Informal Seminar on Stanley-Reisner Theory, UMN, Fall 2002
14 November 2002

Introduction to Gröbner bases, II
Speaker: Jeremy Martin

1. Review

Last time we were looking at a polynomial ring $R = \mathbf{k}[X_1, \ldots, X_n]$ and a proper ideal $I \subset R$. We chose a *term order* $<$ for R, which is a total order on monomials satisfying the properties

- $\mu \mid \mu' \implies \mu \leq \mu'$ and
- $\mu \leq \mu' \implies \nu\mu \leq \nu\mu'$.

With respect to this term order, we can define the *initial term* $\mathrm{in}_<(f)$ of any nonzero polynomial f, and the *initial ideal* of I as

$$\mathrm{in}_<(I) = (\mathrm{in}_<(f) \ : \ f \in I)\,.$$

I said last time that a finite set of generators $(f_1, \ldots, f_r)$ is a *Gröbner basis* for I (with respect to a given term order $<$) if

$$(\mathrm{in}(f_1)_<, \ldots, \mathrm{in}_<(f_r)) = \mathrm{in}_<(I). \tag{1}$$

I'll often suppress the subscript $<$ if we're only talking about one term order.

Theorem 1. *Let $<$ be a term order on R. Then I has a Gröbner basis with respect to $<$.*

Proof. Let $B_0 = \{f_1, \ldots, f_r\}$ be a set of generators for I, and $I_0 = (\mathrm{in}(f_1), \ldots, \mathrm{in}(f_r))$. If $I_0 = \mathrm{in}(I)$, great. If not, then there exists some $g_1 \in I$ such that $\mathrm{in}(g_1) \notin I_0$. Let $B_1 = B_0 \cup \{g_1\}$ and $I_1 = I_0 + (\mathrm{in}(g_1))$. Note that $I_0 \subsetneq I_1$. If $I_1 = \mathrm{in}(I)$, great. If not, then there exists some $g_2 \in I$ such that $\mathrm{in}(g_2) \notin I_1$. So let $B_2 = B_1 \cup \{g_2\}$ and $I_2 = I_1 + (g_2)$. And so on. But R is Noetherian, so this has to stop eventually. That means that there is some k for which $I_k = \mathrm{in}(I)$.

□

By the way, this use of the Noetherian property is typical in proving a lot of the results that make the Gröbner basis machine run smoothly. Another fact along these lines, which I will need later, is that term orders are *Artinian*. That is, every set of monomials has a smallest element. This is completely clear for term orders which refine the partial order by total degree—indeed, those term orders are well-orderings. But in general, it's not too hard to derive the Artinian property from the definition of a term order (see [2, Lemma 15.2]).

Two brief asides:

1. The Gröbner basis is by no means unique; indeed, by the proof, any finite subset of I which contains a Gröbner basis is itself a Gröbner basis. It is not hard to see, however, that all minimal Gröbner bases have the same cardinality (with respect to a fixed term order), namely the minimal number of generators for the initial ideal. In addition, there's a particularly nice kind of minimal Gröbner basis called a *reduced Gröbner basis*, which is unique (see Exercise 15.14 in [2]).

2. You may wonder what happens if we vary the term order. Using the Noetherian property, it can be shown [3, Thm 1.2] that I has only finitely many initial ideals. That is, the term orders on R fall into finitely many equivalence classes, such that $\mathrm{in}_<(I) = \mathrm{in}_{<'}(I)$ if $<$ and $<'$ are in the same equivalence class.

It follows that I has a *universal Gröbner basis*, i.e., a finite subset which is a Gröbner basis for *all* term orders, obtained by taking the union

This is all very well, but how do you produce a Gröbner basis to begin with? How do you decide whether or not one of the B_i's is a Gröbner basis? And if it isn't, how do you get your hands on an element whose initial term needs to be thrown in? Before I answer these (excellent) questions, let's look at one of the easiest problems to solve once you have a Gröbner basis. (This may seem unnecessarily tantalizing, but actually the algorithm for producing a Gröbner basis in the first place depends on this construction.) The problem in question is ideal membership, and I claim that the following algorithm solves it:

Input:	$\{f_1, \ldots, f_r\}$	:	Gröbner basis for an ideal $I \subset R$
	g	:	polynomial in R

Output: An answer to the question "Is $g \in I$?"

