01204211 Discrete Mathematics
Lecture 10a: Polynomials (1)[1]

Jittat Fakcharoenphol

October 15, 2024

[1]This section is from Berkeley CS70 lecture notes.

Quick exercise

For any integer $a \neq 1$, $a - 1 | a^2 - 1$.

Quick exercise

For any integer $a \neq 1$, $a - 1 | a^2 - 1$.

For any integer $a \neq 1$ and $n \geq 1$, $a - 1 | a^n - 1$.

Polynomials

A **single-variable polynomial** is a function $p(x)$ of the form

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

GF(p)

We call a_i's *coefficients*. Usually, variable x and coefficients a_i's are real numbers. The **degree** of a polynomial is the largest exponent of the terms with non-zero coefficients.

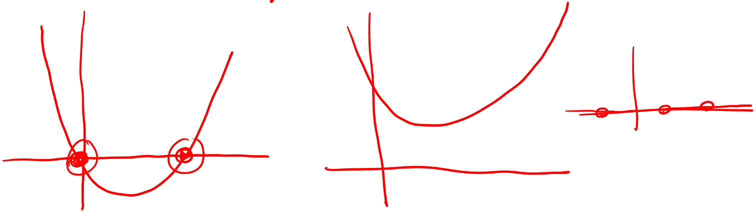
Examples

- $x^3 - 3x + 1$ 3
- $x + 10$ 1
- 10 0
- 0 0

Folklore

degree ≤ 1

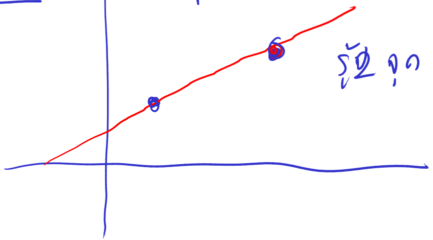
degree ≤ 2



- non-zero polynomial degree d $\boxed{\text{มีราก} \leq d \text{ ตัว.}}$
- polynomial degree $\leq d$ มีราก $> d$ ตัว $\Rightarrow$ poly $= 0$

Folklore

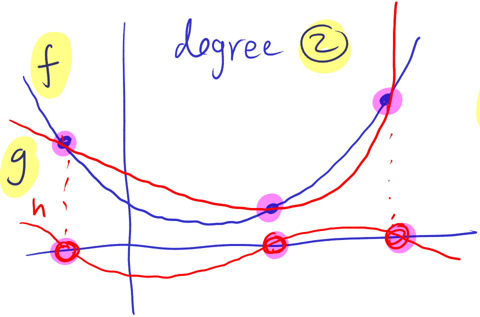
poly degree 1



รู้ 2 จุด หา poly

- degree 3
- รู้ 4 จุด

degree 2



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

$h(x)$ มี degree 2

$$\Rightarrow \boxed{h(x) = 0}$$

$$\Rightarrow f(x) = g(x) \checkmark$$

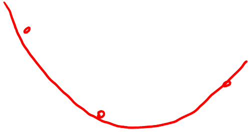
Applications

- Secret sharing

Applications

- Secret sharing
- Error-correcting codes

Basic facts



hw

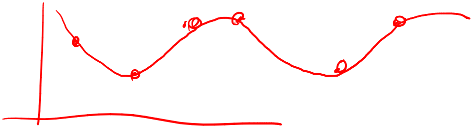
Definition

a is a **root** of polynomial $f(x)$ if $f(a) = 0$.

Properties

Property 1: A non-zero polynomial of degree d has at most d roots.

Property 2: Given $d + 1$ pairs $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ with distinct x_i's, there is a *unique* polynomial $p(x)$ of degree at most d such that $p(x_i) = y_i$ for $1 \leq i \leq d + 1$.



Lemma 1

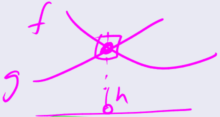
If two polynomials $f(x)$ and $g(x)$ of degree at most d that share $\boxed{d+1}$ points $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$, where all x_i's are distinct, i.e., $f(x_i) = g(x_i) = y_i$, then $f(x) = g(x)$.

Proof.

