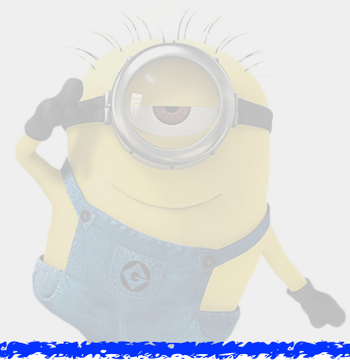
MULTIPARTY COMPUTATION USING SHAMIR'S SECRET SHARING

What does it even mean?

Evil Minions

Good Minions

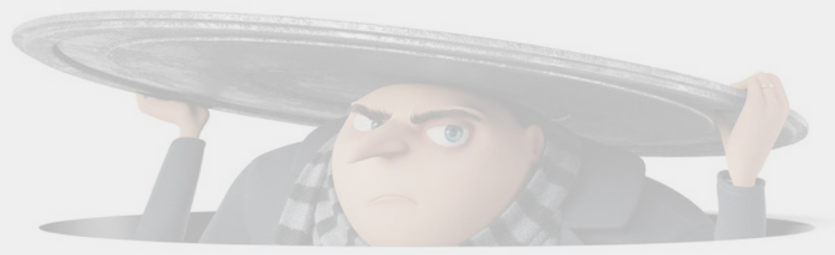


What we want?

At least one good minion participates in the division process

Property of the locks :

Any 3 out of 5 keys can open the cage ;-)



There's always a good guy in the opening process!!

We control the minimum number of people required to open the cage!!

Given n parties

t are corrupted

n-t are good

All interested in some computation such that

At least t+1 needed to do the computation

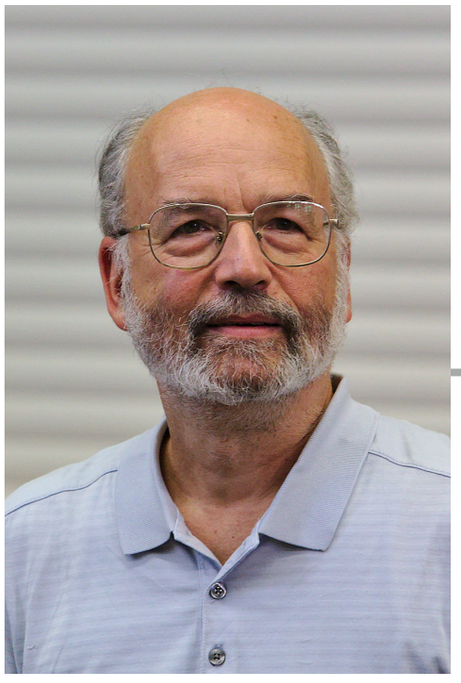
Minions
(good & bad)

Learn the code of lock

MULTIPARTY COMPUTATION

USING

SHAMIR'S SECRET SHARING



Private shares
known just to them

Shamir's Secret Sharing

POLYNOMIALS

POLYNOMIALS

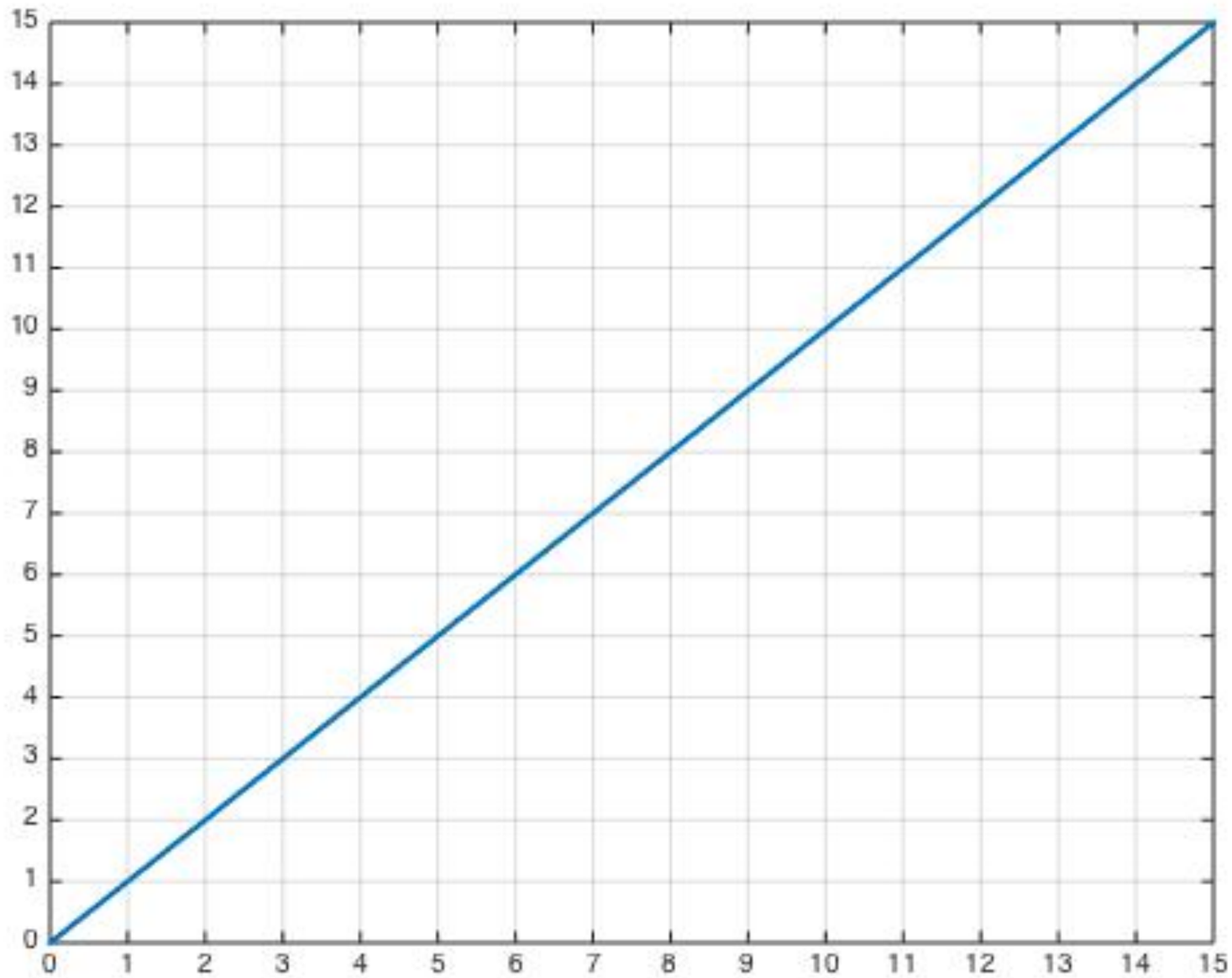
degree

$$a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0$$

- $x - 3$ — 1 — $a_1 x + a_0$
- $2x - 1.3$ — 1
- $5x^2 - 0.5x + 1$ — 2 — $a_2 x^2 + a_1 x + a_0$
- $10x^3 + 9x^2 + 7$ — 3
- 10 — 0

