[x_1, \ldots, x_n]$ such that $I = \langle S\rangle$, then we call S a **basis** of I.

An amazing fact we will see (by theorem 5.7) is *every* ideal in $k[x_1, \ldots, x_n]$ can be finitely generated. Before proving this, we must first discuss how to order monomials in $k[x_1, \ldots, x_n]$.

2.5 Monomial Ordering

When working in a polynomial ring in one indeterminate, ordering is simple and is based on the degree of the term. In $k[x]$, we saw that the leading term was

an important definition in the division algorithm; this will prove to be true in the algorithm for $k[x_1, \ldots, x_n]$ as well. As such, we need to be able to define what a leading term is when we have multiple indeterminants.

A problem arises when we attempt to order monomials for polynomials in $k[x_1, \ldots, x_n]$. How, for example, do we order terms in descending order for the polynomial

$$2x^3y^2z^2 - 13x^5y^2 - 2x^3z^2 + 5y^4 + 3z^5?$$

Instinct may lead us to choose to order based on the total degree, but this decision quickly causes a problem: the first two terms in the example above both have a total degree of 7. As such, total degree alone is not sufficient for ordering monomials in $k[x_1, \ldots, x_n]$. We must then decide how to compare individual indeterminants. This is what we call a monomial ordering. We will use $\succ$ to denote some ordering, for example, $x \succ y$.

When comparing individual monomials, it is common to use the notation

$$\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}.$$

Recall this ordered n-tuple represents the monomial

$$x^\alpha = x_1^{\alpha_1} \cdot \cdots \cdot x_n^{\alpha_n} \in k[x_1, \ldots, x_n].$$

To be able to compare monomials, we need a total ordering. That is, given any two monomials x^α, x^β, exactly one of the following three statements must be true:

$$x^\alpha \succ x^\beta \qquad x^\alpha = x^\beta \qquad x^\beta \succ x^\alpha.$$

Any valid ordering should also have transitivity, i.e., if $x^\alpha \succ x^\beta$ and $x^\beta \succ x^\lambda$, then $x^\alpha \succ x^\lambda$. Furthermore, it is required that for $x^\alpha \succ x^\beta$, and for any monomial x^λ, we have $x^\alpha x^\lambda \succ x^\beta x^\lambda$.

Definition 2.34. A **monomial ordering** $\succ$ on $k[x_1, \ldots, x_n]$ is a relation $\succ$ on $\mathbb{Z}^n_{\geq 0}$, or equivalently, a relation on the set of monomials x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$, satisfying:

i. $\succ$ is a total ordering on $\mathbb{Z}^n_{\geq 0}$.

ii. If $\alpha \succ \beta$, and for $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma \succ \beta + \gamma$.

iii. $\succ$ is a well-ordering on $\mathbb{Z}^n_{\geq 0}$. That is, if $A \subseteq \mathbb{Z}^n_{\geq 0}$ is nonempty, then there is $\alpha \in A$ such that $\beta \succ \alpha$ for every $\beta \neq \alpha$ in A.

The last condition simply states a smallest element must exists under any ordering. This well-ordering property becomes important when discussing the termination of the division algorithm in $k[x_1, \ldots, x_n]$. The following definitions with be useful in the discussion of ordering.

Definition 2.35. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, \ldots, x_n]$ and fix a monomial order $\succ$.

i. The **multidegree** of f is

$$\deg(f) = \max(\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0);$$

(Henceforth, when discussing degree it will be assumed we are discussing the multidegree.)

ii. The **leading coefficient** of f is

$$\mathrm{LC}(f) = a_{\deg(f)} \in k;$$

iii. The **leading monomial** of f is

$$\mathrm{LM}(f) = x^{\deg(f)} \in k;$$

iv. The **leading term** of f is

$$\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f);$$

An equivalent definition for the degree of a polynomial is

$$\deg(f) = \deg(\mathrm{LT}(f)).$$

We will consider three different orderings. Often, when discussing polynomials of three or less variables we often use $k[x, y, z]$, and subscripts $k[x_1, \ldots, x_n]$ when working with polynomials of $n > 3$ indeterminants. One of the most common and instinctive orderings is called **Lexicographic** (Lex) ordering which, as its name suggests, is

much like alphabetical ordering. In $k[x_1, \ldots, x_n]$, Lex ordering assumes

$$x_1 \succ x_2 \succ \cdots \succ x_n, \text{ and } x_i \prec x_i^2 \prec \ldots.$$

For $k[x, y, z]$ it is generally assumed $x \succ y \succ z$. While we can choose any ordering for individual indeterminants, such as $x_n \succ \cdots \succ x_1$, we will assume $x_1 \succ x_2 \succ \cdots \succ x_n$ unless another ordering is explicitly stated.

Example 2.36. For an example, let's consider again the polynomial

$$f = 2x^3y^2z^2 - 13x^5y^2 - 2x^3z^2 + 5y^4 + 3z^5$$

and order it using Lex ordering:

$$-13x^5y^2 + 2x^3y^2z^2 - 2x^3z^2 + 5y^4 + 3z^5.$$

Equivalently, we could compare the individual monomials x^5y^2 and $x^3y^2z^2$ using the notation

$$(5, 2, 0) \succ (3, 2, 2).$$

Another common type of ordering is **Graded Lexicographic** (Grlex) which is similar to Lex ordering but orders monomials by total degree first. Any monomials of a shared total degree are then sorted using Lex ordering. For example, consider the monomials x^3y^3 and x^5. Using Grlex ordering $x^3y^3 \succ x^5$, where the contrary was true with Lex ordering. Let's order the the polynomial f from Example 2.36 in decreasing order using Grlex ordering:

$$f = -13x^5y^2 + 2x^3y^2z^2 - 2x^3z^2 + 3z^5 + 5y^4.$$

The most efficient in terms of computation time, but likely the most difficult conceptually, is **Graded Reverse Lexicographic** (Revgrlex) ordering. Revgrlex orders first by total degree but sorts monomials of shared degree in "reverse" as compared to Grlex. For example, consider we have to order the two monomials x^4y^3z and $x^3y^2z^3$, which both have the same total degree of 8. With Revgrlex ordering we break ties by the smallest degree of z (the "smallest" indeterminate), so $x^4y^3z \succ x^3y^2z^3$, or $(4,3,1) \succ (3,2,3)$. Let's order the polynomial f from Example 2.36 again, instead using Revgrlex ordering:

$$-13x^5y^2 + 2x^3y^2z^2 - 2x^3z^2 + 3z^5 + 5y^4.$$

To compare how we order in Grlex versus Revgrlex, denote

$$\alpha = (\alpha_1, \alpha_2, \alpha_3),\ \beta = (\beta_1, \beta_2, \beta_3),$$

where $|\alpha| = |\beta|$, and $x^\alpha, x^\beta \in k[x_1, x_2, x_3]$. Assume $x_1 \succ x_2 \succ x_3$. If we are using Grlex ordering then we compare α_i and β_i starting from the *left* and are concerned with which one is *largest*, i.e.,

$$(\alpha_1, \alpha_2, \alpha_3) \quad \succ \quad (\beta_1, \beta_2, \beta_3)$$
$$\text{if } \alpha_1 > \beta_1.$$

If we find $\alpha_1 = \beta_1$, we move to the right and compare α_2 and β_2. In general we would compare by continuing to the right until we find $\alpha_i \neq \beta_i$.

If we are using Revgrlex, then we compare α_i and β_i starting from the right and are concerned with which is *smallest*, i.e.,

$$(\alpha_1, \alpha_2, \alpha_3) \quad \succ \quad (\beta_1, \beta_2, \beta_3)$$

$$\text{if } \alpha_3 < \beta_3.$$

In the same sense, we would continue comparing α_i and β_i by moving to the left if we have equality.

3 Ideals and Varieties

In this section we consider the corresponding system of equations for the basis elements of an ideal, and the solutions to this system, or the variety. We also consider the ideal of this variety, and consider ideals generated by monomials.

3.1 Varieties

Definition 3.1. Given $S \subseteq k[x_1, \ldots, x_n]$, the **variety** $\mathbf{V}(S)$ is defined as

$$\mathbf{V}(S) = \{(a_1, \ldots a_n) \in k^n : f(a_1, \ldots a_n) = 0 \text{ for all } f \in S\}.$$

Simply, a variety is the collection of $(a_1, \ldots a_n) \in k^n$ on which all polynomials in S vanish.

Example 3.2. Consider the polynomial $f = x^2 + x - 6 \in \mathbb{C}[x]$, which has the variety

$$\mathbf{V}(x^2 + x - 6) = \{a \in \mathbb{C}^1 : f(a) = 0\} = \{-3, 2\}.$$

Example 3.3. Consider the polynomials $f_1 = -2x + y - 3$ and $f_2 = x - y - 1$ in $\mathbb{C}[x, y]$. The variety $\mathbf{V}(f_1, f_2)$ is the collection of ordered pairs $(x, y) \in \mathbb{C}^2$ which

satisfy both

$$\begin{cases} -2x + y - 3 &= 0 \\ x - y - 1 &= 0 \end{cases} \implies \begin{cases} -2x + y &= 3 \\ x - y &= 1. \end{cases}$$

Using Gaussian elimination, or other algebra techniques, one can find that the only ordered pair which satisfies both equations is $(-4, -5)$. Thus,

$$\mathbf{V}(f_1, f_2) = \{(-4, -5)\}.$$

For $S \subseteq k[x_1, \ldots, x_n]$ we have the variety $V = \mathbf{V}(S)$. If $f \in S$, then clearly f vanishes of V, but consider further the polynomials in $\langle S \rangle$. If $I = \langle S \rangle$ is an ideal, not only can we consider the variety $\mathbf{V}(S)$, but we can also consider the variety of the ideal $\mathbf{V}(\langle S \rangle)$. The following lemma tells us these are equivalent.

Lemma 3.4. *If $I = \langle S \rangle \subseteq k[x_1, \ldots, x_n]$, then $\mathbf{V}(S) = \mathbf{V}(\langle S \rangle)$.*

Proof. By definition, $\mathbf{V}(S) \subset \mathbf{V}(\langle S \rangle)$, but to show $\mathbf{V}(\langle S \rangle) \subset \mathbf{V}(S)$, let $f \in \langle S \rangle = I$. Then, if $S = \{f_1, \ldots, f_s\}$, we can write

$$f = h_1 \cdot f_1 + \cdots + h_s \cdot f_s$$

for $h_i \in k[x_1, \ldots, x_n]$. Then each f_i vanishes for all $(a_1, \ldots, a_n) \in \mathbf{V}(S)$, i.e,

$$f_i(a_1, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq s.$$

Then

$$\begin{aligned} f(a_1, \ldots, a_n) &= h_1(a_1, \ldots, a_n) \cdot f_1(a_1, \ldots, a_n) + \cdots + h_s(a_1, \ldots, a_n) \cdot f_s(a_1, \ldots, a_n) \\ &= h_1(a_1, \ldots, a_n) \cdot 0 + \cdots + h_s(a_1, \ldots, a_n) \cdot 0 \\ &= 0. \end{aligned}$$

Therefore $\mathbf{V}(S) = \mathbf{V}(\langle S \rangle)$. □

The above lemma is useful in proving the following result.

Proposition 3.5. *If S and T are bases of the same ideal in $k[x_1, \ldots, x_n]$, so that $\langle S \rangle = \langle T \rangle$, then $\mathbf{V}(S) = \mathbf{V}(T)$.*

Proof. Let S and $T \in k[x_1, \ldots, x_n]$ be bases of the same ideal I such that $\langle S \rangle = \langle T \rangle = I$. Then consider the variety $\mathbf{V}(S)$. By lemma 3.1, $\mathbf{V}(S) = \mathbf{V}(\langle S \rangle)$. Therefore

$$\mathbf{V}(S) = \mathbf{V}(\langle S \rangle) = \mathbf{V}(\langle T \rangle) = \mathbf{V}(T).$$

□

3.2 Ideals

We can also consider the ideal of a variety, which consists of all such polynomials which vanish on the given variety.

Definition 3.6. Let $V \subseteq k^n$ be an affine variety. Then, we denote

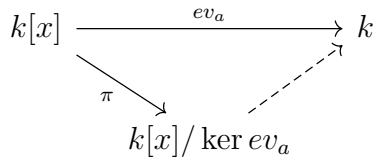
$$\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in V\}.$$

An important observation of the above definition is the following lemma, which tells us $\mathbf{I}(V)$ is in fact an ideal.

Lemma 3.7. *If $V \subseteq k^n$ is an affine variety, then $\mathbf{I}(V) \subseteq k[x_1, \ldots, x_n]$ is an ideal. We call $\mathbf{I}(V)$ the* ***ideal of V****.*

The proof is omitted as $\mathbf{I}(V)$ clearly satisfies the requirements of an ideal. We wish to investigate the relationship between $\mathbf{I}(\mathbf{V}(S))$ and the ideal $\langle S \rangle$ itself. The next lemma states there is a clear relationship if our ideal $\langle S \rangle$ is of the form $\langle x - a \rangle \in k[x]$.

