Applications of Groebner Bases

by

Syed Ali Abbas

BSc. (Physics-Mathematics) University of New Brunswick

A Report Submitted in Partial Fulfilment of
the Requirements for the Degree of

MASTER OF SCIENCE

in the Graduate Academic Unit of Mathematics and Statistics

Supervisor: Dr. Colin Ingalls, PhD, Math & Stats

ABSTRACT

Groebner bases were introduced by Bruno Buchberger in 1965 and they now comprise a major research area in computational algebra and computer science. In this report, I describe the Buchberger algorithm, which is used to compute Groebner bases, and I then present some of their interesting applications that have been developed since their introduction.

Table of Contents

Chapter 1: *Introduction*

1. What is a Groebner Basis?

A Groebner basis is a particular kind of generating subset of an ideal I in a polynomial ring R that possesses a particular type of useful properties. For example, given a set of polynomials A, and its Groebner Basis G, there is a fast algorithm that utilises the polynomials in G to determine whether or not another polynomial f is a combination of those in A. Furthermore, the set of polynomials in a Groebner basis has the same collection of roots as the original polynomials A.

I will show in Chapter 3 that, while the algorithm to find Groebner bases can be slow, all non-zero polynomial ideals do have Groebner bases. For linear functions in any number of variables, computing a Groebner basis is equivalent to performing Gaussian elimination.

The theory of Groebner bases was developed by Bruno Buchberger in 1965, who named them after his advisor Wolfgang Groebner.

Chapter 2: *Key Concepts and Definitions*

1. Ideals

In this section, I define *ideals*, the basic algebraic object that we will be working with for the rest of this report. These ideals will be in the polynomial ring $k[x_1,\cdots,x_n]$, where *k* is the field that we are working in (either real or complex numbers), and the x_i are the variables.

Definition 2.1.1. *A* **monomial** *in* $x_1,\cdots,x_n$ *is a product of the form*

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

were all exponents $\alpha_1,\cdots,\alpha_n$ *are non-negative integers. The* **total degree** *of this monomial is the sum* $\alpha_1+\cdots+\alpha_n$.

Definition 2.1.2. *A* **polynomial** f *in* $x_1,\cdots,x_n$ *with coefficients in k is a finite linear combination* (*with coefficients in k*) *of monomials. We will write a polynomial in f in the form*

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

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

Definition 2.1.3. *Let k be a field, and let* $f_1,\cdots,f_s$ *be polynomials in* $k[x_1,\cdots,x_n]$.

Then we set

$$V(f_1,\cdots,f_s)=\{(a_1,\cdots,a_n)\in k^n \mid f_i(a_1,\cdots,a_n)=0 \textit{ for all } 1\le i\le s\}.$$

We call $V(f_1,\cdots,f_s)$ *the* **affine variety** *defined by* $f_1,\cdots,f_s$.

Definition 2.1.4. A *subset* $I\subset k[x_1,\cdots,x_n]$ *is an* **ideal** *if it satisfies:*

(i) *0* $\in$ *I.*

(ii) *If f, g* $\in$ *I, then f + g* $\in$ *I.*

(iii) *If* $f\in I$ *and* $h\in k[x_1,\cdots,x_n]$, *then h f* $\in$ *I.*

A natural example of an ideal (and the one that I will primarily be working with) is the ideal generated by a finite number of polynomials. Later, in section 3.4, I will show that *all* ideals in polynomial rings of the form $k[x_1,\cdots,x_n]$ are generated by a finite number of polynomials.

Definition 2.1.5. *Let* $f_1, \ldots, f_s$ *be polynomials in* $k[x_1,\cdots,x_n]$. *Then we set*

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

It can be checked that $\langle f_1,\ldots,f_s\rangle$ is an ideal. We will call $\langle f_1,\ldots,f_s\rangle$ the **ideal generated by** $f_1, \ldots, f_s$.

2. Orderings on the Monomials in Polynomial Rings

In this section, I will define an ordering of terms in polynomials. The purpose behind this is to help us devise a multivariate polynomial division algorithm (an extension of the division algorithm for one variable), which I will describe explicitly in the next chapter.

When defining such an order, we would naturally want it to possess some or all of the properties of ordering that we observe in positive integers (for example, it should respect multiplication and well ordering).

But first, we note that we have a one-to-one correspondence between monomials in $k[x_1,\cdots,x_n]$ and n-tuples of non-negative integers (denoted by $\mathbf{Z}^n_{\geq 0}$**)**, where we can reconstruct the monomial $x^\alpha = x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ from the *n*-tuple of exponents $\alpha = (\alpha_1,\cdots,\alpha_n) \in \mathbf{Z}^n_{\geq 0}$. Using this correspondence, we can transfer an ordering $\alpha > \beta$ on $\mathbf{Z}^n_{\geq 0}$ to $k[x_1,\cdots,x_n]$.

Keeping this in mind, we define a monomial ordering in the following way.

Definition 2.2.1. *A* **monomial ordering** *on* $k[x_1,\cdots,x_n]$ *is any relation* $>$ *on* $\mathbf{Z}^n_{\geq 0}$, *or equivalently, any relation on the set of monomials* x^α, α $\in \mathbf{Z}^n_{\geq 0}$, *satisfying:*

(i) $>$ *is a total* (*or linear*) *ordering on* $\mathbf{Z}^n_{\geq 0}$.

(ii) *If $\alpha > \beta$ and $\gamma \in \mathbf{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$.*

(iii) *$>$ is a well-ordering on $\mathbf{Z}^n_{\geq 0}$. This means that every nonempty subset of $\mathbf{Z}^n_{\geq 0}$ has a smallest element under $>$.*

I now present some examples of ordering on *n*-tuples of integers that we will use later in this report.

Definition 2.2.2 (Lexicographic Order). *Let $\alpha = (\alpha_1,\ldots,\alpha_n)$, and $\beta = (\beta_1,\ldots,\beta_n) \in \mathbf{Z}^n_{\geq 0}$. We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in \mathbf{Z}^n$, the left-most nonzero entry is positive. We will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.*

For example:

a. $(2, 0, 1) >_{lex} (0, 3, 3)$ since $\alpha - \beta = (2, -3, -2)$.

b. $(1, 1, 4) >_{lex} (1, 1, 1)$ since $\alpha - \beta = (0, 0, 3)$.

c. Transferring to $k[x_1,\cdots,x_n]$, we see that the variables $x_1,\cdots,x_n$ are ordered in the usual way by the lex ordering:

$$(1, 0,\ldots, 0) >_{lex} (0, 1, 0,\ldots, 0) >_{lex} \ldots >_{lex} (0,\ldots, 0, 1)$$

So $x_1 >_{lex} x_2 >_{lex} \ldots >_{lex} x_n$.

This order is analogous to the ordering of words used in a dictionary, and hence the name.

For our second example, we deal with an order that also takes into account the total degree of each monomial. If we have any $\alpha \in \mathbf{Z}^n_{\geq 0}$, we say that $|\alpha| = \sum_{i=1}^{n} \alpha_i$, which gives us the total degree of the monomial x^{α}. Using this, we define the following order.

Definition 2.2.3 (Graded Lex Order). *Let α, β* $\in \mathbf{Z}^{n}_{\geq 0}$. *We say* $\alpha >_{grlex} \beta$ *if*

$$|\alpha| > |\beta|, \qquad \textit{or} \qquad |\alpha| = |\beta| \textit{ and } \alpha >_{lex} \beta.$$

A similar, but less intuitive, graded order is the graded reverse lexicographic order. One advantage of this order over the previous is that it is more efficient for computations for certain operations [CLOS, page 57].

Definition 2.2.4 (Graded Reverse Lex Order). *Let α, β* $\in \mathbf{Z}^{n}_{\geq 0}$. *We say* $\alpha >_{grevlex} \beta$ *if*

$$|\alpha| > |\beta|, \qquad \textit{or} \qquad |\alpha| = |\beta|$$

and, in $\alpha - \beta \in \mathbf{Z}^{n}$, *the right-most non-zero entry is negative.*

In order to see how these monomial orders apply to polynomials, we introduce the following terminology.

Definition 2.2.5. *Let* $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ *be a nonzero polynomial in* $k[x_1, \cdots, x_n]$ *and let* $>$ *be a monomial order.*

(i) *The* **multidegree** *of* f *is*

$$\text{multideg}(f) = \max(\alpha \in \mathbf{Z}^{n}_{\geq 0} : a_{\alpha} \neq 0)$$

(*the maximum is taken with respect to the assumed order* >).

(ii) *The* **leading coefficient** *of* f *is*

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

(iii) *The* **leading monomial** *of* f *is*

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

(*with coefficient 1, so its coefficient in f is suppressed*).

(iv) *The* **leading term** *of* f *is*

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

To illustrate this, let $f = -4x^2yz + 2z^3 + 5xy^4 + 7xyz^3 \in k[x, y, z]$. If we let > denote the lex order, then we have:

multideg(f) = (2, 1, 1), (corresponding to the monomial $-4x^2yz$)

$LC(f)$ = -4,

$LM(f) = x^2yz$,

$LT(f) = -4x^2yz$.

If we let > denote the grlex order, then:

multideg(f) = (1, 4, 0),

$LC(f)$ = 5,

$LM(f) = xy^4$,

$LT(f) = 5xy^4$.

By letting > denote the grevlex order, we get:

multideg(f) = (1, 4, 0),

$LC(f)$ = 5,

$LM(f) = xy^4$,

$LT(f) = 5xy^4$.

Chapter 3: *Buchberger's Algorithm*

1. *A Multivariable Polynomial Division Algorithm*

In order to compute the Groebner Basis of an ideal, we use a procedure called the **Buchberger Algorithm**. This algorithm utilizes a division algorithm in $k[x_1, \cdots, x_n]$ which extends the polynomial long division algorithm for $k[x]$. In the general case, our goal is to divide $f \in k[x_1, \cdots, x_n]$ by $f_1, \cdots, f_s \in k[x_1, \cdots, x_n]$, which expresses f in the form

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

where the "quotients" $a_1, \cdots, a_s$ and remainder r lie in $k[x_1, \cdots, x_n]$. We also want this remainder r to be as "small" as possible, and this is where the monomial ordering introduced in the previous section will apply.

