Gröbner Bases and their Applications

Kaitlyn Moran

July 30, 2008

1 Introduction

We know from the Hilbert Basis Theorem that any ideal in a polynomial ring over a field is finitely generated [3]. However, there remains question as to the best generators to choose to describe the ideal. Are there generators for a polynomial ideal I that make it easy to see if a given polynomial f belongs to I? For instance, does $2x^2z^2 + 2xyz^2 + 2xz^3 + z^3 - 1$ belong to $I = (x + y + z, xy + xz + yz, xyz - 1)$? Deciding if a polynomial is in an ideal is called the Ideal Membership Problem. In polynomial rings of one variable, we use long division of polynomials to solve this problem. There is a corresponding algorithm for $K[x_1, \ldots, x_n]$, but because there are multiple variables and multiple divisors, the remainder of the division is not unique. Hence a remainder of 0 is a sufficient condition, but not a necessary condition, to determine ideal membership. However, if we choose the correct divisors, then the remainder is unique regardless of the order of the divisors. These divisors are called a Gröbner basis.

In order to define Gröbner bases, we must first discuss monomial orderings.

2 Monomial Orderings

Let K be a field. In $K[x]$, we write polynomials in a canonical way, with the term of highest degree first and each subsequent term of lesser degree than the preceding one. This assists in the long division of polynomials, for we divide the term of highest degree of the dividend by the term of highest degree of the divisor, and if it is not divisible, then we are done. In order to generalize this division algorithm, we must have a corresponding ordering on monomials in $K[x_1, \ldots, x_n]$, called a monomial ordering.

Definition 1. A *monomial ordering* is an order relation $<$ on the set of all monomials of $K[x_1, \ldots, x_n]$ such that

- For any monomials m, n, then exactly one of the following is true:$m < n$, $n < m$, or $m = n$

- If $m_1 < m_2$ and $m_2 < m_3$, then $m_1 < m_3$
- For any monomial $m \neq 1$, $1 < m$
- If $m_1 < m_2$, then $nm_1 < nm_2$ for any monomial n

To discuss the four common examples of monomial orderings, it is helpful to first define a way of discussing the degree of a multivariable monomial, called multidegree.

Definition 2. The *multidegree* of a monomial $m = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ is defined to be $\mathrm{mdeg}(m) = i_1 + \cdots + i_n$.

Now we consider some examples of monomial orderings.

Example 1. Four common monomial orderings are Lex, Deglex, Revlex, and Degrevlex.

- In Lex, the lexicographic ordering, $m_1 = x_1^{i_1} \cdots x_n^{i_n} < x_1^{j_1} \cdots x_n^{j_n} = m_2$ if $i_1 = j_1, \ldots, i_{k-1} = j_{k-1}, i_k < j_k$ for some k. That is, $m_1 < m_2$ if the first variable with different exponents has a lower degree in m_1 than in m_2. Notice this is alphabetical ordering, like words in a dictionary.
- In Deglex, $m_1 = x_1^{i_1} \cdots x_n^{i_n} < x_1^{j_1} \cdots x_n^{j_n} = m_2$ if $\mathrm{mdeg}(m_1) < \mathrm{mdeg}(m_2)$ or if $\mathrm{mdeg}(m_1) = \mathrm{mdeg}(m_2)$ and $m_1 < m_2$ with respect to Lex.
- In Revlex, $m_1 = x_1^{i_1} \cdots x_n^{i_n} < x_1^{j_1} \cdots x_n^{j_n} = m_2$ if $i_n = j_n, \ldots, i_{k+1} = j_{k+1}, i_k > j_k$ for some k. That is, $m_1 < m_2$ if the last variable with different exponents has a higher degree in m_1 than in m_2.
- In Degrevlex, $m_1 = x_1^{i_1} \cdots x_n^{i_n} < x_1^{j_1} \cdots x_n^{j_n} = m_2$ if $\mathrm{mdeg}(m_1) < \mathrm{mdeg}(m_2)$ or if $\mathrm{mdeg}(m_1) = \mathrm{mdeg}(m_2)$ and $m_1 < m_2$ with respect to Revlex.

Each monomial ordering depends on the ordering of the variables. For instance, Lex with the ordering $x > y > z$ is a different ordering than Lex with $y > x > z$. In the above examples, we order $x_1 > x_2 > \cdots > x_n$, but this is arbitrary. Hence for each of the four common monomial orderings, we have $n!$ possible orderings.

Once a monomial ordering is chosen, then the terms of a polynomial can be ordered in an unambiguous way, where each term is less than the preceding term with respect to the chosen ordering. For example, let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$, with $x > y > z$. Each monomial ordering gives a different reordering of the terms of f.

- With respect to Lex, $f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$.
- With respect to Deglex, $f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2$.

- With respect to Revlex, $f = -5x^3 + 4xy^2z + 4z^2 + 7x^2z^2$.
- Finally, with respect to Degrevlex, $f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2$.

This allows us to define some necessary vocabulary for discussing Gröbner bases.

