

Applications of Groebner Bases

Kathleen Iwancio
Michael Singer

1 Introduction

There is a well-known problem in graph theory called the 3-color problem. Given a graph, we would like to know if it can be three colored. Specifically, let \mathcal{G} be a graph with n vertices. Furthermore, suppose that any two vertices share at most one edge. Can each vertex be colored with 3 colors in such a way that adjacent vertices do not have the same color?

Example 1.1 *The graph \mathcal{G} below has five vertices with at most one edge between any two vertices.*

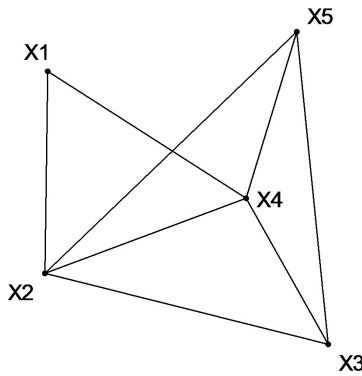


Figure 1: Sample Graph One

We will label our colors by $1, \xi, \xi^2$, where $\xi = e^{\frac{2\pi i}{3}}$ is a cube root of unity. Recall that a cube root of unity satisfies $\xi^3 = 1$. Notice that 1 and ξ^2 are the other two cube roots of unity. Also recall Euler's formula, $e^{\frac{2\pi i}{3}} = \cos(\frac{2\pi}{3}) + i \sin(\frac{2\pi}{3}) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

We want to assign a color to each vertex, and we can represent this by the polynomial equation $x_i^3 - 1 = 0$. (In the above picture i ranges from 1 to 5).

Recall that each vertex will have a color, so $x_i^3 = x_j^3 = 1$. Then for adjacent vertices

$$x_i^3 - x_j^3 = (x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0. \quad (1)$$

Recall though that we want x_i and x_j to have different colors. So the only way to satisfy equation (1) is for $x_i^2 + x_i x_j + x_j^2 = 0$. Consider each pair of adjacent vertices in the above graph.

Then we associate the above graph with the set of polynomials $P = \{x_1^2 + x_1 x_2 + x_2^2, x_1^2 + x_1 x_4 + x_4^2, x_2^2 + x_2 x_4 + x_4^2, x_2^2 + x_2 x_3 + x_3^2, x_2^2 + x_2 x_5 + x_5^2, x_3^2 + x_3 x_4 + x_4^2, x_3^2 + x_3 x_5 + x_5^2, x_4^2 + x_4 x_5 + x_5^2\}$. We can determine whether or not this graph is 3-colorable by checking to see if these polynomials have common solutions.

Then we end up with the following theorem.

Theorem 1.2 *A graph is 3-colorable if and only if the set of polynomials associated with our graph have a common solution in the complex numbers.*

Proof 1.3 *Suppose the given graph is 3-colorable. Recall that $x_i^3 - 1 = 0$ for each i . Then for adjacent vertices x_i, x_j , we have $x_i^3 - x_j^3 = (x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0$. The adjacent vertices are colored differently, so $x_i - x_j \neq 0$. Then $x_i^2 + x_i x_j + x_j^2 = 0$ for some x_i and x_j . This is true for any pair of adjacent vertices. Then the set of polynomials associated with the vertices have at least one common solution.*

Now suppose that the polynomials associated with adjacent vertices have a common solution. This means that there exists x_i, x_j such that $x_i^2 + x_i x_j + x_j^2 = 0$ for all pairs of adjacent vertices. Notice that $x_i \neq x_j$ for this to be true. Then $x_i^3 - x_j^3 = 0$ and we know from above that x_i and x_j will be assigned different colors. Hence the graph is 3-colorable.

The graph in example 1.1 is not 3-colorable. We will discuss later a technique for determining whether or not the polynomials have a common solution. This technique involves using Groebner bases.

Example 1.4 *Consider the graph in Figure 2. Then $P = \{x_1^2 + x_1 x_2 + x_2^2, x_1^2 + x_1 x_3 + x_3^2, x_2^2 + x_2 x_4 + x_4^2, x_2^2 + x_2 x_5 + x_5^2, x_4^2 + x_4 x_5 + x_5^2\}$. These polynomials have a common solution, so the graph in Figure 2 is 3-colorable. A possible solution is $(x_1, x_2, x_3, x_4, x_5) = (1, \xi, \xi^2, \xi^2, 1)$. Suppose we decide to let 1 correspond to the color red, ξ corresponds to green, and ξ^2 corresponds to blue. Then we can color x_1 and x_5 red. The vertex x_2 is green, and x_3 and x_4 are blue.*

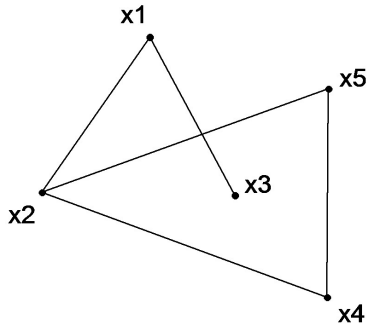


Figure 2: Sample Graph Two

1.1 Exercise

1. Write down the equations associated with the graph in Figure 3.

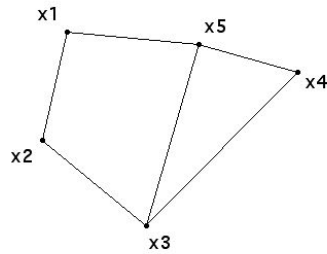


Figure 3: Exercise 1.1

We will begin our discussion by reviewing some concepts from linear algebra and the division algorithm. From there we will move into a discussion of Groebner bases and solving the 3-color problem.

2 Systems of Linear Equations

Consider m equations in n unknowns written in the following way:

$$\begin{aligned}
 a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\
 a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\
 &\vdots \\
 a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m.
 \end{aligned}$$

Recall that by choosing the order $x_1 > x_2 > \dots > x_n$, we can rewrite the above system as the following matrix system.

$$\underbrace{\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}}_{m \times n} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}}_{n \times 1} = \underbrace{\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}}_{m \times 1}$$

We can solve such a system of equations by writing the augmented matrix and using Gaussian elimination. The augmented matrix is given by:

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array} \right).$$

Gaussian elimination uses elementary row operations to write a matrix in row echelon form. Recall there are three elementary row operations.