Theorem 3.1.1. (Division Algorithm in $k[x_1, \cdots, x_n]$). *Fix a monomial order > on* $\mathbf{Z}^n_{\geq 0}$*, and let* $F = (f_1, \cdots, f_s)$ *be an ordered s-tuple of polynomials in* $k[x_1, \cdots, x_n]$*. Then every* $f \in k[x_1, \cdots, x_n]$ *can be written as*

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

where a_i, $r \in k[x_1, \cdots, x_n]$, *and either r* = 0 *or r is a k-linear combination 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 on division by F. Furthermore, if* $a_i f_i \neq 0$, *then we have*

$$\text{multideg}(f) \geq \text{multideg}(a_i f_i).$$

Proof. See [CLOS, page 63].

Example 3.1.2. Consider the case where $f = 3x^2y^3 - 2xy + y^2$, $f_1 = xy - x$ and $f_2 = y^2 + 3$. We will use the lex order with x > y. We set up our division as follows.

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

We notice that the leading term of f_1 divides the leading term of f, so we carry out this division, making sure to indicate which polynomial was the divisor. So we get:

a_1: $3xy^2 + 3xy + 3x$

a_2:

$$\begin{array}{r|l} xy - x & \overline{3x^2y^3 - 2xy + y^2} \\ y^2 + 3 & \underline{3x^2y^3 - 3x^2y^2} \\ & \qquad 3x^2y^2 - 2xy \\ & \qquad \underline{3x^2y^2 - 3x^2y} \\ & \qquad\qquad 3x^2y - 2xy \\ & \qquad\qquad \underline{3x^2y - 3x^2} \\ & \qquad\qquad\quad 3x^2 - 2xy + y^2 \end{array}$$

Now we notice that neither $LT(f_1)$ nor $LT(f_2)$ divides $LT(3x^2 - 2xy + y^2)$. However, $3x^2 - 2xy + y^2$ is *not* the remainder since $LT(f_1)$ divides $2xy$. Thus, we move $3x^2$ to the remainder and we continue dividing. This is something that never happens in the single-variable case.

Now we continue dividing. If we can divide by $LT(f_1)$ or $LT(f_2)$, we proceed as usual, and if neither divides, we move the leading term of the intermediate dividend to the remainder column. This gives us:

$a_1:\quad 3x^2y + 3xy + 3x - 2$

$a_2:\quad 1$

$$\begin{array}{l|l l}
xy - x & 3x^2y^3 - 2xy + y^2 & \\
y^2+3 & \underline{3x^2y^3 - 3x^2y^2} & \underline{\ r\qquad} \\
 & \qquad 3x^2y^2 - 2xy & \\
 & \underline{\qquad 3x^2y^2 - 3x^2y} & \\
 & \qquad\qquad 3x^2y - 2xy & \\
 & \qquad\qquad \underline{3x^2y - 3x^2} & \\
 & \qquad\qquad\quad \underline{3x^2 - 2xy + y^2} & \longrightarrow 3x^2 \\
 & \qquad\qquad\qquad -2xy + y^2 & \\
 & \qquad\qquad\qquad \underline{-2xy + 2x} & \\
 & \qquad\qquad\qquad\quad \underline{-2x + y^2} & \longrightarrow -2x \\
 & \qquad\qquad\qquad\qquad\quad y^2 & \\
 & \qquad\qquad\qquad\qquad\quad \underline{y^2 + 3} & \\
 & \qquad\qquad\qquad\qquad\qquad \underline{-3} & \longrightarrow -3
\end{array}$$

Thus, the remainder is $3x^2 - 2x - 3$, and we obtain:

$$3x^2y^3 - 2xy + y^2 = a_1(xy - x) + a_2(y^2 + 3) + 3x^2 - 2x - 3.$$

2. Monomial Ideals and Dickson's Lemma

In this section, I will describe monomial ideals, since these are what we will mostly be dealing with for the rest of this report. We then go on to study some of their properties.

Definition 3.2.1. *An ideal* $I \subset k[x_1, \cdots, x_n]$ *is a* **monomial ideal** *if there is a subset* $A \subset \mathbf{Z}^n_{\geq 0}$ *(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* $h_\alpha \in k[x_1, \cdots, x_n]$. *In this case, we write* $I = \left\langle x^\alpha \mid \alpha \in A \right\rangle$. *This is equivalent to saying that I can be generated by monomials.*

For some interesting applications of monomial ideals, in particular, their application in computing Hilbert polynomials, I refer the reader to [Sch].

The next theorem is a very important one as it shows that all monomial ideals of $k[x_1, \cdots, x_n]$ are finitely generated.

Theorem 3.2.2 (Dickson's Lemma). *A monomial ideal* $I = \left\langle x^\alpha \mid \alpha \in A \right\rangle \subset k[x_1, \cdots, x_\alpha]$ *can be written in the form* $I = \left\langle x^{\alpha(1)}, \cdots, x^{\alpha(s)} \right\rangle$, *where* $\alpha(1), \ldots, \alpha(s) \in A$. *In particular, I has a finite generating set of monomials.*

Proof. The proof is by induction on *n*, the number of variables. If *n* = 1, then *I* is generated by the monomials x^{α}, where $\alpha \in A \subset \mathbf{Z}_{\geq 0}$. Let β be the smallest possible element of $A \subset \mathbf{Z}_{\geq 0}$. Then x^{β} divides all the other generators, thus $I = \langle x^{\beta} \rangle$.

We now consider the case when *n* > 1. We assume that the theorem holds for *n* – 1. We can name the variables $x_1, x_2, \cdots, x_{n-1}, y$ which allows us to write the monomials in $k[x_1, x_2, \cdots, x_{n-1}, y]$ as $x^{\alpha} y^{m}$, where $\alpha = (\alpha_1, \cdots, \alpha_{n-1}) \in \mathbf{Z}_{\geq 0}^{n-1}$ and $m \in \mathbf{Z}_{\geq 0}$.

Suppose that $I \subset k[x_1, x_2, \cdots, x_{n-1}, y]$ is a monomial ideal. Let *J* be the ideal in $k[x_1, \cdots, x_{n-1}]$ generated by the monomials x^{α} for which $x^{\alpha} y^{m} \in I$ for some $m \geq 0$. Since J is a monomial ideal in $k[x_1, \cdots, x_{n-1}]$, the inductive hypothesis tells us that finitely many x^{α}'s generate J. Let's call them $x^{\alpha(1)}, \cdots, x^{\alpha(s)}$.

For each i between 1 and *s*, the definition of J tells us that $x^{\alpha(i)} y^{m_i} \in I$ for some $m_i \geq 0$. Let *m* be the largest of the m_i. Then, for each *k* between 0 and *m*-1, consider the ideal $J_k \subset k[x_1, \cdots, x_{n-1}]$ generated by the monomials x^{β} such that $x^{\beta} y^{k} \in I$. Again, the inductive hypothesis tells us that J_k has a finite generating set of monomials, say $J_k = \langle x^{\alpha_k(1)}, \cdots, x^{\alpha_k(s_k)} \rangle$.

I claim that I is generated by monomials in the following list:

from J: $x^{\alpha(1)} y^{m}, \cdots, x^{\alpha(s)} y^{m}$,

from J_0: $x^{\alpha_0(1)}, \cdots, x^{\alpha_0(s_0)}$,

from J_1: $x^{\alpha_1(1)} y, \cdots, x^{\alpha_1(s_1)} y$,

$\vdots$

from J_{m-1} : $x^{\alpha_{m-1}(1)}y^{m-1},\cdots,x^{\alpha_{m-1}(s_{m-1})}y^{m-1}$.

First we note that every monomial in I is divisible by one in the list. To see why, let $x^\alpha y^p \in I$. If $p \geq m$, then $x^\alpha y^p$ is divisible by one of the monomials in *J*. And if p < m, then $x^\alpha y^p$ is divisible by one of the monomials in J_p by their construction. Thus the above monomials generate an ideal having the same monomials as *I*, which forces the ideals to be the same. $x_1,\cdots,x_n$

Finally, we need to show that this finite set of generators can be chosen from a given set of generators for the ideal *I*. Switching back to writing the variables as $x_1,\cdots,x_n$, then our monomial ideal is $I = \left\langle x^\alpha \mid \alpha \in A \right\rangle$. We need to show that I is generated by finitely many of the x^α's where $\alpha \in A$. We've already shown that I = $\left\langle x^{\beta(1)},\cdots,x^{\beta(s)} \right\rangle$ for some monomials $x^{\beta(i)}$ in *I*, and, hence, $x^{\beta(i)}$ is divisible by some $x^{\alpha(i)}$ for some $\alpha(i) \in A$ since I is a monomial ideal. Thus we know that I $\subset$ $\left\langle x^{\alpha(1)},\cdots,x^{\alpha(s)} \right\rangle$. But at the same time, $\left\langle x^{\alpha(1)},\cdots,x^{\alpha(s)} \right\rangle$ $\subset I$ by the definition of *I*. Hence, I = $\left\langle x^{\alpha(1)},\cdots,x^{\alpha(s)} \right\rangle$, which completes the proof. □

3. Computing the Groebner Basis using the Buchberger Algorithm.

In this section we will completely answer the question of whether every ideal has a finite generating set. The answer is provided through the Hilbert basis theorem, which was first proved by David Hilbert in 1888. Using the result of this theorem, as well as the multivariate division algorithm and the properties of monomial ideals that we have studied in the previous sections, we will describe the Buchberger algorithm, which gives us a Groebner basis for any ideal in a polynomial ring.

First, for any ideal *I*, we can define its *ideal of leading terms* as follows.

Definition 3.3.1. *Let* $I \subset k[x_1, \cdots, x_n]$ *be an ideal other than* $\{0\}$.