Suppose that $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ and $g(x) = b_d x^d + b_{d-1}x^{d-1} + \cdots + b_0$. Let $h(x) = f(x) - g(x)$, i.e., let $h(x) = c_d x^d + c_{d-1}x^{d-1} + \cdots + c_0$, where $c_i = a_i - b_i$. Note that $h(x)$ is also a polynomial of degree (at most) d.

We claim that $h(x)$ has $\boxed{d+1}$ roots. Note that since $f(x_i) = g(x_i) = y_i$, we have that

$$\boxed{h(x_i)} = f(x_i) - g(x_i) = y_i - y_i = 0,$$

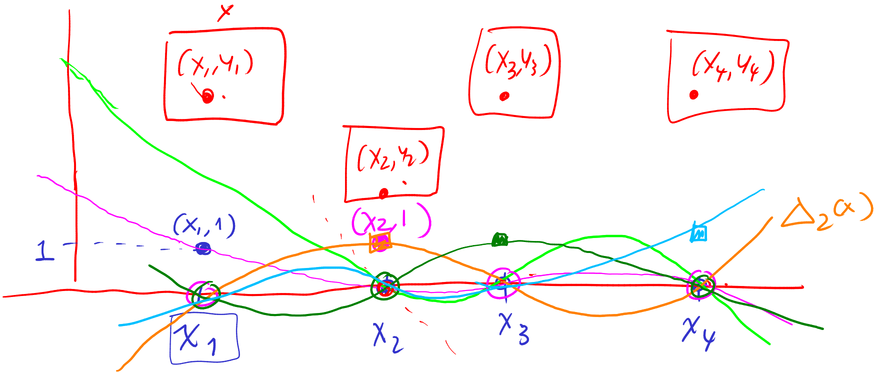


i.e., every x_i is a root of $h(x)$.

From $\boxed{\textbf{Property 1}}$, if $\boxed{h(x)}$ is non-zero it has at most $\boxed{d}$ roots; therefore, $h(x)$ must be zero, i.e., $f(x) - g(x) = 0$ or $f(x) = g(x)$ as required. $\square$

Polynomial interpolation - ideas

$(x_1, y_1), (x_2, y_2), (x_3, y_3)$
(x_4, y_4)



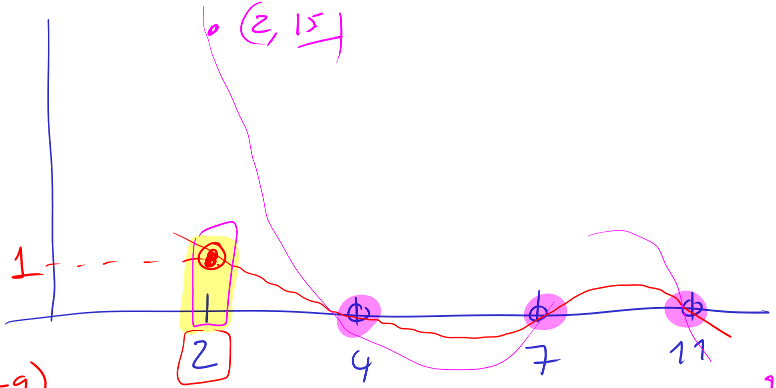
$$\Delta_1(x) = \frac{(x-x_2)(x-x_3)(x-x_4)}{(x_1-x_2)(x_1-x_3)(x_1-x_4)}$$

$$\Delta_2(x) = \frac{(x-x_1)(x-x_3)(x-x_4)}{(x_2-x_1)(x_2-x_3)(x_2-x_4)}$$

$\Delta_3(x)$

$\Delta_4(x)$

Polynomial interpolation - ideas



$(-2)(-5)(-9)$

-90

$$\boxed{\Delta_1(x)} = \frac{(x-4)(x-7)(x-11)}{(2-4)(2-7)(2-11)}$$

เป็น 0 ที่ 4, 7, 11

ค่าที่ได้ตอน $x=2$

Lagrange polynomial

For $d + 1$ points $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$ where all x_i's are distinct, let

$$\Delta_i(x) = \frac{(x - x_1)(x - x_2)\cdots(x - x_{i-1})(x - x_{i+1})\cdots(x - x_{d+1})}{(x_i - x_1)(x_i - x_2)\cdots(x_i - x_{i-1})(x_i - x_{i+1})\cdots(x_i - x_{d+1})}.$$

