Computational Algebraic Geometry Homework 2

Michael Nelson

Problem 1

Exercise 1. Let $\mathbb{F}_2$ be the field with two elements.

1. Show that $x^2y + y^2x$ vanishes on $\mathbb{F}_2^2$.
2. Prove that $\langle x^2 - x, y^2 - y \rangle \subseteq \mathcal{I}(\mathbb{F}_2^2)$.
3. Show that every $f \in \mathbb{F}_2[x, y]$ can be written as
$$f = A(x^2 - x) + B(y^2 - y) + axy + bx + cy + d \tag{1}$$
where $A, B \in \mathbb{F}_2[x, y]$ and $a, b, c, d \in \mathbb{F}_2$.
4. Show that $axy + bx + cy + d \in \mathcal{I}(\mathbb{F}_2^2)$ if and only if $a = b = c = d = 0$.
5. From here, conclude that $\langle x^2 - x, y^2 - y \rangle = \mathcal{I}(\mathbb{F}_2^2)$.

Solution 1. 1. Let $(a, b) \in \mathbb{F}_2^2$ and let $f = x^2y + y^2x$. We have

$$\begin{aligned} f(a, b) &= a^2b + b^2a \\ &= ab + ba \\ &= 2ab \\ &= 0, \end{aligned}$$

where we used the fact that we are working in $\mathbb{F}_2$. It follows that f vanishses on $\mathbb{F}_2^2$.

2. Let $f(x^2 - x) + g(y^2 - y) \in \langle x^2 - x, y^2 - y \rangle$ where $f, g \in \mathbb{F}_2[x, y]$. Then given any $(a, b) \in \mathbb{F}_2^2$, we have

$$\begin{aligned} (f(x^2 - x) + g(y^2 - y))(a, b) &= f(a, b)(a^2 - a) + g(a, b)(b^2 - b) \\ &= f(a, b)(a - a) + g(a, b)(b - b) \\ &= f(a, b) \cdot 0 + g(a, b) \cdot 0 \\ &= 0. \end{aligned}$$

It follows that $f(x^2 - x) + g(y^2 - y) \in \mathcal{I}(\mathbb{F}_2^2)$. Since $f(x^2 - x) + g(y^2 - y)$ was an arbitrary element in $\langle x^2 - x, y^2 - y \rangle$, we see that $\langle x^2 - x, y^2 - y \rangle \subseteq \mathcal{I}(\mathbb{F}_2^2)$.

3. Observe that $\mathcal{G} = \{x^2 - x, y^2 - y\}$ is a Gröbner basis for $\langle x^2 - x, y^2 - y \rangle$ with respect to lexicographic order $(x > y)$. Indeed, the S-polynomial of $x^2 - x$ and $y^2 - y$ is

$$\begin{aligned} S(x^2 - x, y^2 - y) &= y^2(x^2 - x) - x^2(y^2 - y) \\ &= -y^2x + x^2y \\ &= x^2y - xy^2, \end{aligned}$$

and this reduces to 0 when divided by $\mathcal{G}$ using the division algorithm:

$$x^2y - xy^2 = y(x^2 - x) - x(y^2 - y).$$

The monomials which do not belong to $\mathrm{LT}(\mathcal{G})$ are $\{1, x, y, xy\}$. It follows that every polynomial in $\mathbb{F}_2[x, y]$ can be expressed in the form (1).

4. Set $r = axy + bx + cy + d$. If $a = b = c = d = 0$, then $r = 0$, and clearly in this case we have $r \in \mathcal{I}(\mathbb{F}_2^2)$. Conversely, suppose $r \in \mathcal{I}(\mathbb{F}_2^2)$. Evaluating r at $(0,0)$ gives us $d = 0$. Next, evaluating r at $(1,0)$ gives us $b = 0$. Similarly, evaluating r at $(0,1)$ gives us $c = 0$. Finally, evaluating r at $(1,1)$ gives us $a = 0$.