(i) *We denote by* $LT(I)$ *the set of leading terms of elements of I. That is,*

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

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

We have already observed how leading terms play an important role in the multivariate division algorithm for polynomials. Now a question that naturally arises with this definition of an ideal of leading terms is: Given an ideal $I = \langle f_1,..., f_s \rangle$, does $\langle LT(I) \rangle = \langle LT(f_1),..., LT(f_s) \rangle$?

It is obvious that $LT(f_i) \in LT(I) \subset \langle LT(I) \rangle$ from the definition of $\langle LT(I) \rangle$, and this implies that $\langle LT(f_1),..., LT(f_s) \rangle \subset \langle LT(I) \rangle$, but as we shall see with the following example, the reverse inclusion is not necessarily true. That is, $\langle LT(I) \rangle$ can be strictly larger than $\langle LT(f_1),..., LT(f_s) \rangle$.

Example 3.3.2. Let $I = \langle f_1, f_2 \rangle$, where $f_1 = xy^2 + 3y^2$ and $f_2 = x^3 + 3x^2 + 1$, and we use the grlex ordering on monomials in $k[x, y]$. Then $y^2 \cdot f_2 - x^2 \cdot f_1 = y^2$. So is in *I*, and thus $y^2 = LT(y^2) \in LT(I)$. But y^2 is not divisible by $LT(f_1) = xy^2$, nor by $LT(f_2) = x^3$, so that $x^2 \notin \langle LT(f_1), LT(f_2) \rangle$. So in this particular case, we observe that $\langle LT(I) \rangle$ is strictly larger than $\langle LT(f_1),..., LT(f_s) \rangle$.

In this next proposition I will show that $\langle LT(I) \rangle$ is a monomial ideal, and hence it follows from Dickson's Lemma (discussed in the previous section) that it is generated by finitely many leading terms.

Proposition 3.3.3. *Let $I \subset k[x_1, \cdots, x_n]$ be an ideal. Then*

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

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

Proof. (*i*) The leading monomials *LM*(*g*) of elements $g \in I - \{0\}$ generate the monomial ideal $\langle LM(g) \mid g \in I - \{0\} \rangle$. Since *LM*(*g*) and *LT*(*g*) differ only by a nonzero constant, $\langle LM(g) \rangle = \langle LT(I) \rangle$. Thus $\langle LT(I) \rangle$ is a monomial ideal.

(*ii*) Since $\langle LT(I) \rangle$ is generated by monomials *LM*(*g*) for $g \in I - \{0\}$, Dickson's Lemma tells us that $\langle LT(I) \rangle = \langle LM(g_1), \cdots, LM(g_t) \rangle$ for finitely many $g_1, \ldots g_t \in I$. Since $LM(g_i)$ differs from $LT(g_i)$ by a nonzero constant, it follows that $\langle LT(I) \rangle = \langle LT(g_1), \cdots, LT(g_t) \rangle$. □

With this result, and the division algorithm, we can now prove that there exists a finite generating set for every polynomial ideal, thus answering the question put forward at the start of this section.

Theorem 3.3.4 (Hilbert Basis Theorem). *Every ideal* $I \subset k[x_1, \cdots, x_n]$ *has a finite generating set. That is,* $I = \langle g_1, \cdots, g_t \rangle$ *for some* $g_1, \ldots g_t \in I$.

Proof. If $I = \{0\}$, then $I = \langle 0 \rangle$. If I contains some nonzero polynomial, then we can construct a generating set $g_1, \ldots g_t$ for I as follows. Proposition 3.3.3 tells us that there exist $g_1, \ldots, g_t \in I$ such that $\langle LT(g_1), \ldots, LT(g_t) \rangle = \langle LT(I) \rangle$. I claim that I = $\langle g_1, \cdots g_t \rangle$.

It is clear that $\langle g_1, \cdots g_t \rangle \subset I$, since each $g_i \in I$. Conversely, let $f \in I$ be any polynomial. If we apply the division algorithm to divide f by $g_1, \ldots, g_t$, 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 divisible by none of $LT(g_1),\ldots,LT(g_t)$. I claim that $r = 0$, since if $r \neq 0$, then $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1),\ldots, LT(g_t) \rangle$. Thus r must be divisible by some $LT(g_i)$ and hence it cannot be a remainder, which is a contradiction.

Thus $f = a_1 g_1 + \cdots + a_t g_t + 0 \in \langle g_1, \cdots, g_t \rangle$, which shows that $I \subset \langle g_1, \cdots, g_t \rangle$. □

Corollary 3.3.5. *Every ascending chain of ideals $I_1 \subset I_2 \subset I_3 \cdots$ in a polynomial ring is eventually stationary. That is, there is some positive integer n such that $I_m = I_n$ for all $m > n$. This property of polynomial rings is referred to by the term,* **Noetherian**.

Proof. Let $I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_n \subset \cdots$ be an ascending chain of ideals in a polynomial ring R. Consider the set $I = \bigcup_{n=1}^{\infty} I_n$. Since the I_n are increasing, it is clear that I is an ideal of R. So, by the Hilbert Basis Theorem, $I = \langle g_1, \cdots, g_t \rangle$ for some $g_1, \cdots, g_t \in I$. Hence there exists N_i such that $g_i \in I_{N_i}$ for $i = 1, \cdots, t$. Let $N = \max_{1 \le i \le t} N_i$; then $g_i \in I_N$ for all $i = 1, \cdots, t$, and thus $I \subset I_N$. But $I_N \subset I$. Hence $I = I_N$.

In addition to answering the question that I posed earlier, we notice that the basis involved in the proof of the Hilbert basis theorem has the special (and desirable) property that $\langle LT(I) \rangle = \langle LT(g_1),\ldots, LT(g_t) \rangle$. As we had observed in Example 3.3.2 earlier, this is not always the case. We now give these special bases a name.

Definition 3.3.6. *Fix a monomial order. A finite subset* $G = \{g_1, \ldots, g_t\}$ *of an ideal I is said to be a* **Groebner basis** *of I if*

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

Less formally, we say that a set $\{g_1, \cdots, g_t\} \subset I$ is a Groebner basis of I if and only if the leading term of any element of I is divisible by one of the $LT(g_i)$. The proof for the Hilbert Basis Theorem shows us that this subset G has the crucial property, $I = \langle G \rangle$.

A consequence of the Hilbert Basis Theorem is that, since every ideal $I \subset k[x_1, \cdots, x_n]$ has a finite generating set of polynomials, it makes sense to speak of an affine variety defined by an ideal $I \subset k[x_1, \cdots, x_n]$.

Definition 3.3.7. *Let* $I \subset k[x_1, \cdots, x_n]$ *be an ideal. We will denote by* $V(I)$ *the set*

$$V(I) = \{(a_1, \cdots, a_n) \in k^n \mid f(a_1, \cdots, a_n) = 0 \textit{ for all } f \in I\}.$$

I can now prove the claim I had made in the introduction of this report, that the zero sets of an ideal and its Groebner basis are the same.

Proposition 3.3.8. *If* $I = \langle f_1, \cdots, f_s \rangle$, *then* $V(I) = V(f_1, \cdots, f_s)$.

Proof. Since the $f_i \in I$, if $f(a_1,\cdots,a_n) = 0$ for all $f \in I$, then $f_i(a_1,\cdots,a_n) = 0$. Hence $V(I) \subset V(f_1,\cdots,f_s)$. Conversely, let $(a_1,\cdots,a_n) \in V(f_1,\cdots,f_s)$ and let $f \in I$. Since $I = \langle f_1,\cdots,f_s \rangle$, we can write $f = \sum_{i=1}^{s} h_i f_i$ for some $h_i \in k[x_1,\cdots,x_n]$. Hence

$$f(a_1,\cdots,a_n) = \sum_{i=1}^{s} h_i(a_1,\cdots,a_n) f_i(a_1,\cdots,a_s) = \sum_{i=1}^{s} h_i(a_1,\cdots,a_n) \cdot 0 = 0.$$

Thus $V(f_1,\cdots,f_s) \subset V(I)$ and, hence, they are equal. □

Since $I = \langle G \rangle = \langle g_1,\cdots,g_t \rangle$ for any Groebner basis *G* of an ideal *I*, the above proposition proves that $V(I) = V(G)$.

Our final step before describing the Buchberger algorithm is to define the S-polynomial and an alternative definition of a Groebner basis.

Definition 3.3.9. *Let* $f, g \in k[x_1,\cdots,x_n]$ *be nonzero polynomials.*

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

(ii) *The* **S-polynomial** *of* f *and* g *is the combination*

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

So an S-polynomial *S*(*f*, *g*) in effect produces cancellation of the leading terms of f and g.

Theorem 3.3.10. *Let I be a polynomial ideal. Then a basis* $G = \{g_1,\cdots,g_t\}$ *for I is a Groebner basis for I if and only if for all pairs* $i \neq j$*, the remainder on division of* $S(g_i, g_j)$ *by G* (*listed in some order*) *is zero.*

Proof. $(\Rightarrow)$ If G is a Groebner basis, then the set of polynomials $\{g_1,\cdots,g_t\} \in G$ generate *I*. Hence the remainder on division of any polynomial in *I* by G is zero. And since $S(g_i, g_j) \in I$, the remainder on division of S(g_i, g_j) by *G* is zero.

For $(\Leftarrow)$, see [CLOS, page 84].

For the rest of this report, I will use the following notation.

Definition 3.3.11. *For any s-tuple* $F = (f_1,\cdots,f_s)$, *I define* $\overline{f}^F$ *as the remainder of* f *by F.*

We can now explicitly describe the Buchberger algorigthm.

