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

Introduction to Gröbner bases, I Speaker: Jeremy Martin

1. Motivation

1.1. **Computational Commutative Algebra.** Let $R = \mathbf{k}[X_1, \ldots, X_n]$ (or more generally any commutative Noetherian ring) and

$$\begin{aligned} I &= (a_1, \ldots, a_r), \\ J &= (b_1, \ldots, b_s) \end{aligned}$$

nonzero proper ideals of R (i.e., $I, J \neq R$). There are all sorts of questions that we might want to ask about I and J:

1. Determine whether or not a given ring element f lies in I. I.e., determine whether or not there exist ring elements c_i such that

$$f = \sum_{i=1}^{r} a_i c_i.$$

This sounds trivial, but how do you compute the c_i's? There might be lots of possible c_i's that might work, but it's not at all obvious how to design an algorithm for finding even one such list.

It seems that any such algorithm ought to be based on the fact that R is a $\mathbf{k}$-vector space and I is a subspace. After all, in principle, if $W \subset V$ are vector spaces and $v \in V$, then you ought to be able to do something like the following: fix an inner product on V, find a basis for W, compute the projection v' of v onto W, and check whether $v = v'$. One problem with this that R and I are infinite-dimensional vector spaces. Another problem is that it's not clear how to write down a $\mathbf{k}$-basis (i.e., a basis as a $\mathbf{k}$-vector space) for I in terms of its generators.

2. We'd like to be able to compute ideals such as

$$\begin{aligned} & I \cap J, \\ I + J &= \{x + y \ : \ x \in I, \ y \in J\}, \\ IJ &= \{\textstyle\sum x_i y_j \ : \ x_i \in I, \ y_j \in J\}, \\ \sqrt{I} &= \{x \in R \ : \ x^n \in I \text{ for some } n \\ I : J &= \{x \in R \ : \ xJ \subset I\}, \\ \mathrm{Sat}(I, J) &= \{x \in R \ : \ x^n J \subset I \text{ for some } n\}, \end{aligned}$$

etc. By "compute," I mean "give a system of generators for." This is easy to do for $I + J = (a_i + b_j)$ and $IJ = (a_i b_j)$, but highly nontrivial for all the others.

3. Compute numerical invariants of I and J (or, alternatively, of the quotient rings R/I and R/J) such as

- Krull dimension, depth, degree, minimal number of generators, etc.
- the Hilbert series $\mathrm{Hilb}(R/I; t)$ (in the case that I is homogeneous)

4. Compute homological things such as minimal free resolutions, Koszul complexes, Ext, Tor, and whatnot. Also, determine whether R/I has various "niceness" properties such as being Cohen-Macaulay, Gorenstein, normal, regular, etc.

5. While we're at it, it would be nice to find techniques that can be used to study R-modules other than ideals and quotient rings.

1.2. **Monomial Ideals.** In the special case that I and J are *monomial ideals*—that is, generated by monomials—many of these problems are much easier, because we can give explicit $\mathbf{k}$-bases for I and R/I. R has a "God-given" $\mathbf{k}$-basis, namely the set $\mathcal{M}$ of monomials in $x_1, \dots, x_n$, and to say that I is a monomial ideal is to say that I is an ideal which has a k-vector space basis $\mathcal{M}' \subset \mathcal{M}$. So we can solve the ideal membership problem immediately: given $f \in R$, write $f = \sum \mu_i$, where the μ_i are monomials. If every μ_i is divisible by a generator of I, then $f \in I$; otherwise it isn't.

Intersections are also easy for monomial ideals:

Proposition 1. *Let $I = (\mu_1, \dots, \mu_r)$ and $J = (\nu_1, \dots, \nu_s)$, where the μ_i and ν_j are monomials. Then*

$$I \cap J = (\mathrm{lcm}(\mu_i, \nu_j) \ : \ 1 \le i \le r, \ 1 \le j \le s) \ .$$

The proof is left to the reader; it's not hard.

Another example of something that is easy to compute for monomial ideals is the Hilbert series of a quotient ring R/I: it's just the generating function for the k-basis $\mathcal{M}'$ by total degree. In the case that I is principal, generated by a monomial of degree d, it is not hard to see that

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

More generally, if I has a minimal generator of degree d, then you can write down an exact sequence of graded modules

$$0 \to (S/I'')[-d] \to S/I' \to S/I \to 0,$$

where I' and I'' are monomial ideals minimially generated by fewer elements than I itself. This implies that

$$\mathrm{Hilb}(R/I;t) = \mathrm{Hilb}(R/I';t) - \mathrm{Hilb}(R/I'';t)$$

and allows us to calculate $\mathrm{Hilb}(R/I;t)$ by induction. (See p. 321 of Eisenbud for more details.)

Part 1. Gröbner bases

To avoid repeating the hypotheses over and over again, R will be a polynomial ring $\mathbf{k}[x_1, \dots, x_n]$ over a field $\mathbf{k}$, and $I \subset R$ will be an ideal.

Gröbner bases (also known as *standard bases*, or *Gordan bases* around UCSD) provide a method of reducing questions about arbitrary ideals of R to questions about monomial ideals. The basic idea is that for an arbitrary ideal I, we can define "an" associated monomial ideal $\mathrm{in}(I)$, called the *initial ideal* of I, then translate questions about ideals and rings into questions about linear algebra, which are much easier to compute. (The word "an" is in quotes because, as we'll see, you have quite a lot of choice in defining $\mathrm{in}(I)$.)

