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), ..., (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?

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 $S = \{0, \ldots, p-1\}$. 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) Find $p_{-1}(x)$ where $p_{-1}(0) \equiv p_{-1}(1) \equiv 0 \pmod 5$ and $p_{-1}(-1) \equiv 1 \pmod 5$. 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).

(b) Find $p_0(x)$ where $p_0(-1) \equiv p_0(1) \equiv 0 \pmod 5$ and $p_0(0) \equiv 1 \pmod 5$.

(c) Find $p_1(x)$ where $p_1(-1) \equiv p_1(0) \equiv 0 \pmod 5$ and $p_1(1) \equiv 1 \pmod 5$.

Note that $p_{-1}(x), p_0(x), p_1(x)$ correspond to the $\Delta_1(x), \Delta_2(x), \Delta_3(x)$ terms in the Lagrange interpolation formula for points $x_1 = -1, x_2 = 0, x_3 = 1$ respectively.

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

Solution:

(a) We see

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

(b) We see

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

(c) We see

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

(d) Putting everything together,

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

4 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.

Solution:

(a) Create a polynomial of degree 192 and give each country one point. Give the Secretary General $193-55=138$ distinct points, so that if she collaborates with 55 countries, they will have a total of 193 points and can reconstruct the polynomial. Without the Secretary-General, the polynomial can still be recovered if all 193 countries come together. (We do all our work in $\mathrm{GF}(p)$ for some large prime $p \geq\geq 1+193+138$, since we need to distribute a point to each of the countries, 138 points to the Secretary General, and one point for the secret).

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).