CS 70 Discrete Mathematics and Probability Theory
Spring 2017 Rao

DIS 5a

1 Erasure Warm-Up

Working over GF(q), you want to send your friend a message of $n = 4$ packets and guard against 2 lost packets. What is the minimum q you can use? What is the maximum degree of the unique polynomial that describes your message?

Solution:

To guard against 2 lost packets, you want to send $4+2=6$ packets. Since we want q prime, the minimum it can be is 7. Since you have 4 points, your polynomial needs to be degree 3.

Note: Encoding our message in GF(7) requires that our message is not larger than 6.

2 Lagrange Interpolation

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

(a) Find $\Delta_{-1}(x)$ where $\Delta_{-1}(0) = \Delta_{-1}(1) = \Delta_{-1}(2) = 0$ and $\Delta_{-1}(-1) = 1$.

(b) Find $\Delta_0(x)$ where $\Delta_0(-1) = \Delta_0(1) = \Delta_0(2) = 0$ and $\Delta_0(0) = 1$.

(c) Find $\Delta_1(x)$ where $\Delta_1(-1) = \Delta_1(0) = \Delta_1(2) = 0$ and $\Delta_1(1) = 1$.

(d) Find $\Delta_2(x)$ where $\Delta_2(-1) = \Delta_2(0) = \Delta_2(1) = 0$ and $\Delta_2(2) = 1$.

(e) Reconstruct $p(x)$ by using a linear combination of $\Delta_{-1}(x)$, $\Delta_0(x)$, $\Delta_1(x)$, and $\Delta_2(x)$.

Solution:

(a)

$$\Delta_{-1}(x) = \frac{x(x-1)(x-2)}{(-1-0)(-1-1)(-1-2)} = \frac{x(x-1)(x-2)}{-6}$$

(b)

$$\Delta_0(x) = \frac{(x+1)(x-1)(x-2)}{(0+1)(0-1)(0-2)} = \frac{(x+1)(x-1)(x-2)}{2}$$

(c)

$$\Delta_1(x) = \frac{(x+1)(x)(x-2)}{(1+1)(1)(1-2)} = \frac{(x+1)(x)(x-2)}{-2}$$

(d)

$$\Delta_2(x) = \frac{(x+1)(x)(x-1)}{(2+1)(2)(2-1)} = \frac{(x+1)(x)(x-1)}{6}$$

(e) We don't need $\Delta_2(x)$.

$$\begin{aligned} p(x) &= 3\cdot\Delta_{-1}(x) + 1\cdot\Delta_0(x) + 2\cdot\Delta_1(x) + 0\cdot\Delta_2(x) \\ &= -\frac{1}{2}x(x-1)(x-2) + \frac{1}{2}(x+1)(x-1)(x-2) + (-1)x(x+1)(x-2) \\ &= -x^3 + \frac{3}{2}x^2 + \frac{1}{2}x + 1 \end{aligned}$$

3 Where Are My Packets?

Alice wants to send the message (a_0, a_1, a_2) to Bob, where each $a_i \in \{0,1,2,3,4\}$. She encodes it as a polynomial P of degree ≤ 2 over GF(5) such that $P(0) = a_0$, $P(1) = a_1$, and $P(2) = a_2$, and she sends the packets $(0, P(0))$, $(1, P(1))$, $(2, P(2))$, $(3, P(3))$, $(4, P(4))$. Two packets are dropped, and Bob only learns that $P(0) = 4$, $P(3) = 1$, and $P(4) = 2$. Help Bob recover Alice's message.

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

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

(c) Recover Alice's original message.

Solution:

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

(b) Note that we work in GF(5), so $1/x \pmod 5$ means $x^{-1} \pmod 5$.

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

Thus, our original polynomial P is

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

Linear equation way: Writing $P(x) = m_2x^2 + m_1x + m_0$, we solve for the m_i's by solving the linear equation

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

This gives the equation

$$\frac{1}{2}x^2 - \frac{5}{2}x + 4,$$

which, in the modulo 5 world, means $P(x) = 3x^2 + 4$.

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

$$\begin{aligned}P(0) &= 4, \\ P(1) &= 2, \\ P(2) &= 1.\end{aligned}$$

4 Secrets in the United Nations

The United Nations (for the purposes of this question) consists of n countries, each having k representatives. A vault in the United Nations can be opened with a secret combination s. The vault should only be opened in one of two situations. First, it can be opened if all n countries in the UN help. Second, it can be opened if at least m countries get together with the Secretary General of the UN.

(a) Propose a scheme that gives private information to the Secretary General and n countries so that 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: in order for a country to help, all of the country's k representatives must agree. 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 $n-1$ and give each country one point. Give the Secretary General $n-m$ points, so that if he collaborates with m countries, they will have $n-m+m=n$ points and can reconstruct the polynomial. Without the General, n countries can come together and also recover the polynomial. No combination of the General with fewer than m countries can recover the polynomial.

Alternatively:

Have two schemes, one for the first condition and one for the second.

For the first condition: just one polynomial of degree $\leq n-1$ would do, where each country gets one point. The polynomial evaluated at 0 would give the secret.

For the second condition: one polynomial is created of degree $m-1$ and a point is given to each country. Another polynomial of degree 1 is created, where one point is given to the secretary general and the second point can be constructed from the first polynomial if m or more of the countries come together. With these two points, we have a unique 1-degree polynomial, which could give the secret evaluated at 0.

(b) The scheme in part (a) remains the same, but instead of directly giving each country a point on the $n-1$ degree polynomial to open the vault, construct an additional polynomial for each country that will produce that point.

Each country's polynomial has degree $k-1$, and a point is given to each of the k representatives of the country. Thus, when they all get together they can produce a point for either of the schemes.