1. Multiply a row by a nonzero constant.
2. Interchange two rows.
3. Add a multiple of one row to another.

Definition 2.1 A matrix is said to be in **row echelon form** if the following are satisfied:

1. The first nonzero entry in each nonzero row is a one. This entry is called a leading one.
2. Any rows of zeros occur at the bottom.
3. For two successive rows, the leading one in the lower row occurs to the right of the leading one in the above row.

Definition 2.2 A matrix is in **reduced row echelon form** if it is in row echelon form and each column with a leading one has zeros everywhere else.

Example 2.3 The matrix A is in row echelon form, and B is in reduced row echelon form.

$$A = \begin{pmatrix} 1 & * & * & * & * & * \\ 0 & 0 & 1 & * & * & * \\ 0 & 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

$$B = \begin{pmatrix} 1 & * & 0 & 0 & * & * \\ 0 & 0 & 1 & 0 & * & * \\ 0 & 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Algorithm 2.4 (Gaussian Elimination) 1. Locate the left most column not consisting entirely of zeros.

2. If necessary, interchange rows to get a nonzero entry to the top row, first column.

3. Multiply the first row by an appropriate constant to make the leading entry a one.

4. Recall that to be in row echelon form, the entries below the leading one need to be zero, so we add multiples of the top row to lower rows to make the rest of the entries in the column zero.

5. We now fix row one and repeat the process on the remaining rows.

6. Repeat as many times as necessary to get the matrix in row echelon form.

Example 2.5 Consider the matrix:

$$A = \begin{pmatrix} 2 & 2 & 2 & 0 \\ -2 & 5 & 2 & 1 \\ 8 & 1 & 4 & -1 \end{pmatrix}.$$

We use Gaussian elimination to write A in row echelon form. For ease of notation, we refer to rows 1, 2, and 3 as R_1 , R_2 , and R_3 , respectively.

$$\begin{aligned} \begin{pmatrix} 2 & 2 & 2 & 0 \\ -2 & 5 & 2 & 1 \\ 8 & 1 & 4 & -1 \end{pmatrix} &\xrightarrow{\frac{1}{2} \cdot R_1} \begin{pmatrix} 1 & 1 & 1 & 0 \\ -2 & 5 & 2 & 1 \\ 8 & 1 & 4 & -1 \end{pmatrix} \xrightarrow{\substack{2 \cdot R_1 + R_2 \\ -8 \cdot R_1 + R_3}} \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 7 & 4 & 1 \\ 0 & -7 & -4 & -1 \end{pmatrix} \\ &\xrightarrow{\substack{\text{Fix } R_1 \\ \frac{1}{7} \cdot R_2}} \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & \frac{4}{7} & \frac{1}{7} \\ 0 & -7 & -4 & -1 \end{pmatrix} \xrightarrow{7 \cdot R_2 + R_3} \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & \frac{4}{7} & \frac{1}{7} \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

Notice that $-1 \cdot R_2 + R_1$ would put the matrix in reduced row echelon form.

Matrix A in the above example is the augmented matrix for the system of equations:

$$\begin{aligned} 2x + 2y + 2z &= 0 \\ -2x + 5y + 2z &= 1 \\ 8x + y + 4z &= -1. \end{aligned}$$

We can use the row echelon form and back substitution to solve for x , y , and z . The bottom row of zeros tells us that z can take on any value and we get infinitely many solutions. If we let $z = t$, then row 2 tells us $y + \frac{4}{7}t = \frac{1}{7}$. In terms of t , $y = \frac{1}{7} - \frac{4}{7}t$. Then $x = -\frac{3}{7}t - \frac{1}{7}$.

Recall that a linear system of equations may have no solution, a unique solution, or infinitely many solutions.

Example 2.6 Consider the following system of linear equations.

$$\begin{aligned} -2y + 3z &= 1 \\ 3x + 6y - 3z &= -2 \\ 6x + 6y + 3z &= 5 \end{aligned}$$

The augmented matrix for this system is given by

$$A = \begin{pmatrix} 0 & -2 & 3 & 1 \\ 3 & 6 & -3 & -2 \\ 6 & 6 & 3 & 5 \end{pmatrix}.$$

A row echelon form for matrix A is

$$\begin{pmatrix} 1 & 2 & -1 & -\frac{2}{3} \\ 0 & 1 & -\frac{3}{2} & -\frac{1}{2} \\ 0 & 0 & 0 & 6 \end{pmatrix}.$$

The last row says that $0x + 0y + 0z = 6$, which is not possible. So we say that this system is inconsistent, i.e. there are no solutions.

Look back at the system from example 2.5. The system could have been written in the form

$$\begin{pmatrix} 2 & 2 & 2 \\ -2 & 5 & 2 \\ 8 & 1 & 4 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}.$$

We have used the order $x > y > z$ to write this system. We could instead use the order $z > y > x$. This ordering may look different but will give us the same solutions. With $z > y > x$, the system looks like:

$$\begin{pmatrix} 2 & 2 & 2 \\ 2 & 5 & -2 \\ 4 & 1 & 8 \end{pmatrix} \begin{pmatrix} z \\ y \\ x \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}.$$

A possible row echelon form for the augmented matrix is given by

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & -\frac{4}{3} & \frac{1}{3} \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

If we let $x = s$, then $y = \frac{1}{3} + \frac{4}{3}s$ and $z = -\frac{1}{3} - \frac{7}{3}s$. Recall that the other ordering gave us $z = t$, $y = \frac{1}{7} - \frac{4}{7}t$, and $x = -\frac{3}{7}t - \frac{1}{7}$.

