MATH 499: Notes
February 15, 2010

Given an ideal \( I = \langle f_1, \ldots, f_k \rangle \), we’ve seen several examples now of how it is possible that \( f_1, \ldots, f_k \) may not be a Gröbner basis for \( I \), i.e. we may have

\[
\langle \text{LT}(f_1), \ldots, \text{LT}(f_k) \rangle \nsubseteq \langle \text{LT}(I) \rangle.
\]

Essentially, the problem is that it may be possible to cancel out the leading terms of some of the \( f_i \) to get new elements of \( I \) with smaller leading terms.

Let’s look at an example. Consider the ideal \( I = \langle f_1, f_2 \rangle \subseteq R[x, y, z] \) in graded lex order, with \( f_1 = x^2y + y^2z \) and \( f_2 = xy^2 + z^2 \). We can try to cancel out the leading terms of \( f_1 \) and \( f_2 \) in hopes of getting a polynomial in \( I \) with a new leading monomial:

\[
f_3 = yf_1 - xf_2 = y(x^2y + y^2z) - x(xy^2 + z^2) = y^3z - xz^2.
\]

To potentially find more new leading terms of \( I \) that aren’t in \( \langle x^2y, xy^2, y^3z \rangle \), we might, for example try to attempt the same sort of cancellation on the leading terms of \( f_1 \) and \( f_3 \), giving

\[
y^2zf_1 - x^2f_3 = y^2z(x^2y + y^2z) - x^2(y^3z - xz^2) = y^4z^2 + x^3z^2,
\]

whose leading term is already known to be in \( \langle \text{LT}(I) \rangle \) since it is divisible by \( \text{LT}(f_3) \). However, we can divide it by \( f_3 \) (along with \( f_1 \) and \( f_2 \)) to possibly get a remainder in \( I \) with a new leading term

\[
y^4z^2 + x^3z^2 = yzf_3 + (x^3z^2 + yz^3),
\]

and we see that \( f_4 = x^3z^2 + yz^3 \in I \) so that \( x^3z^2 \in \langle \text{LT}(I) \rangle \) is a new leading term which is not divisible by any of \( x^2y, xy^2, y^3z \).

What we’re doing is looking at pairs of polynomials in our current list of generators, \( f_i \) and \( f_j \) and cancelling out their leading terms, and then dividing the result by our current list of generators to potentially get an element of the ideal with a new leading term. It turns out that if we keep doing this until we no longer get anything new in this way out of any pair \((f_i, f_j)\) of our current generators, then we can stop this process and our current list of generators is a Gröbner basis.

More precisely, given monomials \( x^\alpha \) and \( x^\beta \), with \( \alpha = (\alpha_1, \ldots, \alpha_n) \) and \( \beta = (\beta_1, \ldots, \beta_n) \) in \( R[x_1, \ldots, x_n] \), the least common multiple of \( x^\alpha \) and \( x^\beta \) is \( x^\gamma \) where \( \gamma_i = \max\{\alpha_i, \beta_i\} \). If \( x^\gamma \) is the LCM of the leading monomials of \( f \) and \( g \), then we say that the \( S\)-polynomial of \( f \) and \( g \) is the polynomial

\[
S(f, g) = \frac{x^\gamma}{\text{LT}(f)}f - \frac{x^\gamma}{\text{LT}(g)}g.
\]

This is more precisely what we mean above by “cancelling the leading terms” of \( f_i \) and \( f_j \).

Thus to find a Gröbner basis, we claim that all we need to do is start with some generating set of polynomials \( G = \{ f_i \} \), and then keep computing \( S(f_i, f_j) \) for pairs of polynomials in our set and dividing the \( S\)-polynomial by the set \( G \), and adding the remainder to \( G \) if it isn’t zero (and hence its leading term isn’t in \( \langle \text{LT}(G) \rangle \) yet). Eventually this process will stop1 when division of

---

1 This process must stop eventually, because each time a polynomial is added to \( G \), the ideal \( \langle \text{LT}(G) \rangle \) gets bigger, and it is impossible for there to be an infinite ascending chain \( I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \) of ideals in \( R[x_1, \ldots, x_n] \). This fact is equivalent to the claim that any ideal of \( R[x_1, \ldots, x_n] \) is finitely generated. (Hint: Consider \( I = \bigcup \{ f \} \).)
$S(f_i, f_j)$ by the set $G$ yields a zero remainder for every pair $f_i, f_j \in G$, and once that happens, $G$ is a Gröbner basis.

This algorithm for computing a Gröbner basis is called Buchberger’s Algorithm, and it relies on the following theorem (for a proof, see Cox, Little, and O’Shea, 2.6):

**Theorem** (Buchberger’s criterion). Let $G = \{ f_1, \ldots, f_k \} \subset R[x_1, \ldots, x_n]$ be a set of polynomials and $I = \langle G \rangle$ be the ideal they generate. Then $G$ is a Gröbner basis for $I$ if and only if for every pair $1 \leq i, j \leq k$, the remainder on division of $S(f_i, f_j)$ by $G$ is zero.

