A Survey of Gröbner Bases and Their Applications

Departmental Report

Brad A. Lutes

Texas Tech University

Lubbock, TX

June 30, 2004

CONTENTS

CHAPTER 1
INTRODUCTION

The theory of Gröbner bases endows rings of polynomials in several variables with a device similar to the division algorithm for univariate polynomials over a field k.

One of the main advantages of the division algorithm is that given any two polynomials, f and g, it allows us to find their greatest common divisor d. Since the ideal generated by f and g is equal to the ideal generated by d, as a result, one can use the algorithm to compute the principal generators of polynomial ideals given any two generators.

For multivariable polynomials, Hilbert's Basis Theorem guarantees that every ideal has a finite number of generators. In this setting, the notion of greatest common divisor as the principal generator of polynomial ideals in one variable corresponds to the concept of reduced Gröbner bases. At the core of the Gröbner basis theory, there is an algorithm, similar to the long division algorithm in the univariate case, that can be used to produce sets of generators for ideals in the ring of multivariate polynomials with certain properties. The machinery of Gröbner bases also provides algorithms to address problems such as ideal membership, equality of ideals, radical membership, solving polynomial equations and some issues related to integer programming, among others.

In this paper we will provide a survey of some important results in the theory of Gröbner bases along with a discussion of some of the applications mentioned above. First we will see how to determine whether a polynomial f is contained in an ideal. This is called the ideal membership problem. Next we discuss how an answer to this problem leads to a method to determine whether two ideals are equal. Another problem that we will address, also related to the ideal membership problem, is the radical membership problem, that is, to determine whether a polynomial f is contained in the radical of an ideal. We conclude this paper with examples of how Gröbner bases can be used to solve both polynomial equations and integer programming problems.

Our exposition mirrors the approach followed in Adams and Loustaunau's [1].

Many of the examples shown in this manuscript come from exercises not worked out in the bibliography. Unless the full example, namely, the problem and the solution, was produced by the author of this report, a reference is given to where the particular problem was taken from.

CHAPTER 2
PRELIMINARY DEFINITIONS AND RESULTS

Let k be a field. Consider $k[x_1, \ldots, x_n]$ which is the set of all polynomials in the variables $x_1, \ldots, x_n$ with coefficients in k. Note that $k[x_1, \ldots, x_n]$ is a commutative ring with respect to polynomial addition and multiplication. For this paper, $\mathbb{N} = \{0, 1, \ldots\}$.

First we define the most basic components of any polynomial, namely, power products and terms.

Definition 1. *A **power product** is an expression of the form $x_1^{\beta_1} \cdots x_n^{\beta_n}$ where $\beta_i \in \mathbb{N}$, $i = 1, \ldots, n$. A **term** is an expression of the form $ax_1^{\beta_1} \cdots x_n^{\beta_n}, a \in k$.*

Thus, every polynomial in $x_1, \ldots, x_n$ is the sum of finitely many terms.

Much of our exposition deals with the manipulation of ideals in the ring $k[x_1, \ldots, x_n]$, defined below for the sake of completeness.

Definition 2. *Let $I \subseteq k[x_1, \ldots, x_n]$, $I \neq \emptyset$. I is an **ideal** in $k[x_1, \ldots, x_n]$ if*

1. *$f, g \in I$ implies that $f + g \in I$.*
2. *$f \in I$ and $h \in k[x_1, \ldots, x_n]$ implies that $hf \in I$.*

It will be important for us to be able to identify all of the generators of an ideal. One of the most important results in polynomial ideal theory is the Hilbert Basis Theorem, which we do not prove here. (A proof can be found in most relatively advanced texts in algebra, see for instance [3].) This result is important because it says that any ideal in $k[x_1, \ldots, x_n]$ has a finite set of generators.

Theorem 1. *(Hilbert Basis Theorem) Every ideal in $k[x_1, \ldots, x_n]$ is finitely generated. In other words, if I is an ideal in $k[x_1, \ldots, x_n]$, then there exists $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ such that $I = \langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} g_i f_i \mid g_i \in k[x_1, \ldots, x_n], i = 1, \ldots, n \right\}$.*

CHAPTER 3
POLYNOMIAL DIVISION

3.1 UNIVARIATE VERSUS MULTIVARIATE POLYNOMIAL DIVISION

It is assumed that anyone reading this paper already knows how to divide two univariate polynomials using polynomial long division.

The purpose of this section is to highlight how a process similar to univariate division can be carried out with multivariate polynomials. To this end, consider the following example.

Example 1. *Let* $f = x^4 - 3x^3 + 6x^2 + 5x - 1$, $g = 3x^3 + x^2 + 3$ *where* $f, g \in \mathbb{Q}[x]$. *What is* f *divided by* g*?*

$$
\begin{array}{r|l}
 & \frac{1}{3}x - \frac{10}{9} \\
\hline
3x^3 + x^2 + 3 & x^4 - 3x^3 + 6x^2 + 5x - 1 \\
 & \underline{x^4 + \frac{1}{3}x^3 \qquad\qquad + x} \\
 & \quad -\frac{10}{3}x^3 + 6x^2 + 4x - 1 \\
 & \quad \underline{-\frac{10}{3}x^3 - \frac{10}{9}x^2 \qquad - \frac{10}{3}} \\
 & \qquad\qquad \frac{64}{9}x^2 + 4x + \frac{7}{3}
\end{array}
$$

So,

$$\frac{f}{g} = \frac{1}{3}x - \frac{10}{9} + \frac{\frac{64}{9}x^2 + 4x + \frac{7}{3}}{3x^3 + x^2 + 3}$$

or, equivalently,

$$f = \left(\frac{1}{3}x - \frac{10}{9}\right) g + \left(\frac{64}{9}x^2 + 4x + \frac{7}{3}\right).$$

In this example we observe the following:

1. f and g are written so that terms appearing to the left are of higher degree. So for f and g it is clear what the first term, or leading term (denoted $\mathrm{lt}(\cdot)$), is:

$$\mathrm{lt}(f) = x^4, \qquad \mathrm{lt}(g) = 3x^3.$$

2. Observe that $\frac{\mathrm{lt}(f)}{\mathrm{lt}(g)} = \frac{1}{3}x$, or equivalently, $\frac{1}{3}x\ \mathrm{lt}(g) = \mathrm{lt}(f)$.

3. Let $h = -\frac{10}{3}x^3 + 6x^2 + 4x - 1 = f - \frac{\mathrm{lt}(f)}{\mathrm{lt}(g)}g$. We have $\deg(f)$=4 while $\deg(h)$=3. That is, the degree of h, the first remainder of the division, decreases by one. In general, the degree of the remainder on each step decreases in degree by one, thus assuring the process will terminate.

4. The division process stops because there is no term $ax^\nu, \nu \in \mathbb{N}$, such that $(ax^\nu)(3x^3) = \frac{64}{9}x^2$.

In order to produce a division algorithm for multivariate polynomials that mimics the above, we need to define notions similar to those of degree of a polynomial and leading term.

3.1.1 TERM ORDERS

We remind that a total order $<$ on a set S is an order such that for every $a, b \in S$ exactly one of the following relations must hold:

$$a < b, \quad a = b, \quad \text{or} \quad b < a.$$

Let $\mathbb{N}^n = \{(\alpha_1, \ldots, \alpha_n) |\ \alpha_i \in \mathbb{N}, i = 1, \ldots, n\}$ and denote the set of all power products as $\mathbb{T}^n$. For the next definition, we denote $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ by $\mathbf{x}^\alpha$, where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.

Definition 3. *A **term order** on $\mathbb{T}^n$ is a total order $<$ on $\mathbb{T}^n$ such that*

1. $1 < \mathbf{x}^\beta$ *for all* $\mathbf{x}^\beta \in \mathbb{T}^n$, $\mathbf{x}^\beta \neq 1$.

