M3P23, M4P23, M5P23: COMPUTATIONAL ALGEBRA & GEOMETRY

EXAM SOLUTIONS 2013

(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) $S(-x + y^2, -y^2 + z^4) = (xy^2 - y^4) - (xy^2 - xz^4) = xz^4 - y^4$. Upon division by G we obtain zero. Hence $\{-x + y^2, -y^2 + z^4\}$ is a Gröbner basis for I.

(iii) Our result in (ii) is not reduced, since the leading coefficients are -1 in both cases. Moving to $G' = \{x - y^2, y^2 - z^4\}$ we see that this still isn't reduced, since $y^2 \in (\mathrm{LT}(y^2 - z^4))$. Now $\overline{x - y^2}^{y^2 - z^4} = x - z^4$, so we set $G'' = \{x - z^4, y^2 - z^4\}$. We see that this is reduced.

(iv) There are a number of ways of seeing that the output from the computer is wrong. Here are two: First, notice that the Gröbner basis given by the computer is reduced, but the reduced Gröbner basis is unique and so the computer is wrong. Second, notice (from (iii)) that the curve $\mathbb{V}(I)$ can be paramaterised as (t^4, t^2, t), $t \in k$, but $t^6 - t^4 \neq 0$.

(2) (i) Moving to the ideals, we have an ascending chain

$$\mathbb{I}(V_1) \subseteq \mathbb{I}(V_2) \subseteq \ldots$$

By the Ascending Chain Condition this must stabilise for some N with

$$\mathbb{I}(V_N) = \mathbb{I}(V_{N+1}) = \ldots.$$

But $\mathbb{V}(\mathbb{I}(V)) = V$, so $V_N = V_{N+1} = \ldots$.

(ii) Suppose for a contradiction that V cannot be written as a finite union of irreducible varieties. Since V cannot be irreducible by assumption, so there exists $U, W \subset k^n$, $U \neq V$, $W \neq V$, and $V = U \cup W$. But then at least one of U and W cannot be written as a finite union of irreducible varieties; without loss of generality we assume U is such. By induction we obtain a descending chain

$$V \supsetneq U \supsetneq U' \supsetneq \ldots$$

of affine varieties, each of which cannot be written as a finite union of irreducible varieties. But this contradicts (i).

a.m.kasprzyk@imperial.ac.uk

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

(iii) Let $a = (a_1, \ldots, a_n) \in \mathbb{V}(f, g)$. Then $f(a) = 0$ and $g(a) = g_1(a)g_2(a) = 0$. Hence $a \in \mathbb{V}(f, g_1) \cup \mathbb{V}(f, g_2)$. Conversely let $a \in \mathbb{V}(f, g_1) \cup \mathbb{V}(f, g_2)$. Then $f(a) = 0$ and either $g_1(a) = 0$ or $g_2(a) = 0$. In either case, $g(a) = 0$ and so $a \in \mathbb{V}(f, g)$.

(iv) Notice that $x(z-y) + z(z-y) = (z-y)(z+x)$. By repeated application of (iii) we obtain:

$$\begin{aligned}\mathbb{V}(y^2 - x^2, &(z-y)(z+x)) \\ &= \mathbb{V}\left(y - x, (z-y)(z+x)\right) \cup \mathbb{V}\left(y + x, (z-y)(z+x)\right) \\ &= \mathbb{V}(y-x, z-y) \cup \mathbb{V}(y-x, z+x) \cup \mathbb{V}\left(y+x, (z-y)(z+x)\right) \\ &= \mathbb{V}(y-x, z-y) \cup \mathbb{V}(y-x, z+x) \cup \mathbb{V}(y+x, z-y) \cup \mathbb{V}(y+x, z+x).\end{aligned}$$

In each case the curve is paramaterised by, respectively, (t,t,t), $(t,t,-t)$, $(-t,t,t)$, and $(-t,t,t)$. Hence we have an irreducible decomposition into three distinct factors (the final two factors are equal).

(3) (i) Notice that $f = 0$ if and only if at least one of the factors $(x - a_i)^{r_i}$ vanishes. But $(x - a_i)^{r_i} = 0$ if and only if $x = a_i$, hence $\mathbb{V}(f) = \{a_1, \ldots, a_d\} = \mathbb{V}(f_{red})$. Hence $\mathbb{I}(\mathbb{V}(f)) = \mathbb{I}(\mathbb{V}(f_{red})) \supseteq (f_{red})$. Conversely suppose that $g \in \mathbb{I}(\mathbb{V}(f))$. In particular, $g(a_i) = 0$ for all $1 \leq a_i \leq d$, so we can factor g as

$$g = h \prod_{i=1}^{d} (x - a_i)$$

for some $h \in \mathbb{C}[x]$. In particular $g = \frac{1}{c} h f_{red}$, so $g \in (f_{red})$. Hence $\mathbb{I}(\mathbb{V}(f)) = (f_{red})$.