Definition 3. Let $<$ be a monomial ordering on $K[x_1, \dots, x_n]$, and let $f \in K[x_1, \dots, x_n]$, $f \neq 0$. Then f can be uniquely written as $f = c_1m_1 + \cdots + c_km_k$, where $m_1 > m_2 > \cdots > m_k$, and $c_i \neq 0 \; \forall i = 1, \dots, k$. The *leading monomial* of f is $\textsc{lm}(f) = m_1$. The *leading coefficient* of f is $\textsc{lc}(f) = c_1$. The *leading term* of f is $\textsc{lt}(f) = \textsc{lc}(f)\,\textsc{lm}(f) = c_1m_1$.

If I is an ideal in $K[x_1, \dots, x_n]$, we define $\textsc{lm}(I)$ to be the ideal generated by the leading monomials of all elements of I.

Now, one may think that $\textsc{lm}(I)$ is just the ideal generated by the leading monomials of the generators of I, but this is not the case. For example, if $I = (x+y+z, xy+xz+yz, xyz-1)$, and our monomial ordering is Revlex, then the ideal generated by the leading monomials of the generators is $J = (x, xy, xyz) = (x)$. However, $y^2 + yz + z^2 = (y+z)(x+y+z) - (xy + xz + yz) \in I$, so $y^2 \in \textsc{lm}(I)$, but $y^2 \notin J$. However, Gröbner bases provide a simple way to find generators for $\textsc{lm}(I)$, and in fact are defined to have this property.

3 Gröbner Bases

As aforementioned, there is a division algorithm for $K[x_1, \dots, x_n]$, which is a generalization of the traditional approach of long division of polynomials. It involves simultaneously dividing multiple divisors into multiple dividends. In order to understand the usefulness of Gröbner bases, we must first discuss this algorithm.

3.1 A Division Algorithm

In $K[x]$, we divide one polynomial by another through comparing their leading terms. Similarly, in $K[x_1, \dots, x_n]$, we compare leading terms. If the leading term of one of the divisors divides the leading term of the dividend, we multiply that divisor by an appropriate monomial and cancel the leading terms. This is best seen through examples.

Example 2. We will divide $f = xy_1$ by $f_1 = xy + 1$ and $f_2 = y + 1$, using Lex ordering with $x > y$. We may set up our division as follows, leaving space for the necessary monomials:

$$\begin{array}{rl} a_1 : & \\ a_2 : & \\ \begin{array}{r} xy+1 \\ y+1 \end{array} & \sqrt{xy^2+1} \end{array}$$

Now, because f_1 is listed first, we consider $\textsc{lt}\, f$ and $\textsc{lt}\, f_1$. Since $\textsc{lt}\, f_1$ divides $\textsc{lt}\, f$, we write the quotient q in a_1 and then subtract $q \cdot f_1$ from f.

$$\begin{array}{rc}
a_1: & y \\
a_2: & \\
\begin{array}{r} xy+1 \\ y+1 \end{array} & \sqrt{xy^2+1} \\
 & xy^2+y \\
\cline{2-2}
 & -\,y+1
\end{array}$$

Now we repeat the process on the new polynomial p. Since $\textsc{lt}\, f_1$ does not divide $\textsc{lt}\, p$ but $\textsc{lt}\, f_2$ does, we write the quotient in a_2 and then multiply and subtract.

$$\begin{array}{rc}
a_1: & y \\
a_2: & -1 \\
\begin{array}{r} xy+1 \\ y+1 \end{array} & \sqrt{xy^2+1} \\
 & xy^2+y \\
\cline{2-2}
 & -\,y+1 \\
 & -\,y-1 \\
\cline{2-2}
 & 2
\end{array}$$

Because neither $\textsc{lt}\, f_1$ nor $\textsc{lt}\, f_2$ divides the new polynomial, this is our remainder. Hence,

$$\underbrace{xy^2+1}_{f} = (\underbrace{\ y\ }_{a_1})(\underbrace{xy+1}_{f_1}) + (\underbrace{-1}_{a_2})(\underbrace{y+1}_{f_2}) + \underbrace{\ 2\ }_{r}.$$

The previous example ends with a nice remainder. However, it is possible to have a remainder with a leading term that is not divisible by any of the leading terms of the divisors, but one of the leading terms of the divisors divides a different term of the remainder. In this case, the division can continue by moving the leading term to a "remainder" column.

Example 3. Let $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$, and $f_2 = y^2 - 1$. We will use Lex ordering with $x > y$. Performing long division, we see

$$\begin{array}{rlll}
a_1: & x+y & & \\
a_2: & 1 & & r \\
xy-1 & & & \underline{\qquad\quad} \\
y^2-1 & \sqrt{x^2y+xy^2+y^2} & & \\
 & \underline{x^2y-x} & & \\
 & \qquad xy^2+x+y^2 & & \\
 & \qquad \underline{xy^2-y} & & \\
 & \qquad\qquad \underline{x+y^2+y} & & \\
 & \qquad\qquad\quad y^2+y & \rightarrow x & \\
 & \qquad\qquad\quad \underline{y^2-1} & & \\
 & \qquad\qquad\qquad \underline{y+1} & & \\
 & \qquad\qquad\qquad\quad 1 & \rightarrow x+y & \\
 & \qquad\qquad\qquad\quad \overline{0} & \rightarrow x+y+1 &
\end{array}$$

Hence,

$$\underbrace{xy^2+xy^2+y^2}_{f} = (\underbrace{x+y}_{a_1})(\underbrace{xy-1}_{f_1}) + (\underbrace{1}_{a_2})(\underbrace{y^2-1}_{f_2}) + \underbrace{x+y+1}_{r}.$$

This example is a fairly complete illustration of the division algorithm. For a statement of the general algorithm, the reader may consult [1], page 62. This division algorithm proves the following proposition.

