In Example 1 above it is easy to check that $\{x+y^4-y^3+y-1,\ y^4-y^3-1\}$ is again a minimal Gröbner basis for I (this is just $\{f_3+f_4,\ f_4\}$), so even with a fixed monomial ordering on $F[x_1,\ldots,x_n]$ a minimal Gröbner basis for an ideal I is not unique. We can obtain an important uniqueness property by strengthening the condition on divisibility by the leading terms of the basis.

Definition. Fix a monomial ordering on $R = F[x_1,\ldots,x_n]$. A Gröbner basis $\{g_1,\ldots,g_m\}$ for the nonzero ideal I in R is called a *reduced Gröbner basis* if

(a) each g_i has monic leading term, i.e., $LT(g_i)$ is monic, $i = 1,\ldots,m$, and

(b) no term in g_j is divisible by $LT(g_i)$ for $j \neq i$.

Note that a reduced Gröbner basis is, in particular, a minimal Gröbner basis. If $G = \{g_1,\ldots,g_m\}$ is a minimal Gröbner basis for I, then the leading term $LT(g_j)$ is not divisible by $LT(g_i)$ for any $i \neq j$. As a result, if we use polynomial division to divide g_j by the other polynomials in G we obtain a remainder g_j' in the ideal I with the same leading term as g_j (the remainder g_j' does not depend on the order of the polynomials used in the division by (2) of Theorem 23). By Proposition 24, replacing g_j by g_j' in G again gives a minimal Gröbner basis for I, and in this basis no term of g_j' is divisible by $LT(g_i)$ for any $i \neq j$. Replacing each element in G by its remainder after division by the other elements in G therefore results in a reduced Gröbner basis for I. The importance of reduced Gröbner bases is that they are unique (for a given monomial ordering), as the next result shows.

Theorem 27. Fix a monomial ordering on $R = F[x_1,\ldots,x_n]$. Then there is a unique reduced Gröbner basis for every nonzero ideal I in R.

Proof: By Exercise 15, two reduced bases have the same number of elements and the same leading terms since reduced bases are also minimal bases. If $G = \{g_1,\ldots,g_m\}$ and $G' = \{g_1',\ldots,g_m'\}$ are two reduced bases for the same nonzero ideal I, then after a possible rearrangement we may assume $LT(g_i) = LT(g_i') = h_i$ for $i = 1,\ldots,m$. For any fixed i, consider the polynomial $f_i = g_i - g_i'$. If f_i is nonzero, then since $f_i \in I$, its leading term must be divisible by some h_j. By definition of a reduced basis, h_j for $j \neq i$ does not divide any of the terms in either g_i or g_i', hence does not divide $LT(f_i)$. But h_i also does not divide $LT(f_i)$ since all the terms in f_i have strictly smaller multidegree. This forces $f_i = 0$, i.e., $g_i = g_i'$ for every i, so $G = G'$.

One application of the uniqueness of the reduced Gröbner basis is a computational method to determine when two ideals in a polynomial ring are equal.

Corollary 28. Let I and J be two ideals in $F[x_1,\ldots,x_n]$. Then $I = J$ if and only if I and J have the same reduced Gröbner basis with respect to any fixed monomial ordering on $F[x_1,\ldots,x_n]$.

Examples

(1) Consider the ideal $I = (h_1, h_2, h_3)$ with $h_1 = x^2+xy^5+y^4$, $h_2 = xy^6-xy^3+y^5-y^2$, and $h_3 = xy^5 - xy^2$ in $F[x,y]$. Using the lexicographic ordering $x > y$ we find