2. *If* $\mathbf{x}^\alpha < \mathbf{x}^\beta$, *then* $\mathbf{x}^\alpha \mathbf{x}^\gamma < \mathbf{x}^\beta \mathbf{x}^\gamma$, *for all* $\mathbf{x}^\gamma \in \mathbb{T}^n$.

Next we give some examples of term orders that are commonly used. Notice that a term order is meaningless unless an order on the set of variables $\{x_1, \ldots, x_n\}$ has been specified. Unless otherwise noted, we will assume that $x_1 > x_2 > \cdots > x_n$. This simply means that x_1 is our "biggest" or first variable, x_2 the next "biggest", and so on.

Definition 4. *We define the* ***lexicographical ordering*** *(denoted by lex) as follows:*

For $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ *we define*

$$\mathbf{x}^\alpha < \mathbf{x}^\beta \Leftrightarrow \begin{cases} \text{the first coordinates } \alpha_i \text{ and } \beta_i \text{ in } \alpha \text{ and } \beta \\ \text{from the left, which are different, satisfy } \alpha_i < \beta_i. \end{cases}$$

Example 2. *If we let* $x_1 > x_2$*, then according to the lexicographical ordering, we have*

$$1 < x_2 < x_2^2 < x_2^3 < \cdots < x_1 < x_2 x_1 < x_2^2 x_1 < \cdots$$

Definition 5. *We define the* ***degree lexicographical ordering*** *(denoted deglex) as follows:*

For $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ *we define*

$$\mathbf{x}^\alpha < \mathbf{x}^\beta \Leftrightarrow \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \\ \text{or} \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \text{ and } \mathbf{x}^\alpha < \mathbf{x}^\beta \\ \text{with respect to lex with } x_1 > x_2 > \cdots > x_n. \end{cases}$$

So, with the deglex order, we first order by total degree and we break ties by the lex order.

Example 3. *Let* $x_2 > x_1$*. If* $<$ *denotes deglex, we have*

$$1 < x_1 < x_2 < x_1^2 < x_1 x_2 < x_2^2 < x_1^3 < x_1^2 x_2 < \cdots$$

Definition 6. *We define the* ***degree reverse lexicographical ordering*** *(denoted degrevlex) as follows:*

For $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ *we define*

$$\mathbf{x}^{\alpha} < \mathbf{x}^{\beta} \Leftrightarrow \begin{cases} \sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i \\ \textit{or} \\ \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i \textit{ and the first coordinates } \alpha_i \textit{ and } \beta_i \textit{ in} \\ \alpha \textit{ and } \beta \textit{ from the right, which are different, satisfy } \alpha_i > \beta_i. \end{cases}$$

Now choose a term order on $\mathbb{T}^n$. For all $f \in k[x_1, \ldots, x_n]$, we can write

$$f = a_1\mathbf{x}^{\alpha_1} + a_2\mathbf{x}^{\alpha_2} + \cdots + a_r\mathbf{x}^{\alpha_r}$$

where $a_i \in k\backslash\{0\}$, $\mathbf{x}^{\alpha_i}$ are power products, and $\mathbf{x}^{\alpha_1} > \mathbf{x}^{\alpha_2} > \cdots \mathbf{x}^{\alpha_r}$. We define:

(i) the *leading power product* of f to be $\mathrm{lp}(f) = \mathbf{x}^{\alpha_1}$;

(ii) the *leading coefficient* of f to be $\mathrm{lc}(f) = a_1$;

(iii) the *leading term* of f to be $\mathrm{lt}(f) = a_1\mathbf{x}^{\alpha_1}$.

3.1.2 MULTIVARIABLE DIVISION ALGORITHM

In a nutshell, the multivariable division algorithm consists of a sequence of *reduction steps* as follows:

Definition 7. *Let $f, g, h \in k[x_1, \ldots, x_n]$ with $g \neq 0$. We say that f* ***reduces*** *to h modulo g in one step, denoted*

$$f \xrightarrow{g} h,$$

if and only if $\mathrm{lp}(g)$ *divides a non-zero term $a\mathbf{x}^{\alpha}$ that appears in f and*

$$h = f - \frac{a\mathbf{x}^{\alpha}}{\mathrm{lt}(g)}g.$$

This mimics the steps in the univariate polynomial long division: in our previous Example 1, we had $f = x^4 - 3x^3 + 6x^2 + 5x - 1$, $g = 3x^3 + x^2 + 3$ and $h = -\frac{10}{3}x^3 + 6x^2 + 4x - 1$, where h was the first remainder in the division process. Note

that there is a power product in f, namely, $x^4 = \mathrm{lt}(f)$, such that $h = f - \frac{\mathrm{lt}(f)}{\mathrm{lt}(g)}g$, where $\mathrm{lp}(g)=x^3$. That is, h is obtained from f by reduction modulo g in one step.

In the multivariate case, one can think of h in Definition 7 as the remainder of a one step division of f by g.

In the multivariate case, it may also be the case that we have to divide by more than one polynomial at a time. We extend the previous definition to include this possibility:

Definition 8. *Let f, h and $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$ with $f_i \neq 0$ for $i = 1, \ldots, s$. Let $F = \{f_1, \ldots, f_s\}$. We say that f **reduces** to h modulo F, denoted*

$$f \xrightarrow{F}_+ h,$$

if and only if there exist a sequence of indices $i_1, i_2, \ldots, i_t \in \{1, \ldots, s\}$ and a sequence of polynomials $h_1, \ldots, h_{t-1} \in k[x_1, \ldots, x_n]$ such that

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \cdots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h.$$

Definition 9. *A polynomial r is called **reduced** with respect to a set of non-zero polynomials $F = \{f_1, \ldots, f_s\}$ if $r = 0$ or no power product that appears in r is divisible by any one of the $\mathrm{lp}(f_i)$, $i = 1, \ldots, s$. In other words, r cannot be reduced modulo F.*

Definition 10. *If $f \xrightarrow{F}_+ r$ and r is reduced with respect to F, then we call r a **remainder** for f with respect to F.*

We note that many computer algebra systems have packages and commands to perform these computations.

Example 4. *Consider the polynomials $f = x^3y^3 + 2y^2$, $f_1 = 2xy^2 + 3x + 4y^2$, $f_2 = y^2 - 2y - 2$ in $\mathbb{Q}[x, y]$, under the lexicographical order with $x > y$. Let $F = \{f_1, f_2\}$ and $h = -\frac{3}{2}x^3y - 4x^2y^2 - 4x^2y + 2y^2$. We will show that f reduces to h modulo F. First, we reduce f modulo f_1 in one step:*

We have lt(f_1)=$2xy^2$, lp(f_1)=xy^2, and $a\mathbf{x}^\alpha = x^3y^3$ is a power product in f such that lp(f_1) divides it. So, we get

$$\begin{aligned} h_1 &= f - \frac{a\mathbf{x}^\alpha}{lt(f_1)} f_1 \\ &= x^3y^3 + 2y^2 - \frac{x^3y^3}{2xy^2}(2xy^2 + 3x + 4y^2) \\ &= -\frac{3}{2}x^3y - 2x^2y^3 + 2y^2 \end{aligned}$$

that is, $f \xrightarrow{f_1} h_1$.

Next, we reduce h_1 modulo f_2 in one step:

We have lt(f_2)=lp(f_2)=y^2. Since lp(f_2) divides both $-2x^2y^3$ and $2y^2$, we have two choices for $a\mathbf{x}^\alpha$. We let $a\mathbf{x}^\alpha = -2x^2y^3$.

We then get

$$\begin{aligned} h_2 &= h_1 - \frac{a\mathbf{x}^\alpha}{lt(f_2)} f_2 \\ &= -\frac{3}{2}x^3y - 2x^2y^3 + 2y^2 - \frac{-2x^2y^3}{y^2}(y^2 - 2y - 2) \\ &= -\frac{3}{2}x^3y - 4x^2y^2 - 4x^2y + 2y^2 \\ &= h \end{aligned}$$

That is, $h_1 \xrightarrow{f_2} h$.

Hence, $f \xrightarrow{F}_+ h$.

