Polynomials and Secret Sharing

CS 70 Discussion 4B

Raymond Tsao

2025-02-21

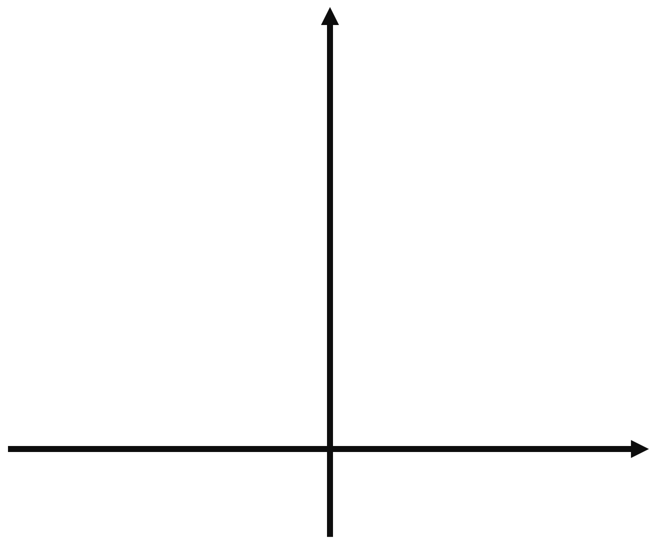
Note: These slides are unofficial course materials. Please use the notes as the only single source of truth.

Problem 3: Lagrange Interpolation

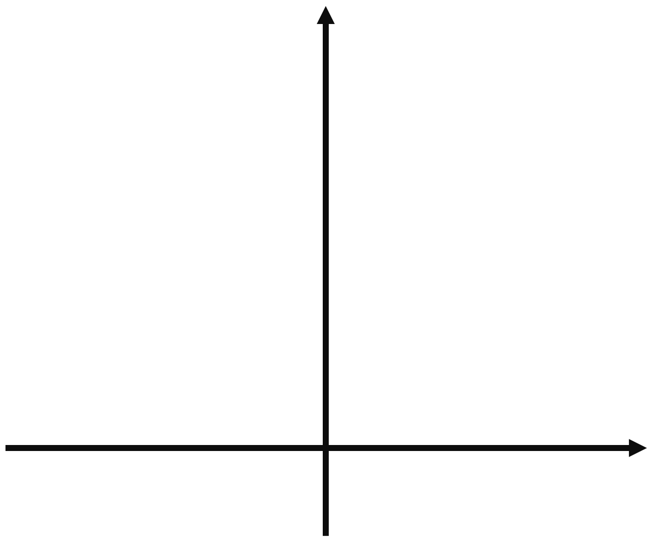
- Given $d + 1$ points, there exists a polynomial of degree at most d that passes through these points

Problem 3: Lagrange Interpolation

- Given $d + 1$ points, there exists a polynomial of degree at most d that passes through these points



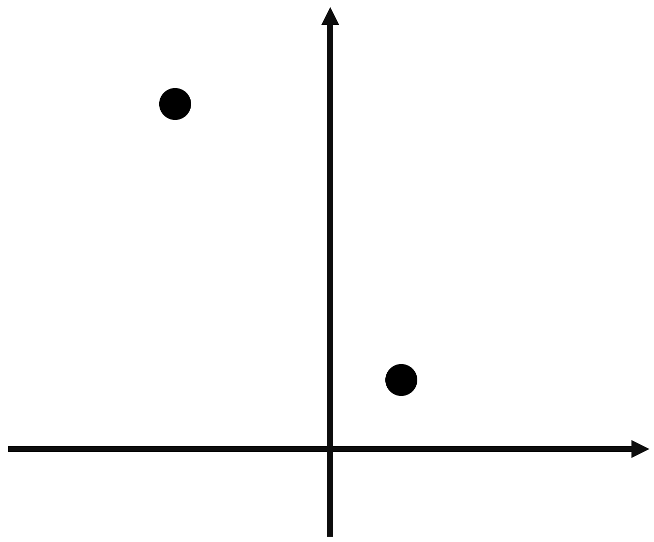
2 points



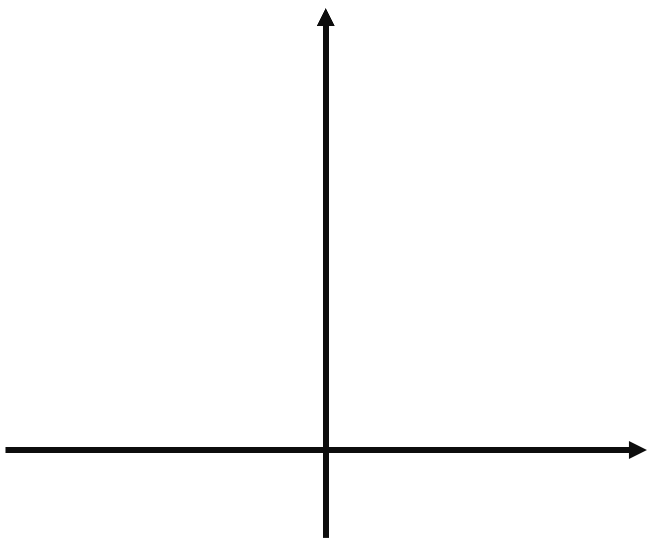
3 points

Problem 3: Lagrange Interpolation

- Given $d + 1$ points, there exists a polynomial of degree at most d that passes through these points