Proposition 4 (Division Algorithm)**.** Fix a monomial ordering. Let $F = (f_1, \dots, f_m)$ be an ordered m-tuple of polynomials in $K[x_1, \dots, x_n]$. Then for every $f \in K[x_1, \dots, x_n]$, f can be written as

$$f = a_1 f_1 + \cdots + a_m f_m + r$$

for some $a_1, \dots, a_n, r \in K[x_1, \dots, x_n]$, where no term of r is divisible by $\text{LT}(f_1), \dots, \text{LT}(f_m)$. We call r the *remainder* of f on division by F.

3.2 Gröbner Bases and Some Properties

Now, we know the division algorithm gives a remainder. However, unlike the familiar division algorithm in one variable, the remainder from this division algorithm is not unique. For example, let $I = (g_1, g_2) = (x^2, xy - y^2)$ and let $f = x^2y$. Now, $f \in I$ since f is a nonzero multiple of one of the generators of I, and so by dividing first by g_1, the remainder of f is 0.

However, by dividing first by g_2, we see

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

This gives the remainder of f is y^3, but $y^3 \neq 0$. Hence the remainder is not unique. However, if we choose the right generators, the remainder is unique, and so it is easy to solve the Ideal Membership Problem. These generators are a Gröbner basis.

Definition 5. Let I be an ideal in $K[x_1, \ldots, x_n]$. A set $g_1, \ldots, g_m$, where $g_i \in I \; \forall 1 \leq i \leq m$, is a Gröbner basis for I if $(\text{LM}(g_1), \ldots, \text{LM}(g_m)) = \text{LM}(I)$.

Proposition 6. If $g_1, \ldots, g_m$ is a Gröbner basis for an ideal I, then $(g_1, \ldots, g_m) = I$.

Proof. Clearly, $(g_1, \ldots, g_m) \subset I$, since $g_i \in I$ for all $1 \leq i \leq m$. Let $f \in I$. Then we can divide f by $\{g_1, \ldots, g_m\}$, so f can be written as

$$f = a_1 g_1 + \cdots + a_m g_m + r$$

where no term in r is divisible by $\text{LM}(g_i)$ for any $i = 1, \ldots, m$. We must show that $r = 0$. Notice that

$$r = f - a_1 g_1 + \cdots + a_m g_m \in I.$$

If $r \neq 0$, $\text{LM}(r) \in \text{LM}(I) = (\text{LM}(g_1), \ldots, \text{LM}(g_m))$. Thus, because $\text{LM}(r)$ is a monomial, $\text{LM}(r)$ must be divisible by some $\text{LM}(g_i)$. This is a contradiction, so $r = 0$ and therefore $f \in (g_1, \ldots, g_m)$. □

Proposition 7. Every ideal $I \subset K[x_1, \ldots, x_n]$ other than (0) has a Gröbner basis.

Proof. $\text{LM}(I)$ is generated by the monomials $\text{LM}(g)$, where $g \in I \setminus \{0\}$. Because $\text{LM}(I) \subset K[x_1, \ldots, x_n]$, $\text{LM}(I)$ is finitely generated, so there exist $g_1, \ldots, g_m$ such that $\text{LM}(I) = (\text{LM}(g_1), \ldots, \text{LM}(g_m))$. By Proposition 6, $\{g_1, \ldots, g_m\}$ generate I. □

Theorem 8. Let $G = (g_1, \ldots, g_m)$ be a Gröbner basis for an ideal I. Let $f \in K[x_1, \ldots, x_n]$. Then there exists a unique $r \in K[x_1, \ldots, x_n]$ such that (i) no term of r divides $\text{LM}(g_i)$ for any i, and (ii) there exists a $g \in I$ such that $f = g + r$.

Proof. The division algorithm for $K[x_1, \ldots, x_n]$ gives $f = a_1 g_1 + \cdots + a_m g_m + r$, which satisfies (i). Define $g = a_1 g_1 + \cdots + a_m g_m$ to satisfy (ii).

To prove uniqueness, let $f = g + r_1 = h + r_2$ as in (ii). Then $r_1 - r_2 = h - g \in I$. Hence, if $r_1 \neq r_2$, then $\text{LM}(r_1 - r_2) \in \text{LM}(I)$, so $\text{LM}(r_1 - r_2)$ is divisible by some $\text{LM}(g_i)$, since $\text{LM}(I)$ is a monomial ideal. However, this contradicts the assumption that no term of r_1 or r_2 divides $\text{LM}(g_i)$ for any i. Hence $r_1 - r_2 = 0$. Therefore, r is unique. □

The r in Theorem 8 denotes the remainder of division of f by G, and the uniqueness of r guarantees that r is the remainder regardless of the order of the elements of G in the division algorithm. This gives us a necessary and sufficient condition for membership to I, thereby solving the Ideal Membership Problem.