Degree 1 polynomials

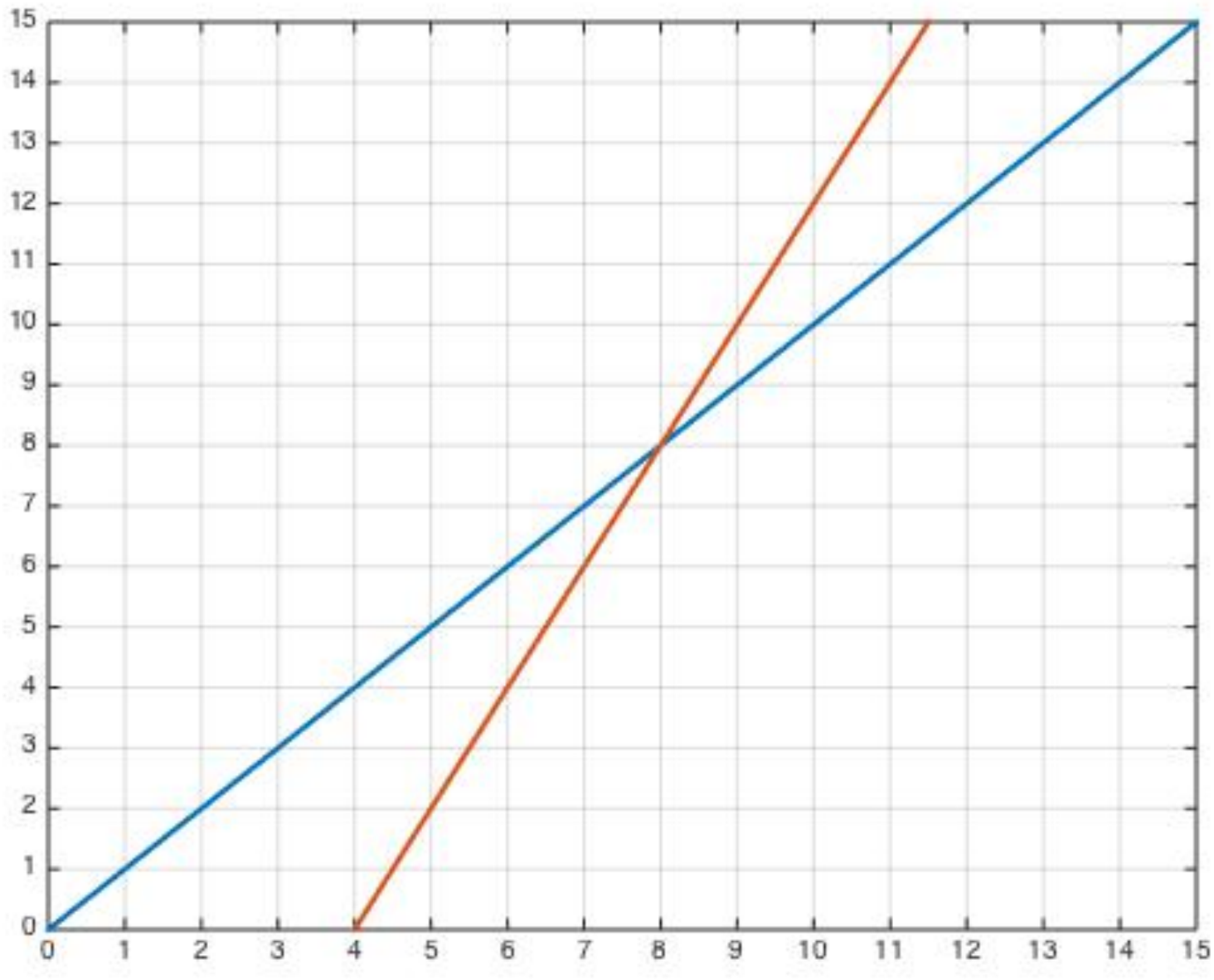
$f(x) = x$



Degree 1 polynomials

$f(x) = x$

$f(x) = 2x - 8$

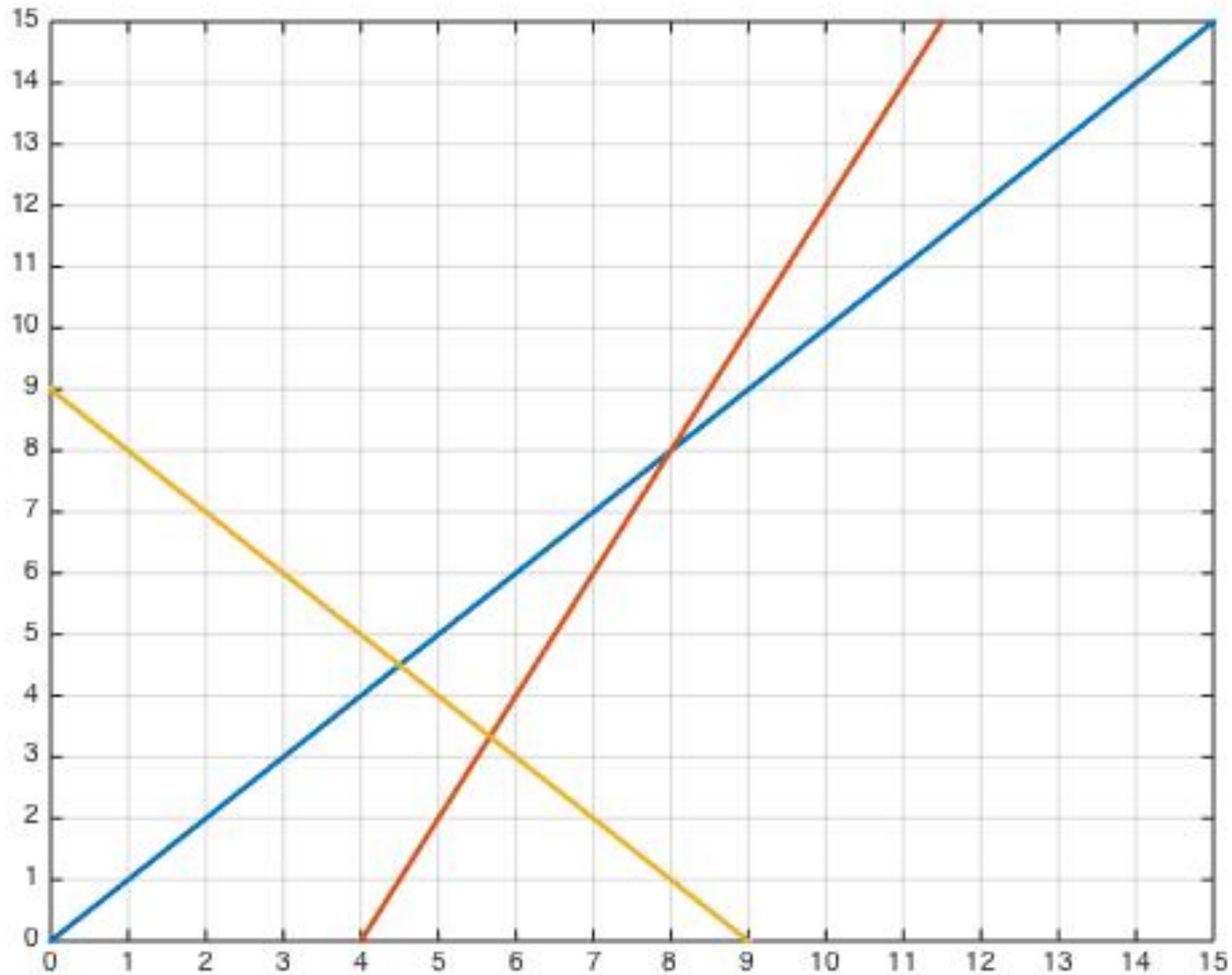


