

1 Polynomial Practice

Note 8

- (a) If f and g are non-zero real polynomials, how many real roots do the following polynomials have at least? How many can they have at most? (Your answer may depend on the degrees of f and g .)
- (i) $f + g$
 - (ii) $f \cdot g$
 - (iii) f/g , assuming that f/g is a polynomial
- (b) Now let f and g be polynomials over $\text{GF}(p)$.
- (i) We say a polynomial $f = 0$ if $\forall x, f(x) = 0$. Show that if $f \cdot g = 0$, it is not always true that either $f = 0$ or $g = 0$.
 - (ii) How many f of degree *exactly* $d < p$ are there such that $f(0) = a$ for some fixed $a \in \{0, 1, \dots, p-1\}$?
- (c) Find a polynomial f over $\text{GF}(5)$ that satisfies $f(0) = 1, f(2) = 2, f(4) = 0$. How many such polynomials of degree at most 4 are there?

Solution:

- (a) (i) It could be that $f + g$ has no roots at all (example: $f(x) = 2x^2 - 1$ and $g(x) = -x^2 + 2$), so the minimum number is 0. However, if the highest degree of $f + g$ is odd, then it has to cross the x -axis at least once, meaning that the minimum number of roots for odd degree polynomials is 1. On the other hand, $f + g$ is a polynomial of degree at most $m = \max(\deg f, \deg g)$, so it can have at most m roots. The one exception to this expression is if $f = -g$. In that case, $f + g = 0$, so the polynomial has an infinite number of roots!
- (ii) A product is zero if and only if one of its factors vanishes. So if $f(x) \cdot g(x) = 0$ for some x , then either x is a root of f or it is a root of g , which gives a maximum of $\deg f + \deg g$ possibilities. Again, there may not be any roots if neither f nor g have any roots (example: $f(x) = g(x) = x^2 + 1$).
- (iii) If f/g is a polynomial, then it must be of degree $d = \deg f - \deg g$ and so there are at most d roots. Once more, it may not have any roots, e.g. if $f(x) = g(x)(x^2 + 1)$, $f/g = x^2 + 1$ has no root.

- (b) (i) There are a couple counterexamples:

Example 1: $x^{p-1} - 1$ and x are both non-zero polynomials on $GF(p)$ for any p . x has a root at 0, and by FLT, $x^{p-1} - 1$ has a root at all non-zero points in $GF(p)$. So, their product $x^p - x$ must have a zero on all points in $GF(p)$.

Example 2: To satisfy $f \cdot g = 0$, all we need is $(\forall x \in S, f(x) = 0 \vee g(x) = 0)$ where $S = \{0, \dots, p-1\}$. We may see that this is not equivalent to $(\forall x \in S, f(x) = 0) \vee (\forall x \in S, g(x) = 0)$.

To construct a concrete example, let $p = 2$ and we enforce $f(0) = 1, f(1) = 0$ (e.g. $f(x) = 1 - x$), and $g(0) = 0, g(1) = 1$ (e.g. $g(x) = x$). Then $f \cdot g = 0$ but neither f nor g is the zero polynomial.

- (ii) We know that in general each of the $d + 1$ coefficients of $f(x) = \sum_{k=0}^d c_k x^k$ can take any of p values. However, the conditions $f(0)$ and $\deg f = d$ impose constraints on the constant coefficient $f(0) = c_0 = a$ and the top coefficient $x_d \neq 0$. Hence we are left with $(p - 1) \cdot p^{d-1}$ possibilities.

- (c) A polynomial of degree ≤ 4 is determined by 5 points (x_i, y_i) . We have assigned three, which leaves $5^2 = 25$ possibilities. To find a specific polynomial, we use Lagrange interpolation:

$$\Delta_0(x) = 2(x-2)(x-4) \quad \Delta_2(x) = x(x-4) \quad \Delta_4(x) = 2x(x-2),$$

and so $f(x) = \Delta_0(x) + 2\Delta_2(x) = 4x^2 + 1$.

2 Lagrange Interpolation in Finite Fields

Note 8

Find a unique polynomial $p(x)$ of degree at most 2 that passes through points $(-1, 3)$, $(0, 1)$, and $(1, 2)$ in modulo 5 arithmetic using the Lagrange interpolation.

- Find $p_{-1}(x)$ where $p_{-1}(0) \equiv p_{-1}(1) \equiv 0 \pmod{5}$ and $p_{-1}(-1) \equiv 1 \pmod{5}$.
- Find $p_0(x)$ where $p_0(-1) \equiv p_0(1) \equiv 0 \pmod{5}$ and $p_0(0) \equiv 1 \pmod{5}$.
- Find $p_1(x)$ where $p_1(-1) \equiv p_1(0) \equiv 0 \pmod{5}$ and $p_1(1) \equiv 1 \pmod{5}$.
- Construct $p(x)$ using a linear combination of $p_{-1}(x)$, $p_0(x)$, and $p_1(x)$.

