Groebner Bases with an Application to Integer Programming

Carolyn Wendler
Senior Exercise

May 17, 2004

0.1 Introduction

The theory of Groebner bases involves a generalization of the theory of polynomials in one variable. They were introduced by Bruno Buchburger in 1965 (Adams x). The significance of Groebner bases lies in the function they provide as computational tools to finding algorithmic solutions to problems in commutative algebra and algebraic geometry. The primary purpose of this paper is to introduce Groebner bases and techniques of working with Groebner bases. To achieve this purpose, the paper will focus on an application of Groebner bases, integer programming, in order to demonstrate how the techniques of Groebner bases work and are applied to solve relevant problems. Linear and Integer programs are a class of optimization problems. There are many real world applications to these problems in many different fields. The general linear programming problem is to either maximize or minimize an objective subject to some constraints. For example, in the telecommunications industry, a provider may need to decide how to supply adequate service to an area of customers while minimizing cost. Or a manufacturer may need to decide how to best allocate resources while maximizing profits. Linear and integer programming are used to help make these decisions. Mathematically, we can use linear programming when the constraints are linear. These types of problems are solvable in polynomial time by using linear algebra (Thomas 119). For a detailed discussion of linear programming methods, see Craig 2003. Integer programs differ from linear programs in that solutions are required to be integral instead of real. It is much more difficult to find integer-only solutions to the problem, and currently, integer programs are not solvable in polynomial time (they are NP-complete) (CLO 1998 363). The techniques of Groebner basis have provided new insight into this problem. These techniques provide rather complicated algorithms for solving integer programs, but they are worth investigating because of the possibility of finding a more efficient solution. This paper will provide the most simple examples that involve few variables with few constraints, yet even these problems involve a good deal of computation. The general integer program is the problem:

Integer Programming Problem *Let* $a_{ij} \in \mathbb{Z}, b_i \in \mathbb{Z}$, *and* $c_j \in \mathbb{R}, i = 1, \ldots, n, j = 1, \ldots, m$; *we wish to find a solution* $(\sigma_1, \sigma_2, \ldots, \sigma_m)$ *in* $\mathbb{N}^m$ *of the system*

$$\begin{aligned} a_{11}\sigma_1 + a_{12}\sigma_2 + \cdots + a_{1m}\sigma_m &= b_1 \\ a_{21}\sigma_1 + a_{22}\sigma_2 + \cdots + a_{2m}\sigma_m &= b_2 \\ &\vdots \\ a_{n1}\sigma_1 + a_{n2}\sigma_2 + \ldots + a_{nm}\sigma_m &= b_n, \end{aligned} \tag{1}$$

which minimizes the "cost function"

$$c(\sigma_1, \sigma_2, \ldots, \sigma_m) = \sum_{j=1}^{m} c_j \sigma_j.$$

(Adams 105)

The main goal of this paper will be to find a method for solving this problem. To do this, we will translate this problem into a problem about polynomials that we can solve using Groebner bases techniques. In dealing with sets of polynomials, we will find that certain sets can be generated by a finite number of polynomials, and in fact can be generated by a Groebner basis. Due to the structure of Groebner bases, this generating set will give us polynomial solutions to our problem. By discovering how we can find the elements of a Groebner basis in a systematic and strategic way, we will solve our main problem.

Chapter 1

Algebra and Geometry: Preliminaries

We will begin with some useful definitions. Polynomials are certainly familiar, but in this paper we will discuss polynomials in n variables $x_1, \ldots, x_n$ with coefficients in an arbitrary field k, which is a generalization of polynomials involving a single variable. First we will define monomials.

Definition 1 *A **monomial** in $x_1, \ldots, x_n$ is a product of the form ${x_1}^{\alpha_1} \cdot {x_2}^{\alpha_2} \ldots {x_n}^{\alpha_n}$, where all of the exponents $\alpha_1, \ldots, \alpha_n$ are nonnegative integers. The **total degree** of this monomial is the sum $\alpha_1 + \cdots + \alpha_n$. We will denote this sum by $\mid \alpha \mid$.*

We will simplify the notation for monomials by letting $\alpha = (\alpha_1, \ldots, \alpha_n)$ be an n-tuple of non-negative integers. Then we write

$$x^\alpha = {x_1}^{\alpha_1} \cdot {x_2}^{\alpha_2} \ldots {x_n}^{\alpha_n}.$$

A polynomial is simply a sum of these monomials with coefficients from our field k.

Definition 2 *A **polynomial** f in $x_1, \ldots, x_n$ with coefficients in a field k is a finite linear combination (with coefficients in k) of monomials. We will write a polynomial f in the form*

$$f = \sum_\alpha a_\alpha x^\alpha, a_\alpha \in k,$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n)$. The set of all polynomials in $x_1, \ldots, x_n$ with coefficients in k is denoted $k[x_1, \ldots, x_n]$.

We will be using the following terminology in our discussion of polynomials:

Definition 3 *Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial in $k[x_1, \ldots, x_n]$.*

1. *We call a_α the **coefficient** of the monomial x^α.*

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

3. *The* ***total degree*** *of f, denoted deg(f), is the maximum $\mid \alpha \mid$ such that the coefficient a_α is nonzero.*

It is clear that, under addition and multiplication, the set of polynomials $k[x_1, \ldots, x_n]$ is a ring. The ring $k[x_1, \ldots, x_n]$ is also commutative under multiplication, and so it is a commutative ring. Thus we call $k[x_1, \ldots, x_n]$ a *polynomial ring.*

Now we will introduce the notion of affine space, within which we will be working.

Definition 4 *Given a field k and a positive integer n, we define the n-dimensional* ***affine space*** *over k to be the set*

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

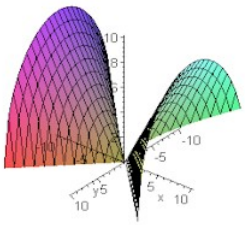
A familiar example of an affine space is the case $k = \mathbb{R}$ and we get the space $\mathbb{R}^n$. To see how polynomials are related to affine space (and thus algebra to geometry), one must regard a polynomial as a function from k^n to k. We can see that the polynomial $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ gives a function

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

We now define a geometric object, based on these ideas.

Definition 5 *Let k be a field, and let $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$. Then we set $V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n : f_i(a_1, \ldots, a_n) = 0$ for all $1 \leq i \leq s\}$. We call $V(f_1, \ldots, f_s)$ the* ***affine variety*** *defined by $f_1, \ldots, f_s$.*

So, an affine variety $\mathbf{V}(f_1, \ldots, f_n) \subset k^n$ is the set of all solutions of the system of equations $f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$. The polynomials $(f_1, \ldots, f_s)$ are said to *vanish* on V. We can picture familiar graphs that are affine varieties, such as circles, ellipses, parabolas, and hyperbolas. The graph of a polynomial function $y = f(x)$ is also the affine variety $V(y - f(x))$. One example of such an affine variety is $V(z^2 + x^2 - y^2)$:



We now define the main algebraic object that will be used in this paper.

Definition 6 *A subset $I \subset k[x_1, \ldots, x_n]$ is an **ideal** if it satisfies:*

1. $0 \in I$.
2. *If $f, g \in I$, then $f + g \in I$.*
3. *If $f \in I$ and $h \in k[x_1, \ldots, x_n]$, then $h \cdot f \in I$. (CLO 29)*

Based on the third property, we say that an ideal *absorbs* elements of the ring under multiplication. So an ideal is an additive subgroup of the ring $k[x_1, \ldots, x_n]$ that absorbs multiplication. The following definition will show that one example of an ideal is the ideal generated by a finite number of polynomials. That is, the group of all polynomial combinations of elements of $k[x_1, \ldots, x_n]$ with a generating set polynomials forms an ideal.

Definition 7 *Let $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$. Then we set*

$$\langle f_1, \ldots, f_s \rangle = \{\sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in k[x_1, \ldots, x_n]\}.$$

*We call $\langle f_1, \ldots, f_s \rangle$ the **ideal generated by** $f_1, \ldots, f_s$. (CLO 29)*

Theorem 1 *Let $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$. Then $\langle f_1, \ldots, f_s \rangle$ is indeed an ideal of $k[x_1, \ldots, x_n]$.*

Proof:
We can see that this is an ideal by showing that the three conditions for an ideal hold for $\langle f_1, \ldots, f_s \rangle$.

1. First we want to show that $0 \in \langle f_1, \ldots, f_s \rangle$. We know $0 \in k[x_1, \ldots, x_n]$, since $k[x_1, \ldots, x_n]$ is a ring. Thus $\sum_{i=1}^{s} 0 \cdot f_i \in \langle f_1, \ldots, f_s \rangle$. Since $0 = \sum_{i=1}^{s} 0 \cdot f_i$, then $0 \in \langle f_1, \ldots, f_s \rangle$.

2. Secondly we need to show that $\langle f_1, \ldots, f_s \rangle$ is closed under addition. Let $f = \sum_{i=1}^{s} p_i f_i \in \langle f_1, \ldots, f_s \rangle$ and $g = \sum_{i=1}^{s} q_i f_i \in \langle f_1, \ldots, f_s \rangle$. Then $f + g = \sum_{i=1}^{s} (p_i + q_i) f_i$. We know that $(p_i + q_i) \in k[x_1, \ldots, x_n]$, since $k[x_1, \ldots, x_n]$ is a ring and thus closed under addition. Therefore, $f + g = \sum_{i=1}^{s} (p_i + q_i) f_i \in \langle f_1, \ldots, f_s \rangle$.

3. Finally, we need to show that $\langle f_1, \ldots, f_s \rangle$ absorbs elements of the ring $k[x_1, \ldots, x_n]$ under multiplication. Let $h \in k[x_1, \ldots, x_n]$ and let $f = \sum_{i=1}^{s} p_i f_i \in \langle f_1, \ldots, f_s \rangle$. Then $h \cdot f = \sum_{i=1}^{s} (h p_i) f_i$. Since $k[x_1, \ldots, x_n]$ is a ring and thus is closed under multiplication, we know that $h p_i \in k[x_1, \ldots, x_n]$. Therefore $h \cdot f = \sum_{i=1}^{s} (h p_i) f_i \in \langle f_1, \ldots, f_s \rangle$ and we are done.
(CLO 29)

∎

The ideals generated by polynomials are computationally important, because an element of the ideal will be a polynomial combination of the basis polynomials. Thus an element of the ideal will have important properties in common with the basis elements, such as common divisors and also will vanish on the same set. We can see this by looking at the following type of ideal, which is constructed using varieties. For an affine variety $V = V(f_1, \ldots, f_s) \subset k^n$ defined by $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, we know that the polynomials $f_1, \ldots, f_s$ vanish on V. But there might be other polynomials that also vanish on V. It turns out that the set of all polynomials vanishing on V is an ideal. Intuitively, this makes sense because any combination of polynomials that vanish on V will also vanish on V.

Definition 8 *Let $V \subset k^n$ be a variety. Define*

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

This ideal is called the ***vanishing ideal of V****.*

We need to show that $I(V)$ is indeed an ideal.

Theorem 2 *Let $V \subset k^n$ be a variety. Then $I(V)$ is an ideal in the ring $k[x_1, \ldots, x_n]$.*

Proof:
To prove that $I(V)$ is an ideal, we need to show that the three conditions for an ideal are met.

1. First we need to show that $0 \in I(V)$, where 0 is the zero polynomial. Since the zero polynomial vanishes on all of k^n, in particular it vanishes on V. Therefore $0 \in I(V)$.

2. Next we need to show that $I(V)$ is closed under addition. Let $f, g \in I(V)$ and let $(a_1, \ldots, a_n)$ be an arbitrary point of V. Then

   $$f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0 + 0 = 0.$$

   Therefore $f + g \in I(V)$.

3. Finally, we need to show that $I(V)$ absorbs elements of the ring $k[x_1, \ldots, x_n]$. Let $f \in I(V)$ and let $h \in k[x_1, \ldots, x_n]$ and pick an arbitrary point $(a_1, \ldots, a_n)$ in V. Then $h(a_1, \ldots, a_n)f(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) \cdot 0 = 0$. So $h \cdot f \in I(V)$, and we are done.

Therefore $I(V)$ is an ideal. ∎

Thus we have had an introduction to ideals and can see why they are interesting algebraic objects. The next chapter will focus on the bases of ideals. In particular, we will prove that every ideal of the ring $k[x_1, \ldots, x_n]$ has a finite basis, and we will introduce a specific type of basis, a Groebner basis for ideals, and will find a method for constructing a finite Groebner basis for every ideal.

Chapter 2

Groebner Bases for Ideals

2.1 Monomial Ideals

As discussed in the previous section, when we are talking about ideals generated by a set of polynomials, an element of these ideals will be a sum of multiples of the basis polynomials. So we can see that in trying to find whether a given polynomial is the element of an ideal, it would be important to discuss whether or not it is divisible by elements of the basis. Divisibility turns out to be an important factor in finding elements of an ideal, as we will see in this chapter, and so one major theme of this chapter will be discussing how we can extend what we know about division of polynomials in one variable to division of polynomials with many (possibly infinitely many) variables. We will begin with a discussion of monomials. Because we are working with multi-variables, it is important to define a way to order monomials according to their degree. This is natural in the one variable case, when we know simply that x^2 has a greater degree than x. In the multi-variable case, however, there are many possible ways of ordering monomials, as long as the ordering meets the following criteria.

Definition 9 *A* ***monomial ordering*** *on* $k[x_1, \ldots, x_n]$ *is any relation* $>$ *on* $\mathbb{Z}^n_{\geq 0}$ *satisfying:*

1. $>$ *is a total (or linear) ordering on* $\mathbb{Z}^n_{\geq 0}$.
2. *If* $\alpha > \beta$ *and* $\gamma \in \mathbb{Z}^n_{\geq 0}$, *then* $\alpha + \gamma > \beta + \gamma$.
3. $>$ *is a well-ordering on* $\mathbb{Z}^n_{\geq 0}$. *This means that every nonempty subset of* $\mathbb{Z}^n_{\geq 0}$ *has a smallest element under* $>$. *(CLO 53)*

Note that we have defined a monomial ordering as an ordering on the n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. We construct a monomial $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ with the n-tuple α as the exponent, and so there is a one-to-one relationship between the

monomials in $k[x_1, \ldots, x_n]$ and $\mathbb{Z}^n_{\geq 0}$. So the ordering $>$ on $\mathbb{Z}^n_{\geq 0}$ gives us an ordering on the monomials in $k[x_1, \ldots, x_n]$. Thus if $\alpha > \beta$, then by the ordering, $x^\alpha > x^\beta$.

Also note that in $\mathbb{Z}^n_{\geq 0}$, addition is done component-wise. So if we have $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n) \in \mathbb{Z}^n_{\geq 0}$, then $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$.

The monomial ordering in the one variable case can also be thought of simply as divisibility. That is, x^2 is greater than x, since x^2 is divisible by x. It is easily seen that divisibility is not a monomial ordering in $k[x_1, \ldots, x_n]$ for $n > 1$. Once we have more than one variable, simple divisibility cannot help us decide in general whether one monomial is greater than another, because, for instance, $x_1 \not\geq x_2$ and $x_2 \not\geq x_1$, and so divisibility does not tell us which monomial is bigger. We must have some way of ordering these variables. A common ordering that is used in $k[x_1, \ldots, x_n]$ is lexicographic ordering, in which the variables are usually ordered simply as $x_1 > x_2 > \cdots > x_n$ or, depending on our notation, alphabetically so that $a > b > \cdots x > y > z$. For lex ordering alone, however, this can be done in $n!$ different ways. So we can see that for $\mathbb{Z}^n$, there are $n!$ different lex orderings. The lexicographic monomial ordering is defined as follows.