Lemma 3.8. *Let $a \in k$ and let $ev_a : k[x] \to k$ be the evaluation homomorphism. Then $\ker(ev_a)$ is an ideal of $k[x]$ where $\ker(ev_a) = \langle x - a \rangle$. Furthermore, by the First Isomorphism Theorem, the following diagram commutes*



such that π is the natural homomorphism $\pi(f(x)) = f(x) + \ker(ev_a)$.

Proof. We claim that $\ker(\mathrm{ev}_a) = \langle x - a \rangle$. To see this, note that every $f \in \langle x - a \rangle$ is of the form

$$f = (x - a) \cdot h$$

for $h \in k[x]$. Clearly $f(a) = (a - a) \cdot h(a) = 0$ and therefore $\ker(\mathrm{ev}_a) \subset \langle x - a \rangle$. To see that $\ker(\mathrm{ev}_a) \subset \langle x - a \rangle$, let $f(x) \in \ker(\mathrm{ev}_a)$ where $f(a) = 0$. By the division algorithm,

$$f(x) = (x-a)q(x) + r(x)$$

where $\deg r(x) < \deg(x-a)$ and thus $r(x)$ must be a constant $r \in k$. Evaluating $f(a)$ we find

$$\begin{aligned} f(a) &= (a-a)q(a) + r \\ &= 0 \cdot q(a) + r \\ &= r \end{aligned}$$

but $f(a) = 0$ therefore $r = 0$. This implies we can write $f(x) \in \ker(\mathrm{ev}_a)$ as

$$f(x) = q(x)(x-a)$$

which is the form of all elements in $\langle x-a \rangle$. □

That is, for $f = x - a \in k[x]$ the $\ker(\mathrm{ev}_a)$ is precisely the ideal $\mathbf{I}(\mathbf{V}(x-a))$. Since we have shown $\ker(\mathrm{ev}_a) = \langle x-a \rangle$, then

$$\mathbf{I}(\mathbf{V}(x-a)) = \langle x-a \rangle.$$

The following example illustrates this.

Example 3.9. Consider the ideal $J \subset \mathbb{C}[x]$ defined by

$$J = \langle x-2 \rangle = \{(x-2) \cdot q(x) : q(x) \in \mathbb{C}[x]\}.$$

From J, we can consider the variety

$$V = \mathbf{V}(x-2) = \{2\}.$$

Furthermore, we can consider the ideal of the variety

$$\mathbf{I}(V) = \{f(x) \in \mathbb{C}[x] : f(2) = 0\}.$$

Clearly $J \subseteq \mathbf{I}(V)$, and to show $\mathbf{I}(V) \subseteq J$, let $f(x) \in \mathbb{C}[x]$ be any polynomial in $\mathbf{I}(V)$ such that $f(2) = 0$. Then, by the division algorithm we can write

$$f(x) = (x-2) \cdot q(x) + r(x)$$

such that $\deg(r(x)) < 1$. Then $r(x)$ must be a constant $r \in \mathbb{C}$ and

$$\begin{aligned} f(2) &= (2-2) \cdot q(2) + r \\ &= (0) \cdot q(2) + r \\ &= r, \end{aligned}$$

but $f(2) = 0$, so therefore $r = 0$. Therefore $J = \langle x-2 \rangle = \mathbf{I}(\mathbf{V}(x-2))$.

The next example further explores this relationship between an ideal $\langle S \rangle$ and an ideal of the variety $\mathbf{I}(\mathbf{V}(S))$, and will show that equality is not always the case.

Example 3.10. Consider $f = x^2 \in k[x]$. The variety $\mathbf{V}(x^2) = 0$ gives the ideal $\mathbf{I}(\mathbf{V}(x^2)) = \mathbf{I}(\{0\})$. Notice also that $\mathbf{I}(\{0\}) = \langle x \rangle$. Therefore, since $\langle x^2 \rangle \subsetneq \langle x \rangle$, we have

$$\langle x^2 \rangle \subsetneq \mathbf{I}(\mathbf{V}(x^2)).$$

The following lemma establishes this relationship in general in $k[x_1, \ldots, x_n]$.

Lemma 3.11. *Let $S \subseteq k[x_1, \ldots, x_n]$. Then, $\langle S \rangle \subseteq \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$.*

The proof is trivial and is illustrated by the preceding example. Given two varieties V and W we can discuss the relationship between their corresponding ideals.

Proposition 3.12. *Let V and W be two affine varieties in k^n.*

i. $V \subseteq W$ if and only if $\boldsymbol{I}(W) \subseteq \boldsymbol{I}(V)$

ii. $V = W$ if and only if $\boldsymbol{I}(V) = \boldsymbol{I}(W)$.

Let us examine the following example in place of a proof.

Example 3.13. Consider the following varieties in k:

$$V_1 = \mathbf{V}(x - 1) \text{ and } V_2 = \mathbf{V}((x - 1)(x + 2)).$$

These varieties have the following ideals, respectively:

$$\mathbf{I}(V_1) = \{f(x) \in k[x] : f(1) = 0\}$$

$$\mathbf{I}(V_2) = \{f(x) \in k[x] : f(1) = 0 \text{ and } f(2) = 0\}.$$

Then we have $V_1 \subseteq V_2$ and $\mathbf{I}(V_2) \subseteq \mathbf{I}(V_1)$.

3.3 Monomial Ideals

Here we consider ideals generated by monomials as they are the building blocks of polynomials.

Definition 3.14. An ideal $I \subseteq k[x_1, \ldots, x_n]$ is a **monomial ideal** if there is a (possibly infinite) subset $A \subseteq \mathbb{Z}^n_{\geq 0}$ such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in k[x_1, \ldots, x_n]$.

Since an element of $\mathbb{Z}^n_{\geq 0}$ is of the form $\alpha = (\alpha_1, \ldots, \alpha_n)$, which represents the monomial $x^\alpha = x_1^{\alpha_1} \cdot \cdots \cdot x_n^{\alpha_n}$, A is simply a collection of monomials x^{α_i} for $\alpha_i \in A$. Then the ideal I consists of linear combinations of these monomials with coefficients $h_\alpha \in k[x_1, \ldots, x_n]$. Hence we can write $I = \langle x^\alpha : \alpha \in A \rangle \subseteq k[x_1, \ldots, x_n]$. For example, $I = \langle x^2y^4, x^3y^3, x^6y^2 \rangle$ is a monomial ideal.

Lemma 3.15. *Let $I = \langle x^\alpha : \alpha \in A \rangle$ be a monomial ideal. Then, a monomial $x^\beta \in I$ if and only if x^β is divisible by x^α for some $\alpha \in A$.*

The proof is trivial and instead we consider the following example.

Example 3.16. Let $I = \langle x^5y^3, x^3y^2 \rangle$. Then clearly $x^6y^6 \in I$ since $x^5y^3 | x^6y^6$, and likewise since $x^5y^3 \nmid x^2y$ and $x^3y^2 \nmid x^2y$, then $x^2y \notin I$.

In general, for $\alpha \in A$, if $x^\beta \in \langle x^\alpha \rangle$, then we must be able to write

$$x^\beta = x^\alpha \cdot x^\gamma \text{ for some } \gamma \in \mathbb{Z}^n_{\geq 0}$$

which implies $\beta = \alpha + \gamma$. That is, we can write the elements of the ideal $I = \langle x^\alpha \rangle$ equivalently as

$$\alpha + \mathbb{Z}^n_{\geq 0} = \{\alpha + \gamma : \gamma \in \mathbb{Z}^n_{\geq 0}\}.$$

Example 3.17. Consider again the monomial ideal $I = \langle x^2y^4, x^3y^3, x^6y^2 \rangle \subseteq k[x, y]$. Elements in this ideal then take the form

$$x^\beta = h_1x^2y^4 + h_2x^3y^3 + h_3x^6y^2$$

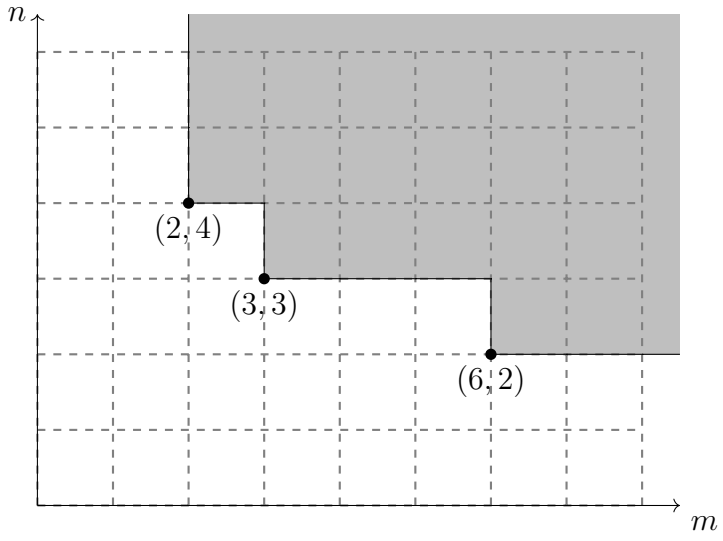
or equivalently

$$x^\beta = \sum_\alpha h_\alpha x^\alpha$$

where $\alpha_1 = (2, 4), \alpha_2 = (3, 3), \alpha_3 = (6, 2)$, and $h_{\alpha_i} \in k[x_1, \ldots, x_n]$. Furthermore, these elements could be represented in the form

$$((2, 4) + \mathbb{Z}^2_{\geq 0}) \cup ((3, 3) + \mathbb{Z}^2_{\geq 0}) \cup ((6, 2) + \mathbb{Z}^2_{\geq 0}).$$

This can also be visualized by the following graph:



where an ordered pair (m, n) denotes the monomial $x^m y^n$. The shaded region consists

of all possible monomials (which occur at the lattice points) of the elements of the ideal I.

Lemma 3.18. *Let I be a monomial ideal, and let $f \in k[x, y]$. Then, the following are equivalent:*

i. $f \in I$.

ii. Every term of f lies in I.

iii. f is a k-linear combination of the monomials in I.

The proof is trivial and the third result gives the following corollary.

Corollary 3.19. *Two monomial ideals are the same if and only if they contain the same monomials.*

Recall by the definition of a monomial ideal, the generating set of monomials may be infinite. The following theorem tells us even if we have an infinite generating set we can always reduce this set to a finite basis.

Theorem 3.20 (Dickson's Lemma)**.** *Let $I = \langle x^\alpha : \alpha \in A \rangle \subseteq k[x_1, \ldots, x_n]$ be a monomial ideal. Then, I can be written in the form $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$, where $\alpha_1, \ldots, \alpha_s \in A$. That is, I has a finite basis.*

We consider an informal sketch of the proof which follows from the proof given in [2]. The proof of this theorem is generally done by induction on the number of indeterminants n. One can see this is true for $n = 1$, and we assume the theorem is

true for $n-1$ as our hypothesis. To see that it holds for n indeterminants, we write $k[x_1, \ldots, x_n]$ as $k[x_1, \ldots, x_{n-1}, y]$ so monomials in $k[x_1, \ldots, x_{n-1}, y]$ take the form $x^\alpha y^m$, for $\alpha = (\alpha_1, \ldots, \alpha_{n-1})$ and $m = (\alpha_n)$. Then to find the generators for an ideal $I \subseteq k[x_1, \ldots, x_{n-1}, y]$, we look at the generators for $J \subseteq k[x_1, \ldots x_{n-1}]$. Specifically, we let J be generated by the elements x^α such that $x^\alpha y^m \in I$. By the induction hypothesis, we know this generating set is finite and we write $J = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$. Then, we choose m such that m is the maximum m_i for $x^{\alpha_i} y^{m_i} \in I$. From here we create a "slice" for each monomial containing y^l for $0 \leq l \leq m-1$, and use these slices to generate ideals. This process will achieve a finite set of generators. Let's consider an example to see how these "slices" work.

Example 3.21. Take the ideal $I = \langle x^2y^4, x^3y^3, x^5y^3, x^6y^2 \rangle \subseteq k[x, y]$. We first find the ideal $J \subseteq k[x]$ where $J = \langle x^\alpha \rangle$ such that $x^\alpha y^m \in I$. We find $J = \langle x^2, x^3, x^5, x^6 \rangle = \langle x^2 \rangle$, which is clearly finitely generated. Then note x^2y^4 contains the largest such $m = 4$. Then we create "slices". Consider the following ideals defined by $J_l = \langle x^\alpha : x^\alpha y^l \in I \rangle$ for $0 \leq l \leq m-1 = 3$, and the ideal J:

$$J_0 = \langle x^\alpha : x^\alpha y^0 \in I \rangle = \emptyset$$

$$J_1 = \langle x^\alpha : x^\alpha y^1 \in I \rangle = \emptyset$$

$$J_2 = \langle x^\alpha : x^\alpha y^2 \in I \rangle = \langle x^6 \rangle$$

$$J_3 = \langle x^\alpha : x^\alpha y^3 \in I \rangle = \langle x^3, x^5 \rangle = \langle x^3 \rangle$$

$$J = \langle x^\alpha : x^\alpha y^m \in I \rangle = \langle x^2 \rangle.$$

If we use the corresponding monomials $x^\alpha y^l \in I$ which come from $J_l \neq \emptyset$, these monomials will be the finite generating set for the ideal I. That is, for this example we see J_2, J_3, and J are nonzero ideals and thus correspond to the monomials for a finite generating set. Therefore $\{x^6y^2, x^3y^3, x^2y^4\}$ is a finite basis for the monomial ideal $I = \langle x^2y^4, x^3y^3, x^5y^3, x^6y^2\rangle$. Though this was clearly already finite this process helps illustrate how we can find a *minimal* basis for a monomial ideal. We see that the slice made with J_3 allowed us to remove the monomial x^5y^3 from the generating set and maintain the same ideal.

