Computational Algebraic Geometry Homework 1

Michael Nelson

Problem 1

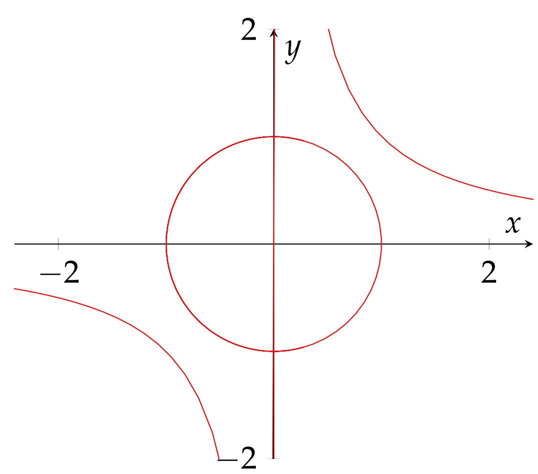
Exercise 1. Consider the system of equations

$$\begin{aligned} x^2 + y^2 - 1 &= 0 \\ xy - 1 &= 0 \end{aligned}$$

These equations describe the intersection of a circle and a hyperbola.

1. Symbolically find all four solutions to this system of equations.
2. Find a polynomial of degree four whose roots are x-values of the solutions you found in part 1.
3. Show that the polynomial that you got from part 2 lies in the ideal $I = \langle x^2 + y^2 - 1, xy - 1 \rangle$.

Solution 1. 1. There are no real solutions to this system of equations, as can be seen in the image below:



However there are complex solutions, which we will find now. From the first equation, we have $y^2 = 1 - x^2$. After squaring the second equation and a substitution, we obtain $(1 - x^2)x^2 = 1$. In other words,

$$x^4 - x^2 + 1 = 0. \tag{1}$$

Observe that $x^4 - x^2 + 1$ is the 12th cyclotomic polynomial, which factors as

$$x^4 - x^2 + 1 = (x - \zeta_{12})(x - \zeta_{12}^5)(x - \zeta_{12}^7)(x - \zeta_{12}^{11}),$$

where $\zeta_{12} = e^{2\pi i/12}$. It follows that the x-coordinates of the four solutions are of the form ζ_{12}^a where $a \in \{1, 5, 7, 11\}$. In fact, we claim that the four solutions to the system of equations above are of the form $(\zeta_{12}^a, \zeta_{12}^{-a})$ where $a \in \{1, 5, 7, 11\}$. Indeed, it is clear that the points $(\zeta_{12}^a, \zeta_{12}^{-a})$ are solutions to the second equation for all $a \in \{1, 5, 7, 11\}$. To see why they satisfy the first equation, first note that

$$\begin{aligned} (\zeta_{12})^2 + (\zeta_{12}^{-1})^2 &= \zeta_{12}^2 + \zeta_{12}^{-2} \\ &= 2\cos(\pi/6) \\ &= 2 \cdot \frac{1}{2} \\ &= 1. \end{aligned}$$

Thus $(\zeta_{12}, \zeta_{12}^{-1})$ is a solution to the first equation. This implies

$$\begin{aligned}(\zeta_{12}^5)^2 + (\zeta_{12}^{-5})^2 &= \zeta_{12}^{10} + \zeta_{12}^{-10} \\ &= \zeta_{12}^{-2} + \zeta_{12}^{2} \\ &= 1,\end{aligned}$$

which shows that $(\zeta_{12}^5, \zeta_{12}^{-5})$ is a solution to the first equation, and

$$\begin{aligned}(\zeta_{12}^7)^2 + (\zeta_{12}^{-7})^2 &= \zeta_{12}^{14} + \zeta_{12}^{-14} \\ &= \zeta_{12}^{2} + \zeta_{12}^{-2} \\ &= 1,\end{aligned}$$

which shows that $(\zeta_{12}^7, \zeta_{12}^{-7})$ is a solution to the first equation, and

$$\begin{aligned}(\zeta_{12}^{11})^2 + (\zeta_{12}^{-11})^2 &= \zeta_{12}^{22} + \zeta_{12}^{-22} \\ &= \zeta_{12}^{-2} + \zeta_{12}^{2} \\ &= 1,\end{aligned}$$

which shows that $(\zeta_{12}^{11}, \zeta_{12}^{-11})$ is a solution to the first equation.

2. They polynomial (1) is of degree four whose roots are x-values of the four solutions to the system of equations.

3. One can obtain (1) another way, via Buchberger's algorithm. Namely, set $f_1 = x^2 + y^2 - 1$ and $f_2 = xy - 1$. Using lexicographic ordering with $y > x$, we calculate the S-polynomial $S(f_1, f_2)$. We have

$$\begin{aligned}S(f_1, f_2) &= xf_1 - yf_2 \\ &= x(y^2 + x^2 - 1) - y(yx - 1) \\ &= x^3 - x + y \\ &= y + x^3 - x.\end{aligned}$$

Next we set $f_3 = S(f_1, f_2)$ and calculate the S-polynomial $S(f_3, f_2)$. We have

$$\begin{aligned}S(f_3, f_2) &= xf_3 - f_2 \\ &= x(y + x^3 - x) - (yx - 1) \\ &= x^4 - x^2 + 1.\end{aligned}$$

In particular, this shows that $x^4 - x^2 + 1 \in I$ since

$$\begin{aligned}x^4 - x^2 + 1 &= xf_3 - f_2 \\ &= x(xf_1 - yf_2) - f_2 \\ &= x^2 f_1 + (-xy - 1)f_2.\end{aligned}$$

Problem 2

Exercise 2. Let I be an ideal of $K[x_1, \dots, x_n]$. Show that $G = \{g_1, \dots, g_s\} \subseteq I$ is a Gröbner basis of I if and only if the leading term of any element of I is divisible by a leading term g_r for some $1 \leq r \leq s$.