The reduction process allows the formulation of the following division algorithm for multivariate polynomials which mirrors the univariate division algorithm:

MULTIVARIABLE DIVISION ALGORITHM

INPUT: $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ with $f_i \neq 0$ for all i.

OUTPUT: $u_1, \ldots, u_s, r$ such that $f = u_1f_1 + \cdots + u_sf_s + r$ and

r is reduced with respect to $\{f_1, \ldots, f_s\}$ and

$$\max(\mathrm{lp}(u_1)\mathrm{lp}(f_1), \ldots, \mathrm{lp}(u_s)\mathrm{lp}(f_s), \mathrm{lp}(r))=\mathrm{lp}(f).$$

INITIALIZATION: $u_1 := 0$, $u_2 := 0$, $\ldots$, $u_s := 0$, $r := 0$, $h := f$

WHILE $h \neq 0$ **DO**

IF there exists i such that $\mathrm{lp}(f_i)$ divides $\mathrm{lp}(h)$ **THEN**

choose i least such that $\mathrm{lp}(f_i)$ divides $\mathrm{lp}(h)$

$u_i := u_i + \frac{\mathrm{lt}(h)}{\mathrm{lt}(f_i)}$

$h := h - \frac{\mathrm{lt}(h)}{\mathrm{lt}(f_i)} f_i$

ELSE

$r := r + \mathrm{lt}(h)$

$h := h - \mathrm{lt}(h)$

Example 5. *Let $f = y^2x + 1$, $f_1 = yx - y$, $f_2 = y^2 - x$, under the deglex ordering with $y > x$.*

We want to divide f by $F = \{f_1, f_2\}$.

Note that $lp(f)$=$lt(f)$=y^2x, $lp(f_1)$=$lt(f_1)$=yx, and $lp(f_2)$=$lt(f_2)$=y^2.

INITIALIZATION: u_1:=0, u_2:=0, r:=0, h:=f

Step 1.

yx=$lp(f_1)$ divides $lp(h)$=$lp(f)$=y^2x

$u_1 := u_1 + \frac{lt(h)}{lt(f_1)} = 0 + \frac{y^2x}{yx} = y$

$h := h - \frac{lt(h)}{lt(f_1)} f_1 = y^2x + 1 - \frac{y^2x}{yx}(yx - y) = y^2 + 1$

Step 2.

yx=$lp(f_1)$ does not divide $lp(h)$=y^2

y^2=$lp(f_2)$ divides $lp(h)$=y^2

$u_2 := u_2 + \frac{lt(h)}{lt(f_2)} = 0 + \frac{y^2}{y^2} = 1$

$h := h - \frac{lt(h)}{lt(f_2)} f_2 = y^2 + 1 - \frac{y^2}{y^2}(y^2 - x) = x + 1$

Step 3.

yx=$lp(f_1)$ does not divide $lp(h)$=x

y^2=$lp(f_2)$ does not divide $lp(h)$=x

$r := r + lt(h) = 0 + x = x$

$h := h - lt(h) = x + 1 - x = 1$

Step 4.

yx=*lp*(f_1) *does not divide* *lp*(h)=1

y^2=*lp*(f_2) *does not divide* *lp*(h)=1

$r := r + lt(h) = x + 1$

$h := h - lt(h) = 1 - 1 = 0$

The algorithm stops and we have that $u_1 = y$, $u_2 = 1$, *and* $r = x + 1$. *Hence,*

$$f \xrightarrow{F}_{+} x + 1$$

and

$$f = yf_1 + f_2 + (x + 1).$$

Note that, in the univariate case, if we divide f by g, the univariate division algorithm produces univariate polynomials q and r such that

$$f = qg + r$$

where q is the quotient and r is the remainder. In the multivariate case, if we divide f by $F = \{f_1, \ldots, f_s\}$, the multivariate division algorithm produces polynomials $u_1, \ldots, u_s, r \in k[x_1, \ldots, x_n]$ such that

$$f = u_1 f_1 + \cdots + u_s f_s + r$$

where the quotients are $u_1, \ldots, u_s$ and r is the remainder. More precisely, we have (see [1] for a proof):

Theorem 2. *Given a set of non-zero polynomials* $F = \{f_1, \ldots, f_s\}$ *and* $f \in k[x_1, \ldots, x_n]$, *the Multivariable Division Algorithm above produces polynomials* $u_1, \ldots, u_s, r \in k[x_1, \ldots, x_n]$ *such that*

$$f = u_1 f_1 + \cdots + u_s f_s + r$$

with r *reduced with respect to* F *and*

$$\mathrm{lp}(f) = \max\left(\max_{1 \le i \le s}(\mathrm{lp}(u_i)\mathrm{lp}(f_i)), \mathrm{lp}(r)\right).$$

CHAPTER 4
GRÖBNER BASES AND BUCHBERGER'S ALGORITHM

We are now ready to approach the core of computer algebra: Gröbner bases.

Definition 11. *A set of non-zero polynomials $G = \{g_1, \ldots, g_t\}$ contained in an ideal I, is called a* ***Gröbner basis*** *for I if and only if for all $f \in I$ such that $f \neq 0$, there exists $i \in \{1, \ldots, t\}$ such that $\mathrm{lp}(g_i)$ divides $\mathrm{lp}(f)$.*

Although the existence of a Gröbner basis for an ideal $I \subseteq k[x_1, \ldots, x_n]$ implies that G is a set of generators for the ideal (see below), we point out that the word basis here should not be interpreted in the usual algebra sense, as elements in I may not be expressed in terms of the elements of G in a unique way.

Example 6. *In Example 8, we will show that a Gröbner basis for the ideal $\langle x^2y + z, xz + y\rangle$ is given by $\{x^2y + z, xz + y, x^3y - y\}$. Notice that $x^3y + xz = (xz + y) + (x^3y - y) = x(x^2y + z)$. So $x^3y + xz \in \langle x^2y + z, xz + y\rangle$ has two different expressions in terms of a single Gröbner basis for the ideal.*

Next we list some important properties of Gröbner bases whose proof can be found in [1]. The first is a characterization for which we need the following definition.

Definition 12. *For a subset S of $k[x_1, \ldots, x_n]$, the* ***leading term ideal*** *of S is the ideal $\mathrm{Lt}(S) = \langle \mathrm{lt}(s) \mid s \in S\rangle$.*

Theorem 3. *Let I be a non-zero ideal of $k[x_1, \ldots, x_n]$. The following statements are equivalent for a set of non-zero polynomials $G = \{g_1, \ldots, g_t\} \subseteq I$.*

(i) *G is a Gröbner basis for I.*

(ii) *$f \in I$ if and only if $f \xrightarrow{G}_+ 0$.*

(iii) *$f \in I$ if and only if $f = \sum_{i=1}^{t} h_i g_i$ with $\mathrm{lp}(f) = \max_{1 \leq i \leq t}(\mathrm{lp}(h_i)\mathrm{lp}(g_i))$.*

(iv) *$\mathrm{Lt}(G) = \mathrm{Lt}(I)$.*

As a consequence of the preceding theorem, we have the important result, pointed out earlier, that a Gröbner basis $G = \{g_1, \ldots, g_t\}$ for I is a set of generators for I, that is, $I = \langle g_1, \ldots, g_t \rangle$.

Another important consequence of the preceding theorem is the fact that every nonzero ideal $I \subseteq k[x_1, \ldots, x_n]$ has a Gröbner basis.

Given a set of generators $f_1, \ldots, f_s$ of an ideal $I \subseteq k[x_1, \ldots, x_n]$, Buchberger's Algorithm produces a Gröbner basis for I. We recall that such a finite set of generators for I always exists by Hilbert's Basis Theorem.

