Polynomials and Secret Sharing

CS70: Discrete Mathematics and Probability Theory

UC Berkeley – Summer 2025

Lecture 10

Ref: Note 8

Today

1. Secret sharing
   The problem
2. Finite fields: $GF(p)$
3. Polynomials
   Commonly seen: over $\mathbb{R}$
   Very useful for us: over $GF(p)$ for prime p
   Properties, evaluation, and interpolation
   Use in secret sharing

Secret Sharing

A secret s is associated with a group of n people, and a "dealer" distributes shares $s_1, s_2, \ldots, s_n$

A (t, n)-threshold secret sharing scheme is a system where:

Secrecy: Any group of $t - 1$ people get no information about secret.

Recovery: Any group of t can combine their shares to compute the secret.

The idea of the day

Two points make a line

Lots of lines go through one point

We'll describe Shamir's Secret Sharing Scheme.

Same Shamir as the "S" in RSA

Based on polynomials — let's review!

Polynomials

A **polynomial** is specified by **coefficients** $a_d, \dots a_0$:

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

$P(x)$ **contains** point (a, b) if $b = P(a)$.
Sometimes say "point (a, b) is on the polynomial $P(x)$"

For the next few slides: $a_1, \dots, a_d \in \mathbb{R}$ and $x \in \mathbb{R}$.

Degree of a polynomial is largest d such that a_d is non-zero
Note: Often polynomial of degree d means "at most d"
$\Rightarrow$ No non-zero coefficient a_k with $k > d$

Special names for some degrees:
Degree 1 polynomial is a *linear function* (plots a *line*)
Degree 2 polynomial is a *quadratic function* (plots a *parabola*)

Concept Check: Polynomials

Consider polynomials:

$$P(x) = 3x^3 + 4x^2 + 5x + 2$$

$$Q(x) = 2x^2 + 3x + 4$$

What is a_1 for $P(x)$? ___5___

What is a_0 for $Q(x)$? ___4___

What is $P(0)$? ___2___

What is $Q(1)$? ___9___

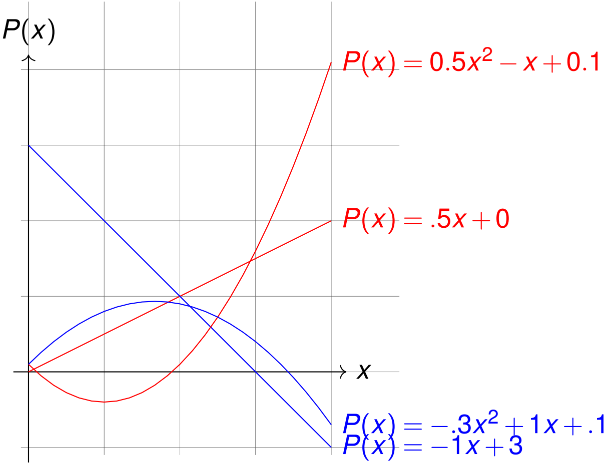
What is the degree of $P(x)$? ___3___

What is the degree of $Q(x)$? ___2___

What is degree of $Q(x) + P(x)$? ___3___

What is degree of $Q(x)P(x)$? ___5___

Line: $P(x) = a_1 x + a_0 = mx + b$



Parabola: $P(x) = a_2 x^2 + a_1 x + a_0 = ax^2 + bx + c$

Finite Fields and Polynomials

A *Finite Field* is a set S with operations $+$ and $\cdot$
... that satisfy certain properties.
For now: just know the term and that is supports $+$ and $\cdot$

For prime p, the *Galois Field* of size p (denoted $GF(p)$) consists of:
The set $\{0,1,\ldots,p-1\}$
$+$ operation is addition mod p
$\cdot$ operation is multiplication mod p

All we need for polynomials is addition and multiplication, so...

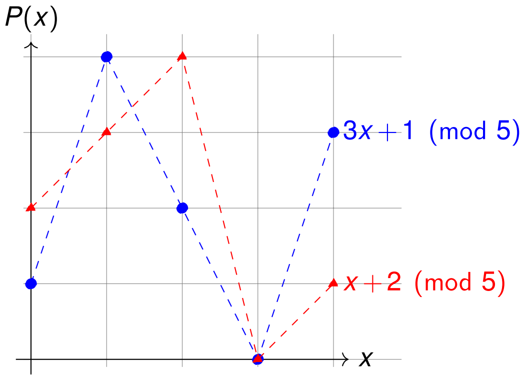
A **polynomial over** $GF(p)$ is

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

where $a_d, \ldots, a_0 \in GF(p)$, $x \in GF(p)$, and operations are performed mod p.