5. We just need to show that $\mathcal{I}(\mathbb{F}_2^2) \subseteq \langle x^2 - x, y^2 - y\rangle$ since part 2 gives us the reverse inclusion. Suppose $f \in \mathcal{I}(\mathbb{F}_2^2)$. By part 3, we can express f in the form (1). Since $f \in \mathcal{I}(\mathbb{F}_2^2)$, the remainder part is zero by part 4: $axy + bx + cy + d = 0$. Therefore f has the form $f = A(x^2 - x) + B(y^2 - y)$, which implies $f \in \langle x^2 - x, y^2 - y\rangle$. Since f was arbitrary, it follows that $\mathcal{I}(\mathbb{F}_2^2) \subseteq \langle x^2 - x, y^2 - y\rangle$.

Problem 2

Exercise 2. Let $f = x^3 - x^2y - x^2z$, $f_1 = x^2y - z$, and $f_2 = xy - 1$.

1. Use the lexicographic order $(x > y > z)$ to compute the remainder r_1 of f when divided by (f_1, f_2) and the remainder r_2 of f when divided (f_2, f_1).
2. Find an expression for $r = r_1 - r_2$ in $\langle f_1, f_2\rangle$, that is, find $A, B \in k[x,y,z]$ such that $r = Af_1 + Bf_2$ for r.

Solution 2. 1. The computation for r_1 is done below:

$$
\begin{array}{ll|l}
 & q_1 : -1 & \\
 & q_2 : & \\
\begin{array}{l} x^2y - z \\ xy - 1 \end{array} & \overline{x^3 - x^2y - x^2z} & \quad r_1 \\
 & \quad -x^2y - x^2z & \overline{x^3 - x^2z - z} \\
 & \quad \underline{-x^2y + z} & \\
 & \qquad -x^2z - z & \\
 & \qquad\quad -z & \\
 & \qquad\quad 0 &
\end{array}
$$

$$x^3 - x^2y - x^2z = -(x^2y - z) + x^3 - x^2z - z$$

We obtain $r_1 = x^3 - x^2z - z$. Next, the computation for r_2 is done below:

$q_1 : -x$

$q_2 :$

$xy-1$, x^2y-z $\Big|$ $x^3 - x^2y - x^2z$

$-x^2y - x^2z$

$-x^2y + x$

$-x^2z - x$

$-x$

0

r_2

$x^3 - x^2z - x$

$$x^3 - x^2y - x^2z = -x(xy-1) + x^3 - x^2z - x$$

We obtain $r_2 = x^3 - x^2z - x$.

2. From the computations above, we see that $-xf_2 + r_2 = -f_1 + r_1$. Thus

$$\begin{aligned} r &= r_1 - r_2 \\ &= -xf_2 + f_1. \end{aligned}$$

Problem 3

Exercise 3. A basis (generating set) $\{x^{\alpha_1}, \ldots, x^{\alpha_s}\}$ for a monomial ideal I is **minimal** if no x^{α_i} divides any x^{α_j} for $i \neq j$.

1. Prove that every monomial ideal has a minimal basis.

2. Prove that every monomial ideal has a *unique* minimal basis.

Solution 3. 1. Let I be a monomial ideal with generating set $\{m_1, \ldots, m_s\}$ (where we assume the coefficient for each m_i is 1). If for some $i \neq j$, we have $m_i \mid m_j$, then we may remove m_j from the generating set $\{m_1, \ldots, m_s\}$ to obtain another generating set of I: $\{m_1, \ldots, m_{j-1}, m_{j+1}, \ldots m_s\}$. Indeed, clearly we have

$$\langle m_1, \ldots, m_{j-1}, m_{j+1}, \ldots m_s \rangle \subseteq \langle m_1, \ldots, m_{j-1}, m_j, m_{j+1}, \ldots, m_s \rangle.$$

We have the reverse inclusion since $m_i \mid m_j$. Thus for each $1 \leq j \leq s$, we remove m_j from $\{m_1, \ldots, m_s\}$ if there exists an $i \neq j$ such that $m_i \mid m_j$. Doing so results in a minimal basis for I.

