M3P23, M4P23, M5P23: COMPUTATIONAL ALGEBRA & GEOMETRY
EXAM SOLUTIONS 2014

(1) (i) Let $G = \{g_1, \ldots, g_m\}$ be a set of generators for the ideal $I \subset k[x_1, \ldots, x_n]$, and fix a monomial order. Then G is a *Gröbner basis* for I if

$$(\mathrm{LT}(I)) = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m)).$$

Buchberger's Criterion states that G is a Gröbner basis if and only if the remainder $\overline{S(g_i, g_j)}^G$ is zero for all $i \neq j$.

(ii) We split the calculation up into four cases.

$a \neq 0, b \neq 0$: The S-polynomial is $S(-ax^2 + y, -by^3 + z) = \frac{x^2z}{b} - \frac{y^4}{a}$. The remainder upon division by $\{y - ax^2, z - by^3\}$ is 0, hence this is a Gröbner basis.

$a = 0, b \neq 0$: The S-polynomial is $S(y, -by^3 + z) = \frac{z}{b}$. The remainder is $\frac{z}{b}$, hence this is not a Gröbner basis.

$a \neq 0, b = 0$: The S-polynomial is $S(-ax^2 + y, z) = -\frac{yz}{a}$. The remainder is 0, hence this is a Gröbner basis.

$a = 0, b = 0$: The S-polynomial is $S(y, z) = 0$, so this is a Gröbner basis.

Thus $\{y - ax^2, z - by^3\}$ is a Gröbner basis for all values a, b except when $a = 0, b \neq 0$.

(iii) A Gröbner basis G is said to be *reduced* if, for all $g \in G$, $\mathrm{LC}(g) = 1$ and no monomial of g lies in $(\mathrm{LT}(G \setminus \{g\}))$.

Using our results in (ii) we know that the set is a Gröbner basis in all cases except when $a = 0, b \neq 0$, which is easy enough to fix. We have the reduced Gröbner bases:

$\{x - y/a, y^3 - z/b\}$	when $a \neq 0, b \neq 0$;
$\{y, z\}$	when $a = 0, b \neq 0$;
$\{x - y/a, z\}$	when $a \neq 0, b = 0$;
$\{y, z\}$	when $a = 0, b = 0$.

(iv) For a given monomial order, the reduced Gröbner basis is unique. Thus we make use of our results in (iii) and see that the two ideals are equal iff $a_1 = a_2$ and $b_1 = b_2$, or $a_1 = a_2 = 0$ and b_1, b_2 free.

(2) (i) (a) Let $f, g \in I_l$. Then $f, g \in I$ and $f, g \in \mathbb{C}[x_{l+1}, \ldots, x_n]$. Hence $f + g \in I$ and $f + g \in \mathbb{C}[x_{l+1}, \ldots, x_n]$, and so $f + g \in I_l$. Now suppose that $f \in I_l$, $g \in \mathbb{C}[x_{l+1}, \ldots, x_n]$. Then $f \in I$ and $g \in \mathbb{C}[x_1, \ldots, x_n]$, hence $gf \in I$. Since $f \in \mathbb{C}[x_{l+1}, \ldots, x_n]$ we have $gf \in \mathbb{C}[x_{l+1}, \ldots, x_n]$, and so $gf \in I_l$.

a.m.kasprzyk@imperial.ac.uk

http://magma.maths.usyd.edu.au/∼kasprzyk/.

(b)

$$\begin{aligned} f \in I_{l+1} &\iff f \in I \cap \mathbb{C}[x_{l+2}, \ldots, x_n] \\ &\iff f \in (I \cap \mathbb{C}[x_{l+1}, x_{l+2}, \ldots, x_n]) \cap \mathbb{C}[x_{l+2}, \ldots, x_n] \\ &\iff f \in I_l \cap \mathbb{C}[x_{l+2}, \ldots, x_n] \end{aligned}$$

(ii) Extension Theorem: Let $I = (f_1, \ldots, f_s) \subset \mathbb{C}[x_1, \ldots, x_n]$ be an ideal. For each $1 \leq i \leq s$, write f_i in the form

$$f_i = g_i(x_2, \ldots, x_n)x_1^{N_i} + \text{terms in which } x_1 \text{ has degree} < N_i,$$

where $N_i \geq 0$ and $g_i \in \mathbb{C}[x_2, \ldots, x_n]$ is non-zero. Let $(a_2, \ldots, a_n) \in \mathbb{V}(I_1)$ be a partial solution. If $(a_2, \ldots, a_n) \notin \mathbb{V}(g_1, \ldots, g_s)$ then there exists $a_1 \in \mathbb{C}$ such that $(a_1, a_2, \ldots, a_n) \in \mathbb{V}(I)$.

The result follows immediately from the Extension Theorem: Since $g_i = c \neq 0$ implies $\mathbb{V}(g_1, \ldots, g_s) = \emptyset$, we have $(a_2, \ldots, a_n) \notin \mathbb{V}(g_1, \ldots, g_s)$ for all partial solutions.

