CS 70, July, 8, 2020

Question of the day:

- Someone gives a gift to Yining, Khalil and Amin.
- The gift is in a locked chest with a long Password.
- How should we share some information about the Password with the instructors, such that at least two of the three instructors need to share their information to figure out the Password?

- Polynomials
- Secret sharing

CS 70, July, 8, 2020

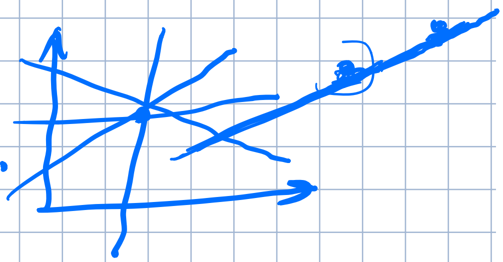
Share Secret among n People.

Secrecy: Any k-1 knows nothing.
Roubustness: Any k knows the secret
Efficient: Minimize Storage

solution ? Polynomials!

The idea:

Two Points make a unique.



This lecture:

d+1 Points make a unique degree d Polynomial.

Polynomials:

$$P(x) = \boxed{a_d x^{d}} + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

P(a) is a degree d Polynomial which is

specified by coefficients $a_0, a_1, \ldots, a_d$

P(x) contains (x_1, y_1) if and only if

$P(x_1) = y_1$

Polynomials over reals: $a_0, \dots, a_d, X \in \mathbb{R}$

Polynomial Examples: $\mathbb{R}$

$d = 1$

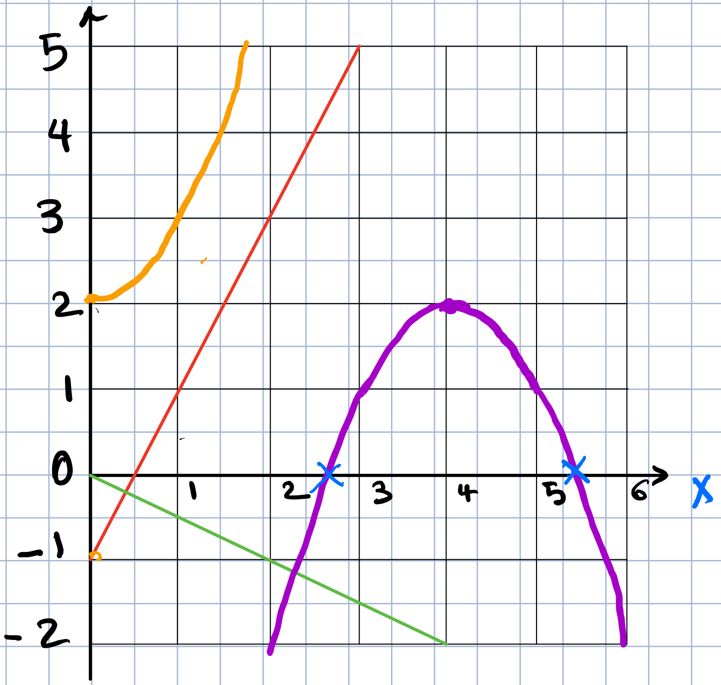
$P(x) = 2X - 1$

$P(x) = -0.5X$

$d = 2$

$P(X) = X^2 + 2$

$P(x) = -x^2 + 8x - 14$



Properties of Polynomials:

Property 1: A non-zero Polynomial of degree d has at most d roots (zeros).

- X_1 is a root if and only if $P(x_1) = 0$

Property 2: Given $d+1$ Pairs $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ with all the x_i distinct, there is a unique Polynomial of degree at most d such that $P(x_i) = y_i$ for $i \in \{1, \dots, d+1\{$

Proof of Property 1:

First we need to review Polynomial division.

If we have a Polynomial degree d, we can divide by a Polynomial of degree $\leq d$ using long division.

$$P(x) = q'(x)\,q(x) + \underline{r(x)}$$

$q'(x)$: the quatient $\qquad$ $r(x)$: the remainder

The degree for $\underline{r(x)}$ is less than the degree of $q(x)$.