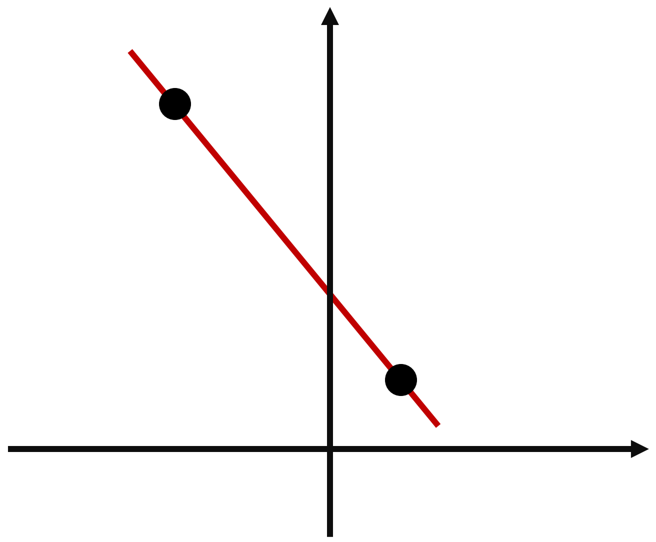
2 points



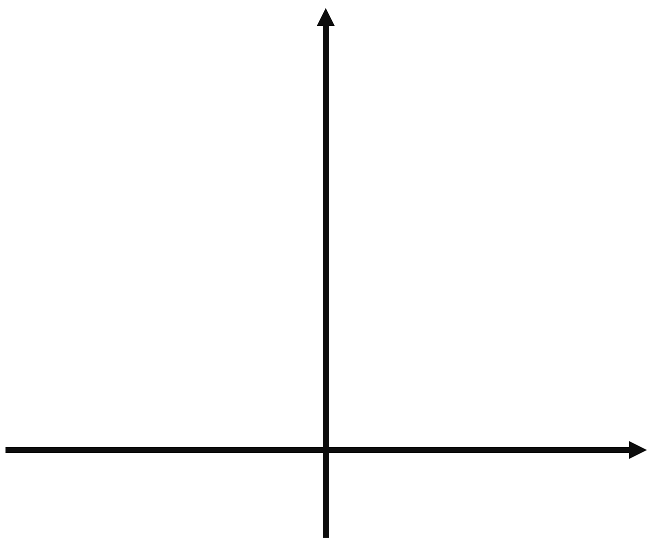
3 points

Problem 3: Lagrange Interpolation

- Given $d + 1$ points, there exists a polynomial of degree at most d that passes through these points



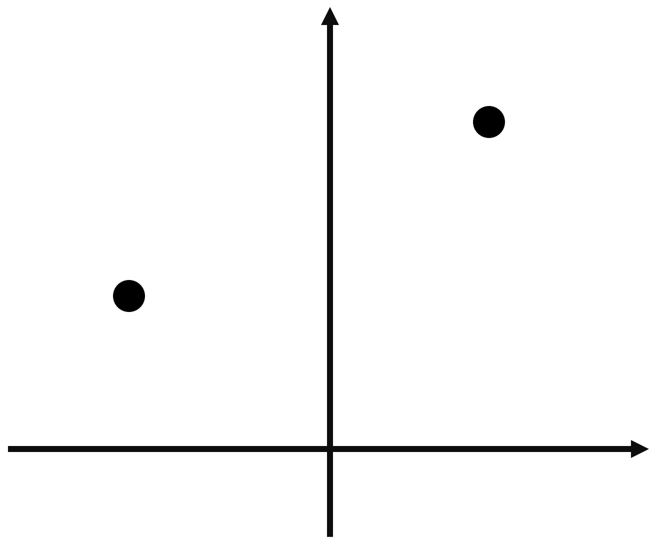
2 points



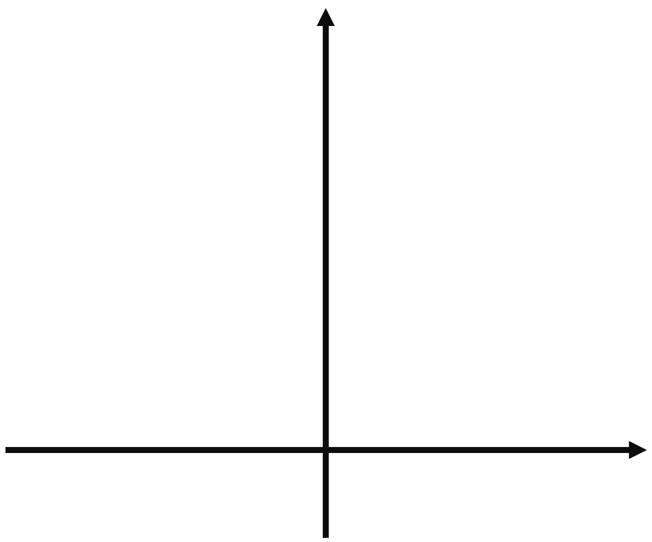
3 points

Problem 3: Lagrange Interpolation

- Given $d + 1$ points, there exists a polynomial of degree at most d that passes through these points