Degree 1 polynomials

f(x) = x

f(x) = 2x - 8

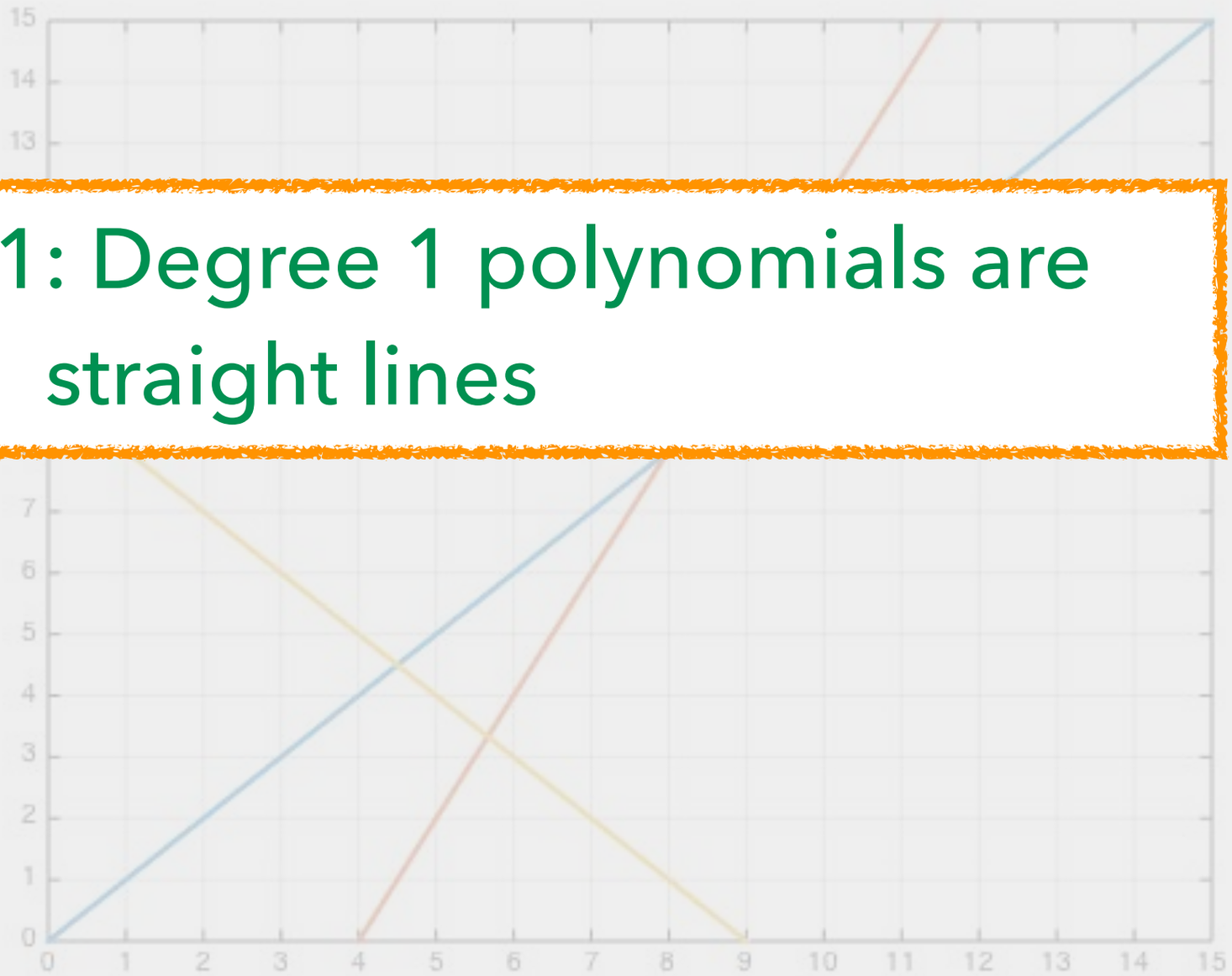
f(x) = -x + 9



Degree 1 polynomials

