Problem Set 1 Solutions

Due: Tuesday, February 16

(1) Let $S = k[x_1, \ldots, x_n]$ where k is a field. Fix a monomial order $>_\sigma$ on $\mathbb{Z}^n_{\geq 0}$.

(a) Show that multideg(fg) = multideg(f)+ multideg(g) for non-zero polynomials $f, g \in S$.

Proof. Say multideg$(f) = \boldsymbol{\alpha}_0$ and multideg$(g) = \boldsymbol{\beta}_0$. Then we can write

$$f = a_0 \mathbf{x}^{\boldsymbol{\alpha}_0} + \sum_{\boldsymbol{\alpha} \in I} a_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}}$$
$$g = b_0 \mathbf{x}^{\boldsymbol{\beta}_0} + \sum_{\boldsymbol{\beta} \in I'} b_{\boldsymbol{\beta}} \mathbf{x}^{\boldsymbol{\beta}}$$

where I and I' are some index sets and $a_0, b_0, a_{\boldsymbol{\alpha}}, b_{\boldsymbol{\beta}}$ are in the field k. Since f and g are non-zero, we know that a_0 and b_0 are non-zero. Furthermore, by the definition of multidegree, $\boldsymbol{\alpha}_0 >_\sigma \boldsymbol{\alpha}$ and $\boldsymbol{\beta}_0 >_\sigma \boldsymbol{\beta}$ for all $\boldsymbol{\alpha} \in I$ and for all $\boldsymbol{\beta} \in I'$. We have

$$fg = a_0 b_0 \mathbf{x}^{\boldsymbol{\alpha}_0 + \boldsymbol{\beta}_0} + a_0 \sum_{\boldsymbol{\beta} \in I'} b_{\boldsymbol{\beta}} \mathbf{x}^{\boldsymbol{\alpha}_0 + \boldsymbol{\beta}} + b_0 \sum_{\boldsymbol{\alpha} \in I} a_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha} + \boldsymbol{\beta}_0} + \sum_{\boldsymbol{\alpha} \in I, \boldsymbol{\beta} \in I'} a_{\boldsymbol{\alpha}} b_{\boldsymbol{\beta}} \mathbf{x}^{\boldsymbol{\alpha} + \boldsymbol{\beta}}.$$

Since $>_\sigma$ is a monomial order, relative ordering of terms is preserved when we multiply monomials. In particular,

$$\boldsymbol{\alpha}_0 + \boldsymbol{\beta}_0 >_\sigma \boldsymbol{\alpha}_0 + \boldsymbol{\beta} >_\sigma \boldsymbol{\alpha} + \boldsymbol{\beta}$$

and

$$\boldsymbol{\alpha}_0 + \boldsymbol{\beta}_0 >_\sigma \boldsymbol{\alpha} + \boldsymbol{\beta}_0 >_\sigma \boldsymbol{\alpha} + \boldsymbol{\beta}$$

for all $\boldsymbol{\alpha} \in I$ and for all $\boldsymbol{\beta} \in I'$. Therefore, since $a_0 b_0 \neq 0$, we must have that multideg(fg) = multideg(f)+ multideg(g) □

(b) A special case of a *weight order* is constructed as follows. Fix $\mathbf{u} \in \mathbb{Z}^n_{\geq 0}$. Then, for $\boldsymbol{\alpha}, \boldsymbol{\beta}$ in $\mathbb{Z}^n_{\geq 0}$, define $\boldsymbol{\alpha} >_{\mathbf{u},\sigma} \boldsymbol{\beta}$ if and only if

$$\mathbf{u} \cdot \boldsymbol{\alpha} > \mathbf{u} \cdot \boldsymbol{\beta}, \quad \text{or} \quad \mathbf{u} \cdot \boldsymbol{\alpha} = \mathbf{u} \cdot \boldsymbol{\beta} \quad \text{and} \quad \boldsymbol{\alpha} >_\sigma \boldsymbol{\beta},$$

where $\cdot$ denotes the usual dot product of vectors. Verify that $>_{\mathbf{u},\sigma}$ is a monomial order.