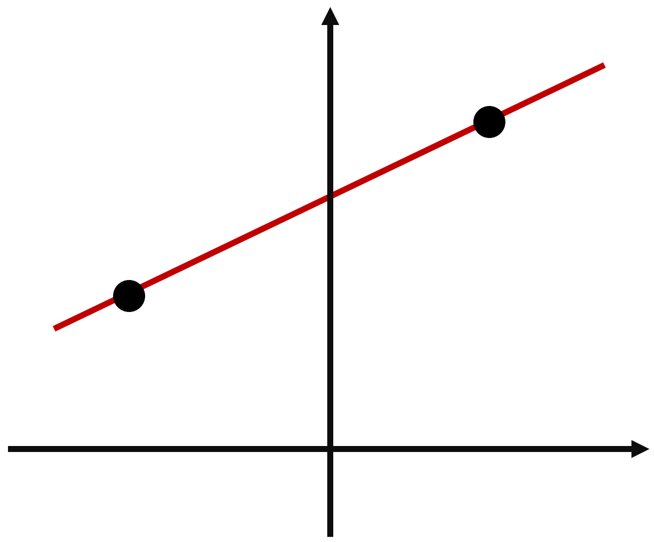
2 points



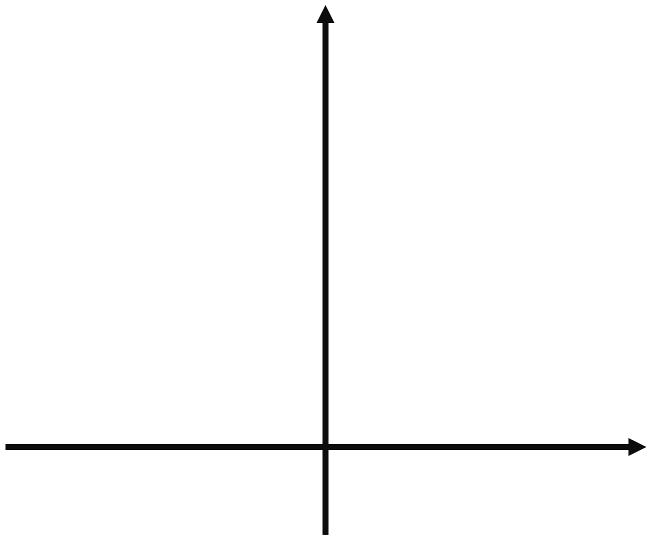
3 points

Problem 3: Lagrange Interpolation

- Given $d + 1$ points, there exists a polynomial of degree at most d that passes through these points



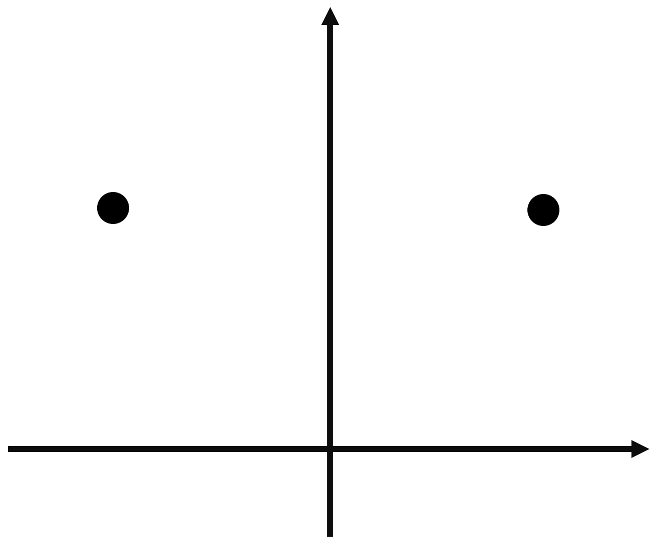
2 points



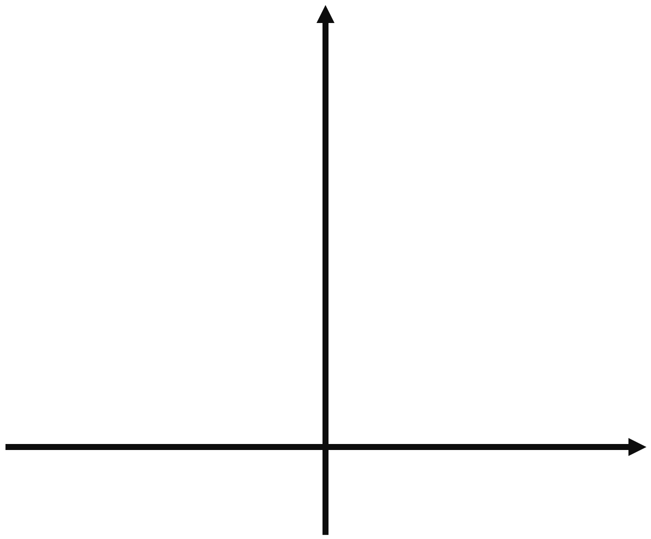
3 points

Problem 3: Lagrange Interpolation

- Given $d + 1$ points, there exists a polynomial of degree at most d that passes through these points



