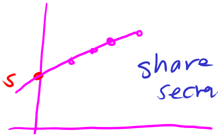


share secret $\boxed{s}$

So $\underline{\underline{2}}$ people can recon $\boxed{s}$

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

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

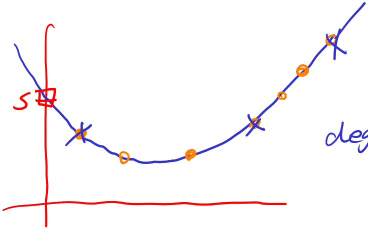
We call a_i's *coefficients*. Usually, variable x and coefficients a_i's are real numbers. The **degree** of a polynomial is the largest exponent of the terms with non-zero coefficients.

Examples

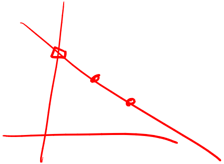
- $x^3 - 3x + 1$
- $x + 10$
- 10
- 0

Folklore

$$f(x) = ax^2 + bx + c$$



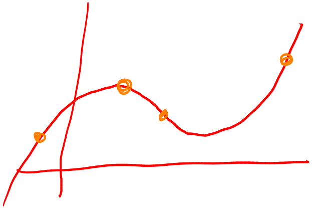
degree 2



$$f(x) = ax + b$$

Polynomial of degree d

$\rightarrow$ need $d+1$ points.



degree 3

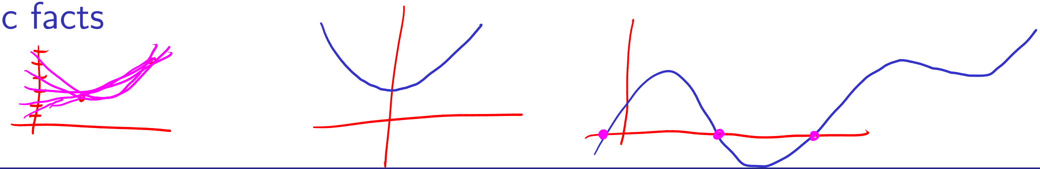
Applications

- Secret sharing

Applications

- Secret sharing
- Error-correcting codes

Basic facts



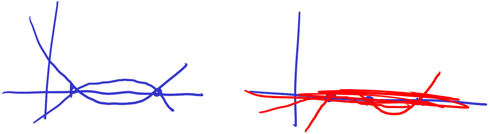
Definition

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 $1 \leq i \leq d+1$.



Basic facts

Definition

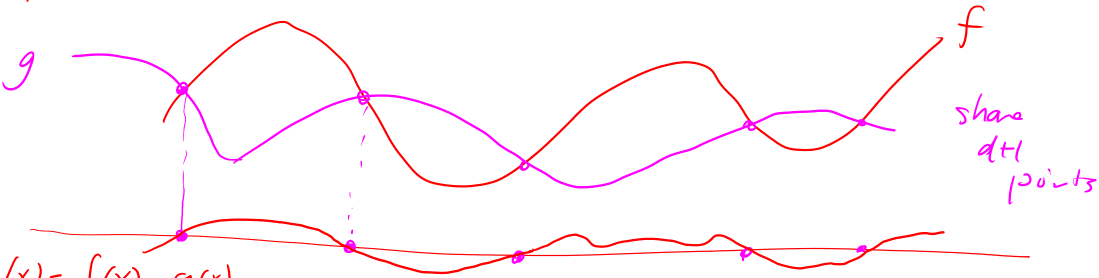
a is a **root** of polynomial $f(x)$ if $f(a) = 0$.

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 $1 \leq i \leq d+1$.

→ (a) There exists at least one polynomial ← Lagrange interp.

(b) If there are more than one, they have to be equal poly degree d



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

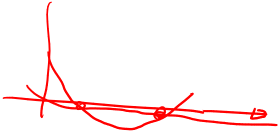
$h(x_i) = 0$

poly degree d

h has $d+1$ roots

2

$h = 0$



Lemma 1

If two polynomials $f(x)$ and $g(x)$ of degree at most d that share $d+1$ points $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$, 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 $d+1$ roots. Note that since $f(x_i) = g(x_i) = y_i$, we have that

$$h(x_i) = f(x_i) - g(x_i) = y_i - y_i = 0,$$

i.e., every x_i is a root of $h(x)$.
From **Property 1**, if $h(x)$ is non-zero it has at most 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