Proof. We first show that $>_{\mathbf{u},\sigma}$ is a total ordering. Let $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{Z}^n_{\geq 0}$. Assume that $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$. Since $\mathbb{Z}_{\geq 0}$ is totally ordered with the usual definition of $>$, *exactly one* of the following cases must be true:

(i) $\mathbf{u} \cdot \boldsymbol{\alpha} > \mathbf{u} \cdot \boldsymbol{\beta}$
(ii) $\mathbf{u} \cdot \boldsymbol{\alpha} < \mathbf{u} \cdot \boldsymbol{\beta}$
(iii) $\mathbf{u} \cdot \boldsymbol{\alpha} = \mathbf{u} \cdot \boldsymbol{\beta}$.

By definition of $>_{\mathbf{u},\sigma}$, if case (i) holds then $\boldsymbol{\alpha} >_{\mathbf{u},\sigma} \boldsymbol{\beta}$. Similarly, if (ii) holds then $\boldsymbol{\beta} >_{\mathbf{u},\sigma} \boldsymbol{\alpha}$. In the case (iii), since $>_\sigma$ is given to be a total order, exactly one of the following cases holds: $\boldsymbol{\alpha} >_\sigma \boldsymbol{\beta}$ and so $\boldsymbol{\alpha} >_{\mathbf{u},\sigma} \boldsymbol{\beta}$; $\boldsymbol{\beta} >_\sigma \boldsymbol{\alpha}$ and so $\boldsymbol{\beta} >_{\mathbf{u},\sigma} \boldsymbol{\alpha}$; or $\boldsymbol{\alpha} =_\sigma \boldsymbol{\beta}$ and so $\boldsymbol{\alpha} =_{\mathbf{u},\sigma} \boldsymbol{\beta}$.

Therefore, exactly one of $\boldsymbol{\alpha} >_{\mathbf{u},\sigma} \boldsymbol{\beta}$ or $\boldsymbol{\beta} >_{\mathbf{u},\sigma} \boldsymbol{\alpha}$ or $\boldsymbol{\alpha} =_{\mathbf{u},\sigma} \boldsymbol{\beta}$ holds. We conclude that $>_{\mathbf{u},\sigma}$ is a total ordering.

To demonstrate the second requirement for a monomial ordering, let $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{Z}^n_{\geq 0}$ such that $\boldsymbol{\alpha} >_{\mathbf{u},\sigma} \boldsymbol{\beta}$. Let $\boldsymbol{\gamma} \in \mathbb{Z}^n_{\geq 0}$. If $\mathbf{u} \cdot \boldsymbol{\alpha} > \mathbf{u} \cdot \boldsymbol{\beta}$, then

$$\mathbf{u} \cdot (\boldsymbol{\alpha} + \boldsymbol{\gamma}) = \mathbf{u} \cdot \boldsymbol{\alpha} + \mathbf{u} \cdot \boldsymbol{\gamma} > \mathbf{u} \cdot \boldsymbol{\beta} + \mathbf{u} \cdot \boldsymbol{\gamma} = \mathbf{u} \cdot (\boldsymbol{\alpha} + \boldsymbol{\gamma})$$

which shows that $\boldsymbol{\alpha} + \boldsymbol{\gamma} >_{\mathbf{u},\sigma} \boldsymbol{\beta} + \boldsymbol{\gamma}$. In the case that $\mathbf{u} \cdot \boldsymbol{\alpha} = \mathbf{u} \cdot \boldsymbol{\beta}$, then $\boldsymbol{\alpha} >_{\sigma} \boldsymbol{\beta}$. Note that

$$\mathbf{u} \cdot (\boldsymbol{\alpha} + \boldsymbol{\gamma}) = \mathbf{u} \cdot \boldsymbol{\alpha} + \mathbf{u} \cdot \boldsymbol{\gamma} = \mathbf{u} \cdot \boldsymbol{\beta} + \mathbf{u} \cdot \boldsymbol{\gamma} = \mathbf{u} \cdot (\boldsymbol{\alpha} + \boldsymbol{\gamma}).$$

However, since $>_{\sigma}$ is a monomial ordering, we must have $\boldsymbol{\alpha} + \boldsymbol{\gamma} >_{\sigma} \boldsymbol{\beta} + \boldsymbol{\gamma}$. Thus again, $\boldsymbol{\alpha} + \boldsymbol{\gamma} >_{\mathbf{u},\sigma} \boldsymbol{\beta} + \boldsymbol{\gamma}$.