Corollary 9. Let G be a Gröbner basis for an ideal I, and let $f \in K[x_1, \ldots, x_n]$. We write $f = g + r$ where $g \in I$ as above. Then $f \in I$ if and only if $r = 0$.

Proof. If $r = 0$, then clearly $f \in I$. If $f \in I$, then $f = f + 0$ satisfies the two conditions of Theorem 8. By uniqueness of r, this means 0 is the remainder of f on division by G. □

3.3 A Criterion for a Gröbner Basis

Now that we have seen uses for Gröbner bases, how do we determine if a given generating set $f_1, \ldots, f_k$ is a Gröbner basis? As discussed previously, not every generating set is a Gröbner basis, because sometimes there are combinations of the generators that have cancellations of leading terms, leaving only smaller terms. These smaller monomials now appear in $\text{LM}(I)$, but are not accounted for in the ideal generated by the leading monomials of the generators of I. For instance, let $I = (xy^2 - y^3, xy)$ and let the ordering be Revlex. Then $-y^3 = (xy^2 - y^3) - y(xy) \in I$, so $y^3 \in \text{LM}(I)$. But $y^3 \notin (\text{LM}(xy^2 - y^3), \text{LM}(xy)) = (xy^2, xy) = (xy)$. To study this, we look at special combinations of the generators, called syzygies and S-polynomials.

Definition 10. Let $R = K[x_1, \ldots, x_n]$, R^k a free module, $f \in R$ and $F = (f_1, \ldots, f_k) \in R^k$. A *syzygy* of F is an element $s = (s_1, \ldots, s_k) \in R^k$ such that $s_1 f_1 + \cdots + s_k f_k = 0$. A *representation* of f with respect to F is an element $H = (h_1, \ldots, h_k)$ such that $h_1 f_1 + \cdots + h_k f_k = f$.

Note that if H and H' are representations of f, then $H - H'$ is a syzygy of F. Similarly, if H is a representation and S is a syzygy of F, then $H + S$ is a representation of f with respect to F.

Proposition 11. Suppose $m_1, \ldots, m_k$ are monomials and $S = (s_1, \ldots, s_k)$ is a syzygy of $(m_1, \ldots, m_k)$. Let e_i denotes the ith basis element of the free module R^k, i.e., $e_i = (0, \ldots, 0, 1, 0 \ldots, 0)$. Then S is a linear combination of the syzygies

$$s_{ij} = \frac{\text{lcm}(m_i, m_j)}{m_i} e_i - \frac{\text{lcm}(m_i, m_j)}{m_j} e_j,$$

where $1 \leq i \leq j \leq k$.

Proof. Since $s_1m_1 + \cdots + s_km_k = 0$, the terms s_im_i must all cancel, so we can assume each s_j is of the form c_jn_j, where n_j is a monomial such that $n_jm_j = x_1^{i_1} \cdots x_n^{i_n} =: m$ for some $i_1, \ldots, i_n \in \mathbb{Z}^+$ for all j. Thus, $c_1 + \cdots + c_k = 0$. The solutions to this are linear combinations of $e_i - e_j$, $1 \le i \le j \le k$. Hence, $(s_1, \ldots, s_k)$ are linear combinations of

$$\frac{m}{m_i}e_i - \frac{m}{m_j}e_j,$$

which is a multiple of s_{ij}. □

Definition 12. Let f_1, f_2 be monic elements of R, and let $<$ be a monomial ordering on R. Then the *S-polynomial* of (f_1, f_2) on $<$ is

$$S(f_1, f_2) = \frac{\operatorname{lcm}(\textsc{lm}(f_1), \textsc{lm}(f_2))}{\textsc{lm}(f_1)}f_1 - \frac{\operatorname{lcm}(\textsc{lm}(f_1), \textsc{lm}(f_2))}{\textsc{lm}(f_2)}f_2.$$

Notice that S-polynomials are designed for cancellation of terms.

Theorem 13 (Criterion for a Gröbner basis)**.** Suppose I is a polynomial ideal, $G = \{f_1, \ldots, f_m\}$ is a basis for I, and $S_{i,j} = S(f_i, f_j)$ are the S-polynomials. Then G is a Gröbner basis of I if and only if for all pairs $i \neq j$, the remainder on division of $S_{i,j}$ by G is zero.

Proof. $\Rightarrow$: If G is a Gröbner basis, then all $S_{i,j} \in I$. Hence by Corollary 9, the remainder on division of $S_{i,j}$ is 0.

$\Leftarrow$: Assume the remainder of $S_{i,j}$ is 0, and let $f \in I$. We need to show that $\textsc{lm}(f) \in (\textsc{lm}(f_1), \ldots, \textsc{lm}(f_m))$. Because $\{f_1, \ldots, f_m\}$ generate I, we can write $f = a_1f_1 + \cdots + a_mf_m$ for some $a_1, \ldots, a_m \in R$. Now, either $\max\{\textsc{lm}(a_if_i)\} > \textsc{lm}(f)$ or $\max\{\textsc{lm}(a_if_i)\} = \textsc{lm}(f)$. In the latter case, then $\textsc{lm}(f) = \textsc{lm}(a_i)\,\textsc{lm}(f_i)$ for some i, so $\textsc{lm}(f) \in (\textsc{lm}(f_1), \ldots, \textsc{lm}(f_m))$, so assume the former is true.

