Plan for PURE Math 2012 Seminar

Week 2

Monday: Polynomial division (Chapter 2, §3) – put some discussion of monomial orders defined by matrices into Tuesday's discussion
Tuesday: Lecture on monomial ideals, Dixon's Lemma; discussion: more on monomial orders (Chapter 2, §4)
Wednesday: Definition of Gröbner bases (Chapter 2, §§5,6) Buchberger's Algorithm (omit proof of Buchberger's S-pair Criterion) (Chapter 2, §7)
Thursday: First examples – Elimination theory (Chaper 2, §8, Chapter 3, §1)

Week 2 Discussions - Polynomial Division, Gröbner Bases, First Applications

Day 1: The Division Algorithm in $k[x_1, \ldots, x_n]$

Background

Given a monomial order, polynomials $f_1, \ldots, f_s$ (the divisors), and another polynomial f, we have seen an algorithm for producing quotients $a_1, \ldots, a_s$ and remainder r satisfying an equation:

$$(*) \qquad f = a_1 f_1 + \cdots + a_s f_s + r,$$

and the conditions that
1) $multideg(a_i f_i) \leq multideg(f)$ for all i where $a_i \neq 0$, and
2) no monomial in r is divisible by any of the $LT(f_i)$.

Discussion Questions

A) Do Problem 1 from Chapter 2, §3 of "IVA" individually and compare your results. What does this say about the uniqueness of the quotients and remainders on division? Explain carefully what they depend on.
B) Do Problem 9 from Chapter 2, §3 of "IVA".
C) Problem 11 from Chapter 2, §3 of "IVA"
   1) The hardest part of this is probably just understanding what all of the notation means. Work out an explicit example first. Take

$$\begin{aligned} f_1 &= x^4 + x^2y + y^3 + 1 \\ f_2 &= x^2y - 3 \\ f_3 &= y^3 - 3y + 1, \end{aligned}$$

   use the *lex* order with $x > y$, and divide f_1, f_2, f_3 into $f = x^5$. Draw a picture in $\mathbf{Z}^2_{\geq 0}$ showing the sets Δ_i and Δ, and verify that the conditions in part c are satisfied for your quotients a_i and your remainder.
   2) Now work out the general proofs. An important lesson here: Never underestimate the power of working out examples to clarify things! But of course, the examples are not always the ultimate goal in mathematics since we usually want to establish general statements!)

Day 2: Dixon's Lemma, More on Monomial Orders

A) Do Problem 4 in §4 of Chapter 2 to practice with ideas connected to Dixon's Lemma.

The main portion of today's discussion is devoted to some additional ideas related to monomial orders. Besides the *lex, grevlex, grlex* orders we discussed in class, there are many other ways to define monomial orders. The following construction gives a general way to understand the process.

Defining a Monomial Order by a Matrix

We have discussed the construction of *weight orders* $>_w$, where we compare two monomials x^α and x^β first by taking dot products of their exponent vectors with a fixed *weight vector* w, the "break ties" if $\alpha \cdot w = \beta \cdot w$ using another order.

Generalizing the weight orders $>_w$, we can also define monomial orders on $k[x_1, \ldots, x_n]$ starting from any $m \times n$ matrix M with

- $m \geq n$,
- $\mathrm{rank}(M) = n$,
- all entries non-negative integers.

(The same construction also works for M with non-negative real entries, but the `GroebnerBasis` command in Mathematica will accept only rational entries in weight vectors, so we will not discuss that extension.) Namely, suppose the *rows* of M are the vectors $w_1, \ldots, w_n$. Then we can compare monomials x^α and x^β by first comparing their w_1-weights, then breaking ties sucessively with the w_2-weights, w_3-weights, and so on through the w_m-weights. In symbols:

$$\begin{aligned}
&x^\alpha >_M x^\beta \Leftrightarrow w_1 \cdot \alpha > w_1 \cdot \beta \\
&\quad \text{or } [(w_1 \cdot \alpha = w_1 \cdot \beta) \text{ and } (w_2 \cdot \alpha > w_2 \cdot \beta)] \\
(1) \qquad &\quad \text{or } [(w_1 \cdot \alpha = w_1 \cdot \beta) \text{ and } (w_2 \cdot \alpha = w_2 \cdot \beta) \text{ and } (w_3 \cdot \alpha > w_3 \cdot \beta)] \\
&\quad \text{or } \cdots \\
&\quad \text{or } [(w_1 \cdot \alpha = w_1 \cdot \beta) \text{ and } \cdots \text{ and } (w_{m-1} \cdot \alpha = w_{m-1} \cdot \beta) \text{ and } (w_m \cdot \alpha > w_m \cdot \beta)]
\end{aligned}$$

Discussion Questions

All the monomial orders we will need can be specified as $>_M$ orders for appropriate matrices M.