Note that $\Delta_i(x)$ is a polynomial of degree d

Lagrange polynomial

For $d+1$ points $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$ where all x_i's are distinct, let

$$\Delta_i(x) = \frac{(x - x_1)(x - x_2)\cdots(x - x_{i-1})(x - x_{i+1})\cdots(x - x_{d+1})}{(x_i - x_1)(x_i - x_2)\cdots(x_i - x_{i-1})(x_i - x_{i+1})\cdots(x_i - x_{d+1})}.$$

Note that $\Delta_i(x)$ is a polynomial of degree d. Also we have that

- For $j \neq i$, $\Delta_i(x_j) =$

Lagrange polynomial

For $d+1$ points $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$ where all x_i's are distinct, let

$$\Delta_i(x) = \frac{(x - x_1)(x - x_2)\cdots(x - x_{i-1})(x - x_{i+1})\cdots(x - x_{d+1})}{(x_i - x_1)(x_i - x_2)\cdots(x_i - x_{i-1})(x_i - x_{i+1})\cdots(x_i - x_{d+1})}.$$

Note that $\Delta_i(x)$ is a polynomial of degree d. Also we have that

- For $j \neq i$, $\Delta_i(x_j) = 0$, and
- $\Delta_i(x_i) =$

Lagrange polynomial

For $d+1$ points $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$ where all x_i's are distinct, let

$$\Delta_i(x) = \frac{(x - x_1)(x - x_2)\cdots(x - x_{i-1})(x - x_{i+1})\cdots(x - x_{d+1})}{(x_i - x_1)(x_i - x_2)\cdots(x_i - x_{i-1})(x_i - x_{i+1})\cdots(x_i - x_{d+1})}.$$

Note that $\Delta_i(x)$ is a polynomial of degree d. Also we have that

- For $j \neq i$, $\Delta_i(x_j) = 0$, and
- $\Delta_i(x_i) = 1$.

Lagrange polynomial

For $d+1$ points $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$ where all x_i's are distinct, let

$$\Delta_i(x) = \frac{(x - x_1)(x - x_2)\cdots(x - x_{i-1})(x - x_{i+1})\cdots(x - x_{d+1})}{(x_i - x_1)(x_i - x_2)\cdots(x_i - x_{i-1})(x_i - x_{i+1})\cdots(x_i - x_{d+1})}.$$

Note that $\Delta_i(x)$ is a polynomial of degree d. Also we have that

- For $j \neq i$, $\Delta_i(x_j) = 0$, and
- $\Delta_i(x_i) = 1$.

We can use $\Delta_i(x)$ to construct a degree-d polynomial

$$p(x) = \underline{y_1 \cdot \Delta_1(x)} + \underline{y_2 \cdot \Delta_2(x)} + \cdots \underline{y_{d+1} \cdot \Delta_{d+1}(x)}.$$

What can you say about $p(x_i)$?

Property 2

Given $d+1$ pairs $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ with distinct x_i's, there is a *unique* polynomial $p(x)$ of degree at most d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

Proof of Property 2.

Using Lagrange interpolation, we know that there exists a polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for all $1 \leq i \leq d+1$.
For uniqueness, assume that there exists another polynomial $g(x)$ of degree d also satifying the condition. Since $p(x)$ and $g(x)$ agrees on more than d points, $p(x)$ and $g(x)$ must be equal from Lemma 1. □

Polynomials over a finite field $\boxed{GF(p)}$

- ทุกตัว mod p
- division $\rightarrow$ คูณด้วย multiplicative inverse.

Examples - evaluation

Suppose that we work over $GF(m)$ where $m = 11$. Let $p(x) = 4 \cdot x^2 + 5 \cdot x + 3$. We have

x	$p(x)$	$p(x) \bmod m$
0	3	3
1	12	1
2	29	7
3	54	10
4	87	10
5	128	7
6	177	1
7	234	3
8	299	2
9	372	9
10	453	2
11	542	3

Examples - interpolation

Let $m = 11$. Suppose that $p(x)$ is a polynomial over $GF(m)$ of degree 2 passing through $(2, 7), (4, 10)$, and $(7, 3)$. Find $p(x)$.