Now, $A = (a_1, \ldots, a_m)$ is a representation of f. We will construct a syzygy Z such that $A' = A + Z$ is another representation of f with $\max\{\textsc{lm}(a_i'f_i)\} < \max\{\textsc{lm}(a_if_i)\}$. Because there is no strictly decreasing sequence of monomials, this process will eventually terminate, and then we will be in the case where $\max\{\textsc{lm}(a_if_i)\} = \textsc{lm}(f)$.

Let $J = \{j : \textsc{lm}(a_jf_j) = \max\{\textsc{lm}(a_if_i)\}\}$. We know the leading terms in $\sum_{i \in J} a_if_i$ cancel in order for $\textsc{lm}(f) < \max\{\textsc{lm}(a_if_i)\}$. Let $S_A = (s_1, \ldots, s_m)$ where $s_i = \textsc{lt}(a_i)$ if $i \in J$ and $s_i = 0$ otherwise. Then S_A is a syzygy for $(\textsc{lm}(f_1), \ldots, \textsc{lm}(f_m))$. By Proposition 11, S_A is a linear combination of s_{ij}'s, so $S_A = \sum_{1 \le i \le j \le m} t_{ij}s_{ij}$. By definition, the s_{ij} represents S_{ij} with respect to $F = (f_1, \ldots, f_m)$, so $s_1f_1 + \cdots + s_mf_m = \sum t_{ij}S_{ij}$. Now, since the remainder of S_{ij} is 0, S_{ij} is a linear combination of f_i's, so $S_{ij} = \sum_{t=1}^m h_{ij,t}f_t$. Now, $H_{ij} = (h_{ij,1}, \ldots, h_{ij,m})$

is a representation of S_{ij} with respect to F, so $s_{ij} - H_{ij}$ is a syzygy of F. Let

$$Z = \sum_{1 \leq i \leq j \leq m} t_{ij}(s_{ij} - H_{ij}),$$

which is also a syzygy of F. Hence, $A - Z = A' = (a'_1, \ldots, a'_m)$ is a representation of f with respect to F. By construction, $\max\{\text{LM}(a_i f_i)\} > \max\{\text{LM}(a'_i f_i)\}$. □

Example 4. We will show that $G = \{x^2, xy - y^2, y^3\}$ is a Gröbner basis for $I = (x^2, xy - y^2)$ with respect to Lex. Notice

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

Hence $y^3 \in I$, so G generates I. Now,

$$S_{1,2} = \frac{\text{lcm}(x^2, xy)}{x^2}(x^2) - \frac{\text{lcm}(x^2, xy)}{xy}(xy - y^2) = x^2y - x^2y + xy^2 = xy^2$$

$$S_{2,3} = \frac{xy^3}{xy}(xy - y^2) - \frac{xy^3}{y^3}y^3 = -y^4$$

$$S_{1,3} = \frac{x^2y^3}{x^2}x^2 - \frac{x^2y^3}{y^3}y^3 = 0$$

Clearly, both $S_{2,3}$ and $S_{1,3}$ give a remainder of 0 when divided by G. Because $xy^2 = y(xy - y^2) + y^3$, then the remainder of $S_{1,2}$ is also 0. Therefore, by Theorem 13, G is a Gröbner basis.

Example 5. Let $I = (x + y + z, xy + xz + yz, xyz - 1)$, $G = \{x + y + z, y^2 + yz + z^2, z^3 - 1\}$, and $I_G = (G)$. We will show that G is a Gröbner basis for I with respect to Lex. Notice

$$xy + xz + yz = (y + z)(x + y + z) - (y^2 + yz + z^2)$$

$$xyz - 1 = yz(x + y + z) - z(y^2 + yz + z^2) + (z^3 - 1)$$

$$y^2 + yz + z^2 = (y + z)(x + y + z) - (xy + xz + yz)$$

$$z^3 - 1 = z^2(x + y + z) - z(xy + xz + yz) + (xyz - 1)$$

Hence $I = I_G$. Now,

$$S_{1,2} = \frac{\text{lcm}(x, y^2)}{x}(x + y + z) - \frac{\text{lcm}(x, y^2)}{y^2}(y^2 + yz + z^2) = -xyz - xz^2 + y^3 + y^2z$$

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

$$S_{1,3} = z^3(x+y+z) - x(z^3-1) = x + yz^3 + z^4 = x + y + z + (y+z)(z^3-1)$$

$$S_{2,3} = z^3(y^2+yz+z^2) - y^2(z^3-1) = y^2 + yz^4 + z^5 = y^2 + yz + z^2 + (yz+z^2)(z^3-1)$$

Therefore, each S_{ij} is divisible by G, so G is a Gröbner basis.

3.4 Buchberger's Algorithm

By Proposition 7, we know that every ideal has a Gröbner basis. Buchberger's algorithm provides instructions to construct a Gröbner basis from any given generating set.