Theorem 3.3.12. (Buchberger Algorithm). *Let* $I = \langle f_1,\ldots,f_s\rangle \neq \{0\}$ *be a polynomial ideal. Then a Groebner basis for I can be constructed in a finite number of steps by the following algorithm:*

```
Input: $F = (f_1,\ldots,f_s)$

Output: a Groebner basis $G = (g_1,\ldots,g_t)$ for $I$, with $F \subset G$

$G := F$

REPEAT
```

```
        $G' := G$
        FOR each pair $\{p, q\}$, $p \neq q$ in $G'$ DO
            $S := \overline{S(p,q)}^{G'}$
            IF $S \neq 0$ THEN $G := G \cup \{S\}$
    UNTIL $G = G'$.
```

Proof. I first show that $G \subset I$ at every stage of the algorithm. It is true initially, and we only change *G* by adding the remainder $S = \overline{S(p,q)}^{G'}$ where $p, q \in G$. Thus, since $S(p,q)$ is in *I*, and we're dividing by $G' \subset I$, we get $G \cup \{S\} \subset I$.

To see that the *G* we obtain when the algorithm terminates is actually a Groebner basis of *I* we note that the algorithm terminates when $G = G'$, which means that $\overline{S(p,q)}^{G} = 0$ for all $p, q \in G$. Hence *G* is a Groebner basis of $\langle G \rangle = I$ by Theorem 6.

To show that the algorithm terminates, we need to see what happens after each pass through the main loop. The set *G* consists of G' (the old *G*) together with nonzero remainders of S-polynomials of elements of G'. So, since $G' \subset G$, we have:

$$\langle LT(G') \rangle \subset \langle LT(G) \rangle \qquad (*)$$

Also, if $G' \neq G$, then $\langle LT(G') \rangle$ is strictly smaller than $\langle LT(G) \rangle$. To see this we consider the nonzero remainder *r* of an S-polynomial that has been adjoined to G'. Since *r* is a remainder on division by G', $LT(r)$ is not divisible by the leading terms of elements of G', and thus $LT(r) \notin \langle LT(G') \rangle$. But $LT(r) \in \langle LT(G) \rangle$, which proves the claim.

By (*) we see that the ideals $\langle LT(G')\rangle$ from successive iterations of the loop form an ascending chain of ideals in $k[x_1,\cdots,x_n]$. But since $k[x_1,\cdots,x_n]$ is Noetherian the chain must eventually stabilize, which means that eventually $G' = G$. So the algorithm does indeed terminate after a finite number of steps. □

Example 3.3.13. Consider $k[x,y]$ with grlex order, and let I = $\langle f_1, f_2\rangle =$ $\langle x^2y-1, xy^2-x\rangle$. Note that $\{f_1, f_2\}$ is not a Groebner basis for I since $LT(S(f_1, f_2))$ = $x^2 \notin \langle LT(f_1), LT(f_2)\rangle$.

So we have:

$G = (f_1, f_2)$

$S(f_1, f_2) = x^2 - y = f_3 \neq 0$

So we add f_3 to G. Repeating this process, we get:

$\overline{S(f_1, f_2)}^G = 0$, but

$\overline{S(f_1, f_3)}^G = y^2 - 1 \neq 0.$

Hence, we must add $f_4 = y^2 - 1$ to our generating set. If we let $G = \{f_1, f_2, f_3, f_4\}$ then

$\overline{S(f_1, f_2)}^G = \overline{S(f_1, f_3)}^G = 0,$

and $\overline{S(f_i, f_4)}^G = 0$ for all $1 \leq i \leq 4$.

Thus a Groebner basis for I is given by

$\{f_1, f_2, f_3, f_4\} = \{x^2y-1, xy^2-x, x^2-y, y^2-1\}$.

4. Minimal and Reduced Groebner Bases

The procedure outlined in Theorem 3.1.6 does give us a Groebner basis for a given polynomial ideal, but it is generally larger than necessary. However, there are some conditions that we can impose on the Groebner basis G so that the Groebner basis obtained is the smallest possible. For this, I introduce the concept of minimal and reduced Groebner bases.

Lemma 3.4.1. *Let G be a Groebner basis for the polynomial idea 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. We know that $\langle LT(G)\rangle = \langle LT(I)\rangle$. If $LT(p) \in \langle LT(G-\{p\})\rangle$, then $\langle LT(G-\{p\})\rangle = \langle LT(G)\rangle$. By definition it follows that G - $\{p\}$ is also a Groebner basis for *I*. □

We can now use the above lemma to define a minimal Groebner basis, which sets all leading coefficients to 1, and removes some unneeded generators.

Definition 3.4.2. *A* **minimal Groebner basis** *for a polynomial ideal I is a Groebner basis G for I such that:*

(i) $LC(p) = 1$ *for all* $p \in G$*, and*

(ii) For all $p \in G, LT(p) \notin \left\langle LT(G-\{p\}) \right\rangle$.

So applying Lemma 1 to the Groebner basis obtained at the end of the previous section, we obtain the following minimal Groebner basis for *I*.

$$\tilde{f}_3 = x^2 - y\,, \quad \tilde{f}_4 = y^2 - 1\,.$$

Unfortunately, a minimal Groebner basis is not unique. For example, another minimal Groebner basis for the same ideal is the following:

(1) $$\tilde{f}_3 = x^2 + ay^2 - y - a\,, \qquad \tilde{f}_4 = y^2 - 1\,.$$

where $a \in k$ is any constant. Fortunately, we can obtain a unique minimal Groebner basis that is smaller than all other.

Definition 3.4.3. *A* **reduced Groebner basis** *for a polynomial ideal I is a Groebner basis G for I such that:*

(i) $LC(p) = 1$ *for all* $p \in G$.

(ii) *For all* $p \in G$, *no monomial of* p *lies in* $\left\langle LT(G-\{p\}) \right\rangle$.

So for the minimal Groebner basis given in (1), setting $a = 0$ gives a *reduced Groebner basis.*

Proposition 3.4.4. *Let* $I \neq \{0\}$ *be a polynomial ideal. Then for a given monomial ordering, I has a unique reduced Groebner basis.*

Proof. Let G be a minimal Groebner basis for I. We say that $g \in G$ is reduced for G if no monomial of g is in $\langle LT(G-\{g\})\rangle$. Once all elements of G are modified in this manner, then G becomes a reduced Groebner basis.

We first note that if g is reduced for G, then g is also reduced for any other minimal Groebner basis of I that contains g, since the definition of reduced only involves the leading terms.

Now, given $g \in G$, let $g' = \overline{g}^{G-\{g\}}$, and define $G' = (G-\{g\}) \cup \{g'\}$. I claim that G' is a minimal Groebner basis for I. To see this, we first note that $LT(g') = LT(g)$, since dividing g by $G - \{g\}$ sends $LT(g)$ to the remainder as it is not divisible by any element of $LT(G - \{g\})$. This shows that $\langle LT(G')\rangle = \langle LT(G)\rangle$. Since G' is contained in I, we see that it is a Groebner basis, and minimal follows after making all the replacements. Also note that g' is reduced for G' by construction.

We apply this same process to all elements of G. The Groebner basis may change each time, but this does not change the reduced state of each element, since once an element is reduced, it stays reduced as we are not changing the leading terms. Thus we have a reduced Groebner basis.

To see that it is unique, suppose that G and G' are reduced Groebner bases for I. So they must also be minimal. This means that that $LT(G) = LT(G')$ since a monomial ideal has a unique minimal generating set of monomials. Thus given $g \in G$, there is $g' \in G'$ such that $LT(g') = LT(g)$. If we show that $g = g'$, then it follows that $G = G'$.

Consider $g - g'$. This is in I, and since G is a Groebner basis, it follows that $\overline{g-g'}^{G} = 0$. But $LT(g') = LT(g)$, hence these terms cancel in $g - g'$, while the remaining terms are divisible by none of $LT(G) = LT(G')$, since G and G' are reduced. This shows that $\overline{g - g'}^{G} = g - g' = 0$. Hence $g = g'$, and thus G is unique. □

As mentioned earlier, for a system of linear equations, computing the Groebner basis is equivalent to performing Gaussian elimination. Computing a *reduced* Groebner basis for a linear system, then, provides us with the reduced row echelon form of the augmented coefficient matrix of the linear system.

Chapter 4: *Applications*

1. Ideal Membership Problem

Given an ideal *I*, it is often of interest to determine whether a given polynomial *f* lies in *I* or not. By using our knowledge of Groebner bases and the Buchberger algorithm, this becomes a simple task. First, I will need to prove that that the remainder of f upon division by the elements of its Groebner basis is unique.

Proposition 4.1.1. *Let* $G = \{g_1, \cdots, g_t\}$ *be a Groebner basis for an ideal* $I \subset k[x_1, \cdots, x_n]$ *and let* $f \in I$. *Then there is a unique* $r \in k[x_1, \cdots, x_n]$ *with the following two properties:*

(i) *No term of r is divisible by one of the* $LT(g_1), \ldots, LT(g_t)$.

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

Proof. See [CLOS, page 81].

Note that though the remainder *r* is unique, the quotients need not be so. Listing the generators g_i in a different order in the division process can result in different values for the quotients. In any case, we can now state the following corollary that describes the criterion for when a polynomial lies in an ideal.

Corollary 4.1.2. *Let* $G=\{g_1,\cdots,g_t\}$ *be a Groebner basis for an ideal* $I\subset k[x_1,\cdots,$ $x_n]$ *and let* $f\in$ $k[x_1,\cdots,x_n]$. *Then* $f\in I$ if and only if $\overline{f}^G=0$.

Proof. ($\Leftarrow$**)** If $\overline{f}^G=0$ then, by definition, $f=a_1g_1+\cdots+a_tg_t$, hence the g_i generate f. That is $f\in\langle g_1,\cdots g_t\rangle$, and thus $f\in I$.

($\Rightarrow$) If $f\in I$, then $f=f+0$ satisfies the two conditions of the previous proposition. Hence $f=a_1g_1+\cdots+a_tg_t+0$, thus $\overline{f}^G=0$. □

So if we carry out the division algorithm on the polynomial f using the polynomials in *G*, then a zero remainder tells us that $f\in$ *I*. A nonzero remainder implies that $f\notin$ *I*.