Before we discuss the algorithm, the following definition is needed:

Definition 13. *Let $L = \operatorname{lcm}(\operatorname{lp}(f), \operatorname{lp}(g))$. The* **S-*polynomial*** *of f and g is defined to be*

$$S(f,g) = \frac{L}{\operatorname{lt}(f)} f - \frac{L}{\operatorname{lt}(g)} g.$$

Example 7. *Let $f = x^3y - xy^2 + 1$, $g = x^2y^2 - y^3 - 1 \in \mathbb{Q}[x,y]$, with deglex, $y > x$, the term order. Then $lp(f) = x^3y$, $lp(g) = x^2y^2$, and so $L = lcm(x^3y, x^2y^2) = x^3y^2$.*

$$\begin{aligned} S(f,g) &= \frac{x^3y^2}{x^3y}(x^3y - xy^2 + 1) - \frac{x^3y^2}{x^2y^2}(x^2y^2 - y^3 - 1) \\ &= x^3y^2 - xy^3 + y - x^3y^2 + xy^3 + x \\ &= y + x \end{aligned}$$

Now let the term order be lex, $y > x$.

Then $lp(f) = xy^2$, $lp(g) = y^3$, and so $L = lcm(xy^2, y^3) = xy^3$.

$$\begin{aligned} S(f,g) &= \frac{xy^3}{-xy^2}(x^3y - xy^2 + 1) - \frac{xy^3}{-y^3}(x^2y^2 - y^3 - 1) \\ &= -x^3y^2 + xy^3 - y + x^3y^2 - xy^3 - x \\ &= -y - x \end{aligned}$$

INPUT: $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n]$ with $f_i \neq 0$ for all i

OUTPUT: $G = \{g_1, \ldots, g_t\}$, a Gröbner basis for $\langle f_1, \ldots, f_s \rangle$

INITIALIZATION: $G := F$, $\mathcal{G} := \{\{f_i, f_j\} \mid f_i \neq f_j \in G\}$

WHILE: $\mathcal{G} \neq \emptyset$ **DO**

Choose any $\{f, g\} \in \mathcal{G}$

$\mathcal{G} := \mathcal{G} - \{\{f, g\}\}$

$S(f, g) \xrightarrow{G}_+ h$, where h is reduced with respect to G

IF $h \neq 0$ **THEN**

$\mathcal{G} := \mathcal{G} \cup \{\{u, h\}\}|$ for all $u \in G\}$

$G := G \cup \{h\}$

Example 8. ([1], Problem 1.7.3(b))

Let $f_1 = x^2y + z, f_2 = xz + y \in \mathbb{Q}[x, y, z]$ and lex, $z > y > x$, be the term order.

INITIALIZATION: $G := \{f_1, f_2\}$, $\mathcal{G} = \{\{f_1, f_2\}\}$

Step 1.

Choose $\{f_1, f_2\}$.

$\mathcal{G} := \emptyset$

$S(f_1, f_2) = \frac{xz}{z}(z + x^2y) - \frac{xz}{xz}(xz + y) = x^3y - y = h$, *which is reduced with respect to G since $lp(f_1) = z$, $lp(f_2) = xz$*

Since $h \neq 0$, let $f_3 := x^3y - y$

$\mathcal{G} := \{\{f_1, f_3\}, \{f_2, f_3\}\}$

$G := \{f_1, f_2, f_3\}$

Step 2.

Choose $\{f_1, f_3\}$.

$\mathcal{G} := \{f_2, f_3\}$

$S(f_1, f_3) = \frac{x^3yz}{z}(x^2y + z) - \frac{x^3yz}{x^3y}(x^3y - y) = x^5y^2 + yz$

Note that $yz + x^5y^2 = y(z + x^2y) + (x^5y^2 - x^2y^2)$

$x^5y^2 - x^2y^2 = x^2y(x^3y - y)$

Therefore, since $S(f_1, f_3) = yf_1 + x^2yf_3$, $S(f_1, f_3) \xrightarrow{G}_+ 0 = h$

Step 3.

Choose $\{f_2, f_3\}$.

$\mathcal{G} := \emptyset$

$S(f_2, f_3) = \frac{x^3yz}{xz}(xz + y) - \frac{x^3yz}{x^3y}(x^3y - y) = x^2y^2 + yz = yf_1$

Thus, $S(f_2, f_3) \xrightarrow{G}_+ 0 = h$

The algorithm ends, $G = \{f_1, f_2, f_3\}$ *is our desired Gröbner basis.*

The following example shows that the algorithm is sensitive to the term order chosen. That is, for the same input of generators $\{f_1, \ldots, f_s\}$, we may get different Gröbner basis outputs, depending on the term order.

Example 9. ([1], Problem 1.7.3(a))

Let f_1, f_2 *be as above but let the term order be deglex,* $x > y > z$.

INITIALIZATION: $G := \{f_1, f_2\}$, $\mathcal{G} := \{\{f_1, f_2\}\}$

Step 1.

Choose $\{f_2, f_1\}$.

$\mathcal{G} := \emptyset$

$S(f_2, f_1) = \frac{x^2yz}{xz}(xz + y) - \frac{x^2yz}{x^2y}(x^2y + z) = xy^2 - z^2 = h$, *which is reduced with respect to* G *since* $lp(f_1) = x^2y$, $lp(f_2) = xz$

Since $h \neq 0$, *let* $f_3 := xy^2 - z^2$ *(Note that* $lp(f_3) = xy^2$*)*

$\mathcal{G} := \{\{f_1, f_3\}\{f_2, f_3\}\}$

$G := \{f_1, f_2, f_3\}$

Step 2.

Choose $\{f_1, f_3\}$.

$\mathcal{G} := \{\{f_2, f_3\}\}$

$S(f_1, f_3) = \frac{x^2y^2}{x^2y}(x^2y + z) - \frac{x^2y^2}{xy^2}(xy^2 - z^2) = xz^2 + yz = zf_2$

So, $S(f_1, f_3) \xrightarrow{G}_+ 0 = h$

Step 3.

Choose $\{f_2, f_3\}$.

$\mathcal{G} := \emptyset$

$S(f_2, f_3) = \frac{xy^2z}{xz}(xz + y) - \frac{xy^2z}{xy^2}(xy^2 - z^2) = y^3 + z^3 = h$, *which is reduced with respect to* G.

Since $h \neq 0$, *let* $f_4 := y^3 + z^3$ *(Note that* $lp(f_4) = y^3$*)*

$\mathcal{G} := \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$

$G := \{f_1, f_2, f_3, f_4\}$

Step 4.

Choose $\{f_4, f_1\}$.

$\mathcal{G} := \{\{f_2, f_4\}, \{f_3, f_4\}\}$

$S(f_4, f_1) = \frac{x^2y^3}{y^3}(y^3 + z^3) - \frac{x^2y^3}{x^2y}(x^2y + z) = x^2z^3 - y^2z = (xz^2 - yz)f_2$

So $S(f_4, f_1) \xrightarrow{G}_+ 0 = h$

Step 5.

Choose $\{f_4, f_2\}$.

$\mathcal{G} := \{\{f_3, f_4\}\}$

$S(f_4, f_2) = \frac{xy^3z}{y^3}(y^3 + z^3) - \frac{xy^3z}{xz}(xz + y) = xz^4 - y^4$

Note that $xz^4 - y^4 = z^3(xz + y) + (-y^4 - yz^3)$

$-y^4 - yz^3 = -y(y^3 + z^3)$

Therefore, since $S(f_4, f_2) = z^3f_2 - yf_4$, $S(f_4, f_2) \xrightarrow{G}_+ 0 = h$

Step 5.

Choose $\{f_4, f_3\}$.

