Mathematics 392 – Seminar in Computational Commutative Algebra
Selected Solutions – Problem Set 4
October 2, 2006

2.4/12 a) Given $u \in \mathbf{Z}^n_{\geq 0}$ and another monomial order $>_\sigma$, we define the weight order $>_{u,\sigma}$ by

$$x^\alpha >_{u,\sigma} x^\beta \Leftrightarrow \begin{cases} u \cdot \alpha > u \cdot \beta & \text{or} \\ u \cdot \alpha = u \cdot \beta & \text{and } x^\alpha >_\sigma x^\beta \end{cases}$$

To show that $>_{u,\sigma}$ is a monomial order, we will use Corollary 6.

(i) First for every pair of monomials x^α and x^β, either $u \cdot \alpha > u \cdot \beta$, or $u \cdot \alpha = u \cdot \beta$, or $u \cdot \alpha < u \cdot \beta$. In the first case, $x^\alpha >_{u,\sigma} x^\beta$; in the last case $x^\beta >_{u,\sigma} x^\alpha$. In the case $u \cdot \alpha = u \cdot \beta$, then we go on and compare using the $>_\sigma$ order. Since that is a monomial order, either $x^\alpha >_\sigma x^\beta$, or $x^\alpha = x^\beta$, or $x^\beta >_\sigma x^\alpha$. We have shown that $>_{u,\sigma}$ is a total order.

(ii) Assume $x^\alpha >_{u,\sigma} x^\beta$ and let x^γ be another monomial. If $u \cdot \alpha > u \cdot \beta$, then by the bilinearity of the dot product:

$$u \cdot (\alpha + \gamma) = u \cdot \alpha + u \cdot \gamma > u \cdot \beta + u \cdot \gamma = u \cdot (\beta + \gamma).$$

This shows $x^{\alpha+\gamma} >_{u,\sigma} x^{\beta+\gamma}$ in this case. If $u \cdot \alpha = u \cdot \beta$, then $x^\alpha >_\sigma x^\beta$. Since $>_\sigma$ is a monomial order, it follows that $x^{\alpha+\gamma} >_\sigma x^{\beta+\gamma}$ also. So $x^{\alpha+\gamma} >_{u,\sigma} x^{\beta+\gamma}$ in this case also.

(iii) Finally, since $u, \alpha \in \mathbf{Z}^n_{\geq 0}$, $u \cdot \alpha \geq 0$. If $u \cdot \alpha > 0$ then $x^\alpha >_{u,\sigma} 1$. On the other hand, if $u \cdot \alpha = 0$, then we compare x^α with 1 using the $>_\sigma$ order. Since $>_\sigma$ is a monomial order $x^\alpha \geq_\sigma 1$. Hence for all α, $x^\alpha \geq_{u,\sigma} 1$, and the criterion of Corollary 6 is satisfied.

d) Let $u = (1, \ldots, 1, 0, \ldots, 0)$ with i 1's at the start. Define the elimination order $>_i$ to be $>_{u,grevlex}$. Suppose x^α is any monomial containing one of the variables x_j, $1 \leq j \leq i$, and x^β is any monomial containing only $x_{i+1}, \ldots, x_n$. Then some $\alpha_j > 0$ for $1 \leq j \leq i$, and $\beta_j = 0$ for all $1 \leq j \leq i$. Hence

$$\begin{aligned} u &= (1, \ldots, 1, 0 \ldots 0) \\ \alpha &= (\alpha_1, \ldots, \alpha_i, *, \ldots, *) \Rightarrow u \cdot \alpha > 0 \\ \beta &= (0, \ldots, 0, \beta_{i+1}, \ldots, \beta_n) \Rightarrow u \cdot \beta = 0 \end{aligned}$$

By the definition of the $>_i$ order, $x^\alpha >_i x^\beta$ since $u \cdot \alpha > u \cdot \beta$ for these monomials.

2.5/8. (Note: for the following proof we assume $k = \mathbf{R}$, or some other infinite field. The same conclusion is valid in all cases, but a slightly different proof would be needed if k is finite).

Let $>$ be the *lex* order with $x > y > z$. We claim $G = \{x - z^2, y - z^3\}$ *is* a Gröbner basis for $I = \langle G \rangle$. To show this, using the result of Problem 5, we must prove that if $f \in I$, then $LT_>(f)$ is divisible by either $x = LT_>(x - z^2)$ or $y = LT_>(y - z^3)$. Begin by applying the division algorithm (same *lex* order) to write

$$f = a(x - z^2) + b(y - z^3) + r. \tag{1}$$

Since no term in r is divisible by either x or y, r is a polynomial in z alone. But now notice that $V(x - z^2, y - z^3)$ is a twisted cubic curve, parametrized by z:

$$V(x - z^2, y - z^3) = \{(z^2, z^3, z) : z \in \mathbf{R}\}.$$

If we substitute $x = z^2$ and $y = z^3$, then since $f \in I$, $f(z^2, z^3, z) = 0$ for all z and we get

$$0 = a \cdot 0 + b \cdot 0 + r(z)$$

for all $z \in \mathbf{R}$. Hence r is the zero polynomial. But then consider what happened at the first step of the division that produced the equation (1). Either $x = LT_>(x - z^2)$ or $y = LT_>(y - z^3)$ must have divided $LT_>(f)$, or else a nonzero term would have been placed in r.

2.5/9. The idea here is the same as in 8. The kernel of the echelon form matrix is a vector subspace V of k^n, which can be parametrized by substituting values for the "free variables" in the corresponding system of linear equations. When we take another polynomial f in the ideal $I = \langle g_1, \ldots, g_m \rangle$ generated by the linear polynomials from the rows of the matrix, it vanishes on the subspace V. So we apply the division algorithm, using any monomial order that makes the leading term of g_i equal to the term from the 1 in the leftmost nonzero position on that row. The result is

$$f = a_1 g_1 + \ldots a_m g_m + r$$

where r depends only on the free variables in the linear system. Substituting the parametrization for V shows that r must be the zero polynomial. But then $LT(f)$ is a multiple of $LT(g_i)$ for some i. Hence $\{g_1, \ldots, g_m\}$ is a Gröbner basis by the result from Problem 5.

2.5/10. We want to use the result from Problem 5 again. Let $I = \langle g \rangle$ be a principal ideal, and let G be any set containing g. We claim that G is a Gröbner basis for I. This follows from the fact that for any two polynomials g, h and any monomial order $>$:

$$LT_>(hg) = LT_>(h) LT_>(g).$$

This is a consequence of the compatibility of $>$ with multiplication in $k[x_1, \ldots, x_n]$. Proof goes like this: Let $x^\alpha = LM_>(g)$ and $x^\beta = LM_>(h)$. Every term in the product hg is $cx^\gamma x^\delta$ for some x^γ in h and some x^δ in g. But then

$$x^\gamma x^\delta \leq LT_>(h) x^\delta \leq LT_>(h) LT_>(g).$$

If $f \in I$, then $f = hg$ for some h. Hence $LT_>(f)$ is a multiple of $LT_>(g)$ by the above. Hence G is a Gröbner basis for I.