MAS400: Solutions 6

Throughout this sheet F will denote an arbitrary field unless otherwise stated.

1. Show that for a given monomial order $\leqslant$ on $R \leqslant F[x_1, \ldots, x_n]$ the reduced Gröbner basis of any ideal $I \leqslant R$ is unique with respect to $\leqslant$. (The reduced Gröbner basis of I can depend on the monomial order chosen.)

   Let $G = \{g_1, \ldots, g_s\}$ be a reduced Gröbner basis for I. Then $\operatorname{lt} g_i \neq \operatorname{lt} g_j$ whenever $i \neq j$ (by the definition of a reduced Gröbner basis), and also $\operatorname{lt} g_i \mid \operatorname{lt} g_j$ whenever $i \neq j$. So order G so that $\operatorname{lt} g_1 < \operatorname{lt} g_2 < \cdots < \operatorname{lt} g_s$. Now let $J := \langle \operatorname{lt} G \rangle = \langle \operatorname{lt} I \rangle$, so that J is a monomial ideal. By Lemma D, if f is a monomial in J then $\operatorname{lt} g_i \mid f$ for some i. Thus for all k, $\operatorname{lt} g_k \notin \langle \operatorname{lt} g_1, \ldots, \operatorname{lt} g_{k-1} \rangle$. Let m_1 be the minimum monomial in J. Then $\operatorname{lt} g_i \mid m_1$ for some i, and thus $\operatorname{lt} g_1 \leqslant \operatorname{lt} g_i \leqslant m_1$. But $\operatorname{lt} g_k \in J$ for all k and so $m_1 \leqslant \operatorname{lt} g_1$, and thus $\operatorname{lt} g_1 = m_1$ (and $i = 1$). Now define m_2 to be the least monomial in J not belonging to $\langle m_1 \rangle$, and for all k let m_k be the least monomial in J not belonging to $\langle m_1, \ldots, m_{k-1} \rangle$ (if such exists). Evidently $\operatorname{lt} g_2 \in J \setminus \langle m_1 \rangle$ and so $m_2 \leqslant \operatorname{lt} g_2$. Since m_2 is divisible by some $\operatorname{lt} g_i$ for $i \neq 1$ we get $\operatorname{lt} g_2 \leqslant \operatorname{lt} g_i \leqslant m_2$ and so $m_2 = \operatorname{lt} g_2$. Similarly, using induction, we get that $m_k = \operatorname{lt} g_k$ for all k. (Note that m_i will be defined for $1 \leqslant i \leqslant s$, but that m_{s+1} will not be since $J = \langle \operatorname{lt} G \rangle$.) Therefore $\operatorname{lt} G$ is uniquely determined, even as a multiset.

   Let $G' = \{h_1, \ldots, h_s\}$ be 'another' reduced Gröbner basis for I where $\operatorname{lt} g_i = \operatorname{lt} h_i$ for all i. The terms of $g_i - h_i$ are not divisible by any of the $\operatorname{lt} g_j$ (resp. $\operatorname{lt} h_j$). (The only terms of g_i or h_i divisible by any $\operatorname{lt} g_j$ or $\operatorname{lt} h_j$ is $\operatorname{lt} g_i = \operatorname{lt} h_i$, in the case $i = j$.)

2. Find an algorithm for reducing a Gröbner basis (for an ideal I of $F = [x_1, \ldots, x_n]$ w.r.t. some monomial order $\leqslant$) to a reduced Gröbner basis. Write the algorithm in pseudo-code.

   Given a Gröbner basis $G = \{g_1, \ldots, g_m\}$ of I we first perform the obvious first steps:

   - Replace g_i by $g_i / \operatorname{lc} g_i$ for all i.
   - Order G so that $\operatorname{lt} g_1 \leqslant \operatorname{lt} g_2 \leqslant \cdots \leqslant \operatorname{lt} g_m$.
   - For $1 \leqslant j \leqslant m$ if there is $i < j$ such that $\operatorname{lt} g_i \mid \operatorname{lt} g_j$ then remove g_j (there will always be an 'unremovable' g_i with this property, for g_i is removed only if $\operatorname{lt} g_k \mid \operatorname{lt} g_i$ for some $k < i$, but then $\operatorname{lt} g_k \mid \operatorname{lt} g_j$).