Example: Divide $4x^2 - 3x + 2$ by $(x-3)$

$$\begin{array}{r|l} & \quad 4x + 9 \\ \hline (x-3) & 4x^2 - 3x + 2 \\ & -(4x^2 - 12x) \\ \hline & 0 + 9x + 2 \\ & \quad -(9x - 27) \\ \hline & \qquad 0 + 29 \end{array}$$

so $\quad P(x) = 4x^2 - 3x + 2 = \overset{q'(x)}{(4x+9)}\,\overset{q(x)}{\underline{(x-3)}} + \overset{r(x)}{\underline{29}}$

Now we can Prove property $\underline{1}$.

Property 1: A non-zero Polynomial of degree d has at most $\underline{d}$ roots.

if and only if

Lemma1: $P(x)$ has root a iff $P(x)/(x-a)$ has remainder 0: $P(x)=(x-a)\,Q(x)+0$

Proof: we know $P(x) = \underbrace{(x-a)}_{1}\,Q(x) + \underbrace{r(x)}_{c}$

$$\boxed{P(x) = (x-a)\,Q(x) + c}$$

$$\begin{cases} \text{If } P(a)=0 = 0 + c \Rightarrow c=0 \rightarrow r=0 \\ \text{If } r=0 \Rightarrow P(x)=(x-a)\,Q(x) \Rightarrow P(a)=0. \end{cases}$$

Lemma 2: $P(x)$ of degree d with distinct roots $a_1, a_2, \ldots, a_d$ can be written as

$$P(x) = c\,(x-a_1)(x-a_2)\cdots(x-a_d)$$

Proof: By induction on d

- Base case: $d=0 \Rightarrow P(x)=c$
- IH: for some $d\geq 0$ $P(x) = c\,(x-a_1)\cdots(x-a_d)$
- Induction step: $P(x)$ of degree $d+1$ with roots $a_1, a_2, \ldots, a_{d+1}$.

By lemma: $\underbrace{P(x)}_{d+1} = \underbrace{(x-a_{d+1})}\,\underbrace{Q(x)}_{d}$

$$P(a_i) = (a_i - a_{d+1})\,Q(a_i) = 0, \quad \forall a_i \mid i\neq d+1$$

$\underbrace{Q(a_i)=0}_{d} \quad \forall\ i \neq d+1$

from IH $Q(x) = c(x-a_1) \text{ ---- } (x-a_d)$

$\Rightarrow \underline{P(x)} = \underline{c(x-a_1) \text{ --- } (x-a_d)}(x-a_{d+1})$

Use Lemma 1 and 2 to Prove Property 1.

For $P(x)$ of degree d

$P(x) = c\,\underline{(x-a_1)} \text{ --- } (x-\underline{a}_d)$

$\forall a \neq a_i ,\ i=\{1,...,d\} \Rightarrow P(a) \neq 0$

$\Rightarrow$ $P(x)$ of degree d has at most d roots.

Proof of Property 2:

Property 2: Given $d+1$ Pairs $(x_1,y_1),\dots,(x_{d+1},y_{d+1})$ with all the x_i distinct, there is a unique Polynomial of degree at most d such that $P(x_i)=y_i$ for $i \in \{1,2,\dots,d+1\}$.

Two steps: 1. Existence. 2. Uniqueness

1. Existence

2 Points ⇒ a unique line

Find the unique $P(x)$ for $(1,3), (2,4)$

$$P(x) = a_1 x + a_0$$

$$\begin{matrix} P(1)=3 \\ P(2)=4 \end{matrix} \Rightarrow \begin{cases} a_1 + a_0 = 3 \\ 2a_1 + a_0 = 4 \end{cases} \Rightarrow a_1 = 1 \quad a_0 = 2$$