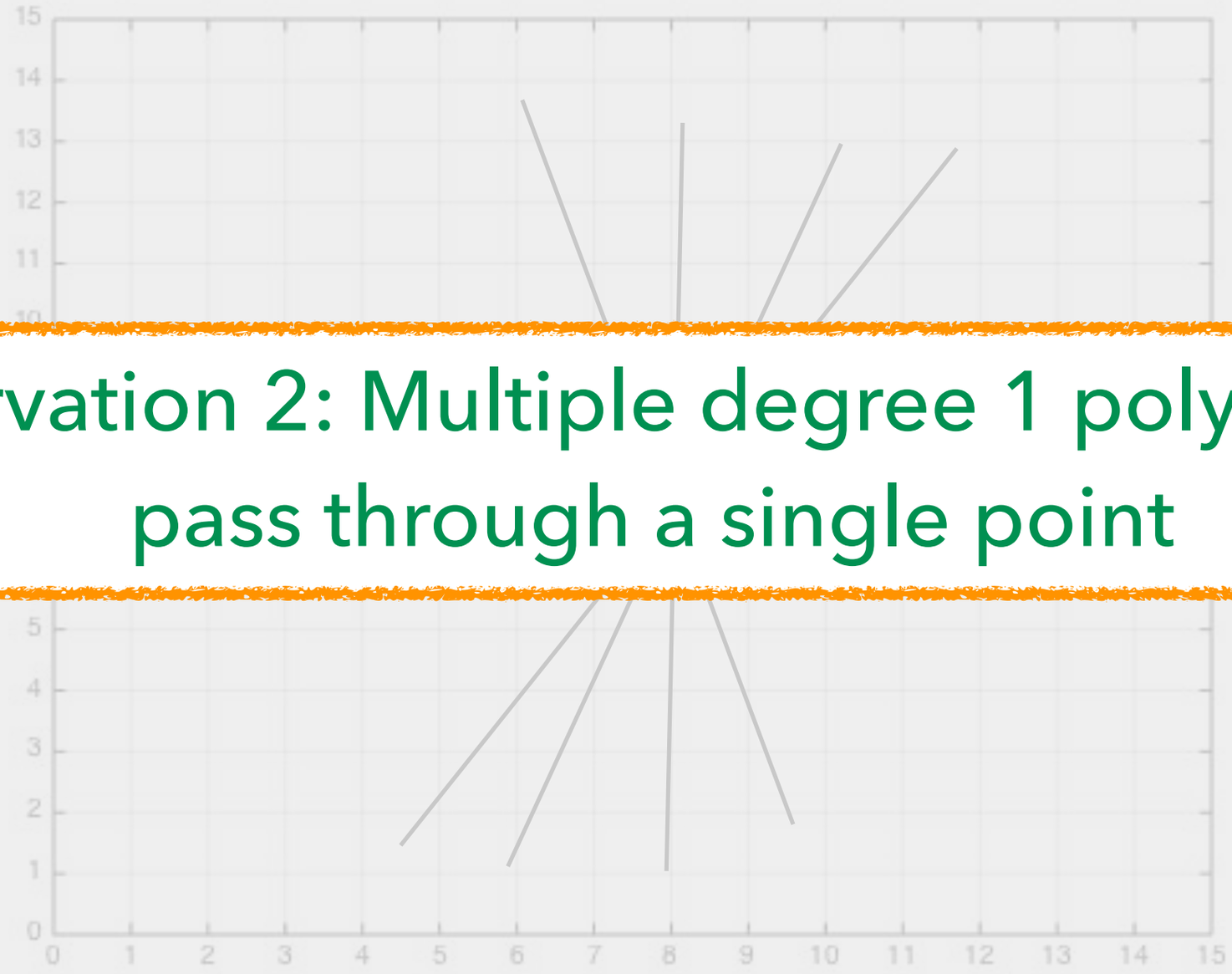
f(x) = x

f(x) = 2x − 8



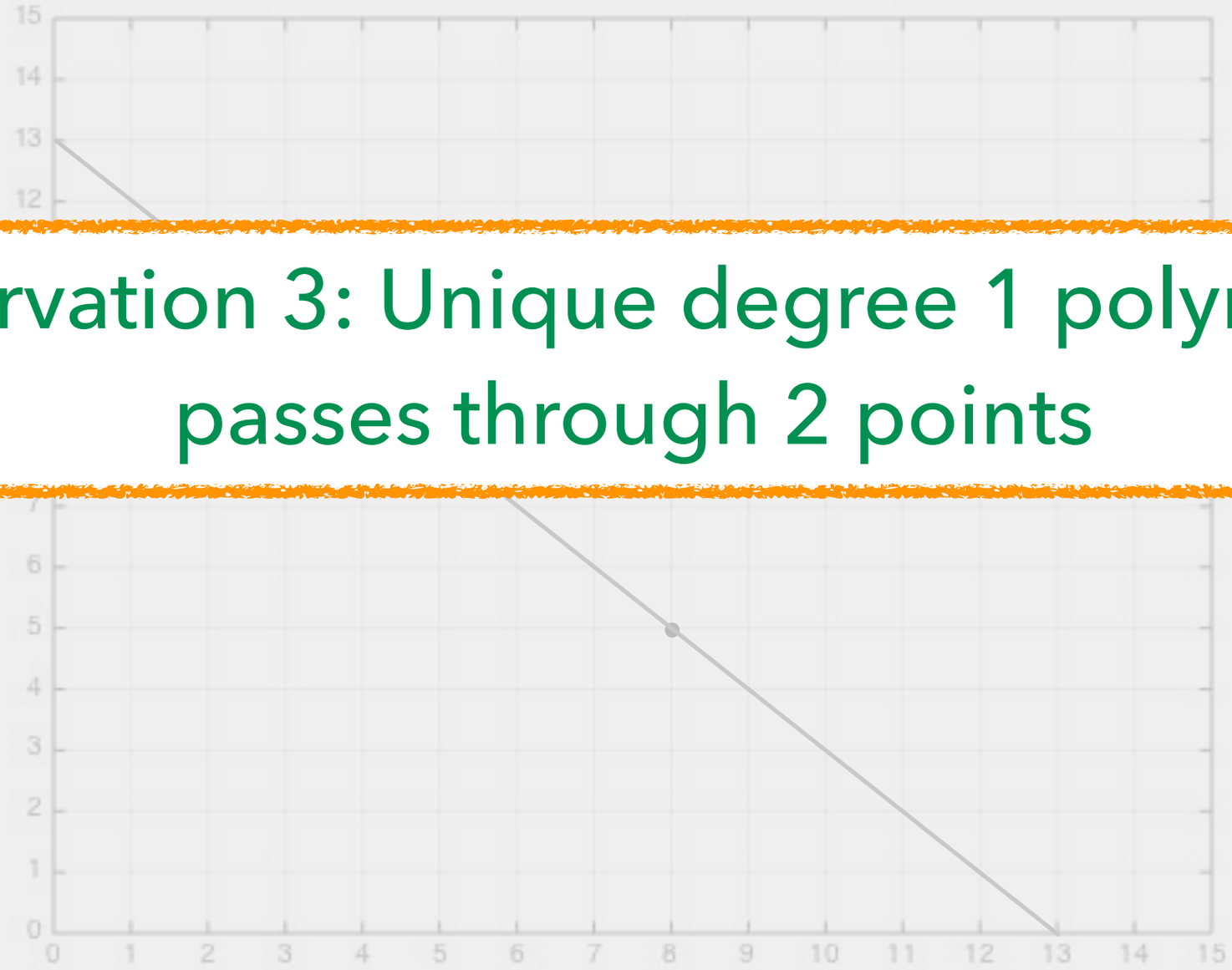
Observation 1: Degree 1 polynomials are straight lines