2.1 Exercises

1. Verify that in example 2.5, $t = 1$ and $s = -\frac{4}{7}$ result in the same solution.

2. Consider the following system of linear equations.

$$\begin{aligned}x + 3y - z &= 0 \\2w + x - 4y + 3z &= 0 \\2w + 3x + 2y - z &= 0 \\-4w - 3x + 5y - 4z &= 0\end{aligned}$$

- (a) Write the augmented matrix for this system.
- (b) Use Gaussian elimination to write the augmented matrix in row echelon form.
- (c) Solve the system for w, x, y, z .

3. Consider the following system of linear equations.

$$\begin{aligned}x + y &= 8 \\3x + 3y &= k\end{aligned}$$

- (a) For what values of k does this system have a solution?
- (b) What value of k gives no solution? Explain.

3 Euclidean Algorithm

We would ultimately like to know if a system of polynomials has a common solution. For linear systems, we use Gaussian elimination to determine whether or not the system has a common solution. We will start our study of nonlinear systems of equations by considering a system of two polynomials of a single variable. In this situation we use the Euclidean algorithm to determine if there is a common solution.

Let K be a field. We can consider finite fields, but we will assume $K = \mathbb{C}$ unless otherwise stated. Then $K[x]$ denotes the ring of polynomials in x with coefficients in K .

Suppose $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$. Recall that for $a_n \neq 0$, we say that p has degree n , denoted $\deg(p) = n$. The leading term of p denoted $LT(p)$ is $a_n x^n$.

Notice that if we have two polynomials f and g , then $\deg(f) \leq \deg(g)$ if and only if $LT(f)$ divides $LT(g)$.

Recall that a subset $I \subseteq K[x]$ is called an **ideal** if the following hold:

1. $0 \in I$.
2. If $f, g \in I$, then $f + g \in I$.
3. If $c \in K[x]$ and $f \in I$, then $cf \in I$.

Theorem 3.1 (Division Algorithm) *If g is a nonzero polynomial in $K[x]$, then every $f \in K[x]$ can be written as $f = qg + r$ where $q, r \in K[x]$. Then r must be zero or have degree less than the degree of g . The polynomials q and r are unique.*

The pseudocode for the division algorithm is given below as appears in [3]. An example will follow.

Algorithm 3.2 *Let $g, f \in K[x]$.*

Input: g, f

Output: q, r

$q := 0, r := f$

While $r \neq 0$ AND $LT(g) | LT(r)$ DO

$q := q + \frac{LT(r)}{LT(g)}$

$r := r - \frac{LT(r)}{LT(g)}g$.

Notice that at the beginning of each step, we check that the remainder is nonzero and compare leading terms. This is the key to the algorithm. If the remainder is still nonzero, and the leading term of g divides the leading term of r , then we run through the division again. The values for r and q are reset, and we go back to the beginning.

Example 3.3 *Let $f(x) = 4x^3 + x^2 - 3x + 1$ and $g(x) = 2x - 3$. We want to rewrite f as $qg + r$ as given in the division algorithm.*

1. *Set $q := 0$ and $r := f = 4x^3 + x^2 - 3x + 1$. We see that $r \neq 0$ AND $2x | 4x^3$. Then let $q := q + \frac{LT(r)}{LT(g)} = 0 + 2x^2$ and $r := r - \frac{LT(r)}{LT(g)}g = 4x^3 + x^2 - 3x + 1 - (4x^3 - 6x^2) = 7x^2 - 3x + 1$.*
2. *Again, $r \neq 0$ AND $2x | 7x^2$. So we run through the steps again. Then $q := 2x^2 + \frac{7}{2}x$ and $r := \frac{15}{2}x + 1$.*
3. *We see $r \neq 0$ and $2x | \frac{15}{2}x$. So $q := 2x^2 + \frac{7}{2}x + \frac{15}{4}$ and $r := \frac{49}{4}$.*
4. *We still have $r \neq 0$, but $2x$ does not divide $\frac{49}{4}$. The algorithm has terminated.*

Then we can write $f = 4x^3 + x^2 - 3x + 1 = (2x^2 + \frac{7}{2}x + \frac{15}{4})(2x - 3) + \frac{49}{4} = qg + r$.

Eventually we will want to generalize this algorithm to polynomials of more than one variable.

Recall the following corollaries to the division algorithm.

Corollary 3.4 *If $a \in K$ and $f(x) \in K[x]$, then $f(a)$ is the remainder when we divide $f(x)$ by $x - a$. Furthermore, a is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.*

In other words, a is a zero of $f(x)$ if and only if the remainder of division of $f(x)$ by $x - a$ is zero.

Corollary 3.5 *If $f \in K[x]$, then f has at most $\deg(f)$ zeros in K where $\deg(f)$ is the degree of f .*

Corollary 3.6 *Every ideal of $K[x]$ is a principal ideal.*

In other words, every ideal of $K[x]$ takes the form $\langle f \rangle$ for $f \in K[x]$. Furthermore, f is unique up to a constant in K .

3.1 Exercise

1. Prove Corollary 3.4.

Suppose we have an ideal $I = \langle f, g \rangle \subset K[x]$. Corollary 3.6 tells us that there is some $h \in K[x]$ such that $I = \langle h \rangle$. How can we find such an h ?

We can find out if two polynomials have a common zero, and answer the above questions using the greatest common divisor.

Definition 3.7 *Let $f, g \in K[x]$. A polynomial $h \in K[x]$ is a greatest common divisor of f and g if the following hold:*

1. h divides f and g .
2. If $p \in K[x]$ also divides f and g , then p divides h .

We denote the greatest common divisor by $h = \text{GCD}(f, g)$.

There are some important properties of GCDs that we must consider.

Theorem 3.8 *Let $f, g, h \in K[x]$ and $h = \text{GCD}(f, g)$. The the following hold:*

1. h is unique up to a constant multiple.
2. h generates the ideal $\langle f, g \rangle$.
3. There is a method for finding h , called the Euclidean Algorithm.

We will write the Euclidean Algorithm in words and then give an example.