Definition 10 ***Lexicographic Order***. *Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{lex} \beta$ if, in the difference $\alpha - \beta \in \mathbb{Z}^n$, the left-most nonzero element is positive. We write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.*

Proposition 1 *The lex ordering $>_{lex}$ is a monomial ordering on $\mathbb{Z}^n_{\geq 0}$.*

Proof:
1. The lex ordering on $\mathbb{Z}^n_{\geq 0}$ is defined based on the numerical values of the components of it elements $(a_1, \ldots, a_n)$. Since numerical ordering is a total ordering on $\mathbb{Z}_{\geq 0}$, it follows directly that $>_{lex}$ is a total ordering.
2. Let $\alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}$ such that $\alpha >_{lex} \gamma$. Then, by definition of lex ordering, the left-most nonzero entry in $\alpha - \beta$ is positive. We now need to order $\alpha + \gamma$ and $\beta + \gamma$. Taking the difference $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$, we see that the left-most nonzero entry is positive. Thus $\alpha + \gamma >_{lex} \beta + \gamma$.
3. To show that $>_{lex}$ is a well-ordering, we will proceed by contradiction. Assume that $<_{lex}$ is not a well-ordering. Then there exists a nonempty subset $S \subset \mathbb{Z}^n_{\geq}$ that has no least element. Let $\alpha_1 \in S$. Then α_1 is not the least elements and so there must exist $\alpha_2 \in S$ such that $\alpha_1 > \alpha_2$. Continuing in this manner, we get an infinite strictly decreasing sequence

$$\alpha_1 >_{lex} \alpha_2 >_{lex} \cdots.$$

By definition of lex ordering, the components in the first entries of these elements form a monotonic decreasing sequence. We know that the numerical order on $\mathbb{Z}_{\geq 0}$ is a well-ordering. So there must be an element α_k for which the first entries of all α_i for $i \geq k$ are equal. Starting with this α_k, the lex ordering, by definition, is determined by the components in the entries after the first one. By the same argument as before,

the sequence of the second entries must have a least element as well. If we continue this argument, we see that there must be some element α_l in the infinite sequence such that all n entries of each vector α_j for $j \geq l$ are equal. Then we have $\alpha_l = \alpha_{l+1}$, by definition of lex ordering. But according to our sequence, $\alpha_l >_{lex} \alpha_{l+1}$. So by contradiction, $>_{lex}$ is a well-ordering. (CLO 55) ∎

Example:

1. $x^2y >_{lex} xy$, since $(2,1) >_{lex} (1,1)$ because $\alpha - \beta = (2,1) - (1,1) = (1,0)$.
2. $xy >_{lex} x$, since $(1,1) >_{lex} (1,0)$ because $\alpha - \beta = (1,1) - (1,0) = (0,1)$.
3. $x^2 >_{lex} xy^2z$, since $(2,0,0) >_{lex} (1,2,1)$ because $\alpha - \beta = (2,0,0) - (1,2,1) = (1,-2,-1)$.

∎

Another example of a monomial ordering is Graded Lexicographic Order, which is based upon the total degree of a monomial. In the case in which the total degrees of two monomials are equal, the tie is broken by using lex order.

Definition 11 ***Graded Lexicographic Order*** *Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say that $\alpha >_{grlex} \beta$ if $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, or $|\alpha| = |\beta|$ and $\alpha >_{lex} \beta$.*

Example:

1. $x^2y >_{grlex} xy$, since $(2,1) >_{grlex} (1,1)$, because $|\alpha| = 3 > 2 = |\beta|$. So these particular monomials are ordered the same as they were under lex ordering.
2. $xy^2z >_{grlex} x^2$, since $(1,2,1) >_{grlex} (2,0,0)$, because $|\alpha| = 4 > 2 = |\beta|$. This is an example of monomials that are ordered differently under graded lex order than lex order.
3. $x^3yz^5 >_{grlex} x^2y^3z^4$, since $(3,1,5) >_{grlex} (2,3,4)$. In this case, $|\alpha| = 9 = |\beta|$, and so we had to revert to lex ordering, under which $\alpha >_{lex} \beta$, because $\alpha - \beta = (3,1,5) - (2,3,4) = (1,-2,1)$.

∎

Another, somewhat less intuitive, monomial ordering is Graded Reverse Lexicographic Order. It works the same as graded lex order, but ties are fixed by, in a sense, a reverse of the lex order. This order turns out to be computationally more efficient when using the algorithms that will be included in this paper.

Definition 12 ***Graded Reverse Lexicographic Order*** *Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say that $\alpha >_{grevlex} \beta$ if $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, or $|\alpha| = |\beta|$, and in $\alpha - \beta \in \mathbb{Z}^n$, the right-most nonzero entry is negative.*

To see that this ordering breaks ties differently than Graded Lex, we will revisit the third pair of monomials in the previous example.

Example:
The pair x^3yz^5 and $x^2y^3z^4$ are ordered differently under Graded Reverse Lex than under Graded Lex or Lex. Under Graded Reverse Lex,

$$x^2y^3z^4 >_{grevlex} x^3yz^5, \text{ since } (2,3,4) >_{grevlex} (3,1,5).$$

In this case, $|\alpha| = 9 = |\beta|$, and so we had to break the tie by taking the difference $\alpha - \beta = (2,3,4) - (3,1,5) = (-1,2,-1)$, and since the right-most nonzero entry is negative, $\alpha >_{grevlex} \beta$. ∎

Now that we have a grasp of monomial orderings, we can return to how these relate to polynomials. We will use the following terms for polynomials under a monomial order:

Definition 13 *Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, \ldots, x_n]$ and let $>$ be a monomial order.*

1. *The **multidegree** of f is*

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

   (the maximum is taken with respect to $>$).

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

$$LC(f) = a_{multideg(f)} \in k.$$

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

$$LM(f) = x^{multideg(f)}$$

   (with coefficient 1).

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

$$LT(f) = LC(f) \cdot LM(f).$$

   (CLO 57)

The following is an illustration of these terms, under Lex Order.

Example:
Let $f = 3x^2y + 4xy \in k[x, y]$ under lex ordering with $x > y$. Then $LC(f) = 3$, $LM(f) = x^2y$, and $LT(f) = 3x^2y$. ∎

Lemma 1 *Let $f, g \in k[x_1, \ldots, x_n]$ be nonzero polynomials. Then:*

1. *$multideg(f \cdot g) = multideg(f) + multideg(g)$.*
2. *If $f + g \neq 0$, then $multideg(f + g) \leq max(multideg(f), multideg(g))$. If, in addition, $multideg(f) \neq multideg(g)$, then equality occurs. (CLO 58)*

Proof:
Let $f = \sum_\alpha a_\alpha x^\alpha$ and $g = \sum_\beta b_\beta x^\beta$ for $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$.
1. We first need to show that $multideg(f \cdot g) = multideg(f) + multideg(g)$.

$$\begin{aligned} f \cdot f &= \sum_\alpha a_\alpha x^\alpha \sum_\beta b_\beta x^\beta \\ &= \sum_\alpha \sum_\beta a_\alpha b_\beta x^\alpha x^\beta \\ &= \sum_\alpha \sum_\beta a_\alpha b_\beta x^{\alpha+\beta}. \end{aligned}$$

Then

$$\begin{aligned} multideg(f \cdot g) &= max(\alpha + \beta \in \mathbb{Z}^n_{\geq 0} : a_\alpha b_\beta \neq 0) \\ &= max(\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0) + max(\beta \in \mathbb{Z}^n_{\geq 0} : a_\beta \neq 0) \\ &= multideg(f) + multideg(g). \end{aligned}$$

2. Assume that $f + g \neq 0$ and that $multideg(f) = multideg(g)$. So $LM(f) = LM(g)$. We need to show that $multideg(f + g) \leq max(multideg(f), multideg(g)$. If $LC(f) + LC(g) = 0$, then the leading terms of f and g cancel and $multideg(f + g) < max(multideg(f), multideg(g)$. If $LC(f) + LC(g) \neq 0$, then $LM(f + g) = LM(f) = LM(g)$.

Assume that $f + g \neq 0$ and that $multideg(f) \neq multideg(g)$. Assume, WLOG, that $multideg(f) > multideg(g)$. Then $LM(f) > LM(g)$ and so $LM(f + g) = LM(f)$. Thus $multideg(f + g) = multideg(f) = max(multideg(f), multideg(g))$. ∎

We are now ready to study the properties of monomial ideals, and we will see formally why divisibility is so important for finding an element of an ideal.

Definition 14 *An ideal $I \subset k[x_1, \ldots, x_n]$ is a **monomial ideal** if there is a subset $A \subset \mathbb{Z}^n_{\geq 0}$ (possibly infinite) such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in k[x_1, \ldots, x_n]$ and $\alpha \in A$. In this case, we write $I = \langle x^\alpha : \alpha \in A \rangle$. (CLO 67)*

It follows directly from the definition of an ideal that a monomial ideal is indeed an ideal.

Example:
An example of a monomial ideal is $I = \langle x^6y^7, x^2y^5, x^5y^3 \rangle \subset k[x, y]$ with corresponding set $A = \{(6, 7), (2, 5), (5, 3)\}$. ∎

So we can see that a monomial ideal I is generated by a set of monomials and the elements of this ideal are polynomials. The following two lemmas describe how we can characterize an element of a monomial ideal, which will later help us to determine whether a given element of the polynomial ring is in an ideal. The first lemma concerns monomials in the ideal.

Lemma 2 *Let $I = \langle x^\alpha : \alpha \in A \rangle$ be a monomial ideal. Then a monomial x^β lies in I if and only if x^β is divisible by x^α for some $\alpha \in A$.*

Proof:

($\Longleftarrow$) Assume x^β is a multiple of x^α for some $\alpha \in A$. From this it follows that $x^\beta \in I$ by the definition of an ideal.

($\Longrightarrow$) Assume $x^\beta \in I$. Then by definition, $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$ where $h_i \in k[x_1, \ldots, x_n]$ and $\alpha(i) \in A$. We can write h_i as a linear combination of monomials, $h_i = a_{p_i}x^{p(i)} + a_{p-1_i}x^{p-1(i)} + \cdots + a_{0_i}$. Then $h_i \cdot x^{\alpha(i)} = a_{p_i}x^{p(i)+\alpha(i)} + a_{p-1}x^{p-1(i)+\alpha(i)} + \cdots + a_{0_i}x^{\alpha(i)}$. So we can see that every term of $\sum_{i=1}^{s} h_i x^{\alpha(i)}$ must be divisible by some $x^{\alpha(i)}$. Since the sum of these terms is the monomial x^β, then each term must be divisible by the same $x^{\alpha(i)}$. Thus x^β must also be divisible by some $x^{\alpha(i)}$. (CLO 67-69) ∎

The next lemma describes how we can characterize a polynomial that is in a given monomial ideal.

Lemma 3 *Let I be a monomial ideal, and let $f \in k[x_1, \ldots, x_n]$. Then the following are equivalent:*

1. *$f \in I$.*
2. *Every term of f lies in I.*
3. *f is a k-linear combination of the monomials in I.*

(CLO 68)

Proof:
We will show that: $3 \Rightarrow 2 \Rightarrow 1 \Rightarrow 3$, and thus prove that the three are equivalent.

($3 \Rightarrow 2$) Assume f is a k-linear combination of the monomials in I. Then every term of f is a multiple of an element of I. So by definition, each term of f is in I. Since I is closed under addition, it follows that the sum of these terms, f, is in I.

($2 \Rightarrow 1$) Assume every term of f lies in I. Then $f \in I$, since I is closed under addition.

($1 \Rightarrow 3$) Let $f \in I$ and assume $I = \langle x^\alpha : \alpha \in A \rangle$. Then by definition, $f = \sum_{i=1}^{s} h_i x^{\alpha(i)}$ where $h_i \in k[x_1, \ldots, x_n]$ and $\alpha(i) \in A$. Let $h_i = a_{0_i} x^{m(i)} + a_{1_i} x^{m-1(i)} + \cdots + a_{m(i)}$. Then $h_i \cdot x^{\alpha(i)} = a_{0_i} x^{m(i)} \cdot x^{\alpha(i)} + a_{1_i} x^{m-1(i)} \cdot x^{\alpha(i)} + \cdots + a_{m(i)} x^{\alpha(i)}$. So the terms of f are linear combinations of monomials $x^{\alpha(i)}$ in I. ∎

Using the previous two lemmas, we can now prove that any monomial ideal has a finite basis, which will be the first step in showing that every ideal has a finite generating set.

Theorem 3 ***Dickson's Lemma*** *A monomial ideal $I = \langle x^\alpha : \alpha \in A \rangle \subset k[x_1, \ldots, x_n]$ can be written down in the form $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, where $\alpha(1), \ldots, \alpha(s) \in A$. In particular, I has a finite basis.*

Proof:
We will prove this Lemma by induction on the number of variables n.

Base Case: Our base case will be $n = 1$. Then I is generated by the monomial x_1^α where $\alpha \in A \subset \mathbb{Z}_{\geq 0}$. We know that $A \subset \mathbb{Z}_{\geq 0}$ has a smallest element β by definition of monomial ordering. So $\beta < \alpha$ for all $\alpha \in A$, and so x_1^β divides all other generators x_1^α. Therefore $I = \langle x_1^\beta \rangle$ by Lemma 2.

Inductive Hypothesis: Assume that $n > 1$ and that the theorem is true for $n - 1$. That is, a monomial ideal $I = \langle x^\alpha : \alpha \in A \rangle \subset k[x_1, \ldots, x_{n-1}]$ can be written down in the form $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, where $\alpha(1), \ldots, \alpha(s) \in A$. Thus if we add a variable y, the monomials in $k[x_1, \ldots, x_{n-1}, y]$ can be written as $x^\alpha y^m$, where $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ and $m \in \mathbb{Z}_{\geq 0}$.

Let $I \subset k[x_1, \ldots, x_{n-1}, y]$ be a monomial ideal, and let J be the monomial ideal in $k[x_1 \ldots, x_{n-1}]$ generated by the monomials x^α for which $x^\alpha y^m \in I$ for some $m \geq 0$. We know that J is in fact an ideal, because the α's for which $x^\alpha y^m \in I$ form a subset $A \subset \mathbb{Z}_{\geq 0}^n$ for which the definition of monomial ideal holds for J. Then by our inductive hypothesis, finitely many of the x^α's generate J, and so we can write $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. Then, by the definition of J, we know that for each i between 1 and s, $x^{\alpha(i)} y^{m_i} \in I$ for some $m_i \geq 0$. Since there is only a finite number of $x^{\alpha(i)}$'s, there is only a finite number of y^{m_i}'s. Let m be the largest of the m_i. Then, for each l between 0 and $m - 1$, consider the ideal $J_l \subset k[x_1, \ldots, x_{n-1}]$ generated by the monomials x^β such that $x^\beta y^l \in I$. That is, J_l is the part of I generated by monomials containing y exactly to the l^{th} power. Again, by our inductive hypothesis, J_l has a finite generating set of monomials, and so we can write, $J_l = \langle x^{\alpha_l(1)}, \ldots, x^{\alpha_l(s_l)} \rangle$.

Claim: I is generated by the following set of monomials:

$$
\begin{array}{llll}
from & J: & x^{\alpha(1)}y^m, \ldots, x^{\alpha(s)}y^m \\
from & J_0: & x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)} \\
from & J_1: & x^{\alpha_1(1)}y, \ldots, x^{\alpha_1(s_1)}y \\
from & J_2: & x^{\alpha_2(1)}y^2, \ldots, x^{\alpha_2(s_2)}y^2 \\
 & \vdots & \\
from & J_{m-1}: & x^{\alpha_{m-1}(1)}y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})}y^{m-1}.
\end{array}
$$

We will prove this claim by showing that the above monomials generate an ideal that has the same elements as I. Let $x^\beta y^p \in I$. Either $p \geq m$ or $p \leq m-1$. We will start with the case where $p \geq m$. We know that J contains all $x^{\alpha(i)}$ such that $x^{\alpha(i)}y^m \in I$. If we divide $x^\beta y^p$ by $y^{p-m} \in I$, we get $x^\beta y^m$, and so we can see that $x^\beta \in J$. Thus $x^\beta y^p$ is divisible by some $x^{\alpha(i)}y^m$ by the construction of J. Therefore, in the case that $p \geq m$, the monomials $x^{\alpha(i)}y^m$ generate elements $x^\beta y^p \in I$.

Our second case is that $p \leq m-1$. By a similar argument, $x^\alpha y^p$ is divisible by some $x^{\beta_p(j)}y^p$ by the construction of J_p. Then it follows from Lemma 2 that the listed monomials generate an ideal having the same monomials as I. It follows directly from part III of Lemma 3 that a monomial ideal is uniquely determined by the monomials it contains. Therefore the ideal generated by the above monomials is the same as I. Thus we have a set of generators for I.

Now we need to show that a finite set of generators can be chosen from this set of generators of the ideal I. To simplify things, we will change our notation by letting $y = x_n$ so that we are again writing the variables $x_1, \ldots, x_n$. So, as we have shown, our monomial ideal is $I = \langle x^\alpha : \alpha \in A \rangle \subset k[x_1, \ldots, x_n]$. We need to show that I is generated by finitely many of the x^α's, where $\alpha \in A$. The above list gave us a finite set of generators for I, since there are s_i monomials on each line for some finite $s_i \in \mathbb{Z}_{\geq 0}$, and there are m lines, for some finite $m \in \mathbb{Z}_{\geq 0}$. We can write this set of generators as $\langle x^{\beta(1)}, \ldots, x^{\beta(t)} \rangle$ for some monomials $x^{\beta(i)} \in I$. Since $I = \langle x^\alpha : \alpha \in A \rangle$, each $x^{\beta(i)}$ is divisible by $x^{\alpha(i)}$ by Lemma 2. Therefore, by replacing each $x^{\beta(i)}$ by $x^{\alpha(i)}$, we get that $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(t)} \rangle$. (CLO 69-70). ∎

The following example will illustrate how the above proof constructs a finite generating set for an ideal.