Proposition 3.22. *A monomial ideal $I \subseteq k[x_1, \ldots, x_n]$ has a basis $x^{\alpha_1}, \ldots, x^{\alpha_s}$ with the property that x^{α_i} does not divide x^{α_j} for $i \neq j$. Furthermore, this basis is unique and is called the* ***minimal basis*** *of I.*

The proof follows closely based on the example below.

Example 3.23. Continuing with the ideal $I = \langle x^2y^4, x^3y^3, x^5y^3, x^6y^2\rangle$, we see the basis x^6y^2, x^3y^3, x^2y^4 is in fact a unique minimal basis of I since none of the elements of the basis divide another element. This was to be expected and is clear based on the graphical representation of this ideal in example 3.17.

4 Division in $k[x_1, \ldots, x_n]$

"The algebra behind the division algorithm is very simple...which makes it surprising that this form of the algorithm was first isolated and exploited only within the

past 50 years" [4]. Examples of such division will quickly show why computational advancements were the turning point in the development of this division algorithm and other lengthy algorithms in the field of computational algebra.

Theorem 4.1. *Let $\succ$ be a monomial ordering on $\mathbb{Z}^n_{\geq 0}$ and let $F = (f_1, \ldots, f_s)$ be an ordered s-tuple of polynomials in $k[x_1, \ldots, x_n]$. Then, every $f \in k[x_1, \ldots, x_n]$ can be written as*

$$f = q_1 f_1 + \cdots + q_s f_s + r$$

*where $q_i, r \in k[x_1, \ldots, x_n]$, and either $r = 0$ or r is a linear combination, with coefficients in k, of monomials, none of which is divisible by any of the $LT(f_1), \ldots, LT(f_s)$. We call r a **remainder** of f on division by F, and often denote it as $\overline{f}^F$. Furthermore, if $q_i f_i \neq 0$, then*

$$\deg(f) \geq \deg(q_i f_i).$$

We prove this theorem by means of examining the pseudo-code for this algorithm and through use of examples. The pseudo-code, as provided by [4], establishes the existence of q_i and r and can be found in Algorithm 3. Furthermore, we will discuss the termination of the algorithm within the section.

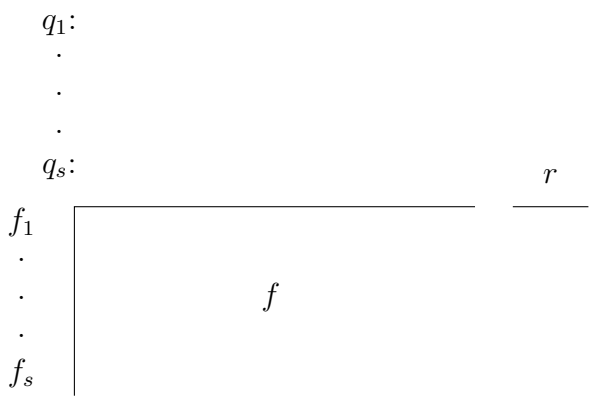
Division in $k[x_1, \ldots, x_n]$ and its algorithm follow closely to that of division in $k[x]$. We will denote the polynomial in the dividend by f, divisors by f_i, and quotients by q_i. First we must fix a monomial order $\succ$, if one is not specified. Since the order in which the divisors themselves are listed may change the result, we will maintain

Algorithm 3: Division in $k[x_1, \ldots, x_n]$

Input : $f_1, \ldots, f_s, f$
Output: $q_1, \ldots, q_s, r$

```
1  q_i := 0
2  r := 0
3  p := f
4  while p ≠ 0 do
5  |  i := 1
6  |  divisionoccured := false
7  |  s := r
8  |  while i ≤ s AND divisionoccurred = false do
9  |  |  if LT(f_i) divides LT(p) then
10 |  |  |  q_i := q_i+LT(p)/LT(f_i)
11 |  |  |  p := p − (LT(p)/LT(f_i)) ∗ f_i
12 |  |  |  divisionoccurred :=true
13 |  |  else
14 |  |  |  i := i + 1
15 |  |  end
16 |  end
17 |  if divisionoccurred = false then
18 |  |  r := r+LT(p)
19 |  |  p := p−LT(p)
20 |  end
21 end
22 RETURN q_1, ..., q_s, r;
```

consistency in which the order of the polynomials as they appear in the basis. To the right of this division, we track any remainder terms we obtain along the way. We set this division up to appear in the following fashion:



As to maintain consistency with the pseudo-code, we initialize $p = f$. If there is more than one divisor we begin by finding the first f_i in which $\mathrm{LT}(f_i)|\mathrm{LT}(p)$. We then perform division of these leading terms $\mathrm{LT}(p)/\mathrm{LT}(f_i)$ and place this value with the corresponding quotient q_i. We then multiply this value by the corresponding f_i, and subtract the result from p. We then redefine p using the result of this subtraction. Next we consider the redefined $\mathrm{LT}(p)$ and continue the process mentioned until we encounter a $\mathrm{LT}(p)$ which is not divisible by any of the $\mathrm{LT}(f_i)$. If this happens we remove this term and place it with our remainder. We proceed with either a "division step" or a "remainder step" until there are no terms remaining for p. Once completed, this process will achieve q_i and r; it is important to note q_i and r are unique *only* for the specified order in which the divisors are listed. In $k[x]$, a wonderful property of division is the uniqueness of the quotient and remainder. If we decide to change the order of the polynomials in our basis, we find we are not guaranteed to achieve the

same quotients and remainder.

As with division in $k[x]$, the division algorithm in $k[x_1, \ldots, x_n]$ will also terminate. Consider at each iteration either a division step or a remainder step is performed. Regardless of which, every time we redefine the dividend p the multidegree drops or p becomes zero. Assuming a division step is performed, observe that we redefine p (denoted here as p') as

$$p' = p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \cdot f_i.$$

Consider the leading term of the polynomial being subtracted from p

$$\mathrm{LT}\left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \cdot f_i\right) = \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \cdot \mathrm{LT}(f_i) = \mathrm{LT}(p).$$

This implies p' has a multidegree which is strictly less than p, assuming $p \neq 0$. This implies whenever we redefine p during a division step the multidegree is strictly decreasing. By the well-ordering property, eventually we must achieve $p = 0$, in which the algorithm terminates.

Next, we consider some examples.

Example 4.2. To illustrate division in $k[x_1, \ldots, x_n]$, consider the following polynomial $f = x^2yz^2 - xy^2 - y^2z + z^3$ which we will divide by

$$F = (f_1, f_2, f_3) = (x^2 - z, y - z, xy) \subset \mathbb{C}[x, y, z].$$

We will use Lex ordering. To begin, we set up the division as follows:

$$
\begin{array}{rl}
q_1\text{:} & \\
q_2\text{:} & \\
q_3\text{:} & \qquad\qquad\qquad\qquad\qquad\qquad\quad r \\
x^2 - z & \left| \begin{array}{l} \\ \\ \\ \end{array} \right. \\
y - z & \left| \begin{array}{l} x^2yz^2 - xy^2 + y^2z + z^3 \\ \\ \end{array} \right. \\
xy & \left| \begin{array}{l} \\ \\ \end{array} \right.
\end{array}
$$

First denote $p = f$ and consider $\mathrm{LT}(p) = x^2yz^2$. Considering each $\mathrm{LT}(f_i)$, we find the first f_i in which $\mathrm{LT}(f_i)|\mathrm{LT}(p)$ is f_1. Then, $\mathrm{LT}(p)/\mathrm{LT}(f_1) = yz^2$. As such, this value is placed with q_1. Multiplying $\mathrm{LT}(p)/\mathrm{LT}(f_1) \cdot f_1 = yz^2$ and subtracting

$$p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_1)} \cdot f_1 = -xy^2 + y^2z + yz^3 + z^3.$$

This result is how we will redefine p. We again consider $\mathrm{LT}(p) = -xy^2$. We see f_2 is the first divisor listed such that $\mathrm{LT}(f_2)|\mathrm{LT}(p)$. This division $\mathrm{LT}(p)/\mathrm{LT}(f_2) = -xy$, so this value is placed with q_2. Again, $\mathrm{LT}(p)/\mathrm{LT}(f_2) \cdot f_2 = -xy^2 + xyz$ is subtracted from p. The result of this is

$$p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_2)} \cdot f_2 = -xyz + y^2z + yz^3 + z^3.$$

These first two iterations of division are shown below.

$q_1 : yz^2$

$q_2 : -xy$

$q_3 :$

$$
\begin{array}{r|l|l}
x^2 - z & & r \\
\cline{2-3}
y - z & x^2yz^2 - xy^2 + y^2z + z^3 & \\
xy & & \\
\cline{2-2}
 & \underline{x^2yz^2 - yz^3} & \\
 & -xy^2 + y^2z + yz^3 + z^3 & \\
 & \underline{-xy^2 + xyz} & \\
 & -xyz + y^2z + yz^3 + z^3 &
\end{array}
$$

We continue until we encounter $\mathrm{LT}(p)$ which is not divisible by any $\mathrm{LT}(f_i)$. After three iterations, we appear to encounter a leading term $-xz^2$ which is not divisible by any of the leading terms of the divisors. As such, we remove this term and place in the remainder column to the right. We continue this algorithm, which is shown in its entirety below.

$q_1 : yz^2$

$q_2 : -xy - xz + yz + z^3 + z^2$

$q_3 : 0$ $\qquad\qquad\qquad\qquad r$

$$
\begin{array}{l|l}
x^2 - z & \\
y - z & x^2yz^2 - xy^2 + y^2z + z^3 \\
xy &
\end{array}
$$

$$
\begin{array}{lll}
\underline{x^2yz^2 - yz^3} & & \\
-xy^2 + y^2z + yz^3 + z^3 & & \\
\underline{-xy^2 + xyz} & & \\
-xyz + y^2z + yz^3 + z^3 & & \\
\underline{-xyz + xz^2} & & \\
\underline{-xz^2 + y^2z + yz^3 + z^3} & \longrightarrow & -xz^2 \\
y^2z + yz^3 + z^3 & & \\
\underline{y^2z - yz^2} & & \\
yz^3 + yz^2 + z^3 & & \\
\underline{yz^3 + z^4} & & \\
yz^2 + z^4 + z^3 & & \\
\underline{yz^2 - z^3} & & \\
\underline{z^4 + 2z^3} & \longrightarrow & -xz^2 + z^4 \\
\underline{2z^3} & \longrightarrow & -xz^2 + z^4 + 2z^3 \\
0 & &
\end{array}
$$

The result of the division implies we can write f as

$$f = (yz^2)(x^2 - z) + (-xy - xz + yz + z^3 + z^2)(y - z) + 0 \cdot (xy) + (-xz^2 + z^4 + 2z^3).$$

Henceforth, we will reference the result of any division using this form.

Recall these quotients and remainder are not necessarily unique if we change the

order of the divisors. When dividing, we always use the *first* divisor listed whose leading term divides the leading term of the dividend. Here we have three divisors, and as such there are six different ways we can permute the divisors, each of which may result in a different remainder and quite possibly a remainder of zero. It can be shown no matter how we list the divisors the remainder in this example is always nonzero. Suppose we change the order of the polynomials in the divisors to $F = (f_3, f_2, f_1) = (xy, y - z, x^2 - z)$. By doing this, we achieve the following result

$$f = (xz^2 - y) \cdot (xy) + (z^2 + yz) \cdot (y - z) + 0 \cdot (x^2 - z) + (2z^3).$$

Unsurprisingly, comparing this result to the previous, we see the remainders differ.

As mentioned, we can determine if a polynomial f is an element of an ideal $I = \langle f_1, \ldots, f_s \rangle$ by dividing f by $F = (f_1, \ldots, f_s)$. If we find the remainder $\overline{f}^F = 0$ this is enough to conclude $f \in I$. Consider the next example, in which changing the order of the divisors causes us to achieve a zero remainder. This illustrates a remainder of zero is a *sufficient* but *not necessary* condition for ideal membership.

