MAS400: Solutions 5

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

1. Fix a monomial order on $R = F[x_1, \ldots, x_n]$ and let $f, f_1, \ldots, f_m \in R$ with $f_1, \ldots, f_m \neq 0$. Suppose that f rem $(f_1, \ldots, f_s) = 0$ for some $s \leqslant m$. Show that f rem $(f_1, \ldots, f_m) = 0$.

   In the solution to Exercises 4, Question 2, we saw that if the remainder is zero after applying multivariate division then the else-part of the while-loop is never executed. So when dividing by $(f_1, \ldots, f_s)$ we always have $\operatorname{lt} f_i \mid \operatorname{lt} p$ (notation p as in algorithm `MultivariateDivision`). We now claim that on division by $(f_1, \ldots, f_s)$ and $(f_1, \ldots, f_m)$ the values of p are the same after j executions of the while-loop (for $j = 0, 1, 2, \ldots t$ where t is the number of times the while-loop operates on division by $(f_1, \ldots, f_s)$), which we show by induction. Certainly this is true for $j = 0$, as $p = f$ then. If it is true after j executions (and $p \neq 0$) then there exists $j \in \{1, \ldots, s\}$ such that $\operatorname{lt} f_j \mid \operatorname{lt} p$, whence there exists $j \in \{1, \ldots, m\}$ such that $\operatorname{lt} f_j \mid \operatorname{lt} p$. Thus the value of i chosen by `MultivariateDivision` such that $\operatorname{lt} f_i \mid \operatorname{lt} p$ satisfies $1 \leqslant i \leqslant m$, and is the same for both divisions. Therefore the values of p are identical after $j + 1$ executions, and therefore identical always. Therefore division by $(f_1, \ldots, f_m)$ terminates after t executions of the while-loop and yields remainder 0.

2. Let F be your favourite field, and choose your favourite monomial order. State your choices clearly. With respect to your choices find a Gröbner basis for I in each of the following cases.

   (a) Ideal $I = \langle xy - 1, y^2 - 1 \rangle$ in $F[x, y]$.

   (b) Ideal $I = \langle xy - 1, xz - 1 \rangle$ in $F[x, y, z]$.

   (c) Ideal $I = \langle xy - 1, yz - 1, zx - 1 \rangle$ in $F[x, y, z]$.

   (d) Ideal $I = \langle xy^2 - 1, xz^2 - 1 \rangle$ in $F[x, y, z]$.

   (e) Ideal $I = \langle x^2y - 1, x^2z - 1 \rangle$ in $F[x, y, z]$.

   (f) Ideal $I = \langle x^2y - 1, y^2z - 1, z^2x - 1 \rangle$ in $F[x, y, z]$.

   Also find a reduced Gröbner basis for each of the above ideals.

   NB: Some of these questions may take a long time.

   I shall take $F = \mathbb{Q}$, and the $\leqslant_{\text{lex}}$ monomial order with $x > y > z$. Sample solutions are as follows. The multivariate division is left as an exercise for the reader.

(a) Take $g_1 = xy - 1$, $g_2 = y^2 - 1$. $S(g_1, g_2) = yg_1 - xg_2 = x - y$ and $S(g_1, g_2)$ rem $(g_1, g_2) = x - y$. So set $g_3 = x - y$. Then $S(g_1, g_2) = x - y$, $S(g_1, g_3) = g_1 - yg_3 = y^2 - 1$ and $S(g_2, g_3) = xg_2 - y^2 g_3 = y^3 - x$ all have zero remainder on division by (g_1, g_2, g_3) (the latter division requires two steps). Therefore $\{g_1, g_2, g_3\} = \{xy - 1, y^2 - 1, x - y\}$ is a Gröbner basis for $I = \langle xy - 1, y^2 - 1\rangle$.

(b) Take $g_1 = xy - 1$, $g_2 = xz - 1$. $S(g_1, g_2) = zg_1 - yg_2 = y - z$ and $S(g_1, g_2)$ rem $(g_1, g_2) = y - z$. So set $g_3 = y - z$. Then $S(g_1, g_2) = y - z$, $S(g_1, g_3) = g_1 - xg_3 = xz - 1$ and $S(g_2, g_3) = yg_2 - xzg_3 = xz^2 - y$ all have zero remainder on division by (g_1, g_2, g_3) (the latter division requires two steps). Therefore $\{g_1, g_2, g_3\} = \{xy - 1, xz - 1, y - z\}$ is a Gröbner basis for $I = \langle xy - 1, xz - 1\rangle$.

(c) Take $g_1 = xy - 1$, $g_2 = yz - 1$ and $g_3 = xz - 1$. Then $S(g_1, g_2) = zg_1 - xg_2 = x - z$, $S(g_1, g_3) = zg_1 - yg_3 = y - z$ and $S(g_2, g_3) = xg_2 - yg_3 = -x + y$. We get $S(g_1, g_2)$ rem $(g_1, g_2, g_3) = x - z$, $S(g_1, g_3)$ rem $(g_1, g_2, g_3) = y - z$, $S(g_2, g_3)$ rem $(g_1, g_2, g_3) = -x + y$. Therefore we set $g_4 = x - z$, $g_5 = y - z$ and $g_6 = -x + y$.

$S(g_1, g_4) = g_1 - yg_4 = yz - 1$, $S(g_1, g_5) = xz - 1$, $S(g_1, g_6) = y^2 - 1$, $S(g_2, g_4) = -x + yz^2$, $S(g_2, g_5) = z^2 - 1$, $S(g_2, g_6) = -x + y^2 z$, $S(g_3, g_4) = z^2 - 1$, $S(g_3, g_5) = xz^2 - y$, $S(g_3, g_6) = yz - 1$, $S(g_4, g_5) = xz - yz$, $S(g_4, g_6) = y - z$, $S(g_5, g_6) = -xz + y^2$ [with leading term written first].