$\mathcal{G} := \emptyset$

$S(f_4, f_3) = \frac{xy^3}{y^3}(y^3 + z^3) - \frac{xy^3}{xy^2}(xy^2 - z^2) = xz^3 + yz^2 = z^2f_2$

So, $S(f_4, f_3) \xrightarrow{G}_+ 0 = h$

The algorithm ends, $G = \{f_1, f_2, f_3, f_4\}$ *is our desired Gröbner basis.*

Moreover, we point out that even in the event that the term order is fixed, uniqueness of Gröbner bases is not guaranteed. Buchberger's Algorithm can produce different Gröbner bases if different f_i are chosen at a given step. In order to achieve uniqueness, one needs to restrict Gröbner bases as follows (see [1]):

Definition 14. *A Gröbner basis $G = \{g_1, \ldots, g_t\}$ is called* ***minimal*** *if for all i, $\mathrm{lc}(g_i)$=1 and for all $i \neq j$, $\mathrm{lp}(g_i)$ does not divide $\mathrm{lp}(g_j)$.*

Definition 15. *A Gröbner basis $G = \{g_1, \ldots, g_t\}$ is called a* ***reduced*** *Gröbner basis if, for all i, $\mathrm{lc}(g_i)$=1 and g_i is reduced with respect to $G - \{g_i\}$. That is, for all i, no non-zero term in g_i is divisible by any $\mathrm{lp}(g_j)$ for any $j \neq i$.*

Under the above, we have:

Theorem 4. *Fix a term order. Then every non-zero ideal I has a unique reduced Gröbner basis with respect to this term order.*

4.0.1 A NOTE ON THE IMPLEMENTATION OF THE ALGORITHM

Finally, we would like to mention that algorithms, such as Buchberger's, to compute Gröbner bases for an ideal have been widely implemented in professional computer algebra systems. The author of this report is more familiar with the MAPLE system which has been used for the computations of examples in the rest of the paper.

We will not discuss the issue of complexity of the algorithm in this report. Some references that can be checked in this regard are [1], [5], [8], [9].

CHAPTER 5
APPLICATIONS OF GRÖBNER BASES

In the remainder of this report, we outline some of the ways Gröbner bases can be used to solve problems in polynomial ideal theory, solving systems of polynomial equations, and integer programming.

5.1 IDEAL THEORETIC APPLICATIONS

5.1.1 IDEAL MEMBERSHIP

The ideal membership problem consists in determining, given a polynomial $f \in k[x_1, \ldots, x_n]$ and an ideal $I \subset k[x_1, \ldots, x_n]$, whether $f \in I$.

So, fix a term order and let $G = \{g_1, \ldots, g_t\} \subseteq I$ be a Gröbner basis for I. To solve this problem, we use one of the characterizations of a Gröbner basis, which we previously called Theorem 3(ii):

$$f \in I \text{ if and only if } f \xrightarrow{G}_+ 0.$$

The process of determining ideal membership is greatly simplified by the use of a computer algebra system. For the remaining examples, we outline the method of solution and provide the corresponding MAPLE code instead of explicitly showing all computations, as was done in the previous examples.

Example 10. ([4], Problem 19, p.332)
Consider $I = \langle -x^3 + y, x^2y - y^2 \rangle$ *and* $f = x^6 - x^5y$. *We show that* $f \in I$.
Fix the term order to be lex, $x > y$. *We first compute the reduced Gröbner basis* G *of* I *using the following MAPLE code:*

```
with(Groebner):
Ideal:=[-x^3+y,x^2*y-y^2]:
G:=gbasis(Ideal,plex(x,y));
```

We get

G:=[$y^3 - y^2, -y^2 + xy^2, x^2y - y^2, x^3 - y$]

Next, we reduce f modulo G:

```
f:=x^6-x^5*y:
normalf(f,G,plex(x,y));
```

MAPLE returns the value 0. So, we conclude that $f \in I$.

Example 11. *Consider $I = \langle x^3 - xy + y^2, x + y^2 \rangle$ and $f = x^6y^2 - 2x^3y^3 + xy^2 + x - y$. We show that $f \notin I$.*
Fix the term order to be degrevlex, $y > x$. The reduced Gröbner basis G is computed as follows:

```
with(Groebner):
Ideal:=[x^3-x*y+y^2,x+y^2]:
G:=gbasis(Ideal,tdeg(y,x));
```

We get

G:=[$x + y^2, x^3 - xy - x$]

Now, we reduce f modulo G:

```
f:=x^6*y^2-2*x^3*y^3+x*y^2+x-y:
normalf(f,G,tdeg(y,x));
```

The result is

$3x^2y - 5xy + 2x^2 - y - 2x$

and so we conclude that $f \notin I$.

5.1.2 EQUALITY OF IDEALS

Another question that arises in the study of polynomial ideals is: given ideals $I, J \in k[x_1, \ldots, x_n]$, determine whether $I = J$, $I \subset J$ or $J \subset I$.

To solve the question of whether $I = J$, Theorem 4 can be used as follows:

Fix a term order. Then every non-zero ideal I has a unique reduced Gröbner basis with respect to this term order. Therefore, if I and J have the same reduced Gröbner basis, they must be equal.

Now, if I and J do not have the same reduced Gröbner basis, then they are not equal but one could be a subset of the other, that is, either $I \subset J$ or $J \subset I$, but not both.

The question of determining whether $I \subset J$ or $J \subset I$ can be answered by solving the question of ideal membership. We now give a criterion, which is a clear consequence of the preceding discussions, to see if $I \subset J$:

Lemma 1. *$I = \langle f_1, \ldots, f_s \rangle \subset J$ if and only if $f_1, \ldots, f_s \in J$.*

We illustrate with some examples.

Example 12. ([4], Problem 23, p.333)
Let

$$\begin{aligned} I &= \langle x^2y + xy^2 - 2y, x^2 + xy - x + y^2 - 2y, xy^2 - x - y + y^3 \rangle \text{ and} \\ J &= \langle x - y^2, xy - y, x^2 - y \rangle \end{aligned}$$

We show that $I = J$. Fix the term order to be lex, $x > y$.
The reduced Gröbner basis of I is given by

```
with(Groebner):
IdealI:=[x^2*y+x*y^2-2*y,x^2+x*y-x+y^2-2*y,x*y^2-x-y+y^3]:
GI:=gbasis(IdealI,plex(x,y));
```

The MAPLE output is

GI:=[$y^2 - y, x - y$]

The reduced Gröbner basis of J is given by

```
with(Groebner):
IdealJ:=[x-y^2,x*y-y,x^2-y]:
```

```
GJ:=gbasis(IdealJ,plex(x,y));
```

The MAPLE output is

GJ:=$[y^2 - y, x - y]$

Since I and J have the same reduced Gröbner basis, $I = J$.

Example 13. *Consider the ideals*

$$\begin{aligned} I &= \langle x^2 + xz, y + y^4 + xz^2 - 3z, y + 2x^2y^2 + xz^2 \rangle \text{ and} \\ J &= \langle x^3 + yz + xy, xyz + 2y^2z^2 - 3x, x^3y - z^2 \rangle \end{aligned}$$

Fix the term order to be degrevlex, $y > z > x$. First, we find the reduced Gröbner basis of I, which we call GI.

```
with(Groebner):
IdealI:=[x^2+x*z,y+y^4+x*z^2-3*z,y+2*x^2*y^2+x*z^2]:
GI:=gbasis(IdealI,tdeg(y,z,x));
```

The result is

GI:=$[x^2 + xz, z^2 - x^2, xy + zy, 2x^2y^2 + x^3 + y, y^4 + x^3 + y - 3z, 4x^5 + x^4 - 2y^3 + 4x^2y + 12x^3 + xy]$

Next, we find the reduced Gröbner basis of J, denoted GJ.

```
with(Groebner):
IdealJ:=[x^3+y*z+x*y,x*y*z+2*y^2*z^2-3*x,x^3*y-z^2]:
GJ:=gbasis(IdealJ,tdeg(y,z,x));
```

The result is

GJ:=$[x^3+zy+xy, 2z^3-zyx-2xz^2+2x^2z+2zy+3x, z^2+zy^2+xy^2, x^2y^2+x^2z+zy, 2y^3x + 2x^2z^2 + 4z^2y - 4xy^2 - z^2 - 3xz + 3x^2]$

Since $GI \neq GJ$, $I \neq J$.

Let us check if $I \subset J$. If $I \subset J$, then the generators of I are members of J.

