CS 70 Discrete Mathematics and Probability Theory
Spring 2021 DIS 4B

1 Polynomial Practice

(a) If f and g are non-zero real polynomials, how many 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 GF(p).

(i) We say a polynomial $f = 0$ if $\forall x, f(x) = 0$. If $f \cdot g = 0$, is it 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 $a \in \{0, 1, \ldots, p-1\}$?

(c) Find a polynomial f over GF(5) that satisfies $f(0) = 1, f(2) = 2, f(4) = 0$. How many such polynomials 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 (we did not look for this case when grading). 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) **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 Little Fermat, $x^{p-1}-1$ 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 $S = \{0, \ldots, p-1\}$. 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) We know by part (b) that any polynomial over GF(5) can be of degree at most 4. 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:

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

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

2 Interpolation Practice

Find the lowest degree polynomial with coefficients in $\mathbb{R}$ that passes through the points $(0,0), (1,2)$, and $(2,-1)$. Now do it again in, with coefficients in GF(3).

Solution:

Using Lagrange interpolation, we need to compute first the polynomial $\Delta_0(x)$ satisfying $\Delta_0(0) = 1$, $\Delta_0(1) = 0$, and $\Delta_0(2) = 0$, and then the analogous ones Δ_2 and Δ_3. To do this we'll set

$$\begin{aligned}
\Delta_0(x) &= \big((0-1)(0-2)\big)^{-1}(x-1)(x-2) = 2^{-1}\left(x^2 - 3x + 2\right) \\
\Delta_1(x) &= \big((1-0)(1-2)\big)^{-1}(x-0)(x-2) = (-1)^{-1}\left(x^2 - 2x\right) \\
\Delta_2(x) &= \big((2-0)(2-1)\big)^{-1}(x-0)(x-1) = 2^{-1}\left(x^2 - x\right).
\end{aligned}$$

The polynomial $f(x)$ with real coefficients passing through the points we want will then be

$$f(x) = 0 * \Delta_0(x) + 2 * \Delta_1(x) - 1 * \Delta_2(x) = -\frac{5}{2}x^2 + \frac{9}{2}x.$$

To do this over GF(3), all we need to do is take the polynomial we just computed and reduce it modulo 3. Since $2^2 = 4 \equiv 1 \bmod 3$, 2 is it's own multiplicative inverse, $-5/2 \equiv -10 \equiv 2 \bmod 3$, and we'll get

$$g(x) = 2x^2.$$

3 When the imposter is sus

10 crewmates in Among Us are deciding whether or not to eject an accused impostor (not one of the 10 crewmates) from their spaceship. The ejection mechanism has a password that is protected by a secret sharing scheme that will only allow the crewmates to eject the accused impostor if certain conditions are met. In the following parts, you will explore different secret sharing schemes to fulfill certain requirements.

(a) Design a secret sharing scheme that will allow the crewmates to eject the accused impostor if and only if at least 5 of the crewmates agree to.

(b) Now, 7 of the crewmates have finished their tasks and 3 of the crewmates have not finished their tasks and you are more inclined to trust the judgement of crewmates who have finished their tasks. Design a secret sharing scheme that will allow the crewmates to eject the accused impostor if and only if **either** at least 3 of the crewmates who finished their tasks agree **or** at least 5 out of all the crewmates agree. Assume that you know which crewmates have finished their tasks and which ones have not beforehand.

(c) The crewmates have decided to split up into groups as they wander around their spaceship to more effectively keep tabs on when the imposter is sus. In particular, 4 of them go to Electrical, 5 of them go to Communications, and 1 stays in Admin. Design a secret sharing scheme that will allow the crewmates to eject the accused impostor if and only if all of the crewmates in one group agree **and** at least one crewmate from another group agrees.

Solution: Solutions may vary.

(a) We can construct a degree 4 polynomial p such that $p(0)$ is the password. We can then distribute one unique point on the polynomial that is not $p(0)$ to each crewmate.

(b) **Solution 1**

We can model this scheme as a system of inequalities to give some intuition on how we might designate the degree of the secret polynomial and the points to give. Denote the degree of the secret polynomial as d and the number of points given to each crewmate who has finished their tasks and each crewmate who has not finished their tasks as x and y, respectively. Our strategy will involve giving more points to crewmates who finished their tasks, i.e. $x > y$, as each of those individual crewmates should be able to contribute more progress to the number of points needed to interpolate. The first constraint can be represented as $3x > d$. For the next constraint, if we adhere to our strategy, the lowest number of points that could involve at least 5 of the crewmates will be the case involving all 3 of those who did not finish their tasks and 2 who did, giving us a constraint of $2x + 3y > d$. Finally, we must ensure that no other configuration of agreements can unlock the secret; the most amount of points that could be collected by any group that does not satisfy either constraint will be the group consisting of 2 crewmates who finished their tasks and 2 who did not, giving us the constraint of $2x + 2y \leq d$. Putting this all

together, we are looking for some $x, y, d \in \mathbb{N}$ that satisfy:

$$\begin{aligned} 3x &> d \\ 2x + 3y &> d \\ 2x + 2y &\leq d \end{aligned}$$

After some experimentation, we realize $x = 5, y = 2, d = 14$ is satisfying assignment, i.e. we can construct a degree 14 polynomial and we will give 5 points to each of the 7 crewmates who have finished their tasks and 2 points to each of the other 3 crewmates who have not finished their tasks.

Solution 2

Another way to approach this problem is to create two different polynomials, one for both possible satisfaction conditions (either 5 crewmates or 3 who have completed their tasks). This way, we can treat the setup as 2 entirely different problems. To allow any 5 crewmates to come together, we can create a degree 4 polynomial and give a distinct point to every crewmate. For the crewmates that have already completed their tasks, we create a degree 2 polynomial and give a distinct point to said crewmates. Lastly, construct both polynomials such that they have the same secret.

(c) We construct 3 polynomials for each group e, c, a for Electrical, Communications, and Admin, respectively, such that $e(0) = c(0) = a(0)$ all yield the secret. Define e to be degree 4, c to be degree 5, and a to be degree 1 and give each crewmate in the Electrical group a different point on e and likewise for the Communications and Admin groups. Finally, give one particular point on e to all crewmates in the Communications and Admin groups, one particular point on c to all crewmates in the Electrical and Admin groups, and one particular point on a to all crewmates in the Electrical and Communications groups.

Now, notice that in order for any of the polynomials to get interpolated, all members of one group must agree and at least one member of another group must agree, as only then will enough points on a polynomial will be revealed. For example, if all of Electrical agrees and one member of Communications agrees, they will have $4 + 1 = 5$ unique points points on e and can interpolate it. However, if only 3 members of Electrical agree and 1 member from both Communications and Admin agree, they will only have $3 + 1 = 4$ unique points, since the Communications and Admin members are given the same point on e, and will be unable to interpolate.

4 To The Moon!

A secret number s is required to launch a rocket, and Alice distributed the values $(1, p(1)), (2, p(2)), \ldots, (n+1, p(n+1))$ of a degree n polynomial p to a group of \$GME holders $\text{Bob}_1, \ldots, \text{Bob}_{n+1}$. As usual, she chose p such that $p(0) = s$. Bob_1 through Bob_{n+1} now gather to jointly discover the secret. However, Bob_1 is secretly a partner at Melvin Capital and already

knows s, and wants to sabotage $\text{Bob}_2, \ldots, \text{Bob}_{n+1}$, 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 order to make the others believe that the secret is s'?

Solution:

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

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

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

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

Subtracting Equation 1 from 2 and solving for y_1', we see that

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

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