Example 4.1.3. Let $I=\langle g_1,g_2\rangle$ = $\langle x^2y-1,xy^2-x\rangle\in$ $\mathbf{C}[x,y]$. Also let f = $3x^2y^2$ $+y^5-4y$. We would like to determine if $f\in I$.

So our first step is to compute a Groebner basis for *I*. Using the lex order, this gives us:

$$G=(f_1,f_2)=(x^2-y,y^2-1).$$

Dividing f by *G* gives:

$$f=3y^2\cdot f_1+(y^3+4y)\cdot f_2.$$

Since the remainder is 0, we see that $f\in I$.

2. Elimination

Another application of Groebner bases is that, given a system of polynomials (in several variables), we can use Groebner bases to systematically eliminate variables from this system of equations. The resulting polynomials, having fewer variables, are generally much easier to solve algebraically.

For example, consider the following system of equations:

$$\begin{aligned} &x^2+y^2+z^2=4, \\ &x^2+2y^2=5, \\ &xz=1. \end{aligned} \tag{1}$$

We define I to be the ideal

$$I=<f_1,f_2,f_3>=<x^2+y^2+z^2-4, x^2+2y^2-5, xz-1>. \tag{2}$$

Computing the Groebner basis for I (using lex order) gives us:

$$\begin{aligned} &g_1=x+2z^3-3z, \\ &g_2=y^2-z^2-1, \\ &g_3=2z^4-3z^2+1. \end{aligned} \tag{3}$$

So, by Proposition 3.3.8., the systems (1) and (3) will have the same set of solutions since they generate the same ideal. We notice here that g_3 is a polynomial in only one variable, so we manipulate it to obtain:

$$g_3=(2z^2-1)(z^2-1).$$

Setting it to zero, we see that the only possible *z's* are ± 1 and $\pm \frac{1}{\sqrt{2}}$. We can now substitute these values into g_2, which we notice is a polynomial in only y and z. This gives us the possible y's. Substituting these values into g_1 gives us all the solutions, which are:

$$(x, y, z) = \left\{\pm(1, \pm\sqrt{2}, 1), \pm(\sqrt{2}, \pm\sqrt{3/2}, 1/\sqrt{2})\right\}$$

This procedure helped us solve our original system of equations by employing two steps.

1 – We were able to obtain polynomials that had the same roots as that in our original equations, but with most of them having fewer variables (this was our **Elimination** step).

2 – Once we solved the simpler equation, we used the solutions to this to obtain our complete set of solutions (**Extension** step).

The basic idea behind *elimination theory* is that we can carry out these steps in general.

Definition 4.2.1. *Given* $I = \langle f_1, ..., f_s \rangle \subset k[x_1, \cdots, x_n]$, *the kth* **elimination ideal** I_k *is the ideal of* $k[x_{k+1}, \cdots, x_n]$ *defined by*

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

In this way, I_k contains all polynomials in I that have the variables $x_1, \ldots, x_k$ eliminated. This brings us to the Elimination Theorem which states the following.

Theorem 4.2.2 (The Elimination Theorem). *Let $I \subset k[x_1, \cdots, x_n]$ be an ideal. And let G be a Groebner basis of I with respect to lex order where $x_1 > x_2 > \ldots > x_n$. Then, for every $0 \le k \le n$, the set*

$$G_k = G \cap k[x_{k+1}, \cdots, x_n]$$

is a Groebner basis of the kth elimination ideal I_k.

Proof. Fix k between 0 and n and suppose that $G = \{g_1, \ldots, g_m\}$. Without loss of generality, we can assume that $G_k = \{g_1, \ldots, g_r\}$. I will first show that I_k is generated by G_k. Since $G_k \subset I_k$, we have $\langle g_1, \cdots, g_r \rangle \subset I_k$ since I_k is an ideal. Now using the division algorithm with the lex order, we divide any f in I_k by $g_1, \ldots, g_m$. We note that,

1. Since $G = \{g_1, \ldots, g_m\}$ is a Groebner basis of I and $f \in I$, the remainder of f on division by G is zero; and
2. Since we are using the lex order, the leading terms of $g_{r+1}, \cdots, g_m$ must involve one of $x_1, \cdots x_k$ and hence, are greater than every monomial in $f \in k[x_{k+1}, \cdots, x_n]$.

Thus, when applying the division algorithm, $g_{r+1}, \cdots, g_m$ will not appear and hence every f in I_k can be written as $f = h_1 g_1 + \cdots + h_r g_r + 0 \cdot g_{r+1} + \cdots + 0 \cdot g_m + 0$. This tells us that $f \in \langle g_1, \cdots, g_r \rangle$, which proves that G_k is generated by I_k. Note that this also shows that for any $f \in I_k$, $\overline{f}^{G} = \overline{f}^{G_k} = 0$.

Now to show that G_k is a Groebner basis, Theorem 3.3.10 tells us that it is sufficient to show that for all $1 \leq i < j \leq r$, the remainder of $S(g_i, g_j)$ on division by G_k is zero. But $S(g_i, g_j)$ lies in I_k since g_i and g_j do, thus the remainder of $S(g_i, g_j)$ on division by G_k is zero. Thus Theorem 3.3.10 confirms that G_k is a Groebner basis. This completes the proof of the Elimination Theorem. □

This tells us that the polynomial $g_3 \in G$ obtained in our example was not just some random way of eliminating x and y from equations f_1 through f_3 – it is the best possible way to do so, since any other polynomial that eliminates x and y is generated by g_3.

Using the elimination theorem we can obtain partial solutions $(a_{k+1}, \cdots, a_n)$ for our set of functions with variables $(x_1, \cdots, x_k)$ eliminated. Now to see which of these solutions extend to our complete set of functions, we use the *extension theorem.*

Theorem 4.2.3 (The Extension Theorem). *Let $I = \langle f_1, ..., f_s \rangle \subset \mathbf{C}[x_1, \cdots, x_n]$ and let I_1 be the first elimination ideal of I. For each $1 \leq i \leq s$, write f_i in the form*

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

where $N_i \geq 0$ and $g_i \in \mathbf{C}[x_2, \cdots, x_n]$ is nonzero. (We set $g_i = 0$ when $f_i = 0$.) Suppose that we have a partial solution $(a_2, \cdots, a_n)$ in the variety of I_1. If $(a_2, \cdots, a_n)$ is not in the variety of $g_1, ..., g_s \in G$, then there exists $a_1 \in \mathbf{C}$ such that $(a_1, \cdots, a_n)$ is in the variety of I.

Note that this theorem is only stated for the field k = **C**. It is false over **R** since the **R** is not an algebraically closed field.

Proof. See [CLOS, page 117].

For example, we consider the equations

$$xy = 1,$$

$$xz = 1.$$

We set $I = \langle xy - 1, xz - 1 \rangle$, and applying the elimination theorem gives us

$$I_1 = y - z.$$

Thus the partial solutions are given by (a, a). Extending these to the complete solutions we obtain (1/a, a, a). But we notice that this extension is not valid when a = 0. So the only partial solution that does not extend is (0, 0), which is the partial solution where the leading coefficients y and z of x vanish. But the *Extension Theorem* tells us that the extension step can fail when the leading coefficients vanish simultaneously.

It should be noted that in projective space, *all* partial solutions extend.

3. Intersection of Ideals

In this section I consider the problem where, given two ideals in a polynomial ring, we try to determine their intersection. The first question that naturally arises is whether this intersection will also be an ideal. This brings us to the first proposition of this section.

Proposition 4.3.1. *If I and J are ideals in $k[x_1,\cdots,x_n]$, then $I\cap J$ is also an ideal.*

Proof. Note that $0\in I\cap J$, since $0\in I$ and $0\in J$. If $f\in I\cap J$ and $g\in I\cap J$, then $f+g\in I$ and $f+g\in J$. Hence $f+g\in I\cap J$. To test whether or not we have closure under multiplication, let $f\in I\cap J$ and let h be any polynomial in $k[x_1,$ $\cdots,x_n]$. Since $f\in I$, and I is an ideal, then $f\cdot h\in I$. Similarly, $f\cdot h\in J$, and hence $f\cdot h\in I\cap J$. □

So to restate our problem, if we are given two ideals, and a set of generators for each, we wish to compute the set of generators for their intersection. To do this we need a bit of notation and a lemma.

If I is an ideal in $k[x_1,\cdots,x_n]$ and $f(t)\in k[t]$ a polynomial in a single variable *t*, then $f\,I$ denotes the ideal in $k[x_1,\cdots,x_n,t]$ generated by the set of polynomials

$\{f \cdot h : h \in I\}$. Note that the ideal I in $k[x_1,\cdots,x_n]$ is *not* an ideal in $k[x_1,\cdots,x_n,t]$. So with this notation we have

$$fI \ = \ f(t)I = \left\langle f(t)h(x) : h(x) \in I \right\rangle.$$

Lemma 4.3.2.

(i) *If I is generated as an ideal in $k[x_1,\cdots,x_n]$ by $p_1(x),\cdots,p_r(x)$, then fI is generated as an ideal in $k[x_1,\cdots,x_n,t]$ by $f \cdot p_1(x),\cdots, f \cdot p_r(x)$.*

(ii) *If $g(x,t) \in fI$ and a is any element of the field k, then $g(x,a) \in I$.*

Proof. To prove the first assertion, note that any $g \in fI$ can be expressed as a sum of terms of the form $h(x,t) \cdot f \cdot p(x)$, with $h \in k[x_1,\cdots,x_n,t]$. But since *I* is generated by the p_i, we can write $p(x)$ as $p(x) = \sum_{i=1}^{r} q_i(x) p_i(x)$. Hence we have $h(x,t) \cdot f \cdot$

$$p(x) = \sum_{i=1}^{r} h(x,t) q_i(x) p_i(x) f \ .$$

Now for each i, $h(x,t) \cdot q_i(x) \in k[x_1,\cdots,x_n,t]$. Thus $h(x,t) \cdot f \cdot p(x)$ belongs to an ideal in $k[x_1,\cdots,x_n,t]$ generated by $f \cdot p_1(x),\cdots, f \cdot p_r(x)$. Since *g* is a sum of such terms, $g \in \left\langle f \cdot p_1(x),\cdots, f \cdot p_r(x) \right\rangle$, which proves (i).