Equivalently, if

$$x^2 + xz \xrightarrow{GJ}_+ 0$$

$$y + y^4 + xz^2 - 3z \xrightarrow{GJ}_+ 0$$

$$y + 2x^2y^2 + xz^2 \xrightarrow{GJ}_+ 0$$

then $I \subset J$.

Computing the reductions on MAPLE:

```
normalf(x^2+x*z,GJ,tdeg(y,z,x));
normalf(y+y^4+x*z^2-3*z,GJ,tdeg(y,z,x));
normalf(y+2*x^2*y^2+x*z^2,GJ,tdeg(y,z,x));
```

We get

$$x^2 + xz$$

$$y + y^4 + xz^2 - 3z$$

$$y + xz^2 - 2x^2z - 2zy$$

We conclude that $I \not\subset J$.

Now, we check whether $J \subset I$. *If* $J \subset I$, *then the generators of* J *must all reduce to 0 modulo* GI.

We compute the reductions on MAPLE:

```
normalf(x^3+y*z+x*y,GI,tdeg(y,z,x));
normalf(x*y*z+2*y^2*z^2-3*x,GI,tdeg(y,z,x));
normalf(x^3*y-z^2,GI,tdeg(y,z,x));
```

The output is

$$x^3$$

$$-3x - x^3 - y - x^2y$$

$$x^3y - x^2$$

So, J is not a subset of I.

5.1.3 RADICAL MEMBERSHIP

We will see in this section that radical membership reduces to ideal membership. Before we do this, let us define the radical of an ideal.

Definition 16. *Let I be an ideal of $k[x_1, \ldots, x_n]$. The **radical** of I, denoted $\sqrt{I}$, is defined as*

$$\sqrt{I} = \{f \in k[x_1, \ldots, x_n] \mid \textit{there exists } e \in \mathbb{N} \ \textit{ such that } \ f^e \in I\}.$$

The reader can easily verify that $\sqrt{I}$ is indeed an ideal. We next state a criterion, based on Hilbert's Nullstellensatz, to determine whether $f \in \sqrt{I}$. For a proof, see [1].

Theorem 5. *Let $I = \langle f_1, \ldots, f_k \rangle$ be an ideal in $k[x_1, \ldots, x_n]$. Then $f \in \sqrt{I}$ if and only if $1 \in \langle f_1, \ldots, f_s, 1 - wf \rangle \subseteq k[x_1, \ldots, x_n, w]$, where w is a new indeterminate.*

In particular, if $1 \in \langle f_1, \ldots, f_s, 1 - wf \rangle$, then $f \in \sqrt{I}$. So we can apply the ideal membership techniques to the problem of whether $1 \in \langle f_1, \ldots, f_s, 1 - wf \rangle$ in order to solve the problem of radical membership. Consequently, a method of solution would be to first find the reduced Gröbner basis G of $\langle f_1, \ldots, f_s, 1 - wf \rangle$. Then we must determine whether 1 reduces to 0 modulo G. In the process we can also find the smallest $e \in \mathbb{N}$ such that $f^e \in I$. This is illustrated in the next example.

Example 14. *Let*

$$\begin{aligned} f_1 &= x^4y^2 + z^2 - 4xy^3z - 2y^5z \\ f_2 &= x^2 + 2xy^2 + y^4 \\ f &= yz - x^3 \end{aligned}$$

Consider $I = \langle f_1, f_2 \rangle \subseteq \mathbb{Q}[x, y, z]$. We show that $f \in \sqrt{I}$.

We must check whether $1 \xrightarrow{G_w}_+ 0$, *where* G_w *is the reduced Gröbner basis of* $\langle f_1, f_2, 1 - wf\rangle$.

Computing the reduced Gröbner basis for this ideal under the lexicographical order, $x > y > z > w$, *we have:*

```
f1:=x^4*y^2+z^2-4*x*y^3*z-2*y^5*z:
f2:=x^2+2*x*y^2+y^4:
f:=y*z-x^3:
with(Groebner):
WIdeal:=[f1,f2,1-w*f]:
G_w:=gbasis(WIdeal,plex(x,y,z,w));
```

The output is

```
G_w:=[1]
```

Clearly, $1 \xrightarrow{G_w}_+ 0$, *so* $1 \in \langle f_1, f_2, 1 - wf\rangle$ *which means that* $f \in \sqrt{I}$.

This means $f^e \in I$ *for some* e. *We will find this* e *by observing that* $f^e \in I$ *if and only if* $f^e \xrightarrow{G}_+ 0$, *where* G *is the reduced Gröbner basis for the ideal* I. *The following MAPLE code gives us* G:

```
with(Groebner):
Ideal:=[f1,f2]:
G:=gbasis(Ideal,plex(x,y,z));
```

The output is

$$\texttt{G:=[}z^3 + 3y^5z^2 + 3zy^{10} + y^{15}, y^{12} + 4z^2x + 4y^5zx + 6y^7z + 5y^2z^2, -z^2 + 4xy^3z + 2y^5z + 4xy^8 + 3y^{10}, x^2 + 2xy^2 + y^4\texttt{]}$$

Now we reduce f,f^2, f^3, ... *modulo* G, *and the first instance in which this reduction is 0, then we will have found the desired* e *(note that the way* e *is computed guarantees it is the smallest one). First, we compute* $f^i \xrightarrow{G}_+ 0$ *for* $i = 1, 2, 3$.

```
normalf(f,G,plex(x,y,z));
```

```
normalf(f^2,G,plex(x,y,z));
normalf(f^3,G,plex(x,y,z));
```

The MAPLE output is

$$yz - 3xy^4 - 2y^6$$
$$-\frac{1}{2}y^2z^2 - y^7z - \frac{1}{2}y^{12}$$
$$0$$

Thus, $f^3 \in I$.

In the next example we try to bound the value of e instead of reducing each of f, f^2, f^3, ... modulo G systematically.

Example 15. *Let*

$$\begin{aligned} f_1 &= y^5 - x^{15}y^2 \\ f_2 &= x^{40} \\ f &= x^2y^4 + 3y \end{aligned}$$

We show that $f \in \sqrt{\langle f_1, f_2 \rangle}$.

Computing the reduced Gröbner basis for the ideal $\langle f_1, f_2, 1 - wf \rangle$ *under lex,* $w > x > y$, *we have:*

```
with(Groebner):
f1:=y^5-x^15*y^2:
f2:=x^40:
f:=x^2*y^4+3*y:
G_w:=gbasis([f1,f2,1-w*f],plex(w,x,y));
```

The output is

```
G_w:=[1]
```

So, $f \in \sqrt{I}$. In other words, $f^e \in \langle f_1, f_2 \rangle$ for some $e \in \mathbb{N}$. The reduced Gröbner basis G of this ideal, using lex, $y > x$, is given by

```
with(Groebner):
G:=gbasis([f1,f2],plex(y,x));
```

The output shows that $\{f_1, f_2\}$ is already a reduced Gröbner basis:

G:=[$y^5 - x^{15}y^2, x^{40}$]

Observe that the lowest power of x that occurs in f_1,f_2 is 15, and the lowest for y is 2. Since lp(f)=x^2y^4, e has to be at least 8. So we start with $e = 8$:

```
normalf(f^8,G,plex(y,x));
```

The output is $6561y^2x^{30} \neq 0$. Now try $e = 9$, $e = 10$ and $e = 11$.

```
normalf(f^9,G,plex(y,x));
normalf(f^10,G,plex(y,x));
normalf(f^11,G,plex(y,x));
```

The outputs are

$19683y^3x^{30}$

$59049x^{30}y^4$

0

Thus, $f^{11} \in \langle f_1, f_2 \rangle$, and $e = 11$ is the lowest such exponent.

