CS 70 Discrete Mathematics and Probability Theory
Fall 2019 Alistair Sinclair and Yun S. Song

DIS 5

1 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 $\mathrm{GF}(3)$.

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

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

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

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

2 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 $192-55=137$ 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.

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).

3 Where Are My Packets?

Alix wants to send the message (a_0,a_1,a_2) to Bo, where each $a_i \in \{0,1,2,3,4\}$. She encodes this message using a polynomial f of degree ≤ 2 over GF(5) with the property that $f(0)=a_0$, $f(1)=a_1$, and $f(2)=a_2$, and she sends the packets $(0,f(0))$, $(1,f(1))$, $(2,f(2))$, $(3,f(3))$, $(4,f(4))$. Two packets are dropped, and Bob only learns that $f(0)=4$, $f(3)=1$, and $f(4)=2$. Help Bo recover Alix's message!

(a) Find the multiplicative inverses of 1, 2, 3, and 4 modulo 5.

(b) Find the original polynomial f, either by using Lagrange interpolation or solving a system of linear equations.

(c) Recover Alix's original message.

Solution:

(a) Inverse pairs modulo 5: $(1,1),(2,3),(4,4)$.

(b) Let's do it first with Lagrange interpolation; note that we work in GF(5), so $1/a \pmod 5$

means $a^{-1} \pmod 5$.

$$\begin{aligned}
\Delta_0(x) &= \frac{(x-3)(x-4)}{(0-3)(0-4)} \\
&= \frac{x^2-7x+12}{(-3)(-4)} \\
&\equiv (x^2-7x+12)(-2)(-4) \pmod 5 \\
&\equiv 3(x^2+3x+2) \pmod 5 \\
&\equiv 3x^2+4x+1 \pmod 5 \\
\Delta_3(x) &= \frac{(x-0)(x-4)}{(3-0)(3-4)} \\
&= \frac{x^2-4x}{(3)(-1)} \\
&\equiv (x^2-4x)(2)(-1) \pmod 5 \\
&\equiv 3(x^2+x) = 3x^2+3x \pmod 5 \\
\Delta_4(x) &= \frac{(x-0)(x-3)}{(4-0)(4-3)} \\
&= \frac{x^2-3x}{(4)(1)} \\
&\equiv (x^2-3x)(4)(1) \pmod 5 \\
&\equiv 4(x^2+2x) = 4x^2+3x \pmod 5
\end{aligned}$$

Thus, our original polynomial f is

$$\begin{aligned}
4\Delta_0(x)+1\Delta_3(x)+2\Delta_4(x) &= 4(3x^2+4x+1)+(3x^2+3x)+2(4x^2+3x) \\
&\equiv (2x^2+x+4)+(3x^2+3x)+(3x^2+x) \pmod 5 \\
&\equiv 3x^2+4 \pmod 5.
\end{aligned}$$

Alternatively, we can write $f(x) = m_2x^2+m_1x+m_0$, and the following system of linear equations to find the m_i's:

$$\begin{bmatrix} 0 & 0 & 1 \\ 9 & 3 & 1 \\ 16 & 4 & 1 \end{bmatrix} \begin{bmatrix} m_2 \\ m_1 \\ m_0 \end{bmatrix} = \begin{bmatrix} 4 \\ 1 \\ 2 \end{bmatrix}.$$

This gives

$$f(x) = \frac{1}{2}x^2 - \frac{5}{2}x + 4 \equiv 3x^2+4 \pmod 5.$$

(c) To recover (a_0, a_1, a_2), we compute

$$\begin{aligned}
P(1) &= 2, \\
P(2) &= 1.
\end{aligned}$$

In other words, the message that Alix's transmitted was 42112, consisting of the message 421 plus the two characters 12 from the error correcting scheme.

4 Prime Polynomials

A polynomial $f(x)$ is called *prime* if it has degree at least 1 and it is not possible to write it as $f(x) = g(x)h(x)$, where g and h both have smaller degree than f. Prove that there are infinitely many prime polynomials with coefficients in GF(q). You may want to review the proof that there are infinitely many prime numbers, and it may in addition be helpful to prove that every polynomial is either prime or can be written as a product of prime polynomials.

Solution:

This proof is in the same spirit as the proof that there are infinitely many prime numbers. First, if $f(x)$ is any polynomial, we claim that either $f(x)$ is prime or it can be written as a product of prime polynomials. Let's do this by strong induction on the *degree* of $f(x)$. As a base case, every degree one polynomial is prime: if we could write $x - a = g(x)h(x)$, then the degree of one of g or h must be zero, and consequently the degree of the other must be one. Now, assume that every polynomial of degree $1, \ldots, k$ can be written as a product of prime polynomials, and let $f(x)$ have degree $k+1$. Either $f(x)$ is prime, or we can write it as $f(x) = g(x)h(x)$ for g and h of degree at most k. But both p and q can be written as a product of primes, so we are done.

Assume, seeking a contradiction, that there are only finitely many primes $p_1(x), p_2(x), \ldots, p_k(x)$, and consider the polynomial

$$f(x) = p_1(x)p_2(x)\cdots p_k(x) + 1.$$

It cannot be that $f(x)$ is prime, because it has degree larger than any of $p_1(x), \ldots, p_k(x)$. On the other hand, we can write it as a product of prime polynomials, so it must be that $p_i(x)$ divides $f(x)$ for some i. In other words,

$$p_i(x)q(x) = f(x) = p_1(x)\cdots p_i(x)\cdots p_k(x) + 1,$$

and we can rearrange to see that

$$p_i(x)\left(q(x) - p_1(x)\cdots p_{i-1}(x)p_{i+1}(x)\cdots p_k(x)\right) = 1.$$

But this is impossible because $p_i(x)$ has degree at least one. Since we've found a contradiction, there must be infinitely many prime polynomials.