Awkward reality we'll get back to: Need p "large enough" for our polynomials

Polynomial: $P(x) = a_d x^d + \cdots + a_0 \pmod p$



Finding an intersection of points with different slopes (different m)

$$x+2 \equiv 3x+1 \pmod 5$$
$$\implies 2x \equiv 1 \pmod 5 \implies x \equiv 3 \pmod 5$$

Multiplicative inverse of 2 mod 5 is 3.

$GF(p)$ with prime $p \implies$ mult inverse for any $a \neq 0$
$\implies ax \equiv b \pmod p$ always has a unique solution

Two Points Make a Line...

Fact: Given $d+1$ points with different x values, there is exactly one polynomial of degree $\leq d$ that contains those points.

Two points specify a line.

Three points specify a parabola.

This is true for polynomials over $\mathbb{R}$ *and* polynomials over $GF(p)$.

Quick Facts

Two points determine a line.

Say points are (x_1, y_1) and (x_2, y_2)

Important facts associated with this:

(A) Line is $y = mx + b$ (Remember slope/intercept form?)

(B) Plug in a point gives an equation: $y_1 = mx_1 + b$

(C) Plug in a point gives an equation: $y_2 = mx_2 + b$

(D) Two equations, two unknowns (m and b)

(E) Unique solution as long as $x_1 \neq x_2$

Notation: Two Points on a Line

Polynomial: $a_n x^n + \cdots + a_0$.

Question: Which are true for line $mx + b$?

(A) $a_1 = m$

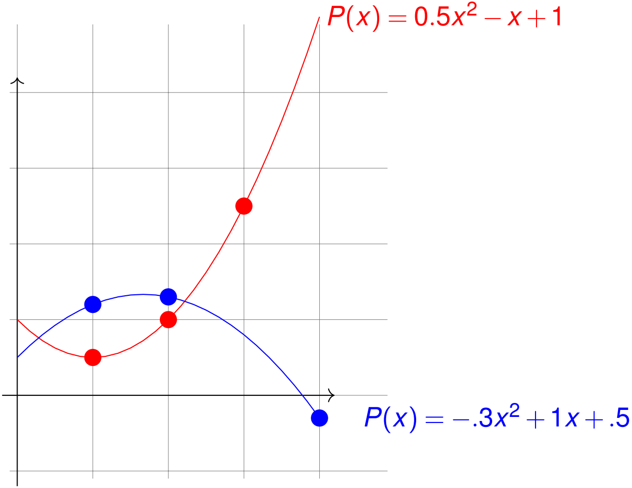
(B) $a_1 = b$

(C) $a_0 = m$

(D) $a_0 = b$

Answer: (A) and (D)

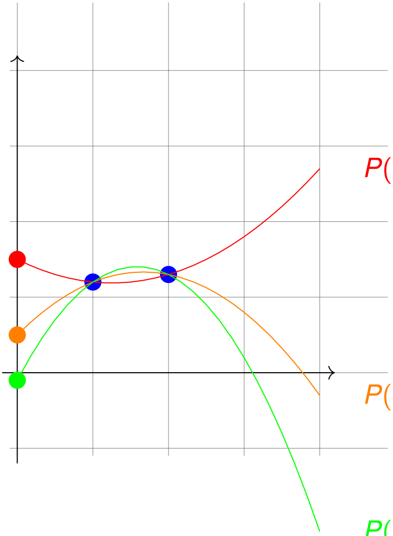
3 points determine a parabola.



Fact: Exactly 1 degree $\leq d$ polynomial contains $d+1$ given points. [1]

[1] Points with different x values.

2 points not enough.



$P(x) = .2x^2 - .5x + 1.5$

$P(x) = -.3x^2 + 1x + .5$

$P(x) = -.6x^2 + 1.9x - .1$

There is $P(x)$ contains blue points and *any* $(0, y)$!

Modular Arithmetic and Secrets

Shamir's (k,n)**-threshold Scheme:** Uses an appropriate p (more later...)

Secret $s \in GF(p)$

1. Choose $a_0 = s$, and random $a_1, \ldots, a_{k-1} \in GF(p)$
2. Let $P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots a_0$ (with $a_0 = s$)
3. Share i is point $(i, P(i))$ (Remember: evaluate mod p)

Recovery: Any k shares gives secret:
Knowing k pts $\implies$ only one $P(x)$ $\implies$ evaluate $P(0)$.

Secrecy: Any $k-1$ shares give nothing:
Knowing $\leq k-1$ pts $\implies$ any $P(0)$ is possible.

Quick Check!

The polynomial from the scheme: $P(x) = 2x^2 + 1x + 3 \pmod 5$.

