Math 615: Lecture of January 12, 2007

Example. Now consider

$$f = x_1x_2x_3,\ g_1 = x_1x_2 + x_3^2,\ g_2 = x_1x_3 + x_2^2$$

in $F = R = K[x_1, x_2, x_3]$ with hlex as the monomial order. On the one hand,

$$f = x_3g_1 + 0 \cdot g_2 - x_3^3$$

is a standard expression with remainder $-x_3^3$, while

$$f = 0 \cdot g_1 + x_2g_2 - x_2^3$$

is a standard expression with remainder $-x_2^3$. Therefore, even the remainder is not unique in general, although it is in important cases that we shall soon discuss.

Gröbner bases

Before proceeding further, we want to comment on the use of the word "basis." By a *basis* for a module we simply mean a set of generators for the module. There is no implication that these generators are linearly independent. If we are working with a free module, the term *free basis* will mean basis of linearly independent elements. In the phrase "free module with ordered basis" the basis is understood to be a free basis.

Over a field K, every module is free. We shall use the terms "vector space basis" and "K-vector space basis" for a set of linearly independent generators in the field case.

Throughout this section $R = K[x_1, \ldots, x_n]$ is a polynomial ring over a field K, $\mathcal{M}$ denotes the set of monomials in R, F is a finitely generated free R-module with ordered basis, and $>$ is a fixed monomial order on F.

The following very easy result is, nonetheless, extraordinarily useful.

Theorem. *Let $M \subseteq F$ be a submodule. If $N \subseteq M$ is a submodule such that $\mathrm{in}(N) = \mathrm{in}(M)$, then $N = M$.*

Proof. We shall give two proofs. First, suppose $N \neq M$. Consider the set $\mathcal{S}$ of monomials of F that occur in the initial term of an element of $M - N$. If this set is non-empty, it has a least element with respect to $>$, since monomial orders are well-orderings. Suppose that $f \in M - N$ has initial term $c\nu$ where ν is the least element of $\mathcal{S}$. Then $\nu \in \mathrm{in}(M) = \mathrm{in}(N)$ occurs as the initial term of some element $g \in N$, and then $f - cg$ contains only terms strictly smaller than ν. But this element is still in $M - N$, and its initial term must be smaller than ν, contradicting the minimality of ν. $\square$

Here is an alternative argument. We know that $\text{in}(M) = \text{in}(N)$ is finitely generated, since it is a monomial module. We may therefore choose finitely many elements $g_1, \ldots, g_r \in N$ whose initial terms generated $\text{in}(M)$. Let $f \in M$ be given. By the division algorithm, there is a regular expression

$$f = \sum_{j=1}^{r} q_j g_j + h$$

for f in terms of the g_i. Then $h \in M$, but no term of h is divisible by any $\text{in}(g_j)$. This implies that $h = 0$, for otherwise its initial term $\text{in}(h) \in \text{in}(M)$ and so must be divisible by some $\text{in}(g_j)$. But this shows that $f \in N$. $\square$

We are immediately led to make the following definition. Let $M \subseteq F$ be any submodule. Then $g_1, \ldots, g_r$ is called a *Gröbner basis* for M if the elements $\text{in}(g_1), \ldots, \text{in}(g_r)$ are a basis for $\text{in}(M)$. We know that since $\text{in}(M)$ is monomial, it is finitely generated, and so a Gröbner basis for M always exists.

Theorem. *Every submodule M of F has a Gröbner basis.* $\square$

Theorem. *A Gröbner basis for $M \subseteq F$ is a basis for M.*

Proof. This is immediate from the first Theorem on p. 1. $\square$

Corollary (Hilbert basis theorem). *Every submodule of F is finitely generated. In particular, every ideal of $R = K[x_1, \ldots, x_n]$ is finitely generated.*

Proof. The submodule or ideal has a (finite) Gröbner basis, which is then a basis. $\square$

We also have:

Theorem. *Let $M \subseteq F$ be a submodule. The monomials of F* not *in* $\text{in}(M)$ *give a K-vector space basis for F/M.*

Proof. We first show that the set of monomials $\mathcal{Q}$ in F and not in $\text{in}(M)$ are linearly independent over K. If we have a linear relation on these monomials, we find that a nonzero linear combination of monomials in $\mathcal{Q}$ is an element f of M. But then the initial term of $f \in M$ involves a monomial not in $\text{in}(M)$, a contradiction.

Now let $f \in F$ be given, and let $g_1, \ldots, g_r$ be a Gröbner basis for M. By the division algorithm, we can write $f = \sum_{j=1}^{r} q_j g_j + h$, where h is in the K-span of $\mathcal{Q}$. But then $f \equiv h \bmod M$. $\square$

Corollary. *Let $M \subseteq F$ and let $g_1, \ldots, g_r$ be a Gröbner basis for M. Then for all $f \in F$, the remainder h in any standard expression*

$$f = \sum_{j=1}^{r} q_j g_j + h$$

is unique, i.e., h is the same no matter what standard expression is chosen.

In particular, $f \in F$ is an element of M if and only if the remainder in any standard expression for f in terms of the Gröbner basis $g_1, \ldots, g_r$ is 0.

Proof. The remainder h is a K-linear combination of monomials in $\mathcal{Q}$, the set of monomials of F not in $\mathrm{in}(M)$. Any two remainders represent the same element of F/M, and so the result follows at once from the preceding Theorem.

The final statement is then obvious. $\square$

Notice that if we can find a Gröbner basis $g_1, \ldots, g_r$ for $M \subseteq F$ (or for $I \subseteq R$), the result above gives an effective test for whether an element $f \in F$ (respectively, R) is in M (respectively, I): one simply uses the division algorithm to find a remainder for f in terms of $g_1, \ldots, g_r$, and $f \in M$ (respectively, I) if and only if the remainder is 0.