(ii) is proved immediately by substituting *a* for *t* in $h(x,t)$. □

Theorem 4.3.3. *Let I, J be ideals in $k[x_1,\cdots,x_n]$. Then*

$$I \cap J = \left(tI + (1-t)J\right) \cap k[x_1,\cdots,x_n].$$

Proof. First note that $tI+(1-t)J$ is an ideal in $k[x_1,\cdots,x_n,t]$. Now suppose that $f\in I\cap J$. Since $f\in I$, we have $t\cdot f\in tI$. Similarly, $f\in J\Rightarrow(1-t)\cdot f\in(1-t)J$. Thus $f=t\cdot f+(1-t)\cdot f\in tI+(1-t)J$. Since $I,J\subset k[x_1,\cdots,x_n]$, we get $f\in$ $\left(tI+(1-t)J\right)\cap k[x_1,\cdots,x_n]$.

To show inclusion in the other direction, let $f\in\left(tI+(1-t)J\right)\cap k[x_1,\cdots,x_n]$. Then $f(x)=g(x,t)+h(x,t)$, where $g(x,t)\in tI$ and $h(x,t)\in(1-t)J$. Setting t = 0, we observe that $g(x,0)\in 0I=0$. Thus $f(x)=h(x,0)$, and hence $f(x)\in J$ by our previous lemma. Setting t = 1 gives us $f(x)=g(x,1)+0$, hence $f(x)\in I$ by our previous lemma. Since f belongs to both I and J, we get $f\in I\cap J$, which completes the proof. □

The above result, along with the Elimination Theorem from the previous chapter, provides us with an algorithm for computing the intersection of two ideals. If $I=\left\langle f_1,\cdots,f_r\right\rangle$ and $J=\left\langle g_1,\cdots,g_s\right\rangle$ are ideals in $k[x_1,\cdots,x_n]$, we consider the ideal:

$$\left\langle tf_1,\cdots,tf_r,(1-t)g_1,\cdots,(1-t)g_s\right\rangle\subset k[x_1,\cdots,x_n,t]$$

and compute a Groebner basis with respect to lex order in which t is greater than x_i. The elements of this basis which do not contain the variable t will form a basis of $I\cap J$.

Example 4.3.4. Consider the following ideals

$$I = \left\langle x^4 + x^3 y + x^3 z^2 - x^2 y^2 + x^2 yz^2 - xy^3 - xy^2 z^2 - y^3 z^2 \right\rangle \in k[x, y, z]$$

and

$$J = \left\langle x^4 + 2x^3 z^2 - x^2 y^2 + x^2 z^4 - 2xy^2 z^2 - y^2 z^4 \right\rangle \in k[x, y, z].$$

We consider the ideal $tI + (1-t)J$ in $k\left[t, x, y, z\right]$. Computing its Groebner basis using a computer algebra program (I use Maple® 11) with respect to lex order with $t > x > y > z$, we get:

$$G = \{-y^3 z^4 - xy^2 z^4 + x^2 yz^4 + x^3 z^4 - 2xy^3 z^2 - 2x^2 y^2 z^2 + 2x^3 yz^2 + 2x^4 z^2 - x^2 y^3 - x^3 y^2$$
$$+ x^4 y + x^5, tx^3 y - tx^3 z^2 + tx^2 yz^2 - txy^3 + txy^2 z^2 - ty^3 z^2 - x^2 y^2 + x^4 - 2xy^2 z^2 + 2x^3 z^2 -$$
$$y^2 z^4 + x^2 z^4 - tx^2 z^4 + ty^2 z^4, -x^4 - 2x^3 z^2 + x^2 y^2 - x^2 z^4 + 2xy^2 z^2 + y^2 z^4 + tx^4 + 2tx^3 z^2$$
$$- tx^2 y^2 + tx^2 z^4 - 2txy^2 z^2 - ty^2 z^4\}.$$

Hence, by the Elimination Theorem,

$$\{-y^3 z^4 - xy^2 z^4 + x^2 yz^4 + x^3 z^4 - 2xy^3 z^2 - 2x^2 y^2 z^2 + 2x^3 yz^2 + 2x^4 z^2 - x^2 y^3 - x^3 y^2 + x^4 y$$
$$+ x^5\}$$

is a Groebner basis of $\left(tI + (1-t)J\right) \cap k\left[x, y, z\right]$. Thus

$$I \cap J = < -y^3 z^4 - xy^2 z^4 + x^2 yz^4 + x^3 z^4 - 2xy^3 z^2 - 2x^2 y^2 z^2 + 2x^3 yz^2 + 2x^4 z^2 - x^2 y^3 - x^3 y^2$$
$$+ x^4 y + x^5 > .$$

4. The 3-Color Problem

Here I will discuss how we can apply Groebner bases to solve the well-known 3-color problem in graph-theory: determining whether a graph can be 3-colored. More precisely, given a graph with *n* vertices, we want to color the vertices in such a way that only 3 colors are used, and no adjacent vertices have the same color. If the graph can be colored in this manner, then it is called *3-colorable*. This is similar to the 3-color problem for a map, where the vertices represent the contiguous regions to be colored, and connected vertices represent adjacent regions. I discuss the *3*-color problem in particular, even though the approach I describe works for any coloring. The equivalent *2*-color problem is exceedingly simple, since the presence of any odd-cycle ensures that it is not 2-colorable. The 3-color problem appears adequately complicated to warrant deeper analysis.

The following is an example of a graph that is 3-colorable. Labelling the colors as 1, 2 and 3, one possible coloring combination that manifests 3-colorability is displayed below:

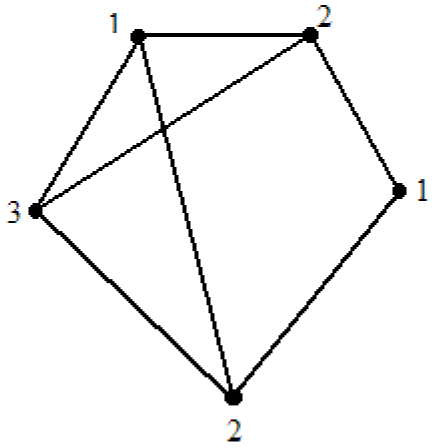

FIGURE 4.4.1.

An example of a graph that is *not* 3-colorable is the following:

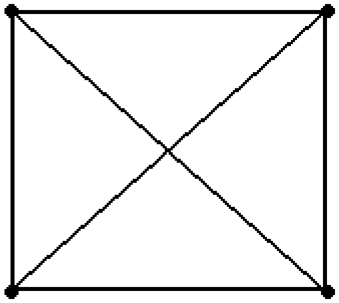

FIGURE 4.4.2.

In order to set this problem up mathematically, first we let $\omega = e^{\frac{2\pi i}{3}}$ be a cube root of unity (i.e. $\omega^3 = 1$). We can now represent the three colors by 1, ω and ω^2. We let

$x_1,\ldots,x_n$ be variables representing the distinct vertices of our graph Ĝ. Each vertex is to be assigned one of the three colors 1, ω or ω^2. This gives us the following n equations:

$$x_i^3 - 1 = 0, \quad 1 \le i \le n. \qquad (*)$$

The 3-colorability condition adds the condition that if two vertices x_i and x_j are connected by an edge, they need to be colored differently. Now since $x_i^3 = x_j^3$, we have:

$$x_i^3 - x_j^3 = 0$$

$$\Rightarrow (x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0$$

But since $x_i \neq x_j$, we have:

$$x_i^2 + x_i x_j + x_j^2 = 0. \qquad (**)$$

Now we define I to be the ideal of $\mathbf{C}[x_1,\cdots,x_n]$ generated by the polynomials in (*), and for each pair of vertices x_i, x_j connected by an edge by the polynomials in (**). We now consider the variety $V(I)$ contained in $\mathbf{C}^n$, and the following theorem follows immediately:

Theorem 4.4.1. The graph Ĝ is 3-colorable if and only if $V(I) \neq \emptyset$.

Proof: Obvious.

Now to determine whether $V(I\ ) \neq Ø$, we can use Groebner bases. We compute a reduced Groebner basis G for I, and if $1 \in G$ then $V(I\ ) = Ø$ and the graph is not 3-colorable. Otherwise, it is so.

Example 1. Consider the graph Ĝ below:

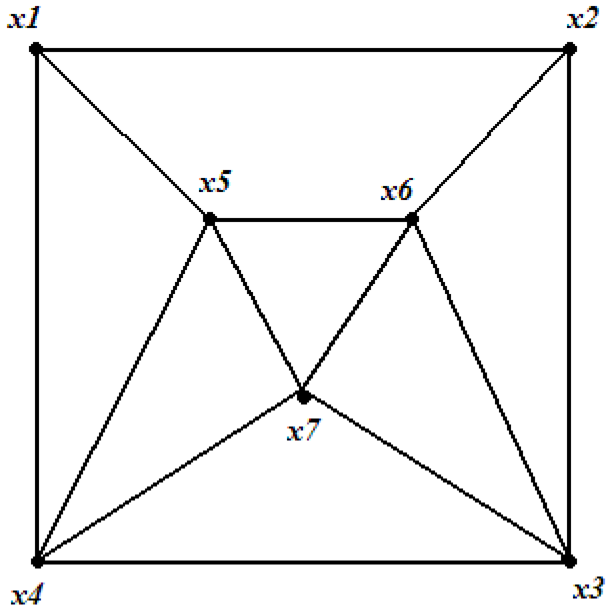

FIGURE 4.4.3.