Finally, to show that $>_{\mathbf{u},\sigma}$ is a well-ordering, we apply the Corollary to Dickson's Lemma and verify that $\boldsymbol{\alpha} \geq_{\mathbf{u},\sigma} \mathbf{0}$ for all $\boldsymbol{\alpha} \in \mathbb{Z}^n_{\geq 0}$. Since $\boldsymbol{\alpha} \in \mathbb{Z}^n_{\geq 0}$, it is true that $\mathbf{u} \cdot \boldsymbol{\alpha} \geq 0 = \mathbf{u} \cdot \mathbf{0}$. If $\mathbf{u} \cdot \boldsymbol{\alpha} > 0$ then we are done. If the dot product is zero, then we must have $\boldsymbol{\alpha} \geq_{\sigma} \mathbf{0}$ since $>_{\sigma}$ is a well-ordering itself and so $\boldsymbol{\alpha} \geq_{\mathbf{u},\sigma} \mathbf{0}$ yet again. □

(c) A particular example of a weight order is the *elimination order* which was introduced by Bayer and Stillman. Fix an integer $1 \leq i \leq n$ and let $\mathbf{u} = (1, \ldots, 1, 0, \ldots, 0)$, where there are i 1's and $n - i$ 0's. Then the *ith elimination order* $>_i$ is the weight order $>_{\mathbf{u},grevlex}$. Prove that $>_i$ has the following property: if $\mathbf{x}^{\boldsymbol{\alpha}}$ is a monomial in which one of $x_1, \ldots, x_i$ appears, then $\mathbf{x}^{\boldsymbol{\alpha}} >_i \mathbf{x}^{\boldsymbol{\beta}}$ for *any* monomial $\mathbf{x}^{\boldsymbol{\beta}}$ involving only $x_{i+1}, \ldots, x_n$. Does this property hold for the graded reverse lexicographic order?

Solution: We first prove the desired result and then compare the elimination order with the graded reverse lexicographic order.

Proof. By the definitions of $\mathbf{u}, \mathbf{x}^{\boldsymbol{\alpha}}$ and $\mathbf{x}^{\boldsymbol{\beta}}$, it is clear that $\mathbf{u} \cdot \boldsymbol{\alpha} > 0$ yet $\mathbf{u} \cdot \boldsymbol{\beta} = 0$. Thus, by definition, $\mathbf{x}^{\boldsymbol{\alpha}} >_i \mathbf{x}^{\boldsymbol{\beta}}$. □

This property does not hold for the graded reverse lexicographic order. For example, let $i = 1$ and $S = k[x_1, x_2]$ where $x_1 >_{grevlex} x_2$. Then $x_2^3 >_{grevlex} x_1$.

(2) Let I be a non-zero ideal in $k[x_1, \ldots, x_n]$. Let $G = \{g_1, \ldots, g_t\}$ and $F = \{f_1, \ldots, f_r\}$ be two minimal Gröbner bases for I with respect to some fixed monomial order. Show that $\{LT(g_1), \ldots, LT(g_t)\} = \{LT(f_1), \ldots, LT(f_r)\}$.

Proof. Since both F and G are minimal Gröbner bases for I, we have that the leading coefficient of each f_i and g_j must equal 1. Consider f_1. Since G is a Gröbner basis for I and $f_1 \in I$, there is some g_i such that $LT(g_i)$ divides $LT(f_1)$. Renumber if necessary so that $i = 1$. Then, since $g_1 \in I$ and F is a Gröbner basis for I, there must exist some f_j such that $LT(f_j)$ divides $LT(g_1)$. We conclude that $LT(f_j)$ divides $LT(f_1)$. But, since F is given to be minimal, $LT(f_1)$ is not in the ideal generated by the leading terms in $F - \{f_1\}$. We conclude that $j = 1$ and so $LT(f_1) = LT(g_1)$. We repeat this argument starting with f_2. We again have that there exists some g_l such that $LT(g_l)$ divides $LT(f_2)$. Since F is a minimal Gröbner basis and $LT(f_1) = LT(g_1)$, we know that $l \neq 1$. We may relabel, if necessary, to assume that $l = 2$. Arguing as above yields $LT(f_2) = LT(g_2)$. Continuing in this fashion, we see that this procedure must stop at which point $t = r$ and, after relabeling, $LT(f_i) = LT(g_i)$ for $i = 1, \ldots, t$. □