Solution:

- (a) We see

$$\begin{aligned} p_{-1}(x) &\equiv (x-0)(x-1)((-1-0)(-1-1))^{-1} \\ &\equiv (2)^{-1}x(x-1) \pmod{5} \\ &\equiv 3x(x-1) \pmod{5}. \end{aligned}$$

(b) We see

$$\begin{aligned} p_0(x) &\equiv (x+1)(x-1)((0+1)(0-1))^{-1} \\ &\equiv (-1)^{-1}(x-1)(x+1) \pmod{5} \\ &\equiv 4(x-1)(x+1) \pmod{5}. \end{aligned}$$

(c) We see

$$\begin{aligned} p_1(x) &\equiv (x+1)(x-0)((1+1)(1-0))^{-1} \\ &\equiv (2)^{-1}x(x+1) \pmod{5} \\ &\equiv 3x(x+1) \pmod{5}. \end{aligned}$$

(d) Putting everything together,

$$\begin{aligned} p(x) &= 3p_{-1}(x) + 1p_0(x) + 2p_1(x) \\ &= 9x(x-1) + 4(x-1)(x+1) + 6x(x+1) \\ &\equiv 4x^2 - 3x - 4 \pmod{5} \\ &\equiv 4x^2 + 2x + 1 \pmod{5}. \end{aligned}$$

3 Secrets in the United Nations

Note 8 A vault in the United Nations can be opened with a secret combination $s \in \mathbb{Z}$. In only two situations should this vault be opened: (i) all 193 member countries must agree, or (ii) at least 55 countries, plus the U.N. Secretary-General, must agree.

- (a) Propose a scheme that gives private information to the Secretary-General and all 193 member countries so that the secret combination s can only be recovered under either one of the two specified conditions.
- (b) The General Assembly of the UN decides to add an extra level of security: each of the 193 member countries has a delegation of 12 representatives, all of whom must agree in order for that country to help open the vault. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary-General and to each representative of each country.

Solution:

- (a) Create a polynomial of degree 192 and give each country one point. Give the Secretary General $193 - 55 = 138$ distinct points, so that if she collaborates with 55 countries, they will have a total of 193 points and can reconstruct the polynomial. Without the Secretary-General, the polynomial can still be recovered if all 193 countries come together. (We do all our work in $\text{GF}(p)$ where $p \geq d + 1$).

Alternatively, we could have one scheme for condition (i) and another for (ii). The first condition is the secret-sharing setup we discussed in the notes, so a single polynomial of degree 192 suffices, with each country receiving one point, and evaluation at zero returning the combination s . For the second condition, create a polynomial f of degree 1 with $f(0) = s$, and give $f(1)$ to the Secretary-General. Now create a second polynomial g of degree 54, with $g(0) = f(2)$, and give one point of g to each country. This way any 55 countries can recover $g(0) = f(2)$, and then can consult with the Secretary-General to recover $s = f(0)$ from $f(1)$ and $f(2)$.

- (b) We'll layer an *additional* round of secret-sharing onto the scheme from part (a). If t_i is the key given to the i th country, produce a degree-11 polynomial f_i so that $f_i(0) = t_i$, and give one point of f_i to each of the 12 delegates. Do the same for each country (using different f_i each time, of course).

4 To The Moon!

Note 8 A secret number s is required to launch a rocket, and Alice distributed the values $(1, p(1)), (2, p(2)), \dots, (n+1, p(n+1))$ of a degree n polynomial p to a group of \$GME holders $\text{Bob}_1, \dots, \text{Bob}_{n+1}$. As usual, she chose p such that $p(0) = s$. Bob_1 through Bob_{n+1} now gather to jointly discover the secret. However, **Bob₁ is secretly a partner at Melvin Capital and already knows s , and wants to sabotage $\text{Bob}_2, \dots, \text{Bob}_{n+1}$, making them believe that the secret is in fact some fixed $s' \neq s$.** How could he achieve this? In other words, what value should he report (in terms variables known in the problem, such as s', s or y_1) in order to make the others believe that the secret is s' ?

Solution:

We know that in order to discover s , the Bobs would compute

$$s = y_1 \Delta_1(0) + \sum_{k=2}^{n+1} y_k \Delta_k(0), \quad (1)$$

where $y_i = p(i)$. Bob_1 now wants to change his value y_1 to some y'_1 , so that

$$s' = y'_1 \Delta_1(0) + \sum_{k=2}^{n+1} y_k \Delta_k(0). \quad (2)$$

Subtracting Equation 1 from 2 and solving for y'_1 , we see that

$$y'_1 = (\Delta_1(0))^{-1} (s' - s) + y_1,$$

where $(\Delta_1(0))^{-1}$ exists, because $\deg \Delta_1(x) = n$ with its n roots at $2, \dots, n+1$ (so $\Delta_1(0) \neq 0$).