$$P(x) = x + 2$$

3 Points ⇒ A unique quadratic function.

Find the unique $P(x)$ for $(1,7);(2,13);(3,37)$

$$P(x) = a_2 x^2 + a_1 x + a_0$$

$$\begin{matrix} P(1)=2 \Rightarrow \\ P(2)=4 \Rightarrow \\ P(3)=0 \Rightarrow \end{matrix} \begin{cases} a_2 + a_1 + a_0 = 7 \\ 4a_2 + 2a_1 + a_0 = 13 \\ 9a_2 + 2a_1 + a_0 = 27 \end{cases} \Rightarrow \begin{matrix} a_2 = 2, \ a_1 = 1 \\ a_0 = 4 \end{matrix}$$

In General

$d+1$ Points: $(x_1, y_1); (x_2, y_2), \dots, (x_{d+1}, y_{d+1})$

$$P(x) = a_d x^d + \cdots + a_0$$

solve
$$\begin{cases} a_d x_1^d + \cdots + a_0 = y_1 \\ \vdots \\ a_d x_{d+1}^d + \cdots + a_0 = y_{d+1} \end{cases}$$

Does the solution exist?

To Prove the existense, use Lagrange interpolation:

Delta Polynomial: for set of values $x_1, \dots, x_{d+1}$

$$\Delta_i(x) = \begin{cases} 1 & \text{if } x = x_i \\ 0 & \text{if } x = x_j \text{ and } x_j \neq x_i \end{cases}$$

why is it useful to interpolate a polynomial Passing $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$?

- $y_1 \Delta_1(x)$ contains $\boxed{(x_1, y_1)}$
- $y_2 \Delta_2(x)$ contains (x_2, y_2)

$\vdots \qquad \vdots$

- $y_{d+1} \Delta_{d+1}(x)$ contains (x_{d+1}, y_{d+1})

sum over

$$P(x) = y_1 \Delta_1(x) + \dots + y_{d+1} \Delta_{d+1}(x)$$

$$\begin{cases} P(x_1) = y_1 \\ P(x_2) = y_2 \\ \vdots \\ P(x_{d+1}) = y_{d+1} \end{cases}$$

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

$$= \begin{cases} 1 & x = x_i \\ 0 & x = x_j,\ x_j \neq x_i \end{cases}$$

$\underline{\Delta_i(x)} =$

$$\begin{cases} P(1) = 5 \\ P(2) = 6 \\ P(3) = 9 \end{cases}$$

$$\Delta_1(x) = \frac{\boxed{(x-2)}\boxed{(x-3)}}{(\underset{\uparrow}{1}-2)(\underset{\uparrow}{1}-3)}$$

$$\Delta_2(x) = \frac{(x-1)(x-3)}{\underline{(2-1)}(2-3)}$$

Uniqueness: At most one Polynomial of degree d hits d+1 Points.

Remember Property $\underline{1}$: Any non-zero Polynomial of degree d has at most d roots.

Proof of uniqueness: Proof by contradition

Assume two differen Polynomials $P(x)$, $Q(x)$ hit the d+1 Points.

Defin $R(x) = \underline{P(x)} - \underline{Q(x)}$

$$\begin{cases} \underline{R(x) \text{ is degree}} \ d \\ R(x_i) = P(x_i) - Q(x_i) = y_i - y_i = 0 \\ \quad \forall i \in \{1, \dots, d+1\} \end{cases}$$

R has $\underline{d+1}$ roots.

Polynomials on Finite Fields:

what if $x \in \mathbb{N}$ or $x \in \mathbb{Z}$

Does Property 1 and 2 still hold?

For Polynomial interPolation and Proof of Property 1 and 2 we can add, subtract multiply and divide (except 0).

$x \in \mathbb{N}$: subtracting two numbers may not be a natural number.