Example 4.3. (Example 5 in [4]) Let $f = xy^2 - x$ and let I be the ideal generated by $I = \langle xy - 1, y^2 - 1 \rangle$. Assuming Lex order, let $F = (f_1, f_2) = (xy - 1, y^2 - 1) \subset \mathbb{C}[x, y]$ and observe the result of the division of f by F

$$f = y \cdot (xy - 1) + 0 \cdot (y^2 - 1) + (-x + y).$$

We see $\overline{f}^F = -x + y \neq 0$. This division is not sufficient enough to claim f has membership in the ideal I, as we have not performed division for every possible order

of the basis elements. If we maintain the same basis but change the order of the elements to $F^* = (f_2, f_1) = (y^2 - 1, xy - 1)$, we achieve the following result upon division

$$f = x \cdot (y^2 - 1) + 0 \cdot (xy - 1) + 0.$$

Now we have a remainder of zero which is sufficient for us to conclude $f \in I$.

Undoubtedly, performing division in $k[x_1, \ldots, x_n]$ just once can prove to be a lengthy process and is certainly one we would like to avoid performing repetitively. A computer algebra system can help make this process quicker, but what happens if we have potentially tens or hundreds of divisors? Is there a way to remedy the issue of the lack of uniqueness in remainders? It will be shown that a Gröbner basis corrects for such an issue and as a result division need only be performed once to check for ideal membership.

5 Gröbner Bases

5.1 Gröbner Basis and Hilbert Basis Theorem

Before defining a Gröbner basis, we discuss the Ascending Chain Condition which will prove to be a useful result.

Definition 5.1. An **ascending chain** of ideals is a nested increasing sequence of ideals $I_i \subseteq k[x_1, \ldots, x_n]$ such that

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

Example 5.2. The following is a finite ascending chain of ideals

$$\langle x_1 \rangle \subseteq \langle x_1, x_2 \rangle \subseteq \cdots \subseteq \langle x_1, \dots, x_n \rangle.$$

If we attempt to extend this chain further by including some $f \in k[x_1, \dots, x_n]$ so that $\langle x_1, \dots, x_n \rangle \subseteq \langle x_1, \dots, x_n, f \rangle$, then either $\langle x_1, \dots, x_n \rangle = \langle x_1, \dots, x_n, f \rangle$ or $\langle x_1, \dots, x_n, f \rangle = k[x_1, \dots, x_n]$. If $f \in \langle x_1, \dots, x_n \rangle$ then clearly f need not be included in $\langle x_1, \dots, x_n \rangle$ and we are done. If $f \notin \langle x_1, \dots, x_n \rangle$, then let $f \in k[x_1, \dots, x_n]$. We will show $\langle x_1, \dots, x_n, f \rangle = k[x_1, \dots, x_n]$. By the division algorithm we can write

$$f = q_1 x_1 + \cdots + q_n x_n + r$$

such that none of the monomials of r are divisible by $x_1, \dots, x_n$. Therefore, since $f \in k[x_1, \dots, x_n]$ this would imply r must be a constant. Observe that we can write

$$r = f - q_1 x_1 - \cdots - q_n x_n \in \langle x_1, \dots x_n, f \rangle.$$

Since r is a constant in $\langle x_1, \dots, x_n, f \rangle$, then clearly $1 \in \langle x_1, \dots, x_n, f \rangle$ and therefore $\langle x_1, \dots, x_n, f \rangle = k[x_1, \dots, x_n]$.

This example illustrates there is a maximal ideal for every polynomial ring.

Definition 5.3. An ideal $I \subseteq k[x_1, \dots, x_n]$ is said to be **maximal** if $I \subsetneq k[x_1, \dots, x_n]$, and any ideal J containing I is either I itself or $k[x_1, \dots, x_n]$.

The following theorem was first applied to ring theory by Amelia Emmy Noether, who is often referred to as "the mother of modern algebra". Noether, who was invited

to Göttingen by David Hilbert in 1919, helped develop much of the theory behind commutative algebra, especially in her famous 1921 paper "Theory of Ideals in Ring Domains" [1].

Theorem 5.4 (The Ascending Chain Condition)**.** *Let*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

be an ascending chain of ideals in $k[x_1, \dots, x_n]$*. Then, there exists an* $N \geq 1$ *such that*

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

Proof. This condition is equivalent to saying every ideal in $k[x_1, \dots, x_n]$ can be finitely generated, which is precisely the statement of the Hilbert Basis Theorem (Theorem 5.7). □

Before we define a Gröbner basis, a few more definitions and propositions are in order. We will also discuss the Hilbert Basis Theorem, which guarantees us the property of finiteness. A Gröbner basis will also allow us to perform division a single time to see the result of the remainder, as these special bases afford us a uniqueness property of remainders regardless of which order we choose for our divisors. Recall division in $k[x_1, \dots, x_n]$, in general, did not enjoy this property. This made answering the question of ideal membership a potentially lengthy process if our basis for the ideal consisted of many polynomials.

Definition 5.5. Let $I \subseteq k[x_1, \ldots, x_n]$ be a nonzero ideal with some monomial ordering on $k[x_1, \ldots, x_n]$.

i. We denote $\mathrm{LT}(I)$ as the set of leading terms of nonzero elements of I

$$\mathrm{LT}(I) = \{cx^\alpha : \text{there exists } f \in I \setminus \{0\} \text{with } \mathrm{LT}(f) = cx^\alpha\}.$$

ii. We denote $\langle \mathrm{LT}(I) \rangle$ as the ideal generated by the elements of $\mathrm{LT}(I)$.

The following is an important and powerful proposition, as it states for an ideal $I \subseteq k[x_1, \ldots, x_n]$, $\langle \mathrm{LT}(I) \rangle$, a potentially infinite generating set, can instead be generated by a finite collection of leading terms of polynomials in I.

Proposition 5.6. *Let $I \subseteq k[x_1, \ldots, x_n]$ be a nonzero ideal. Then,*

i. $\langle LT(I) \rangle$ is a monomial ideal;

ii. There are $g_1, \ldots, g_t \in I$ such that $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$.

Proof. Clearly, since elements $g \in \mathrm{LT}(I)$ are monomials with some constant multiple then $\langle \mathrm{LT}(I) \rangle$ is a monomial ideal since leading terms and leading monomials will generate the same ideal. Since $\langle \mathrm{LT}(I) \rangle$ is a monomial ideal, then by Dickson's lemma (Theorem 3.20), $\langle \mathrm{LT}(I) \rangle$ has a finite basis generated by monomials $g_1, \ldots, g_t$, and therefore $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. □

For $G = \{g_1, \ldots, g_t\}$, we often denote

$$\langle G \rangle = \langle g_1, \ldots, g_t \rangle$$

and

$$\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle.$$

Theorem 5.7 (Hilbert Basis Theorem)**.** *Every ideal $I \subseteq k[x_1, \ldots, x_n]$ has a finite generating set. In other words, $I = \langle G \rangle$ for some $G = \{g_1, \ldots, g_t\} \in I$.*

Proof. If I is the trivial ideal then $I = \langle 0 \rangle = \{0\}$, which is clearly finite. If I is nonempty then it must contain some nonzero polynomial in I. Then fix a monomial ordering $\succ$. Note $\langle \mathrm{LT}(I) \rangle$ exists and by proposition 5.6 we can find a finite number of $G = \{g_1, \ldots, g_t\} \in I$ such that

$$\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle$$

We will show $I = \langle G \rangle$. To do this, it suffices to show $\langle G \rangle \subseteq I$ and $I \subseteq \langle G \rangle$. The first inclusion is trivial as $g_1, \ldots, g_t \in I$ implies $\langle G \rangle = \langle g_1, \ldots, g_t \rangle \subseteq I$.

To see that $I \subseteq \langle G \rangle$, let f be any polynomial in I. Then by the division algorithm in $k[x_1, \ldots, x_n]$ we can divide f by G and write

$$f = q_1 g_1 + \cdots + q_t g_t + r$$

such that no terms of r are divisible by any $\mathrm{LT}(g_i)$. Then we can write

$$r = f - q_1 g_1 - \cdots - q_t g_t \in I.$$

Note if r is nonzero, then $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. By lemma 3.15 this implies $\mathrm{LT}(r)$ must be divisible by some $\mathrm{LT}(g_i)$. This contradicts the fact that no terms of r are divisible by any $\mathrm{LT}(g_i)$, therefore r must be zero and we can write

$$f = q_1 g_1 + \cdots + q_t g_t + 0 \in \langle g_1, \ldots, g_t \rangle.$$

This implies all $f \in I$ can be generated by $\langle g_1, \ldots, g_t \rangle$, and thus $I \subseteq \langle G \rangle$. Therefore $I = \langle G \rangle$. □

Definition 5.8. Fix a monomial order $\succ$ on the polynomial ring $k[x_1, \ldots, x_n]$. A finite subset $G = \{g_1, \ldots, g_t\}$ of a nonzero ideal $I \subseteq k[x_1, \ldots, x_n]$ is said to be a **Gröbner basis** if

$$\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle.$$

An equivalent, and maybe more intuitive definition bridged by lemma 3.15, is $\{g_1, \ldots, g_t\}$ is a Gröbner basis if and only if the leading term of any element in I is divisible by some $\mathrm{LT}(g_i)$. Gröbner bases have many useful properties and applications, and fortunately, every nonzero ideal in $k[x_1, \ldots, x_n]$ has such a basis.

Corollary 5.9. *For a fixed monomial ordering $\succ$, every ideal $I \subseteq k[x_1, \ldots, x_n]$ has a Gröbner basis and any Gröbner basis for an ideal I is a basis of I.*

The proof follows directly from the Hilbert Basis Theorem (Theorem 5.7).

Example 5.10. Let $I \subseteq \mathbb{C}[x, y]$ be the ideal generated by $I = \langle f_1, f_2 \rangle$ where $f_1 = x^2y - 1$ and $f_2 = xy^2 - x$, and use Lex ordering. Our goal is to determine if $F = \{f_1, f_2\}$ is a Gröbner basis for the ideal I. If F is in fact a Gröbner basis, this implies the leading term of *any* nonzero element of I must be divisible by the leading term of at least one of the polynomials in our basis. Equivalently, by the definition of a Gröbner basis,

$$\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle = \langle \mathrm{LT}(I) \rangle.$$

Recall any element of I can be written in the form

$$\langle f_1, f_2 \rangle = \{h_1 \cdot f_1 + h_2 \cdot f_2 : h_i \in \mathbb{C}[x, y]\}.$$

Consider the polynomial $x^2 - y$ which is an element of I, which can be shown by

$$\begin{aligned} yf_1 + (-x)f_2 &= y(x^2y - 1) + (-x)(xy^2 - x) \\ &= (x^2y^2 - y) + (-x^2y^2 + x^2) \\ &= x^2 - y. \end{aligned}$$

This result indicates F in *not* a Gröbner basis. Notice the leading term of this polynomial $\mathrm{LT}(x^2 - y) = x^2$ is *not* divisible by x^2y nor xy^2, which are the leading terms $\mathrm{LT}(f_1)$ and $\mathrm{LT}(f_2)$ respectively.

Proposition 5.11. *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal and let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for I. Then given $f \in k[x_1, \ldots, x_n]$, there is a unique $r \in k[x_1, \ldots, x_n]$ with the following two properties:*

i. No term of r is divisible by any of the $LT(G)$.

ii. There is a $g \in I$ such that $f = g + r$.

In particular, r is the remainder on division of f by G no matter how the elements of G are listed when using the division algorithm.

Proof. The properties follow by the division algorithm. Since uniqueness of remainders is an important part of Gröbner bases, we consider the proof. Assume we can write $f = g+r$ for some $g \in I$. Suppose the contrary that we can also write $f = g'+r'$ for some $g' \in I$ where $r \neq r'$. Then we have

$$g + r = g' + r' \implies g - g' = r - r'.$$

Since $g, g' \in I$, then $g - g' \in I$ and therefore $r - r' \in I$. This implies that

$$\mathrm{LT}(r - r') \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(G) \rangle.$$

That is, $\mathrm{LT}(g_i)|(r - r')$ for some $g_i \in G$, which is a contradiction. Therefore $r = r'$ which implies r is unique. □

As a result of the second condition, we have the following corollary.

Corollary 5.12. *Let G be a Gröbner basis for an ideal $I \subseteq k[x_1, \ldots, x_n]$ and let $f \in k[x_1, \ldots, x_n]$. Then $f \in I$ if and only if the remainder on the division of f by G is zero.*

Example 5.13. Recall the previous example where $F = \{x^2 - 1, xy^2 - x\} = \{f_1, f_2\}$, which we have already determined is *not* a Gröbner basis for $I = \langle x^2 - 1, xy^2 - x \rangle$. Because this is not a Gröbner basis, a unique remainder is not guaranteed. To see this, let $f = x^5y^2 - x^4 - x^2y + y^3$ and divide f by $F = (x^2 - 1, xy^2 - x) = (f_1, f_2)$.