However, at this point we do not have an effective method for finding a Gröbner basis for M given a set of generators of M. We shall develop such a method, called the *Buchberger algorithm*, at which point we have a solution for the problem of giving an effective test for membership in M or I when we know specific generators for M or I.

Before discussing the Buchberger algorithm, we want to discuss restrictions on a Gröbner basis for M (or I) that make it unique.

A Gröbner basis $g_1, \ldots, g_r$ for $M \subseteq F$ is called *minimal* if the monomials occurring in $\mathrm{in}(g_1), \ldots, \mathrm{in}(g_r)$ are the minimal monomials in $\mathrm{in}(M)$. Evidently, every Gröbner basis for M has a subset that is a minimal Gröbner basis. Notice that every minimal Gröbner basis for M has the same cardinality as the set of minimal monomials $\mathrm{in}(M)$. We shall say that an ordered Gröbner basis $g_1, \ldots, g_r$ for $M \subseteq F$ is *reduced* if it satisfies the following four conditions:

(1) $g_1, \ldots, g_r$ is minimal.

(2) $\mathrm{in}(g_1) > \mathrm{in}(g_2) > \cdots > \mathrm{in}(g_r)$.

(3) Every $\mathrm{in}(g_i)$ is a monomial, i.e., the coefficient in every initial term is 1.

(4) For all $i \neq j$, $\mathrm{in}(g_i)$ does not divide any term in g_j.

There is variation in the literature in the use of the term "reduced Gröbner basis," but conditions (1) and (4) are always assumed. We have chosen the usage that makes a reduced Gröbner basis for M unique, as we shall see below.

As already noted, any Gröbner basis has a subset that is minimal, and the elements can then be ordered uniquely so that the sequence of initial terms is strictly decreasing.

Obviously, one can multiply each term by the reciprocal of the coefficient of the initial term, and therefore conditions (1), (2), and (3) are readily achieved. Note that it is obvous that the sequence of initial terms is then the same as the sequence of minimal monomial generators of $\text{in}(M)$, arranged in strictly decreasing order. We can guarantee condition (4) as follows. Replace g_1 by its remainder in a standard expression with respect to division by $g_2, \ldots, g_r$. Then replace g_2 by its remainder in a standard exrpession with respect to division by $g_3, \ldots, g_r$. Continue in this way for $r-1$ steps. At the ith step, replace g_i by its remainder in a standard expression with respect to division by $g_{i+1}, \ldots, g_r$.

It is easy to see that the result satisfies all of the conditions (1) — (4). The first three conditions are not disturbed. Given $i < j$, $\text{in}(g_i)$ is bigger than any term in g_j, and so cannot divide g_j, while no term in g_i is divisible by $\text{in}(g_j)$, because g_i is the remainder in a standard expression for division by elements one of which has the same initial term as g_j. Note that while the g_k change, their initial terms do not change.

Since we can use the deterministic division algorithm at each step, we see that we can pass algorithmically from a Gröbner basis to a reduced Gröbner basis. We have now proved the first statement in the Theorem below.

Theorem. *Let $M \subseteq F$ (or $I \subseteq R$) be given. Then M (respectively, I) has a reduced Gröbner basis, and it is unique.*

Proof. It remains only to prove uniqueness and, as usual, it suffices to consider the case of modules. We need only show that if $g_1, \ldots, g_r$ and $g'_1, \ldots, g'_r$ are two reduced Gröbner bases for M, then $g_i = g'_i$ for all i. We know *a priori* that $\text{in}(g_i) = \text{in}(g'_i)$ for all I. We use reverse induction on i. Apply the division algorithm to find a standard expression for g'_r in terms of $g_1, \ldots, g_r$. We know that the remainder will be 0. Moreover, at every stage, the initial terms of $g_1, \ldots, g_{r-1}$ are too large to be used. At the very first step in the algorithm, we subtract g_r from g'_r to produce an element of M all of whose terms involve only monomials $< \text{in}(g_r) = \text{in}(g'_r)$. Since this is the least monomial in $\text{in}(M)$, it follows that $g_r - g'_r = 0$. This gives the base step of the induction.

Now assume that $i < r$ and that $g_j = g'_j$ for $j > i$. Perform the division algorithm for g'_i with respect to $g_1, \ldots, g_r$. The terms $g_1, \ldots, g_{i-1}$ are all too large ever to be used. At the first step, one gets $g_i - g'_i$: the initial terms cancel, all remaining terms are strictly smaller than $\text{in}(g_i) = \text{in}(g'_i)$, and none of them is divisible by $\text{in}(g_j)$ for $j > i$, since this is true for all terms but the greatest in both g_i and g'_i. Since the remainder must be 0, we must have that $g_i - g'_i = 0$, and so $g_i = g'_i$, as required. $\square$

Revisited example. Consider again the example on p. 1, in which $g_1 = x_1x_2 + x_3^2$ and $g_2 = x_1x_3 + x_2^2$. The elements g_1 and g_2 are certainly minimal generators for an ideal I of $K[x_1, x_2, x_3]$. They are not, however, a Gröbner basis using hlex. The initial terms of these two elements are x_1x_2 and x_1x_3. Note that $x_3g_1 - x_2g_2 = x_3^3 - x_2^3$ has initial term $-x_2^3$, which shows that $\text{in}(g_1)$ and $\text{in}(g_2)$ are not the only minimal elements of $\text{in}(I)$. In fact, we know this *a priori*, since remainders of division with respect to g_1, g_2 are not unique.