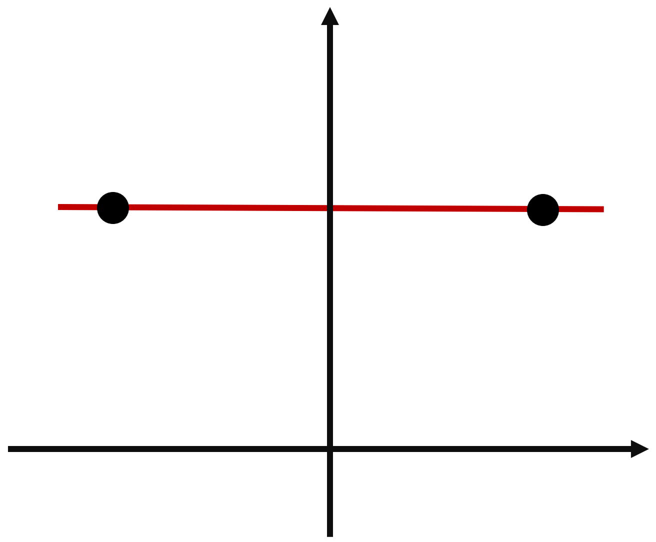
2 points



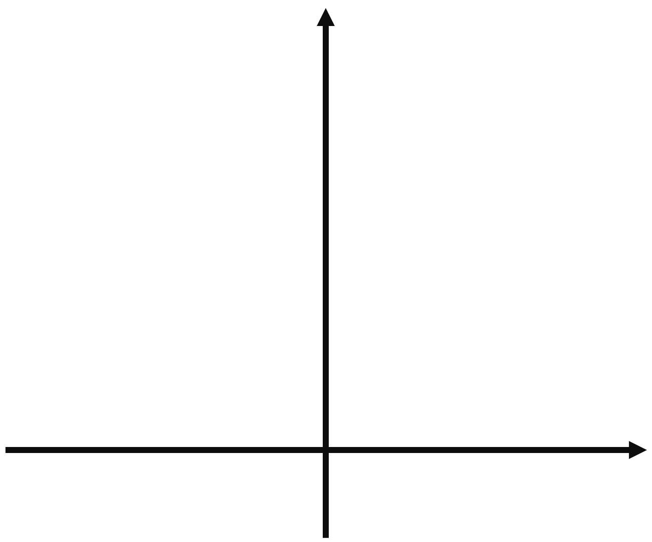
3 points

Problem 3: Lagrange Interpolation

- Given $d + 1$ points, there exists a polynomial of degree at most d that passes through these points



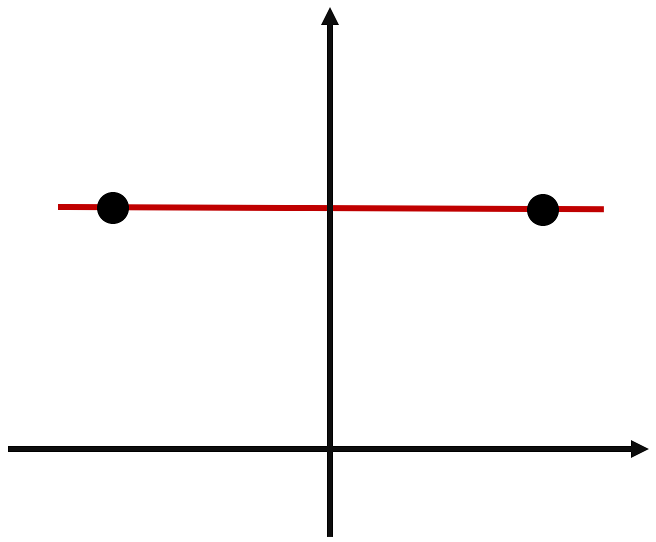
2 points



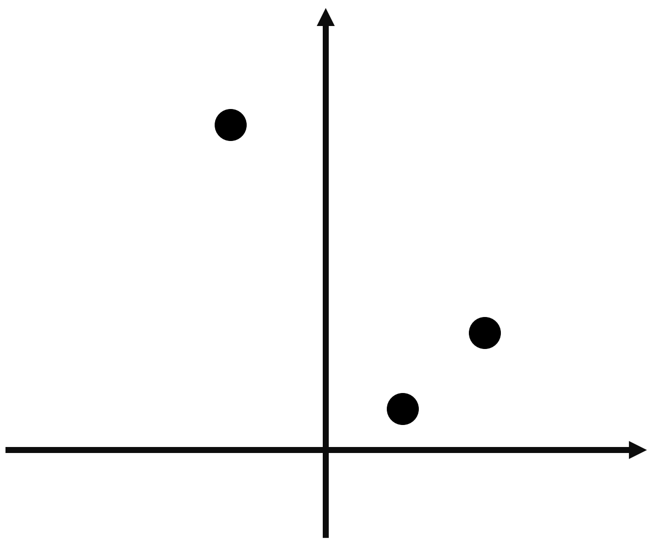
3 points

Problem 3: Lagrange Interpolation

- Given $d + 1$ points, there exists a polynomial of degree at most d that passes through these points