Given an ideal $I = (f_1, \ldots, f_m)$, calculate all of the S-polynomials. Divide the S-polynomials by $\{f_1, \ldots, f_m\}$.. If the remainder is nonzero, extend $(f_1, \ldots, f_m)$ with the remainder. Calculate all of the S-polynomials which have not previously been calculated, and repeat the process until all of the remainders of the S-polynomials are zero.

This process will terminate in a finite number of steps. For each nonzero remainder, the leading monomial of the remainder is not in $(\textsc{lm}(f_1), \ldots, \textsc{lm}(f_m))$, so extending the generating set of I also extends the monomial ideal generated by the leading monomials of the generating set of I. Because the ideal of leading monomials of the generating set is a subset of $\textsc{lm}(I)$ and $\textsc{lm}(I)$ has a finite generating set, the process will terminate. Additionally, this algorithm does give a Gröbner basis by Theorem 13.

Example 6. Let $I = (x^2y-1, xy^2-x) = (g_1, g_2)$, and let the monomial ordering be Deglex. Then $S_{1,2} = y(x^2y-1) - x(xy^2-x) = -y+x^2$. Since $\textsc{lm}(-y+x^2) = x^2$ is not divisible by either $\textsc{lm}(g_1)$ or $\textsc{lm}(g_2)$, $g_3 = x^2-y$. Continuing the algorithm, $S_{1,3} = (x^2y-1) - y(x^2-y) = -1+y^2$, so $\textsc{lm}(S_{1,3}) = y^2$. Hence $g_4 = y^2-1$. Further,

$$S_{2,3} = x(xy^2-x) - y^2(x^2-y) = y^4 - x^2$$

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

so the remainder of $S_{2,3}$ divided by G is $g_5 = -y+1$. Now,

$$S_{1,4} = y(x^2y-1) - x^2(y^2-1) = x^2 - y = g_3$$

$$S_{2,4} = (xy^2-x) - x(y^2-1) = 0$$

$$S_{3,4} = y^2(x^2-y) - x^2(y^2-1) = -y^3 + x^2 = -yg_4 + g_3$$

Hence each of these are divisible by $\{g_1, g_2, g_3, g_4\}$. The reader may verify that for every $i = 1, 2, 3, 4$, $S_{i,5}$ is divisible by $\{g_1, g_2, g_3, g_4, g_5\}$. Therefore, $\{g_1, g_2, g_3, g_4, g_5\}$ is a Gröbner basis for I.

4 Applications of Gröbner Bases

As aforementioned, Gröbner bases provide a solution to the Ideal Membership Problem. If f is a polynomial and I is an ideal, then we can determine if $f \in I$ by finding a Gröbner basis G for I and calculating the unique remainder of f divided by G. As in Corollary 9, this remainder is 0 if and only if $f \in I$.

Example 7. Let $I = (x+y+z, xy+xz+yz, xyz-1)$ and $f = 2x^2z^2+2xyz^2+2xz^3+z^3-1$. As proven in Example 5, a Gröbner basis for I is $G = \{x+y+z, y^2+yz+z^2, z^3-1\}$. Performing long division, we see that

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

Hence $f \in I$.

Example 8. Let $I = (xz-y^2, x^3-z^2)$ and $f = xy - 5z^2 + x$. With respect to Deglex, a Gröbner basis for I is $G = \{xz-y^2, x^3-z^2, x^2y^2-z^3, xy^4-z^4, y^6-z^5\}$. Now, $\text{LM}(G) = (xz, x^3, x^2y^2, xy^4, y^6)$. Clearly, $\text{LM}(f) = xy \notin \text{LM}(G)$, so therefore $f \notin I$.

Another application of Gröbner bases lies in algebraic geometry. Smith [3] shows that the projective closure of an affine variety is the vanishing of the homogenization of the ideal. However, the homogenization of the ideal is not always equal to the ideal generated by the homogenization of the generators. Yet if the generating set is a Gröbner basis, these are equal.

Proposition 14. Let I be an ideal in $K[x_1, \ldots, x_n]$, and let $\text{h}(I)$ be its homogenization in $K[x_1, \ldots, x_n, y]$. Suppose $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for I with respect to a graded monomial order, i.e., a monomial ordering that depends on multidegree of polynomials. Then $\text{h}(G) = \{\text{h}(g_1), \ldots, \text{h}(g_m)\}$ is the Gröbner basis for $\text{h}(I)$.

Proof. Because $\text{h}(G) \subset \text{h}(I)$, it suffices to show that $\text{LM}(\text{h}(I)) = (\text{LM}(\text{h}(g_1)), \ldots, \text{LM}(\text{h}(g_m)))$, or if $f \in \text{h}(I)$ is homogeneous, then $\text{LM}(f) \in (\text{LM}(\text{h}(g_1)), \ldots, \text{LM}(\text{h}(g_m)))$. Because f is homogeneous, $f = y^p\,\text{h}(g)$ for some $h \in I$ and some $p \in \mathbb{Z}^+$. Now, since the monomial ordering is graded, for any $h \in \text{h}(I)$, $\text{LM}(\text{h}(h)) = \text{LM}(h)$. Hence, $\text{LM}(f) = y^p\,\text{LM}(\text{h}(g)) = y^p\,\text{LM}(g)$. So

$$\text{LM}(f) \in (\text{LM}((g_1)), \ldots, \text{LM}((g_m))) = (\text{LM}(\text{h}(g_1)), \ldots, \text{LM}(\text{h}(g_m))). \qquad \square$$