This gives the following result:

$$f = q_1 f_1 + q_2 f_2 + r_1$$
$$f = (x^3y + x - 1)(x^2y - 1) + (0)(xy^2 - x) + (-3x^4 + x + y^3 - 1).$$

We find the remainder $r_1 = -3x^4+x+y^3-1$. If we change the order of the polynomials to $F^* = (xy^2 - x, x^2 - 1) = (f_2, f_1)$, and divide f by F^*, we find

$$f = q_1^* f_2 + q_2^* f_1 + r_2$$
$$f = (x^4)(xy^2 - x) + (-1)(x^2y - 1) + (x^5 - x^4 + y^3 - 1).$$

Notice $r_2 = x^5 - x^4 + y^3 - 1 \neq -3x^4 + x + y^3 - 1 = r_1$. Because division by F did not produce a unique remainder when the order of divisors was changed, this further supports that F is *not* a Gröbner basis. Regardless, by Corollary 5.9 we should be able to find a Gröbner basis for I.

Definition 5.14. Let f, $g \in k[x_1, \ldots, x_n]$ be nonzero polynomials. Then,

i. We denote the **least common multiple** of the leading monomials of f and g by

$$\mathrm{LCM}(f, g) = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g));$$

ii. We denote the S-**polynomial** of f and g by the combination

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

Example 5.15. Assume Lex order and let $f = x^3y + xy^3 - y^5$ and $g = xy^2 - y^4$ be polynomials in $k[x,y]$. Then, to find the S-polynomial of f and g we first find $\text{LCM}(f,g)$.

$$\begin{aligned}\text{LCM}(f,g) &= \text{lcm}(\text{LM}(f), \text{LM}(g)) \\ &= \text{lcm}(x^3y, xy^2) \\ &= x^3y^2.\end{aligned}$$

Then,

$$\begin{aligned}S(f,g) &= \frac{\text{LCM}(f,g)}{\text{LT}(f)} \cdot f - \frac{\text{LCM}(f,g)}{\text{LT}(g)} \cdot g \\ &= \frac{x^3y^2}{x^3y}(x^3y + xy^3 - y^5) - \frac{x^3y^2}{xy^2}(xy^2 - y^4) \\ &= y(x^3y + xy^3 - y^5) - x^2(xy^2 - y^4) \\ &= (x^3y^2 + xy^4 - y^6) - (x^3y^2 + x^2y^4) \\ &= xy^4 - y^6 + x^2y^4.\end{aligned}$$

Notice before the final simplification of the S-polynomial, the leading term of

$\frac{\text{LCM}(f,g)}{\text{LT}(f)} \cdot f$ and $\frac{\text{LCM}(f,g)}{\text{LT}(g)} \cdot g$ cancel. This is the purpose of the S-polynomial. S-polynomials are crucial to Gröbner bases and, as we will soon see, so is their remainder upon division by a basis F. As such, we denote the remainder of $S(f,g)$ upon division by some basis F by $\overline{S(f,g)}^F$.

Before moving to the algorithm for constructing Gröbner bases, an important lemma is in order. Note if we have a collection of polynomials with a shared degree, say δ, the only way for the sum of all of these polynomials to have a degree that is strictly less than δ is if the sum causes all leading terms to cancel. The following lemma shows S-polynomials are responsible for this canceling, and furthermore, it illustrates that S-polynomials will always produce a polynomial of a strictly smaller degree.

Lemma 5.16. *Suppose we have a sum* $\sum_{i=1}^{s} c_i f_i$, *where* $\deg(f_i) = \delta \in \mathbb{Z}^n_{\geq 0}$ *for all* i. *If* $\deg(\sum_{i=1}^{s} c_i f_i) < \delta$, *then* $\sum_{i=1}^{s} c_i f_i$ *is a linear combination, with coefficients in* k, *of the* S*-polynomials* $S(f_j, f_k)$ *for* $1 \leq j,\ k \leq s$ *where* $\deg(S(f_j, f_k)) < \delta$. *That is,*

$$\sum_{i=1}^{s} c_i f_i = \sum_{j,k} c_{j,k} S(f_j, f_k).$$

Proof. What this lemma states is if cancellation occurs among leading terms of polynomials sharing the same degree, this cancellation is equivalent to the cancellation occurring in S-polynomials. First let c_i include any constants of f_i. This allows us to assume $\text{LT}(f_i)$ is a monomial and that $\deg(f_i) = \delta$. Furthermore, we can conclude

that for all $i \neq j$

$$\text{LCM}(f_i, f_j) = \delta.$$

This implies f_i and f_j have the same leading monomial and therefore

$$S(f_i, f_j) = f_i - f_j.$$

Furthermore, since the sum $\sum_{i=1}^{s} c_i f_i$ has a degree strictly less than δ, then the sum of the leading coefficients should sum to zero. That is, $\sum_{i=1}^{s} c_i = 0$.

Using summation by parts, we set $f_{s+1} = 0$ and $C_i = c_1 + c_2 + \ldots c_i$ (which implies $C_s = \sum_{i=1}^{s} c_i = 0$) to achieve

$$\begin{aligned}
\sum_{i=1}^{s} c_i f_i &= (f_{s+1} - f_s)C_s - \sum_{i=1}^{s-1}(f_{i+1} - f_i)C_i \\
&= (0 - f_s) \cdot 0 - \sum_{i=1}^{s-1}(f_{i+1} - f_i)C_i \\
&= -\sum_{i=1}^{s-1} S(f_{i+1}, f_i)C_i
\end{aligned}$$

which is a linear combination of S-polynomials, as desired. □

That is, if we have $\deg(\sum_{i=1}^{s} f_i) < \delta$ where $\deg(f_i) = \delta$ for all i, then the cancellation occurring among leading terms is precisely the cancellation occurring due to the S-polynomial. This can be seen by

$$\sum_{i=1}^{s} f_i = \sum_{i=1}^{s-1} S(f_{i+1}, f_i)$$

since the polynomials in the summation on the left are all of degree δ, but the polynomials in the summation on the right all consist of polynomials of degree *strictly less than* δ, then the cancellation and decrease in degree are due to the S-polynomial.

5.2 Buchberger's Algorithm

Theorem 5.17 (Buchberger's Criterion)**.** *Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ of I is a Gröbner basis of I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G (listed in some order) is zero.*

Proof. Clearly, if we have a Gröbner basis G, then division by G results in a unique remainder. Since any $S(g_i, g_j) \in I$, then $\overline{S(g_i, g_j)}^G = 0$.

For the other direction, we use the idea of the proof given in [4]. Suppose we have a generating set $G = \langle g_1, \ldots, g_t \rangle$ and $\overline{S(g_i, g_j)}^G = 0$ for all $i \neq j$. To show G is in fact a Gröbner basis, we need to show $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$, for any nonzero $f \in I$. Since $f \in I$ and G is a generating set of I, we can write

$$f = h_1 g_1 + \cdots + h_t g_t.$$

Then, the degree of f is

$$\deg(f) \leq \max\{\deg(h_i g_i)\}.$$

Denote $\max\{\deg(h_i g_i)\} = \delta$. First, it is important to note there are many choices for $h_1, \ldots, h_t$. The choice of such polynomials will be those for which δ is minimal. That

is, we are looking for δ such that

$$\delta = \max\{\deg(h_1 g_1), \ldots, \deg(h_t g_t)\} \leq \tilde{\delta} = \max\{\deg(\tilde{h}_1 g_1), \ldots, \deg(\tilde{h}_t g_t)\}$$

for all $\tilde{h}_1, \ldots, \tilde{h}_t$ such that $f = \tilde{h}_1 g_1 + \cdots + \tilde{h}_t g_t$.

Now we have $\deg(f) \leq \delta$. This leaves us with two cases to consider: $\deg(f) = \delta$ or $\deg(f) < \delta$. If $\deg(f) = \delta$, then $\deg(f) = \deg(h_i g_i)$ for some i, which implies $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g_i)$. This means $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$.

On the other hand, if $\deg(f) < \delta$, we will see this contradicts the minimality of δ. To see this, write f as

$$\begin{aligned} f &= h_1 g_1 + \cdots + h_t g_t \\ &= \sum_{\deg(h_i g_i) = \delta} h_i g_i + \sum_{\deg(h_i g_i) < \delta} h_i g_i \\ &= \sum_{\deg(h_i g_i) = \delta} \mathrm{LT}(h_i) g_i + \sum_{\deg(h_i g_i) = \delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{\deg(h_i g_i) < \delta} h_i g_i. \end{aligned}$$

Note the last two summations contain polynomials whose degree is strictly *less than* δ. Since we are assuming $\deg(f) < \delta$, this implies

$$\deg\left(\sum_{\deg(h_i g_i) = \delta} \mathrm{LT}(h_i) g_i \right) < \delta.$$

That is, we see the polynomials inside the summation all have degree δ, but the sum itself has degree strictly less than δ. Then by lemma 5.16 we must be able to write

this sum equivalently as a linear combination of S-polynomials. Observe that we can write $\mathrm{LT}(h_i) = c_i x^{\alpha_i}$, and so we have

$$\sum_{\deg(h_i g_i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{\deg(h_i g_i)=\delta} c_i x^{\alpha_i} g_i.$$

Then, we have the S-polynomials

$$S(x^{\alpha_j} g_j, x^{\alpha_k} g_k) = x^{\delta - \gamma_{jk}} S(g_j, g_k)$$

where $x^{\delta-\gamma_{jk}} = \mathrm{LCM}(g_i, g_k)$. Now, we have

$$\begin{aligned}
\sum_{\deg(h_i g_i)=\delta} \mathrm{LT}(h_i) g_i &= \sum_{\deg(h_i g_i)=\delta} c_i x^{\alpha_i} g_i \\
&= \sum_{j,k} c_{jk} S(x^{\alpha_j} g_j, x^{\alpha_k} g_k) \\
&= \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k)
\end{aligned}$$

and thus

$$\deg(S(x^{\alpha_j} g_j, x^{\alpha_k} g_k)) = \deg(x^{\delta-\gamma_{jk}} S(g_j, g_k)) < \delta. \tag{5.1}$$

Note since $\overline{S(g_j, g_k)}^{G} = 0$, we have the following

$$S(g_j, g_k) = \sum_{l=1}^{t} a_{jkl} g_l \implies x^{\delta-\gamma_{jk}} S(g_j, g_k) = \sum_{l=1}^{t} b_{jkl} g_l$$

where $a_{jkl}, b_{jkl} \in k[x_1, \ldots, x_n]$ and $b_{jkl} = a_{jkl} x^{\delta - \gamma_{jk}}$. Furthermore, by the division algorithm we have

$$\deg(a_{jkl} g_l) \leq \deg(S(g_j, g_k)). \tag{5.2}$$

Using equations 5.1 and 5.2, we see

$$\deg(b_{jkl} g_l) = \deg(x^{\delta - \gamma_{jk}} a_{jkl} g_l) \leq \deg(x^{\delta - \gamma_{jk}} S(g_j, g_k)) < \delta.$$

Then we have

$$\sum_{\deg(h_i g_i) = \delta} \mathrm{LT}(h_i) g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k) = \sum_{j,k} \sum_{l=1}^{t} c_{jk} b_{jkl} g_l.$$

Now, we write f as

$$\begin{aligned} f &= \sum_{\deg(h_i g_i) = \delta} \mathrm{LT}(h_i) g_i + \sum_{\deg(h_i g_i) = \delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{\deg(h_i g_i) < \delta} h_i g_i \\ &= \sum_{j,k} \sum_{l=1}^{t} c_{jk} b_{jkl} g_l + \sum_{\deg((h_i - \mathrm{LT}(h_i)) g_i) < \delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{\deg(h_i g_i) < \delta} h_i g_i \end{aligned}$$

and since $\deg(b_{jkl} g_l) < \delta$ for all j, k, l we have

$$f = \sum_{i=1}^{s} \tilde{h}_i g_i.$$

This implies f can be written as a linear combination of the basis elements with

coefficients in $k[x_1, \ldots, x_n]$. It also implies

$$\tilde{\delta} = \max\{\deg(\tilde{h}_1 g_1), \ldots, \deg(\tilde{h}_t g_t)\} < \delta = \max\{\deg(h_1 g_1), \ldots, \deg(h_t g_t)\},$$

but δ was chosen to be minimal, so this contradicts the minimality of δ. Thus $\deg(f) = \delta$ and therefore G must be a Gröbner Basis. □

Buchberger's Criterion is useful for determining if a basis is, in fact, a Gröbner basis. So what if this criterion tells us we fail to have a Gröbner basis? Can we construct one from the given basis? This is precisely the purpose of Buchberger's Algorithm. This algorithm takes some basis F and adds nonzero remainders of $\overline{S(f_i, f_j)}^F$ to F until we achieve a zero remainder for all S-polynomials in F. That is, we add $\overline{S(f_i, f_j)}^F \neq 0$ to F for all $i \neq j$ until $\overline{S(f_i, f_j)}^F = 0$ for all $i \neq j$. Then the new basis F, which now includes all of these nonzero remainders, is a Gröbner basis.

The crucial piece of this algorithm, as with most algorithms, is finiteness. A Gröbner basis must be a *finite* subset of polynomials. How can we be sure this algorithm will eventually terminate and produce a finite basis? We consider this in the proof of the theorem below.