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

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

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

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. $\square$

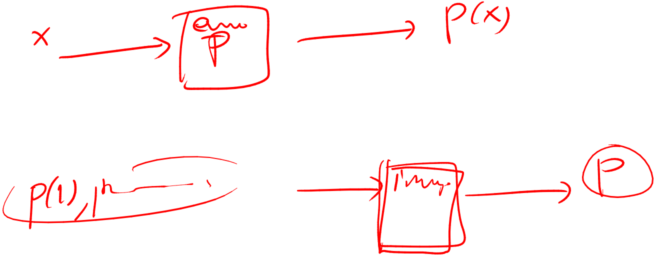
Polynomials over a finite field $GF(p)$

$GF(11)$

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

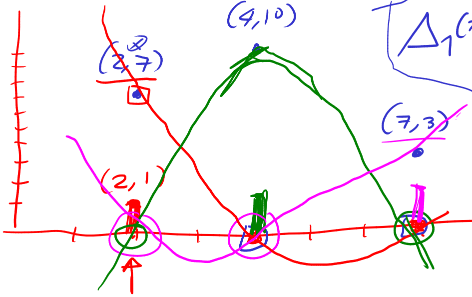


Examples - interpolation

$$7\cdot\Delta_1(x) + 10\cdot\Delta_2(x) + 3\Delta_3(x)$$

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 $p(x)$.

$$\Delta_3(x) = \frac{(x-2)(x-4)}{(7-2)(7-4)} = \boxed{}$$



$$\boxed{\Delta_1(x) = \frac{(x-4)(x-7)}{(2-4)(2-7)}} = \frac{x^2+6}{10} = 10x^2+60 = \underline{10x^2+5} \pmod{11}$$

$$\Delta_2(x) = \frac{(x-2)(x-7)}{(4-2)(4-7)} = \frac{x^2-9x+3}{5} = 9(x^2+2x+3) = \underline{9x^2+7x+5}$$

Examples - interpolation

$$\boxed{y_1 \cdot \Delta_1(x) + y_2 \cdot \Delta_2(x) + y_3 \cdot \Delta_3(x)}$$

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 $p(x)$.

$$\frac{6x^2 + 4x + 8}{-2} =$$

Let

$$(x_1, y_1) \qquad (x_2, y_2) \qquad (x_3, y_3)$$

$$\Delta_1(x) \rightarrow \begin{matrix} 1 & \text{at} & x_1 \\ 0 & \text{at} & x_2 \\ 0 & \text{at} & x_3 \end{matrix} \qquad \frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)}$$

$$\Delta_3(x) \rightarrow \begin{matrix} 0 & \text{at} & x_1 \\ 0 & \text{at} & x_2 \\ 1 & \text{at} & x_3 \end{matrix} \qquad \frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)}$$

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

- $\Delta_1(x) = \frac{(x-4)(x-7)}{(2-4)(2-7)} = \frac{x^2-11x+28}{(-2)\cdot(-5)} = \frac{x^2+6}{10} = 10x^2 + 5$
- $\Delta_2(x) = \frac{(x-2)(x-7)}{(4-2)(4-7)} = \frac{x^2-9x+14}{2\cdot(-3)} = \frac{x^2+2x+3}{5} = 9x^2 + 7x + 5$
- $\Delta_2(x) = \frac{(x-2)(x-4)}{(7-2)(7-4)} = \frac{x^2-6x+8}{5\cdot3} = \frac{x^2+5x+8}{4} = 3x^2 + 4x + 2$

2	4	7
1	0	0
0	1	0
0	0	1
7	10	3

Thus,

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

Secret sharing scheme - settings

secret s

n people, $k \leq n$

share $\boxed{s}$ so that - any group of $k-1$ people know nothing on s

- group of k people → learn $\boxed{s}$

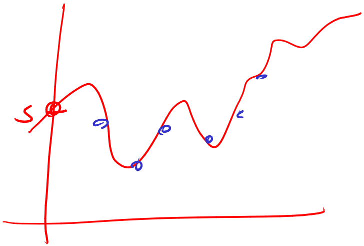
Secret sharing scheme - settings

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

Secret sharing scheme

- Secret s
- Pick random polynomial f of degree $k-1$

  s.t. $f(0) = s$



- give person i

  $\boxed{(x_i, f(x_i))}$

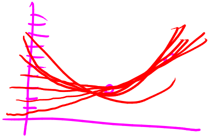
Secret sharing scheme

$$P(x) = a_k x^{k-1} + a_n x^{k-2} + a x^{k-3} + a_1 x^1 + \boxed{s}$$

- 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 $1 \le i \le n$.
- Correctness: for any set of k people, recover $P(x)$ ✓

using Lagrange interpolation

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?