B)

1) For instance, show that the *lex* order with $x_1 > \ldots > x_n$ on $k[x_1, \ldots, x_n]$ is defined by $M = I_n$, the $n \times n$ identity matrix.
2) Show that the *grevlex* order, with $x > y > z$, is defined by the matrix

$$M_{grevlex} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

(The same pattern works for polynomial rings in any number of variables.)

3) Negative entries can also appear in these matrices. For instance, show that the *grevlex* order with $x > y > z$ could also defined using

$$M_{grevlex} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$$

What is the corresponding matrix for the *grevlex* order with $x_1 > x_2 > \cdots > x_n$?

C) The *grlex* (graded lex) order in $k[x, y, z]$ compares monomials first by total degree (weight vector $w_1 = [1, 1, 1]$), then breaks ties by the *lex order*. This shows $>_{grlex} = >_M$ for the matrix M here:

$$M = M_{grlex} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Show that we could also use

$$M' = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

That is, show the last row in M is actually superfluous. (Hint: Making comparisons as in (1), when would we ever need to use the last row?)

D) Show that if the $m \times n$ matrix of rational numbers M satisfies

- $m \geq n$,
- $\text{rank}(M) = n$ (the largest possible for a matrix of this shape),
- the uppermost nonzero entry in each *column* (i.e. the first nonzero entry down from the top of the column) is positive.

then (1) defines a monomial order $>_M$. Be sure you see and explain why the condition on the rank of M is necessary.

E) In Sage/Singular, we can define monomial orders by this process. For instance, to define a weight order with $w = (2, 4, 8)$ and ties broken by *grevlex* with $x > y > z$, it might be most natural to use

$$M = \begin{pmatrix} 2 & 4 & 8 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

But Singular requires an invertible square matrix to define a monomial order. So, we need to pick a set of $n = 3$ linearly independent rows out of this matrix M. But which ones?? The choice of any three linearly independent rows gives *some monomial order*, but it may not be the one we want. Here is an example. Consider the two matrices:

$$M' = \begin{pmatrix} 2 & 4 & 8 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} \qquad M'' = \begin{pmatrix} 2 & 4 & 8 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

(In M' we have omitted the fourth row of M, while in M'', we have omitted the third row of M.)

1) Consider the monomials x^2z^2 and y^3z. Which is bigger under the matrix order $>_{M'}$? Which is bigger under the matrix order $>_{M''}$? Which should be bigger under the weight order $>_{w,grevlex}$ (comparing w-weights first, then breaking ties with $>_{grevlex}$)? What does this say about the matrices M' and M'' – which is *not* the "right" 3×3 matrix to use?
2) Given an $m \times n$ matrix M defining an order $>_M$, describe a general method for picking the correct $n \times n$ submatrix M' of M to define the same order, and prove that your method is correct.

Day 3: Gröbner Bases (Finally!)

Background

We have now seen the definition of a *Gröbner basis.* Given an ideal $I \subset k[x_1, \ldots, x_n]$ and a monomial order $>$, a Gröbner basis for I is a set of polynomials $\{g_1, \ldots, g_t\} \subset I$ with the property that the leading terms of the g_i generate the ideal of all leading terms of elements of I: in symbols:

$$\langle LT(g_1), \ldots, LT(g_t)\rangle = \langle LT(I)\rangle.$$

Gröbner bases exist for all non-zero ideals because of the result we called Dickson's Lemma. Recall the idea: Every monomial ideal has a finite generating set. So if we apply this to the monomial ideal $\langle LT(I)\rangle$ and get a finite generating set $\{x^{\alpha(1)}, \ldots, x^{\alpha(t)}\}$, then there are polynomials $g_i \in I$ with $LT(g_i) = x^{\alpha(i)}$ for all i, and the g_i form a Gröbner basis for I by the definition. Soon, we will learn a criterion for when a set is a Gröbner basis and an algorithm for finding them (both discovered by the Austrian mathematician Bruno Buchberger). For now, we want to get a feeling for what the definition means.

The S-polynomial of two polynomials f, g with respect to a monomial order $>$ is defined in "IVA" as:

$$S(f,g) = \frac{x^\gamma}{LT(f)} f - \frac{x^\gamma}{LT(g)} g,$$

where $x^\gamma = LCM(LM(f), LM(g))$. By Buchberger's Criterion, we know that $G = \{g_1, \ldots, g_t\} \subset I$ is a Gröbner basis for I if and only if

$$\overline{S(g_i, g_j)}^G = 0$$

for all pairs (i,j) with $1 \leq i < j \leq t$.

This gives the idea behind an algorithm for computing Gröbner bases we discussed in class, starting from an arbitrary ideal basis $F = \{f_1, \ldots, f_s\}$ for I. We start with $G = F$, compute S-polynomial remainders, and adjoin any non-zero polynomials we find to the set G. This process is iterated until Buchberger's Criterion is satisfied, and we have a Gröbner basis. The resulting algorithm is called *Buchberger's Algorithm* for Gröbner bases.

Discussion Questions

From Chapter 2, §5 of "IVA" do:

A) Problem 5. (This gives an alternate form of the condition defining a Gröbner basis that is sometimes useful.)