2. Suppose $\{m_1, \ldots, m_s\}$ and $\{m'_1, \ldots, m'_{s'}\}$ are two minimal bases for I. Let $1 \leq i \leq s$. Then since $m_i \in \langle m'_1, \ldots, m'_{s'} \rangle$, there must exist some $1 \leq i' \leq s'$ such that $m'_{i'} \mid m_i$. Similarly, since $m'_{i'} \in \langle m_1, \ldots, m_s \rangle$, there must exist some $1 \leq j \leq s$ such that $m_j \mid m'_{i'}$. Since $m_j \mid m'_{i'}$ and $m'_{i'} \mid m_i$, we see that $m_j \mid m_i$. Since $\{m_1, \ldots, m_s\}$ is minimal, we must in fact have $j = i$. It follows that $m_i \mid m'_{i'}$ and $m'_{i'} \mid m_i$, which implies $m_i = m'_{i'}$ since we are assuming the coefficient for each m_i and $m'_{i'}$ is 1.

What we've shown so far is that for each $1 \leq i \leq s$ there exists some $1 \leq i' \leq s'$ such that $m_i = m'_{i'}$. In fact, such an i' is uniquel. Indeed, if $m_i = m'_{j'}$ for some $1 \leq j' \leq s'$, then clearly $m'_{i'} \mid m'_{j'}$, which implies $i' = j'$ by minimality $\{m'_1, \ldots, m'_{s'}\}$. Thus we have a one-one and onto correspondence from $\{m_1, \ldots, m_s\}$ to $\{m'_1, \ldots, m'_{s'}\}$; in fact they are the same set: $\{m_1, \ldots, m_s\} = \{m'_1, \ldots, m'_{s'}\}$. Therefore every monomial ideal has a *unique* minimal basis.

Problem 4

Exercise 4. Consider $\mathbb{Z}^n \subseteq \mathbb{C}^n$. Prove that if f vanishes on $\mathbb{Z}^n$, then f is the zero polynomial. From this, conclude that $\mathcal{I}(\mathbb{Z}^n) = \langle 0 \rangle$.

Solution 4. We prove this by induction on n. The base case $n = 1$ follows from the fact that any nonzero polynomial has at most finitely many roots, thus if $f \in \mathbb{C}[x]$ vanishes on all of $\mathbb{Z}$, then it must be the zero polynomial. Now suppose we have proven the theorem for some $n \geq 1$. Let $f \in \mathbb{C}[x_1, \dots, x_n, y]$ and suppose f vanishes on $\mathbb{Z}^{n+1}$. Express f as

$$f = c_d y^d + \cdots + c_1 y + c_0$$

where $c_0, c_1, \dots, c_d \in \mathbb{C}[x_1, \dots, x_d]$. Now let $(a_1, \dots, a_n) \in \mathbb{Z}^n$. Then

$$f|_{x_1=a_1,\dots,x_n=a_n} = c_d(a_1, \dots, a_n)y^d + \cdots + c_1(a_1, \dots, a_n)y + c_0(a_1, \dots, a_n)$$

is a polynomial in y which vanishes on all of $\mathbb{Z}$ by assumption. It follows that $f|_{x_1=a_1,\dots,x_n=a_n}$ is the zero polynomial (by the base case), and thus $c_i(a_1, \dots, a_n) = 0$ for each $1 \leq i \leq d$. Since $(a_1, \dots, a_n)$ is arbitrary, we see that c_i vanishes on all of $\mathbb{Z}^n$. It follows by induction on n that $c_i = 0$ for all $1 \leq i \leq d$. Thus f is the zero polynomial.

Problem 5

Exercise 5. Consider the system of equations

$$\begin{aligned} 2x^2 + y^2 &= 3 \\ x^2 + xy + y^2 &= 3 \end{aligned}$$

1. Compute a Gröbner basis for the corresponding ideal using the lexicographic order ($y > x$).
2. Symbolically find the four common solutions to these equations.
3. Let f be the smallest degree polynomial in I in y (that is, x does not appear in the polynomial). Symbolically, find the roots of f and compare them to what you found in part 2.