5.2 SOLVING SYSTEMS OF POLYNOMIAL EQUATIONS

Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. In this section, our aim is to solve the system

$$\begin{aligned} f_1 &= 0 \\ &\vdots \\ f_s &= 0 \end{aligned} \tag{5.1}$$

We seek solutions $(a_1, \ldots, a_n) \in \overline{k}^n$ where $\overline{k}$ is the algebraic closure of k. Before we actually begin to search for solutions, we need to determine whether the system has any solutions. The following theorem gives a criterion to that effect. For a proof, see [1]. Here, $G = \{g_1, \ldots, g_t\}$ is the reduced Gröbner basis of $\langle f_1, \ldots, f_s \rangle$.

Theorem 6. ([1], p.63) *There are no solutions to the system $f_1 = 0, f_2 = 0, \ldots, f_s = 0$ in $\overline{k}^n$ if and only if $G = \{1\}$.*

Definition 17. *Consider the ideal $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$. If (5.1) has finitely many solutions, we say the ideal $\langle f_1, \ldots, f_s \rangle$ is **zero-dimensional**.*

Theorem 7. ([1], Theorem 2.2.7) *$\langle f_1, \ldots, f_s \rangle$ is zero-dimensional if and only if for every $i = 1, \ldots, n$, there exists $j \in \{1, \ldots, t\}$ such that $\mathrm{lp}(g_j) = x_i^\nu$ for some $\nu \in \mathbb{N}$.*

Now, suppose we have a system of linear polynomial equations:

$$\begin{aligned} f_1 &= 0 \\ &\vdots \\ f_s &= 0 \end{aligned}$$

This system can be solved by Gaussian elimination: write the system as

$$M \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

where M is the coefficient matrix corresponding to the system. Transform M into row echelon form by elementary row operations and then use back-substitution to solve for $x_1, \ldots, x_n$.

Note that in Gaussian elimination we are eliminating variables so that we work with a simpler system of equations with same solution set as the original one. We would like to have a device similar to Gaussian elimination for a system of nonlinear multivariate polynomials. The next statement guarantees we can do this provided

(i) $I = \langle f_1, \ldots, f_s \rangle$ is zero-dimensional.

(ii) We use the lexicographical term order.

Theorem 8. ([1], p.65) *Let I be a zero-dimensional ideal and G be the reduced Gröbner basis for I with respect to the lex term order with $x_1 < x_2 < \cdots < x_n$. Then we can order $g_1, \ldots, g_t$ such that g_1 contains only the variable x_1, g_2 contains only the variables x_1 and x_2 and $\mathrm{lp}(g_2)$ is a power of x_2, g_3 contains only the variables x_1, x_2 and x_3 and $\mathrm{lp}(g_3)$ is a power of x_3, and so forth until g_n.*

In other words, if I is zero-dimensional for the lexicographical order, then the situation is similar to the linear case: g_1 contains only x_1, so we solve $g_1 = 0$ for x_1 and substitute into g_2, then g_2 contains only x_2, and so on.

Example 16. ([2], Problem 12, p.113) *We want to solve*

$$f_1 = x^2 + yz + x = 0$$
$$f_2 = z^2 + xy + z = 0$$
$$f_3 = y^2 + zx + y = 0$$

To that end, fix the term order to be lex, $x > y > z$. We first find the Gröbner basis of $\langle f_1, f_2, f_3 \rangle$:

```
f1:=x^2+y*z+x:
f2:=z^2+x*y+z:
f3:=y^2+z*x+y:
with(Groebner):
Ideal:=[f1,f2,f3]:
G:=gbasis(Ideal,plex(x,y,z));
```

The output is

G:=[$z^2 + 3z^3 + 2z^4, 2z^3y + 2yz^2 + z^3 + z^2, -2yz^2 - yz - z^2 - z + y^2 + y, zx + 2yz^2 +$
$yz + z^2 + z, z^2 + yx + z, x^2 + yz + x$]

Note that the first polynomial in G is entirely in z. The third contains only z and y and its leading power product is y^2. The last polynomial contains x, y, and z and its leading power product is x^2. These make the ideal $\langle f_1, f_2, f_3 \rangle$ zero dimensional.

Now we must solve the following system:

$$\begin{aligned} z^2 + 3z^3 + 2z^4 &= 0 \\ 2z^3y + 2yz^2 + z^3 + z^2 &= 0 \\ -2yz^2 - yz - z^2 - z + y^2 + y &= 0 \\ zx + 2yz^2 + yz + z^2 + z &= 0 \\ z^2 + yx + z &= 0 \\ x^2 + yz + x &= 0 \end{aligned}$$

The first equation implies that z is either 0, $-\frac{1}{2}$, or -1.

If $z = 0$, our system becomes

$$\begin{aligned} y^2 + y &= 0 \\ yx &= 0 \\ x^2 + x &= 0 \end{aligned}$$

We notice by simple examination that the set $\{y^2 + y, yx, x^2 + x\}$ is already a reduced Gröbner basis of the ideal it generates, namely $\langle y^2 + y, yx, x^2 + x \rangle$, as no leading power product of a polynomial in the set divides a term in the remaining polynomials. We confirm this fact with Maple:

```
with(Groebner):
gbasis([y^2+y,y*x,x^2+x],plex(x,y));
```

The output is

$y^2 + y, yx, x^2 + x$

So we are left to solve

$$\begin{aligned} y^2 + y &= 0 \\ yx &= 0 \\ x^2 + x &= 0 \end{aligned}$$

The first equation implies that y *is either* 0 *or* -1*. If* $y = 0$ *then* $x^2 + x = 0$ *which implies that* $x = 0$ *or* $x = -1$*. If* $y = -1$ *then we have the system*

$$\begin{aligned} -x &= 0 \\ x^2 + x &= 0 \end{aligned}$$

The only solution is $x = 0$*.*

Our solutions so far are $(0, 0, 0)$*,* $(-1, 0, 0)$*,* $(0, -1, 0)$*.*

If $z = -1$*, our system becomes*

$$\begin{aligned} y^2 &= 0 \\ -x + 2y &= 0 \\ yx &= 0 \\ x^2 - y + x &= 0 \end{aligned}$$

We find the Gröbner basis of $\langle y^2, -x + 2y, yx, x^2 - y + x \rangle$*:*

```
with(Groebner):
gbasis([y^2,-x+2*y,y*x,x^2-y+x],plex(x,y));
```

The output is

y, x

We immediately have that $x = y = 0$*. So another solution is* $(0, 0, -1)$*.*

If $z = -\frac{1}{2}$, our system becomes

$$\begin{aligned} \frac{1}{4}y + \frac{1}{8} &= 0 \\ y^2 + y + \frac{1}{4} &= 0 \\ -\frac{1}{2}x - \frac{1}{4} &= 0 \\ yx - \frac{1}{4} &= 0 \\ x^2 + x - \frac{1}{2}y &= 0 \end{aligned}$$

We find the Gröbner basis of $\langle \frac{1}{4}y + \frac{1}{8}, y^2 + y + \frac{1}{4}, -\frac{1}{2}x - \frac{1}{4}, yx - \frac{1}{4}, x^2 + x - \frac{1}{2}y \rangle$*:*

```
with(Groebner):
gbasis([(1/4)*y+1/8,y^2+y+1/4,-(1/2)*x-1/4,y*x-1/4,x^2+x-(1/2)*y],plex(x,y));
```

The output is

$2y + 1, 2x + 1$

Immediately, we have that $x = y = -\frac{1}{2}$*. So our solution here is* $(-\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2})$*.*
Thus, all the solutions are $(0, 0, 0)$*,* $(-1, 0, 0)$*,* $(0, -1, 0)$*,* $(0, 0, -1)$*, and* $(-\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2})$*.*

5.3 INTEGER PROGRAMMING

For our last application we consider the following integer programming problem (see [1], 2.8.): Let $a_{ij} \in \mathbb{Z}$, $b_i \in \mathbb{Z}$, and $c_j \in \mathbb{R}$, with $i = 1, \ldots, n$ and $j = 1, \ldots, m$. We seek a solution $(\sigma_1, \sigma_2, \ldots, \sigma_m) \in \mathbb{N}^m$ of the system

$$\begin{array}{ccccccccc} a_{11}\sigma_1 & + & a_{12}\sigma_2 & + & \cdots & + & a_{1m}\sigma_m & = & b_1 \\ a_{21}\sigma_1 & + & a_{22}\sigma_2 & + & \cdots & + & a_{2m}\sigma_m & = & b_2 \\ & & & & \vdots & & & & \\ a_{n1}\sigma_1 & + & a_{n2}\sigma_2 & + & \cdots & + & a_{nm}\sigma_m & = & b_n \end{array} \qquad (\dagger)$$

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

In this paper, we will only consider the special case when the a_{ij}'s and b_i's are non-negative integers. For a more detailed discussion on the use of Gröbner basis techniques to solve integer programming problems the reader is referred to [1], as well as the expository papers [6] and [7].

