CS 70 Discrete Mathematics and Probability Theory
Summer 2020 Course Notes **DIS 3C**

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 $a \in \{0,1,\dots,p-1\}$?

(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 $S=\{0,\dots,p-1\}$. 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 $f(x)=\sum_{k=0}^{d}c_kx^k$ 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 Rational Root Theorem

The rational root theorem states that for a polynomial

$$P(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0,$$

$a_0,\cdots,a_n\in\mathbb{Z}$, if $a_0,a_n\neq 0$, then for each rational solution $\frac{p}{q}$ such that $\gcd(p,q)=1$, $p|a_0$ and $q|a_n$. Prove the rational root theorem.

Solution: If $\frac{p}{q}$ is a root of the polynomial P, we can write

$$P\left(\frac{p}{q}\right)=a_n\left(\frac{p}{q}\right)^n+\cdots+a_1\left(\frac{p}{q}\right)+a_0=0.$$

Multiplying both sides by q^n we get

$$p(a_np^{n-1}+a_{n-1}qp^{n-1}+\cdots+a_1q^{n-1})=-a_0q^n$$

From this we can see that p divides a_0q^n; however, recall that p and q are coprime, so p must divide a_0, as desired.

If instead we chose to factor out q, we have

$$q(a_{n-1}p^{n-1}+\cdots+a_0q^{n-1})=-a_np^n$$

and for the same reasons we can say that q divides a_n.

3 Secrets in the United Nations

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 $193-55=138$ points, so that if she collaborates with 55 countries, they will have a total of 192 points and can reconstruct the polynomial. Without the Secretary-General, the polynomial can still be recovered if all 192 countries come together. (We do all our work in 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 ith 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 Old Secrets, New Secrets

In order to share a secret number s, Alice distributed the values $(1,p(1)),(2,p(2)),\dots,(n+1,p(n+1))$ of a degree n polynomial p with her friends $\text{Bob}_1,\dots,\text{Bob}_{n+1}$. As usual, she chose p such that $p(0)=s$. Bob_1 through Bob_{n+1} now gather to jointly discover the secret. Suppose that for some reason Bob_1 already knows s, and wants to play a joke on $\text{Bob}_2,\dots,\text{Bob}_{n+1}$, 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 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 $\Delta_1(0) \neq 0$).