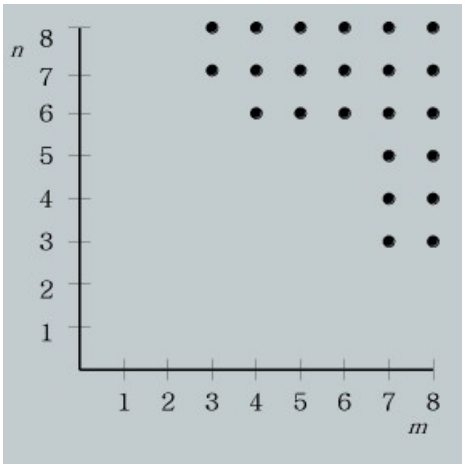
Example:
We will use the steps of the above proof to find a finite generating set for the ideal $I = \langle x^7y^3, x^4y^6, x^3y^7 \rangle \in k[x, y]$ (Note that we already have a finite generating set for the ideal, but it is still a useful example to see how the proof would construct one).

Let J be defined, as above, as a monomial ideal generated by the monomials x^α for which $x^\alpha y^{m_i} \in I$ for some $m_i > 0$. We can see that the largest of these m_i's, for our example, is $m = 7$. Thus we let $J = \langle x^3 \rangle \subset k[x]$; that is, J is generated by the monomials x^α for which $x^\alpha y^7 \in I$. We then construct other monomial ideals, the J_k's from our proof, for each $0 \leq k \leq 6 = m - 1$. And so we get that $J_0 = J_1 = J_2 = \{0\} \subset k[x]$, since no monomials in the generating set, and thus no monomials in I, have a y factor of degree 0, 1, or 2. Next we get, $J_3 = J_4 = J_5 = \langle x^7 \rangle \subset k[x]$, since x^7y^3 is in the generating set of I, and all monomials in I that can be written $x^\alpha y^3$, $x^\alpha y^4$, or $x^\alpha y^5$, for any $\alpha \geq 7$, will be generated by the element x^7y^3 of the generating set. Finally, we get $J_6 = \langle x^4 \rangle \subset k[x]$, since x^4y^6 is in the generating set of I and generates monomials in I that can be written $x^\alpha y^6$. As the proof dictates, we then pick a finite generating set from each of these J_k ideals, which in our case will be the generating monomial for each one. This gives us

$$\begin{array}{rrcl} from & J & : & x^3y^7 \\ from & J_3 & : & x^7y^3 \\ from & J_4 & : & x^7y^4 \\ from & J_5 & : & x^7y^5 \\ from & J_6 & : & x^4y^6. \end{array}$$

This gives us the finite generating set $I = \langle x^3y^7, x^7y^3, x^7y^4, x^7y^5, x^4y^6 \rangle$. ∎

We can also look at an illustration of this example that shows how the theorem works. If for each $x^m y^n$, we plot (m, n) on the first quadrant in the plane:



So we can visualize the ideal $I = \langle x^7y^3, x^4y^6, x^3y^7 \rangle$ by seeing that the elements of the generating set correspond to the corner points on the graph, and each plotted point represents a monomial in I. The ideals J_k are horizontal slices of this area. That is, J from our example includes all points in the area along the line $n = 7$ and up, and we can see that these elements can be generated by x^3y^7, because this is the leftmost corner of this area. J_6 is the area including the points to the right of and on the line $m = 4$ and above and on the line $n = 6$. The others are easily seen as well.

2.2 Division Algorithm for $k[x_1, \ldots, x_n]$

In the previous section, we saw how important division is for determining whether a polynomial is in a given monomial ideal. We will see in the next section that division is used in a similar way to determine whether a polynomial is in any given ideal. In order to do division with monomials in $k[x_1, \ldots, x_n]$, we needed to define a monomial ordering. In the same way, we need to now define a division algorithm for $k[x_1, \ldots, x_n]$ so that we can divide polynomials. To see how we can do this, we will first look at the one variable case in which we have the following algorithm for division.

Theorem 4 ***Division Algorithm for k[x]*** *Let k be a field and let g be a nonzero polynomial in $k[x]$. Then every $f \in k[x]$ can be written as*

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

where $q, r \in k[x]$, and either $r = 0$ or $deg(r) < deg(g)$. Furthermore, q and r are unique, and the following is an algorithm for determining q and r:

Let $g, f \in I$. Start by letting $q_0 = 0$ and $r_0 = f$.
Then, for as long as $r_n \neq 0$ and $LT(g)$ divides $LT(r_n)$, where $n \in \mathbb{N}$, repeat the following:

Let $q_{n+1} = q_n + LT(r_n)/LT(g_n)$ and let $r_{n+1} = r_n - (LT(r_n)/LT(g)) \cdot g$.
If $r_n = 0$ or $LT(g)$ does not divide $LT(r_n)$, then let $r = r_n$ and $q = q_n$,
and the algorithm is complete.

(Adams 26)

We can check that the above values assigned in the algorithm work, by observing that : $f = q \cdot g + r = (q + LT(r)/LT(g)) \cdot g + (R - (LT(r)/LT(g)) \cdot g)$. We will use the following example to demonstrate how this algorithm works:

Example:

Let $f = 3x^4 + 4x^2 + 2x + 1$.
Let $g = x^2 + 3x$.
Then $r_0 = 3x^4 + 4x^2 + 2x + 1$ and $q_0 = 0$.

- Since $LT(g) = x^2$ divides $LT(r_0) = 3x^4$, we let

$$q_1 = q_0 + LT(r_0)/LT(g) = 3x^4/x^2 = 3x^2$$

and

$$\begin{aligned} r_1 = r_0 - (LT(r_0)/LT(g)) \cdot g &= 3x^4 + 4x^2 + 2x + 1 - 3x^2(x^2 + 3x) \\ &= -9x^3 + 4x + 2x + 1. \end{aligned}$$

- Then $LT(g) = x^2$ divides $LT(r_1) = -9x^3$, and so we let

$$q_2 = q_1 + LT(r_1)/LT(g) = 3x^2 + (-9x^3/x^2) = 3x^2 - 9x$$

and

$$\begin{aligned} r_2 = r_1 - (LT(r_1)/LT(g)) \cdot g &= -9x^3 + 4x^2 + 2x + 1 - (-9x^3/x^2)(x^2 + 3x) \\ &= 31x^2 + 2x + 1. \end{aligned}$$

• Then $LT(g) = x^2$ divides $LT(r_2) = 31x^2$, and so we let

$$q_3 = q_2 + LT(r_2)/LT(g) = 3x^2 - 9x + (31x^2/x^2) = 3x^2 - 9x + 31$$

and

$$\begin{aligned} r_3 = r_2 - (LT(r_2)/LT(g)) \cdot g &= 31x^2 + 2x + 1 - (31x^2/x^2)(x^2 + 3x) \\ &= -91x + 1. \end{aligned}$$

• Then $LT(g) = x^2$ does not divide $LT(r_3) = -91x$. And so we get

$$3x^4 + 4x^2 + 2x + 1 = q \cdot (x^2 + 3x) + r = (3x^2 - 9x + 31)(x^2 + 3x) + (-91x + 1).$$

It is easy to see how these steps correspond to how division is usually done:

$$\begin{array}{rl} & \overbrace{}^{q_3} \\ & \overbrace{}^{q_2} \\ & \overbrace{3x^2}^{q_1} -9x +31 \\ x^2 + 3x \overline{)\, 3x^4 + 4x^2 + 2x + 1} & \\ \quad -\underline{(3x^4 + 9x^3)} & \\ \quad -9x^3 + 4x^2 + 2x + 1 & \}r_1 \\ \quad -\underline{(-9x^3 - 27x^2)} & \\ \quad 31x^2 + 2x + 1 & \}r_2 \\ \quad -\underline{(31x^2 + 93x)} & \\ \quad -91x + 1 & \}r_3 \end{array}$$

Thus we can see that the algorithm works, and that it will always terminate in a finite number of steps, since this is true for "normal" division. ∎

We will now construct a division algorithm for $k[x_1, \ldots, x_n]$.

Theorem 5 ***Division Algorithm in*** $k[x_1, \ldots, x_n]$ *We start by fixing a monomial order* $>$ *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*

$$f = a_1 f_1 + \cdots a_s f_s + r,$$

where $a_i, r \in k[x_1, \ldots, x_n]$, and either $r = 0$ or r is a linear combination, with coefficients in k, of monomials, none of which is divisible by any of $LT(f_1), \ldots, LT(f_s)$. We will call r a remainder of f upon division by F.
Furthermore, if $a_i f_i \neq 0$, the we have

$$multideg(f) \geq multideg(a_i f_i).$$

(CLO 62)

To prove the above statement, i.e. the existence of $a_1, \ldots, a_s$ and r, we will give an algorithm for their construction that operates for any given $F = (f_1, \ldots, f_s) \subset k[x_1, \ldots, x_n]$ and $f \in k[x_1, \ldots, x_n]$. Note that, unlike the one variable case in which the quotient and remainder are unique, this division algorithm does not guarantee the uniqueness of $a_1, \ldots, a_s$ and r.

Proof:
Fix a monomial order $>$ on $\mathbb{Z}^n_{\geq 0}$ and let $F = (f_1, \ldots, f_s)$ be an ordered s-tuple of polynomials in $k[x_1, \ldots, x_n]$. Pick $f \in k[x_1, \ldots, x_n]$. Unlike the one-variable case, when we do division in multi-variables, terms are added to the remainder throughout the division process rather than just at the end. So there are two steps to the process. At the start of the algorithm, we set $h = f$ and $r = 0$, and we will keep adding remainder terms to r throughout the algorithm. The first step is that whenever some $LT(f_i)$ divides $LT(h)$, then we divide the monomial h by f_i in the way that occurs in the algorithm for the one-variable case. That is, we begin with a quotient $q_i = 0$. Then we let $q_i = q_i + \frac{LT(h)}{LT(f_i)}$ and $h = h - \frac{LT(h)}{LT(f_i)} \cdot f_i$. Once $LT(h)$ is no longer divisible by any $LT(f_i)$, this step terminates, as in the one-variable case. We then move on to the second step: Whenever $LT(h)$ is not divisible by any $LT(f_i)$, we add $LT(h)$ to the remainder column. That is, we let $r = r + LT(h)$ and $h = h - LT(h)$. We return to the first step once we have moved enough terms of h to the remainder column that $LT(h)$ is divisible by some $LT(f_i)$. We stop this process once we have $p = 0$.

We will now prove that this algorithm works by showing that

$$f = q_1 f_1 + \cdots q_s f_s + h + r \tag{2.1}$$

at every stage of the process. When $h = f$ and $r = 0$, it is clearly true that $f = h + r$. Assume that 2.1 holds for some step k of the algorithm. Then the next step is either a step in which division occurs or a step in which we add a term to the remainder. If division occurs, then $LT(h)$ is divided by some $LT(f_i)$. Then according to our algorithm

$$q_i f_i + h = (q_i + LT(h)/LT(f_i)) \cdot f_i + (h - (LT(h)/LT(f_i)) \cdot f_i)$$

which does not change the sum $q_i f_i + h$. This division step keeps all other terms the same and so 2.1 holds in this case. If, instead, we add a term to the remainder in

this step, then according to our algorithm,

$$h + r = (h - LT(h)) + (r + LT(h))$$

which does not change the sum $h + r$. Thus 2.1 holds in this case as well. The algorithm stops when $h = 0$. At this point,

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

in which, by the steps of the algorithm, no terms of r are divisible by any $LT(f_i)$. Thus, by induction, 2.1 holds in all cases.

Now we need to show that the algorithm terminates. Note that in each step of the algorithm we are always subtracting $LT(h)$ from h. Thus, after every step, the $multideg(h)$ decreases. If the algorithm never terminated, then we would have an infinite decreasing sequence of multidegrees from each step of the algorithm. But this would be a contradiction, since our monomial order $>$ must be a well-ordering by the definition of a monomial order. Thus the set of multidegrees taken for h at each step of the algorithm must have a least element, and since each step gives us a smaller multidegree, $h = 0$ must happen eventually. Thus we will be able to divide, using this algorithm, in a finite number of steps.

Finally, we need to show that if $q_i f_i \neq 0$, then $multideg(f) \geq multideg(q_i f_i)$. By Lemma 1, we know that $multideg(q_i f_i) = multideg(q_i) + multideg(f_i)$. Also, since every term of q_i is equal to $\frac{LT(h)}{LT(f)}$ for some value of h, we know that $multideg(q_i) = multideg(h) - multideg(f)$ for some value of h. So we have $multideg(q_i f_i) = multideg(h) - multideg(f) + multideg(f_i)$. Since $h = f$ at the start of the algorithm and we know that $multideg(h)$ decreases after every step, we know that $multideg(h) \leq multideg(f)$ for all values of h. Similarly, we know from our algorithm that since $q_i f_i \neq 0$, $multideg(f_i) \leq multideg(f)$. Thus

$$\begin{aligned} multideg(q_i f_i) &= multideg(h) - multideg(f) + multideg(f_i) \\ &\leq 2multideg(f) - multideg(f) \\ &= multideg(f). \end{aligned}$$

QED (Adams 28, 31, CLO 62). ∎

The following example will demonstrate this algorithm.

Example:
We will divide $f = x^3y^2 + xy + x + 1$ by $f_1 = x^3 + 1$ and $f_2 = y^2 + 1$ using lex order with $x > y$. Then according to our algorithm, we get the following (since terms are added to the remainder throughout the algorithm's process, we write the remainder column on the right to keep track of the terms that go to the remainder):

$$q_1 : y^2$$

$$
\begin{array}{lcll}
 & q_2: & & \\
x^3+1 & \sqrt{x^3y^2+xy+x+1} & \underline{r} & \\
y^2+1 & & & \\
 & -\underline{(x^3y^2+y^2)} & & \\
 & \underline{xy+x-y^2+1} & \longrightarrow xy+x & \\
 & -y^2+1 & &
\end{array}
$$

After dividing f by the leading term of f_1, we get the polynomial $xy+x-y^2+1$ with no terms that are divisible by the leading term of f_1. Furthermore, the first two terms, xy and x are not divisible by the leading term of f_2, and so these go to the remainder column. We are left with $-y^2+1$ and we divide this by the leading term of f_2.

$$
\begin{array}{lcll}
 & q_1: y^2 & & \\
 & q_2: -1 & & \\
x^3+1 & \sqrt{x^3y^2+xy+x+1} & \underline{r} & \\
y^2+1 & & & \\
 & -\underline{(x^3y^2+y^2)} & & \\
 & \underline{xy+x-y^2+1} & \longrightarrow xy+x & \\
 & -y^2+1 & & \\
 & -\underline{(-y^2-1)} & & \\
 & 2 & \longrightarrow xy+x+2 &
\end{array}
$$

After dividing by the leading term of f_2, we get the 2, and so this term is sent to the remainder column and we have a total remainder of $xy+x+2$. Thus we obtain

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

∎

This generalization of the division algorithm fails to be as efficient as the one variable division algorithm. The remainders are not guaranteed to be unique; they depend on the ordering of the s-tuple of polynomials $F=(f_1,\ldots,f_s)$. The following is a simple example demonstrating that remainders are not uniquely determined. In the example, F has two elements, and the remainder of the polynomial we pick, upon division by F, is shown to be different depending on the order of the two elements of F.

Example:
Let $f_1 = x^2y-2x, f_2 = y^3+4 \in k[x,y]$. We will use lex order with $x>y$.

Let $f = x^2y^3 - 2xy^2 \in k[x, y]$.
Our first case will be $F = (f_1, f_2)$.
Then

$$\begin{array}{rr} & y^2 \\ x^2y - 2x & \sqrt{x^2y^3 - 2xy^2} \\ y^3 + 4 & \\ & \underline{-(x^2y^3 - 2xy^2)} \\ & 0 \end{array}$$

So $x^2y^3 - 2xy^2 = y^2 \cdot (x^2y - 2x) + 0 \cdot (y^3 + 4) + 0$.

In our second case, we will let $F = (f_2, f_1)$.
Then

$$\begin{array}{rr} & x^2 \\ y^3 + 4 & \sqrt{x^2y^3 - 2xy^2} \\ x^2y - 2x & \\ & \underline{-(x^2y^3 + 4x^2)} \\ & -2xy^2 - 4x^2 \end{array}$$

So $x^2y^3 - 2xy^2 = x^2 \cdot (y^3 + 4) + 0 \cdot (x^2y - 2x) - 2xy^2 - 4x^2$.
So we can see that the two cases produced two different remainders, 0 and $-2xy^2-4x^2$, respectively, due to a switch in the order of the polynomials in F. ∎

In the first case, the remainder of 0 told us that f was in the ideal $\langle f_1, f_2 \rangle$ by Lemma 2. But if we had only looked at the second case, we would not have known that f was in $\langle f_1, f_2 \rangle$. Thus, for an ideal $I = \langle f_1, \ldots, f_n \rangle$, we know that a polynomial $f \in k[x_1, \ldots, x_n]$ is in the ideal if the remainder of f upon division by I is zero, but this is not a *necessary* condition for ideal membership. Our goal is to establish such a necessary condition.

