CS 70 Discrete Mathematics and Probability Theory
Fall 2026 Hug, Sabin

DIS 4

Polynomials Intro

Note 8

Polynomial: $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$; in terms of roots, $f(x) = a(x-r_1)(x-r_2)\cdots(x-r_k)$

Degree of a polynomial: the highest exponent in the polynomial

Galois Field: denoted as GF(p), it's basically just a fancy way of saying that we're working modulo p, for a prime p

Properties (true over $\mathbb{R}$ and also over GF(p)):

- Polynomial of degree d has at most d roots.
- Exactly one polynomial of degree at most d passes through $d+1$ points.

Lagrange Interpolation: Given $d+1$ points (x_1, y_1), (x_2, y_2), …, (x_{d+1}, y_{d+1}), we define

$$\Delta_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}, \quad i = 1, 2, \ldots d+1.$$

The unique polynomial through all points is $f(x) = \sum_{i=1}^{d+1} y_i \cdot \Delta_i(x)$.

1 Polynomial Fill in the Blank

Note 8

Fill in each blank, and provide a brief justification.

(a) A degree d nonzero polynomial over $\mathbb{R}$ has at most ____ roots.

(b) A degree d nonzero polynomial over GF(p) has at most min(____, p) roots.

(c) d distinct points determine a unique polynomial of degree at most ____.

(d) For every prime p, every polynomial over GF(p) with degree $\geq p$ is equivalent to a polynomial of degree at most ____. (Two polynomials are equivalent if they evaluate to the same value for every $x \in \text{GF}(p)$.)

2 How Many Polynomials?

Note 8

Let $P(x)$ be a polynomial of degree at most 2 over GF(5). As we saw in lecture, we need $d+1$ distinct points to determine a unique polynomial of degree at most d, so knowing the values for say, $P(0)$, $P(1)$, and $P(2)$ would be enough to recover P. (For this problem, we consider two polynomials to be distinct if they return different values for some input.)

(a) Assume that we know $P(0) = 1$, and $P(1) = 2$. Now consider $P(2)$. How many values can $P(2)$ have? How many distinct possibilities for P do we have?

(b) Now assume that we only know $P(0) = 1$. We consider $P(1)$ and $P(2)$. How many different $(P(1), P(2))$ pairs are there? How many distinct possibilities for P do we have?

(c) Now, let P be a polynomial of degree at most d on GF(p) for some prime p with $p > d$. Assume we only know P evaluated at $k \leq d+1$ different values. How many different possibilities do we have for P?

3 Lagrange Interpolation in Finite Fields

Note 8

In this problem, we will break down the terms of Lagrange interpolation by working through an example, where we want to 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.

(a) First, assume we have polynomials $\Delta_{-1}(x)$, $\Delta_0(x)$, and $\Delta_1(x)$ satisfying the following congruences modulo 5:

$$\begin{aligned} \Delta_{-1}(-1) &\equiv 1, & \Delta_{-1}(0) &\equiv 0, & \Delta_{-1}(1) &\equiv 0, \\ \Delta_0(-1) &\equiv 0, & \Delta_0(0) &\equiv 1, & \Delta_0(1) &\equiv 0, \\ \Delta_1(-1) &\equiv 0, & \Delta_1(0) &\equiv 0, & \Delta_1(1) &\equiv 1. \end{aligned}$$

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

(*Note*: Notice that for the Δ_i's in this question, the subscript i refers to an actual value of x.)

(b) Find $\Delta_{-1}(x)$. In other words, find a degree 2 polynomial that has roots at $x = 0$ and $x = 1$ and evaluates to 1 at $x = -1$ (all in modulo 5).

(c) Find $\Delta_0(x)$.

(d) Find $\Delta_1(x)$.

(e) Now, let's put it all together! Find $p(x)$ by using your linear combination in part (a) and your polynomials constructed above.

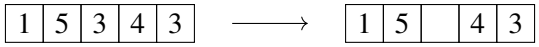
(f) How does performing Lagrange interpolation over GF(p) differ from interpolation over $\mathbb{R}$?