The secret is: __3__

Share 1 is $(1, y_1)$, where $y_1 =$ __1__

Note: Equivalent to have $y_1 = 6$, but keep small for efficiency!

Share 2 is $(2, y_2)$, where $y_2 =$ __3__

True/False: We could use $(0,3)$ as a share. _False_

That's the secret!

True/False: There is a degree-2 polynomial through $(1, y_1)$, $(2, y_2)$, for *any* secret $s \in GF(5)$ _True_

For a line, $a_1 x + a_0 = mx + b$ contains points $(1,3)$ and $(2,4)$.

$$\begin{aligned} P(1) = m \cdot 1 + b &\equiv m + b \equiv 3 \pmod{5} \\ P(2) = m \cdot 2 + b &\equiv 2m + b \equiv 4 \pmod{5} \end{aligned}$$

Subtract first from second: b's cancel to get $m \equiv 1 \pmod{5}$

Now:

$$\begin{aligned} m + b &\equiv 3 \pmod{5} \\ m &\equiv 1 \pmod{5} \end{aligned}$$

Backsolve: $b \equiv 2 \pmod{5}$. Secret is 2.

And the line is...

$$y = x + 2 \pmod{5}.$$

Interpolation for Quadratics

For a quadratic polynomial, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$.

Plug in points to find equations.

$$\begin{aligned} P(1) = a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ P(2) = 4a_2 + 2a_1 + a_0 &\equiv 4 \pmod 5 \\ P(3) = 4a_2 + 3a_1 + a_0 &\equiv 0 \pmod 5 \end{aligned}$$

$$\begin{aligned} a_2 + a_1 + a_0 &\equiv 2 \pmod 5 \\ 3a_1 + 2a_0 &\equiv 1 \pmod 5 \\ 4a_1 + 2a_0 &\equiv 2 \pmod 5 \end{aligned}$$

Subtracting 2nd from 3rd yields: $a_1 = 1$.
$a_0 = (2 - 4(a_1))2^{-1} = (-2)(2^{-1}) = (3)(3) = 9 \equiv 4 \pmod 5$
$a_2 = 2 - 1 - 4 \equiv 2 \pmod 5$

So polynomial is $2x^2 + 1x + 4 \pmod 5$

General: For k Points

Given points: $(x_1, y_1); (x_2, y_2) \cdots (x_k, y_k)$.

Solve...

$$
\begin{array}{rcll}
a_{k-1}x_1^{k-1} + \cdots + a_0 & \equiv & y_1 & \pmod{p} \\
a_{k-1}x_2^{k-1} + \cdots + a_0 & \equiv & y_2 & \pmod{p} \\
 & \cdot & & \\
 & \cdot & & \\
a_{k-1}x_k^{k-1} + \cdots + a_0 & \equiv & y_k & \pmod{p}
\end{array}
$$

Will this always work?

As long as solution **exists** and it is **unique!** And...

Modular Arithmetic Fact: Exactly 1 degree $\leq d$ polynomial with arithmetic modulo prime p contains $d+1$ pts.

Another Construction: Lagrange Interpolation!

For a quadratic, $a_2x^2 + a_1x + a_0$ hits $(1,2);(2,4);(3,0)$.

Find $\Delta_1(x)$ polynomial contains $(1,1);(2,0);(3,0)$.

Zeros at $x = 2$ and $x = 3$... Try $(x-2)(x-3) \pmod 5$.

Plug in $x = 1$: $(x-2)(x-3) = (1-2)(1-3) = (-1)(-2) = 2 \pmod 5$

Oops – need 1. Idea: Can we divide the whole thing by 2?

No division... but can multiply by inverse of 2 (which is 3 mod 5)

$\Delta_1(x) = 3(x-2)(x-3) = 3x^2 + 3 \pmod 5$ contains $(1,1);(2,0);(3,0)$

$\Delta_2(x) = 4(x-1)(x-3) = 4x^2 + 4x + 2 \pmod 5$ contains (1,0); (2,1); (3,0).

$\Delta_3(x) = 3(x-1)(x-2) = 3x^2 + x + 1 \pmod 5$ contains (1,0); (2,0); (3,1).

Now consider: $P(x) = 2\Delta_1(x) + 4\Delta_2(x) + 0\Delta_3(x)$

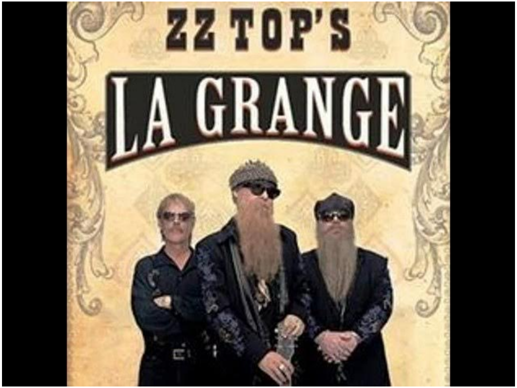
$\Delta_2(x)$ zeros out values at $x = 1$ and $x = 3$, leaving just $x = 2$

1's and 0's enabling/disabling values: a lot like CRT!