The polynomials corresponding to Ĝ are:

$$x_i^{\ 3} - 1, \text{ for } i = 1,\ldots,7$$

And

$$x_i^{\ 2} + x_i x_j + x_j^{\ 2}, \text{ for the pairs } (i, j) \in \{(1,2),(1,4),(1,5),(2,3),(2,6),(3,4),$$

$$(3,6),(3,7),(4,5),(4,7),(5,6),(5,7),(6,7)\}.$$

We now compute a Groebner basis G using the lex-ordering for the ideal I corresponding to the above polynomials, and obtain $G = \{1\}$. Hence, Ĝ is *not* 3-colorable.

If, on the other hand, we remove the edge connecting x_6 to x_7, our graph takes the following form.

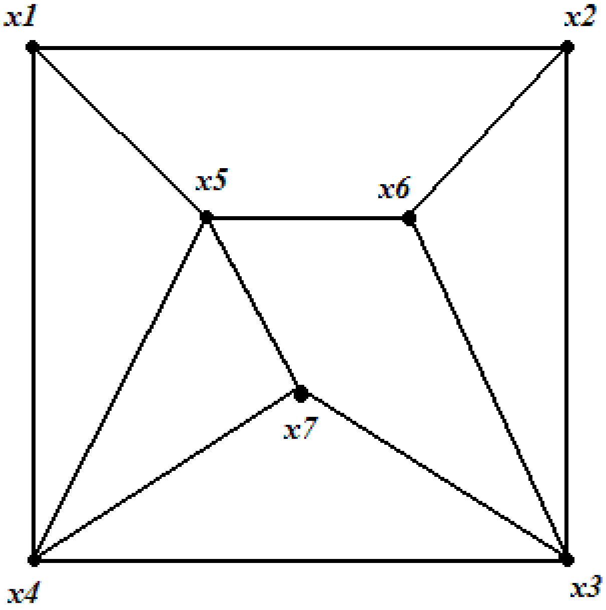

FIGURE 4.4.4.

The only difference to I is that it no longer contains the polynomial $x_6^2 + x_6x_7 + x_7^2$.

Computing the reduced Groebner basis, we obtain:

$$G = \{x_7^3 - 1, -x_7 + x_6, x_5^2 + x_5x_7 + x_7^2, x_5 + x_7 + x_4, x_3 - x_5, x_5 + x_2 + x_7, x_1 - x_7\}.$$

Since $1 \notin G$, we have that $V(I) \neq \emptyset$, and hence Ĝ is 3-colorable. Referring to the three colors as c_1, c_2 and c_3, one possible coloring combination is the following:

$x_1 \longrightarrow c_{1;}$ $x_2 \longrightarrow c_{2;}$ $x_3 \longrightarrow c_{3;}$ $x_4 \longrightarrow c_{2;}$ $x_5 \longrightarrow c_{3;}$ $x_6 \longrightarrow c_{1;}$ $x_7 \longrightarrow c_{1.}$

5. Integer Programming

Integer programming is the problem of solving linear equations where the solution must be in non-negative integers and should minimize a given “cost function”. These kinds of problems arise often in scientific and engineering applications, and there are several books on this subject that can be referred to for further reading; for example, see [Schri].

Our strategy here is to convert the integer programming problem into a problem about polynomials, and then solve this polynomial problem using Groebner bases, and use this to obtain the solution to our original integer programming problem.

So our objective is to find a solution $(z_1, z_2, ..., z_m)$ in $\mathbf{N}^{\mathrm{m}}$ of the system

(*)

$$\begin{aligned} a_{11}z_1 + a_{22}z_2 + ... + a_{1m}z_m &= b_1 \\ a_{21}z_1 + a_{22}z_2 + ... + a_{2m}z_m &= b_2 \\ &\vdots \\ a_{n1}z_1 + a_{n2}z_2 + ... + a_{nm}z_m &= b_n . \end{aligned}$$

which minimizes the “cost” function

(**)

$$c(z_1, z_2, \cdots, z_m) = \sum_{j=1}^{m} c_j z_j \; .$$

Initially I will solve the system (*) without taking into account the cost function. To do this, I introduce a variable for each linear equation in the system above, say $x_1,\ldots,x_n$, and a variable for each unknown z_j, say $y_1,\ldots,y_m$. We can now represent the system as:

$$x_i^{a_{i1}z_1+\cdots a_{im}z_m} = x_i^{b_i} \quad \text{for } i = 1,\ldots,n.$$

Then (*) can be written as a single equation of monomials

$$x_1^{a_{11}z_1+\cdots a_{1m}z_m} \cdots x_n^{a_{n1}z_1+\cdots a_{nm}z_m} = x_1^{b_1} \cdots x_n^{b_n}.$$

Which can be rearranged to obtain:

(***) $$\left(x_1^{a_{11}} \cdots x_n^{a_{n1}}\right)^{z_1} \cdots \left(x_1^{a_{1m}} \cdots x_n^{a_{nm}}\right)^{z_m} = x_1^{b_1} \cdots x_n^{b_n}.$$

The left hand side monomial in the above equation can be considered as the image of the monomial $y_1^{z_1} \cdots y_m^{z_m}$ under the polynomial map

$$\begin{aligned} &k[y_1,\cdots,y_m] \xrightarrow{\varphi} k[x_1,\cdots,x_n] \\ &y_j \mapsto x_1^{a_{1j}} \cdots x_n^{a_{nj}}. \end{aligned}$$

Then it is clear that if we assume that all the a_{ij}'s and b_i's are non-negative, there exists a solution $(z_1, z_2, ..., z_m) \in \mathbf{N}^{\mathrm{m}}$ of system (*) iff the monomial $x_1^{b_1} \cdots x_n^{b_n}$ is the image under φ of a monomial in $k[y_1,\cdots,y_m]$. Moreover if $x_1^{b_1} \cdots x_n^{b_n} = \varphi\left(y_1^{z_1} \cdots y_m^{z_m}\right)$, then $\left(z_1, \cdots z_m\right) \in \mathbf{N}^{\mathrm{m}}$ is a solution of (*).

We now consider the following Lemma:

Lemma 4.5.1. *We use the notation above and assume that all a_{ij}'s and b_i's are non-negative. If $x_1^{b_1} \cdots x_n^{b_n}$ is in the image of φ, then it is the image of a monomial $\left(y_1^{z_1} \cdots y_m^{z_m}\right) \in k[y_1,\cdots,y_m]$.*

Proof. See [AL, page 107].

We can now use the following procedure for determining whether (*) has a solution, and for finding a solution:

(i) Compute a Groebner basis G for $K = \left\langle y_j - x_1^{a_{1j}} \cdots x_n^{a_{nj}} \mid j = 1, \cdots, m \right\rangle$ with respect to an elimination order with the x variables larger than the y variables;

(ii) Find the remainder h of the division of the monomial $x_1^{b_1} \cdots x_n^{b_n}$ by G;

(iii) If $h \notin k[y_1, \cdots, y_m]$, then (*) does not have non-negative integer solutions.

If $h = y_1^{z_1} \cdots y_m^{z_m}$, then $y_1^{z_1} \cdots y_m^{z_m}$ is a solution of (*).

For example, consider the system:

$$\text{(\#)} \qquad \begin{aligned} 3z_1 + 2z_2 + z_3 &= 10 \\ 4z_1 + 3z_2 + z_3 &= 12. \end{aligned}$$

Using the procedure described above, we have two x variables, x_1, x_2, one for each equation, and three y variables, y_1, y_2, y_3, one for each unknown. The corresponding polynomial map is given by

$$k[y_1, y_2, y_3] \xrightarrow{\varphi} k[x_1, x_2]$$

$$\begin{aligned} y_1 &\mapsto x_1^3 x_2^4 \\ y_2 &\mapsto x_1^2 x_2^3 \\ y_3 &\mapsto x_1 x_2 . \end{aligned}$$

So $K = \left\langle y_1 - x_1^3x_2^4, y_2 - x_1^2x_2^3, y_3 - x_1x_2 \right\rangle \subset k[y_1, y_2, y_3, x_1, x_2]$. The Groebner basis for K with respect to the lex order with $x_1 > x_2 > y_1 > y_2 > y_3$ is $G = \{f_1, f_2, f_3, f_4\}$, where:

$$f_1 = y_1 - y_2y_3$$

$$f_2 = x_2y_3^2 - y_2$$

$$f_3 = x_1y_2 - y_3^3$$

$$f_4 = x_1x_2 - y_3.$$

Then dividing $x_1^{10}x_2^{12}$ by f_2 , f_3 and f_4 gives us:

$$x_1^{10}x_2^{12} \xrightarrow{\{f_2, f_3, f_4\}} y_2^2y_3^6.$$

So $h = y_2^2y_3^6 = y_1^0y_2^2y_3^6$. Using the exponents of h we get that (0, 2, 6) is a solution of (#).

