ALGEBRA III
SEPTEMBER 21, 2004

GABRIEL C. DRUMMOND-COLE

Next time we'll be meeting in the computer lab. You all have played with unix, or linux, yes? Well, you may want to look at some documentation for Macaulay beforehand.

So do you remember the Gr obner basis? We were working in the ring $S = k[x_1, \dots, x_n]$, and $\succ$, a term order. For $f \in S$ you can pick out the leading term $in_\succ(f) = lt_\succ(f)$. From I you can get $in_\succ(I) = \langle in_\succ(f) | f \in I \rangle$, which is finitely generated. Now, a system of generators $f_1, \dots, f_m$ of I whose leading terms generate the appropriate monomial ideal is called a Gr obner basis.

Lemma 1. *If $J \subset I$ as ideals in S, then $in_\succ(J) = in_\succ(I)$ implies $J = I$.*

This is extremely powerful. You'll use it over and over again. Assume you have $f \in I$ with $f \notin J$. Take it so that the $in_\succ(f)$ is the smallest of $\{in_\succ(g) : g \in I \backslash J\}$. Then $in_\succ(f) \in in_\succ(I) = in_\succ(J)$. Then there is $g \in J$ with $in_\succ(f) = in_\succ(g)$. Then $f - g$ is in I but not in J. But the initial term is strictly smaller than that of f, a contradiction.

Most of the proofs about Gr obner bases are of this type, mainly bookkeeping.

Corollary 1. *A gr obner basis generates the ideal.*

Proof: $J = (f_1, \dots, f_m) \subset I$ has $in_\succ(J) = in_\succ(I)$.

Corollary 2. *If $I \subset S$ is an ideal, then I is finitely generated.*

Proof: Pick a term order, find a finite set of generators of $in_\succ(I)$ $\{in_\succ(f_1), \dots, in_\succ(f_m)\}$. Then $\{f_1, \dots, f_m\}$ are a Gr obner basis for I, and so generate it.

Lemma 2. *Macaulay's Lemma*
Let $I \subset S$, and $\succ$ a monomial order. The set of monomials not in $in_\succ(I)$ form a basis over k for S/I.

This is as a vector space, and of course depends a lot on the order. This was the promise. Find a monomial ideal so that the monomials not in it form a basis for the quotient, and we did it.

So let's prove this, and let's construct a Gr obner basis. Can we make this basis unique? As we did it there is no uniqueness.

Now, how do we prove this lemma? First we have to show independence. Let the "basis" set be B. If we have $\sum u_i m_i = 0$ with $u_i \in k, m_i \in B$, this means the sum p is in I.

We can assume that all u_i are nonzero. Then $in_\succ(p) \in \ in_\succ(I)$. This is just $n_i m_i$ for some i. But then $m_i \in B$, a contradiction since B consists of the monomials not in $in_\succ(I)$.

Now to show that B generates S/I, we have to show that anything mod I can be written as a combination of the b's. So I want to show that B and I generate the whole polynomial ring. So by contradiction we assume that B and I do not generate S as a vector space. So suppose we have f not in the span of B and I, and choose such an f with the smallest initial term out of the set of such. Now $in_{\succ}(f)$ is either in B or in $in_{\succ}(I)$. If this sits in B then I can subtract it yielding a new vector $f - in_{\succ}(f)$ not in the span of B and I with a smaller initial term, a contradiction.

If on the other hand, if $in_{\succ}(f) \in in_{\succ}(I)$, then there is a $g \in I$ with $in_{\succ}(g) = in_{\succ}(f)$. Then again there is a contradiction with the element $f - g$, which is not in the span of B and I but has a smaller initial.

So most of the proofs here will be of this type. They're not so hard once you have the idea.

Okay, there are two things I want to talk now. How do we generalize division? Second, how do you compute a Gr obner basis. I won't prove that. I'll tell you where you can see the proof, for instance in Eisenbud's book, but it's generally like this and will take half an hour.

So when you have one variable, division gives you a remainder which is smaller than what you had.