Step 1: If $\text{in}(g) \notin \text{in}(I) = (\text{in}(f_1), \ldots, \text{in}(f_r))$ (which is easy to check), then answer **NO** and terminate.
Step 2: Otherwise, find f_i such that $\text{in}(g)$ is divisible by f_i.
Step 3: Set $h := \frac{\text{in}(g)}{\text{in}(f_1)} f_1$ and $g := g' - h$.
Step 4: If $g' = 0$, then answer **YES** and terminate. Otherwise, set $g := g'$ and go to Step 1.

Why does this work? First of all, $g' \equiv g \pmod{I}$, so if the algorithm returns YES, then we have actually produced an explicit R-linear combination of the f_i's which equals g. On the other hand, if $\text{in}(g') \notin \text{in}(I)$, then by definition $g' \notin I$, so $g \notin I$ as well. Okay, but why is the algorithm guaranteed to terminate? The key point is that after each iteration of Step 3, we have

$$\text{in}(g_1) < \text{in}(g)$$

since g and h have the same leading term, so the leading term of g' is some other monomial appearing in one of g or h, which means that it is less than $\text{in}(g)$. Since term orders are Artinian, the algorithm must terminate eventually.

This procedure is referred to as *reduction*, and is quite similar to (in fact, it generalizes) the division algorithm. If feeding g into the algorithm produces g' at some stage, we will say that "g can be reduced to g' modulo the f_i," and write

$$g \xrightarrow[\{f_i\}]{} g'.$$

(or just $g \to g'$).

This gives an idea of how we might construct an algorithm to enlarge a generating set $\{f_1, \ldots, f_r\}$ for I into a Gröbner basis. Start by pretending that it really is. Think up a polynomial $g \in I$ and reduce it modulo $\{f_i\}$. If $g \to g'$ and $\text{in}(g') \notin (\text{in}(f_1), \ldots, \text{in}(f_r))$, why then we just throw g into the putative Gröbner basis, enlarging the initial ideal.

There are a couple of problems. First, how do you go about thinking up appropriate g's to feed into the machine? After all, if $g \to 0$, it just says that $\text{in}(g) \in (\text{in}(f_1), \ldots, \text{in}(f_r))$; that doesn't mean that a different g wouldn't reduce to something outside $\text{in}(I)$. Second of all, how do you know when to stop? The solution is provided by *Buchberger's algorithm*.

For $f, g \in R$, define their *S-polynomial* (S stands for "syzygy") to be

$$S(f,g) \;=\; \frac{\text{in}(f_2)}{\text{lcm}(\text{in}(f_1), \text{in}(f_2))}\, f_1 \;-\; \frac{\text{in}(f_1)}{\text{lcm}(\text{in}(f_1), \text{in}(f_2))}\, f_2.$$

As before, we have rigged $S(f,g)$ to ensure that the leading terms cancel. So this might be a way of producing new elements of I whose initial term is not divisible by either $\text{in}(f_1)$ or $\text{in}(f_2)$. Of course, we have to take $S(f,g)$ and reduce it modulo our partial Gröbner basis to find out whether we've really gotten something new. Buchberger's criterion says, in effect, that we don't have to do anything fancier than compute and reduce a bunch of S-polynomials. That is:

Theorem 2 (Buchberger)**.** *Let $I = (f_1, \ldots, f_r) \subset R$. If, for every $1 \le i < j \le r$,*

$$S(f_i, f_j) \xrightarrow[\{f_i\}]{} 0,$$

then the f_i's form a Gröbner basis for I.

I don't intend to prove this (if you're interested, it is Theorem 15.8 in [2]), but I do want to work through an example. First, though, I want to tell you one way in which it's related to Stanley-Reisner theory, which is after all supposed to be the topic of this seminar.

Theorem 3. *Let $I \subset R$. For any term order $<$ on R, the set of monomials not in $\mathrm{in}_<(I)$ form a basis for R/I as a $\mathbf{k}$-vector space.*

Such monomials are called *standard monomials* for I (with respect to $<$).