The goal here is to find a solution to the system by first translating the problem into one about polynomials and then solving the polynomial problem by means of Gröbner basis techniques. A solution obtained in this way is then translated into a solution of the original problem.

To this end, n variables $x_1, \ldots, x_n$ and m variables $y_1, \ldots, y_m$ are introduced (note that n is the number of equations in the system and m the number of unknowns σ_i). Then the system (†) can be written as

$$x_i^{a_{i1}\sigma_1 + \cdots + a_{im}\sigma_m} = x_i^{b_i}, \text{ for } i = 1, \ldots, n. \qquad (\ddagger)$$

In turn, (‡) can be expressed as the single equation:

$$x_1^{a_{11}\sigma_1 + \cdots + a_{1m}\sigma_m} \cdots x_n^{a_{n1}\sigma_1 + \cdots + a_{nm}\sigma_m} = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$$

or, equivalently,

$$(x_1^{a_{11}} x_2^{a_{21}} \cdots x_n^{a_{n1}})^{\sigma_1} \cdots (x_1^{a_{1m}} x_2^{a_{2m}} \cdots x_n^{a_{nm}})^{\sigma_m} = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}.$$

Now consider the polynomial map

$$\phi : k[y_1, \ldots, y_m] \longrightarrow k[x_1, \ldots, x_n]$$

defined by

$$\phi(y_j) = x_1^{a_{1j}} x_2^{a_{2j}} \cdots x_n^{a_{nj}}.$$

Notice that $\phi(y_1^{\sigma_1} y_2^{\sigma_2} \cdots y_m^{\sigma_m}) = (x_1^{a_{11}} x_2^{a_{21}} \cdots x_n^{a_{n1}})^{\sigma_1} \cdots (x_1^{a_{1m}} x_2^{a_{2m}} \cdots x_n^{a_{nm}})^{\sigma_m}$.

The next statements provide an algorithm for determining solutions to our system.

Lemma 2. ([1], p.106) *There exists a solution* $(\sigma_1, \sigma_2, \ldots, \sigma_m) \in \mathbb{N}^m$ *if and only if the power product* $x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$ *is the image under* ϕ *of a power product in* $k[y_1, \ldots, y_m]$. *Moreover, if* $x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n} = \phi(y_1^{\sigma_1} y_2^{\sigma_2} \cdots y_m^{\sigma_m})$, *then* $(\sigma_1, \sigma_2, \ldots, \sigma_m) \in \mathbb{N}^m$ *is a solution.*

Lemma 3. ([1], p.107) *If $x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$ is in the image of ϕ, then it is the image of a power product $y_1^{\sigma_1}y_2^{\sigma_2}\cdots y_m^{\sigma_m} \in k[y_1,\ldots,y_m]$.*

The algorithm stemming from the proof of Lemma 3 ([1], p.107) is as follows:

1. Compute a Gröbner basis G for $K = \langle y_j - x_1^{a_{1j}}x_2^{a_{2j}}\cdots x_n^{a_{nj}} \mid j = 1,\ldots,m\rangle$ 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 power product $x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$ by G.
3. If $h \notin k[y_1,\ldots,y_m]$, then the system 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.

Example 17. *Consider the system*

$$\begin{aligned} 5\sigma_1 &+ \sigma_2 &+ 6\sigma_3 &= 35\\ \sigma_1 &+ 3\sigma_2 &+ 4\sigma_3 &= 21\\ 3\sigma_1 &+ 2\sigma_2 &+ \sigma_3 &= 12 \end{aligned}$$

and cost function $c(\sigma_1,\sigma_2,\sigma_3) = 100\sigma_1 + \sigma_2 + 5\sigma_3$.

We have the variables x_1 and x_2 for each equation and the variables y_1, y_2, and y_3 for each unknown. Also, $a_{11} = 5$, $a_{12} = 1$, $a_{13} = 6$, $a_{21} = 1$, $a_{22} = 3$, $a_{23} = 4$, $a_{31} = 3$, $a_{32} = 2$, $a_{33} = 1$, $b_1 = 35$, $b_2 = 21$, and $b_3 = 12$.

The map $\phi : \mathbb{Q}[y_1,y_2,y_3] \longrightarrow \mathbb{Q}[x_1,x_2,x_3]$ is defined as

$$\phi(y_1) = x_1^{a_{11}}x_2^{a_{21}}x_3^{a_{31}} = x_1^5x_2x_3^3$$

$$\phi(y_2) = x_1^{a_{12}}x_2^{a_{22}}x_3^{a_{32}} = x_1x_2^3x_3^2$$

$$\phi(y_3) = x_1^{a_{13}}x_2^{a_{23}}x_3^{a_{33}} = x_1^6x_2^4x_3$$

So $K = \langle y_1 - x_1^5x_2x_3^3, y_2 - x_1x_2^3x_3^2, y_3 - x_1^6x_2^4x_3\rangle$. We find the reduced Gröbner basis for K with respect to lex, $x_1 > x_2 > x_3 > y_1 > y_2 > y_3$, and we also find the remainder of the division of $x_1^{b_1}x_2^{b_2}x_3^{b_3} = x_1^{35}x_2^{21}x_3^{12}$:

```
with(Groebner):
G:=gbasis([y1-(x1)^5*(x2)*(x3)^3,y2-(x1)*(x2)^3*(x3)^2,y3-(x1)^6*(x2)^4*(x3)],
plex(x1,x2,x3,y1,y2,y3)):
normalf((x1)^35*(x2)^21*(x3)^12,G,plex(x1,x2,x3,y1,y2,y3));
```

The output, h, is

$(y1)^2 \ (y2) \ (y3)^4$

Thus, $\sigma_1 = 2$, $\sigma_2 = 1$, and $\sigma_3 = 4$ and the minimum of c is 221.

Note that in this example, we only had one solution so finding the minimum of c was trivial.

BIBLIOGRAPHY

[1] William W. Adams and Philippe Loustaunau. *An Introduction to Gröbner Bases*. American Mathematical Society, Providence, RI, 1994.

[2] Stephen R. Czapor. Gröbner Basis Methods for Solving Algebraic Equations. Ph.D. Thesis. University of Waterloo, Canada, 1988.

[3] Serge Lang. *Algebra*, Revised Third Edition. Springer-Verlag, New York, 2002.

[4] David S. Dummit and Richard M. Foote. *Abstract Algebra*, Third Edition. John Wiley and Sons, Inc., Hoboken, NJ, 2004.

[5] Franz Winkler. *Polynomial Algorithms in Computer Algebra*. Springer-Verlag Wien, New York, 1996.

[6] Rekha R. Thomas. A Geometric Buchberger Algorithm for Integer Programming. *Mathematics of Operations Research* **20** (1995): 864-884.

[7] Rekha R. Thomas. Applications to Integer Programming. *Proceedings of Symposia in Applied Mathematics* **53** (1998): 119-141.

[8] Dung T. Huynh. A Superexponential Lower Bound for Gröbner Bases and Church-Rosser Commutative Thue Systems. *Information and Control* **68** (1986): 196-206.

[9] David Bayer and Michael Stillman. On the Complexity of Computing Syzygies. *J. Symbolic Computation* **6** (1988): 135-147.