Proposition 1. *Say you have $g_1, \ldots, g_t, f \in S$. This will be division of f by the g_i. In one variable it will be division by the gcd. Then there exists an $f = \sum_{i=1}^{t} h_i g_i + f'$ such that none of the monomials in f' is in $\langle in_{\succ}(g_1), \ldots, in_{\succ}(g_n)\rangle$, and such that the initial of f is at least equal to $in_{\succ}(h_i g_i)$ for all i.*

This is not unique. The choices will have to do with ordering. So what's the proof? You look to the initial term $in_{\succ}(f)$. If it's not divisible by $in_{\succ}(g_i)$ then you're done. Then f is its own remainder. Otherwise, $in_{\succ}(f) = in_{\succ}(g_i)m_i$. This is not unique. Then you can subtract $\lambda m_i g_i$ and repeat the process with a smaller polynomial. Keep going. This process terminates finitely. Once it terminates, you have the remainder.

There is a way to make the remainder unique. Let me state this. We'll put slightly stronger conditions here; the proof is as before. So the alternative is to write $f = \sum h_i g_i + f'$ with the property that the monomials of h_j lie in the set of monomials n of S such that $n\, in_{\succ}(g_j) \notin \langle in_{\succ}(g_1), \ldots, in_{\succ}(g_{j-1})\rangle$ and such that the monomials of f' do not lie in $\langle in_{\succ}(g_1), \ldots, in_{\succ}(g_n)\rangle$. This is slightly stronger. It's called determinant division. You prove it by picking, every time, the smallest i such that you can write $in_{\succ}(f) = in_{\succ}(g_i)m_i$.

Exercise 1. *Show that with determinant division the remainder is unique.*

Here's a special case. So what happens if I divide an f by a Gr obner basis $g_1, \ldots, g_t$ for $\langle g_1, \ldots, g_t\rangle$? Then the remainder of f by division is unique. It's called the normal form of f, $Normal_{g_1,\ldots,g_n}(f)$.

For the proof, look to $\bar{f}$ in S/I. Then the normal form is exactly the expression of $\bar{f}$ in the basis B of monomials not in $in_{\succ}(I)$.

So now we can answer one of our questions, how I can check ideal membership.

Corollary 3. *Say $I \subset S$, $f \in S$. Does $f \in I$? Choose a term order $\succ$, compute a Gr obner basis $g_1, \ldots, g_t$ with respect to $\succ$ for I, and then $Normal_{(g_1,\ldots,g_t)} = 0$ if and only if $f \in I$.*

If the normal form is zero, then f is clearly in I.

Note that this doesn't work with just a set of generators. The remainder can be nonzero even though f is in I.

Two more things. How can you make Gr obner bases unique, and how many are there?

Lemma 3. *If you have $I \subset S$, then I has only finitely many initial ideals.*

There are infinitely many orders, such as the weighted orders $\underline{x}^{\underline{\alpha}} \succ \underline{x}^{\underline{\beta}}$ if $\sum \alpha_i \gamma_i > \sum \beta_i \gamma_i$.

This is related to Newton polytopes. These have a lot to say. It's kind of the convex hull of the exponents in $\mathbb{R}^n$.

As a consequence, every ideal has a universal Gr obner basis, a Gr obner basis with respect to any order. Put all of the finitely many finite Gr obner bases together; then you get a Gr obner basis under any order.

Example 1. $M = \begin{pmatrix} x_{11} & \dots & x_{1n} \\ x_{21} & \dots & x_{2n} \end{pmatrix}$. *Let $S = k[x_{ij}, i \in 1, 2$ and $j \in 1, \dots, n$. Then the universal Gr obner basis is the collection of 2×2 matrices of M.*

Definition 1. *$(g_1, \dots, g_t)$ is a minimal GB for $I = \langle g_1, \dots, g_t \rangle$ if $in_\succ(g_i)$ is not divisible by $in_\succ(g_j)$ for $j \neq i$. Then this is a collection of minimal generators for $in_\succ(I)$.*

Definition 2. *$(g_1, \dots, g_t)$ is a reduced GB if $in_\succ(g_j)$ does not divide any monomial of g_i for $i \neq j$.*

Up to monotonicity this is unique. I'm going to sketch the proof and leave the details as an exercise.