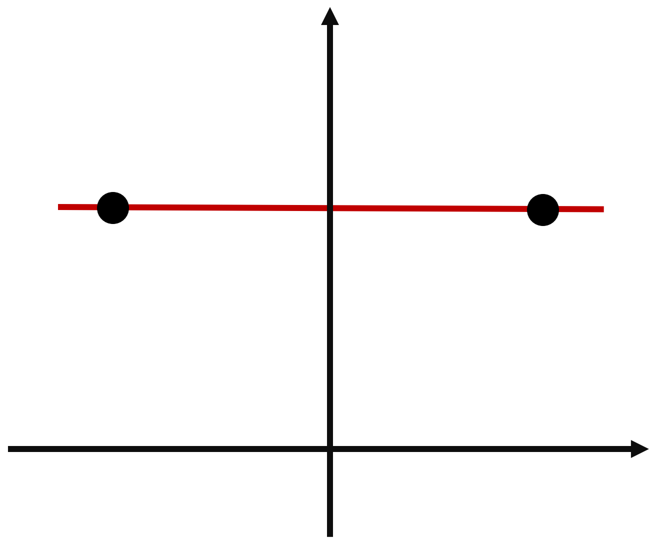
2 points



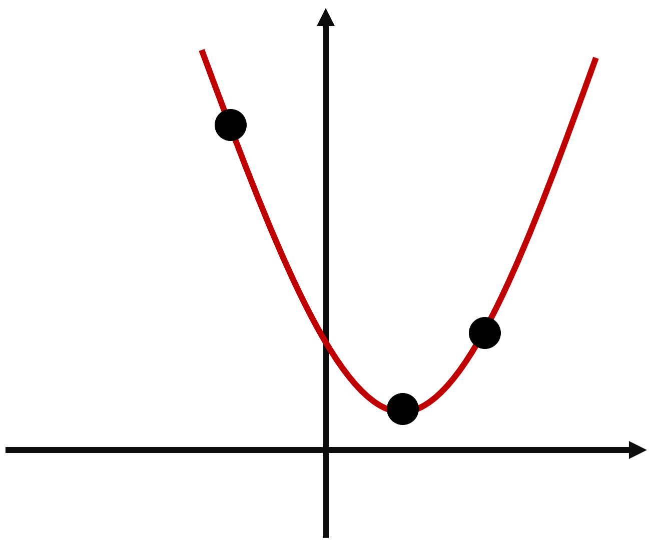
3 points

Problem 3: Lagrange Interpolation

- Given $d + 1$ points, there exists a polynomial of degree at most d that passes through these points



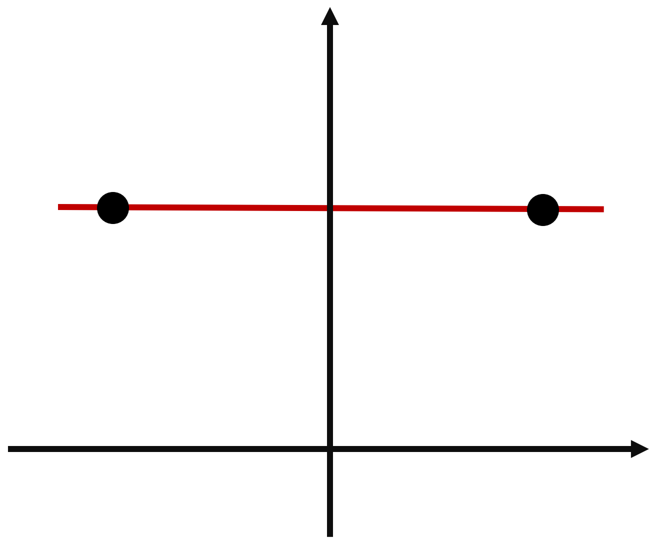
2 points



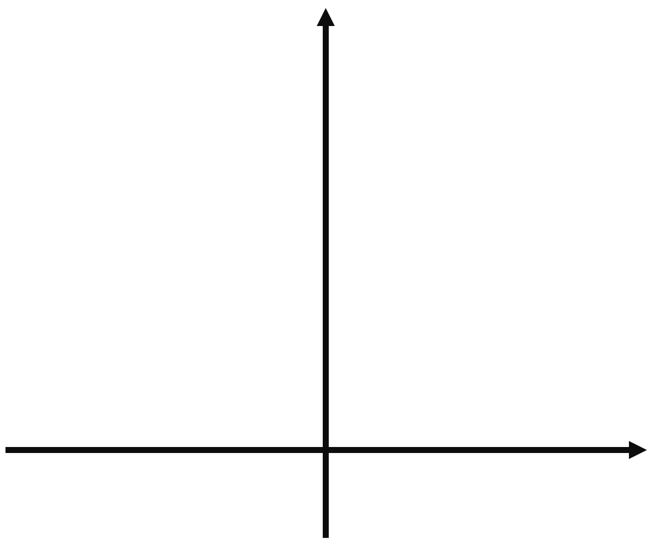
3 points

Problem 3: Lagrange Interpolation

- Given $d + 1$ points, there exists a polynomial of degree at most d that passes through these points