(iii) Let $G = \{x^2 - xz + 1, y - z^2 + 1\}$ be the lex-ordered Gröbner basis. The Elimination Theorem tells us that $G \cap \mathbb{C}[y, z] = \{y - z^2 + 1\}$ is a Gröbner basis for I_1, and $G \cap \mathbb{C}[z] = \varnothing$ is a Gröbner basis for I_2. Hence $\mathbb{V}(I_2) = \mathbb{C}$ and every partial solution can be extended via a trivial application of (ii). Continuing, we have $\mathbb{V}(I_1) = \{(t^2 - 2, t) \mid t \in \mathbb{C}\}$, and once more (ii) tells us that every partial solution can be extended. Finally, we have that

$$\begin{aligned} \mathbb{V}(I) = &\left\{\left(\frac{t}{2} + \frac{1}{2}\sqrt{t^2 - 4}, t^2 - 2, t\right) \mid t \in \mathbb{C}\right\} \cup \\ &\qquad\left\{\left(\frac{t}{2} - \frac{1}{2}\sqrt{t^2 - 4}, t^2 - 2, t\right) \mid t \in \mathbb{C}\right\} \end{aligned}$$

is the set of solutions to the system of equations.

Since any paramaterisable variety is irreducible, we see that $\mathbb{V}(I)$ has two components.

(3) (i) $\mathbb{V}(I) := \{(a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}$.

Let $(a_1, \ldots, a_n) \in \mathbb{V}(I_2)$. Then $f(a_1, \ldots, a_n) = 0$ for all $f \in I_2$. But $I_1 \subseteq I_2$ by assumption, hence $f(a_1, \ldots, a_n) = 0$ for all $f \in I_1$, and so $(a_1, \ldots, a_n) \in \mathbb{V}(I_1)$.

(ii) Let $I_1 = (y - x^2, z - x^3)$ and $I_2 = ((y - x^2)^2 + (z - x^3)^2)$. Since $I_2 \subset I_1$, we have that $\mathbb{V}(I_1) \subset \mathbb{V}(I_2)$. Conversely let $(a, b, c) \in \mathbb{V}(I_2) \subset \mathbb{R}^3$, so that $(b - a^2)^2 + (c - a^3)^2 = 0$. The only possibility is that both $b - a^2 = 0$ and $c - a^3 = 0$ (since we're working over $\mathbb{R}$), hence $(a, b, c) \in \mathbb{V}(I_1)$. Hence $\mathbb{V}(I_1) = \mathbb{V}(I_2)$.

(iii) Let $I = (f_1, \ldots, f_m) \subset \mathbb{R}[x_1, \ldots, x_n]$ be an ideal, and set

$$g = f_1^2 + \ldots + f_m^2.$$

The ideal $I' = (g)$ is contained in I, and so $\mathbb{V}(I) \subset \mathbb{V}(I')$. Conversely let $(a_1, \ldots, a_n) \in \mathbb{V}(I')$, so that

$$f_1(a_1, \ldots, a_n)^2 + \ldots + f_m(a_1, \ldots, a_n)^2 = 0.$$

Since we're working over $\mathbb{R}$, it much be that $f_i(a_1, \ldots, a_n) = 0$ for each $1 \leq i \leq m$. Hence $(a_1, \ldots, a_n) \in \mathbb{V}(I)$ and so $\mathbb{V}(I') \subset \mathbb{V}(I)$. We conclude that $\mathbb{V}(I) = \mathbb{V}(I')$, as required.

(iv) If $\mathbb{V}(f_1, \ldots, f_s) = \mathbb{V}(g)$ then $\sqrt{(f_1, \ldots, f_s)} = \sqrt{(g)}$ by the Nullstellensatz. Consider the radical ideal (x, y), and suppose that $(x, y) = \sqrt{(g)}$ for some $g \in \mathbb{C}[x, y]$. Then $x^n = hg$ for some $n \in \mathbb{Z}_{>0}$ and $h \in \mathbb{C}[x, y]$, and we see that g is a power of x. Similarly $y^m = h'g$, and so g is a power of y. Hence $g \in \mathbb{C}$, which is a contradiction.

(4) (i) Given an ideal $I \subset k[x_1, \ldots, x_n]$ we define

$$\sqrt{I} := \{f \in k[x_1, \ldots, x_n] \mid f^m \in I \text{ for some } m > 0\}.$$

Let $I \subset \mathbb{C}[x_1, \ldots, x_n]$ be an ideal. Then $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$.