Lemma 4. *Reduced Gr obner bases exist and are unique.*

Corollary 4. *$I = J$ if and only if they have the same reduced Gr obner basis.*

To prove the lemma, let's make a tiny definition.

Definition 3. *$g \in G$ is called reduced with respect to G if no monomial in g is divisible by $in_\succ((G\{g\}))$.*

There are two observations. If g is reduced for G and we modify G to G' so that they have the same initial terms, then g is still reduced with respect to G.

So start with a minimal G, with $g \in G$. Compute g' which is the remainder with respect to division by $G \backslash \{g\}$. I claim that $G \rightsquigarrow G' = G \backslash \{g\} \cup \{g'\}$ yields a Gr obner basis, and that g' is reduced with respect to it.

Now, why is this true? Since G is minimal, the initial term is not divisible and stays as the initial term of the remainder. So the monomials that come from G' are the same as the monomials from G.

Why is it unique? That's what's left to prove. This I'll leave as an exercise.

Exercise 2. *If G_1 and G_2 are minimal GB then $in_\succ(G_1) = in_\succ(G_2)$.*

If G_1 and G_2 are reduced then their initials are the same. For $g \in G_1$ there exists $h \in G_2$ with $in_{\succ}(g) = in_{\succ}(h)$. Then $g - h$ is in I; what is its normal form with respect to G_1? It's zero because this tests for ideal membership. Then the initial term of $g - h$ is strictly smaller than the initial term of g. Then it's not divisible by anything in G_1. Who can it be divisible by? The monomials from g in the sum can't be divisible by any of the other elements since G_1 is reduced. So the difference is 0.

You've seen these in linear algebra, not knowing it. Let I be linear forms $\langle \subset k[x_1, \ldots, x_n] \rangle$. Say we have a system of equations $\left\{ \begin{array}{cccc} x_1 + & \cdots & -7x_{11} & = 0 \\ \cdots & \cdots & \cdots & \cdots \end{array} \right\}$. There's a row-echelon form, and the reduced row-echelon form. The first is a minimal GB and the second is a reduced GB, for the ideal generated by these linear forms. This is in *lex*.

Exercise 3. *Show this*

Now I'd like to show how you compute a Gr obner basis. There are other things, like how do you compute the intersection of two ideals? How do you compute the colon? Lagrange multipliers are good candidates for this sort of thing; this is why you can't give hard problems on them to calculus students.

So suppose $g_1 = x^2, g_2 = xy + y^2, x > y$ and we're in *lex*. Then the initials are x^2, xy. Is this a Gr obner basis? Look at the lcm or the gcd. So $gcd(in(g_1), in(g_2)) = x$, and the lcd is x^2y. So I look at $(in(g_2)/x)g_1 - (in(g_1)/x)g_2$; this kills the initials. This is $yg_1 - xg_2 = -xy^2$. Now we have a problem. This is an element of the ideal, and its initial is divisible by the initial of g_2. So I kill it by division, and I get $-xy^2 = -yg_2 + y^3$. Now y^3 is not in the monomial ideal generated by $in(g_1), in(g_2)$ so that the pair is not a Gr obner basis. So add in $g_3 = y^3$.

The algorithm is the following. The lcm/gcd trick is called the S-pair $S(g_1, g_2)$.
This is $\frac{in(g_2)}{gcd(in(g_1),in(g_2))} g_1 - \frac{in(g_1)}{gcd(in(g_1),in(g_2))} g_2$. This is called the Buchberger criterion. If $S(g_i, g_j)$ reduce to zero mod $g_1, \ldots, g_m$, for all $i \neq j$, then $(g_1, \ldots, g_m)$ is a Gr obner basis.

It's easy to show that the process terminates, if you start with a generating collection and adding in new elements. Unfortunately it's an exponential process. You don't need to check all the S-pairs. Essentially if the initial terms are relatively prime, then it reduces for free to zero. If you want to see the proof of this, it's a little bit time consuming, it's in Eisenbud's book.

Returning to our example, $S(g_1, g_2)$ reduces now. We still have to check $S(g_1, g_3)$ and $S(g_2, g_3)$.

Now what is the point to each of the orders? Which Gr obner bases help me solve which problems? So more next time. Next time we meet in S235.