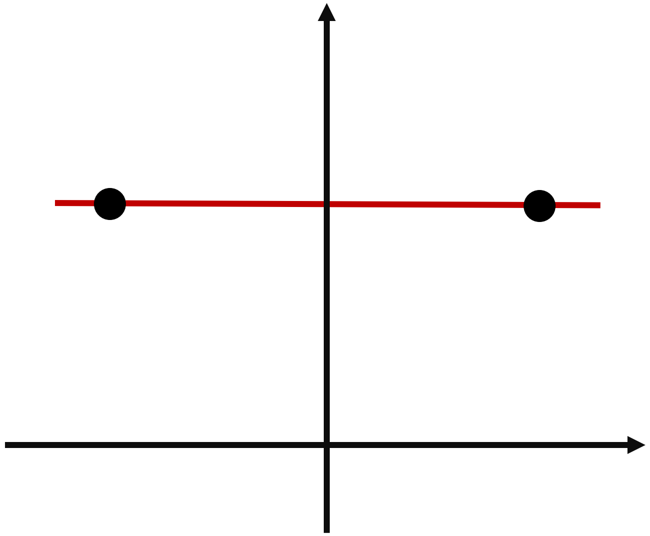
2 points



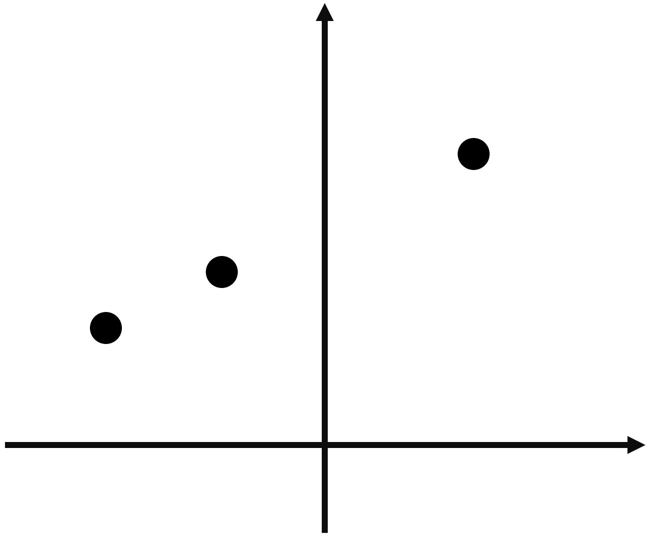
3 points

Problem 3: Lagrange Interpolation

- Given $d + 1$ points, there exists a polynomial of degree at most d that passes through these points



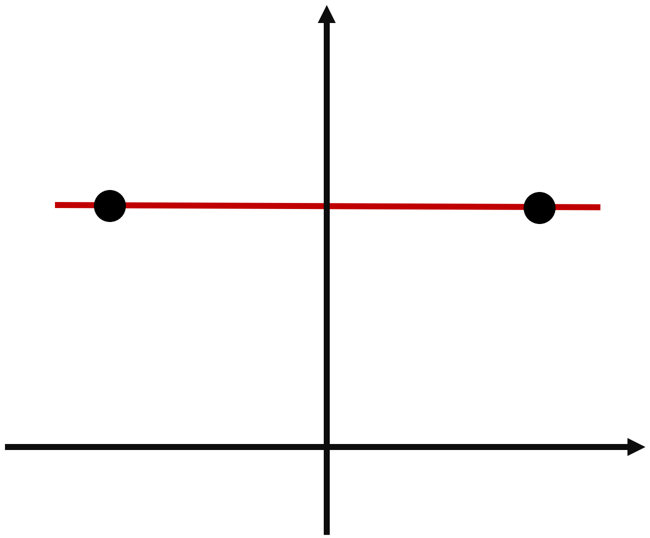
2 points



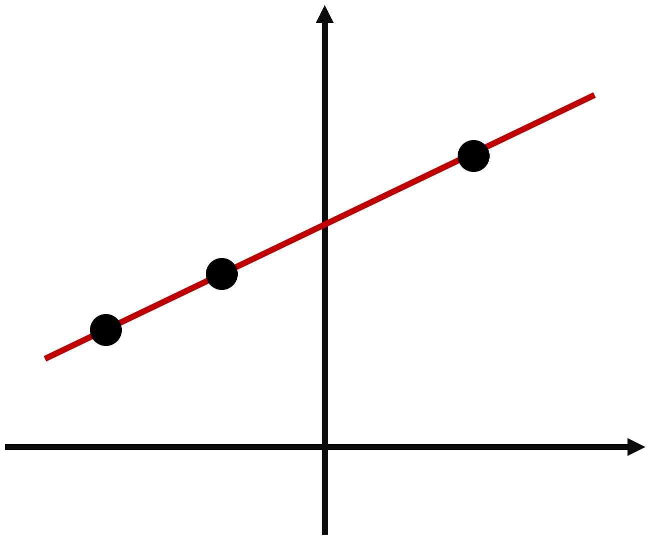
3 points

Problem 3: Lagrange Interpolation

- Given $d + 1$ points, there exists a polynomial of degree at most d that passes through these points