2.3 Groebner Bases

Now that we have proven that a monomial ideal has a finite generating set of monomials, we will use this fact to show that *every* ideal has a finite generating set. To do this, we will introduce a monomial ideal that is generated by the leading terms of each polynomial in the ideal. Once we have a monomial ordering, each $f \in k[x_1, \ldots, x_n]$ has a unique leading term denoted $LT(f)$ and these leading terms generate a monomial ideal.

Definition 15 *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal other than 0.*

1. *We denote by LT(I) the set of leading terms of elements of I. Thus,*

$$LT(I) = \{cx^\alpha : \textit{there exists } f \in I \textit{ with } LT(f) = cx^\alpha\}.$$

2. *We denote by $\langle LT(I)\rangle$ the ideal generated by the elements of $LT(I)$.*

Note that if we are given a finite generating set for I, say $I = \langle f_1, \ldots, f_s\rangle$, then $\langle LT(f_1), \ldots, LT(f_s)\rangle$ and $\langle LT(I)\rangle$ may be different ideals. The following example illustrates this.

Example:
Consider $I = \langle x^2 + 1, xy\rangle$ with $<$ as a lex ordering with $x > y$.
Then $LT(x^2 + 1) = x^2$ and $LT(xy) = xy$. So, $\langle LT(x^2 + 1), LT(xy)\rangle = \langle x^2, xy\rangle$.
Since, $y(x^2 + 1) - x(xy) = y$, we know $y \in I$ and so $LT(y) \in \langle LT(I)\rangle$.
However, $LT(y) = y \notin \langle x^2, xy\rangle$.
Therefore $\langle LT(I)\rangle \neq \langle LT(x^2 + 1), LT(xy)\rangle$. ∎

Even though $\langle LT(f_1), \ldots, LT(f_s)\rangle$ and $\langle LT(I)\rangle$ may be different ideals, the next theorem will show that there is a set of polynomials in the ideal I for which they are the same.

Proposition 2 *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal.*

1. *$\langle LT(I)\rangle$ is a monomial ideal.*

2. *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:
Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. We will show that the above two conditions hold.

1. We know that the leading monomials $LM(g)$ of elements $g \in I \setminus \{0\}$ generate the monomial ideal $\langle LM(g) : g \in I \setminus \{0\}\rangle$. Let $x^{\alpha(i)} \in \langle LM(g) : g \in I \setminus \{0\}\rangle$ be the leading monomial of g_i and $a_{\alpha_i} \in k$ be the leading coefficient of g_i. Then $a_{\alpha_i} \cdot x^{\alpha(i)} \in \langle LM(g) : g \in I \setminus \{0\}\rangle$. Now start with $a_{\alpha_j} g_j \in \langle LT(g) : g \in I \setminus \{0\}\rangle$. Then $a_{\alpha_j}^{-1} \in k$, since k is a field. So $a_{\alpha_j}^{-1} \cdot a_{\alpha_j} g_j = g_j \in \langle LM(g) : g \in I \setminus \{0\}\rangle$. Thus $\langle LM(g) : g \in I \setminus \{0\}\rangle = \langle LT(g) : g \in I \setminus \{0\}\rangle = \langle LT(I)\rangle$. Therefore $\langle LT(I)\rangle$ is a monomial ideal.

2. By Dickson's Lemma, we know that the monomial ideal
$\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$ for finitely many $g_1, \ldots, g_s \in I$.
(CLO 73-74).

∎

We will now complete this series of theorems by proving that *every* polynomial ideal has a finite generating set. The set of monomials $g_1, \ldots, g_s$ in the above theorem such that $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$ are in fact a finite generating set for the ideal I. We will fix a monomial ordering and use the division algorithm defined for polynomials in $k[x_1, \ldots, x_n]$.

Theorem 6 ***(Hilbert Basis Theorem)*** *Every ideal $I \subset k[x_1, \ldots, x_n]$ has a finite generating set. That is, $I = \langle g_1, \ldots, g_t \rangle$ for some $g_1, \ldots, g_t \in I$.*

Proof:
If $I = 0$, then our generating set is 0, and we are done. If I contains some nonzero polynomial, then by Proposition 1, there are $g_1, \ldots, g_t \in I$ such that $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$.

Show: $I = \langle g_1, \ldots, g_t \rangle$.

($\supseteq$) We know that $\langle g_1, \ldots, g_t \rangle \subset I$, since each $g_i \in I$.

($\subseteq$) Let $f \in I$ be any polynomial. If we divide f by $\langle g_1, \ldots, g_t \rangle$ (using the division algorithm), then we get an expression of the form

$$f = a_1 g_1 + \cdots + a_t g_t + r$$

where every term in r is not divisible by any $LT(g_i), \ldots, LT(g_t)$. We need to show that $r = 0$. Note that

$$r = f - a_1 g_1 - \cdots - a_t g_t \in I.$$

So, since $r \in I$, then $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Then by Lemma 2, $LT(r)$ must be divisible by some $LT(g_i)$. But, unless $r = 0$, this contradicts what it means for r to be a remainder by the division algorithm. Thus,

$$f = a_1 g_1 + \cdots + a_t g_t + 0 \in \langle g_1, \ldots, g_t \rangle,$$

and so $f \in I$. Therefore $I \subset \langle g_1, \ldots, g_t \rangle$. (CLO 1997 74). ∎

As a consequence of the Hilbert Basis theorem, we have an important geometric result. We can now describe the set of zeros of an ideal I as the set of zeros common to finitely many polynomials. We introduced varieties as the sets of solutions to a finite set of polynomial equations, and now, even though every nonzero ideal $I \subset k[x_1, \ldots, x_n]$ contains infinitely many polynomials, it makes sense to talk about the affine variety defined by that ideal.

Definition 16 *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. We will denote by $V(I)$ the set*

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

The following is a proof that this set $V(I)$ is indeed an affine variety.

Proposition 3 *$V(I)$ is an affine variety. In particular, if $I = \langle f_1, \ldots, f_s \rangle$, then $V(I) = V(f_1, \ldots, f_s)$.*

Proof:
By the Hilbert Basis Theorem, $I = \langle f_1, \ldots, f_s \rangle$ for a finite set of polynomials $f_1, \ldots, f_s \in I$.
Claim: $V(I) = V(f_1, \ldots, f_s)$.

($\subseteq$) Let $(a_1, \ldots, a_n) \in V(I)$. Let $f_i \in I$ be a generating polynomial of I. Then, since $f(a_1, \ldots, a_n) = 0$ for all $f \in I$, $f_i(a_1, \ldots, a_n) = 0$. So $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$. Thus $V(I) \subset V(f_1, \ldots, f_s)$.
($\supseteq$) Let $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$ and let $f \in I$. Since $I = \langle f_1, \ldots, f_s \rangle$, we can write

$$f = \sum_{i=1}^{s} h_i f_i$$

for some $h_i \in k[x_1, \ldots, x_n]$. Thus

$$\begin{aligned} f(a_1, \ldots, a_n) &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) \\ &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) \cdot 0 = 0. \end{aligned}$$

So $V(f_1, \ldots, f_s) \subset V(I)$. Therefore $V(f_1, \ldots, f_s) = V(I)$. (CLO 77) ∎

We chose the basis $\{g_1, \ldots, g_t\}$ in the Hilbert Basis theorem so that it had the property $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Yet we saw in our example above that this property does not hold for all bases. Every ideal, however, has such a basis, and it is known as a Groebner basis. We will see in the next section that Groebner bases are very useful algebraic tools, and we will see how they can solve our question of determining whether an element of $k[x_1, \ldots, x_n]$ is in a given ideal.

Definition 17 *Fix a monomial order. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal I is said to be a* ***Groebner basis*** *if*

$$\langle LT(g_1), \ldots, LT(g_t) \rangle = \langle LT(I) \rangle.$$

Corollary 1 *Fix a monomial order $>$ on $k[x_1, \ldots, x_n]$, and let $I \subset k[x_1, \ldots, x_n]$ be an ideal. Then I has a Groebner basis. Furthermore, any Groebner basis of I is a basis of I.*

Proof:
Let I be a nonzero ideal. Then the set $G = \{g_1, \ldots, g_t\}$ constructed in the proof of Theorem 6 is a Groebner basis by definition, and therefore every ideal has a Groebner basis. Then for a Groebner basis G, $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$ and so $I = \langle g_1, \ldots, g_t \rangle$ by the proof of Theorem 6. Therefore G is a basis for I. ∎

2.4 Properties of Groebner Bases

Groebner bases yield some very useful algebraic results. In this paper, we have been discussing what is known as the Ideal Membership Problem, that is, finding a way to

determine whether a given polynomial is an element of an ideal. This can be done with Groebner basis due to the important fact that the remainder of a polynomial in $k[x_1, \ldots, x_n]$ on division by a Groebner basis is unique. That is, when a polynomial is reduced by the elements of a Groebner basis of an ideal, the remainder is unique, no matter what the order of the elements of G when using the division algorithm. If we let $G = \{g_1, \ldots, g_t\}$ be a Groebner basis, then the remainder of f on division by G will be denoted

$$r = \overline{f}^G.$$

Proposition 4 *If $G = \{g_1, \ldots, g_t\}$ is a Groebner basis for I and $f \in k[x_1, \ldots, x_n]$, then $f \in I$ if and only if the remainder of f on division by $g_1, \ldots, g_t$ is zero. (Cox 7)*

The following is a partial proof that will be completed by the next result.

Proof:
($\Leftarrow$) If $f \in I$, then we know that f can be written as a combination of $g_1, \ldots, g_t$. So we can see that there must be some way to divide f by G that gives us a remainder of zero, but on the other hand, as we have seen, if we divide any way that we please we might not get a zero remainder...
($\Rightarrow$) If $f \in I$, then the remainder of f on division by $g_1, \ldots, g_t$ is zero, as we saw in the proof of Theorem 6. ∎

So the above proposition tells us when an element of a ring is an element of a given ideal, by using the a Groebner basis for the ideal. But this is only useful when we know that the zero remainder upon division by a Groebner basis is unique. Since we have developed a division algorithm for $k[x_1, \ldots, x_n]$, we can now use this division algorithm to prove the following crucial property about Groebner bases.

Proposition 5 *If $G = \{g_1, \ldots, g_t\}$ is a Groebner basis for I and $f \in k[x_1, \ldots, x_n]$, then f can be written uniquely in the form*

$$f = g + r$$

where $g \in I$ and no term of r is divisible by any $LT(g_i)$.

Proof:
Let $G = \{g_1, \ldots, g_t\}$ be a Groebner basis for an ideal $I \subset k[x_1, \ldots, x_n]$ and let $f \in k[x_1, \ldots, x_n]$. Then by the division algorithm, we get $f = a_1g_1 + \cdots + a_tg_t + r$, where $a_i \in k[x_1, \ldots, x_n]$ and no term of r is divisible by any $LT(g_i)$. Thus $a_1g_1 + \cdots + a_tg_t \in I$, since G is a basis for I. This proves the existence of r satisfying the conditions of the proposition, and now it remains to show that r is unique.

Suppose $f = g_1 + r_1 = g_2 + r_2$, satisfying the conditions of Proposition 3. Then $r_1 - r_2 = g_2 - g_1 \in I$. If $r_1 - r_2 \neq 0$, then $LT(r_1 - r_2) \in \langle LT(I) \rangle$. Since, by

definition of a Groebner basis, $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$, then $LT(r_1 - r_2)$ is divisible by some $LT(g_i)$ by Lemma 2. But no term of r_1 or r_2 is divisible by any $LT(g_1, \ldots, g_t)$. Thus it is not possible that $LT(r_1 - r_2) \neq 0$. So $r_1 = r_2$, and we have proved uniqueness of the remainder of a polynomial upon division by a Groebner basis. (CLO 79) ∎

So what we have shown is that remainders of f upon division by G are unique, no matter what order we put the elements of G when we divide f by them. That is, if $G = \{g_1, \ldots, g_n\}$, we can divide f by $\{g_1, \ldots, g_n\}$ or $\{g_n, \ldots, g_1\}$ or any other order you would like and still get the same remainder in the end. Therefore we have found our necessary condition for ideal membership (to restate Proposition 2): for an ideal $I \subset k[x_1, \ldots, x_n]$ and a Groebner basis G of I, a polynomial $f \in k[x_1, \ldots, x_n]$ is in I if and only if the remainder of f upon division by G is zero. This test for ideal membership is useless unless we have a Groebner basis for our ideal. In the following section we will establish a criteria for determining whether a given basis is a Groebner basis and thereby gain an algorithm for constructing a Groebner basis from any given basis for an ideal.

2.5 Computing a Groebner Basis

The definition of a Groebner basis alone does not give us a way of determining whether a given basis of an ideal I is a Groebner basis or not, unless we were to check every leading term of the elements of I to see if $LT(g_i)$ for some $g_i \in G$ divides it, but we have no real way of doing this. If a generating set $\{f_1, \ldots, f_n\}$ of an ideal I is not a Groebner basis, then there must be a leading term in $\langle LT(I)\rangle$ that is not in $\langle LT(f_1), \ldots, LT(f_n)\rangle$. For this to happen, there would have to be a polynomial combination in which the leading terms of the elements of the basis cancel, leaving only smaller terms, the greatest of which is less than any of the leading terms of the basis. But this combination would be in the ideal, and so the smaller leading term would be in $\langle I\rangle$, but not in $\langle LT(f_1), \ldots, LT(f_n)\rangle$. The following definitions will help us to address these cancellations:

Definition 18 *Let $f, g \in k[x_1, \ldots, x_n]$ be nonzero polynomials.*

1. *If $multideg(f) = \alpha$ and $multideg(g) = \beta$, then let $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = max(\alpha_i, \beta_i)$ for each $1 \leq i \leq n$. We call x^γ the **least common multiple** of $LM(f)$ and $LM(g)$, written $x^\gamma = LCM(LM(f), LM(g))$.*

2. *The **S-polynomial** of f and g is the combination*

$$S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g.$$

Example:
Let $f_1 = x^4y + x^2y + x$ and $f_2 = x^2y^2 - y^2 \in k[x, y]$. So $multideg(f_1) = (4, 1)$ and $multideg(f_2) = (2, 2)$. Then using lex order with $x > y$, we get $\gamma = (4, 2)$. So $x^\gamma = x^4y^2$ and x^γ is the LCM of x^4y and x^2y^2. Computing the S-polynomial of f_1 and f_2 then gives us

$$\begin{aligned} S(f_1, f_2) &= (x^4y^2)/(x^4y) \cdot f_1 - (x^4y^2)/(x^2y^2) \cdot f_2 \\ &= y \cdot f_1 - x^2 \cdot f_2 \\ &= y(x^4y - x^2y + x) - x^2(x^2y^2 - y^2) \\ &= x^4y^2 - x^2y^2 + xy - x^4y^2 + x^2y^2 \\ &= xy \in \langle f_1, f_2 \rangle. \end{aligned}$$

So we get the polynomial xy, which is a linear combination of f_1 and f_2 with elements of $k[x, y]$, and thus $xy \in \langle f_1, f_2 \rangle$ by definition of an ideal. Note that since $LT(xy)$ is divisible neither by $LT(f_1) = x^4y$ or $LT(f_2) = x^2y^2$, then we know that, by definition, $\{f_1, f_2\}$ is <u>not</u> a Groebner basis of $\langle f_1, f_2 \rangle$. ∎

So we can see that these S-polynomials are designed to produce cancellation of leading terms. In fact, every cancellation of leading terms among polynomials of the same multidegree results from an S-polynomial type of cancellation, as will be proven by the following lemma. Using this knowledge, we will be able to establish a criterion for testing whether a generating set of an ideal is a Groebner basis.