Algorithm 3.9 (Euclidean Algorithm) *Suppose f and g are polynomials in $K[x]$.*

1. When we take f divided by g , we will get some polynomial times g plus a remainder.
2. We then look at g and divide by the remainder. This will give us a new polynomial and a new remainder. (See the picture below).

3. Now look at the old remainder that we just divided by and divide by the new remainder.
4. Continue in this fashion until the final remainder is zero.
5. The previous remainder (nonzero) is the GCD of f and g .

$$\begin{aligned}
 f &= q_1 g + r_1 \\
 g &= q_2 r_1 + r_2 \\
 r_1 &= q_3 r_2 + r_3 \\
 &\vdots \\
 r_{(n-2)} &= q_{(n+1)} r_{(n-1)} + r_n \\
 r_{(n-1)} &= q_{(n+2)} r_n + 0
 \end{aligned}$$

Figure 4: Euclidean Algorithm

Example 3.10 Let $K = \mathbb{R}$, $f(x) = x^6 - 1$, and $g = x^4 - 1$.

$$\begin{aligned}
 x^6 - 1 &= x^2(x^4 - 1) + (x^2 - 1) \text{ (Divide } f \text{ by } g \text{ and write } f = qg + r.) \\
 x^4 - 1 &= (x^2 + 1)(x^2 - 1) + 0 \text{ (Let } f_1 = g, g_1 = r. \text{ Write } f_1 = q_1 g_1 + r_1.)
 \end{aligned}$$

Then the GCD of f and g is $x^2 - 1$. We kept applying the division algorithm until the remainder was zero. Then $GCD(x^6 - 1, x^4 - 1) = x^2 - 1$ tells us that $\langle x^6 - 1, x^4 - 1 \rangle = \langle x^2 - 1 \rangle$. We also see that 1 and -1 are common zeros for $x^6 - 1 = x^4 - 1 = 0$. (This is because $x - 1$ and $x + 1$ are common factors of $x^6 - 1$ and $x^4 - 1$.)

If $GCD(f, g) = 1$, we say that f and g are relatively prime. They have no common zeros. The polynomials have common roots if the GCD has roots.

Let K be a field. Recall that a field is called **algebraically closed** if each polynomial with coefficients in K has roots in K .

Corollary 3.11 If K is an algebraically closed field and $f, g \in K[x]$, then f and g have no common solution if and only if $1 \in \langle f, g \rangle$.

This corollary will also hold for polynomials of more than one variable, and we will describe a way to determine whether or not 1 is in the ideal generated by such polynomials.

The program **Maple** has a command for calculating the greatest common divisor of two polynomials. The command is `gcd(f,g)`, where f and g are polynomials. They may be multivariate.

Recall that there are two questions we have been considering in this section.

1. How do we find out if two polynomials in $K[x]$ have a common solution?
2. If $I = \langle f, g \rangle$ is an ideal in $K[x]$, how do we find $h \in K[x]$ such that $I = \langle f, g \rangle = \langle h \rangle$?

We can ask the same questions when we have more than 2 polynomials. Suppose $f_1, \dots, f_s \in K[x]$ for $s \geq 2$. Then we get the following theorem.

Theorem 3.12 *Let $f_1, \dots, f_s \in K[x]$.*

1. $GCD(f_1, \dots, f_s)$ exists and is unique up to a nonzero constant.
2. $\langle GCD(f_1, \dots, f_s) \rangle = \langle f_1, \dots, f_s \rangle$.
3. For $s > 3$, $GCD(f_1, \dots, f_s) = GCD(f_1, GCD(f_2, \dots, f_s))$.
4. There is an algorithm for finding the GCD.

Suppose we have $f_1, f_2, f_3 \in K[x]$. To find $g = GCD(f_1, f_2, f_3)$, we first find $h = GCD(f_1, f_2)$. Then $g = GCD(f_1, f_2, f_3) = GCD(h, f_3)$. We can find the GCD for $s > 3$ in a similar manner.

3.2 Exercises

1. Given $f(x) = 3x^4 + x^3 + 2x^2 + 1$ and $g(x) = x^2 + 4x + 2$, use the division algorithm to write $f = qg + r$.
2. Let $f(x) = x^3 - 3x + 2$ and $g(x) = x^4 - 1$.
 - (a) Find $GCD(f, g)$.
 - (b) Do f and g have any common solutions? If so, what are they?

We will now shift our focus to polynomials of more than one variable.

4 Monomials, Polynomials, and Ideals

Denote the ring of polynomials in variables x_1, x_2, \dots, x_n by $K[x_1, x_2, \dots, x_n]$, where K is some field.

Consider the monomial $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$, where $\alpha_1, \dots, \alpha_n$ are positive integers.

Definition 4.1 *The total degree of the above monomial is defined to be the sum $\alpha_1 + \dots + \alpha_n$. This sum is sometimes denoted by $|\alpha|$.*

We can write the above monomial as x^α , where $x = (x_1, \dots, x_n)$ and $\alpha = (\alpha_1, \dots, \alpha_n)$.

A polynomial in the variables x_1, \dots, x_n can be written as a finite linear combination of monomials, where the coefficients are in the field K . For example, let $f(x) = \sum_{\alpha} a_{\alpha} x^{\alpha}$ for $a_{\alpha} \in K$.

Then we get the following definitions.

Definition 4.2 *The coefficient of x_{α} is a_{α} .*

Definition 4.3 *For $a_{\alpha} \neq 0$, $a_{\alpha} x^{\alpha}$ is called a term of f .*

Definition 4.4 *The total degree of the polynomial f is the maximum value of $|\alpha|$ such that $a_{\alpha} x^{\alpha} \neq 0$.*

Example 4.5 *Let $f(x, y, z) = 2x^2y^3z + 3x^2y^2z^2 - 5x^3 \in \mathbb{Z}[x, y, z]$. We can write this as $f(\mathbf{x}) = 2\mathbf{x}^{\alpha} + 3\mathbf{x}^{\beta} + 5\mathbf{x}^{\gamma}$, where $\mathbf{x} = (x, y, z)$, $\alpha = (2, 3, 1)$, $\beta = (2, 2, 2)$, and $\gamma = (3, 0, 0)$. This polynomial has 3 terms. The total degree of f is 6. Notice that two of the terms have total degree 6. This is something we will have to deal with later. We want to be able to order the terms of a polynomial in several variables.*

The definition for ideal remains the same for $K[x_1, \dots, x_n]$. Let $f_1, \dots, f_s \in K[x_1, \dots, x_n]$. The **ideal generated** by these polynomials is denoted by $I = \langle f_1, \dots, f_s \rangle$. Any polynomial in I can be written as $\sum_{i=1}^s g_i f_i$, where $g_1, \dots, g_s \in K[x_1, \dots, x_n]$.