4.1 Elimination Theory

A third application of Gröbner bases lies in elimination theory. Elimination theory gives a way to solve systems of polynomial equations by eliminating some of the variables from some equations, and then back-solving. For example, if our system of polynomials is

$$\begin{cases} x^2+y+z &= 1 \\ x+y^2+z &= 1 \\ x+y+z^2 &= 1 \end{cases}$$

then we can consider the ideal $I = (x^2+y+z-1, x+y^2+z-1, x+y^2+z-1)$. A Gröbner basis for I is:

$$\begin{aligned} g_1 &= x+y+z^2-1 \\ g_2 &= y^2-y-z^2+z \\ g_3 &= 2yz^2+z^4-z^2 \\ g_4 &= z^6-4z^4+4z^3-z^2 \\ &= z^2(z-1)^2(z^2+2z-1) \end{aligned}$$

Notice that g_4 is only in terms of z, so we can obtain the possible values of z from this equation. We see that z can be 0, 1, or $-1 \pm \sqrt{2}$. Since both g_3 and g_4 are in terms of only y and z, we can substitute for z and obtain the possible values for y. From here, we can solve for the possible values of x. This system of equations has 5 solutions:

$$(1,0,0), (0,1,0), (0,0,1), (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}), (-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}).$$

In solving this system of equations, the process can be divided into two parts. First, we eliminate variables, called the Elimination Step, and then we extend our solutions by back-solving, called the Extension Step.

First, we study the Elimination Step. Note that observing that g_4 is only in terms of z can also be stated as

$$g_4 \in I \cap \mathbb{C}[z].$$

Generalizing this leads to a definition.

Definition 15. Let $I = (f_1, \ldots, f_m) \subset K[x_1, \ldots, x_n]$. The kth *elimination ideal* I_k is the ideal of $K[x_{k+1}, \ldots, x_n]$ defined as

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

Solving the Elimination Step means finding polynomials in I that are not in terms of $x_1, \ldots, x_k$, which amounts to finding the kth elimination ideal. Gröbner bases makes this easy.

Theorem 16 (The Elimination Theorem)**.** Let I be an ideal and G a Gröbner basis with respect to Lex, where $x_1 > x_2 > \ldots > x_n$. Then, for every $0 \leq k \leq n$, the set

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

is a Gröbner basis for I_k.

Proof. Fix k. Since $G_k \subset I_k$, so it suffices to show that $(\text{LM}(G_k)) = \text{LM}(I_k)$. Clearly, $(\text{LM}(G_k)) \subset \text{LM}(I_k)$.

Let $f \in I_k$. We want to show that $\text{LM}(f)$ is divisible by $\text{LM}(g)$ for some $g \in G_k$. Now, $f \in I$, so $\text{LM}(f)$ divisible by $\text{LM}(g)$ for some $g \in G$. Since $f \in I_k$, this means that $\text{LM}(g)$ involves only $x_{k+1}, \ldots, x_n$. Since the ordering is Lex with $x_1 > x_2 > \ldots > x_n$, this means all terms of g only involve $x_{k+1}, \ldots, x_n$, so $g \in K[x_{k+1}, \ldots, x_n]$. Hence $g \in G_k$. □

Now we may turn our attention to solving the Extension Step. First, we define a partial solution.

Definition 17. Let I be a systems of equations in $K[x_1, \ldots, x_n]$. A solution $(a_{k+1}, \ldots, a_n) \in \mathbb{V}(I_k)$ is a partial solution of the original equations.

When we solve the equation in one variable, we find a partial solution. To extend a partial solution, we want to find a coordinate a_k such that $(a_k, a_{k+1}, \ldots, a_n) \in \mathbb{V}(I_{k-1})$. If $I_{k-1} = (g_1, \ldots, g_m)$, then we want solutions $x_k = a_k$ to the equations

$$g_1(x_k, a_{k+1}, \ldots, a_n) = \cdots = g_m(x_k, a_{k+1}, \ldots, a_n) = 0.$$

These are polynomials in one variable, so the possible a_k is just the roots of the greatest common divisor of the m polynomials. However, they might not have a common root, so not all partial solutions extend to complete solutions.

Example 9. Consider the following system of equations:

$$\begin{cases} xy &= & 1 \\ xz &= & 1 \end{cases}$$

Clearly, $I_1 = (y - z)$. So, the partial solutions are of the form (a, a), since these are precisely the elements in I_1. Hence the complete solutions are $(1/a, a, a)$, because $x = 1/y = 1/x$, if $a \neq 0$. If $a = 0$, the system is not consistent, so this does not admit a complete solution.

We extend a partial solution one coordinate at a time until we have completed it, so we only need to study extensions by one coordinate. For now, we shall restrict to the case where $k = 1$.

Theorem 18. Let $I = (f_1, \dots, f_m) \subset \mathbb{C}[x_1, \dots, x_n]$. For each $0 \leq i \leq m$, write

$$f_i = g_i(x_2, \dots, x_n)x_1^{N_i} + \text{terms of degree} < N_i.$$

Suppose $(a_2, \dots, a_n)$ is a partial solution. If $(a_2, \dots, a_n) \notin \mathbb{V}(g_1, \dots, g_m)$, then there exists $a_1 \in \mathbb{C}$ such that $(a_1, \dots, a_n) \in \mathbb{V}(I)$.