Lemma 4 *Suppose we have a sum $f = \sum_{i=1}^s c_i f_i$, where $c_i \in k$ and $multideg(f_i) = \delta \in \mathbb{Z}_{\geq 0}^n$ for all i. If $multideg(f = \sum_{i=1}^s c_i f_i) < \delta$, then $f = \sum_{i=1}^s c_i f_i$ is a linear combination, with coefficients in k, of the S-polynomials $S(f_j, f_l)$ for $1 \leq j, l \leq s$. Furthermore, each $S(f_i, f_l)$ has multidegree $< \delta$.*

Proof:
Assume that we have a sum $\sum_{i=1} c_i f_i$ where $c_i \in k$ and $multideg(f_i) = \delta \in \mathbb{Z}\,{}_{\geq 0}^{n}$ for all i. Write $f_i = a_i x^\delta +$ lower terms, where $a_i = LC(f_i)$. Then $c_i a_i$ is the leading coefficient of $c_i f_i$.
Since each $c_i f_i$ has multidegree δ and their sum has a strictly smaller multidegree, then it follows from the hypothesis that $\sum_{i=1}^s c_i a_i = 0$, since all the leading terms must cancel in order for the sum to have a lesser degree than δ. Thus each $S(f_i, f_j)$ has multidegree $< \delta$, because cancellation of the leading terms must occur. Also, by definition, $S(f_i, f_j) = \frac{1}{a_i} f_i - \frac{1}{a_j} f_j$, since $multideg(f_i) = multideg(f_j) = \delta$. Thus we have

$$\begin{aligned} f &= c_1 f_1 + \cdots + c_s f_s \\ &= c_1 a_1 (\frac{1}{a_1} f_1) + \cdots + c_s a_s (\frac{1}{a_s}). \end{aligned}$$

Then we can form the following telescoping sum:

$$\begin{aligned} f &= c_1a_1(\frac{1}{a_1}f_1 - \frac{1}{a_2}f_2) + (c_1a_1 + c_2a_2)(\frac{1}{a_2}f_2 - \frac{1}{a_3}f_3) + \cdots \\ &\quad +(c_1a_1 + \cdots + c_{s-1}a_{s-1})(\frac{1}{a_{s-1}}f_{s-1} - \frac{1}{a_s}f_s) + (c_1a_1 + \cdots + c_sa_s)\frac{1}{a_s}f_s \\ &= c_1a_1S(f_1, f_2) + (c_1a_1 + c_2a_2)S(f_2, f_3) + (c_1a_1 + \cdots + c_{s-1}a_{s-1})S(f_{s-1}, f_s) + \cdots \\ &\quad +(c_1a_1 + \cdots + c_sa_s)\frac{1}{a_s}f_s, \end{aligned}$$

since $S(f_i, f_j) = \frac{1}{a_i}f_i - \frac{1}{a_j}f_j$.
Then we can eliminate the last term:

$$\begin{aligned} f &= c_1a_1S(f_1, f_2) + (c_1a_1 + c_2a_2)S(f_2, f_3) + \cdots \\ &\quad +(c_1a_1 + \cdots + c_{s-1}a_{s-1})S(f_{s-1}, f_s), \end{aligned}$$

since $c_1a_1 + \cdots c_sa_s = 0$.
Therefore f is a linear combination, with coefficients in k, of the S-polynomials $S(f_j, f_l)$ for $1 \leq j, l \leq s$. (Adams 41) ∎

We can use S-polynomials in this way to tell if a set of generators is a Groebner basis, according to the following criterion. As we have already discussed, for G to be a Groebner basis of an ideal I, all polynomial combinations of the basis elements must have leading terms that are generated by leading terms of the basis elements. Since we have proven that all cancellations of leading terms are created by S-polynomials, then it is sufficient to test these polynomials to see if they have leading terms that are generated by elements of the basis, which is exactly what the following criterion does.

Theorem 7 ***Buchberger's S-Pair Criterion*** *A basis $\{g_1, \ldots, g_t\} \subset I$ is a Groebner basis of I if and only if for all pairs $i < j$, we have*

$$\overline{S(g_i, g_j)}^G = 0.$$

Proof:
($\Rightarrow$) If $G = \{g_1, \ldots, g_t\}$ is a Groebner basis for $I = \langle g_1, \ldots, g_t\rangle$, then $S(g_i, g_j) \in I$. Then we know by Proposition 2 that $\overline{S(g_i, g_j)}^G = 0$ for all $i \neq j$. This completes the proof of this direction.

($\Leftarrow$) Assume $\overline{S(g_i, g_j)}^G = 0$ for all $i \neq j$.

Let $f \in I$ be a nonzero polynomial. By definition of Groebner basis, we need to show the following:

Show: $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$.

Let

$$f = \sum_{i=1}^{t} h_i g_i. \tag{2.2}$$

Define $\delta = max_{1\leq i\leq t}\{multideg(h_i g_i)\}$. There are possibly quite a few ways that f can be written as 2.2, that is, there are quite a few ways that f can be written as a linear combination of the g_i's. For each such expression, we get a possibly different δ. Since monomial order is a well-ordering (for every nonempty set there is a minimal element on $<$), we can select an expression 2.2 for f such that δ is minimal. So we will let 2.2 be the linear combination of g_i's so that $\delta = max_{1\leq i\leq t}\{multideg(h_i g_i)\}$ is minimal.

Now either $multideg(f) = \delta$ or $multideg(f) < \delta$. If $multideg(f) = \delta$, then $LT(f)$ is divisible by $LT(g_i)$. Thus $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$, and we are done.

Now we will assume that $multideg(f) < \delta$, and using the fact that δ is minimal, we will come up with a contradiction. That is, we will find another $\sum_{i=1}^{t} h_i g_i$ expression for f with a smaller δ, and this will be a contradiction.
Let $m(i) = multideg(h_i g_i)$.
Then, by isolating the terms with multidegree δ, we get

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} LT(h_i) g_i \qquad (2.3) \\ &\quad + \underbrace{\sum_{m(i)=\delta} (h_i - LT(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i}_{m(i)<\delta} \qquad (2.4) \end{aligned}$$

We can see that the terms on the right all have multidegree $< \delta$, since we split the leading terms of the h_i's away from the rest of the equation. Then, since we have assumed that $multideg(f) < \delta$, we know that $\sum_{m(i)} LT(h_i) g_i$ must have multidegree less than δ.
Let $LT(h_i) = c_i x^{\alpha(i)}$.
Then $\sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ has the form of the equation of Lemma 4, since $m(i) = \delta$ for each term, and the sum has multidegree less than δ. Thus, by Lemma 4, the $\sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ is a linear combination of the S-polynomials $S(x^{\alpha(j)} g_j, x^{\alpha(l)} g_l)$.
By definition of S-polynomial,

$$\begin{aligned} S(x^{\alpha(i)} g_j, x^{\alpha(l)} g_l) &= \frac{x^\delta}{x^{\alpha(j)} LT(g_j)} x^{\alpha(j)} g_j - \frac{x^\delta}{x^{\alpha(l)} LT(g_l)} x^{\alpha(l)} g_l \\ &= \frac{x^\delta}{LT(g_j)} g_j - \frac{x^\delta}{LT(g_l)} g_l. \end{aligned}$$

To simplify, let $x^{\gamma_{jl}} = LCM(LM(g_j), LM(g_l))$.
So

$$\begin{aligned}\frac{x^\delta}{LT(g_j)}g_j - \frac{x^\delta}{LT(g_l)}g_l &= \frac{x^{\delta-\gamma_{jl}}\cdot x^{\gamma_{jl}}}{LT(g_j)}g_j - \frac{x^{\delta-\gamma_{jl}}\cdot x^{\gamma_{jl}}}{LT(g_l)}g_l \\ &= x^{\delta-\gamma_{jl}}S(g_j,g_l).\end{aligned}$$

Therefore we have the following equation, where there are constants $c_{jl} \in k$ such that

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{j,l} c_{jl}x^{\delta-\gamma_{jl}}S(g_j,g_l). \tag{2.5}$$

By our assumption, $\overline{S(g_j,g_l)}^G = 0$. Thus, by the division algorithm, we can write $S(g_j,g_l)$ as a linear combination of elements of G:

$$S(g_j,g_l) = \sum_{i=1}^{t} a_{ijl}g_i,$$

where $a_{ijl} \in k[x_1,\ldots,x_n]$.
Also by the division algorithm,

$$multideg(a_{ijl}g_i) \leq multideg(S(g_j,g_l))$$

for all i,j,l.
So, we can write:

$$x^{\delta-\gamma_{jl}}S(g_j,g_l) = \sum_{i=1}^{t} b_{ijl}g_i, \tag{2.6}$$

where $b_{ijl} = x^{\delta-\gamma_{jl}}a_{ijl}$.
Then, by our second conclusion from the division algorithm, we know that

$$multideg(b_{ijl},g_i) \leq multideg(x^{\delta-\gamma_{jl}}S(g_j,g_l))$$

and

$$multideg(x^{\delta-\gamma_{jl}}S(g_j,g_l)) < \delta \tag{2.7}$$

by Lemma 5, since each $S(g_i,g_l)$ has multidegree $< \delta$.
If we substitute 2.6 into 2.5, we get the equation:

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{j,l} c_{jl}x^{\delta-\gamma_{jl}}S(g_j,g_l) = \sum_{j,l} c_{jl}(\sum_i b_{ijl}g_i) = \sum_i \tilde{h_i}g_i$$

where $multideg(\tilde{h_i}g_i) < \delta$ by 2.7.
Then if we substitute $\sum_{m(i)=\delta} LT(h_i)g_i = \sum_i \tilde{h_i}g_i$ back into equation 2.4, we get that all terms in that sum have multidegree $< \delta$. Therefore we have obtained an expression for f that is a polynomial combination of the g_i's where all terms have multidegree

$< \delta$. Thus δ is not minimal, and we we have a contradiction. So $multideg(f) = \delta$, and as we have already shown in our first case, this gives us $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$ and we are done. (CLO 82-84 and Adams 41-42) ∎

We can see that this Criterion not only detects Groebner bases but also suggests a way to construct a Groebner basis from a basis F that does not fit the Criterion: add the nonzero remainder $\overline{S(f_i, f_j)}^F$ to the set F and test it again (Cox 8). The following example will show how this method works.

Example:
Let $F = \{f_1, f_2\} = \{x^4y - x^2y, x^2y^2 - y^2\}$. We already know, from the previous example, that $\overline{S(f_1, f_2)}^F = xy = f_3$. So set $F_1 = \{f_1, f_2, f_3\} = \{x^4y - x^2y, x^2y^2 - y^2, xy\}$. Then compute:

$$\begin{aligned} \bullet S(f_1, f_2) &= xy \\ &= 0 \cdot f_1 + 0 \cdot f_2 + 1 \cdot f_3 + 0. \end{aligned}$$

Thus $\overline{S(f_1, f_2)}^{F_1} = 0$.

$$\begin{aligned} \bullet S(f_1, f_3) &= \frac{x^4y}{x^4y} \cdot f_1 - \frac{x^4y}{xy} \cdot f_3 \\ &= f_1 - x^3 \cdot f_3 \\ &= x^4y - x^2y - x^4y \\ &= -x^2y. \end{aligned}$$

Since $-x^2y$ is not divisible by $LT(f_1)$ or $LT(f_2)$, we divide $-x^2y$ by f_3:

$$\begin{array}{rl} & -x \\ xy & \sqrt{-x^2y} \\ & \underline{-(-x^2y)} \\ & 0 \end{array}$$

Thus $\overline{S(f_1, f_3)}^{F_1} = 0$.

$$\begin{aligned} \bullet S(f_2, f_3) &= \frac{x^2y^2}{x^2y^2} \cdot f_2 - \frac{x^2y^2}{xy} \cdot f_3 \\ &= 1 \cdot (x^2y^2 - y^2) - (xy) \cdot (xy) \\ &= x^2y^2 - y^2 - x^2y^2 \\ &= -y^2. \end{aligned}$$

Since $-y^2$ is not divisible by $LT(f_1), LT(f_2)$, or $LT(f_3)$, $\overline{S(f_2,f_3)}^{F_1} = -y^2 = f_4$.
Adding these two nonzero remainders to F_1, gives

$$F_2 = \{f_1, f_2, f_3, f_4\} = \{x^4y - x^2y + x, x^2y^2 - y^2, xy, -y^2\}.$$

This time $\overline{S(f_i,f_j)}^{F_2} = 0 \ \forall \ i \neq j$.
So the Groebner basis of $\langle x^3 - 2xy, x^2y - x - 2y^2\rangle$ for lex order with $x > y$ is

$$F_2 = \{f_1, f_2, f_3, f_4\} = \{x^4y - x^2y + x, x^2y^2 - y^2, xy, -y^2\}.$$

∎

The above example shows how the following algorithm for computing a Groebner basis works. As ideals are generally defined by their generating sets, this algorithm gives a method for constructing a Groebner basis for any given ideal. It will be proven that the algorithm holds for all polynomials rings and bases in general.

Theorem 8 ***Buchberger's Algorithm*** *Given $f_1, \ldots, f_s \subset k[x_1, \ldots, x_n]$, consider the algorithm which starts with $F = f_1, \ldots, f_s$ and then repeats the two steps:*

1. *(Compute Step) Compute $\overline{S(f_i,f_j)}^{G}$ for all $f_i, f_j \in F$ with $i < j$.*
2. *(Augment Step) Augment F by adding the nonzero $\overline{S(f_i,f_j)}^{F}$.*

until the Compute Step gives only zero remainders. This algorithm always terminates (in a finite number of steps) and the final value of F is a Groebner basis of $\langle f_1, \ldots, f_s\rangle$. (Cox 8)

If the reader is interested, a more precise version of the algorithm is given in CLO 87 or Adams 43.

Theorem 9 *Given $F = \{f_1, \ldots, f_s\}$ with $f_i \neq 0$ $(1 \leq i \leq s)$, Buchberger's Algorithm will produce a Groebner basis for the ideal $I = \langle f_1, \ldots, f_s\rangle$.*

Proof:
First we need to show that the algorithm terminates in a finite number of steps. We will proceed by contradiction by assuming that the algorithm does not terminate. Then, as the algorithm progresses, we keep constructing sets F_i strictly larger than F_{i-1} and obtain a strictly increasing infinite sequence

$$F_1 \subset F_2 \subset F_3 \subset \cdots.$$

Each F_i is obtained from F_{i-1} by adding some $h \in I$ to F_{i-1}, where $h = \overline{S(f_i,f_j)}^{F_{i-1}} \neq 0$ for some elements $f_i, f_j \in F_{i-1}$. Since h is reduced with respect to F_{i-1}, we have

that $LT(h) \notin LT(F_{i-1})$. Yet $LT(h) \in LT(F_i)$. Thus we get the following strictly ascending chain of ideals

$$\langle LT(F_1)\rangle \subset \langle LT(F_2\rangle \subset \langle LT(F_3)\rangle \subset \cdots.$$

This contradicts the Ascending Chain Condition (see Appendix). Therefore the algorithm must terminate and $\langle LT(F_{i-1})\rangle = \langle LT(F_i)\rangle$ for some i.

Now we need to show that the final value of F, which we will call F' is a Groebner basis of $I = \langle f_1, \ldots, f_s\rangle$. We first need to show that $F' \subset I$. Since $F \subset I$, then p, q and hence $S(p, q)$ are in I, and thus every $\overline{S(p,q)}^F$ is in I. Thus when we enlarge F, we enlarge it by elements of I and so $F' \subset I$.

Furthermore, since $F = \langle f_1, \ldots f_s\rangle \subseteq F''$, we know that F' is a basis for I. Moreover, if $f_i, f_j \in F'$, then $\overline{S(g_i, g_j)}^{F'} = 0$ by construction. Therefore, F' is a Groebner basis for I by Buchberger's S-Pair Criterion. (CLO 88, Adams 42). ∎

Buchberger's algorithm is crucial in the computations using Groebner bases. There are more efficient versions of this algorithm for computing a Groebner basis, which cut down on computation time, and these are presented in CLO 2.9, if the reader is interested. Furthermore, the Groebner bases computed by the algorithm given in Theorem 8, often have more generators than necessary. Since we are using these generators in solving the integer programming problem, we can cut down on computation time by eliminating the extra ones, according to the following fact.

Lemma 5 *Let G be a Groebner basis for the polynomial ideal I. Let $p \in G$ be a polynomial such that $LT(p) \in \langle LT(G - p)\rangle$. Then $G - p$ is also a Groebner basis for I.*

Proof:
Since G is a Groebner basis of I, $\langle LT(G)\rangle = \langle LT(I)\rangle$. If $\langle LT(P)\rangle \in \langle LT(G - p)\rangle$, then $LT(G - p) = LT(G)$. Therefore $G - p$ is also a Groebner basis for I. (CLO 89) ∎

By removing unneeded generators from a Groebner basis and multiplying by constants so that all of the leading coefficients are 1, a *unique* reduced Groebner basis can be obtained for any ideal.

Definition 19 *A **reduced Groebner basis** for a polynomial ideal I is a Groebner basis G for I such that:*

1. *LC(p) = 1 for all $p \in G$.*
2. *For all $p \in G$, no monomial of p lies in $\langle LT(G - p)\rangle$.*

This result is especially useful when working with complicated integer programming problems or other applications using Groebner bases. For the purposes of this paper, we will only be looking at simple examples that can be done by hand, and so a proof of the above result will not be included here. If the reader is interested, there is a discussion of this result in CLO 2.7.