Now we consider the more general case, where the a_{ij}'s and b_{i}'s in (*) are any integers, not necessarily non-negative. We now end up with negative exponents on the x variables, which cannot be obtained from the polynomial ring $k[x_1, \cdots, x_n]$. So we introduce a new indeterminate w and we work in the localized ring $k[x_1, \cdots, x_n, w]/I$, where $I = \langle x_1x_2 \cdots x_nw - 1 \rangle$. We may choose non-negative integers a'_{ij} and α_j, for each $j = 1,\ldots,m$ and $i = 1,\ldots,n$ such that for each $j = 1,\ldots,m$ we have

$$\left(a_{1j}, \cdots a_{nj}\right) = \left(a'_{1j}, \cdots, a'_{nj}\right) + \alpha_j\left(-1, \cdots, -1\right).$$

Then in the affine ring $k[x_1, \cdots, x_n, w]/I$ we define the coset $x_1^{a_{1j}} \cdots x_n^{a_{nj}} + I$ as:

$$x_1^{a_{1j}}\cdots x_n^{a_{nj}} + I = x_1^{a'_{1j}}\cdots x_n^{a'_{nj}} w^{\alpha_j} + I\,.$$

Similarly, $(b_1,\cdots,b_n)=(b'_1\cdots b'_n)+\beta(-1,\cdots,-1)$, and we define

$$x_1^{b_1}\cdots x_n^{b_n} + I = x_1^{b'_1}\cdots x_n^{b'_n} w^{\beta} + I\,.$$

We therefore get the following equation that corresponds to (***)

$$\left(x_1^{a'_{11}}\cdots x_n^{a'_{n1}} w^{\alpha_1}\right)^{z_1}\cdots\left(x_1^{a'_{1m}}\cdots x_n^{a'_{nm}} w^{\alpha_m}\right)^{z_m} + I = x_1^{b'_1}\cdots x_n^{b'_n} w^{\beta} + I\,.$$

As before, we notice that the left hand side of this equation can be viewed as a monomial $y_1^{z_1}\cdots y_m^{z_m}$ under the algebra homomorphism

$$\begin{aligned}&k[y_1,\cdots,y_m]\xrightarrow{\varphi}k[x_1,\cdots,x_n,w]/I\\&y_j\mapsto x_1^{a'_{1j}}\cdots x_n^{a'_{nj}} w^{\alpha j} + I.\end{aligned}$$

So, as before, $(z_1,\cdots z_m)\in \mathbf{N}^{\mathrm{m}}$ is a solution of (*) if and only if $x_1^{b'_1}\cdots x_n^{b'_n} w^{\beta} + I$ is the image under φ of a monomial in $k[y_1,\cdots,y_m]$. Furthermore, $(z_1,\cdots z_m)$ is a solution of (*) if $x_1^{b'_1}\cdots x_n^{b'_n} w^{\beta} + I = \varphi\left(y_1^{z_1}\cdots y_m^{z_m}\right)$.

Lemma 4.5.2. *We use the notation above. If* $x_1^{b'_1}\cdots x_n^{b'_n} w^{\beta} + I$ *is in the image of* φ, *then it is the image of a monomial* $y_1^{z_1}\cdots y_m^{z_m}\in k[y_1,\cdots,y_m]$.

Proof. See [AL, page 109].

For example, consider the system:

$$\begin{aligned}&2z_1+z_2-3z_3+z_4=4\\ \text{(\#\#)}\qquad&\\&-3z_1+2z_2-2z_3-z_4=-3\end{aligned}$$

We have two x variables, x_1, x_2, one for each equation, and four y variables, y_1, y_2, y_3, y_4, one for each unknown. We consider the ideal $I = \langle x_1 x_2 w - 1 \rangle$ of $k[x_1, x_2, w]$ and the algebra homomorphism

$$k[y_1, y_2, y_3, y_4] \xrightarrow{\varphi} k[x_1, x_2, w]/I$$

$$\begin{aligned} y_1 &\mapsto x_1^5 w^3 + I \\ y_2 &\mapsto x_1^1 x_2^2 + I \\ y_3 &\mapsto x_2^1 w^3 + I \\ y_4 &\mapsto x_1^2 w + I \end{aligned}$$

Thus $K = \langle y_1 - x_1^5 w^3, y_2 - x_1 x_2^2, y_3 - x_2 w^3, y_4 - x_1^2 w, x_1 x_2 w - 1 \rangle$. The Groebner basis for K with respect to the lex order with $x_1 > x_2 > w > y_1 > y_2 > y_3 > y_4$ is $G = \{f_1, f_2, f_3, f_4, f_5\}$, where:

$$\begin{aligned} f_1 &= y_2^5 y_3^3 y_4^4 - 1 \\ f_2 &= y_1 - y_2^3 y_3^2 y_4^5 \\ f_3 &= w - y_2 y_3 y_4 \\ f_4 &= x_2 - y_2^2 y_3 y_4 \\ f_5 &= x_1 - y_2^2 y_3 y_4^2. \end{aligned}$$

Now since $x_1^4 x_2^{-3} + I = x_1^7 w^3 + I$, we reduce the monomial $x_1^7 w^3$ by G to get:

$$\begin{aligned} x_1^7 w^3 \quad &\xrightarrow{\{f_3, f_5\}} \quad y_2^{17} y_3^{10} y_4^{17} \\ &\xrightarrow{f_1} \quad y_2^{12} y_3^7 y_4^{13} \\ &\xrightarrow{f_1} \quad y_2^7 y_3^4 y_4^9 \end{aligned}$$

$$\xrightarrow{f_1} \qquad y_2^2 y_3 y_4^5 .$$

And $h = y_2^2 y_3 y_4^5$ is reduced with respect to *G*. We could also have reduced $y_2^{17} y_3^{10} y_4^{17}$ in the following manner:

$$\begin{aligned} y_2^{17} y_3^{10} y_4^{17} &\xrightarrow{f_2} \qquad y_1 y_2^{14} y_3^8 y_4^{12} \\ &\xrightarrow{f_2} \qquad y_1^2 y_2^{11} y_3^6 y_4^7 \\ &\xrightarrow{f_2} \qquad y_1^3 y_2^8 y_3^4 y_4^2 . \end{aligned}$$

The exponents of the different monomials obtained in this reduction give us the following solutions of (##)

(0, 17, 10, 17), (0, 12, 7, 13), (0, 7, 4, 9), (0, 2, 1, 5), (1, 14, 8, 12), (2, 11, 6, 7), and (3, 8, 4, 2).

We now return to the original problem. We want to find solutions of (*) that minimize the cost function (**). As previously, the only requirement on the term order for (*) is that we have an elimination order between the *x*, *w*, and the *y* variables with the *x* and *w* variables larger. The strategy for minimizing the cost function is to use the c_j's to define such a term order.

Definition 4.5.3. A term order $<_c$ on the y variables is said to be compatible with the cost function c and the map φ if

$$\begin{matrix} \varphi(y_1^{z_1} \cdots y_m^{z_m}) = \varphi(y_1^{z'_1} \cdots y_m^{z'_m}) \\ and \\ c(z_1, \cdots, z_m) < c(z'_1, \cdots, z'_m) \end{matrix} \Rightarrow y_1^{z_1} \cdots y_m^{z_m} <_c y_1^{z'_1} \cdots y_m^{z'_m} .$$

The following proposition now shows that compatible term orders on the *y* variables give rise to solutions of (*) with minimum cost.

Proposition 4.5.4. *We use the notation set above. Let G be a Groebner basis for K with respect to an elimination order with the x and w 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* $x_1^{b_1'} \cdots x_n^{b_n'} w^{\beta} \xrightarrow{G} y_1^{z_1} \cdots y_m^{z_m}$, *where* $y_1^{z_1} \cdots y_m^{z_m}$ *is reduced with respect to G, then* $(z_1, \cdots, z_m)$ *is a solution of* (*) *which minimizes the cost function c.*

Proof. See [AL, page 111].

Since our process of obtaining the minimal solution relies on the term order being used, a different minimal solution may be obtained if we use a different order, as long as we have an elimination order with the *x* and *w* variables larger than the *y* variables, and the order on the *y* variables is compatible with *c* and φ.

In general the term order $<_c$ is not easy to obtain (For details, I refer you to the original paper [CoTr]). But when the cost function contains only positive constants, then the case is simple. In this case we can use the following term order: first order monomials using the cost function, and break any ties with any other order.

For example, consider the system (##) with the following cost function:

$$c(z_1, z_2, z_3, z_4) = 10z_1 + z_2 + z_3 + 100z_4 .$$

We will use the lex order on *w* and *x* so that $x_1 > x_2 > w$. Next the monomials in *y* are first ordered using the cost function, and any ties that emerge are broken using lex ordering with $y_1 > y_2 > y_3 > y_4$. This means that:

$$y_1^{z_1} y_2^{z_2} y_3^{z_3} y_4^{z_4} < y_1^{z_1'} y_2^{z_2'} y_3^{z_3'} y_4^{z_4'}$$

if and only if

$$10z_1 + z_2 + z_3 + 100z_4 < 10z_1' + z_2' + z_3' + 100z_4'$$

or

$$10z_1 + z_2 + z_3 + 100z_4 = 10z_1' + z_2' + z_3' + 100z_4' \text{ and}$$

$$y_1^{z_1} y_2^{z_2} y_3^{z_3} y_4^{z_4} <_{lex} y_1^{z_1'} y_2^{z_2'} y_3^{z_3'} y_4^{z_4'}.$$

We then use an elimination order with the *x* and *w* variables larger than the *y* variables, and compute the reduced Groebner basis for *K*. This gives us:

$$G = \{w - y_1 y_2^3 y_3^2, y_4 - y_1 y_2^2 y_3, x_1 - y_1^2 y_2^6 y_3^3, x_2 - y_1 y_2^4 y_3^2, y_1^4 y_2^{`3} y_3^2 - 1\}.$$

Reducing $x_1^7 w^3$ with respect to *G* gives us:

$$x_1^7 w^3 \xrightarrow{G} y_1^5 y_2^{12} y_3^6$$

which gives the solution (5, 12, 6, 0). And this is the solution of minimum cost.

Groebner bases are not the sole approach to solving integer programming problems. It was proved by H. W. Lenstra, Jr. in 1983 that, for a fixed number of variables, such a problem can be solved in polynomial time [AWW]. I was unable to find any concrete data comparing the speed of the approach for solving integer programming problems using Groebner bases to other approaches.

Bibliography

[AL] W. Adams and Philippe Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, Volume 3, American Mathematical Society, 1994, 102-111.

[AWW] K. Aardal, R. Weismantel, and L. Wosley, *Non-standard approaches to integer programming*, Discrete Applied Mathematics, Volume 123 , Issue 1-3 (November 2002), ISSN:0166-218X.

[CLOS] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer Verlag, Berlin and New York, 1992, 29-186.

[CoTr] P. Conti and C. Traverso, *Buchberger algorithm and integer programming*, in AAECC'9, Lecture Notes in Computer Science, Vol. 539, 130-139, Springer Verlag, 1991.

[Sch] H. Schenck, *Computational Algebraic Geometry*, Cambridge University Press, London Mathematical Society student texts; 58, 2003, 10, Page 55.

[Schri] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley, Chichester, NY, 1998.