So now we have a Gröbner basis $G = \{g_1, \ldots, g_m\}$ such that $\operatorname{lt} g_1 < \operatorname{lt} g_2 < \cdots < \operatorname{lt} g_m$ and $\operatorname{lc} g_i = 1$ for all i. Evidently $\operatorname{lt} g_j$ does not divide any term of g_i whenever $i < j$. We now produce a reduced Gröbner basis $G = \{g'_1, \ldots, g'_m\}$ for I, where $\operatorname{lt} g_i = \operatorname{lt} g'_i$ for all i. This is done recursively as follows. Let $g'_1 = g_1$. Initially, we assign $g'_2 = g_2$. Now let t be the largest term of g'_2 divisible by $\operatorname{lt} g_1$ and define (new) $g'_2 := g'_2 - (t/\operatorname{lt} g_1)g_1$, and continue until no such term exists. This does not alter $\operatorname{lt} g_i$ for any i. Similarly once we have assigned $g'_1, \ldots, g'_{k-1}$ we initially let $g'_k = g_k$, and let t be the largest term of g'_k divisible by a $\operatorname{lt} g_i$ (where necessarily $i < k$) and define (new) $g'_k := g'_k - (t/\operatorname{lt} g_i)g_i$, and continue until no such term exists. (I'll leave it to you to show that this process terminates for each k.) The final $\{g'_1, \ldots, g'_m\}$ is a reduced Gröbner basis for I.)

Pseudo-code is given on a separate sheet. (The reduced Gröbner bases given below satisfy $\operatorname{lt} g_1 > \operatorname{lt} g_2 > \cdots$.)

3. Let G be a Gröbner basis for the non-zero ideal $I \leqslant F[x]$. Show that there exists $f \in F[x]$ such that $f \in G$ and $I = \langle f \rangle$.

If $f \neq 0$ then $\operatorname{lt} f \in \{1, x, x^2, \ldots\}$, and if $g \in I \setminus \{0\}$ and $\operatorname{lt} g = x^i$ then for all $j \geqslant 0$ we have $gx^j \in I$ and $\operatorname{lt}(gx^j) = x^{i+j}$. Therefore $\langle \operatorname{lt} G \rangle = \langle \operatorname{lt} I \rangle = \{x^m, x^{m+1}, x^{m+2}, \ldots\}$ for some $m \in \mathbb{N}$. So pick $g \in G$ such that $\operatorname{lt} g = x^m$, so that $\langle \operatorname{lt} G \rangle = \langle \operatorname{lt} g \rangle$, and so $\{g\}$ is a Gröbner basis for I, in particular $I = \langle g \rangle$ and $\{g\} \subseteq G$. (The reader may like to ponder the proof where I showed that all non-zero ideals I of $F[x]$ are generated by any element $g \in I$ where $\deg g$ is minimal among non-zero elements of I.)

4. Use elimination ideals to determine the following affine varieties.

(a) $\mathbb{V}(xy - 1, y^2 - 1) \subseteq \mathbb{C}^2$.
(b) $\mathbb{V}(xy - 1, xz - 1) \subseteq \mathbb{C}^3$.
(c) $\mathbb{V}(xy - 1, yz - 1, zx - 1) \subseteq \mathbb{C}^3$.
(d) $\mathbb{V}(xy^2 - 1, xz^2 - 1) \subseteq \mathbb{C}^3$.
(e) $\mathbb{V}(x^2y - 1, x^2z - 1) \subseteq \mathbb{C}^3$.
(f) $\mathbb{V}(x^2y - 1, y^2z - 1, z^2x - 1) \subseteq \mathbb{C}^3$.
(g) $\mathbb{V}(x^3y - 1, xy^3 - 1) \subseteq \mathbb{C}^2$.

Recall that $\leqslant_{\mathrm{lex}}$ (with $x > y > z$) is a j-elimination order for all relevant j. Except for the last one we calculated reduced Gröbner bases of the corresponding ideals in $\mathbb{Q}[x,y]$ or $\mathbb{Q}[x,y,z]$ w.r.t. $\leqslant_{\text{lex}}$ with $x > y > z$ on the last exercise sheet. Answers are as follows.

(a) $\{x-y, y^2-1\}$.

(b) $\{xz-1, y-z\}$.

(c) $\{x-z, y-z, z^2-1\}$.

(d) $\{xz^2-1, y^2-z^2\}$.

(e) $\{x^2z-1, y-z\}$.

(f) $\{x-z^7, y-z^4, z^9-1\}$.

(g) $\{x-y^5, y^8-1\}$.

It was remarked in lectures that calculations for things like Multivariate Division and Gröbner Basis are unaltered when passing to field extensions. So the above are also reduced Gröbner bases for the appropriate ideals of $\mathbb{C}[x,y]$ or $\mathbb{C}[x,y,z]$ (depending on case). (The affine varieties will vary subtlely on field extension.) Using the notation $\mathbb{C}^\times := \mathbb{C}\setminus\{0\}$, $\zeta = \exp(2\pi\mathrm{i}/9)$, $\omega = \exp(2\pi\mathrm{i}/8)$ the solutions are as follows.

(a) $\mathbb{V}(xy-1, y^2-1) = \{\,(a,a) : a \in \{1,-1\}\,\}$.

(b) $\mathbb{V}(xy-1, xz-1) = \{\,(a^{-1},a,a) : a \in \mathbb{C}^\times\,\}$.

(c) $\mathbb{V}(xy-1, yz-1, zx-1) = \{\,(a,a,a) : a \in \{1,-1\}\,\}$.