(ii) $\sqrt{I} = \{f \in k[x_1, \ldots, x_n] \mid f^m \in I \text{ for some } m \in \mathbb{Z}_{>0}\}$.
Let k be an algebraically closed field, $I \subset k[x_1, \ldots, x_n]$ an ideal. The Nullstellensatz states that $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$.

(iii) The variety is given by the line $x = 0$. By applying the Nullstellensatz we see that $\sqrt{I} = (x)$.

(4) (i) If $x^\beta = x^\gamma x^\alpha$ for some $x^\alpha \in I$ then $x^\beta \in I$ by the definition of an ideal. Conversely suppose that $x^\beta \in I$, so that

$$x^\beta = \sum_{i=1}^{m} h_i x^{\alpha_i}, \qquad \text{for some } h_i \in k[x_1, \ldots, x_n], \alpha_i \in A.$$

Expanding the right-hand side as a sum of monomials, we see that each monomial is divisible by x^{α_i} for some $\alpha_i \in A$. Hence the same must be true of the left-hand side.

(ii) Notice that $y(x^3 - 2xy) - x(x^2y - 2y^2 + x) = -x^2$, hence $x^2 \in \mathrm{LT}(I)$. But clearly $x^2 \notin (x^3, x^2y)$, hence the supposition is false.

(iii) By assumption there exists some $f \in I$ such that $\mathrm{LT}(f) \notin (\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_m))$. By applying the Division Algorithm we that $\overline{f}^{f_1,\ldots,f_m} \neq 0$ (since the leading term will not cancel).

(5) **Mastery Question.**

(i) If $\overline{f}^G = 0$ then the Division Algorithm gives

$$f = a_1 g_1 + \ldots + a_m g_m + 0,$$

where whenever $a_i g_i \neq 0$ we have that multideg $(f) \geq$ multideg $(a_i g_i)$. Hence $f \to_G 0$.

(ii) By the Division Algorithm we see that $xy^2 - x = y \cdot (xy+1) + 0 \cdot (y^2-1) + (-x-y)$, i.e. the remainder is non-zero. But $xy^2 - x = 0 \cdot (xy+1) + x \cdot (y^2-1)$ and so $f \to_G 0$.

(iii) Without loss of generality we will assume that we have multiplied f and g through by non-zero constants such that $\mathrm{LC}(f) = \mathrm{LC}(g) = 1$. Writing $f = \mathrm{LM}(f) + p$ and $g = \mathrm{LM}(g) + q$, for some $p, q \in k[x_1, \ldots, x_n]$, we see that

$$\begin{aligned} S(f,g) &= \mathrm{LM}(f)\,\mathrm{LM}(g) + p\mathrm{LM}(g) - \mathrm{LM}(f)\,\mathrm{LM}(g) - q\mathrm{LM}(f) \\ &= p\mathrm{LM}(g) - q\mathrm{LM}(f) \\ &= p(g-q) - q(f-p) \\ &= pg - qf. \end{aligned}$$

We have that $\mathrm{LM}(pg) = \mathrm{LM}(p)\,\mathrm{LM}(g)$ and $\mathrm{LM}(qf) = \mathrm{LM}(q)\,\mathrm{LM}(f)$. Since $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$ are coprime, and since $\mathrm{LM}(p) < \mathrm{LM}(f)$ and $\mathrm{LM}(q) < \mathrm{LM}(g)$, we conclude that $\mathrm{LM}(p)\,\mathrm{LM}(g) \neq \mathrm{LM}(q)\,\mathrm{LM}(f)$. Hence the leading monomials do not cancel, so multideg $(S(f,g)) = \max\{\text{multideg}\,(pg), \text{multideg}\,(qf)\}$. Thus $S(f,g) \to_G 0$.

(iv) Our result in (iii) means that we can avoid performing the S-polynomial computation for pairs $f, g \in G$ whenever the leading monomials are coprime; in those cases we know *a priori* that $S(f,g) \to_G 0$. This is a significant improvement over the traditional Buchberger's Criterion, since the computation $\overline{S(f,g)}^G$ involving the Division Algorithm is expensive.

(v) Notice that x^3 and yz are coprime, as are x^3 and z^4. Thus the only pair we need to check is $yz + y$ and z^4. In this case $S(yz+y, z^4) = yz^3$. Suppose that

$$yz^3 = p(x^3 + y) + q(yz + y) + rz^4, \qquad p, q, r \in k[x, y, z].$$

In order for $yz^3 \to_G 0$ we require that the multidegree of each term is at most yz^3. From this we conclude that $r = 0$ and $p \in k$. We see that no solution is possible, hence this is not a Gröbner basis.