Solution 5. 1. First we set $f_1 = y^2 + 2x^2 - 3$, $f_2 = y^2 + yx + x^2 - 3$, and $\mathcal{F}_1 = \{f_1, f_2\}$. Now we compute the S-polynomial

$$\begin{aligned} S(f_2, f_1) &= f_2 - f_1 \\ &= (y^2 + yx + x^2 - 3) - (y^2 + 2x^2 - 3) \\ &= yx - x^2. \end{aligned}$$

The S-polynomial $S(f_2, f_1)$ remains the same when we divide it by $\mathcal{F}_1$; that is

$$S(f_1, f_2)^{\mathcal{F}_1} = yx - x^2.$$

Now we set $f_3 = yx - x^2$ and $\mathcal{F}_2 = \{f_1, f_2, f_3\}$. If we divide f_1 with respect to $\mathcal{F}_2 \backslash \{f_1\}$, we obtain

$$f_1^{\mathcal{F}_2 \backslash \{f_1\}} = 0,$$

thus we may replace $\mathcal{F}_2$ with $\mathcal{F}_3 = \{f_2, f_3\}$. Now we compute the S-polynomial

$$\begin{aligned} S(f_2, f_3) &= x f_2 - y f_2 \\ &= x(y^2 + yx + x^2 - 3) - y(yx - x^2) \\ &= 2yx^2 + x^3 - 3x \end{aligned}$$

When we divide $S(f_2, f_3)$ with respect to $\mathcal{F}_3$, we obtain

$$S(f_2, f_3)^{\mathcal{F}_3} = 3x^3 - 3x.$$

Now we set $f_4 = x^3 - x$ and $\mathcal{F}_4 = \{f_2, f_3, f_4\}$. We claim that $\mathcal{F}_4$ is a Gröbner basis. Indeed, we have

$$\begin{aligned} S(f_2, f_4) &= x^3 f_2 - y^2 f_2 \\ &= x^3(y^2 + yx + x^2 - 3) - y^2(x^3 - x) \\ &= y^2 x + yx^3 + x^5 - 3x^3, \end{aligned}$$

and when we divide $S(f_2, f_4)$ with respect to $\mathcal{F}_4$, we obtain

$$S(f_2, f_4)^{\mathcal{F}_4} = 0.$$

Similarly, we have $S(f_3, f_4)^{\mathcal{F}_4} = 0$ and $S(f_2, f_3)^{\mathcal{F}_4} = 0$.

2. To find the four common solutions, we use the Gröbner basis:

$$\begin{aligned} y^2 + xy + x^2 - 3 &= 0 \\ xy - x^2 &= 0 \\ x^3 - x &= 0. \end{aligned}$$

First we solve the third equation in x: from $x^3 - x = 0$, we see that $x = \{0, 1, -1\}$. If $x = 0$, then from the first two equations we see that $y^2 - 3 = 0$, thus $y = \pm\sqrt{3}$. It is easy to check that $(0, \sqrt{3})$ and $(0, -\sqrt{3})$ are two solutions to the system of equations above. To find the other two solutions, first assume $x = 1$. Then from the second equation, we see that $y = 1$. The point $(1, 1)$ is also a solution to the first equation, so $(1, 1)$ is a solution to the system of equations above. Finally assume $x = -1$. Then from the second equation, we see that $y = -1$. The point $(-1, -1)$ is also a solution to the first equation, so $(-1, -1)$ is a solution to the system of equations above. So all four solutions are given below:

$$\{(0, \sqrt{3}), (0, -\sqrt{3}), (1, 1), (-1, -1)\}.$$

3. Using Singular, we compute a Gröbner basis with respect to lexicographic order $(x > y)$. We obtain $\mathcal{G} = \{y^4 - 4y^2 + 3, 2x + y^3 - 3y\}$. Thus $f = y^4 - 4y^2 + 3$. The roots of f are seen in the way it factors:

$$y^4 - 4y^2 + 3 = (y - 1)(y + 1)(y - \sqrt{3})(y + \sqrt{3}).$$

These four y-coordinates agree with the points we found above.