(3) Suppose that $I = (g_1, \dots, g_t)$ is a non-zero ideal of $k[x_1, \dots, x_n]$ and fix a monomial order on $\mathbb{Z}^n_{\geq 0}$. Suppose that for all f in I we obtain a zero remainder upon dividing f by $G = \{g_1, \dots, g_t\}$ using the Division Algorithm. Prove that G is a Gröbner basis for I. (We showed the converse of this statement in class.)

Solution: Below are two possible proofs for this exercise.

Proof. We argue by contradiction and suppose that G is not a Gröbner basis for I. Clearly, $(\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t)) \subseteq \mathrm{in}(I)$. Thus, we must have $\mathrm{in}(I) \nsubseteq (\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t))$. Let $f \in I$ be a non-zero polynomial such that $\mathrm{LT}(f) \notin (\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t))$. Apply the Division Algorithm to divide f by G. Then, since $\mathrm{LT}(f)$ is not divisible by $\mathrm{LT}(g_i)$ for any i, the first step of the algorithm yields that $\mathrm{LT}(f)$ is added to the remainder column. This is a contradiction to the hypothesis that when we divide f by G we obtain a zero remainder. Therefore, G must be a Gröbner basis for I. $\square$

Proof. We saw in class that G is a Gröbner basis if and only if for all pairs $i \neq j$, the remainder on division of the S-polynomial $S(g_i, g_j)$ is zero. By definition,

$$S(g_i, g_j) = \frac{\mathrm{LCM}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))}{\mathrm{LT}(g_i)} g_i - \frac{\mathrm{LCM}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))}{\mathrm{LT}(g_j)} g_j.$$

Since $I = (g_1, \dots, g_t)$, we see that each S-polynomial $S(g_i, g_j)$ is in I. Thus, by assumption, when we divide $S(g_i, g_j)$ by G we obtain a zero remainder. We conclude that G is a Gröbner basis for I. $\square$

(4) Consider the ideal $I = (xy + z - xz, x^2 - z) \subset k[x, y, z]$. For what follows, use the graded reverse lexicographic order with $x > y > z$. You are not permitted to use a computer algebra system for this exercise. Be sure to show all of your work.

(a) Apply Buchberger's Algorithm to find a Gröbner basis for I. Is the result a reduced Gröbner basis for I?

Solution: Start by letting $g_1 = xy - xz + z$, $g_2 = x^2 - z$ and $G = \{g_1, g_2\}$. Then

$$S(g_1, g_2) = \frac{x^2 y}{xy} g_1 - \frac{x^2 y}{x^2} g_2 = -x^2 z + xz + yz.$$

Applying the Division Algorithm to divide $S(g_1, g_2)$ by G yields

$$S(g_1, g_2) = -z g_2 + xz + yz - z^2.$$

We let $g_3 = xz + yz - z^2$ (the remainder from dividing $S(g_1, g_2)$ by G) and append this to G. Thus, $G = \{g_1, g_2, g_3\}$. We then calculate

$$S(g_1, g_3) = \frac{xyz}{xy} g_1 - \frac{xyz}{xz} g_3 = -y^2 z - xz^2 + yz^2 + z^2.$$

Applying the Division Algorithm to divide $S(g_1, g_3)$ by G yields

$$S(g_1, g_3) = -z g_3 - y^2 z + 2yz^2 - z^3 + z^2.$$

We let $g_4 = -y^2 z + 2yz^2 - z^3 + z^2$ (the remainder from dividing $S(g_1, g_3)$ by G) and append this to G. Thus, $G = \{g_1, g_2, g_3, g_4\}$. We show that G is a Gröbner basis for I

by demonstrating that $S(g_1, g_4), S(g_2, g_3), S(g_2, g_4)$ and $S(g_3, g_4)$ have zero remainders when divided by G. The end results are:

$$\begin{aligned}
S(g_1, g_4) &= \frac{xy^2z}{xy}g_1 - \frac{xy^2z}{-y^2z}g_4 = xyz^2 - xz^3 + xz^2 + yz^2 \\
&= z^2g_1 + zg_3 \\
S(g_2, g_3) &= \frac{x^2z}{x^2}g_2 - \frac{x^2z}{xz}g_3 = -xyz + xz^2 - z^2 \\
&= -zg_1 \\
S(g_2, g_4) &= \frac{x^2y^2z}{x^2}g_2 - \frac{x^2y^2z}{-y^2z}g_4 = 2x^2yz^2 - x^2z^3 + x^2z^2 - y^2z^2 \\
&= 2xz^2g_1 + (z^3 + z^2)g_2 - 2z^2g_3 + zg_4 \\
S(g_3, g_4) &= \frac{xy^2z}{xz}g_3 - \frac{xy^2z}{-y^2z}g_4 = y^3z + 2xyz^2 - y^2z^2 - xz^3 + xz^2 \\
&= 2z^2g_1 + (z^2 + z)g_3 - (y + z)g_4.
\end{aligned}$$

Note that G is *not* a reduced Gröbner basis for I. For example, the monomial $-xz$ is a term of g_1 and $LT(g_3) = xz$. So, $-xz$ is in the ideal generated by the leading terms in $G - \{g_1\}$.

(b) Use your answer from part (a) to determine if $f = xy^3z - z^3 + xy$ is in I.

Solution: Dividing f by the Gröbner basis G found in part (a) yields

$$f = (y^2z + yz^2 + z^3 + 1)g_1 + (z^3 + 1)g_3 + zg_4 + (-yz^4 + z^5 - 3yz^3 - 2z^3 - yz + z^2 - z).$$

Since the remainder $r = -yz^4 + z^5 - 3yz^3 - 2z^3 - yz + z^2 - z$ is non-zero, f is not in the ideal I.

(5) Consider the affine variety $V = \mathbf{V}(x^2+y^2+z^2-4, x^2+2y^2-5, xz-1)$ in $\mathbb{C}^3$. Use a computer algebra system and Gröbner bases to find all the points of V.

Solution: Let $I = (x^2 + y^2 + z^2 - 4, x^2 + 2y^2 - 5, xz - 1) \subset \mathbb{C}[x, y, z]$. Using CoCoA and working with lexicographic order with $x >_{lex} y >_{lex} z$, we find that a Gröbner basis for I is $G = \{g_1, g_2, g_3\}$ where

$$\begin{aligned}
g_1 &= y^2 - z^2 - 1 \\
g_2 &= -x - 2z^3 + 3z \\
g_3 &= -2z^4 + 3z^2 - 1
\end{aligned}$$

Thus $V = \mathbf{V}(g_1, g_2, g_3)$. Note that g_3 depends on z alone. Using the quadratic formula we see that

$$g_3 = 0 \iff z = -1, 1, \frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}.$$

Setting $z = 1$, we see that

$$g_2 = 0 \iff x = 1$$

and

$$g_1 = 0 \iff y = -\sqrt{2}, \sqrt{2}.$$

Setting $z = -1$, we see that

$$g_2 = 0 \iff x = -1$$

and

$$g_1 = 0 \iff y = -\sqrt{2}, \sqrt{2}.$$

Setting $z = \dfrac{1}{\sqrt{2}}$, we see that

$$g_2 = 0 \iff x = \sqrt{2}$$

and

$$g_1 = 0 \iff y = \sqrt{\frac{3}{2}}, -\sqrt{\frac{3}{2}}.$$

Setting $z = \dfrac{-1}{\sqrt{2}}$, we see that

$$g_2 = 0 \iff x = -\sqrt{2}$$

and

$$g_1 = 0 \iff y = \sqrt{\frac{3}{2}}, -\sqrt{\frac{3}{2}}.$$

Therefore,

$$V = \left\{(1, \pm\sqrt{2}, 1), (-1, \pm\sqrt{2}, -1), \left(\sqrt{2}, \pm\sqrt{\frac{3}{2}}, \frac{1}{\sqrt{2}}\right), \left(-\sqrt{2}, \pm\sqrt{\frac{3}{2}}, \frac{-1}{\sqrt{2}}\right)\right\}.$$