Degree 1 polynomials



Observation 2: Multiple degree 1 polynomials pass through a single point

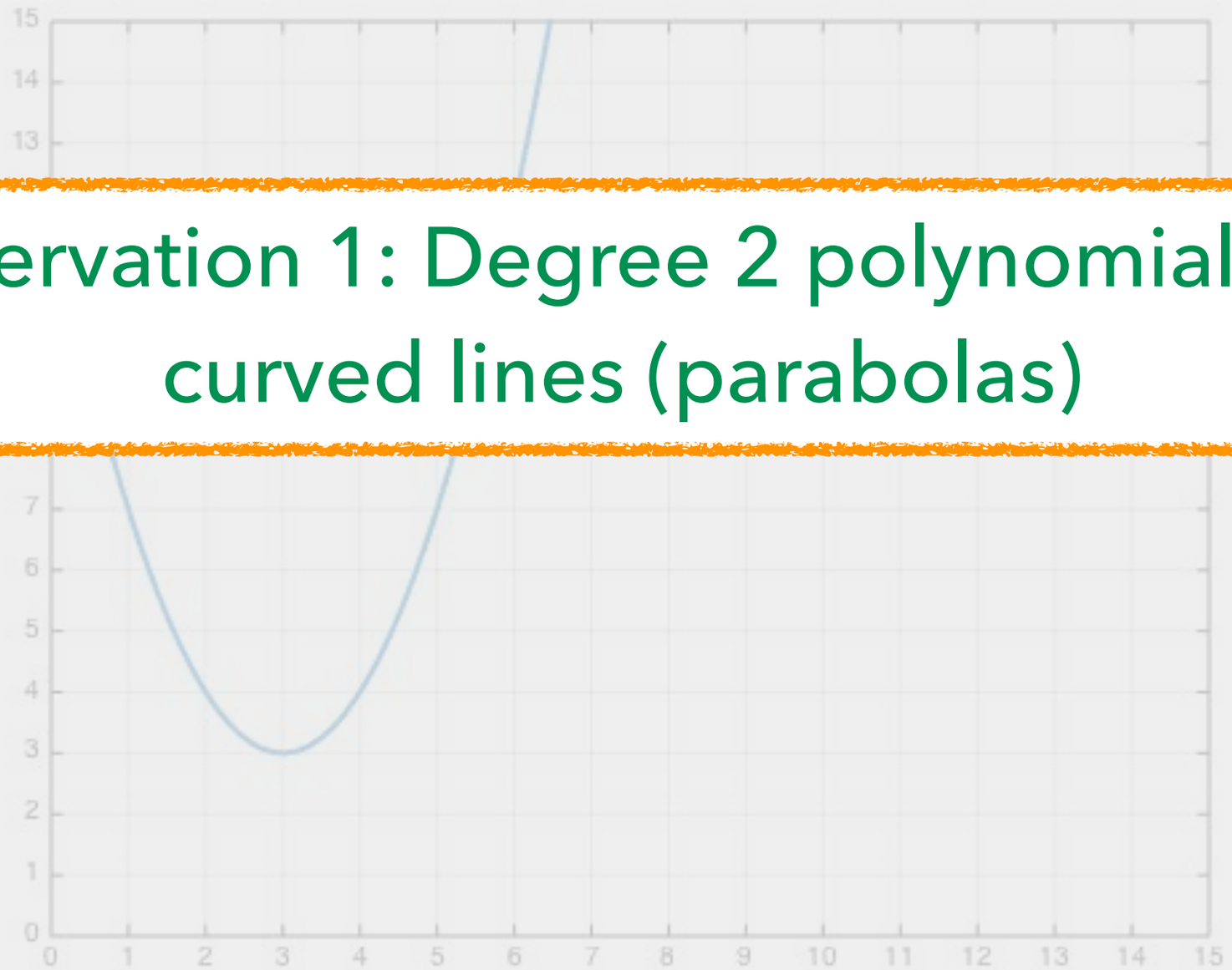
Degree 1 polynomials



Observation 3: Unique degree 1 polynomial passes through 2 points