Theorem 5.18 (Buchberger's Algorithm)**.** *Let $I = \langle f_1, \ldots, f_s \rangle$ be a nonzero polynomial ideal. Then a Gröbner basis for I can be constructed in a finite number of steps by the following algorithm.*

Algorithm 4: Buchberger's Algorithm [4]

Input : $F = (f_1, \ldots, f_s)$
Output: $G = (g_1, \ldots, g_t)$, where G is a Gröbner basis for I and $F \subseteq G$

```
1  G := F repeat
2  |  G' := G;
3  |  for each pair {p, q}, p ≠ q ∈ G' do
4  |  |  r := S(p, q)^{G'} if r ≠ 0 then
5  |  |  |  G := G ∪ {r}
6  |  |  end
7  |  end
8  |  G = G'
9  until;
10 RETURN G;
```

Proof. Consider at each step of the algorithm we begin with some basis, say G' and adjoin any nonzero remainders of S-polynomials. Denote this larger basis as G. Then we have $G' \subseteq G$ with equality occurring only when the algorithm terminates. This also implies $\langle \mathrm{LT}(G') \rangle \subseteq \langle \mathrm{LT}(G) \rangle$. Assuming we do not have equality, then $\langle \mathrm{LT}(G') \rangle \subsetneq \langle \mathrm{LT}(G) \rangle$. Observe when $G' \neq G$ then there exists a remainder r adjoined to G which is not in G'. Since r is the remainder found upon division by G', the definition of a remainder implies that no term of r is divisible by any $\mathrm{LT}(G')$ and therefore $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G') \rangle$. However, $\mathrm{LT}(r) \in \langle \mathrm{LT}(G) \rangle$. That is, we see each step of the algorithm creates an ascending chain of ideals

$$\langle \mathrm{LT}(G') \rangle \subseteq \langle \mathrm{LT}(G) \rangle.$$

By the Ascending Chain Condition (Theorem 5.4), this chain will eventually stabilize after a *finite* number of iterations and eventually we will achieve

$$\langle \mathrm{LT}(G') \rangle = \langle \mathrm{LT}(G) \rangle.$$

Therefore we have $G' = G$, and the algorithm terminates and produces a finite Gröbner basis. □

Let us continue with the basis from the previous example and use Buchberger's Algorithm to create a Gröbner basis.

Example 5.19. Continuing with the divisors $F = (f_1, f_2)$ from Example 5.10, where $f_1 = x^2y - 1$ and $f_2 = xy^2 - x$, we have determined F is *not* a Gröbner Basis and will construct a Gröbner basis using F. First, we find the S-polynomial of f_1 and f_2

$$\begin{aligned} S(f_1, f_2) &= \frac{x^2y^2}{x^2y}(x^2y - 1) - \frac{x^2y^2}{xy^2}(xy^2 - x) \\ &= x^2y^2 - y - (x^2y^2 - x^2) \\ &= x^2 - y. \end{aligned}$$

Next, performing division of $S(f_1, f_2)$ by F, we achieve the following remainder

$$\overline{S(f_1, f_2)}^F = x^2 - y \neq 0.$$

Because of this nonzero remainder, we denote this $f_3 = x^2 - y$ and add it to F; now $F = (x^2y - 1, xy^2 - x, x^2 - y)$. We will repeat this process until $\overline{S(f_i, f_j)}^F = 0$ for all $i \neq j$. Observe

$$S(f_1, f_3) = y^2 - 1 = \overline{S(f_1, f_3)}^F$$

which is nonzero, so we denote $f_4 = y^2 - 1$ and add it to F. Now $F = (x^2y - 1, xy^2 - x, x^2 - y, y^2 - 1)$. Then,

$$S(f_1, f_4) = x^2 - y$$

which notice $S(f_1, f_4) = x^2 - y = f_3$. Because of this, $\overline{S(f_1, f_4)}^F = 0$. Since we achieved a remainder of 0 we leave F unchanged and continue the algorithm. From here we find $\overline{S(f_i, f_j)}^F = 0$ for all pairs $i \neq j$. Therefore we may terminate the algorithm and the resulting basis

$$G = \{x^2y - 1, xy^2 - x, x^2 - y, y^2 - 1\}$$

is a Gröbner basis. In Listing 1 we verify that these polynomials form a Gröbner basis for $I = \langle f_1, f_2 \rangle$.

Listing 1: Maple 2020 output for example 5.19

```
G := [x^2y - 1, xy^2 - x, x^2 - y, y^2 - 1];

            G := [x^2y - 1, xy^2  - x, x^2  - y, y^2  - 1]

IsBasis(G, plex(x, y));

                                  true
```

Is this the *only* Gröbner basis for $I = \langle x^2y - 1, xy^2 - x \rangle$? It is possible, but it's likely there are many different Gröbner bases for I. Is there a way to find a *unique* Gröbner basis? Yes, but first we find what is called a minimal Gröbner Basis.

Lemma 5.20. *Let G be a Gröbner basis of $I \subseteq k[x_1, \ldots, x_n]$. Let $p \in G$ be a polynomial such that $LT(p) \in \langle LT(G \setminus \{p\})\rangle$. Then, $G \setminus \{p\}$ is also a Gröbner basis for I.*

Proof. Since clearly $\mathrm{LT}(p) \in \langle \mathrm{LT}(G)\rangle$ and $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\})\rangle$, then we have $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(G \setminus \{p\})\rangle$. Since G is a Gröbner basis then $G \setminus \{p\}$ is also a Gröbner basis. □

This reduction may still not be unique, though.

Example 5.21. Returning to the Gröbner basis we found in the previous example where $G = \{x^2y - 1, xy^2 - x, x^2 - y, y^2 - 1\} = \{g_1, \ldots, g_4\}$, we will find a minimal Gröbner basis for G. Notice $\mathrm{LT}(g_1) = x^2y = y \cdot (\mathrm{LT}(g_3))$ and similarly $\mathrm{LT}(g_2) = xy^2 = x \cdot (\mathrm{LT}(g_4))$. By the lemma 5.20, we can remove g_1 and g_2 from our Gröbner basis G and we will still remain with a Gröbner basis for the ideal. We now have a *minimal* Gröbner Basis consisting of the polynomials

$$g_3 = x^2 - y, \text{ and } g_4 = y^2 - 1;$$

the remaining polynomials in G have leading terms that *cannot* be written in terms of $\langle \mathrm{LT}(G)\rangle$, though that does not necessarily mean this is the *only* minimal Gröbner basis for G. For example,

$$g_3^* = x^2 - ay^2 - y, \text{ and } g_4 = y^2 - 1$$

is also a minimal Gröbner basis for the same ideal for any $a \in \mathbb{C}$. This can be seen by the fact that

$$\langle \mathrm{LT}(g_3), \mathrm{LT}(g_4) \rangle = \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_3^*), \mathrm{LT}(g_4) \rangle.$$

This example indicates there may be infinitely different *minimal* Gröbner bases for an ideal. Notice first that all minimal Gröbner bases for an ideal I will consist of the same leading terms. Fortunately we can find a *unique* minimal basis which we refer to as the *reduced* Gröbner basis.

Definition 5.22. A **reduced Gröbner basis** for a polynomial ideal I is a Gröbner basis G for I such that:

i. $\mathrm{LC}(p) = 1$ for all $p \in G$.

ii. For all $p \in G$, no monomial of p lies in $\langle \mathrm{LT}(G \setminus \{p\}) \rangle$.

Example 5.23. In the previous example notice the $\mathrm{LC}(g_i) = 1$ for all i, so we do not need to worry about reducing any leading coefficients. If some $\mathrm{LC}(g_i) \neq 1$, we would multiply g_i by an appropriate constant c such that $c \cdot (\mathrm{LC}(g_i)) = 1$. That is, $G = \{x^2 - y, y^2 - 1\}$ is in fact the reduced Gröbner basis for I as none of the polynomials have a monomial which can be generated by the leading term of any other polynomial. We again verify this claim in Listing 2 using Maple 2020.

Listing 2: Maple 2020 output for example 5.23

```
B := Basis(G, plex(x, y));

                    B := [y^2  - 1, x^2  - y]
```

Theorem 5.24. *Let I be a nonzero polynomial ideal. Then, for a given monomial ordering I has a reduced Gröbner basis and the reduced Gröbner basis is unique.*

Proof. To prove existence, we first consider the process of "fully reducing" and element $g \in G$, where G is some *minimal* Gröbner basis for an ideal I. We say g is "fully reduced" if no monomial of g is in $\mathrm{LT}\langle(G \setminus \{g\})\rangle$. Since all minimal Gröbner bases consist of polynomials with the same leading terms, then g is fully reduced for any minimal Gröbner basis for the ideal I.

Denote $g' = \overline{g}^{G\setminus\{g\}}$. Including this remainder in the basis G and removing the element g, we now denote $G' = (G \setminus \{g\}) \cup \{g'\}$. We claim G' is also a minimal basis for the ideal I. Consider that $\mathrm{LT}(g) \in g'$ since $\mathrm{LT}(g) \notin \mathrm{LT}\langle(G \setminus \{g\})\rangle$. Then G' and G both consist of polynomials with the same leading terms, i.e.,

$$\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(G')\rangle.$$

Since G is by definition a Gröbner basis, then $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(G)\rangle$. Therefore

$$\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(G')\rangle.$$

By applying the process of fully reducing each necessary element in G, we maintain a Gröbner basis for the ideal I. Furthermore, we maintain minimality as well, since "fully reducing" each element results in removing a single element from the basis, and returning a single remainder. If we find $g' = 0$, then this implies the assumption that G was minimal was not satisfied.

Next, we show that this process will produce a unique reduced basis by means of a contradiction. Suppose both G and $\tilde{G}$ are unique reduced Gröbner bases for the ideal I. Then by definition they are both minimal and therefore consist of polynomials

with the same leading terms. That is,

$$\mathrm{LT}(G) = \mathrm{LT}(\tilde{G}) \implies \langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(\tilde{G}) \rangle.$$

For $g \in G, \tilde{g} \in \tilde{G}$ such that $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$, note that $g, \tilde{g} \in I$. Thus,

$$g - \tilde{g} \in I \implies \overline{g - \tilde{g}}^{G} = 0.$$

Since $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$, then $g - \tilde{g}$ must cause a cancellation among the leading terms. By definition, since G and $\tilde{G}$ are minimal, then none of the remianing terms of $g - \tilde{g}$ will be divisible by any of the $\mathrm{LT}(G) = \mathrm{LT}(\tilde{G})$. Thus

$$0 = \overline{g - \tilde{g}}^{G} = g - \tilde{g},$$

which implies that $g = \tilde{g}$, and therefore $G = \tilde{G}$. □

Since a reduced Gröbner basis is *unique* it is often referred to as *the* Gröbner basis. If the basis is not unique then it is simply *a* Gröbner basis. The preceding theorem gives us the following corollary.

Corollary 5.25. *Let I, $J \subseteq k[x_1, \ldots, x_n]$ be ideals. Then, $I = J$ if and only if $G_I = G_J$, where G_I, G_J are the reduced Gröbner bases of I, J respectively.*

5.3 History

Before considering applications of Gröbner bases, where did these bases get their name? In the early 1960's, computing systems were in rapid development which ushered in advancements in computational algebra. In fact, Bruno Buchberger was

among the team of researchers at the very first computer laboratory. It is in this laboratory where Gröbner bases were first implemented [6]. Bruno Buchberger established these bases and his algorithm in 1965 in his PhD thesis, the title of which translates to "An algorithm for finding the basis elements of the residue class ring of a zero-dimensional polynomial ideal". He wrote this thesis under the supervision of his advisor Wolfgang Gröbner, whom he named such bases after. In his thesis he sought to "find a termination criterion for the algorithm and to sufficiently systematize it so that it is suitable for implementation on an electronic computer" [2]. He succeeded, but around ten years passed before his work was properly noticed. Today most computer algebra systems are equipped with Buchberger's algorithm. [6]

With computing power ever expanding during the 1970's, the recognition of his work drew him back to computational algebra. Arguably, his dedication to the field has kept it thriving. In 1985, when the field began to slow, he founded the Journal of Symbolic Computation. Shortly after, he founded the *Research Institute for Symbolic Computation* (RISC). With his help the field continued to expand, and as such so did the RISC. So much so that it eventually found its new home in a castle. Finally, with the help of his colleges, he created the *Softwarepark Hagenberg*: "one of the most dynamic and successful technology parks in Austria" [6].

Now that we are equipped with Buchberger's algorithm, we lastly consider some examples and applications and a brief discussion on the complexity.

5.4 Applications

For some ideal $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$, if $f_1, \ldots, f_s$ are all linear polynomials then finding a Gröbner basis is equivalent to the familiar process of Gaussian Elimination. If we create a system of equations from the polynomials in our ideal and find the reduced row echelon form of the corresponding matrix the resulting matrix will give the same polynomials as the reduced Gröbner basis. Though Buchberger's algorithm may be too powerful of a weapon for such a system, it helps illustrate the process for nonlinear systems.