In our above example, it turns out though that we would have been better off first trying to cancel the leading terms of $f_2$ and $f_3$: the polynomial

$$f_5 = yz f_2 - xf_3 = yz(xy^2 + z^2) - x(y^3z - xz^2) = x^2 z^2 + yz^3$$

has a leading term which properly divides that of $f_4$, and in fact we see that once we have $f_5 \in I$, the polynomial $f_4$ is redundant since $f_4 = xf_5$. We must then check the $S$-polynomials of $f_5$ with $f_1$, $f_2$, and $f_3$ (this is enough since we’ve already looked at every pair from $f_1, f_2, f_3$):

- $S(f_1, f_5) = z^2(x^2y + y^2z) - y(x^2z^2 + yz^3) = 0$,
- $S(f_2, f_5) = xz(x^2y^2 + z^2) - y^2(x^2z^2 + yz^3) = -y^3z^3 + xz^4 = -z^2f_3$,
- $S(f_3, f_5) = x^2z(y^3z - xz^2) - y^3(x^2z^2 + yz^3) = -y^4z^3 - x^3z^3 = -yz^2f_3 - xzf_5$,

and we see that the remainders are all zero, so $\{f_1, f_2, f_3, f_5\}$ is a Gröbner basis for $I$.

**Elimination of variables**

We may want to try to find elements of an ideal $I \subset R[x_1, \ldots, x_n]$ which only involve some of the variables $x_i, \ldots, x_n$. For example, to find an implicit equation for the curve given parametrically by $\left( \frac{a(t)}{p(t)}, \frac{b(t)}{q(t)} \right)$, we would like to find an element of the ideal $\langle p(t)x - a(t), q(t)y - b(t) \rangle$ that only involves $x$ and $y$ and not $t$.

It turns out that to do this, all we need to do is find a Gröbner basis for the ideal in Lex order. This is because in Lex order, if the leading term of a polynomial only involves the variables $x_i, \ldots, x_n$, then in fact all of its terms involve only $x_i, \ldots, x_n$. Thus we have

$$LT(I \cap R[x_i, \ldots, x_n]) = LT(I) \cap R[x_i, \ldots, x_n]$$

and if $G$ is a Gröbner basis for $I$ in Lex order, then $G \cap R[x_i, \ldots, x_n]$ is a Gröbner basis (and hence a generating set!) for $I \cap R[x_i, \ldots, x_n]$.

Thus, to “eliminate” variables from our ideal (i.e. find the polynomials in the ideal which only involve the other variables), we just need to put the variables to be eliminated first in Lex order and find a Gröbner basis for the ideal. This is something very special about Lex order: none of the other orders we’ve looked at are “elimination orders” in this sense.

\(^2\)The set $\{f_1, f_2, f_3, f_4, f_5\}$ is also a Gröbner basis for this ideal, but $f_4$ is redundant, so we may as well leave it out.

\(^3\)See 3.1 in Cox, Little, O’Shea for more details.
Sample Code

Here is a sample session in Macaulay 2 computing a Gröbner basis for $I = \langle x^2y + y^2z, xy^2 + z^2 \rangle \subseteq \mathbb{R}[x, y, z]$ in graded lex order:

Macaulay 2, version 1.2
with packages: Elimination, IntegralClosure, LLLBases, PrimaryDecomposition, ReesAlgebra, SchurRings, TangentCone

```plaintext
i1 : R=QQ[x,y,z,MonomialOrder=>GLex]
o1 = R

i2 : f=x^2*y+y^2*z
2 2
o2 = x y + y z
o2 : R

i3 : g=x*y^2+z^2
2 2
o3 = x*y + z
o3 : R

i4 : I=ideal(f,g)
2 2 2 2
o4 = ideal (x y + y z, x*y + z )
o4 : Ideal of R

i5 : gens gb I
o5 = | xy2+z2 x2y+y2z y3z-xz2 x2z2+yz3 |
       1 4
o5 : Matrix R <--- R

i6 : h=y^4*z^2+x^3*z^2
```
\[ o6 = yz + xz \]
\[ o6 : R \]
\[ i7 : h \% I \]
\[ o7 = 0 \]
\[ o7 : R \]
\[ i8 : h // gens gb I \]
\[ o8 = \{3\} | -xyz | \]
\[ \{3\} | y2z | \]
\[ \{4\} | 0 | \]
\[ \{4\} | x | \]
\[ \]
\[ 4 \quad 1 \]
\[ o8 : Matrix R \leftarrow R \]
Here is some code computing the same Gröbner basis in Singular:

```plaintext
SINGULAR

A Computer Algebra System for Polynomial Computations

version 3-1-0

by: G.-M. Greuel, G. Pfister, H. Schoenemann

Mar 2009

FB Mathematik der Universität, D-67653 Kaiserslautern

> ring R = 0,(x,y,z),Dp; //Dp = glex, lp=lex, dp=grevlex
> poly f=x^2*y+y^2*z;
> poly g=x*y^2+z^2;
> ideal I=f,g; // An "ideal" for Singular is just a list of polynomials.
> I;
I[1]=x^2*y+y^2*z
I[2]=x*y^2+z^2
> ideal gI=groebner(I);
> gI;
gI[1]=x*y^2+z^2
gI[2]=x^2*y+y^2*z
gI[3]=y^3*z-x*z^2
gI[4]=x^2*z^2+y*z^3
> poly h=y^4*z^2+x^3*z^2; // Next we will divide h by the list of polynomials I, which
> reduce(h,I); // gives a warning since we aren’t dividing by a Groebner basis.
// ** I is no standard basis
y^4*z^2+x^3*z^2
> reduce(h,gI);
0
```