The proof of this uses resultants, so it will not be covered here.[1]

This theorem means that the Extension Step fails only when the leading coefficients of the polynomials vanish simultaneously. To return to Example 9, we see that the leading coefficients of x are y and z in each polynomial. Thus $\mathbb{V}(g_1, g_2) = \mathbb{V}(y, z)$, which contains only the point $(0, 0)$, the lone point which cannot be extended.

An easy corollary to this theorem occurs when the leading coefficients are constant.

Corollary 19. Assume that for some i, $f_i = cx_1^N$+terms of degree $< N$. Then if $(a_2, \dots, a_n) \in \mathbb{V}(I_1)$, then there exists a_1 such that $(a_1, a_2, \dots, a_n) \in \mathbb{V}(I)$.

Proof. Follows immediately from $c \neq 0 \Rightarrow \mathbb{V}(g_1, \dots, g_m) = \emptyset$. □

4.1.1 The Geometry of Elimination

Now, we will study a geometric interpretation of elimination theory. Elimination corresponds to projecting a variety onto a lower dimensional subspace.

Definition 20. Let $V = \mathbb{V}(f_1, \dots, f_m) \subset \mathbb{C}^n$. We define the projection map

$$\begin{aligned} \pi_k : \mathbb{C}^n &\rightarrow \mathbb{C}^{n-k} \\ (a_1, \dots, a_n) &\mapsto (a_{k+1}, \dots, a_n) \end{aligned}$$

Notice $\pi_k(V) \subset \mathbb{C}^{n-k}$.

We can relate this projection map to the kth elimination ideal.

Proposition 21. $\pi_k(V) \subset \mathbb{V}(I_k)$.

Proof. Let $f \in I_k$ and $(a_1, \dots, a_n) \in V$. Then f vanishes at $(a_1, \dots, a_n)$, but f involves only $x_{k+1}, \dots, x_n$, so

$$f(a_{k+1}, \dots, a_n) = f(\pi_k(a_1, \dots, a_n)) = 0.$$

Hence f vanishes at all points of $\pi_k(V)$. □

[1] For a version of the proof, the reader can consult [1], page 161.

Now, we have a precise definition for $\pi_k(V)$, using our new knowledge from Proposition 21.

$$\pi_k(V) = \{(a_{k+1}, \ldots, a_n) \in \mathbb{V}(I_k) : \exists a_1, \ldots, a_k \in \mathbb{C} \text{ with } (a_1, \ldots, a_k, a_{k+1}, \ldots, a_n) \in V\}.$$

So $\pi_k(V)$ is exactly the partial solutions which extend to complete solutions. For instance, if we return to Example 9, we see that $\pi_k(V) = \{(a, a) \in \mathbb{C}^2 : a \neq 0\}$.

Although $\pi_1(V)$ is not necessarily an affine variety, the Closure Theorem provides a strong statement about the relationship between $\pi_k(V)$ and $\mathbb{V}(I_k)$.

Theorem 22 (The Closure Theorem)**.** $\mathbb{V}(I_k)$ is the smallest affine variety containing $\pi_k(V) \subset \mathbb{C}^{n-k}$.

Proof. We have shown that $\mathbb{V}(\mathbb{I}(S))$ is the smallest affine variety containing S, so we must show that $\mathbb{V}(I_k) = \mathbb{V}(\mathbb{I}(\pi_k(V)))$. By the lemma, we know $\pi_k(V) \subset \mathbb{V}(I_k)$. Since $\mathbb{V}(\mathbb{I}(\pi_k(V)))$ is the smallest variety containing $\pi_k(V)$, this imples that $\mathbb{V}(\mathbb{I}(\pi_k(V))) \subset \mathbb{V}(I_k)$.

Suppose $f \in \mathbb{I}(\pi_k(V))$, so $f(a_{k+1}, \ldots, a_n) = 0$ for all $(a_{k+1}, \ldots, a_n) \in \pi_k(V)$. Then $f(a_1, \ldots, a_k, a_{k+1}, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in V$, since f only involves $x_{k+1}, \ldots, x_n$. By Nullstellensatz, $f^N \in I$ for some integer N. But since f does not depend on $x_1, \ldots, x_k$, neither does f^N, so $f \in I_k$. So, $f \in \sqrt{I_k}$, hence $\mathbb{I}(\pi_k(V)) \subset \sqrt{I_k}$. Thus, $\mathbb{V}(I_k) = \mathbb{V}(\sqrt{I_k}) \subset \mathbb{V}(\mathbb{I}(\pi_k(V)))$. □

This shows that the projection map projects a variety into a very specific lower-dimensional variety, which is in fact the Zariski closure of the projection.

References

[1] Cox, David, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms.* Springer: New York, 1997.

[2] Fröberg, Ralf. *An Introduction to Gröbner Bases.* John Wiley and Sons: Chichester, 1997.

[3] Smith, Karen. *An Invitation to Algebraic Geometry.* Springer: New York, 2000.