Chapter 3

Elimination Theory

We will now return to our main problem of solving a system of equations, and we will see how Groebner bases will give us a method for doing this involving n variables. There are two steps that allow us to solve a system of equations. The first is that we can *eliminate* variables by manipulating the equations, allowing us to find simpler equations with fewer variables. The second is that we can *extend* the solutions of these simpler equations back into our original equations. These steps are called the Elimination Step and the Extension Step, respectively. Elimination theory involves generalizing these steps. The Elimination Step can be generalized as follows:

Definition 20 *Given $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$, the lth* ***elimination ideal*** *I_l is the ideal of $k[x_{l+1}, \ldots, x_n]$ defined by*

$$I_l = I \cap k[x_{l+1}, \ldots, x_n].$$

So the elements of I_l are all the equations that follow from $f_1 = \cdots = f_s = 0$ and eliminate the variables $x_1, \ldots, x_l$. We can easily see that I_l is indeed an ideal of $k[x_{l+1}, \ldots, x_n]$:

Proposition 6 *The lth elimination ideal I_l, defined above, is an ideal of $k[x_{l+1}, \ldots, x_n]$.*

Proof:
Let I be an ideal and let $I_l = I \cap k[x_{l+1}, \ldots, x_n]$. Then $0 \in I_l$, because $0 \in I$ and $0 \in k[x_{l+1}, \ldots, x_n]$. I_l is closed under addition, since I and $k[x_{l+1}, \ldots, x_n]$ are closed under addition, and the sum of any two polynomials with variables $x_{l+1}, \ldots, x_n$ must be a polynomial with these variables. It only remains to show that I_l absorbs elements of the ring $k[x_{l+1}, \ldots, x_n]$ under multiplication. Pick $f \in I_l$ and $g \in k[x_{l+1}, \ldots, x_n]$. Then $f \in I$ and so $f \cdot g \in I$. Also $f \cdot g \in k[x_{l+1}, \ldots, x_n]$ and so $f \cdot g \in I_l$. Therefore I_l is an ideal. ∎

One of the goals of elimination theory is to give a systematic procedure for finding elements (preferably generators) of each I_l. It turns out that we can find bases of

all these ideals by using Groebner bases with lex ordering (Cox 10). The following result will show that given an ideal I, elements of the Groebner basis of the ideal that involve only the variables $x_{l+1}, \ldots, x_n$ form the Groebner basis of the lth elimination ideal I_l.

Theorem 10 *If $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$ is an ideal and $G = \{g_1, \ldots, g_t\}$ is a Groebner basis for I for lex order with $x_1 > \cdots > x_n$, then for each $0 \leq l \leq n$, the set*

$$G_l = G \cap k[x_{l+1}, x_{l+2}, \ldots, x_n]$$

is a Groebner basis for the elimination ideal

$$I_l = I \cap k[x_{l+1}, x_l, \ldots, x_n].$$

Proof:
Since $G \subset I$, we know $G_l \subset I_l$. Let $f \in I_l$. We need to show that $LT(f)$ is divisible by $LT(g)$ for some $g \in G_l$. By definition of I_l, we know that $f \in I$ and thus $LT(f)$ is divisible by $LT(g)$ for some $g \in G$, since G is a Groebner basis of I. Since $f \in I_l$, its leading term $LT(f)$ involves only the variables $x_{l+1}, \ldots, x_n$. So the same must be true for $LT(g)$. Note that since we are using lex ordering with $x_1 > x_2 > \cdots > x_n$, any monomial involving $x_1, \ldots, x_l$ is greater than all monomials in $k[x_{l+1}, \ldots, x_n]$. It follows that $LT(g) \in k[x_{l+1}, \ldots, x_n]$ implies that $g \in k[x_{l+1}, \ldots, x_n]$. Thus $g \in G \cap k[x_{l+1}, \ldots, x_n] = G_l$. So we have shown that any $f \in I_l = I \cap k[x_{l+1}, \ldots, x_n]$ is divisible by $LT(g)$ for some $g \in G_l = G \cap k[x_{l+1}, \ldots, x_n]$. Therefore, G_l is a Groebner basis of I_l by definition of Groebner basis. (CLO 113-114 and Cox 10). ∎

More efficient monomial orders can be used other than lex ordering if we are solving a problem for which we want to eliminate *certain* variables. Rather than eliminating the first variable x_1, and then eliminating x_2, and so on, there are quicker methods that take less computing time. We can establish an elimination order in which we order the variables according to how we want to eliminate them, and we will create such orders in the next section.

The elimination theorem gives us partial solutions of the original system that we need to extend to a complete solution (if there is one). If we transfer this problem to geometry, as before, we can talk about affine varieties in relation to the problem of finding solutions to a system of equations. Recall that an ideal $I \subset k[x_1, \ldots, x_n]$, yields an affine variety

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

The elimination theorem allows us to describe points of $V(I)$ by building them up one coordinate at a time. If we pick the lth coordinate, then we can find the elimination ideal I_l. Then a solution $(a_{l+1}, \ldots, a_n) \in V(I_l)$ is a partial solution to our original

system of equations. To extend this solution in $V(I_l)$ to a complete solution in $V(I)$, we need to find a_l so that $(a_l, a_{l+1}, \ldots, a_n)$ lies in the variety $V(I_{l-1})$ of the next elimination ideal (CLO 114). The Extension Theorem gives a way to determine whether a partial solution $(a_l, \ldots, a_n) \in V(I_l)$ can be extended in such a way to a solution $(a_{l-1}, \ldots, a_n) \in V(I)$. We include the Extension Theorem below, without proof, for the sake of completion and because it is an interesting result. We will not be using this result in this paper and the proof of the theorem is beyond the scope of this paper. If the reader is interested, a discussion of the extension theorem can be found in CLO 3.1 with the complete proof in CLO 3.6.

Theorem 11 ***(The Extension Theorem)*** *Let $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$ and let I_1 be the first elimination ideal of I. For each $1 \leq i \leq s$, write f_i in the form*

$$f_i = g_i(x_2, \ldots, x_n)x_1^{N_i} + \text{ terms in which } x_1 \text{ has degree} < N_i,$$

where $N_i \geq 0$ and $g_i \in \mathbb{C}[x_2, \ldots, x_n]$ is nonzero. Suppose that we have a partial solution $(a_2, \ldots, a_n) \in V(I_1)$. If $(a_2, \ldots, a_n) \notin V(g_1, \ldots, g_s)$, then there exists $a_1 \in \mathbb{C}$ such that $(a_1, a_2, \ldots, a_n) \in V(I)$ (CLO 115).

Note the Extension Theorem is defined over the field $\mathbb{C}$ and it is false in $\mathbb{R}$.

Chapter 4

Integer Programming

Recall that the integer programming problem can be defined as follows:

Integer Programming Problem *Let $a_{ij} \in \mathbb{Z}, b_i \in \mathbb{Z}$, and $c_j \in \mathbb{R}$, $i = 1, \ldots, n$, $j = 1, \ldots, m$; we wish to find a solution $(\sigma_1, \sigma_2, \ldots, \sigma_m)$ in $\mathbb{N}^m$ of the system*

$$\begin{aligned} a_{11}\sigma_1 + a_{12}\sigma_2 + \cdots + a_{1m}\sigma_m &= b_1 \\ a_{21}\sigma_1 + a_{22}\sigma_2 + \cdots + a_{2m}\sigma_m &= b_2 \\ &\cdot \\ &\cdot \\ &\cdot \\ a_{n1}\sigma_1 + a_{n2}\sigma_2 + \ldots + a_{nm}\sigma_m &= b_n, \end{aligned} \tag{4.1}$$

which minimizes the "cost function"

$$c(\sigma_1, \sigma_2, \ldots, \sigma_m) = \sum_{j=1}^{m} c_j \sigma_j.$$

(Adams 105)

Our strategy for solving the integer programming problem will first be to transfer it into a problem about polynomials. Then we can use the tools we gained from Chapter 2 to compute the Groebner basis and the methods from Elimination Theory in Chapter 3 to find a solution to the problem. We will then transfer this solution back into a solution of the integer programming problem.

First, we transfer this problem into a problem about polynomials by assigning a variable to each linear equation in 4.1. We will let these variables be $x_1, x_2, \ldots, x_n$ for the n equations of 4.1. Then, we can represent any equation of 4.1 as the following:

$$x_i^{a_{i1}\sigma_1 + \cdots + a_{im}\sigma_m} = x_i^{b_i},$$

for $i = 1, \ldots, n$ in which we form a monomial equation by letting the ith equation of the system be the exponent of a variable x_i. But we are looking for a solution to the

entire system, and so we must use each of these equations to form a single equation that represents the system. The product of all the monomials $x_i^{a_{i1}\sigma_1+\cdots+a_{im}\sigma_m}$ set equal to the product of all the monomials $x_i^{b_i}$'s will be a single monomial equation that represents the system. So we can write 4.1 as

$$x_1^{a_{11}\sigma_1+\cdots+a_{1m}\sigma_m}\cdots x_n^{a_{n1}\sigma_1+\cdots+a_{mn}\sigma_m} = x_1^{b_1}\cdots x_n^{b_n}.$$

By grouping the factors with exponents that are multiples of σ_i together, we get

$$(x_1^{a_{11}}x_2^{a_{21}}\cdots x_n^{a_{n1}})^{\sigma_1}\cdots(x_1^{a_{1m}}x_2^{a_{2m}}\cdots x_n^{a_{nm}})^{\sigma_m} = x_1^{b_1}\cdots x_n^{b_n}.$$

Then, to find the solutions, we form a polynomial map $\varphi : k[y_1,\ldots,y_m] \mapsto k[x_1,\ldots,x_n]$ such that $\varphi(y_i) = x_1^{a_{1j}}\cdots x_n^{a_{nj}}$, according to the following definition:

Definition 21 *A **polynomial map***

$$\varphi : k[y_1,\ldots,y_m] \mapsto k[x_1,\ldots,x_n]$$

is a homomorphism between polynomial rings $k[y_1,\ldots,y_m]$ and $k[x_1,\ldots,x_n]$ (see Appendix), which is a k-vector space linear transformation.

Note that a polynomial map is uniquely determined by $\varphi : y_i \mapsto f_i$, where $f_i \in k[x_1,\ldots,x_n], 1 \le i \le m$. That is, a polynomial map is uniquely determined by where it sends each variable y_i. So if $h \in k[y_1,\ldots,y_m]$ such that $h = \sum_v c_v y_1^{v_1}\cdots y_m^{v_m}$, where $c_v \in k, v = (v_1,\ldots,v_m) \in \mathbb{Z}_{\ge 0}^m$, and only finitely many c_v's are non-zero, then we have

$$\varphi(h) = \sum_v c_v y_1^{v_1}\cdots y_m^{v_m} = \sum_v c_v f_1^{v_1}\cdots f_m^{v_m} = h(f_1,\ldots,f_m) \in k[x_1,\ldots,x_n].$$

That is, $\varphi(h)$ depends entirely on the way the variables y_i from $k[y_1,\ldots,y_m]$ are assigned to polynomials f_i in $k[x_1,\ldots,x_n]$. With the necessary language in place, we are now ready to explain how to find a solution to the system.

Lemma 6 *Assume all a_{ij}'s and b_i's are non-negative. Then there exists a solution $(\sigma_1,\sigma_2,\ldots,\sigma_m) \in \mathbb{Z}_{\ge 0}^m$ of 4.1 if and only if the monomial $x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$ is in the image under φ of a monomial in $k[y_1,\ldots,y_m]$.*
Moreover, if $x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n} = \varphi(y_1^{\sigma_1}y_2^{\sigma_2}\cdots y_m^{\sigma_m})$, then $(\sigma_1,\sigma_2,\ldots,\sigma_m) \in \mathbb{Z}_{\ge 0}^m$ is a solution to 4.1.

Proof:
We will do both directions of this proof at once by assuming that there exists a solution $(\sigma_1,\sigma_2,\ldots,\sigma_m) \in \mathbb{Z}_{\ge 0}^m$ of 4.1 and showing this is an equivalent to the statement that the monomial $x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$ is in the image under φ of a monomial in $k[y_1,\ldots,y_m]$.

Assume there exists a solution $(\sigma_1, \sigma_2, \ldots, \sigma_m) \in \mathbb{Z}_{\geq 0}^m$ of 4.1. As we have shown, this means that

$$(x_1^{a_{11}} x_2^{a_{21}} \cdots x_n^{a_{n1}})^{\sigma_1} \cdots (x_1^{a_{1m}} x_2^{a_{2m}} \cdots x_n^{a_{nm}})^{\sigma_m} = x_1^{b_1} \cdots x_n^{b_n}.$$

And so, according to our map, it is equivalent to say that

$$(\varphi(y_1))^{\sigma_1} \cdots (\varphi(y_m))^{\sigma_m} = x_1^{b_1} \cdots x_n^{b_n}.$$

Then, by definition of homomorphism (and φ is a homomorphism) the following is equivalent to the above statement.

$$\varphi(y_1^{\sigma_1} \cdots y_m^{\sigma_m}) = x_1^{b_1} \cdots x_n^{b_n}.$$

Therefore the monomial $x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$ is in the image under φ of a monomial in $k[y_1, \ldots, y_m]$, and we have shown that this is equivalent to $(\sigma_1, \sigma_2, \ldots, \sigma_m) \in \mathbb{Z}_{\geq 0}^m$ being a solution to 4.1.
(Adams 106). ∎

Now we know from this lemma that to find a solution to our system, we are looking for a monomial $y^\sigma = y_1^{\sigma_1} \cdots y_m^{\sigma_m}$ st $\varphi(y^\sigma) = x^b$. Or, equivalently, if we have $x^b \in Im(\varphi)$, we need to find y^σ. That is, our next goal is to find a method for determining whether an element of $k[x_1, \ldots, x_n]$ is in the image of a polynomial map such as φ. To do this, we will begin by studying the structure of the image of φ.

The image of φ is defined as $Im(\varphi) = \{f \in k[x_1, \ldots, x_n] |$ there exists $h \in k[y_1, \ldots, y_m]$ with $f = \varphi(h)\}$. By definition of a ring homomorphism, we know that the image of φ is a sub-ring of $k[x_1, \ldots, x_n]$, since it is closed under addition and multiplication, additive inverses exist in $Im(\varphi)$, and all other properties of a ring are inherited from $k[x_1, \ldots, x_n]$ (see Appendix; these properties are easily seen from the definition of a ring homomorphism). We will denote $Im(\varphi) = k[f_1, \ldots, f_m]$, since by definition, all polynomials in $Im(\varphi)$ are linear combinations of the polynomials f_i.

Also recall from algebra the definition of the kernel of φ,

$$ker(\varphi) = \{h \in k[y_1, \ldots, y_m] | \varphi(h) = 0\}.$$

We know from algebra (and it is easily seen) that $ker(\varphi)$ is an ideal of $k[y_1, \ldots, y_m]$, using the definition of ring homomorphism. Then by the First Isomorphism Theorem (see Appendix), we know that

$$Im(\varphi) \cong k[y_1, \ldots, y_m]/ker(\varphi).$$

by a mapping

$$\phi : k[y_1, \ldots, y_m]/ker(\varphi) \mapsto k[f_1, ..., f_m]$$

defined by

$$g + ker(\varphi) \mapsto \varphi(g).$$

Theorem 12 *$\phi : k[y_1, \ldots, y_m]/ker(\varphi) \to k[f_1, ..., f_m]$ defined by $g + ker(\varphi) \mapsto \varphi(g)$ is a polynomial map. (Adams 80).*

Proof:
We need to show that ϕ is a homomorphism between rings. We already know that $k[f_1, \ldots, f_m]$ is a ring, and we know from algebra that $k[y_1, \ldots, y_m]/ker(\varphi)$ is a ring. So we need to show that ϕ is a ring homomorphism to complete the proof.

Let $g_1 + ker(\varphi), g_2 + ker(\varphi) \in k[y_1, \ldots, y_m]/ker(\varphi)$. First we need to show that addition is preserved. So we calculate

$$\begin{aligned} \phi(g_1 + ker(\varphi) + g_2 + ker(\varphi)) &= \phi(g_1 + g_2 + ker(\varphi)) \\ &= \varphi(g_1 + g_2) \\ &= \varphi(g_1) + \varphi(g_2) \\ &= \phi(g_1 + ker(\varphi)) + \phi(g_2 + ker(\varphi)), \end{aligned}$$

since φ is a ring homomorphism. Next we need to show that the zero element is mapped to zero.

$$\phi(0 + ker(\varphi)) = \phi(ker(\varphi)) = 0.$$

Finally, we need to show that multiplication is preserved.

$$\begin{aligned} \phi((g_1 + ker(\varphi))(g_2 + ker(\varphi))) &= \phi(g_1 g_2 + ker(\varphi)) \\ &= \varphi(g_1 g_2) \\ &= \varphi(g_1)\varphi(g_2) \\ &= (\phi(g_1 + ker(\varphi))(\phi(g_2) + ker(\varphi)), \end{aligned}$$

since φ is a ring homomorphism. ∎

So we can see how crucial the $ker(\varphi)$ is to the structure of the image of φ. We will now find a way to construct, through elimination theory, a Groebner basis of $ker(\varphi)$ and this will give us an algorithm for determining whether a polynomial f is in the image of φ, which is our goal.

First, we need the following technical lemma.