$S(h_1, h_2) \equiv S(h_1, h_3) \equiv 0 \bmod \{h_1, h_2, h_3\}$ and $S(h_2, h_3) \equiv y^5 - y^2 \bmod \{h_1, h_2, h_3\}$ Setting $h_4 = y^5 - y^2$ we find $S(h_i, h_j) \equiv 0 \bmod \{h_1, h_2, h_3, h_4\}$ for $1 \leq i < j \leq 4$, so

$$x^2 + xy^5 + y^4, \quad xy^6 - xy^3 + y^5 - y^2, \quad xy^5 - xy^2, \quad y^5 - y^2$$

is a Gröbner basis for I. The leading terms of this basis are x^2, xy^6, xy^5, y^5. Since y^5 divides both xy^6 and xy^5, we may remove the second and third generators to obtain a minimal Gröbner basis $\{x^2 + xy^5 + y^4, y^5 - y^2\}$ for I. The second term in the first generator is divisible by the leading term y^5 of the second generator, so this is not a reduced Gröbner basis. Replacing $x^2 + xy^5 + y^4$ by its remainder $x^2 + xy^2 + y^4$ after division by the other polynomials in the basis (which in this case is only the polynomial $y^5 - y^2$), we are left with the reduced Gröbner basis $\{x^2 + xy^2 + y^4, y^5 - y^2\}$ for I.

(2) Consider the ideal $J = (h_1, h_2, h_3)$ with $h_1 = xy^3 + y^3 + 1$, $h_2 = x^3y - x^3 + 1$, and $h_3 = x + y$ in $F[x, y]$. Using the lexicographic monomial ordering $x > y$ we find $S(h_1, h_2) \equiv 0 \bmod \{h_1, h_2, h_3\}$ and $S(h_1, h_3) \equiv y^4 - y^3 - 1 \bmod \{h_1, h_2, h_3\}$. Setting $h_4 = y^4 - y^3 - 1$ we find $S(h_i, h_j) \equiv 0 \bmod \{h_1, h_2, h_3, h_4\}$ for $1 \leq i < j \leq 4$, so

$$xy^3 + y^3 + 1, \quad x^3y - x^3 + 1, \quad x + y, \quad y^4 - y^3 - 1$$

is a Gröbner basis for J. The leading terms of this basis are xy^3, x^3y, x, and y^4, so $\{x + y, y^4 - y^3 - 1\}$ is a minimal Gröbner basis for J. In this case none of the terms in $y^4 - y^3 - 1$ are divisible by the leading term of $x + y$ and none of the terms in $x + y$ are divisible by the leading term in $y^4 - y^3 - 1$, so $\{x + y, y^4 - y^3 - 1\}$ is the reduced Gröbner basis for J. This is the basis for the ideal I in Example 1 following Proposition 26, so these two ideals are equal:

$$(x^3y - xy^2 + 1, x^2y^2 - y^3 - 1) = (xy^3 + y^3 + 1, x^3y - x^3 + 1, x + y)$$

(and both are equal to the ideal $(x + y, y^4 - y^3 - 1)$).

Gröbner Bases and Solving Algebraic Equations: Elimination

The theory of Gröbner bases is very useful in explicitly solving systems of algebraic equations, and is the basis by which computer algebra programs attempt to solve systems of equations. Suppose $S = \{f_1, \ldots, f_m\}$ is a collection of polynomials in n variables $x_1, \ldots, x_n$ and we are trying to find the solutions of the system of equations $f_1 = 0$, $f_2 = 0, \ldots, f_m = 0$ (i.e., the common set of zeros of the polynomials in S). If $(a_1, \ldots, a_n)$ is any solution to this system, then every element f of the ideal I generated by S also satisfies $f(a_1, \ldots, a_n) = 0$. Furthermore, it is an easy exercise to see that if $S' = \{g_1, \ldots, g_s\}$ is *any* set of generators for the ideal I then the set of solutions to the system $g_1 = 0, \ldots, g_s = 0$ is the *same* as the original solution set.

In the situation where $f_1, \ldots, f_m$ are *linear* polynomials, a solution to the system of equations can be obtained by successively eliminating the variables $x_1, x_2, \ldots$ by elementary means—using linear combinations of the original equations to eliminate the variable x_1, then using these equations to eliminate x_2, etc., producing a system of equations that can be easily solved (this is "Gauss-Jordan elimination" in linear algebra, cf. the exercises in Section 11.2).