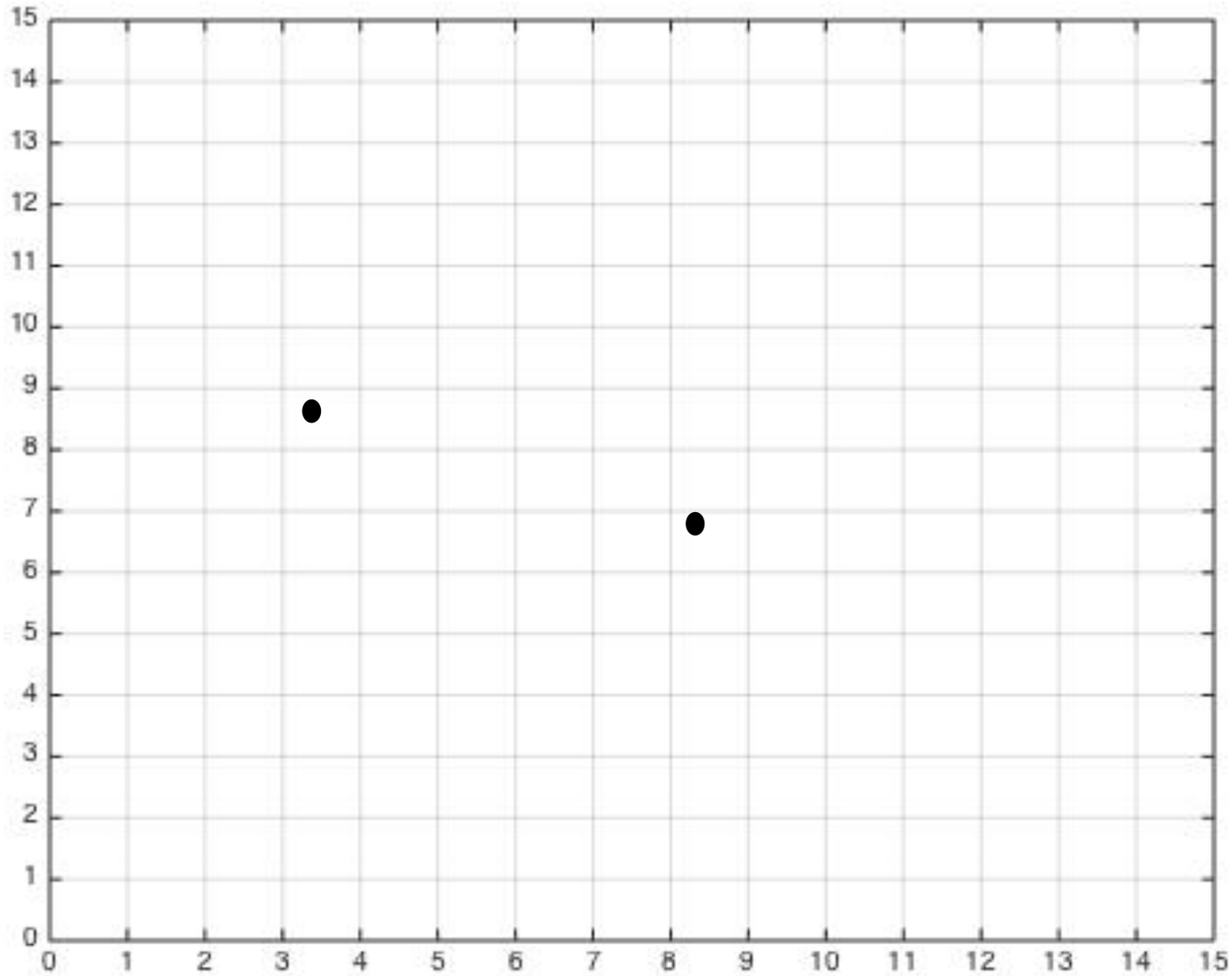
Degree 2 polynomials

$f(x) = x^2 - 6x + 12$

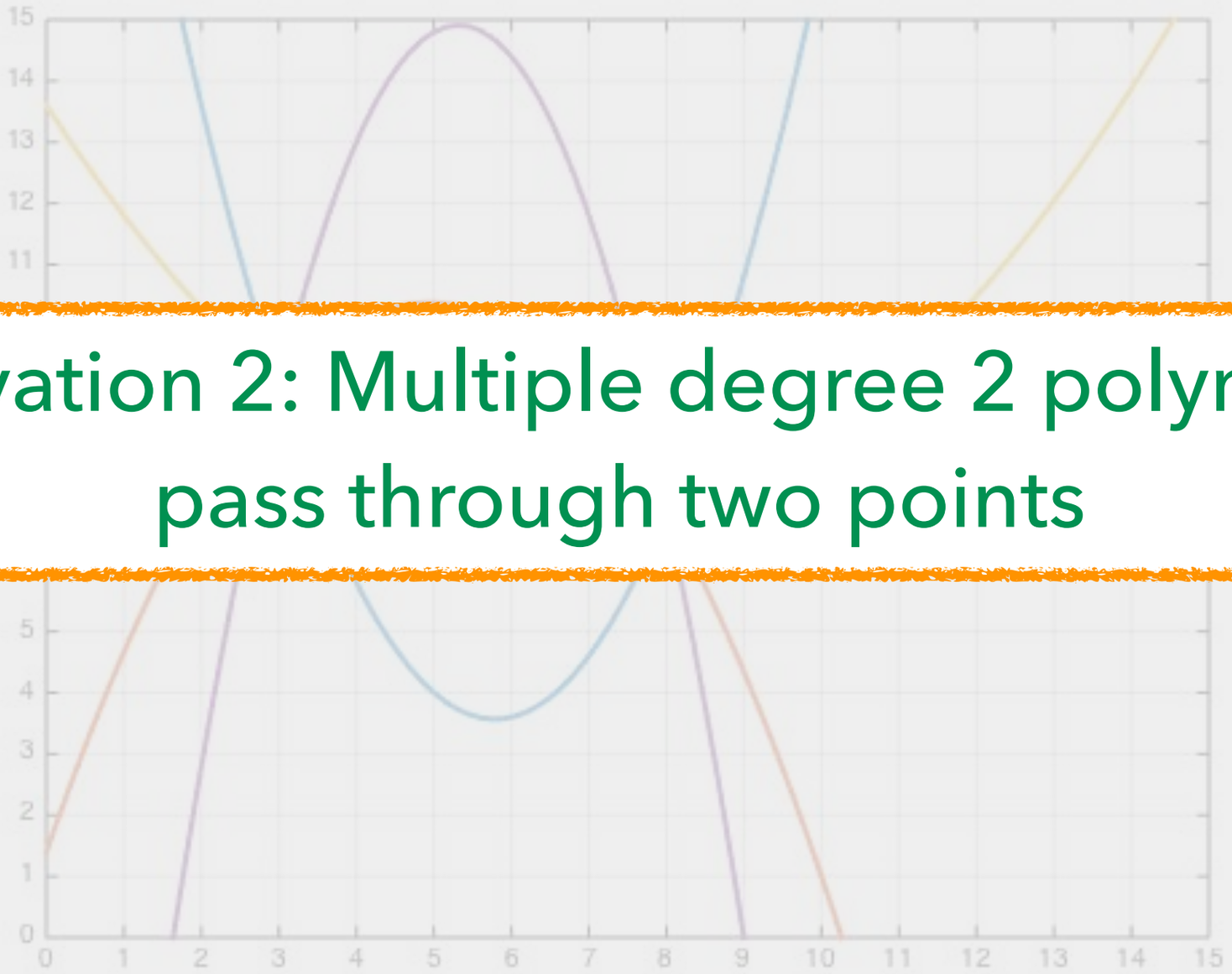


Observation 1: Degree 2 polynomials are curved lines (parabolas)

