1 Polynomials Intro

Note 8

Polynomial: $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$; 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 $\mathrm{GF}(p)$, 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 $\mathrm{GF}(p)$):

- 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 $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$, we define

$$\Delta_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}.$$

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

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.

(a) Consider the $\Delta_i(x)$ polynomials in Lagrange interpolation. What is the value of $\Delta_i(x)$ for $x = x_i$, and what is its value for $x = x_j$, where $j \neq i$? How is this similar to the process of computing a solution with CRT?

(b) If we perform Lagrange interpolation over $\mathrm{GF}(p)$ instead of over $\mathbb{R}$, what is different?

2 Polynomial Practice

(a) If f and g are non-zero real polynomials, how many real 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 $\mathrm{GF}(p)$.

    (i) We say a polynomial $f = 0$ if $\forall x, f(x) = 0$. Show that if $f \cdot g = 0$, it is not always 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 $\mathrm{GF}(5)$ that satisfies $f(0) = 1, f(2) = 2, f(4) = 0$. How many such polynomials of degree at most 4 are there?

3 Lagrange Interpolation in Finite Fields

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 $p_{-1}(x)$, $p_0(x)$, and $p_1(x)$ satisfying:

$$p_{-1}(0) \equiv p_{-1}(1) \equiv 0 \pmod 5; \quad p_{-1}(-1) \equiv 1 \pmod 5$$
$$p_0(-1) \equiv p_0(1) \equiv 0 \pmod 5; \quad p_0(0) \equiv 1 \pmod 5$$
$$p_1(-1) \equiv p_1(0) \equiv 0 \pmod 5; \quad p_1(1) \equiv 1 \pmod 5$$

Construct $p(x)$ using a linear combination of $p_{-1}(x)$, $p_0(x)$, and $p_1(x)$.

(b) Find $p_{-1}(x)$. 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 $p_0(x)$.

(d) Find $p_1(x)$.

(e) Now, lets put it all together! Create a suitable polynomial $p(x)$ by using the linear combination and polynomials constructed above.