Proof. It is clear that different linear combinations of standard monomials represent different elements of R/I. On the other hand, any member of R is congruent to some such linear combination, by the reduction algorithm. It □

Corollary 1. *If $I \subset R$ is a homogeneous ideal, so that R/I is a graded ring, then*

$$\mathrm{Hilb}(R/I; t) \;=\; \mathrm{Hilb}(R/\,\mathrm{in}_<(I); t)$$

for all term orders $<$.

This is in itself a nice fact, because a homogeneous ideal $I \subset \mathbf{k}[X_1 \ldots, X_n]$ corresponds to a subvariety of projective $(n-1)$-space (at least if I is radical, but let's not go there), and the Hilbert series encodes a bunch of nice geometric invariants, such as the dimension, degree, and arithmetic genus. As we saw last time, the Hilbert series of a monomial ideal can be computed explicitly.

If you're really lucky, the ideal I that you want to study might have a squarefree initial ideal. In this case, you can in principle calculate the Hilbert series combinatorially by looking at the Stanley-Reisner complex. For an example of this, see the speaker's Ph.D. thesis!

Example 1. Let $R = \mathbf{k}[x, y, z]$, and take $<$ to be reverse-lex order with $x > y > z$. Let I be the homogeneous ideal generated by

$$\begin{aligned} f_1 &= \underline{xy} - z^2, \\ f_2 &= \underline{y^2} - xz. \end{aligned}$$

(When working with explicit polynomials, it is convenient to underline the leading term.) The S-pair of the two generators is

$$f_3 := S(f_1, f_2) \;=\; yf_1 - xf_2 \;=\; xy^2 - yz^2 - xy^2 + x^2z \;=\; -yz^2 + \underline{x^2z}.$$

Since

$$\mathrm{in}(f_3) = x^2z \notin (\mathrm{in}(f_1), \mathrm{in}(f_2)) = (xy, y^2),$$

it follows by Buchberger that $\{f_1, f_2\}$ is not a Gröbner basis. However, as we will show, $\{f_1, f_2, f_3\}$ is a Gröbner basis. By Buchberger's theorem, it is enough to check that $S(f_1, f_3)$ and $S(f_2, f_3)$ reduce to zero modulo $\{f_1, f_2, f_3\}$. Indeed,

$$\begin{aligned} S(f_1, f_3) &= xzf_1 - yf_3 \;=\; -xz^3 + \underline{y^2z^2} \\ &\to (-xz^3 + y^2z^2) - y^2 f_2 \;=\; 0 \end{aligned}$$

and

$$\begin{aligned} S(f_2,f_3) &= x^2zf_2 - y^2f_3 \;=\; \underline{-x^3z^2} + y^3z^2 \\ &\to (-x^3z^2+y^3z^2) + xzf_3 \;=\; \underline{y^3z^2} - xyz^3 \\ &\to (y^3z^2 - xyz^3) - yz^2f_2 \;=\; 0. \end{aligned}$$

So $\{f_1,f_2,f_3\}$ really is a Gröbner basis, and

$$\mathrm{in}_<(I) \;=\; \left(xy, y^2, x^2z\right).$$

Let's compute its Hilbert series. Let $I' = (xy, y^2)$, so that $\mathrm{in}_<(I) = I' + (x^2z)$. As described last time, there is an exact sequence of maps

$$R[-3] \xrightarrow{x^2z} R/I' \to R/\,\mathrm{in}_<(I) \to 0$$

of graded R-modules (recall that $R[-d]$ means the free R-module generated by a single element of degree d). The kernel of the first map is

$$\begin{aligned} I' : x^2z &\stackrel{\text{def}}{=} \{\mu \in R \;:\; x^2z\mu \in I'\} \\ &= (y), \end{aligned}$$

so we have the short exact sequence

$$0 \to S[-3] \to R/I' \to R/\,\mathrm{in}_<(I) \to 0,$$

where $S = R/(y) = \mathbf{k}[x,z]$, which says that

$$\mathrm{Hilb}(R/I;t) \;=\; \mathrm{Hilb}(R/I';t) - \mathrm{Hilb}(S[-3];t).$$

The Hilbert series of S is just $(1-t)^{-2}$; however, the shift in grading means that we have to multiply by t^3. Meanwhile,

$$R/I' = \underbrace{\mathbf{k}[x,y]/(xy,y^2)}_{T}[z],$$

and T is a $\mathbf{k}$-vector space with basis $\{1, y, x, x^2, x^3, \ldots\}$, so

$$\mathrm{Hilb}(T;t) \;=\; t + \frac{1}{1-t} \;=\; \frac{1+t-t^2}{1-t}, \qquad \text{and} \qquad \mathrm{Hilb}(R/I';t) \;=\; \frac{1+t-t^2}{(1-t)^2}.$$