4.1 Exercise

1. Verify that $\langle f_1, \dots, f_s \rangle$ is an ideal for $f_1, \dots, f_s \in K[x_1, \dots, x_n]$.

A converse to the above statement says that every ideal $I \in K[x_1, \dots, x_n]$ is finitely generated. By finitely generated, we mean that $I = \langle f_1, \dots, f_s \rangle$ for some $s > 0$ and $f_1, \dots, f_s \in K[x_1, \dots, x_n]$. This is known as the Hilbert Basis Theorem.

5 Monomial Ordering

For polynomials of a single variable, it is easy to order the terms according to degree. Example 4.5 demonstrates that this does not work for polynomials of multiple variables. We need a different approach to ordering polynomials in $K[x_1, \dots, x_n]$.

We will use the convention that $x_1 > x_2 > \dots > x_n$. Suppose we have two monomials, x^{α} and x^{β} , where $x = (x_1, \dots, x_n)$, $\alpha = (\alpha_1, \dots, \alpha_n)$, and

$\beta = (\beta_1, \dots, \beta_n)$. We need some way of defining what it means for $\alpha > \beta$. Then it is not too difficult to see that the ordering on x_1, \dots, x_n and $\alpha > \beta$ will allow us to say $x^\alpha > x^\beta$.

We need to define our ordering in such a way that we are guaranteed that one of the following holds:

$$x^\alpha > x^\beta \tag{2}$$

$$x^\alpha = x^\beta \tag{3}$$

$$x^\alpha < x^\beta. \tag{4}$$

Definition 5.1 A **total ordering** on $K[x_1, \dots, x_n]$ is a relation $>$ such that the following hold.

1. If $x^\alpha > x^\beta$ and if $x^\alpha < x^\beta$, then If $x^\alpha = x^\beta$. (Antisymmetric)
2. $<$ is transitive.
3. One of (1), (2), and (3) listed above holds. (Completeness)

Definition 5.2 A **well-order** on a set is a total ordering such that any nonempty subset has a smallest element.

Example 5.3 The natural numbers are a well-ordered set.

Definition 5.4 We define a **monomial ordering** on $K[x_1, \dots, x_n]$ as a relation $>$ on the set of monomials x^α such that

1. $>$ is a total ordering.
2. If $x^\alpha > x^\beta$, and x^γ is another monomial, then $x^\alpha x^\gamma > x^\beta x^\gamma$.
3. $>$ is a well-ordering.

The best way to understand the definition is probably by example.

Example 5.5 Write $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_n)$. Then $\alpha >_{lex} \beta$ if in the difference $\alpha - \beta$, the left-most nonzero entry is positive. By difference, we mean vector difference. If $\alpha >_{lex} \beta$, then $x^\alpha >_{lex} x^\beta$. This order is called **lexicographic**, and it is a monomial ordering.

Notice that $x_1 >_{lex} \dots >_{lex} x_n$. We can rewrite this as $(1, 0, 0, \dots, 0) >_{lex} (0, 1, 0, \dots, 0) >_{lex} \dots >_{lex} (0, 0, 0, \dots, 1)$.

Let $f(x, y, z) = 2x^2y^3z + 3x^2y^2z^2 - 5x^3 \in \mathbb{Z}[x, y, z]$. In this case $x >_{lex} y >_{lex} z$. Recall $\alpha = (2, 3, 1), \beta = (2, 2, 2)$, and $\gamma = (3, 0, 0)$. Then the terms are ordered in the following way: $-5x^3 >_{lex} 2x^2y^3z >_{lex} 3x^2y^2z^2$.

Notice that lexicographic order, or lex, is used to order words in the dictionary. This is where it gets its name. There are many other monomial orderings, but lexicographic will serve our purposes.

5.1 Exercise

1. Order the following monomials using lex with $x > y > z$.

(a) $-3x^3y^2z^2$

(b) $5x^3y^2z$

(c) $x^3y^3z^4$

(d) $-x^3y^2z^4$

(e) $x^2y^2z^2$

Now that we know how to order monomials, we can discuss how to order the terms in a polynomial.

Definition 5.6 We define the **multidegree** of a polynomial $f = \sum_{\alpha} a_{\alpha}x^{\alpha} \in K[x_1, \dots, x_n]$ by the maximum value α . The maximum is found using the chosen monomial order. We denote the multidegree of f by $\text{multideg}(f)$.

Definition 5.7 The **leading coefficient** of f is denoted by $LC(f)$ is is the value of a_{α} corresponding to the $\text{multideg}(f) = \alpha$.

Definition 5.8 The **leading monomial** of f is $\mathbf{x}^{\text{multideg}(f)}$ and is denoted $LM(f)$.

Definition 5.9 The **leading term** of f is the leading coefficient times the leading monomial. We can write this $LT(f) = LC(f) \cdot LM(f)$.

Example 5.10 If we use lex order on $f(x, y, z) = 2x^2y^3z + 3x^2y^2z^2 - 5x^3$, then we get the following:

1. $\text{multideg}(f) = (3, 0, 0)$.

2. $LC(f) = -5$.

3. $LM(f) = x^3$.

4. $LT(f) = -5 \cdot x^3 = -5x^3$.

5. $f(x, y, z) = -5x^3 + 2x^2y^3z + 3x^2y^2z^2$ is written in decreasing order.