$x \in \mathbb{Z}$: division of two numbers may not be an integer

what if

Polynomials with arithmetic modulo P:

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_0 \pmod{P}$$

$$a_d, \dots, a_0 \in \{0, \dots, P-1\}$$

$x \in \{0, \dots, P-1\}$, P is Prime number

Addition, subtraction and multiPlication (modP) are allowed

Division? if $\gcd(x, P) = 1$. so the inverse of x exist for all $\{1, \dots, P-1\}$

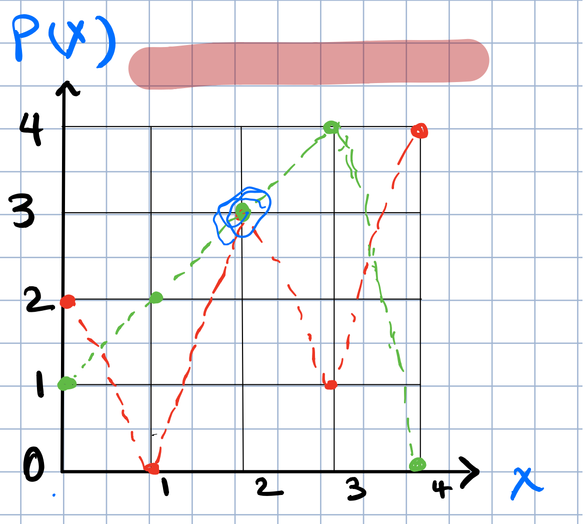
Hence, property 1 and 2 hold if the coefficient of $P(x)$ are (mod P) for a prime P.

This is over a Finite Field, denoted by F_p or $GF(p)$ (Galois Field)

The field is set of elements with addition subtraction, multiplication and inverses.

Note the result of operators on the elements of the field is an element in the field.

Examples: $P(x) \pmod P$



$P_1(x) = 3X + 2 \pmod 5$

$P_2(x) = X + 1 \pmod 5$

Intersection of $P_1(x)$ and $P_2(x)$?

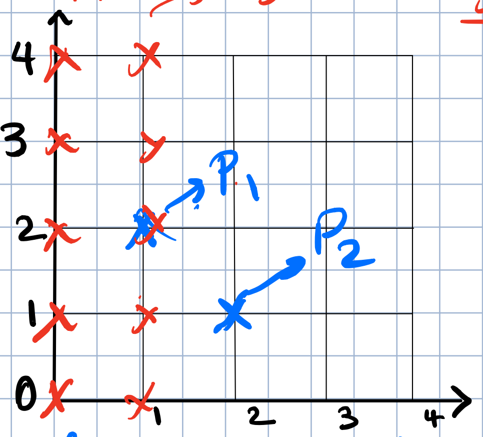
$$3X + 2 = x + 1 \pmod 5$$

$$\overset{3}{\Rightarrow} (2X \equiv (-1) \equiv 4) \pmod 5$$

$$X \equiv 12 \equiv 2 \pmod 5 \quad \boxed{X = 2}$$

$P(x) \pmod 5$

$\boxed{d=2}$ 3 Point are needed



$P_0 \rightarrow 5 \times 5 = \underline{5}^2$

If 2 Points are given

there are five Polynomials with degree 2 that Pass through P_1, P_2.

Application: Secret Sharing

Share Secret among n People.

Secrecy: Any K-1 Knows nothing

Roubustness: Any k Knows the secret

Efficient: Minimize Storage

Shamir's $\underline{K}$ out of $\underline{n}$ scheme:

Secret $\underline{s} \in \underline{\{0, \dots, p-1\}}$

1. Choose $a_0 = s$, and random $a_1, \dots, a_{k-1}$ $\in \{1, \dots, p-1\}$
2. Let $P(x) = a_{k-1}x^{k-1} + \dots + a_0$

   where $a_0 = s$.
3. Share Points $(i, P(i) \bmod p)$ with ith $i \in \{1, \dots, n\}$

Result: Any K Points gives the Polynomial. The secret $s = a_0$

$$P(0) = a_0 \Rightarrow \text{secret}$$

So

- with K shares, reconstruct $P(X)$
- with K-1 shares, any of P values are Possible for $P(0)$!