Outline

Lagrange interpolation

secret sharing scheme

Roots of polynomial over F

Observations

① If $f(x) \in F[X]$ has degree 1, how many roots can f have?

$f(x) = ax+b$, $a \neq 0$, $a, b \in F$

If r is a root, then $f(r) = ar+b = 0$

$$r = \frac{-b}{a}$$

Answer: One root.

② Let $f(x) = x^2+1$, a polynomial over degree 2.
How many roots of f can they be?

$f(x) \in \mathbb{C}[x]$, roots are i, $-i$

$f(x) \in \mathbb{R}[x]$, no root

$f(x) \in \mathbb{F}_2[x]$, root is 1,

Theorem

A polynomial of degree d over a field can have at most d roots.

Corollary (0-polynomial)

If $p(x) \in F[x]$ is of degree at most d but has at least $d+1$ roots, then $p(x) = 0$

Proof: (Homework)

Hint: proof by induction over the degree of the polynomial

Interpolation

"Given points $(a_1, b_1), (a_2, b_2), \ldots, (a_{d+1}, b_{d+1})$

find a polynomial $f(x)$ such that $f(x)$ fits

the points".

$a_i, b_i \in F$, $a_1, a_2, \ldots, a_{d+1}$ distinct

Find $f(x) \in F[x]$ such that

$f(a_i) = b_i$

and $\text{degree}(f) \leq d$

Q1: For any $d+1$ pairs of points, does there exist $f \in F[x]$ that fits these points?

Q2: Could there be more than one polynomial that fit these points?

Theorem: There exists at most one $f(x) \in F[x]$ that interpolates $(a_1, b_1), \dots, (a_{d+1}, b_{d+1})$. where $dg(f) \leq d$

$(a_1, b_1), \dots, (a_{d+1}, b_{d+1})$ a_i are distinct.

suppose $f(x), g(x) \in F[x]$ fit these points.

and degree(f), degree$(g) \leq d$.

$h(x) = f(x) - g(x)$

$h(a_i) = f(a_i) - g(a_i) = b_i - b_i = 0$

h will have $d+1$ roots $(a_1, a_2, \dots, a_{d+1})$

degree of $h(x) \leq d$.

By corollary (0-polynomial), $h(x) = 0$

$\therefore f(x) = g(x)$

Remark: The theorem fails when F is not a field.

$f(x) = 3x \in \mathbb{Z}_6[x]$

roots: $0, 2, 4$

degree $f = 1$

Lagrange Interpolation

Construct $f(x) \in F[x]$ that

interpolates $(a_1, b_1), \dots, (a_{d+1}, b_{d+1})$.

where $a_i, b_i \in F$, $a_1, \dots a_{d+1}$ are distinct

degree $(f) \le d$

Find $c_d, c_{d-1}, \dots, c_0 \in F$ s.t

$f(x) = c_d x^d + c_{d-1} x^{d-1} + \dots + c_0$

such that

$f(a_i) = b_i$

Special case 1

$f(a_1) = 1$

$f(a_i) = 0 \quad \forall i \neq 1 \Rightarrow a_2, \dots, a_{d+1}$ are the roots

---

Let $f_1(x) = (x - a_2)(x - a_3) \dots (x - a_{d+1})$

Then $f_1(a_i) = 0, \ i \ge 2$

$f_1(a_1) = (a_1 - a_2)(a_1 - a_3) \dots (a_1 - a_{d+1})$

So, $f(x) = \dfrac{f_1(x)}{f_1(a_1)}$

Special case 2

$f(a_2) = 1$

$f(a_i) = 0 \quad i \neq 2$

So, $f(x) = \dfrac{f_2(x)}{f_2(a_2)}$

where $f_2(x) = (x-a_1)(x-a_3)(x-a_4) \cdots (x-a_{d+1})$

In general,

Let $g_i(x) = \dfrac{f_i(x)}{f_i(a_i)}$

Where $f_i(x) = \prod_{\substack{1 \leq j \leq d+1 \\ j \neq i}} (x - a_j)$

Then $g_i(x) = \begin{cases} 1 & \text{if } x = a_i \\ 0 & \text{o/w} \end{cases}$

$f(x) = b_1 g_1(x) + b_2 g_2(x) + \cdots + b_{d+1} g_{d+1}(x)$

Then $f(a_i) = b_i$ for $1 \leq i \leq d+1$

degree of $f = d$

Secret Sharing Scheme

(t,n) - threshold secret sharing scheme:

share a secret among n people in such a way that

1. any t of them can recover the secret
2. less than t of them can not recover the secret

Idea: Split secret into shares, distributed over all n participants such a way that

1. knowledge of at least t shares can recover the secret.
2. knowledge of less than t shares give no information on the secret.

(n, n)- scheme

secret : $s \in \mathbb{Z}_m$

shares : random $n-1$ values from $\mathbb{Z}_m$

$s_1, \ldots s_{n-1}$

$s_n = s - s_1 - s_2 - \ldots - s_{n-1} \mod m$

Distribute s_i to participant i

recover : $s = s_1 + s_2 + \ldots + s_n \mod m$

Can any $n-1$ of the shares recover secret ?

NO.

For example, if s_2 is unknown,

and all other shares are known,

$T = s_1 + s_3 + \ldots + s_n$

$s = T + s_2$

knowledge of T gives no information of s without knowledge of s_2

(t, n) - Sharing secret scheme

Based on polynomial interpolation over finite field F.

Secret : $S \in GF(q)$ (finite field of order q)

Shares : Choose $t-1$ random values over $GF(q)$

$a_1, a_2, \ldots, a_{t-1}$

$a_0 = S$

Build a secret polynomial

$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1}$

The share for participant i is $(i, f(a_i))$

Recovery : Given any t shares, say $(1, f(a_1)), (2, f(a_2)) \ldots, (t, f(a_t))$ construct $f(x)$ such that f fits these shares. Compute $a_0 = f(0)$

If less than t participants pool the shares, can they recover secret?

See Homework 12.