6 Division in $K[x_1, \dots, x_n]$

Now that we can order the terms of a polynomial in $K[x_1, \dots, x_n]$, we can perform division in $K[x_1, \dots, x_n]$.

Theorem 6.1 Fix a term order. (We will use lex). Let F be the set (f_1, \dots, f_s) of polynomials in $K[x_1, \dots, x_n]$. Let $f \in K[x_1, \dots, x_n]$. Then we can write $f = a_1f_1 + \dots + a_sf_s + r$, where r is either zero or no monomial in r is divisible by any leading term of the f_i .

We will denote the remainder of division of f by F by \bar{f}^F . The pseudocode for division is given below as it appears in [3].

Algorithm 6.2 Let $f \in K[x_1, \dots, x_n]$ and $F = (f_1, \dots, f_s)$.

Set $a_i := 0 \forall i$, $r := 0$, $p := f$

Is $LT(p)$ divisible by $LT(f_i)$ for some i ?

If yes, take the smallest value of i and set $a_i := a_i + \frac{LT(p)}{LT(f_i)}$, $p := p - \frac{LT(p)}{LT(f_i)}p_i$.

If $LT(p)$ is not divisible by one of $LT(f_i)$, then let $p := p - LT(p)$ and $r := r + LT(p)$.

Is $p = 0$? If it is then stop.

If $p \neq 0$ then check to see if $LT(p)$ is divisible by $LT(f_i)$ for some i and proceed until $p = 0$.

Example 6.3 Let $f = x^2y^2z + xz$ and $F = (f_1, f_2)$, where $f_1 = xy - z$ and $f_2 = z$. The leading term of f is x^2y^2z and is divisible by $LT(f_1) = xy$. Then $a_1 = xyz$ and we set $f = p = xyz^2 + xz$. The leading term of p is xyz^2 which is also divisible by $LT(f_1) = xy$. Then $a_1 = xyz + z^2$ and p becomes $xz + z^3$. So $LT(p) = xz$, which is divisible by $LT(f_2) = z$. Then $a_2 = x$ and $p = z^3$. We get $LT(p) = z^3$ divisible by $LT(f_2) = z$. Finally we set $a_2 = x + z^2$ and $p = 0$. Therefore we can write $f = (xyz + z^2)f_1 + (x + z^2)f_2$.

6.1 Exercises

1. Verify that $f = (xyz + z^2)f_1 + (x + z^2)f_2$ from example 6.3.
2. Divide $f = x^2y + xy^2 + y^2$ by $f_1 = y^2 - 1$ then by $f_2 = xy - 1$. Use this to write $f = a_1f_1 + a_2f_2 + r$.
3. Divide f by f_2 then f_1 .
4. What do you notice about the remainder?

7 S-Polynomials

Recall that our ultimate goal is to determine whether or not polynomials in $K[x_1, \dots, x_n]$ have common solutions. We would also like to determine what those solutions are. In order to achieve this goal, we will look at the ideal generated by the polynomials of interest. We will describe a method for manipulating these polynomials to get an equivalent set of polynomial generators, called a Groebner basis. A Groebner basis will make it easy to see if there is a common solution to the polynomials. Note that this is exactly what we do for linear systems and univariate systems using Gaussian elimination and the Euclidean algorithm, respectively. A key concept we will use is that of S-polynomials.

Definition 7.1 Let $f, g \in K[x_1, \dots, x_n]$ be nonzero. Let $\text{multideg}(f) = \alpha$ and $\text{multideg}(g) = \beta$. Then define $\gamma = (\gamma_1, \dots, \gamma_n)$ for $\gamma_i = \max(\alpha_i, \beta_i)$. Then the monomial x^γ is called the **least common multiple** of $LM(f)$ and $LM(g)$. We denote this by $LCM(LM(f), LM(g))$.

Definition 7.2 We define the **S-polynomial** for polynomials f and g by $S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g$, where $x^\gamma = LCM(LM(f), LM(g))$.

Example 7.3 Let $f = x^3y^2 - x^2y^3 + x$ and $g = 3x^4y + y^2$ in $\mathbb{R}[x, y]$. Using lex order, $LM(f) = x^3y^2$ and $LM(g) = x^4y$. Notice that $LCM(LM(f), LM(g)) = x^4y^2$. Then $S(f, g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g = x \cdot f - \frac{1}{3}y \cdot g = x^4y^2 - x^3y^3 + x^2 - (x^4y^2 + \frac{1}{3}y^3) = -x^3y^3 + x^2 - \frac{1}{3}y^3$.

Notice that the S-polynomial, $S(f, g)$, cancels the leading terms of f and g . Also observe that $S(f, g) = -S(g, f)$.

Example 7.4 Consider the linear equations $f = x + 2y - z$ and $g = -3x - y + 4z$. Use lex order with $x > y > z$. Then $s = S(f, g) = -5y - z$. Notice that this eliminated one of the variables. This would allow us to solve the homogeneous system by writing y in terms of z and then solving for x in terms of z . We observe then that for linear equations the S-polynomial behaves like row reduction.

Example 7.5 Now look at the univariate system in $\mathbb{C}[x]$.

$$\begin{aligned} f &= 2x^3 - 7x^2 + 9x - 4 = 0 \\ g &= 2x^2 - 5x + 4 = 0 \end{aligned}$$

Then $S(f, g) = -2x^2 + 5x - 4 = -gcd(f, g)$. We see that the S-polynomial is acting like the division algorithm for a univariate system.

Maple has a command for calculating S-polynomials. This command is in the Groebner package. We include this package by typing “with(Groebner)” at the top of the worksheet. The command is $S\text{Polynomial}(f, g, \text{order})$, where f and g are polynomials and order is the monomial order we are using. To use lex order with $x > y > z$, the command is $\text{plex}(x, y, z)$.

7.1 Exercises

1. Let $f = 4x^2z - 7y^2$ and $g = xyz^2 + 3xz^4$. Find $S(f, g)$.
2. Use the S-polynomial to solve the following system. Verify your solution.

$$\begin{aligned} f = x + 2y + 3z &= 0 \\ g = -2x - y - z &= 0 \end{aligned}$$

8 Groebner Bases

We can use S -polynomials to define a Groebner basis.

