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

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

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

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.

1 Intro to Lagrange Interpolation

Note 8

(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) Instead of performing Lagrange interpolation over $\mathbb{R}$, let us interpolate over $\mathrm{GF}(p)$. What can we no longer take for granted when working in $\mathrm{GF}(p)$, and what should we do instead?

2 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:

$$\begin{aligned}
\Delta_{-1}(0) \equiv \Delta_{-1}(1) \equiv 0 \pmod 5;\ \ \Delta_{-1}(-1) \equiv 1 \pmod 5\\
\Delta_{0}(-1) \equiv \Delta_{0}(1) \equiv 0 \pmod 5;\ \ \Delta_{0}(0) \equiv 1 \pmod 5\\
\Delta_{1}(-1) \equiv \Delta_{1}(0) \equiv 0 \pmod 5;\ \ \Delta_{1}(1) \equiv 1 \pmod 5
\end{aligned}$$

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

3 Polynomial Practice

Note 8

(a) Suppose that f and g are non-zero real polynomials. For each of the following identities, prove that it is true for all such f and g, or give a counterexample.

(i) $\deg(f+g) = \max(\deg f, \deg g)$.

(ii) $\deg(f \cdot g) = \deg f + \deg g$.

(iii) If f/g is a polynomial, then $\deg(f/g) = \deg f - \deg g$.

(b) Now let f be a polynomial over $\mathrm{GF}(p)$.

(i) Let $d < p$ be a fixed degree, and let $c \in \{0, 1, \ldots, p-1\}$ also be fixed. How many f of degree *exactly* d are there such that $f(0) = c$ for some fixed c?

(ii) Suppose $p = 5$. How many f of degree *at most* 4 are there that satisfy $f(0) = 1, f(2) = 2, f(4) = 0$? (For additional practice, find such an f of degree 2.)

(c) Now let f and g be polynomials over $\mathrm{GF}(p)$. 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 $g = 0$.

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.