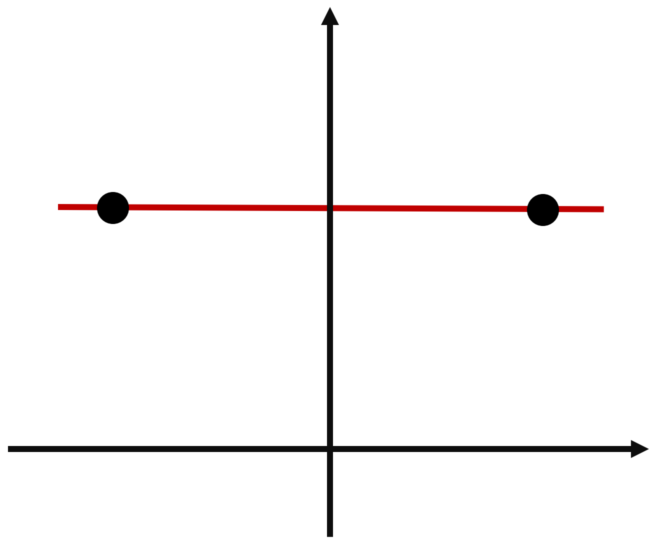
2 points



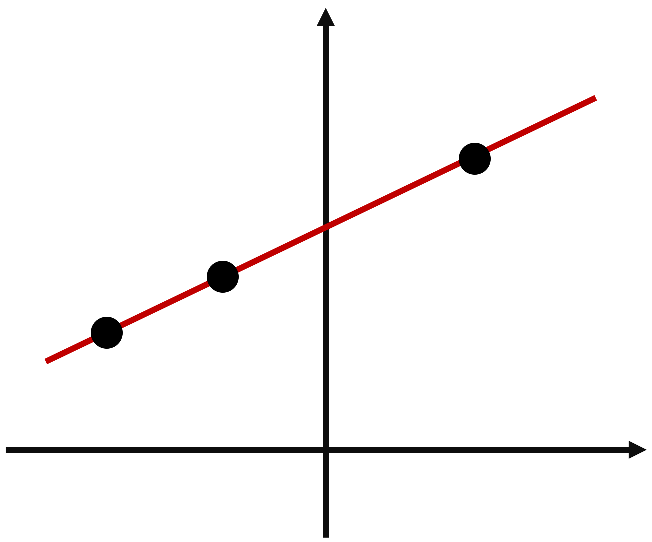
3 points

Problem 3: Lagrange Interpolation

- Given $d + 1$ points, there exists a polynomial of degree at most d that passes through these points



2 points



3 points

Problem 3: Lagrange Interpolation

(a) Find polynomial $p_{-1}(x)$ with roots at $x = 0, 1$ and passes through $(-1, 1)$

For simplicity, let's ignore $(mod\ 5)$

Recall that if polynomial f has roots at $x = a$

$$f(x) = (x - a) \cdot q(x)$$

$$p_{-1}(x) = k(x - 0)(x - 1)$$

Since it passes through $(-1, 1)$, we can solve for k

$$p_{-1}(x) = \frac{\boxed{(x - 0)(x - 1)}}{\boxed{(-1 - 0)(-1 - 1)}}$$

Roots

Ensure that $p_{-1}(-1) = 1$

Problem 3: Lagrange Interpolation

$$a \equiv 1 \pmod 3$$
$$\boxed{\begin{aligned} a &\equiv 0 \pmod 5 \\ a &\equiv 0 \pmod 7 \end{aligned}}$$

$$p_{-1}(-1) = 1$$
$$\boxed{\begin{aligned} p_{-1}(0) &= 0 \\ p_{-1}(1) &= 0 \end{aligned}}$$

Step 1: Combine equation with zeros (divisibility argument)

$$a = 5 \cdot 7 \cdot k$$

$$p_{-1}(x) = x \cdot (x-1) \cdot k$$

Step 2: Solve for k

$$a = 5 \cdot 7 \cdot k \equiv 1 \pmod 3$$

$$\begin{aligned} 1 &= p_{-1}(-1) \\ &= (-1-0) \cdot (-1-1) \cdot k \end{aligned}$$

Problem 3: Lagrange Interpolation

(b) Find polynomial $p_0(x)$ with roots at $x = -1, 1$ and passes through $(0, 1)$

$$p_0(x) = k(x+1)(x-1)$$

$$p_0(x) = \frac{(x+1)(x-1)}{(0+1)(0-1)}$$

(c) Find polynomial $p_1(x)$ with roots at $x = -1, 0$ and passes through $(1, 1)$

$$p_1(x) = k(x+1)(x-0)$$

$$p_1(x) = \frac{(x+1)(x-0)}{(1+1)(1-0)}$$

Problem 3: Lagrange Interpolation

Caveat: We are working in $(mod\ 5)$!

Solution: Take $(mod\ 5)$ of every number

$$p_{-1}(x) = \frac{(x-0)(x-1)}{(-1-0)(-1-1)} = 2^{-1}(x-0)(x-1) = 3x(x-1)$$

$$p_0(x) = \frac{(x+1)(x-1)}{(0+1)(0-1)} = (-1)^{-1}(x+1)(x-1) = 4(x+1)(x-1)$$

$$p_1(x) = \frac{(x+1)(x-0)}{(1+1)(1-0)} = 2^{-1}(x+1)(x-0) = 3x(x+1)$$

Problem 3: Lagrange Interpolation

CRT:

$$\begin{matrix} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{matrix} = 1 \cdot \begin{matrix} a \equiv 1 \pmod{3} \\ a \equiv 0 \pmod{5} \\ a \equiv 0 \pmod{7} \end{matrix} + 3 \cdot \begin{matrix} b \equiv 0 \pmod{3} \\ b \equiv 1 \pmod{5} \\ b \equiv 0 \pmod{7} \end{matrix} + 4 \cdot \begin{matrix} c \equiv 0 \pmod{3} \\ c \equiv 0 \pmod{5} \\ c \equiv 1 \pmod{7} \end{matrix}$$

Now we have:

$$\begin{matrix} p(-1) = 3 \\ p(0) = 1 \\ p(1) = 2 \end{matrix} = 3 \cdot \begin{matrix} p_{-1}(-1) = 1 \\ p_{-1}(0) = 0 \\ p_{-1}(1) = 0 \end{matrix} + 1 \cdot \begin{matrix} p_0(-1) = 0 \\ p_0(0) = 1 \\ p_0(1) = 0 \end{matrix} + 2 \cdot \begin{matrix} p_1(-1) = 0 \\ p_1(0) = 0 \\ p_1(1) = 1 \end{matrix}$$

So $p(x) = 3p_{-1}(x) + p_0(x) + 2p_1(x)$!