Putting all this together, we get

$$\begin{aligned} \mathrm{Hilb}(R/I;t) &= \frac{1+t-t^2}{(1-t)^2} - \frac{t^3}{(1-t)^2} \\ &= \frac{1+t-t^2-t^3}{(1-t)^2} \\ &= \frac{1+2t+t^2}{1-t}. \end{aligned} \tag{2}$$

We can read off quite a bit of information from this. First of all, $\dim R/I = 1$, the order of the pole of $\mathrm{Hilb}(R/I;t)$. In particular, $\operatorname{codim} I = 2$, the number of generators of I, so I is a complete intersection (in particular, it is Gorenstein and Cohen-Macaulay, if you know what those properties are). Its degree is 4, which you can obtain by plugging in $t = 1$ in the numerator of (2). (We would expect this; in general, the degree of a complete intersection is the product of the degrees of the generators, and here they are both quadratic.)

Example 2. Let $R = \mathbf{k}[a,b,c,d,e,f]$, and let $I = (bd-ae, cd-af, ce-bf)$. That is, I is the ideal generated by the 2×2 minors of the matrix

$$\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}.$$

Believe it or not, these generators are a universal Gröbner basis [3, Ex. 1.4]. If $<$ is reverse-lex order, then

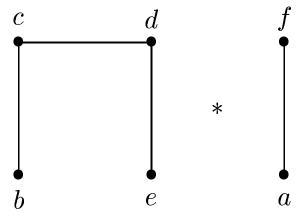
$$\mathrm{in}_<(I) = (ce, cd, bd).$$

This is squarefree, so we can associate with it a Stanley-Reisner simplicial complex Δ. Since no generator of $\mathrm{in}_<(I)$ is divisible by a or f, these vertices are *cone points* of Δ. That is, if Σ is the simplex whose unique facet is $\{a,f\}$, then

$$\Delta \;=\; \Delta' * \Sigma \;\stackrel{\text{def}}{=}\; \{F \cup G \;:\; F \in \Delta',\ G \in \Sigma\}$$

for some simplicial complex Δ' on $\{b,c,d,e\}$. The operator $*$ is called "simplicial join," and behaves fairly nicely: in particular, joining Δ' with a simplex does not change its h-vector. (By the way, the smallest subcomplex $\Delta' \subset \Delta$ such that Δ is the join of Δ' with a simplex is called the *core* of Δ.)

Meanwhile, $\Delta' = \langle bc, be, de\rangle$. Therefore,

$\Delta \quad =$ 

It's pretty easy to see that Δ' is shellable, with h-vector $(1,2)$. Thus the same holds for Δ. Moreover,

$$\dim R/I = \dim R/\,\mathrm{in}_<(I) = 1 + \dim\Delta = 4,$$

so

$$\mathrm{Hilb}(R/I;t) = \frac{1+2t}{(1-t^4)}.$$

By the way, I is not a complete intersection because its codimension (namely $6-4=2$) is smaller than the number of generators, namely 3. In addition, it is not Gorenstein, because the h-vector is not palindromic. However, the fact that Δ is shellable implies that the Stanley-Reisner ring $\mathbf{k}[\Delta] = R/\,\mathrm{in}_<(I)$ is Cohen-Macaulay, which in turn implies that R/I is Cohen-Macaulay. (That shellability implies CM-ness is far from obvious, but may be proved later in this seminar. For details, see [1].)

References

[1] W. Bruns and J. Herzog. *Cohen-Macaulay rings.* Cambridge Univ. Press, Cambridge, revised edition, 1993.
[2] D. Eisenbud. *Commutative Algebra with a view to Algebraic Geometry.* Springer-Verlag, New York, 1995.
[3] B. Sturmfels. *Gröbner Bases and Convex Polytopes.* American Math. Soc., 1996.