Degree 2 polynomials



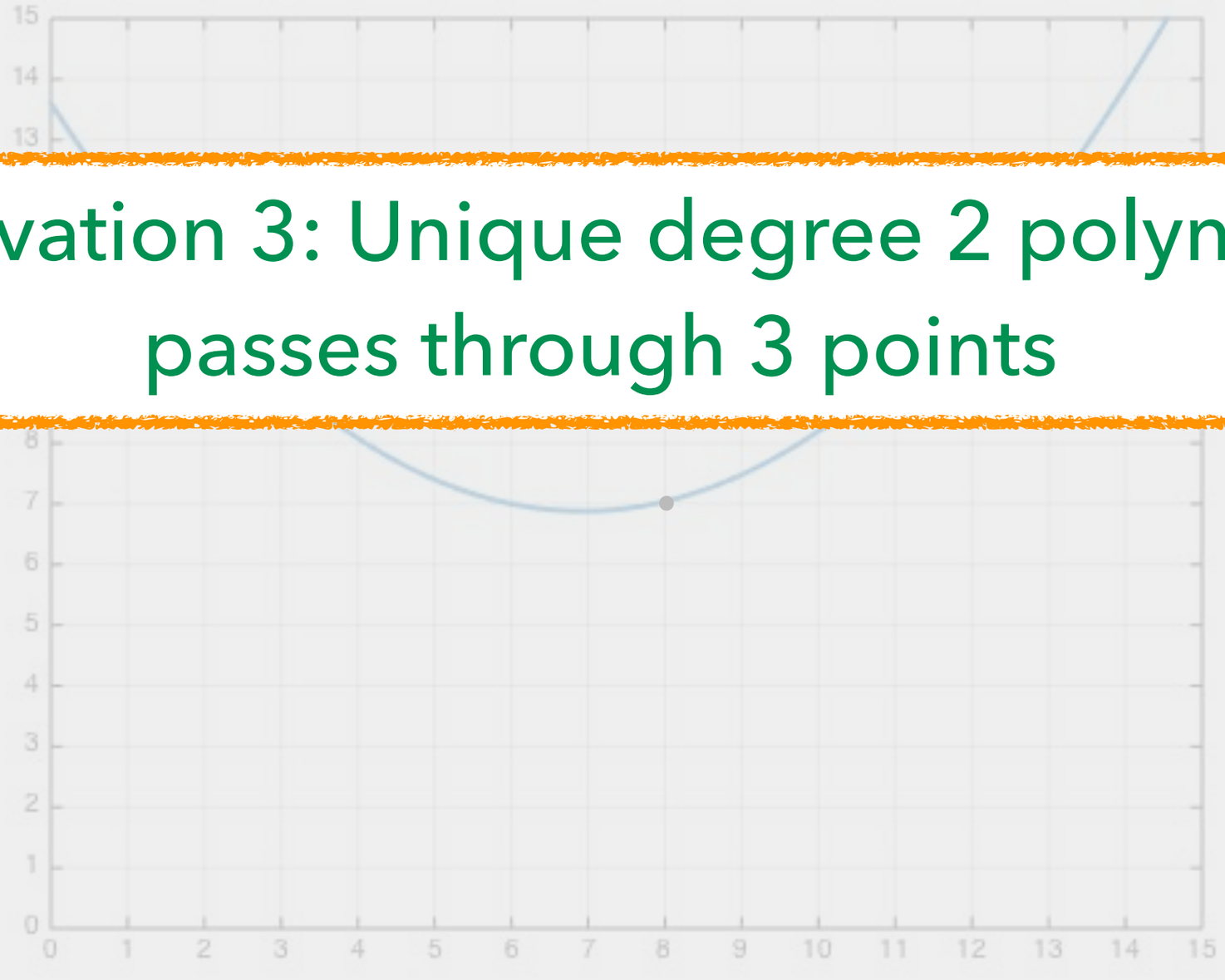
Degree 2 polynomials



Observation 2: Multiple degree 2 polynomials pass through two points

Degree 2 polynomials

$f(x) = 0.140x^2 - 1.94x + 13.6$



Observation 3: Unique degree 2 polynomial passes through 3 points

Property 1 of polynomials

Infinite degree 1 polynomials pass through a single point

Infinite degree 2 polynomials pass through two points

⋮

Infinite degree d polynomials pass through d points

Property 2 of polynomials

Degree 1 polynomial is uniquely determined by 2 points

Degree 2 polynomial is uniquely determined by 3 points

⋮

Degree d polynomial is uniquely determined by d+1 points

But can we protect the BANANA using polynomials

Shamir's secret sharing

Alice

Bob

Charlie

Trusted Gru

Shamir's secret sharing

$$f(x) = -x + 13$$

secret : $f(0) = 13$

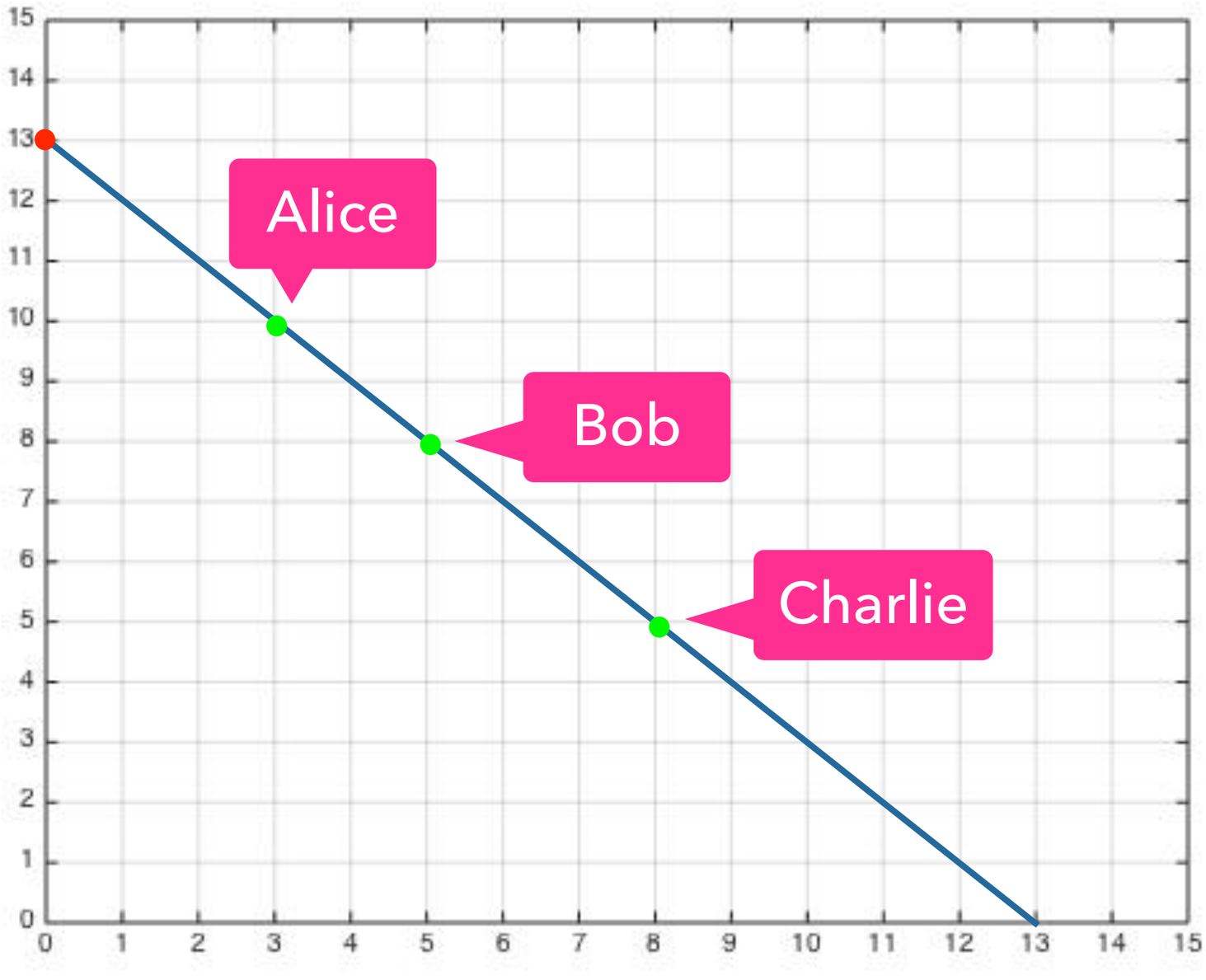
shares : $f(3)$, $f(5)$, $f(8)$

Choose a degree 1 polynomial

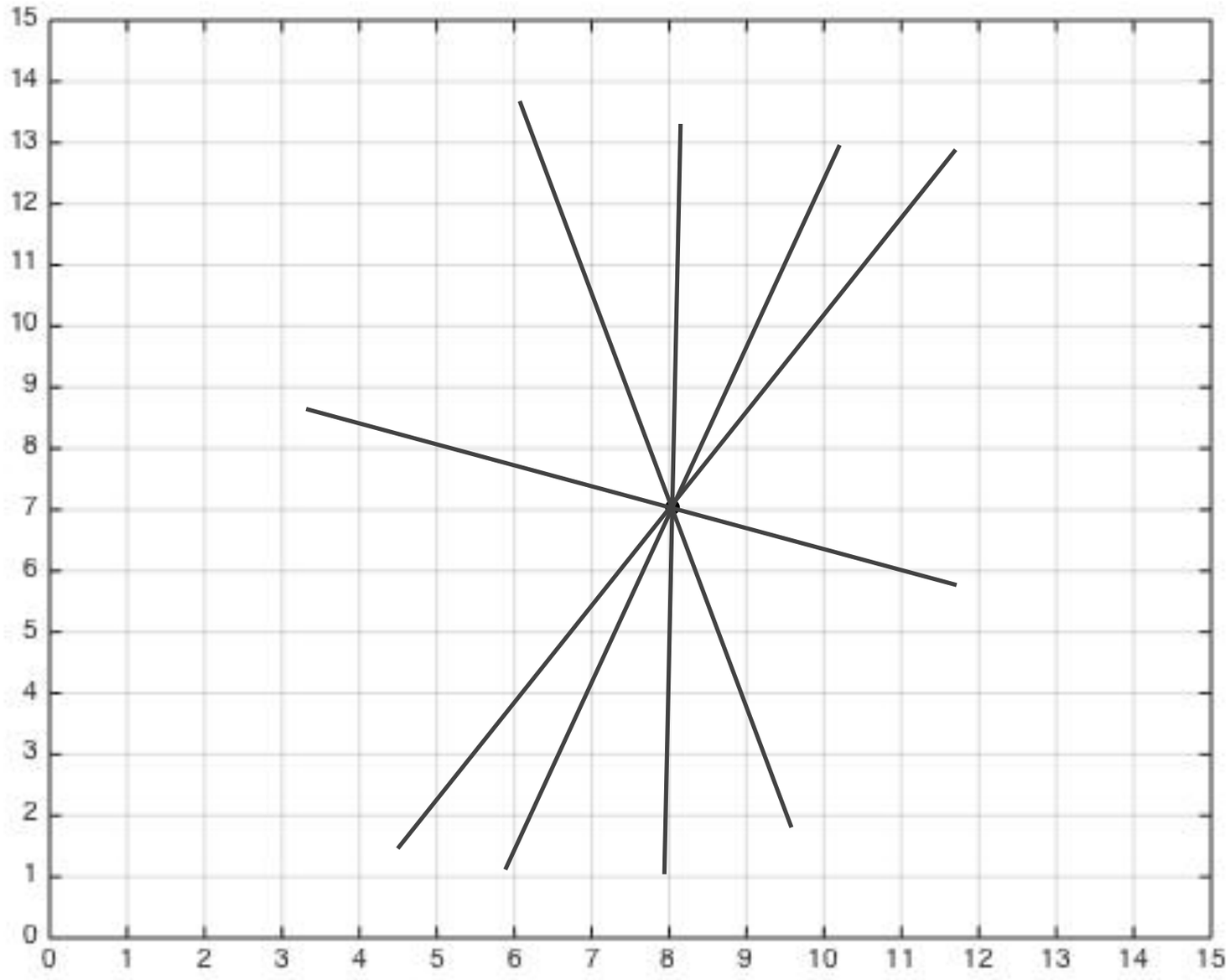
Secret in f(0)

Compute three shares by computing f at three more points

Distribute the shares to the parties

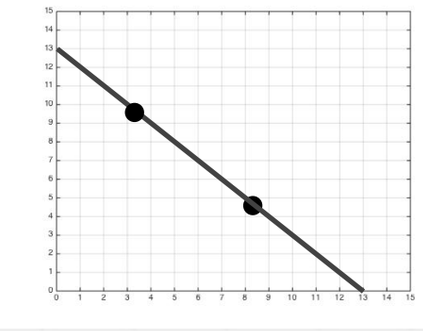


What is making it hard for Charlie to compute the secret using just his share?



Recall

Degree 1 polynomial is uniquely determined by 2 points



shares : f(3) , f(5) , f(8)

Choose a secret degree 1 polynomial

Hide the secret in f(0)

Com

f at three more points

Distribute the shares to the parties

Alice Bob

Bob Charlie

Alice Charlie

Bob

At least 2 points needed to learn f

Once f is learnt, compute the secret f(0)

PLAY TIME

GUESS MY SECRET

What if we need more than 2 people to be able to compute the secret ?