We have $S(g_i, g_j)$ rem $(g_1, g_2, g_3, g_4, g_5, g_6) = 0$ for $1 \leqslant i < j \leqslant 6$ except for $(i, j) \in \{(2, 5), (3, 4)\}$, when the remainder is $z^2 - 1$.

(The calculation that $S(g_2, g_3)$ rem $(g_1, g_2, g_3, g_4, g_5, g_6) = 0$ requires two steps of MV-Div, despite the fact that $S(g_2, g_3) = g_6$. The most difficult calculations require three steps of MV-Div; these were required to calculate the remainder after dividing $S(g_2, g_6)$ and $S(g_5, g_6)$ by $(g_1, g_2, g_3, g_4, g_5, g_6)$.)

Anyway, we set $g_7 = z^2 - 1$, and calculate $S(g_1, g_7) = xy - z^2$, $S(g_2, g_7) = y - z$, $S(g_3, g_7) = x - z$, $S(g_4, g_7) = x - z^3$, $S(g_5, g_7) = y - z^3$, $S(g_6, g_7) = x - yz^2$.

We have $S(g_i, g_j)$ rem $(g_1, g_2, g_3, g_4, g_5, g_6, g_7) = 0$ for $1 \leqslant i < j \leqslant 7$. By Question 1, we 'only' have to perform these MV-Divs if $j = 7$ or $(i, j) \in \{(2, 5), (3, 4)\}$.

We are now done, and a Gröbner basis for $\langle xy - 1, yz - 1, xz - 1\rangle$ is $\{g_1, \ldots, g_7\} = \{xy - 1, yz - 1, xz - 1, x - z, y - z, -x + y, z^2 - 1\}$.

`GröbnerBasis` takes quite a long time here. To speed up the process, we observe that if $r = f$ rem $(f_1, \ldots, f_s)$ then the ideals $\langle f, f_1, \ldots, f_s \rangle$ and $\langle r, f_1, \ldots, f_s \rangle$ coincide [Proof: Exercise]. With the notation of this question, observe that $g_6 = g_5 - g_4$, and that g_4, g_5, g_6 have total degree 1, while g_1, g_2, g_3 have total degree 2. We calculate that g_1 rem $(g_4, g_5) = g_2$ rem $(g_4, g_5) = g_3$ rem $(g_4, g_5) = z^2 - 1$. Thus $I = \langle f_1, f_2, f_3 \rangle = \langle g_1, g_2, g_3 \rangle = \langle g_1, g_2, g_3, g_4, g_5 \rangle = \langle g_4, g_5, g_7 \rangle$, where $g_7 = z^2 - 1$. By considering just three S-polynomials we find that $\{x - z, y - z, z^2 - 1\} = \{g_4, g_5, g_7\}$ is a [reduced] Gröbner basis for I.

(d) Take $g_1 = xy^2 - 1$, $g_2 = xz^2 - 1$. $S(g_1, g_2) = z^2 g_1 - y^2 g_2 = y^2 - z^2$ and $S(g_1, g_2)$ rem $(g_1, g_2) = y^2 - z^2$. So set $g_3 = y^2 - z^2$. Then $S(g_1, g_2) = y^2 - z^2$, $S(g_1, g_3) = g_1 - xg_3 = xz^2 - 1$ and $S(g_2, g_3) = y^2 g_3 - xz^2 g_3 = xz^4 - y^2$ all have zero remainder on division by (g_1, g_2, g_3) (the latter division requires two steps). Therefore $\{g_1, g_2, g_3\} = \{xy^2 - 1, xz^2 - 1, y^2 - z^2\}$ is a Gröbner basis for $I = \langle xy^2 - 1, xz^2 - 1 \rangle$.

(e) Take $g_1 = x^2 y - 1$, $g_2 = x^2 z - 1$. $S(g_1, g_2) = zg_1 - yg_2 = y - z$ and $S(g_1, g_2)$ rem $(g_1, g_2) = y - z$. So set $g_3 = y - z$. Then $S(g_1, g_2) = y - z$, $S(g_1, g_3) = g_1 - x^2 g_3 = x^2 z - 1$ and $S(g_2, g_3) = yg_2 - x^2 z g_3 = x^2 z^2 - y$ all have zero remainder on division by (g_1, g_2, g_3) (the latter division requires two steps). Therefore $\{g_1, g_2, g_3\} = \{x^2 y - 1, x^2 z - 1, y - z\}$ is a Gröbner basis for $I = \langle x^2 y - 1, x^2 z - 1 \rangle$.

(f) Not done yet, as `GröbnerBasis` takes too long.

Reduced Gröbner bases 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) $\{x^2 z - 1, y - z\}$.

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

The major step is just to eliminate elements in the Gröbner bases given above whose leading term is divisible by the leading term of another element in the Gröbener basis (eliminate the terms one by one). One

also normalises the terms of the Gröbner basis so that their leading coefficients are 1. One might have to make other adjustments to the Gröbner basis before it is in reduced form (see Question 2 on next sheet).

Changing the monomial order will change the reduced Gröbner basis. For example if we have $\leqslant_{\text{lex}}$ monomial order with $y > x > z$ then the answer to Part (a) is $\{y-x, x^2-1\}$, while the answers to the other parts remain the same [with some reordering if we insist that the elements in a Gröbner basis be ordered by their leading terms].

If the monomial order is $\leqslant_{\text{grlex}}$ with $x > y > z$ then the answers to Parts (a)–(e) remain the same [up to reordering] and the answer to Part (f) is $\{yz^3 - x, z^4 - y, y^3 - z^3, y^2z - 1, x^2 - yz, xy - z^2, xz - y^2\}$.