Another way to think of a Gröbner basis is that it lets you "straighten" quotient rings R/I. For instance, suppose I is homogeneous, but not a monomial ideal. Then R/I is a perfectly good graded ring, hence it has a Hilbert series. But the Hilbert series is difficult to compute directly the way we did with quotients by monomial ideals, because we have to find a convenient basis to express elements of the quotient ring. If you know a Gröbner basis of I, however, then you know an explicit *monomial* basis for R/I, so you can find the Hilbert series.

The "naive" way to change an arbitrary nonzero polynomial into a monomial is to replace it with one of the monomials appearing in it:

$$x^2y + x^4z^3 + \underline{wy^3} + wxyz \ \rightsquigarrow\ wy^3.$$

This is actually not so far from the way we're going to transform an arbitrary ideal of I into an monomial ideal: choose a set of generators f_i for I, then for each f_i, choose a monomial μ_i appearing in f_i. Then replace I with the ideal (μ_i). Of course, we can't just do this at random. We need to have some sort of sensible way of choosing the monomials μ_i, namely: let $<$ be a total ordering on $\mathcal{M}$, and replace each f_i with the monomial appearing in it which is greatest with respect to $<$. Also, $<$ must satisfy some "natural" conditions, i.e., it must be a *term order* in the following sense:

Definition 1. *A term order on R is a total ordering $<$ on the monomials of R which satisfies the following properties:*

- *refines the partial ordering given by divisibility; that is, if $\mu \mid \mu'$, then $\mu \leq \mu'$; and*
- *is compatible with multiplication, in the sense that for all monomials ν,*

$$\mu \leq \mu' \quad \Longrightarrow \quad \nu\mu \leq \nu\mu'.$$

The three most commonly used orders are as follows. Let $\mu = x_1^{a_1}x_2^{a_2}\dots x_n^{a_n}$ and $\nu = x_1^{b_1}x_2^{b_2}\dots x_n^{b_n}$, and suppose that the variables x_i are ordered by

$$x_1 > x_2 > \cdots > x_n. \tag{1}$$

Lexicographic order. $\mu >_{lex} \nu$ if there exists some $i \in \{1, 2, \dots, n\}$ such that $a_i > b_i$, and $a_j = b_j$ for all $j < i$.

Graded lexicographic order. This is similar to lex order, but the first criterion is total degree. That is, $\mu >_{glex} \nu$ if $\deg(\mu) > \deg(\nu)$, or if $\deg(\mu) = \deg(\nu)$ and $\mu >_{lex} \nu$.

Reverse lexicographic order. No, it's not the opposite of $<_{lex}$. The idea is that instead of looking for higher powers of more important variables, we are looking for lower powers of less important variables. That is, $\mu >_{rlex} \nu$ if $\deg(\mu) > \deg(\nu)$, or if there exists some $i \in \{1, 2, \dots, n\}$ such that $a_i < b_i$, and $a_j = b_j$ for all $j > i$. Perhaps surprisingly, this is the "best" term order to use for many applications.

For instance, the ten quadratic monomials in $k[a, b, c, d]$, listed largest to smallest in lex order, are

$$a^2,\ ab,\ ac,\ ad,\ b^2,\ bc,\ bd,\ c^2,\ cd,\ d^2,$$

while in reverse lex order they are

$$a^2,\ ab,\ b^2,\ ac,\ bc,\ c^2,\ ad,\ bd,\ cd,\ d^2.$$

In what follows, $<$ is always a term order on R.

Definition 2. *Let $f \in R$, so that we may write $f = \sum_{i \in I} c_i\mu_i$, where I is a finite index set, the μ_i are monomials, and $c_i \in \mathbf{k}$. The initial term of f with respect to $<$, written $\mathrm{in}_<(f)$ or $\mathrm{in}(f)$, is that term $c_i\mu_i$ such that μ_i is maximal.*

Definition 3. *The initial ideal of I with respect to $<$ is*

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

The fundamental reason that this is so useful is the following theorem, due to Macaulay (it's Theorem 15.3 in Eisenbud):

Theorem 1. *The set of monomials not in $\mathrm{in}_<(I)$ is a basis for R/I as a k-vector space.*

In particular, $R/I \cong R/\operatorname{in}(I)$ as vector spaces. If I is homogeneous, then this implies that R/I and $R/ini(I)$ have the same Hilbert series.

It is obvious that if $\{f_i\}$ are generators for I, then

$$\operatorname{in}_<(I) \supseteq (\operatorname{in}_<(f_i)).$$

However, the reverse inclusion is NOT in general true. It's not hard to come up with a counterexample. Suppose we have a term order $<$ on $\mathbf{k}[x, y, z]$ in which $x > y > z$. Consider the ideals

$$I = (x - y), \qquad J = (x - y,\ x - z).$$

Then $\operatorname{in}_<(x - y) = \operatorname{in}_<(x - z) = x$, but surely we can't want to replace both I and J with the monomial ideal (x), which doesn't even have the same codimension as J. Besides, choosing a different set of generators for J would produce more initial terms: $J = (x - y,\ y - z)$, and $\operatorname{in}(y - z) = (y)$. So it looks as if we should replace J with the monomial ideal (x, y), rather than x.

Definition 4. *A finite subset $\{f_1, \ldots, f_r\} \subset I$ is a Gröbner basis for I with respect to $<$ if*

$$\operatorname{in}_<(I) = (\operatorname{in}_<(f_i)).$$

Theorem 2. *Every ideal of R has a Gröbner basis.*

Proof: Left as an exercise. (Hint: Use the fact that R is Noetherian.)

It's not clear from the definition how to get your hands on a Gröbner basis. Fortunately, there is an algorithm, due to Buchberger, which takes as input a set of generators for an ideal and outputs a Gröbner basis.