Prop 2: Degree d polynomial is uniquely determined by d+1 points

Ans: Use higher order (degree) polynomial

If t bad people, use a degree t polynomial

Hence, t+1 points needed to "learn" the polynomial

Secure secret sharing

vs

Insecure secret sharing

Anyone with < t+1 shares should not have more information than the one with 0 shares

2 - - -

- 0 - -

- - 1 -

- - - ?

Secure secret sharing

vs

Insecure secret sharing

Anyone with < t+1 shares should not have more information than the one with less

secret : 2017

INSECURE !!

0 Shares

- - - -

10 * 10 * 10 * 10

- 0 - -

- - 1 -

3 Shares

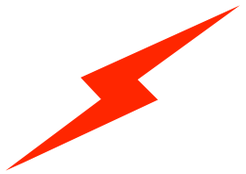
2 0 1 -

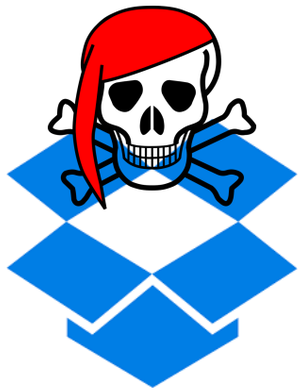
10

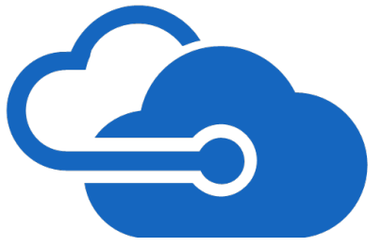
- - - 7

Real World Applications

Uploading personal data

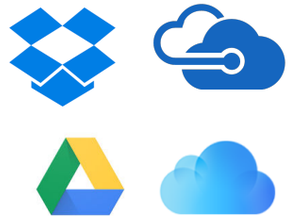




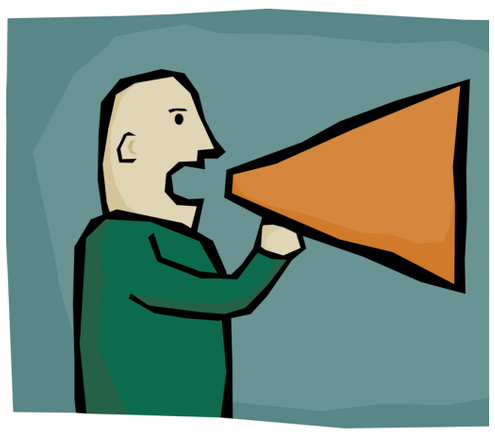


Real World Applications

Uploading personal data



Error Correcting Codes



I will ki I will kill you

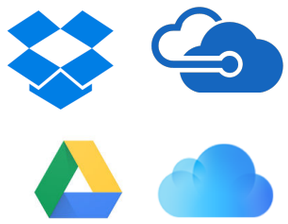
Channel

Sender

Receiver

Real World Applications

Uploading personal data



Error Correcting Codes

Add redundancy to the message to correct the errors introduced

I will kiss you

n shares

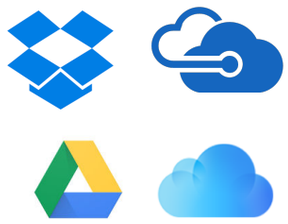
Any t+1 will recreate the message

A lot more corruptions needed to corrupt the message

Precisely, n - t

Real World Applications

Uploading personal data



Error Correcting Codes

Add redundancy to the message to correct the errors introduced

Storing highly sensitive data

- Encryption keys
- Missile launch codes
- Numbered bank accounts

THE MORSE CODE

Questions ?