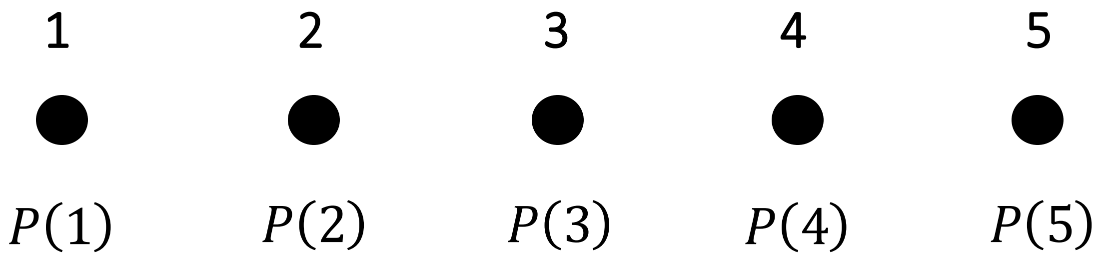
Problem 4: Secret Sharing

Suppose there are 5 people. Devise a scheme such that

- Any group of 3 people can unlock the secret s
- Any group with < 3 people cannot unlock the secret s

Idea: 3 points specify a unique polynomial of degree at most 2

Let P be degree 2 polynomial, with $P(0) = s$

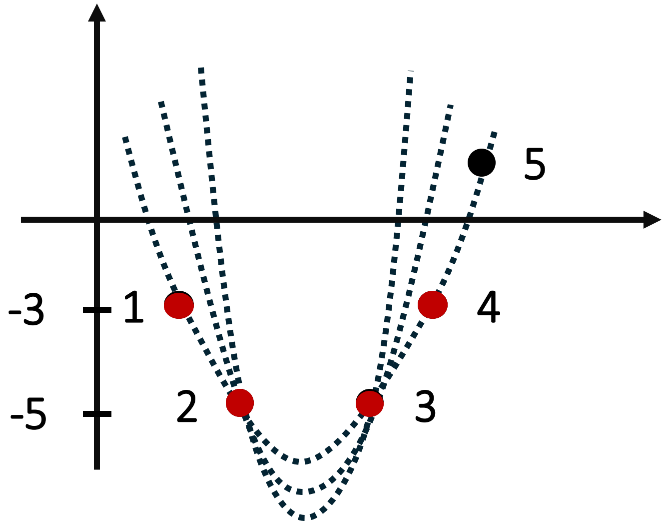


$n = 5$ people

Problem 4: Secret Sharing

Example: Suppose $s = 1$, define $P(x) = x^2 - 5x + 1$

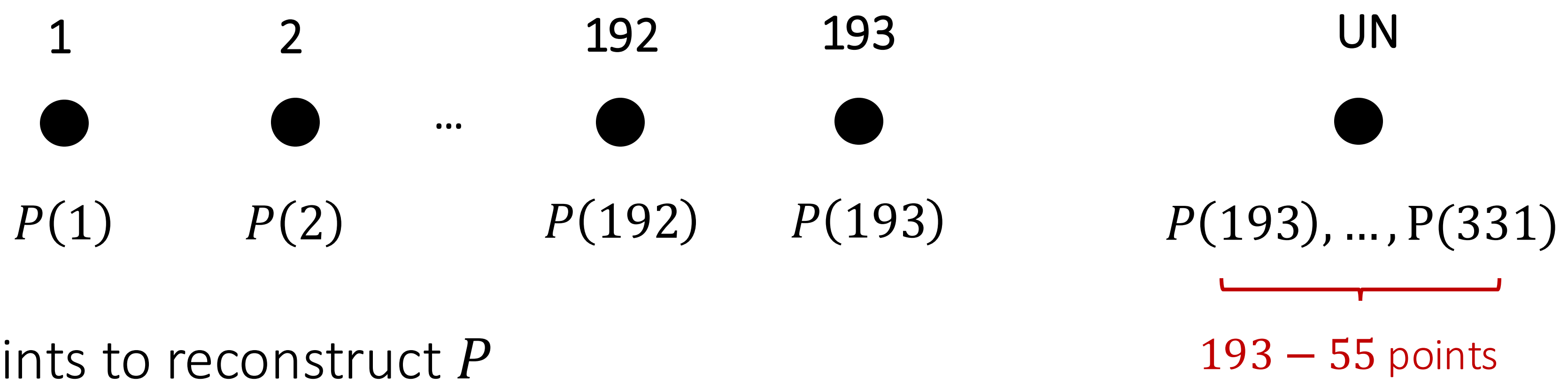
1	2	3	4	5
$P(1)$	$P(2)$	$P(3)$	$P(4)$	$P(5)$
-3	-5	-5	-3	1



Problem 4: Secret Sharing

(a) What if we only considered the first condition?

Consider any polynomial P of degree 192, with $P(0) = s$



Need 193 points to reconstruct P

- Case 1: Need all 193 countries to get 193 points
- Case 2: 55 countries (55 points) + UN Secretary

We need 193 points,

but only got 55 points!

Problem 4: Secret Sharing

(b) Idea: We encode the $P(i)$ as a secret as well!

Consider any polynomial Q of degree 12, with $Q(0) = P(1)$