1 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), $\ldots$, (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 GF(p) instead of over $\mathbb{R}$, what is different?

Solution:

(a) Here, we have $\Delta_i(x_i) = 1$, whereas $\Delta_i(x_j) = 0$ for $i \neq j$.

This is very similar to how we computed the b_i's in CRT. Recall how we defined b_i such that $b_i \equiv 1 \pmod{m_i}$, but $b_i \equiv 0 \pmod{m_j}$ for $j \neq i$. The reason why we defined the b_i's this way is so that we can compute a solution to exactly one of the equations in the system, while not affecting any of the others.

The Δ_i's here serve the exact same purpose, as a polynomial that passes through exactly one of the points, and does not affect the value at any of the other points.

(b) The only difference is that we no longer have any division; we use the modular inverse instead. The definition of $\Delta_i(x)$ becomes

$$\Delta_i(x) = \left(\prod_{j \neq i}(x - x_j)\right)\left(\prod_{j \neq i}(x_i - x_j)\right)^{-1} \pmod{p}.$$

2 Polynomial Practice

Note 8

(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?

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. 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) There are a couple counterexamples:

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 FLT, $x^{p-1}-1$ 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 $f(x) = \sum_{k=0}^{d} c_k x^k$ 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) 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 $f(x) = \Delta_0(x) + 2\Delta_2(x) = 4x^2 + 1$.

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

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

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.

Solution:

(a) We know that each respective $p_n(x)$ will be 1 when $x = n$, and 0 at the two other relevant points. Thus, $p(x)$ can be created by a linear combination of $p_n(x)$'s multiplied by the required y value at $x = n$. Giving $p(x) = 3p_{-1}(x) + 1p_0(x) + 2p_1(x)$

(b) We see

$$\begin{aligned} p_{-1}(x) &\equiv (x-0)(x-1)\big((-1-0)(-1-1)\big)^{-1} \\ &\equiv (2)^{-1}x(x-1) \pmod 5 \\ &\equiv 3x(x-1) \pmod 5. \end{aligned}$$

(c) We see

$$\begin{aligned} p_0(x) &\equiv (x+1)(x-1)\big((0+1)(0-1)\big)^{-1} \\ &\equiv (-1)^{-1}(x-1)(x+1) \pmod 5 \\ &\equiv 4(x-1)(x+1) \pmod 5. \end{aligned}$$

(d) We see

$$\begin{aligned} p_1(x) &\equiv (x+1)(x-0)\big((1+1)(1-0)\big)^{-1} \\ &\equiv (2)^{-1}x(x+1) \pmod 5 \\ &\equiv 3x(x+1) \pmod 5. \end{aligned}$$

(e) Putting everything together,

$$\begin{aligned} p(x) &= 3p_{-1}(x) + 1p_0(x) + 2p_1(x) \\ &= 9x(x-1) + 4(x-1)(x+1) + 6x(x+1) \\ &\equiv 4x^2 - 3x - 4 \pmod 5 \\ &\equiv 4x^2 + 2x + 1 \pmod 5. \end{aligned}$$