SIMU 1999 - Gröbner Basis Seminar
Week 2 Discussions-Monomial Orders, Polynomial Division, Gröbner Bases

Day 1: Monomial Orders

In class today, we introduced the definition of a *monomial order* in the polyomial ring $k[x_1, \ldots, x_n]$. This was an ordering $>$ on the monomials x^α (or equivalently on the exponent vectors α) such that:

1) $>$ is a total (linear) order on vectors with nonnegative integer components. (This means that for every pair of monomials x^α and x^β, exactly one of the following is true: either $x^\alpha > x^\beta$, or $x^\alpha = x^\beta$, or $x^\beta > x^\alpha$.)
2) For all α, β, γ, we have
$$\alpha > \beta \Rightarrow \alpha + \gamma > \beta + \gamma$$
3) $>$ is a well-ordering. (In other words, every non-empty subset of monomials or exponent vectors has a smallest element under $>$).

Today, we want to think about some of the implications of this definition.

Discussion Questions

A) To practice with monomial orders, do Problems 1,2 from Chapter 2, §2 of "IVA".

B) Show that in $k[x, y]$, the graded lexicographic and graded reverse lexicographic orders are the same. Is this true for $n > 2$?

C) Suppose we try to define an order $>$ by omitting the first part of the definition of the graded lexicographic order, so that $\alpha > \beta$ if the rightmost entry in $\alpha - \beta$ is negative. Do we get a monomial order? Why or why not?

D) We could also try to define an order $>_w$ by comparing the "total weights" of two monomials with respect to a given weight vector w on the variables. That is, for a monomial x^α, we think of the variable x_i as having weightw_i (from the vector w). We compute $\alpha \cdot w = \alpha_1 w_1 + \cdots + \alpha_n w_n$ and say $x^\alpha >_w x^\beta$ if $\alpha \cdot w > \beta \cdot w$.
   1) Let $n = 2$ and $w = (3, 5)$. Is $>_w$ a monomial order? Why or why not?
   2) Let $n = 2$ again and $w = (1, \sqrt{2})$. Same question.

Challenge Question

What property of the components of the vector w would guarantee that $>_w$ *does* define a monomial order on $k[x_1, \ldots, x_n]$? (The fact that $\sqrt{2}$ is not a rational number in part 2 of D is important, but it is not the whole story!)

Day 2: More on Monomial Orders

Background

In addition to the *lex, grevlex, grlex* orders we discussed in class, there are many other ways to define monomial orders as well. The following construction gives a very general way to understand the process.

Defining a Monomial Order by a Matrix

In the lab last time, we 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

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

(The same construction also works for M with non-negative real entries, but the `Groebner` package will accept only integer entries, 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:

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

Discussion Questions

A) Show that if the matrix M satisfies
   - $m \geq n$,
   - $\text{rank}(M) = n$,
   - all entries non-negative integers

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

B) All the monomial orders we will need can be specified as $>_M$ orders for appropriate matrices M. For instance, show that the *lex* order with $x > y > z$ on $\mathbf{Q}[x, y, z]$ is defined by the identity matrix

$$M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Show that the *grevlex* order, with $x > y > z$, is defined by the matrix

$$M_2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

(The same patterns work for polynomial rings in any number of variables.)

C) The *grlex* (graded lex) order 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

$$M_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Show that we could also use

$$M_3' = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

That is, show the last row in M_3 is actually superfluous. (Hint: Making comparisons as in (1) when would we ever need to use the last row?)

D) In Maple, we can define monomial orders by this process, but we must use *square* $n \times n$ matrices. For instance, to define a weight order with $w = (2,4,8)$ and ties broken by *grevlex* with $x > y > z$, it is most natural to use

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

But Maple will not accept this! 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 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.

Day 3: 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) $multideg(a_i f_i) \le multideg(f)$ 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 Problems 1,2 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) Do Problem 11 from Chapter 2, §3 of "IVA". (*Suggestion:* The hardest part of this is probably just understanding what all of the notation means. Try working out an explicit example first, maybe with $f_1 = x^4 + x^2y + y^3 + 1$, $f_2 = x^2y - 3$, $f_3 = y^3 - 3y + 1$using the *lex* order with $x > y$, and $f = x^5$. 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. Then think about what happens in division and work out the general proofs.)

Day 4: 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 $\{g_1, \ldots, g_t\}$ 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. Next week, 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.

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.)

Challenge Question

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?).