B) Problem 6. (This is probably the most useful property of Gröbner bases: If G is a Gröbner basis for I and $f \in I$, then the remainder on division of f by G is guaranteed to be zero!)

C) Problems 7, 8. (*Suggestion:* Try "making" some other polynomials in the ideals, and see if you can tell whether the condition for Gröbner bases from Problem 5 is always true.)

D) Consider an ideal $I \subset k[u_1, \ldots, u_m, v_1, \ldots, v_n]$ for $n, m \geq 1$ generated by polynomials of the following form:

$$I = \langle v_1 - f_1(u_1, \ldots, u_m), \ldots, v_n - f_n(u_1, \ldots, u_m)\rangle$$

where the f_i are arbitrary polynomials. Show that the given generators form a Gröbner basis for I with respect to some particular monomial order (which one?).

E) Let $f_1 = x^3y - x$ and $f_2 = y^2 - x$.

1) Is $\{f_1, f_2\}$ a Gröbner basis for $I = \langle f_1, f_2\rangle$ with respect to the *lex* order, $x > y$ or with $y > x$? Why or why not?

2) Apply Buchberger's Algorithm to find Gröbner bases for the ideal $I = \langle f_1, f_2\rangle$ first using the lex order with $x > y$, and second using the lex order with $y < x$. Your results should look quite different.

Day 4: Elimination

We have now seen the Elimination and Extension Theorems from Chapter 3, §1. The Elimination Theorem shows that lexicographic Gröbner bases systematically eliminate variables "as much as possible" in the following sense.

- (Elimination Theorem) Let I be an ideal in $k[x_1, \ldots, x_n]$, and G a Gröbner basis of I with respect to the *lex* order with $x_1 > x_2 > \cdots > x_n$. Let $I_i = I \cap k[x_{i+1}, \ldots, n]$ be the ith elimination ideal of I. Then $G_i = G \cap k[x_{i+1}, \ldots, n]$ is a Gröbner basis of I_i for each i, $1 \leq i \leq n - 1$.
- The Extension Theorem then gives a condition under which $(a_{i+1}, \ldots, a_n) \in V(I_i)$ can be extended to $(a_i, a_{i+1}, \ldots, a_n) \in V(I_i)$.

Discussion Questions

A) Using Sage/Singular, I computed a Gröbner basis for the ideal $I = \langle x^2 + y^2 + z^2 - 4, xz - y, y^2 - z^2 + 1\rangle$ with respect to the *lex* order, $x > y > z$, and found the output:

$$2z^4 - 4z^2 - 1, y^2 - z^2 + 1, x - 2yz^3 + 4yz.$$

1) Using the Elimination Theorem, give Gröbner bases for the elimination ideals $I_1 = k[y,z]$ and $I_2 = k[z]$.
2) What does the Extension Theorem say about the number of points in the variety $\mathbf{V}(I) \in \mathbf{C}^2$? What are those points?

B) In this problem, we will see reasons for some of the patterns you may have noticed in various examples. Let V be a finite set in $\mathbf{C}^n$ and let $I = \mathbf{I}(V) = \langle f_1, \ldots, f_s \rangle \subset \mathbf{C}[x_1, \ldots, x_n]$ be the ideal of all polynomials that are zero at all the points of V.

1) Show that for each i, $1 \leq i \leq n$, I must include a nonzero polynomial $p_i(x_i)$ that depends only on the variable x_i.
2) Show that if we compute a Gröbner basis G for I with respect to a lex order $>_i$ with x_i as the *last* - *i.e. smallest* variable, then $p_i(x_i)$ must appear in that Gröbner basis G. (Hint: If $cx_i^\alpha = LT_{>_i}(p_i(x_i))$ is the leading term of $p_i(x_i)$, then some Gröbner basis element g in G must have a leading term (with respect to this special *lex* order $>_i$ which divides cx_i^α. What does that say about the form of g?
3) Let V be a finite set in $\mathbf{C}^3$ which is in *"general position" in the sense that the z-coordinates of the points of V are distinct*. Let $I = \mathbf{I}(V)$. What does the Gröbner basis for $I = \mathbf{I}(V)$ with respect to the *lex* order, $x > y > z$ look like? (How many polynomials will it contain, what are their forms, etc.?)
4) What would the corresponding statement be for finite V in "general position" in $\mathbf{C}^n$ for general $n \geq 2$?

Additional Hints for 3 and 4: Note that the "general position" hypothesis is *not* satisfied, for instance, for the Gröbner basis from question B above (*Why not?*) Think about what part 2 tells you here. You will get one of the Gröbner basis elements that way. Then, what do the others look like? For instance, is there a polynomial of the form $y - f(z)$ in the ideal (hence in the first elimination ideal $I \cap \mathbf{C}[y,z]$? Must it appear in the *lex* Gröbner basis? If so, why? Then, what about polynomials involving x? The answer is a special case of a result sometimes called the "Shape Lemma."