(d) $\mathbb{V}(xy^2-1, xz^2-1) = \{\,(a^{-2},\pm a,a) : a \in \mathbb{C}^\times\,\}$.

(e) $\mathbb{V}(x^2y-1, x^2z-1) = \{\,(\pm/\sqrt{a^{-1}},a,a) : a \in \mathbb{C}^\times\,\} = \{\,(a,a^{-2},a^{-2}) : a \in \mathbb{C}^\times\,\}$.

(f) $\mathbb{V}(x^2y-1, y^2z-1, z^2x-1) = \{\,(a^7,a^4,a) : a \in \{1,\zeta,\zeta^2,\zeta^3,\zeta^4,\zeta^5,\zeta^6,\zeta^7,\zeta^8\}\,\}$.

(g) $\mathbb{V}(x^3y-1, xy^3-1) = \{\,(a^5,a) : a \in \{1,\omega,\omega^2,\omega^3,\omega^4,\omega^5,\omega^6,\omega^7\}\,\}$.

We did Part (b) in lectures. We'll do Part (d) as a sample solution. Here we have $G_2 = G \cup \mathbb{C}[z] = \varnothing$, $G_1 = G \cup \mathbb{C}[y,z] = \{y^2-z^2\}$ and $G_2 = G \cup \mathbb{C}[x,y,z] = G = \{xz^2-1, y^2-z^2\}$. Thus $I_2 = 0 \subseteq \mathbb{C}[z]$, $I_1 = \langle y^2-z^2\rangle \subseteq \mathbb{C}[y,z]$ and $I_0 = I = \langle xz^2-1, y^2-z^2\rangle \subseteq \mathbb{C}[x,y,z]$. Therefore $\mathbb{V}I_2 = \{\,(a) : a \in \mathbb{C}\,\}$. Fix $a \in \mathbb{C}$. We get

$$\{\,b : b \in \mathbb{C} \mid (b,a) \in \mathbb{V}I_1\,\} = \mathbb{V}(y^2-a^2) = \{a,-a\}$$

and so $\mathbb{V}I_1 = \{\, (\pm a, a) : a \in \mathbb{C} \,\}$. Fix $a \in \mathbb{C}$ and $\varepsilon \in \{1, -1\}$. Then

$$\{\, b : b \in \mathbb{C} \mid (b, \varepsilon a, a) \in \mathbb{V}I_0 \,\} = \mathbb{V}(xa^2 - 1, (\varepsilon a)^2 - a^2) = \mathbb{V}(xa^2 - 1).$$

If $a = 0$ we get $\mathbb{V}(xa^2-1) = \varnothing$, otherwise $\mathbb{V}(xa^2-1) = a^{-2}$. Therefore $\mathbb{V}I = \mathbb{V}I_0 = \{\, (a^{-2}, \pm a, a) : a \in \mathbb{C}^\times \,\}$.

It should be noted that these particular examples are more easily solved not using Gröbner bases and elimination ideals. In this question, we are being asked to solve systems of equations of the form $x^i y^j z^k = 1$, $i, j, k \in \mathbb{N}$, where in each case, and for each relevant variable, there is at least one equation involving that variable. Moreover, generally there are enough equations involving a variable to allow substitution to take place. For example in Part (f) we are trying to solve $x^2y - 1 = y^2z - 1 = z^2x - 1$ or $x^2y = y^2z = z^2x = 1$, whence $0 \notin \{x, y, z\}$. Now $z^2x = 1$ gives $x = z^{-2}$, whence we obtain the system of equations $z^{-4}y = y^2z = 1$. Thus $y = z^4$ and $y^2z = 1$ gives $z^9 = 1$. So we get the same answer as above.

For the system of equations $x^my - 1 = xy^m - 1 = 0$ for $m \geqslant 2$ (generalisation of Part (g)) the equation $xy^m - 1 = 0$ gives $y \neq 0$ and $x = y^{-m}$, and substituting into $x^my - 1 = 0$ gives $y^{-m^2}y - 1 = 0$, or $y^{m^2-1} = 1$. So $(x, y) = (\lambda^{-mi}, \lambda^i)$ for some $i \in \{0, \ldots, m^2-2\}$ where $\lambda = \exp(2\pi \mathrm{i}/(m^2-1))$. (I'll leave it is an exercise for you to see this works.) Therefore

$$\mathbb{V}(x^my - 1, xy^m - 1) = \{\, (\lambda^{-mi}, \lambda^i) : 0 \leqslant i \leqslant m^2 - 2 \ (i \in \mathbb{Z}) \,\} \subseteq \mathbb{C}.$$

Note that if $m \geqslant 2$ then the reduced Gröbner basis for $\langle x^my - 1, xy^m - 1\rangle$ is $\{x - y^{m^2-m-1}, y^{m^2-1}\}$. Exceptional behaviour occurs when $m = 1$ (or -1).