Example 5.26. Consider the following ideal

$$I = \langle 3x - 6y + 21w, x - 2y - z + 2w, 2x - 4y + 2z + 24w \rangle \subseteq \mathbb{C}[w, x, y, z].$$

Assume Lex order where $x \succ y \succ z \succ w$. Then consider the corresponding system of equations

$$3x - 6y + 21w = 0$$

$$x - 2y - z + 2w = 0$$

$$2x - 4y + 2z + 24w = 0.$$

Consider the corresponding coefficient matrix, row echelon form matrix (ref), and *reduced* row echelon form (rref) matrix of the system, respectively:

$$\begin{pmatrix} 3 & -6 & 0 & 21 \\ 1 & -2 & -1 & 2 \\ 2 & -4 & 2 & 24 \end{pmatrix} \xrightarrow{\text{ref}} \begin{pmatrix} 1 & -2 & -1 & 2 \\ 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{\text{rref}} \begin{pmatrix} 1 & -2 & 0 & 7 \\ 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let's see how this relates to the process of finding a minimal Gröbner Basis and then the *reduced* Gröbner basis. First we use Buchberger's criterion to determine if $F = (3x-6y+21w, x-2y-z+2w, 2x-4y+2z+24w)$ already form a Gröbner basis for I. Denote $f_1 = 3x-6y+21w, f_2 = x-2y-z+2w, f_3 = 2x-4y+2z+24w$. Note $\overline{S(f_1,f_2)}^F = z+5w$, which is nonzero, so we add this polynomial to our basis. We now have $F = (3x-6y+21w, x-2y-z+2w, 2x-4y+2z+24w, z+5w)$. From here it can be shown $\overline{S(f_i,f_j)}^F = 0$ for all $i \neq j$. That is, the current basis F is a Gröbner basis, but it is no where near minimal. Notice first we can write $3 \cdot (\text{LT}(f_2)) = \text{LT}(f_1)$ as well as $2 \cdot (\text{LT}(f_2)) = \text{LT}(f_3)$. Therefore we can remove f_1 and f_3 from the basis F and we will still have a Gröbner basis for I. We now have the basis

$$G = \{x - 2y - z + 2w, z + 5w\}$$

which notice corresponds to the ref matrix found above. Furthermore, denoting

$$g_1 = x - 2y - z + 2w \text{ and } g_2 = z + 5w,$$

notice g_1 contains a monomial which can be found in $\langle \text{LT}(G \setminus \{g_1\}) \rangle$. Because of this, it is not a *reduced* Gröbner basis. Dividing g_1 by g_2 we obtain a remainder $r = x - 2y + 7w$. We let this be g_1. Now for g_1 and g_2 we see that none of the monomials of either polynomial can be written using the leading term of the other polynomial. We have thus achieved the unique reduced Gröbner basis

$$G = \{x - 2y + 7w, z + 5w\}$$

which corresponds to the rref form of the corresponding system of equations of the polynomials from the ideal I This example shows the process for finding a reduced Gröbner basis is a generalization of Gaussian Elimination and finding the reduced row echelon form of a system of linear equations.

As mentioned the question of ideal membership can be answered using division. For $F = (f_1, \ldots, f_s)$ we can determine if an element f lies in the ideal $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$ if $\overline{f}^F = 0$. Since a Gröbner basis G exists for the ideal I we can use the Gröbner basis instead to determine ideal membership.

Example 5.27. Consider the polynomial $f = xy^3 - z^2 + y^5 - z^3$ and use Revgrlex ordering. We question whether or not this polynomial lies in the ideal $I = \langle f_1, f_2 \rangle = \langle -x^3 + y, x^2y - z \rangle \subseteq \mathbb{C}[x, y, z]$. We can answer this question by first finding a Gröbner basis, specifically the reduced Gröbner basis via a computer algebra system:

$$G = \{g_1, g_2, g_2\} = \{x^3 - y, yx^2 - z, y^2 - xz\}.$$

Then dividing f by G we find $\overline{f}^G = 0$ since

$$f = 0 \cdot g_1 + (z^2 + z) \cdot g_2 + (xy + y^3 + xyz) \cdot g_3.$$

Therefore f must be an element of the ideal I.

Example 5.28 (A problem from [8])**.** Assume we have values a, b, c such that the

following equations are satisfied:

$$a + b + c = 3$$

$$a^2 + b^2 + c^2 = 5$$

$$a^3 + b^3 + c^3 = 7.$$

We can use these polynomials to show $a^4 + b^4 + c^4 = 9$. If we regard a, b, c as indeterminants and use Lex ordering, we consider the ideal

$$I = \langle f_1, f_2, f_3 \rangle = \langle a + b + c - 3, a^2 + b^2 + c^2 - 5, a^3 + b^3 + c^3 \rangle \subseteq \mathbf{I}(\mathbf{V}(f_1, f_2, f_3)).$$

This ideal is a subset of the set of all polynomials which are also satisfied by the values a, b, and c. That implies if $f = a^4 + b^4 + c^4 - 9 \in I$, then f is also in the ideal of the variety and therefore it is also satisfied by the values a, b, and c. To determine this we first find the reduced Gröbner basis of the ideal to be

$$G = \{g_1, g_2, g_3\} = \{a + b + c - 3, b^2 + bc - 3b + c^2 - 3c + 2, 3c^3 - 9c^2 + 6c + 2\}.$$

We find for $f = a^4 + b^4 + c^4 - 9$, that $\overline{f}^G = 0$. We verify this information further in Listing 3 using Maple 2020.

Listing 3: Maple 2020 output for example 5.28

```
B := [a + b + c - 3, a^2 + b^2 + c^2 - 5, a^3 + b^3 + c^3 -
   7];
        B := [a + b + c - 3, a^2 + b^2 + c^2 - 5, a^3 + b^3 + c
           ^3 - 7]
```

```
G := Basis(B, plex(a, b, c));

       G := [3c^3 - 9c^2 + 6c + 2, b^2 + bc + c^2 - 3b - 3c +

          2, a + b + c - 3]

NormalForm(a^4 + b^4 + c^4 - 9, G, plex(a, b, c));

                                  0
```

The command "NormalForm" computes the remainder upon division by the basis G.

We can also use this Gröbner basis to show $a^5 + b^5 + c^5 \neq 11$. We find now for $f = a^5 + b^5 + c^5 - 11$, $\overline{f}^G = -\frac{4}{3} \neq 0$, and verify this in Listing 4.

Listing 4: Maple 2020 output for example 5.28

```
NormalForm(a^5 + b^5 + c^5 - 11, G, plex(a, b, c));

                                 -4/3
```

As such, the values for a, b, and c do *not* satisfy $a^5 + b^5 + c^5 = 11$, but we can find d such that $a^5 + b^5 + c^5 = d$ is satisfied for the given values. Consider the equation $f = a^5 + b^5 + c^5$; computing the remainder of f upon division by G we find $\overline{f}^G = \frac{29}{3}$. This remainder is, in fact, the value for d which satisfies our equation. This can be seen by the fact

$$\begin{aligned} f &= q_1 g_1 + q_2 g_2 + q_3 g_3 + r \\ a^5 + b^5 + c^5 &= q_1 g_1 + q_2 g_2 + q_3 g_3 + \frac{29}{3} \\ a^5 + b^5 + c^5 - \frac{29}{3} &= q_1 g_1 + q_2 g_2 + q_3 g_3 \end{aligned}$$

for the unique q_1, q_2, q_3 found during division. That is, we see $a^5 + b^5 + c^5 - \frac{29}{3} \in I$ and therefore $a^5 + b^5 + c^5 = \frac{29}{3}$. We can use the same idea to find which constant d will satisfy $a^6 + b^6 + c^6 = d$ as well. For this equation we find the remainder upon division by G to be $\frac{19}{3}$, which means

$$a^6 + b^6 + c^6 = \frac{19}{3}.$$

We again verify that both of these polynomials are in the ideal with the Maple 2020 in Listing 5.

Listing 5: Maple 2020 output for example 5.28

```
NormalForm(a^5 + b^5 + c^5 - 29/3, G, plex(a, b, c));

                                0

NormalForm(a^6 + b^6 + c^6 - 19/3, G, plex(a, b, c));

                                0
```

Example 5.29. Consider the equations

$$x^2 + y^2 + z^2 = 1$$

$$x^2 + y^2 + z^2 = 2x$$

$$2x - 3y = z.$$

These equations determine the ideal

$$I = \langle x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z \rangle \subseteq \mathbb{C}[x, y, z]$$

which we will use to determine all the points in the variety $\mathbf{V}(I)$. While we could use $F = (x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z)$, let us instead use the Gröbner basis of the ideal using Lex order. Listing 6 contains the Maple 2020 commands and output for finding the Gröbner basis for the ideal.

Listing 6: Maple 2020 output for example 5.29

```
B := [x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z];

        B := [x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x -
           3y - z]

G := Basis(B, plex(x, y, z));

              G := [40z^2 - 8z - 23, 3y + z - 1, 2x - 1]
```

Denote $G = \{g_1, g_2, g_3\} = \{2x - 1, 3y + z - 1, 40z^2 - 8z - 23\}$. Notice how convenient the resulting Gröbner basis is. The polynomial g_3 is exclusively in terms of a single indeterminant z, g_2 is in terms of only z and y, and the last polynomial g_1 is only in terms of x. The next example will illustrate this elimination of variables even further. Certainly this system, which will have equivalent common solutions as the original system, is much easier to solve. Solving $g_1 = 0$ we find $x = \frac{1}{2}$. Since g_3 is a quadratic equation we can easily solve it as well and find $z = \frac{8 \pm \sqrt{3744}}{80}$. This allows us to substitute these values for z into g_2, and we achieve the following two

solutions to the system

$$x = \frac{1}{2}, y = \frac{\sqrt{26} - 6}{20}, z = \frac{8 - \sqrt{3744}}{80}$$
$$x = \frac{1}{2}, y = -\frac{\sqrt{26} - 6}{20}, z = \frac{8 + \sqrt{3744}}{80}.$$

The reduced Gröbner basis will have this "nice" property when using Lex order. In general, we will find that in a Gröbner basis, as we work towards g_n, the polynomials will begin to be eliminate indeterminants. These indeterminants will be eliminated in the order in which is determined by the monomial ordering used. For example if we have polynomials in $k[x, y, z]$, where $x \succ y \succ z$, we will find the first indeterminant to be eliminated is x. This allows for a "back-substitution" of sorts similar to that of Gaussian Elimination with back substitution. A system of equations in this form should make finding common solutions simpler than its original counterpart.

This elimination of indeterminants that occurs as we proceed through the the polynomials in a Gröbner basis has shown to be computationally irrelevant [5]. That is, the order in which indeterminants are eliminated does not change the solutions. The importance of the elimination of variables is the fact that we achieve at least one polynomial which is in terms of a single indeterminant, making finding solutions to some system "simpler". Although, in some application problems, we may wish to eliminate indeterminants in a particular order. Consider the next example, which contains polynomials in $\mathbb{C}[x, y, z]$, but through the use of Lagrange multipliers, an additional indeterminant λ is introduced, though we are not concerned with it's

solutions. Thus, we may wish to eliminate it first.

Example 5.30 (A variation of a problem in [4])**.** Find the extrema of $f(x, y) = 2x^2 + 3y^2 - 4x - 5$ be subject to the constraint $g(x, y) = x^2 + y^2 = 16$. This is a calculus problem which makes use of Lagrange multipliers to solve. Recall

$$\nabla f = \lambda \nabla g,$$

where ∇f and ∇g are defined to be the gradients of f and g respectively. The solutions to this system will give the critical points, or the location of such extrema. This gives us the following two equations as well as the equation of the constraint itself:

$$\begin{cases} 4x - 4 &= \lambda \cdot 2x \\ 6y &= \lambda \cdot 2y \\ x^2 + y^2 &= 16 \end{cases} \implies \begin{cases} 4x - 4 - 2\lambda x &= 0 \\ 6y - 2\lambda y &= 0 \\ x^2 + y^2 - 16 &= 0. \end{cases}$$

As one may expect we can find and utilize a Gröbner basis for this system of polynomials. Using a computer algebra system and Lex order with $\lambda \succ x \succ y$, one can find the resulting reduced Gröbner basis for the ideal

$$I = \langle 4x - 4 - 2\lambda x, 6y - 2\lambda y, x^2 + y^2 - 16 \rangle$$

is

$$G = \{y^3 - 12y, xy + 2y, x^2 + y^2 - 16, -y^2 + 16\lambda + 2x - 32\}.^1$$

It is again important to note we have a polynomial of a single indeterminant y (which is also last in order), and then we have two polynomials in terms of only x and y, the

[1]The Maple 2020 output verifying this can be found in the Appendix in listing 7.

next lowest indeterminants in terms of order. We have only one equation in terms of all three indeterminants. If we set the elements of our Gröbner basis equal to zero, this system proves simple to solve. The first equation gives the solutions

$$y^3 - 12y = 0 \implies y(y^2 - 12) = 0 \implies y = 0 \text{ or } y = \pm 2\sqrt{3}.$$

Using these solutions in the next equation, we see for $y = 0$, x can take on infinitely many solutions; when $y = \pm 2\sqrt{3}$ we get

$$x(\pm 2\sqrt{3}) + 2(\pm 2\sqrt{3}) = 0 \implies \pm 2\sqrt{3}(x + 2) = 0 \implies x = -2.$$

This gives us the solution $(-2 \pm 2\sqrt{3})$ which, notably, satisfies the proceeding equation $x^2 + y^2 - 16 = 0$. Also for this equation, when $y = 0$ we achieve the solution $x = \pm 4$. Since we are not actually concerned with solutions for λ this means we have the four critical points $\{(-2, \pm 2\sqrt{3}), (\pm 4, 0)\}$. Using the first and second derivative tests, it can be shown that $f(x, y)$ subject to the circle $x^2 + y^2 = 16$ attains a maximum of 47 twice at the points $(-2, \pm 2\sqrt{3})$ and a minimum of 11 at the point $(4, 0)$.