Error Correcting Codes and Secret Sharing Intro

Note 8
Note 9

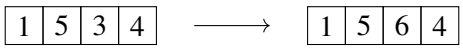
Secret Sharing: We make use of the fact that there is a unique polynomial of degree d passing through a given set of $d+1$ points. This means that if we require k people to come together in order to find a secret, we should use a polynomial of degree $k-1$, and give each person one point. There are more complicated schemes if there are more conditions, but they all use the same concept.

Erasure errors: A packet/point $(x, P(x))$ is *lost* in the communication channel.



Protection: (n packets, k errors) interpolate polynomial through the message points, send $n+k$ packets on the polynomial

General errors: A packet is *modified* in the communication channel.



Protection: (n packets, k errors) interpolate polynomial through the message points, send $n+2k$ packets on the polynomial

Berlekamp–Welch Algorithm:

Variables: sent message packets m_i, received packets r_i, error locations e_i

Polynomials:

- $P(x)$: original polynomial through message (this is what we want)
- $E(x) = (x-e_1)(x-e_2)\cdots(x-e_k)$: error locator polynomial
- $Q(x) = P(x)E(x)$, or $Q(i) = P(i)E(i) = r_iE(i)$ for all i

$Q(x)$ and $E(x)$ are unknown, but we can solve for them using a system of equations.

4 Berlekamp-Welch Warm Up

Note 9

Suppose you want to send a length-n message over an unreliable channel. You obtain $P(x)$, the polynomial that passes through your message packets.

(a) What is the degree of $P(x)$? Why?

(b) If there are at most k erasure errors, how many packets should you send? If there are at most k general errors, how many packets should you send?

Suppose the unreliable channel can corrupt up to k general errors, and you send an appropriate number of packets based on part (b). Your recipient uses Berlekamp-Welch to correct the general errors.

(c) What do the roots of the error polynomial $E(x)$ represent? Does your recipient know these roots?

(d) When does $r_i = P(i)$? When does r_i not equal $P(i)$? Using these two cases, prove that $Q(i) = P(i)E(i) = r_iE(i)$ for each received packet index i.

(e) What is the maximum degree of $E(x)$? Using the information about the degree of $E(x)$ and $P(x)$ from part (a), what is the maximum degree of $Q(x)$?

(f) How many unknown coefficients are there in total across $Q(x)$ and $E(x)$?

Upon knowing the degrees of $Q(x)$ and $E(x)$, your recipient writes the equation $Q(i) = r_i E(i)$ for each received packet.

(g) How many equations does your recipient have? Do they have enough equations to solve for all of the unknown coefficients?

(h) Your recipient obtains $Q(x)$ and $E(x)$. How do they recover $P(x)$ and the original message?

5 Berlekamp-Welch Algorithm

Note 9

Steve wants to send you a message $(m_0, m_1, m_2) = (1, 1, 4)$ of length $n = 3$, using an error-correcting code for $k = 1$ general error, doing arithmetic over GF(5).

[*Note*: The packet indices for this problem begin with 0, not 1.]

(a) Steve constructs a polynomial $P(x) \pmod 5$ of degree at most 2, so that

$$P(0) = 1, \qquad P(1) = 1, \qquad P(2) = 4.$$

Find $P(x)$, and determine the codeword $(c_0, c_1, c_2, c_3, c_4)$ that Steve transmits.

You receive the message $(0,1,4,0,4)$ from Steve, knowing that one packet was corrupted. (Recall that since you're the recipient, you do not know the original message and $P(x)$.)

(b) Write, but do not solve, the system of linear equations that you will use in the Berlekamp-Welch algorithm to find $Q(x)$ and $E(x)$.

(c) You solve the system of equations you wrote in part (b) to obtain $Q(x) = 4x^3 + x^2 + x$ and $E(x) = x$. How do you recover the original message from $Q(x)$ and $E(x)$?

6 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.