Definition 8.1 Let $I = \langle f_1, \dots, f_s \rangle \in K[x_1, \dots, x_n]$. Then $G = \{g_1, \dots, g_t\} \in K[x_1, \dots, x_n]$ is a **Groebner basis** if and only if $\overline{S(g_i, g_j)}^G = 0$ for all $i \neq j$.

We can use **Maple** to find the remainder of a polynomial under division by a set of polynomials. Again the command for this is in the Groebner package. The command is `NormalForm(f, g, order)` where f is a polynomial and g is the list of polynomials we divide by. Again, we will use `plex(x1, ..., xn)` for lex order.

Example 8.2 Suppose $f = xy^2 + x^2y + y^2$ and we wish to divide by $G = \{xy - 1, y^2 - 1\}$. We can use the following Maple code.

```
> with(Groebner);
> f := x*y^2+x^2*y+y^2:
> G := {x*y-1, y^2-1}:
> NormalForm(f, G, plex(x, y));
1 + y + x
```

Then f divided by the polynomials in G has a remainder of $1 + x + y$.

Theorem 8.3 Every nonzero ideal $I \in K[x_1, \dots, x_n]$ has a Groebner basis, G , with respect to a fixed monomial order. The set G is also a basis for the ideal I .

We will not go through the proof of this theorem. To prove it, we would present an algorithm and show that the algorithm terminates and gives us what we want. We will present the pseudocode for Buchberger's algorithm as it appears in [3].

Algorithm 8.4 (Buchberger's Algorithm) Let $I = \langle f_1, \dots, f_s \rangle \in K[x_1, \dots, x_n]$ be a nonzero ideal. We would like to find a Groebner basis G for I .

Input: $F = (f_1, \dots, f_s)$

Output: G

Let $G := F$.

Repeat the following steps:

$G' = G$

For each pair of distinct $\{p, q\} \in G'$, let $S := \overline{S(p, q)}^{G'}$.

If $S \neq 0$, then set $G := G \cup \{S\}$.

Stop when $G = G'$.

In words, we look at each pair f_i, f_j , $i \neq j$, in F and calculate the S -polynomial. Then divide the S -polynomial by the set F . If the remainder is nonzero, we add it to F . Then we repeat the process for each pair until all remainders are zero. Notice that once you get a zero remainder for a pair, you don't need to retest that pair. Once zero, the remainder will remain zero regardless of the addition of more polynomials.

8.1 Exercise

1. Use Buchberger's algorithm with **Maple** to calculate a Groebner basis for $I = \langle x^2y - 1, xy^2 - x \rangle$. (Use lex order).

Recall that in $K[x_1, \dots, x_n]$, when we divide f by $\{f_1, \dots, f_s\}$, the remainder is not unique as it was for division in $K[x]$. As a result, Groebner bases are not unique. We may also end up with more polynomials than we need to generate I .

Lemma 8.5 *Suppose G is a Groebner basis for an ideal $I \subseteq K[x_1, \dots, x_n]$. Let $p \in G$ such that $LT(p) \in \langle LT(G - \{p\}) \rangle$. Then $G - \{p\}$ is a Groebner basis for I .*

Definition 8.6 *A minimal Groebner basis for $I \subseteq K[x_1, \dots, x_n]$ is a Groebner basis G such that the following hold.*

1. The leading coefficient of each $p \in G$ is 1.
2. For any polynomial $p \in G$, $LT(p)$ is not in the ideal generated by $\{LT(G - \{p\})\}$

This gets rid of the redundant polynomials in a Groebner basis G . It does not guarantee uniqueness. We can further reduce a Groebner basis.

Definition 8.7 *A Groebner basis G is called a reduced Groebner basis if the following are satisfied.*

1. The leading coefficient of each polynomial in G is one.
2. Any monomial of a polynomial p in G is not in the ideal generated by the leading terms of the other polynomials in G . (i.e., Any monomial in p does not lie in $\langle LT(G - \{p\}) \rangle$).

Theorem 8.8 *Let $I \subseteq K[x_1, \dots, x_n]$ be a nonzero ideal. Then I has a unique reduced Groebner basis with respect to the given monomial order.*

Observe what happens when $\{f_1, \dots, f_s\} \in K[x_1, \dots, x_n]$ are linear.

Example 8.9 *Consider the system of linear equations*

$$\begin{aligned} 3x - 6y - 2z &= 0 \\ 2x - 4y + 4w &= 0 \\ x - 2y - z - w &= 0. \end{aligned}$$

Then $I = \langle f = 3x - 6y - 2z, g = 2x - 4y + 4w, h = x - 2y - z - w \rangle$ is the ideal in $K[x, y, z]$ associated with this system. We will calculate a Groebner basis for I . Suppose $x > y > z$ and use lex order. The polynomial $S(f, g)$ is the only one that will give a nonzero remainder when divided by $\{f, g, h\}$. Then a

Groebner basis for I is $G = \{3x-6y-2z, 2x-4y+4w, x-2y-z-w, -4z-12w\}$.

Then a minimal Groebner basis is $G' = \{x-2y-z-w, z+3w\}$. The reduced Groebner basis for I is $\tilde{G} = \{x-2y+2w, z+3w\}$.

Recall that the matrix associated with our system of linear equations is the following.

$$A = \begin{pmatrix} 3 & -6 & -2 & 0 \\ 2 & -4 & 0 & 4 \\ 1 & -2 & -1 & -1 \end{pmatrix}.$$

Writing the matrix associated with the equations in G' we get the following row echelon matrix.

$$\begin{pmatrix} 1 & -2 & -1 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The reduced Groebner basis gives us the matrix below, which is in row reduced echelon form.

$$\begin{pmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Observe then that finding a minimal Groebner basis and/or a reduced Groebner basis with respect to lex ordering generalizes row reduction for polynomial equations. As with row reduction, Groebner basis calculations will simplify the problem of finding solutions to systems of polynomial equations. Groebner bases also allow us to test ideal membership.