Examples - interpolation

Let $m = 11$. Suppose that $p(x)$ is a polynomial over $GF(m)$ of degree 2 passing through $(2, 7), (4, 10)$, and $(7, 3)$. Find $p(x)$.
Let

Examples - interpolation

Let $m = 11$. Suppose that $p(x)$ is a polynomial over $GF(m)$ of degree 2 passing through $(2, 7), (4, 10)$, and $(7, 3)$. Find $p(x)$.

Let

- $\Delta_1(x) = \frac{(x-4)(x-7)}{(2-4)(2-7)} = \frac{x^2-11x+28}{(-2)\cdot(-5)} = \frac{x^2+6}{10} = 10x^2 + 5$

Examples - interpolation

Let $m = 11$. Suppose that $p(x)$ is a polynomial over $GF(m)$ of degree 2 passing through $(2,7),(4,10)$, and $(7,3)$. Find $p(x)$.

Let

- $\Delta_1(x) = \frac{(x-4)(x-7)}{(2-4)(2-7)} = \frac{x^2-11x+28}{(-2)\cdot(-5)} = \frac{x^2+6}{10} = 10x^2+5$
- $\Delta_2(x) = \frac{(x-2)(x-7)}{(4-2)(4-7)} = \frac{x^2-9x+14}{2\cdot(-3)} = \frac{x^2+2x+3}{5} = 9x^2+7x+5$

Examples - interpolation

Let $m = 11$. Suppose that $p(x)$ is a polynomial over $GF(m)$ of degree 2 passing through $(2, 7), (4, 10)$, and $(7, 3)$. Find $p(x)$.

Let

- $\Delta_1(x) = \frac{(x-4)(x-7)}{(2-4)(2-7)} = \frac{x^2-11x+28}{(-2)\cdot(-5)} = \frac{x^2+6}{10} = 10x^2 + 5$
- $\Delta_2(x) = \frac{(x-2)(x-7)}{(4-2)(4-7)} = \frac{x^2-9x+14}{2\cdot(-3)} = \frac{x^2+2x+3}{5} = 9x^2 + 7x + 5$
- $\Delta_2(x) = \frac{(x-2)(x-4)}{(7-2)(7-4)} = \frac{x^2-6x+8}{5\cdot 3} = \frac{x^2+5x+8}{4} = 3x^2 + 4x + 2$

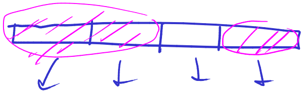
Thus,

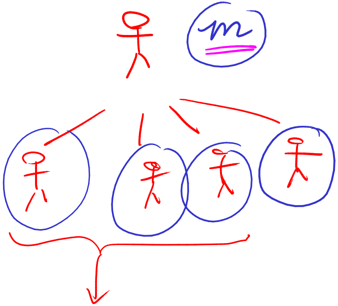
$$\begin{aligned} p(x) &= 7\Delta_1(x) + 10\Delta_2(x) + 3\Delta_3(x) \\ &= (70x^2 + 35) + (90x^2 + 70x + 50) + (9x^2 + 12x + 6) \\ &= 4x^2 + 5x + 3 \end{aligned}$$

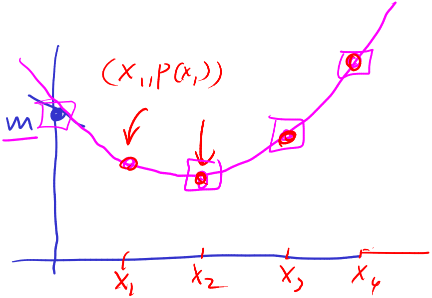
Secret sharing scheme - settings

$\boxed{p > m}$

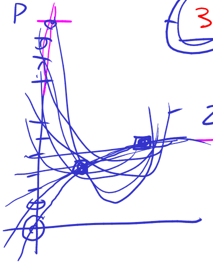
GF(p)







3 คนขึ้นไป เอาความลับกลับมาได้



2 คน ไม่รู้อะไรเลย.