Solution 2. Denote denote $m_r = \mathrm{LT}(g_r)$ for each $1 \leq r \leq s$. First suppose G is a Gröbner basis of I. By definition, this means $\mathrm{LT}(I) = \langle m_1, \dots, m_s \rangle$, where

$$\mathrm{LT}(I) = \{\text{monomials } m \mid m = \mathrm{LT}(f) \text{ for some } f \in I\}.$$

In particular, if m is the lead term of an element $f \in I$, then $m \in \langle m_1, \dots, m_s \rangle$ which implies

$$m = f_1 m_1 + \cdots + f_s m_s \tag{2}$$

for some $f_1, \dots, f_s \in K[x_1, \dots, x_n]$. Now clearly every monomial term on the right-hand side of (2) is divisible by some m_r. Thus m must be divisible by some m_r.

Conversely, suppose the leading term of every element of I is divisible by m_r for some $1 \leq r \leq s$ (where m_r depends on the element in question). This implies $\mathrm{LT}(I) \supseteq \langle m_1, \dots, m_s \rangle$. Since each $g_r \in I$, the reverse inclusion holds as well. Thus $\mathrm{LT}(I) = \langle m_1, \dots, m_s \rangle$, or equivalently, G is a Gröbner basis of I.

Problem 3

Exercise 3. An ideal I is a **radical ideal** if whenever $f^k \in I$, then $f \in I$. The **radical** of an ideal I is defined as $\sqrt{I} = \{f \mid f^k \in I \text{ for some } k \in \mathbb{N}_{\geq 1}\}$.

1. Let $X \subseteq \mathbb{A}_K^n$ and prove that $\mathcal{I}(X)$ is a radical ideal.

2. Let I and J be ideals such that $\sqrt{I} = \sqrt{J}$. Prove that $\mathcal{V}(I) = \mathcal{V}(J)$.

Solution 3. 1. Suppose that $f^k \in \mathcal{I}(X)$ for some $k \in \mathbb{N}_{\geq 1}$. This means $f^k(x) = 0$ for all $x \in X$. Since K is a field, the only nilpotent element in K is the zero element, and thus $f(x) = 0$ for all $x \in X$. This implies $f \in \mathcal{I}(X)$; in particular, $\mathcal{I}(X)$ is a radical ideal.

2. First note that $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$. Indeed, we have $\mathcal{V}(I) \supseteq \mathcal{V}(\sqrt{I})$ since $I \subseteq \sqrt{I}$ and since $\mathcal{V}$ is inclusion-reversing. For the reverse inclusion, suppose $x \in \mathcal{V}(I)$ and $f \in \sqrt{I}$. Then $f^k(x) = 0$ for some $k \in \mathbb{N}_{\geq 1}$. As noted above, this implies $f(x) = 0$ since K is a field. Since $f \in \sqrt{I}$ is arbitrary, it follows that $x \in \mathcal{V}(\sqrt{I})$, and since $x \in \mathcal{V}(I)$ is arbitrary, it follows that $\mathcal{V}(I) \subseteq \mathcal{V}(\sqrt{I})$. Thus, we have

$$\begin{aligned}\mathcal{V}(I) &= \mathcal{V}(\sqrt{I}) \\ &= \mathcal{V}(\sqrt{J}) \\ &= \mathcal{V}(J).\end{aligned}$$

Problem 4

Exercise 4. Let V be an algebraic variety. We say V is **reducible** if there exist algebraic varieties V_1 and V_2 that are properly contained in V such that $V = V_1 \cup V_2$. A variety is **irreducible** if it is not reducible. Prove that V is irreducible if and only if $\mathcal{I}(V)$ is a prime ideal.

Solution 4. Suppose $\mathcal{I}(V)$ is a prime ideal and suppose $V = V_1 \cup V_2$ where V_1, V_2 are two varieties properly contained in V. Then

$$\begin{aligned}\mathcal{I}(V) &= \mathcal{I}(V_1 \cup V_2) \\ &= \mathcal{I}(V_1) \cap \mathcal{I}(V_2)\end{aligned}$$

and since $\mathcal{I}(V)$ is prime, we must either have $\mathcal{I}(V) \supseteq \mathcal{I}(V_1)$ or $\mathcal{I}(V) \supseteq \mathcal{I}(V_2)$. Without loss of generality, assume $\mathcal{I}(V) \supseteq \mathcal{I}(V_1)$. Now we apply $\mathcal{V}$ to both sides to get $V \subseteq V_1$. Thus V is irreducible.

Conversely, suppose V is irreducible and suppose $fg \in \mathcal{I}(V)$ for some $f, g \in K[x_1, \ldots, x_n]$. Then $\langle fg \rangle \subseteq \mathcal{I}(V)$, and after applying $\mathcal{V}$ to both sides, we obtain

$$\begin{aligned}V &\subseteq \mathcal{V}(\langle fg \rangle) \\ &= \mathcal{V}(f) \cup \mathcal{V}(g).\end{aligned}$$

Since V is irreducible, either $\mathcal{V}(f) \supseteq V$ or $\mathcal{V}(g) \supseteq V$. Without loss of generality, say $\mathcal{V}(f) \supseteq V$. Applying $\mathcal{I}$ to both sides, we obtain $f \in \mathcal{I}\mathcal{V}(f) \subseteq \mathcal{I}(V)$. It follows that $\mathcal{I}(V)$ is prime.

Problem 5

Exercise 5. Complete the introductory quiz.

Solution 5. Done.