Lemma 7 *Let $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ be elements of a commutative ring R. Then the element $a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_n^{\alpha_n} - b_1^{\alpha_1} b_2^{\alpha_2} \cdots b_n^{\alpha_n}$, where $\alpha_i \in \mathbb{Z}_{\geq 0}$, is in the ideal $\langle a_1 - b_1, a_2 - b_2, \ldots, a_n - b_n \rangle$. (Adams 80)*

Proof:
This proof will be done by induction on the number of variables n.
Base Case: Let $n = 1$. Then for $a_1, b_1 \in R$, $a_1^{\alpha_1} - b_1^{\alpha_1} = (a_1 - b_1)(a_1^{\alpha-1} + a_1^{\alpha-2} b_1 + \cdots + a_1 b_1^{\alpha-2} + b_1^{\alpha-1}) \in \langle a_1 - b_1 \rangle$. (This is easily checked by dividing $a_1^{\alpha} - b_1^{\alpha}$ by $a_1 - b_1$.) For purposes of clarity, we will show the next case $n = 2$, so that it is easier to see how

our inductive step works later.
For $a_1, a_2, b_1, b_2 \in R$,

$$a_1^{\alpha_1}a_2^{\alpha_2} - b_1^{\alpha_1}b_2^{\alpha_2} = a_2^{\alpha_2}(a_1^{\alpha_1} - b_1^{\alpha_1}) + b_1^{\alpha_1}(a_2^{\alpha_2} - b_2^{\alpha_2}).$$

Then, by our first case, $(a_1^{\alpha_1} - b_1^{\alpha_1})$ is a multiple of $(a_1 - b_1)$ and $(a_2^{\alpha_2} - b_2^{\alpha_2})$ is a multiple of $(a_2 - b_2)$. Thus $a_2^{\alpha_2}(a_1^{\alpha_1} - b_1^{\alpha_1}) + b_1^{\alpha_1}(a_2^{\alpha_2} - b_2^{\alpha_2}) \in \langle a_1 - b_1, a_2 - b_2\rangle$ by the definition of an ideal.

Inductive Hypothesis: Assume for $n \leq k$ and $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in R$ that $a_1^{\alpha_1}a_2^{\alpha_2}\cdots a_n^{\alpha_n} - b_1^{\alpha_1}b_2^{\alpha_2}\cdots b_n^{\alpha_n}$ in in the ideal $\langle a_1 - b_1, a_2 - b_2, \ldots, a_n - b_n\rangle$.
Now we need to show that $a_1^{\alpha_k}a_2^{\alpha_2}\cdots a_{k+1}^{\alpha_{k+1}} - b_1^{\alpha_1}b_2^{\alpha_2}\cdots b_{k+1}^{\alpha_{k+1}}$ is in the ideal $\langle a_1 - b_1, a_2 - b_2, \ldots, a_{k+1} - b_{k+1}\rangle$.
Note that

$$a_1^{\alpha_1}a_2^{\alpha_2}\cdots a_{k+1}^{\alpha_{k+1}} - b_1^{\alpha_1}b_1^{\alpha_1}\cdots b_{k+1}^{\alpha_{k+1}} = a_{k+1}^{\alpha_{k+1}}(a_1^{\alpha_1}\cdots a_k^{\alpha_k} - b_1^{\alpha_1}\cdots b_k^{\alpha_k}) + b_1^{\alpha_1}\cdots b_k^{\alpha_k}(a_{k+1}^{\alpha_{k+1}} - b_{k+1}^{\alpha_{k+1}}).$$

Then we know from our hypothesis that

$$a_{k+1}^{\alpha_{k+1}}(a_1^{\alpha_1}\cdots a_k^{\alpha_k} - b_1^{\alpha_1}\cdots b_k^{\alpha_k}) \in \langle a_1 - b_1, a_2 - b_2, \ldots, a_k - b_k\rangle.$$

Also

$$b_1^{\alpha_1}\cdots b_k^{\alpha_k}(a_{k+1}^{\alpha_{k+1}} - b_{k+1}^{\alpha_{k+1}}) \in \langle a_{k+1} - b_{k+1}\rangle.$$

Therefore

$$a_{k+1}^{\alpha_{k+1}}(a_1^{\alpha_1}\cdots a_k^{\alpha_k} - b_1^{\alpha_1}\cdots b_k^{\alpha_k}) + b_1^{\alpha_1}\cdots b_k^{\alpha_k}(a_{k+1}^{\alpha_{k+1}} - b_{k+1}^{\alpha_{k+1}}) \in \langle a_1 - b_1, a_2 - b_2, \ldots, a_{k+1} - b_{k+1}\rangle.$$

Therefore, by induction, the lemma is true for any n. (Hint from Adams 81). ∎

Now we are able to find elements of $ker(\varphi)$ in the following way.

Theorem 13 *Let* $K = \langle y_1 - f_1, \ldots, y_m - f_m\rangle \subseteq k[y_1, \ldots, y_m, x_1, \ldots, x_n]$, *for* $f_i \in k[x_1, \ldots, x_n]$.
Then $ker(\varphi) = K \cap k[y_1, \ldots, y_m]$.

Proof:
($\supseteq$) Let $g \in K \cap k[y_1, \ldots, y_m]$. Then we can write

$$g(y_1, \ldots, y_m) = \sum_{i=1}^{m}(y_i - f_i(x_1, \ldots, x_n))h_i(y_1, \ldots, y_m, x_1, \ldots, x_n),$$

where $h_i \in k[y_1, \ldots, y_m, x_1, \ldots, x_n]$. We know that $\varphi(g)$ maps $y_i \mapsto f_i$. By construction, we can see that when we evaluate g at $(f_1, \ldots, f_m)$, we get

$$\varphi(g) = \sum_{i=1}^{m}(f_i(x_1, \ldots, x_n) - f_i(x_1, \ldots, x_n))(h_i(y_1, \ldots, y_m, x_1, \ldots, x_n)) = 0.$$

Thus $g \in ker(\varphi)$.
($\subseteq$) Let $g \in ker(\varphi)$. Then since, $g \in k[y_1, \ldots, y_m]$, we let

$$g = \sum_v c_v y^v,$$

where $c_v \in k$, $v = (v_1, \ldots, v_m)$, and finitely many c_v's are nonzero. Then, since $g(f_1, \ldots, f_m) = 0$,

$$\begin{aligned} g &= g - g(f_1, \ldots, f_m) \\ &= \sum_v c_v y_1^{v_1} \cdots y_m^{v_m} - \sum_v c_v f_1^{v_1} \cdots f_m^{v_m} \\ &= \sum_v c_v (y_1^{v_1} \cdots y_m^{v_m} - f_1^{v_1} \cdots f_m^{v_m}). \end{aligned}$$

By Lemma 7, each term in the above sum is in the ideal $K = \langle y_1 - f_1, \ldots, y_m - f_m \rangle$, and therefore $g \in K \cap k[y_1, \ldots, y_m]$. QED.
(Adams 80-81) ∎

We can now have a way to find elements in the kernel of φ, by computing a Groebner basis for $ker(\varphi)$ in the following way. First, by Buchberger's algorithm, we can compute a Groebner basis G for the ideal $K = \langle y_1 - f_1, \ldots y_m - f_m \rangle$ in $k[y_1, \ldots, y_m, x_1, \ldots, x_n]$ with respect to a lex ordering with $x_1 > x_2 > \cdots > y_1 > \cdots > y_m$. Then a Groebner basis for $K \cap k[y_1, \ldots, y_m]$ will be precisely the polynomials of the Groebner basis G of K that do not have any x variables, by the Elimination Theorem. The following example illustrates this process.

Example:
Let $\phi : Q[a, b, c] \to Q[x, y]$ be the map defined by

$$\begin{aligned} a &\longmapsto x^2 y \\ b &\longmapsto xy \\ c &\longmapsto y^3 \end{aligned}$$

We first compute a Groebner basis for the ideal $K = \langle a - x^2 y, b - xy, c - y^3 \rangle \subseteq Q[a, b, c, x, y]$ with respect to lex term ordering on the x, y variables with $x > y$ and revlex ordering on the a, b, c variables with $a > b > c$ and with an elimination order in which the x, y variables are larger than the a, b, c variables.

$$\begin{aligned} \bullet S(a - x^2 y, b - xy) &= \frac{x^2 y}{-x^2 y}(-x^2 y + a) - \frac{x^2 y}{-xy}(-xy + b) \\ &= xb - a. \end{aligned}$$

$$\begin{aligned} \bullet S(a - x^2 y, c - y^3) &= \frac{x^2 y^3}{-x^2 y}(-x^2 y + a) - \frac{x^2 y^3}{-y^3}(-y^3 + c) \\ &= x^2 c - a y^2. \end{aligned}$$

$$\begin{aligned} \bullet S(b-xy, c-y^3) &= \frac{xy^3}{-xy}(-xy+b) - \frac{xy^3}{-y^3}(-y^3+c) \\ &= xc - by^2. \end{aligned}$$

Thus $F_1 = \{a - x^2y, b - xy, c - y^3, xb - a, x^2c - ay^2, xc - by^2\}$.
Then we compute the S-polynomials:

$$\begin{aligned} \bullet S(a-x^2y, xc-by^2) &= \frac{x^2y^2b}{-x^2y}(-x^2y+a) - \frac{x^2y^2b}{-by^2}(xc-by^2) \\ &= x^3c - yab. \end{aligned}$$

Then $\overline{x^3c - yab}^{F_1} = 0$.

$$\begin{aligned} \bullet S(b-xy, x^2c-ay^2) &= \frac{x^2yc}{-xy}(-xy+b) - \frac{x^2yc}{x^2c}(x^2c-ay^2) \\ &= -xbc + ay^3. \end{aligned}$$

Then $\overline{-xbc + ay^3}^{F_1} = -b^2y^2 - ac$.

$$\begin{aligned} \bullet S(b-xy, c-y^3) &= \frac{xy^3}{-xy}(-xy+b) - \frac{xy^3}{-y^3}(-y^3+c) \\ &= xc - by^2. \end{aligned}$$

Then $\overline{-xbc + y^3a}^{F_1} = -ac + a + c$.
Therefore we have a Groebner basis for $K = \langle a-x^2y, b-xy, c-y^3\rangle$, $G = \{a-x^2y, b-xy, c-y^3, xb-a, x^2c-ay, xc-by^2, -b^2y^2-ac, -ac+a+c\}$.
Therefore a Groebner basis for $ker(\phi)$ is

$$G \cap k[a,b,c] = \{-ac + a + c\}.$$

∎

Now that we can construct a Groebner basis for $ker(\varphi)$, we will return to our main goal of finding an algorithm to determine whether an element $f \in k[x_1, \ldots, x_n]$ is in the image of the map φ. This is accomplished by the following theorem.

Theorem 14 *Let $K = \langle y_1 - f_1, \ldots, y_m - f_m\rangle \subseteq k[y_1, \ldots, y_m, x_1, \ldots, x_n]$ be the ideal considered in the above Theorem, and let G be a Groebner basis for K with respect to an elimination order with the x variables larger than the y variables. Then $f \in k[x_1, \ldots, x_n]$ is in the image of φ if and only if there exists $h \in k[y_1, \ldots, y_m]$ such that $\overline{f}^G = h$. In this case, $f = \varphi(h) = h(f_1, \ldots, f_m)$. (Adams 82)*

Before looking at the formal proof, we will discuss the intuition behind this theorem. We know that $f \in Im(\varphi)$ if and only if $f = \varphi(h)$, for some $h \in k[y_1, \ldots, y_m]$. From the first isomorphism theorem, we know that there is a direct relationship $\varphi(h) \leftrightarrow h + ker(\varphi)$. Thus $f \in Im(\varphi)$ if and only if f corresponds to some $h + ker(\varphi)$ for some $h \in k[y_1, \ldots, y_m]$. It follows that $f \in Im(\varphi)$ if and only if $f = \sum_{i=1} g_i p_i + h$, where $G = \{g_1, \ldots, g_s\}$ is a Groebner basis for $ker(\varphi), p_i \in k[y_1, \ldots, y_m]$. This is true if and only if $\overline{f}^G = h$. Therefore, we can see that $f \in Im(\varphi)$ if and only if $\overline{f}^G = h$, for some $h \in k[y_1, \ldots, y_m]$ and in this case, $f = \varphi(h)$, which is what the theorem states. The following is a formal proof that will pin down the details of this argument.

Proof:
($\Rightarrow$) Let $q \in k[x_1, \ldots, x_n]$ be in $Im(\varphi)$. Then $q = h(f_1, \ldots, f_m)$ for some $h \in k[y_1 \ldots, y_m]$. Consider the polynomial

$$q(x_1, \ldots, x_n) - h(y_1, \ldots, y_m) \in k[y_1, \ldots, y_m, x_1, \ldots, x_n].$$

Then by construction of h,

$$q(x_1, \ldots, x_n) - h(y_1, \ldots, y_m) = h(f_1, \ldots, f_m) - h(y_1, \ldots, y_m).$$

We can see that the polynomial $h(f_1, \ldots, f_m) - h(y_1, \ldots, y_m)$ has monomial pairs $f_1^{\alpha_1} \ldots f_m^{\alpha_m} - y_1^{\alpha_1} \ldots y_m^{\alpha_m}$. Thus $h(f_1, \ldots, f_m) - h(y_1, \ldots, y_m) \in K$ by Lemma 7 and so $h(x_1, \ldots, x_m) - h(y_1, \ldots, y_m) \in K$ by substitution. Therefore $\overline{q(x_1, \ldots, x_n) - h(y_1, \ldots, y_n)}^G = 0$ by Proposition 2. This implies that $\overline{q(x_1, \ldots, x_n)}^G = \overline{h(y_1, \ldots, y_m)}^G$, because we have unique remainders. Let $\overline{q(x_1, \ldots, x_n)}^G = \overline{g(y_1, \ldots, y_m)}^G = m$. Since $h \in k[y_1, \ldots, y_m]$, h can only be reduced by polynomials in G which have leading terms in the y variables alone. If the leading term of a polynomial has no x variables, then the polynomial must have no x variables, since x variables are greater than y variables according to our elimination order. Thus the polynomials of G used to reduce h must be polynomials in $k[y_1, \ldots, y_m]$. Therefore $m \in k[y_1, \ldots, y_m]$. Thus $\overline{q(x_1, \ldots, x_n)}^G = m \in k[y_1, \ldots, y_m]$, and this completes this direction of the proof.

($\Leftarrow$) Pick $q \in k[x_1, \ldots, x_n]$. Let $\overline{q}^G = h$, where $h \in k[y_1, \ldots, y_m]$. Then $q - h \in K$, and so by definition of K we can write

$$q(x_1, \ldots, x_n) - h(y_1, \ldots, y_m) = \sum_{i=1}^{m} g_i(y_1, \ldots, y_m, x_1, \ldots, x_n)(y_i - f_i(x_1, \ldots, x_n)).$$

Since $\varphi(y_i) = f_i$, then if we can map each y_i to f_i,

$$\begin{aligned}
\varphi(q(x_1, \ldots, x_n) - h(y_1, \ldots, y_m)) &= \sum_{i=1}^{m} \varphi(g_i(y_1, \ldots, y_m, x_1, \ldots, x_n)(y_i - f_i(x_1, \ldots, x_n)) \\
&= \sum_{i=1}^{m} (g_i(f_1, \ldots, f_m, x_1, \ldots, x_n)(f_i(x_1, \ldots, x_n) - f_i(x_1, \ldots, x_n)) \\
&= 0.
\end{aligned}$$

Thus, by definition of homomorphism,

$$\begin{aligned}\varphi(q(x_1,\ldots,x_n)-h(y_1,\ldots,y_m)) &= \varphi(q(x_1,\ldots,x_n))-\varphi(h(y_1,\ldots,y_m))\\ &= q(x_1,\ldots,x_n)-h(f_i,\ldots,f_m)\\ &= 0.\end{aligned}$$

Therefore we have $q = h(f_1,\ldots,f_m) = \varphi(h)$, and so q is in the image of φ. (Adams 82)

∎

We now have an algorithm to determine whether a polynomial is in the image of a polynomial mapping. In our case, in the application of these tools to integer programming, we are just working with monomials, but this does not change how the above theorem works. Our polynomial map φ will map monomials to monomials, so that the ideal considered in Theorem 14 will be $K = \langle y_j - x_1^{\alpha_{1j}} x_2^{\alpha_{2j}} \cdots x_n^{\alpha_{nj}} | 1 \le j \le m\rangle$. That is, the f_j's, which represent the image of the variables y_i's under φ will be monomials x^{α_j}'s (where $\alpha_j = (\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{nj})$). Therefore we now have a method for determining whether the following system has a solution, and for finding a solution.

$$\begin{aligned}a_{11}\sigma_1 + a_{12}\sigma_2 + \cdots + a_{1m}\sigma_m &= b_1\\ a_{21}\sigma_1 + a_{22}\sigma_2 + \cdots + a_{2m}\sigma_m &= b_2\\ &\vdots\\ a_{n1}\sigma_1 + a_{n2}\sigma_2 + \ldots + a_{nm}\sigma_m &= b_n.\end{aligned}$$

Our method, following from Lemma 6 and Theorem 14, is the following:

1. Compute a Groebner basis G for $K = \langle y_j - x_1^{\alpha_{1j}} x_2^{\alpha_{2j}} \cdots x_n^{\alpha_{nj}} | 1 \le j \le m\rangle$ with respect to an elimination order with the x variables larger than the y variables;
2. Find the remainder h of the division of the monomial $x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$ by G;
3. If $h \notin k[y_1,\ldots,y_m]$, then the System 4.1 does not have non-negative integer solutions. If $h = y_1^{\sigma_1} y_2^{\sigma_2} \cdots y_m^{\sigma_m}$, then $(\sigma_1, \sigma_2, \ldots, \sigma_m)$ is a solution of System 4.1 (Adams 107).