The situation for polynomial equations that are nonlinear is naturally more complicated, but the basic principle is the same. If there is a nonzero polynomial in the

ideal I involving only one of the variables, say $p(x_n)$, then the last coordinate a_n is a solution of $p(x_n) = 0$. If now there is a polynomial in I involving only x_{n-1} and x_n, say $q(x_{n-1}, x_n)$, then the coordinate a_{n-1} would be a solution of $q(x_{n-1}, a_n) = 0$, etc. If we can successively find polynomials in I that eliminate the variables $x_1, x_2, \ldots$ then we will be able to determine all the solutions $(a_1, \ldots, a_n)$ to our original system of equations explicitly.

Finding equations that follow from the system of equations in S, i.e., finding elements of the ideal I that do not involve some of the variables, is referred to as *elimination theory*. The polynomials in I that do not involve the variables $x_1, \ldots, x_i$, i.e., $I \cap F[x_{i+1}, \ldots, x_n]$, is easily seen to be an ideal in $F[x_{i+1}, \ldots, x_n]$ and is given a name.

Definition. If I is an ideal in $F[x_1, \ldots, x_n]$ then $I_i = I \cap F[x_{i+1}, \ldots, x_n]$ is called the i^{th} *elimination ideal* of I with respect to the ordering $x_1 > \cdots > x_n$.

The success of using elimination to solve a system of equations depends on being able to determine the elimination ideals (and, ultimately, on whether these elimination ideals are nonzero).

The following fundamental proposition shows that if the lexicographic monomial ordering $x_1 > \cdots > x_n$ is used to compute a Gröbner basis for I then the elements in the resulting basis not involving the variables $x_1, \ldots, x_i$ not only determine the i^{th} elimination ideal, but in fact give a Gröbner basis for the i^{th} elimination ideal of I.

Proposition 29. (*Elimination*) Suppose $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for the nonzero ideal I in $F[x_1, \ldots, x_n]$ with respect to the lexicographic monomial ordering $x_1 > \cdots > x_n$. Then $G \cap F[x_{i+1}, \ldots, x_n]$ is a Gröbner basis of the i^{th} elimination ideal $I_i = I \cap F[x_{i+1}, \ldots, x_n]$ of I. In particular, $I \cap F[x_{i+1}, \ldots, x_n] = 0$ if and only if $G \cap F[x_{i+1}, \ldots, x_n] = \emptyset$.

Proof: Denote $G_i = G \cap F[x_{i+1}, \ldots, x_n]$. Then $G_i \subseteq I_i$, so by Proposition 24, to see that G_i is a Gröbner basis of I_i it suffices to see that $LT(G_i)$, the leading terms of the elements in G_i, generate $LT(I_i)$ as an ideal in $F[x_{i+1}, \ldots, x_n]$. Certainly $(LT(G_i)) \subseteq LT(I_i)$ as ideals in $F[x_{i+1}, \ldots, x_n]$. To show the reverse containment, let f be any element in I_i. Then $f \in I$ and since G is a Gröbner basis for I we have

$$LT(f) = a_1(x_1, \ldots, x_n)LT(g_1) + \cdots + a_m(x_1, \ldots, x_n)LT(g_m)$$

for some polynomials $a_1, \ldots, a_m \in F[x_1, \ldots, x_n]$. Writing each polynomial a_i as a sum of monomial terms we see that $LT(f)$ is a sum of monomial terms of the form $ax_1^{s_1} \ldots x_n^{s_n} LT(g_i)$. Since $LT(f)$ involves only the variables $x_{i+1}, \ldots, x_n$, the sum of all such terms containing any of the variables $x_1, \ldots, x_i$ must be 0, so $LT(f)$ is also the sum of those monomial terms only involving $x_{i+1}, \ldots, x_n$. It follows that $LT(f)$ can be written as a $F[x_{i+1}, \ldots, x_n]$-linear combination of some monomial terms $LT(g_t)$ where $LT(g_t)$ does not involve the variables $x_1, \ldots, x_i$. But by the choice of the ordering, if $LT(g_t)$ does not involve $x_1, \ldots, x_i$, then neither do any of the other terms in g_t, i.e., $g_t \in G_i$. Hence $LT(f)$ can be written as a $F[x_{i+1}, \ldots, x_n]$-linear combination of elements $LT(G_i)$, completing the proof.

Note also that Gröbner bases can be used to eliminate any variables simply by using an appropriate monomial ordering.