Theorem 8.10 *Let G be a Groebner basis for $I = \langle f_1, \dots, f_s \rangle \subseteq K[x_1, \dots, x_n]$, and let $f \in K[x_1, \dots, x_n]$. Then $f \in I$ if and only if dividing f by G results in a zero remainder.*

This simply says that f is in the ideal if and only if f can be written as a finite combination of elements in the Groebner basis G . In the exercises in 6.1, we gave an example of a polynomial f and a set $F = \{f_1, f_2\}$ where the remainder depends on how we list the polynomials in F . One can show that the remainder under division by a Groebner basis is unique. The remainder does not depend on the order in which we list elements of G .

Example 8.11 *Let $I \in K[x, y, z]$ be generated by $\{-x^3 + y, x^2y - z\}$. Is $f = xy^3 - z^2 + y^5 - z^3$ in I ?*

The reduced Groebner basis for I is $G = \{y^5 - z^3, -y^2 + zx, y^3x - z^2, x^2y - z, x^3 - y\}$. We find that $\bar{f}^G = xy^3 - z^2$, so f is not in I .

Let $g = -x^4 + xy + x^3yz - xz^2$. Is g in I ? Notice $\bar{g}^G = 0$, so g is in I .

Example 8.12 Let $I = \langle x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z \rangle \subseteq K[x_1, \dots, x_n]$. This corresponds to the system:

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

We would like to see if these polynomials have a common solution. Start by finding a Groebner basis $G = \{2x - 1, 3y + z - 1, 40z^2 - 8z - 23\}$. Notice that the first polynomial depends only on z , and the third polynomial depends only on x . We have reduced the problem to the following equivalent system:

$$\begin{aligned} 2x &= 1 \\ 3y + z &= 1 \\ 40z^2 - 8z - 23 &= 0 \end{aligned}$$

These equations are easy to solve. We get the following solutions $\{(\frac{1}{2}, \frac{3}{10} - \frac{\sqrt{26}}{20}, \frac{1}{10} + \frac{3\sqrt{26}}{20}), (\frac{1}{2}, \frac{3}{10} + \frac{\sqrt{26}}{20}, \frac{1}{10} - \frac{3\sqrt{26}}{20})\}$.

Sometimes we want to know if the polynomials $f_1, \dots, f_s \in K[x_1, \dots, x_n]$ have a common solution, but we don't necessarily want to find the solution. We answer this question using the following theorem.

Theorem 8.13 (Weak Nullstellensatz) Let K be algebraically closed, and let $f_1, \dots, f_s \in K[x_1, \dots, x_n]$. The polynomials fail to have a common solution if and only if $1 \in I = \langle f_1, \dots, f_s \rangle$.

The question now becomes: How can we tell if $1 \in I$? We can tell by looking at the reduced Groebner basis.

Theorem 8.14 Let $I \in K[x_1, \dots, x_n]$ be an ideal such that $1 \in I$. Then the reduced Groebner basis for I is $G = \{1\}$.

Proof 8.15 Suppose $1 \in I$. Then $I = \langle 1 \rangle$. Let $G = \{g_1, \dots, g_t\}$ be a Groebner basis for I . Since $1 \in I$ we can conclude that 1 divided by G results in a zero remainder. This implies that g_i is constant for some i . Recall that the remainder under division by a Groebner basis is unique regardless of the order the elements are listed in. Relist the elements so that g_1 is constant. Then the rest of the elements of G are constant multiples of g_1 . By Lemma 8.5, we can remove g_2, \dots, g_t from G . Multiply g_1 by an appropriate constant to get $g_1 = 1$. Then $G = \{1\}$ is the unique reduced Groebner basis for I .

We can use **Maple** to calculate a Groebner basis using the command $\text{Basis}(F, \text{order})$, where F is a list of polynomials and order is the monomial ordering.

Consider example 1.1 above. In order to determine whether the graph is 3-colorable, we find the Groebner basis for the ideal $I = \langle x_1^2 + x_1x_2 + x_2^2, x_1^2 + x_1x_4 + x_4^2, x_2^2 + x_2x_4 + x_4^2, x_2^2 + x_2x_3 + x_3^2, x_2^2 + x_2x_5 + x_5^2, x_3^2 + x_3x_4 + x_4^2, x_3^2 + x_3x_5 + x_5^2, x_4^2 + x_4x_5 + x_5^2 \rangle$. (I is the ideal generated by the polynomials associated with the graph.)

8.2 Exercises

1. Use Maple to calculate a Groebner basis for the ideal I from example 1.1.
2. Refer back to Exercise 1.1 and determine whether or not the graph is 3-colorable.
3. Consider the graph in Figure 5.
 - (a) List the polynomials associated with this graph.
 - (b) Find a Groebner basis for the ideal generated by the associated polynomials.
 - (c) Determine whether or not the graph is 3-colorable.

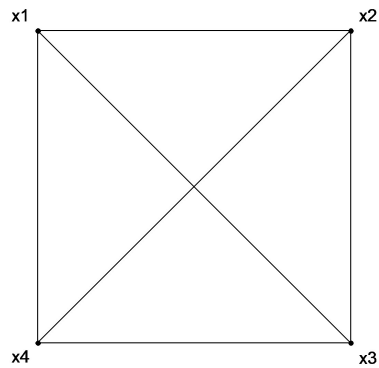


Figure 5: Graph with 4 Vertices

References

- [1] Adams, William W. and Loustaunau, Philippe. *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, Vol. 3. Providence, Rhode Island: American Mathematical Society, 1994.
- [2] Anton, Howard and Rorres, Chris. *Elementary Linear Algebra: Applications Version*. New York: John Wiley and Sons, Inc., 2000.
- [3] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Texts in Mathematics. New York, New York: Springer-Verlag New York Inc., 1997.
- [4] Gallian, Joseph A. *Contemporary Abstract Algebra*. Boston, New York: Houghton Mifflin Company, 2002.