Notice that the coefficients in the preceding example remain relatively small, and the resulting equations prove relatively quick and simple to solve. As mentioned in previously, Buchberger's algorithm may produce polynomials with large coefficients and total degrees. Consider the next example, in which the total degrees stay relatively low, but the coefficients happen to become much larger than most examples

we have considered thus far.

Example 5.31 (A problem from [4])**.** Find the local minimum and maximum values of

$$f(x, y, z) = x^3 + 2xyz - z^2$$

subject to the constraint $g(x, y, z) = x^2 + y^2 + z^2 = 1$. Again, using the method of Lagrange multipliers we attain a local minimum or maximum when

$$\begin{cases} 3x^2 + 2yz &= \lambda \cdot 2x \\ 2xz &= \lambda \cdot 2y \\ 2xy - 2z &= \lambda \cdot 2z \\ x^2 + y^2 + z^2 &= 1. \end{cases} \implies \begin{cases} 3x^2 + 2yz - 2\lambda x &= 0 \\ 2xz - 2\lambda y &= 0 \\ 2xy - 2z - 2\lambda z &= 0 \\ x^2 + y^2 + z^2 - 1 &= 0. \end{cases}$$

This system of equations may prove difficult to solve using usual methods from high school algebra and calculus. Instead, we may wish to compute a Gröbner basis. Using the polynomials in the equations above, we generate an ideal

$$I = \langle 3x^2 + 2yz - 2\lambda x, 2xz - 2\lambda y, 2xy - 2z - 2\lambda z, x^2 + y^2 + z^2 - 1 \rangle.$$

We again assume Lex order with $\lambda \succ x \succ y \succ z$ and achieve the following (reduced)

Gröbner basis[2]

$$-335232z^6 + 477321z^4 - 11505yz - 134419z^2 + 7670\lambda - 11505x,$$

$$x^2 + y^2 + z^2 - 1,$$

$$-19584z^5 + 25987z^3 + 3835xy - 6403z,$$

$$-1152z^5 + 3835yz^2 - 1404z^3 + 3835xz + 2556z,$$

$$-9216z^5 + 3835y^3 + 3835yz^2 + 11778z^3 - 3835y - 2562z,$$

$$-6912z^5 + 3835y^2z + 10751z^3 - 3839z,$$

$$-1152z^6 + 118yz^3 + 1605z^4 - 118yz - 453z^2,$$

$$1152z^7 - 1763z^5 + 655z^3 - 44z.$$

Our instinct may be a system with four equations would be easier to solve than one with eight, but consider that most equations in our original system contained all four indeterminants. Examining the above polynomials we notice only the first is in terms of all four indeterminants. Furthermore, λ is the first indeterminant to be eliminated among the polynomials that follow. As we proceed down the list, x is eliminated next, and finally y. We find the final polynomial to be exclusively in terms of z. This is what we should expect. If we set this polynomial equal to zero and solve the corresponding equation, we should be able to use these zeros to back substitute into the previous equations.

[2]The Maple 2020 output verifying this can be found in the Appendix in listing 8.

Then, using methods from high-school algebra, we solve

$$1152z^7 - 1763z^5 + 655z^3 - 44z = 0$$

and we find the zeros

$$z = 0, \ \pm 1, \ \pm \frac{2}{3}, \ \pm \frac{\sqrt{11}}{8\sqrt{2}}.$$

We can now solve the previous equation for y. From here we can continue to back substitute solutions until we achieve the following collection of solutions (x, y, z) (in which solutions for λ are omitted, as it is no longer needed for the minimum and maximum values):

$$(\pm 1, 0, 0), \qquad (0, \pm 1, 0), \qquad (0, 0, \pm 1), \qquad (-\frac{2}{3}, \frac{1}{3}, \frac{2}{3}),$$
$$(-\frac{2}{3}, -\frac{1}{3}, -\frac{2}{3}), \qquad (-\frac{3}{8}, -\frac{3\sqrt{11}}{8\sqrt{2}}, \frac{\sqrt{11}}{8\sqrt{2}}), \qquad (-\frac{3}{8}, \frac{3\sqrt{11}}{8\sqrt{2}}, -\frac{\sqrt{11}}{8\sqrt{2}})$$

Since the elements of this basis generate the same ideal as I, the variety of the Gröbner basis will give us the solutions to the original system. From here we can use the second derivative test from calculus to determine which of these points are local minimums or maximums. While a few of these points are saddle points, or prove to be inconclusive by the second partial derivative test, we find a global maximum

occurring at a single point, and a global minimum occurring at two points:

$$\begin{aligned}(1,0,0) &\implies f(1,0,0) = 1\\ \left(-\frac{2}{3},-\frac{1}{3},-\frac{2}{3}\right) &\implies f\left(-\frac{2}{3},-\frac{1}{3},-\frac{2}{3}\right) = -\frac{28}{27}\\ \left(-\frac{2}{3},\frac{1}{3},\frac{2}{3}\right) &\implies f\left(-\frac{2}{3},\frac{1}{3},\frac{2}{3}\right) = -\frac{28}{27}.\end{aligned}$$

Additionally we have the a local minimum of -1 occurring at three points:

$$\begin{aligned}(-1,0,0) &\implies f(-1,0,0) = -1\\ (0,0,1) &\implies f(0,0,1) = -1\\ (0,0,-1) &\implies f(0,0,-1) = -1.\end{aligned}$$

5.5 Complexity and Improvements

Often a computer is used to find a Gröbner bases. While it is now clear the algorithm terminates, this does not imply it happens quickly. Moreover, the total degrees and coefficients on the elements in a Gröbner basis may become complicated or large. In the "worst case", finding a Gröbner basis for an ideal $I = \langle S \rangle$ such that $\deg(f) \leq d$ for all $f \in S$, may lead to polynomials of degree as large as 2^{2^d} [7]. Clearly $2^{2^d} \to \infty$ rapidly as $d \to \infty$. However, it has been shown that this upper bound is much more reasonable in the case of ideals in $k[x_1, \ldots, x_n]$ for $n \leq 3$. Moreover, "on average", the required run time and storage space tends to be practical for most

applications [4].

With research on-going in the field of commutative algebra, it comes to no surprise that many have found ways to improve Buchberger's Algorithm. As mentioned, the order in which variables are eliminated will not change the solutions. As a result, further research has been conducted to determine the "best" monomial ordering in order to reduce complexity. Revgrlex generally is the most efficient for Buchberger's original algorithm. In 2007, Quoc-NamTran found an algorithm for the most effective monomial ordering for use in Buchberger's algorithm for *fixed* ideals [9]. Since many application problems with Gröbner bases involve a given, fixed ideal, this has proven to be a very useful result.

In an attempt to reduce run time and size of total degree and coefficients, one may consider changing the monomial ordering [5]. Example 5.31 contains a Gröbner basis in which coefficients became arguably large, though there are many examples which contain polynomials with significantly larger total degree and size of coefficients. To help reduce this problem, a dynamic algorithm was offered in 1993 by Peter Gritzmann and Bernd Sturmfels, which changes the monomial ordering throughout iterations of Buchberger's algorithm [5]. In [5], Gritzmann and Sturmfels provide an example of a polynomial ideal $I = \{x^5 + y^3 + z - 1, x^2 + y^2 + z - 1, x^6 + y^5 + z^3 - 1\} \subseteq k[x, y, z]$; using Lex order with $x \prec y \prec z$ and Buchberger's original algorithm, they find a Gröbner basis for I containing a polynomial of degree 21 and a 19-digit coefficient. The largest coefficient their dynamic algorithm produced for the same ideal was only

three digits. In the same year, Massimo Caboara offers a dynamic algorithm as well, and together with John Perry, they improved the algorithm further around 20 years later [3]. Needless to say, the field of computational algebra continues to grow thanks to the work of Bruno Buchberger and many other mathematicians.

6 Conclusion

S-polynomials and the division algorithm in $k[x_1, \ldots, x_n]$ may be comprised of basic algebra, but both are evidently incredibly fundamental results. That is why it is surprising to hear how recent of an achievement Buchberger's algorithm is, which hinges mainly on S-polynomials and the division algorithm. Quickly, this fact becomes less surprising when one realizes the true power of this algorithm is achieved because of the development of computational methods. Because of Bruno Buchberger's devotion to his field, and the contributions of mathematicians before him, research continues to grow in the fields of commutative algebra and computational algebraic geometry.

Appendices

The following Maple 2020 output verifies the Gröbner basis in 5.30.

Listing 7: Maple 2020 output for example 5.30

```
B := [-2wx + 4x - 4, -2wy + 6y, x^2 + y^2 - 16];

          B := [-2wx + 4x - 4, -2wy + 6y, x^2 + y^2 - 16]

G := Basis(B, plex(w, x, y));

    G := [y^3 - 12y, xy + 2y, x^2 + y^2 - 16, -y^2 + 16w + 2x

       - 32]
```

The following Maple 2020 output verifies the Gröbner basis in 5.31.

Listing 8: Maple 2020 output for example 5.31

```
B := [-2wx + 3x^2 + 2yz, -2wy + 2xz, -2wz + 2xy - 2z, x^2 + y

   ^2 + z^2 - 1];

          B := [-2wx + 3x^2 + 2yz, -2wy + 2xz, -2wz + 2xy - 2z

              , x^2 + y^2 + z^2 - 1]

G := Basis(B, plex(w, x, y, z));

G := [1152z^7 - 1763z^5 + 655z^3 - 44z, -1152z^6 + 118yz^3 +

   1605z^4 - 118yz - 453z^2, -6912z^5 + 3835y^2z + 10751z^3 -

   3839z, -9216z^5 + 3835y^3 + 3835yz^2 + 11778z^3 - 3835y -

   2562z, -1152z^5 + 3835yz^2 - 1404z^3 + 3835xz + 2556z,

   -19584z^5 + 25987z^3 + 3835xy - 6403z, x^2 + y^2 + z^2 - 1,

-335232z^6 + 477321z^4 - 11505yz - 134419z^2 + 7670w - 11505x]
```

References

[1] Aldo Brigaglia. Emmy Noether. In Mathematical Lives (pp 43-52). Springer International Publishing, 2011.

[2] B. Buchberger, Ein Algorithmus zum auffinden der basiselemente des restklassenrings nach einem nulldimensionalen polynomideal, Doctoral Thesis, Mathematical Institute, University of Innsbruck, 1965. English translation: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal by M.P. Abramson, *Journal of Symbolic Computation*, **41**(3-4), 475-511 (2006). doi:10.1016/j.jsc.2005.09.007

[3] M. Caboara, J. Perry, Reducing the size and number of linear programs in a dynamic Gröbner basis algorithm, *Applicable Algebra in Engineering, Communication and Computing*, **25**, 99–117(2014). doi: 10.1007/s00200-014-0216-5

[4] D.A. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer International Publishing, 2015.

[5] P. Gritzmann, B. Sturmfels, Minkowski Addition of Polytopes: Computational Complexity and Applications to Gröbner Bases, *SIAM Journal on Discrete Mathematics*, Philadelphia **6**(2), 246-269 (1993). doi:10.1137/0406019

[6] H. Hong, D. Kapur, P. Paule, F. Winkler, Bruno Buchberger —A Life Devoted to Symbolic Computation, *Journal of Symbolic Computation*, **41**(3-4), 255-258 (2006). doi:10.1016/j.jsc.2005.09.005

[7] E.W. Mayr, A.R. Meyer, The complexity of the word problems for commutative semigroups and polynomial ideals, *Advances in Mathematics*, **46**(3), 305-329 (1982) doi: 10.1016/0001-8708(82)90048-2

[8] James Stewart. Partial Derivatives. In *Calculus* (7th ed., pp. 981-988). Brooks/-Cole Publishing, Pacific Grove, CA, 2012.

[9] Q.-N. Tran, A new class of term orders for elimination, *Journal of Symbolic Computation*, **42**(5), 533-548 (2007). doi:10.1016/j.jsc.2006.08.006