We will consider a simple example that illustrates the above method.

Example:
We will let our system be:

$$\begin{aligned}2\sigma_1 + \sigma_2 &= 3\\ \sigma_1 + \sigma_2 + 3\sigma_3 &= 5\end{aligned}$$

Letting the x_1 represent the first equation and x_2 represent the second, we then have that

$$(x_1^2x_2)^{\sigma_1}(x_1x_2)^{\sigma_2}(x_2^3)^{\sigma_3} = x_1^3x_2^5$$

Then our ideal is $K = \langle y_1 - x_1^2x_2, y_2 - x_1x_2, y_3 - x_2^3\rangle$. Conveniently, this is equivalent to the ideal in the previous example (by converting the variables $a = y_1, b = y_2, c = y_3, x = x_1$, and $y = x_2$). Thus we already have the following Groebner basis for K, $G = \{y_1 - x_1^2x_2, y_2 - x_1x_2, y_3 - x_2^3, x_1y_2 - y_1, x_1^2y_3 - x_2y_1, x_1y_3 - x_2^2y_2, x_2^2y_2^2 - y_1y_3, -y_1y_3 + y_1 + y_3\}$.
Dividing $x_1^3x_2^5$ by terms in G until we get a remainder that is no longer divisible by G gives us:

$$\begin{array}{rc}
 & q_3 : y_1y_2 \\
 & q_2 : x_2^3y_1 \\
 & q_1 : x_1x_2^4 \\
x_1^2x_2 - y_1 & \sqrt{x_1^3x_2^5} \\
x_1x_2 - y_2 & \underline{-(x_1^2x_2^5 - x_1x_2^4y_1)} \\
x_2^3 - y_3 & x_1x_2^4y_1 \\
 & \underline{-(x_1x_2^4y_1 - x_2^3y_1y_2)} \\
 & x_2^3y_1y_2 \\
 & \underline{-(x_2^3y_1y_3 - y_1y_2y_3)} \\
 & y_1y_2y_3
\end{array}$$

Thus we get a solution $y_1y_2y_3$. Translating this back into the integer programming problem, using the exponents of the y_i's, gives us: $\sigma_1 = 1, \sigma_2 = 1, \sigma_3 = 1$, which is indeed a solution to our system. ∎

So far we have only considered the case where the coefficients of the equations in our integer programming problem are positive. Handling the case where some coefficients are negative cannot work in the same way, because when we translate the problem into polynomials, we will have negative exponents and this cannot be done in the polynomial ring $k[x_1, \ldots, x_n]$. This case is not conceptually different, however, and analogous theorems to Lemma 6 and Theorems 13 and 14 that handle this case can be found in Adams 2.8. For the purposes of this paper, we will handle only the non-negative case.

Now that we have found solutions $(\sigma_1, \sigma_2, \ldots, \sigma_m)$ of system 4.1, to complete our goal we want to find the solutions that minimize the cost function $c(\sigma_1, \sigma_2, \ldots, \sigma_m) = \sum_{j=1}^{m} c_j\sigma_j$. In our method for obtaining solutions, we have an elimination order with the x variables larger than the y variables. In order to minimize the cost function, we will use the c_j's to define a term order on y variables in the following way.

Definition 22 *A term order $<_c$ on the y variables is said to be* ***compatible with the cost function*** *c and the map φ if*

$$\begin{aligned} &\{\varphi(y_1^{\sigma_1}y_2^{\sigma_2}\cdots y_m^{\sigma_m}) = \varphi(y_1^{\sigma'_1}y_2^{\sigma'_2}\cdots y_m^{\sigma'_m}) \\ \textit{and} \qquad &c(\sigma_1,\ldots,\sigma_m) <_c (\sigma'_1,\ldots,\sigma'_m)\} \end{aligned}$$

$$\implies \qquad y_1^{\sigma_1}y_2^{\sigma_2}\cdots y_m^{\sigma_m} <_c y_1^{\sigma'_1}y_2^{\sigma'_2}\cdots y_m^{\sigma'_m}.$$

That is, if we have two monomials in $k[y_1,\ldots,y_m]$ mapping to $x_1^{b_1}\cdots x_n^{b_n}$, and the cost function when evaluated at one solution is less than when it is evaluated at the other, then a term order that is compatible with this would order the monomial of the lesser solution as less that the monomial of the solution that is greater. Such a term order on the y variables gives us solutions of system 4.1 which minimize the cost function as our final result shows.

Proposition 7 *Let G be a Groebner basis for K with respect to an elimination order with the x variables larger than the y variables, and an order $<_c$ on the y variables which is compatible with the cost function c and the map φ. If $\overline{x_1^{b'_1}x_2^{b'_2}\cdots x_n^{b'_n}}^G = y_1^{\sigma_1}\cdots y_m^{\sigma_m}$, where $y_1^{\sigma_1}\cdots y_m^{\sigma_m}$ is reduced with respect to G, then $(\sigma_1,\ldots,\sigma_m)$ is a solution of system 4.1. (Adams 110)*

Proof:
Let G be a Groebner basis for $K = \langle y_j - x_1^{a_{1j}}x_2^{a_{2j}}\cdots x_n^{a_{nj}} | 1 \le j \le m\rangle$ with respect to an elimination order with the x variables larger than the y variables, and an order $<_c$ on the y variables which is compatible with the cost function c and the map φ. Let $\overline{x_1^{b'_1}x_2^{b'_2}\cdots x_n^{b'_n}w^\beta}^G = y_1^{\sigma_1}\cdots y_m^{\sigma_m}$, with $y_1^{\sigma_1}\cdots y_m^{\sigma_m}$ reduced with respect to G. Then $(\sigma_1,\ldots,\sigma_m)$ is a solution of system 4.1 by Lemma 6. Now we want to show that $(\sigma_1,\ldots,\sigma_m)$ is a minimal solution.
Proceed by contradiction. Assume there exists a solution $(\sigma'_1,\ldots,\sigma'_m)$ of system 4.1 such that $\sum_{j=1}^m c_j\sigma'_j < \sum_{j=1}^m c_j\sigma_j$. Then by definition of a ring homomorphism, since $\varphi(y_1^{\sigma_1}\cdots y_m^{\sigma_m}) = \varphi(y_1^{\sigma'_1}\cdots y_m^{\sigma'_m})$,

$$\varphi(y_1^{\sigma_1}\cdots y_m^{\sigma_m}) - \varphi(y_1^{\sigma'_1}\cdots y_m^{\sigma'_m}) = \varphi(y_1^{\sigma_1}\cdots y_m^{\sigma_m} - y_1^{\sigma'_1}\cdots y_m^{\sigma'_m}) = 0.$$

Therefore $y_1^{\sigma_1}\cdots y_m^{\sigma_m} - y_1^{\sigma'_1}\cdots y_m^{\sigma'_m} \in ker(\varphi)$. By Theorem 13, $ker(\varphi) \subseteq K$, and so $y_1^{\sigma_1}\cdots y_m^{\sigma_m} - y_1^{\sigma'_1}\cdots y_m^{\sigma'_m} \in K$. Thus $\overline{y_1^{\sigma_1}\cdots y_m^{\sigma_m} - y_1^{\sigma'_1}\cdots y_m^{\sigma'_m}}^G = 0$ by Proposition 2. We will arrive at a contradiction to this. Since, by assumption, $y_1^{\sigma_1}\cdots y_m^{\sigma_m} >_c y_1^{\sigma'_1}\cdots y_m^{\sigma'_m}$, then $LT(y_1^{\sigma_1}\cdots y_m^{\sigma_m} - y_1^{\sigma'_1}\cdots y_m^{\sigma'_m}) = y_1^{\sigma_1}\cdots y_m^{\sigma_m}$. But $y_1^{\sigma_1}\cdots y_m^{\sigma_m}$ is already reduced with respect to G, and therefore, by the division algorithm, $y_1^{\sigma_1}\cdots y_m^{\sigma_m} - y_1^{\sigma'_1}\cdots y_m^{\sigma'_m}$ cannot reduce to 0 by G. Thus, by contradiction, we have that $y_1^{\sigma_1}\cdots y_m^{\sigma_m}$ is a solution that minimizes the cost function c. (Adams 111) ∎

In the case where the cost function has only positive coefficients, which is the only case we have discussed, a term order that is compatible with the cost function and the map φ is one that orders monomials using the cost function and breaks ties using any other monomial order (Adams 111). For example, if our integer programming problem had m unknowns, then we could order the monomials with y variables using the cost function and break any ties by lex order with $y_1 > y_2 > \cdots > y_m$. That is, $y_1^{\sigma_1} y_2^{\sigma_2} \cdots y_m^{\sigma_m} < y_1^{\sigma_1'} y_2^{\sigma_2'} \cdots y_m^{\sigma_m'}$ if and only if either the cost function evaluated at $(\sigma_1, \ldots, \sigma_m)$ is less than when it is evaluated at $(\sigma_1', \ldots, \sigma_m')$ or the cost is equal for both and $y_1^{\sigma_1} y_2^{\sigma_2} \cdots y_m^{\sigma_m} <_{lex} y_1^{\sigma_1'} y_2^{\sigma_2'} \cdots y_m^{\sigma_m'}$. In the above example, we have only one solution to our system. Having a solution that minimizes cost is only meaningful if there is more than one possible solution. Without an ordering that is compatible with the cost function, multiple solutions to the system can arise when we are reducing the monomial $x_1^{b_1} x_2^{b_2} \cdots x_m^{b_m}$ by the Groebner basis G of our ideal K (step 2 of our method for finding a solution to our system). During this reduction, $x_1^{b_1} x_2^{b_2} \cdots x_m^{b_m}$ can be reduced to multiple monomials in y variables before the reduction is complete. The exponents of each of these monomials is a solution to our system. In an involved problem, there may be many solutions and it may be complicated to check these to find a minimal one. As we have just proven, an ordering that is compatible with our cost function gives us only the minimal solution (although multiple minimal solutions may exist).

4.1 Conclusion

This paper has provided an insight into the theory of Groebner bases as well as a brief introduction to the techniques of working with Groebner bases through a discussion of their application to integer programming. One can see that the application of these techniques can become very complicated computationally, and all but the most simple cases require the use of a Computer Algebra System. Yet, through the integer programming example, one can see how Groebner bases are an important computational tool. Groebner bases have a wide range of applications, including Computer Aided Geometric Design and Coding Theory (Cox). Improvements on the algorithms discussed in this paper are currently being researched.

4.2 Acknowledgements

I would like to thank Professor Ivelisse Rubio, University of Puerto Rico, for motivating my interest in the study of Groebner Bases and for suggesting its applications to integer programming as an interesting topic to explore. I would also like to thank Professor Murli Gupta, Professor E. Arthur Robinson, and Professor Katherine Gurski, hosts of The George Washington University Summer Program For Women In Mathematics, for providing an excellent summer experience that introduced me to the topics

of this paper.

Appendix A

Group Theory

A.1 Ascending Chain Condition

This result shows that there cannot be an infinite strictly ascending chain of ideals, but that at some point, one will reach an ideal that is the biggest possible in the chain.

Theorem 15 *Let $I_1 \subset I_2 \subset I_3 \subset \cdots$ be an ascending chain of ideals in $k[x_1, \ldots, x_n]$. Then there exists an $N \geq 1$ such that $I_N = I_{N+1} = I_{N+2} = \cdots$.*

Proof:
Consider $I = \cup_{i=1}^{\infty} I_i$. We will first show that I is an ideal in $k[x_1, \ldots, x_n]$. Let $f, g \in I$. Then there are ideals I_i and I_j contained in I such that $f \in I_i$ and $g \in I_j$. Assume, WLOG, that $I_i \subset I_j$. Then $f, g \in I_j$. Thus $f \pm g$ and $f \cdot g \in I_j$, so $f \pm g$ and $f \cdot g \in I$. Also, since $-f, 0 \in I_j$, $-f, 0 \in I$. So I is a subring of $k[x_1, \ldots, x_n]$. Now we need to show that I absorbs elements of $k[x_1, \ldots, x_n]$ under multiplication to finish the proof that I is an ideal. Let $f \in I$ and $h \in k[x_1 \ldots, x_n]$. Then $f \in I_i$ for some I_i. Since I_i is an ideal, $f \cdot h \in I_i$. Thus $f \cdot h \in I$. Therefore I is an ideal.

So by the Hilbert Basis Theorem, I must have a finite generating set. So we can say, $I = \langle f_1, \ldots, f_s \rangle$. Each generator f_i must be in one of the $I_j's$ such that $f_i \in I_{j_i}$ for some j_i. We have a finite set of these I_{j_i}, and so we can let N be the maximum of the j_i. Then, by the construction of the ascending chain, $f_i \in I_N$ for all i. Thus

$$I = \langle f_1, \ldots, f_s \rangle \subset I_N \subset I_{N+1} \subset \cdots \subset I.$$

Therefore all subsequent ideals following I_N in the chain are equal. (CLO 76) ∎

A.2 Group Homomorphisms

Some results from algebra about the mappings of groups are given here.

Definition 23 *A map ϕ of a group G into a group G' is a* ***group homomorphism*** *if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.*

This idea can be expanded to the following definition for rings.

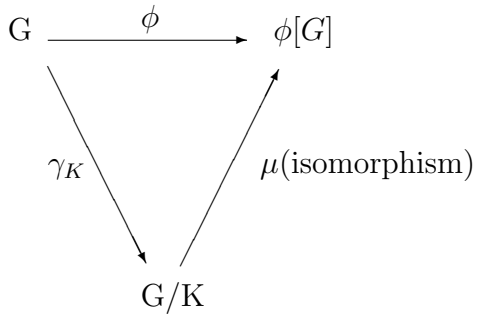
Definition 24 *A map ϕ of a ring R into a ring S is a* ***ring homomorphism*** *if the following conditions hold for all $a, b \in R$:*

1. *Addition is preserved: $\phi(a + b) = \phi(a) + \phi(b)$, and*
2. *Multiplication is preserved: $\phi(ab) = \phi(a)\phi(b)$.*

Note that the zero element is mapped to zero, since by part 1, $\phi(0_R) = \phi(0_R + 0_R) = \phi(0_R) + \phi(0_R) = 2\phi(0_R)$. Thus $\phi(0_R) = 0_S$. Also, a homomorphism must preserve the additive inverse map, since for $a \in R, \phi(a) + \phi(-a) = \phi(a - a) = \phi(0_R) = 0_S$ and so $-\phi(a) = \phi(-a)$.

Theorem 16 ***First Isomorphism Theorem*** *Let $\phi : G \to G'$ be a homomorphism with kernel K, and let $\gamma_k : G \to G/K$ be the canonical homomorphism. There is unique isomorphism $\mu : G/K \to \phi[G]$ such that $\phi(x) = \mu(\gamma_k(x))$ for each $x \in G$. (Fraleigh 210)*

This theorem states that there is an isomorphism between the cosets of G (mod the elements of the kernel of ϕ) and the image of G under ϕ. The following is an illustration of this theorem.



Bibliography

[1] Adams, Loustaunau. *An Introduction to Groebner Bases, Graduate Studies in Mathematics*, AMS, Rhode Island. 1994.

[2] Craig, Joe. "L^2 : Leopntief Models and Linear Programming." *Kenyon College Senior Comps*. 2003.

[3] Cox, David A. "Introduction to Groebner bases." *Applications of Computational Algebraic Geometry*.Ed. Cox and Sturmfels, AMS, Rhode Island. 1998. 1-22.

[4] Cox, Little, O'Shea. *Ideals, Varieties, and Algorithms, second edition*, Springer, New York. 1997.

[5] Cox, Little, O'Shea. *Using Algebraic Geometry*, Springer, New York. 1998.

[6] Fraleigh, John. *Abstract Algebra*, Addison-Wesley, New York. 1998.

[7] Greuel, Pfister. "Grobner bases and algebraic geometry." *Grobner Bases and Applications*. Ed. Buchberger and Winkler, Cambridge University Press. 1998. 109-143.

[8] Hosten, R. Thomas. "Grobner bases and integer programming." *Grobner Bases and Applications*. Ed. Buchberger and Winkler, Cambridge University Press. 1998. 144-157.

[9] Thomas, John B. "Applications to Integer Programming." *Applications of Computational Algebraic Geometry*. Ed. Cox and Sturmfels, AMS, Rhode Island. 1998. 119-140.