(ii) Let $I = \left(x^2 - x - 2, x(y^2 - 1)\right) \subset \mathbb{C}[x, y]$. We see that $\mathbb{V}(I) = \mathbb{V}(x^2 - x - 2) \cap \mathbb{V}(x(y^2 - 1)) \subset \mathbb{C}^2$. Now $\mathbb{V}(x^2 - x - 2) = \mathbb{V}(x - 2) \cup \mathbb{V}(x + 1)$ is given by the union of the two lines $x = 2$ and $x = -1$. $\mathbb{V}(x(y^2 - 1)) = \mathbb{V}(x) \cup \mathbb{V}(y - 1) \cup \mathbb{V}(y + 1)$ is the union of the three lines $x = 0$ and $y = \pm 1$. Hence $\mathbb{V}(I)$ equals the four points $\{(-1, \pm 1), (2, \pm 1)\}$. The Nullstellensatz tells us that

$$\sqrt{I} = \mathbb{I}(\mathbb{V}(I)) = \left((x + 1)(x - 2), y^2 - 1\right).$$

That $y^2 - 1 \in \sqrt{I}$ is immediate.

(iii) If $f \in \sqrt{\cap_i I_i}$ then $f^m \in \cap_i I_i$ for some integer $m > 0$. Since $f^m \in I_i$, we have that $f \in \sqrt{I_i}$. Hence $f \in \cap_i \sqrt{I_i}$.
Conversely let $f \in \cap_i \sqrt{I_i}$. Then, for each $i \in \Gamma$, there exist $m_i > 0$ such that $f^{m_i} \in I_i$. Let $m := \max\{m_i \mid i \in \Gamma\}$. Then $f^m \in I_i$ for all $i \in \Gamma$, and hence $f \in \sqrt{\cap_i I_i}$.

(iv) Notice that

$$(f) = \bigcap_{i=1}^{d} \left((x - a_i)^{r_i}\right).$$

Since $\sqrt{((x - a_i)^{r_i})} = (x - a_i)$, the result follows immediately from (iii).

(5) **Mastery Question.**

(i) Let $g_1, g_2 \in I : (f^\infty)$. Then there exists $m_1, m_2 \in \mathbb{Z}_{>0}$ such that $f^{m_1} g_1 \in I$ and $f^{m_2} g_2 \in I$. Setting $m := \max\{m_1, m_2\}$ we see that $f^{2m} g_1 g_2 = f^m g_1 \cdot f^m g_2 \in I$, and so $g_1 g_2 \in I : (f^\infty)$. Now let $g \in I : (f^\infty)$, $h \in \mathbb{C}[x_1, \ldots, x_n]$. Then $f^m g \in I$ and so $f^m gh \in I$, hence $gh \in I : (f^\infty)$.

(ii) Given two ideals $I, J \subset \mathbb{C}[x_1, \ldots, x_n]$, the *colon ideal* is the set

$$I : J := \{g \in \mathbb{C}[x_1, \ldots, x_n] \mid fg \in I \text{ for all } f \in J\}.$$

Since (f^m) is principal, we have that $I : (f^m) = \{g \in \mathbb{C}[x_1, \ldots, x_n] \mid f^m g \in I\}$. Suppose that $g \in I : (f^m)$. Then $f^m g \in I$, and so $f^{m+1} g \in I$. Hence $g \in I : (f^{m+1})$, and we have an ascending chain of ideals.
By the Ascending Chain Condition there exists some $N \in \mathbb{Z}_{>0}$ such that this stabilises, i.e. such that $I : (f^m) = I : (f^{m+1})$ for all $m \geq N$. We will show that

$I : (f^\infty) = I : (f^N)$. Clearly $I : (f^N) \subseteq I : (f^\infty)$ by definition of the saturation. Let $g \in I : (f^\infty)$. Then there exists some $m \in \mathbb{Z}_{>0}$ such that $f^m g \in I$, hence $g \in I : (f^m)$, hence $g \in I : (f^N)$.

(iii) Let $g \in I : (f^\infty)$. By (ii) we have that $f^N g \in I \subset \tilde{I}$. Write

$$1 = f^N y^N + (1 - f^N y^N) = f^N y^N + (1 - fy)(1 + fy + \ldots + f^{N-1} y^{N-1}).$$

Multiplying through by g we obtain

$$g = f^N g y^N + (1 - fy)(1 + fy + \ldots + f^{N-1} y^{N-1}) g.$$

Since $f^N g, 1 - fy \in \tilde{I}$ and $g \in \mathbb{C}[x_1, \ldots, x_n]$ we conclude that $g \in \tilde{I} \cap \mathbb{C}[x_1, \ldots, x_n]$. Conversely suppose that $g \in \tilde{I} \cap \mathbb{C}[x_1, \ldots, x_n]$. Then

$$g = \sum_{i=1}^{s} p_i f_i + q(1 - yf)$$

for some $p_i, q \in \mathbb{C}[x_1, \ldots, x_n, y]$. Setting $y = 1/f$ gives $g = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, 1/f) f_i$. Clearing out the denominators by multiplying through by a sufficiently large power m of f gives $f^m g = \sum_{i=1}^{s} P_i(x_1, \ldots, x_n) f_i$, where the $P_i \in \mathbb{C}[x_1, \ldots, x_n]$. Hence $f^m g \in I$, and so $g \in I : (f^\infty)$.