→ $\forall$ m' ใดๆ

$\exists$ polynomial ที่ผ่าน 2 จุด + $(0, m')$

degree 2

$$p(x) = a_2 x^2 + a_1 x + \boxed{m}$$

Secret sharing scheme - settings

- There are $\boxed{n}$ people, a secret s, and an integer $\boxed{k}$.
- We want to "distribute" the secret in such a way that any set of $\boxed{k-1}$ people cannot know anything about s, but any set of $\boxed{k}$ people can reconstruct s.

- degree $k-1$
- $p(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots a_1 x + \boxed{s}$
- 160n $(1, p(1)), (2, p(2)), (3, p(3)), \ldots$

mod $\boxed{p}$

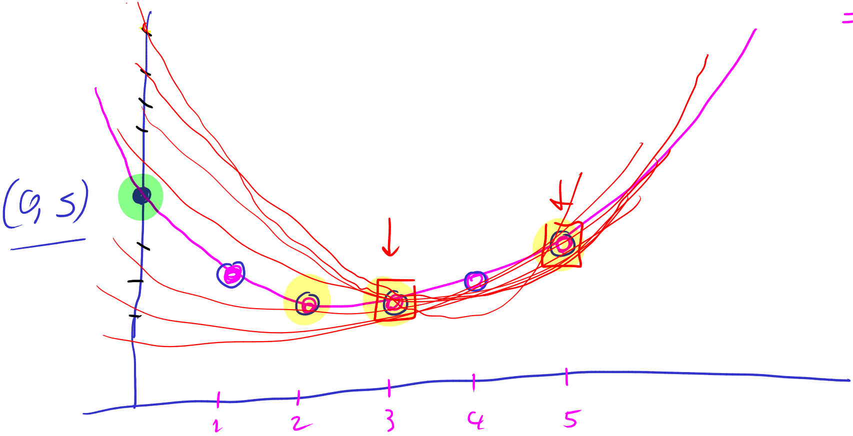
$p > s$

$p > n$

Secret sharing scheme

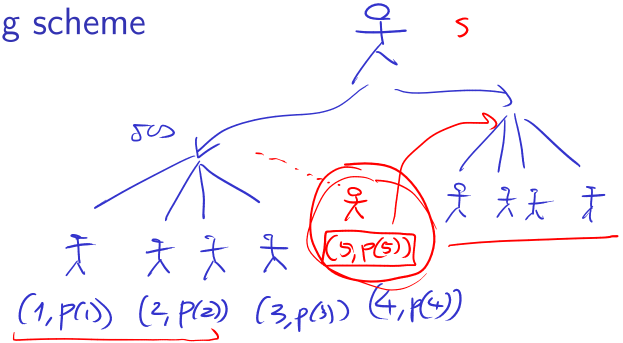
รู้ 3 จุด ⇒ รู้ poly

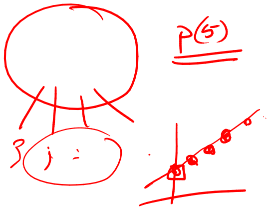
⇒ degree 2



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

Secret sharing scheme





→ • รวม 3 คน ถอดรหัสได้

degree 2

$p(x) = a_2 x^2 + a_1 x + s$

• รวม 2 คน + 2 ที่ปรึกษา ถอดรหัสได้

Secret sharing scheme

- Pick m to be larger than n and s. (Much larger than s, i.e., $m >>> s$.)
- Pick a random polynomial of degree $k-1$ such that $P(0) = s$.
- Give $P(i)$ to person i, for $1 \leq i \leq n$.
- Correctness: for any set of k people,

Secret sharing scheme

- Pick m to be larger than n and s. (Much larger than s, i.e., $m >>> s$.)
- Pick a random polynomial of degree $k-1$ such that $P(0) = s$.
- Give $P(i)$ to person i, for $1 \leq i \leq n$.
- Correctness: for any set of k people,
- Correctness: for any set of $k-1$ people, how many possible candidate secrets compatible with the information these people have?