Multiplying and adding you get... (really – you do it!)

$P(x) = 2x^2 + x + 4 \pmod 5$ – the same as before.

Quiz



True or False: Billy Gibbons wrote the ZZ Top hit song “La Grange” while studying polynomial interpolation in CS70.

Answer: Ummmm...... no.

Delta Polynomials: General (Any Degree)

For set of x-values, $x_1, \ldots, x_{d+1}$.

$$\Delta_i(x) = \begin{cases} 1, & \text{if } x = x_i. \\ 0, & \text{if } x = x_j \text{ for } j \neq i. \\ ?, & \text{otherwise.} \end{cases}$$

Given $d+1$ points, use Δ_i functions to go through points?
$(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$

Will $y_1\Delta_1(x)$ contain (x_1, y_1)?

Will $y_2\Delta_2(x)$ contain (x_2, y_2)?

Does $y_1\Delta_1(x) + y_2\Delta_2(x)$ contain (x_1, y_1) and (x_2, y_2)? See the idea?

Function that contains all points?

$$P(x) = y_1\Delta_1(x) + y_2\Delta_2(x) \ldots + y_{d+1}\Delta_{d+1}(x)$$

Existence of Interpolating Polynomial

Modular Arithmetic Fact: Exactly 1 degree $\leq d$ polynomial with arithmetic modulo prime p contains $d+1$ pts.

Proof of at least one polynomial: Use $\mathbb{R}$ for intuition...
Given points: $(x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})$.

$$\Delta_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)} = \prod_{j \neq i}(x - x_j) \prod_{j \neq i}(x_i - x_j)^{-1}$$

Numerator is 0 at $x_j \neq x_i$ (d terms in product $\longrightarrow$ degree d)
"Denominator" makes it 1 at x_i (not really a denominator... mult by inverses)

$\Delta_i(x_j) = 0$ if $i \neq j$ and $\Delta_i(x_i) = 1$

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

hits points $(x_1, y_1); (x_2, y_2) \cdots (x_{d+1}, y_{d+1})$

since $P(x_i) = y_1(0) + y_2(0) \cdots + y_i(1) \cdots + y_{d+1}(0)$

Construction proves the existence of a polynomial!

Uniqueness

Uniqueness Fact. At most one degree d polynomial hits $d+1$ points.

Roots Theorem: Any non-zero degree d polynomial has at most d roots.

For example....

Non-zero line (degree 1 polynomial) can intersect $y=0$ at only one x

A parabola (degree 2), can intersect $y=0$ at only two x's

We'll prove this later...

Proof of "Uniqueness Fact":

Assume two different degree d polynomials $P(x)$ and $Q(x)$ hit the points.

$P(x)$ and $Q(x)$ *different* means $P(x)-Q(x)$ is non-zero.

$P(x)$ and $Q(x)$ have degree d, so $P(x)-Q(x)$ is degree $\leq d$.

They both hit the same $d+1$ points, so difference is zero at those points.

$\Rightarrow P(x)-Q(x)$ is non-zero degree d with $d+1$ roots. Contradiction! $\square$

To prove Roots Theorem, need to review polynomial division...

Polynomial Division

Divide $4x^2 - 3x + 2$ by $(x - 3)$ modulo 5.

```
              4x + 4   remainder 4
      -----------------
x - 3 ) 4x^2 - 3x + 2
        4x^2 - 2x
        ----------
              4x + 2
              4x - 2
              -------
                   4
```

$4x^2 - 3x + 2 \equiv (x-3)(4x+4) + 4 \pmod 5$

In general, divide $P(x)$ by $(x-a)$ gives $Q(x)$ and remainder r.

That is, $P(x) = (x-a)Q(x) + r$ where $Q(x)$ has degree $d-1$.

Proof of Roots Theorem

Lemma 1: $P(x)$ has root a iff $P(x)/(x-a)$ has remainder 0:
$P(x) = (x-a)Q(x)$ where $Q(x)$ has degree $d-1$.

Proof: Divide $P(x)$ by $x-a$ to get $P(x) = (x-a)Q(x) + r$.
Evaluate at a: $P(a) = (a-a)Q(a) + r = r$. So a is a root iff $r = 0$. $\square$

Lemma 2: $P(x)$ has roots $r_1, \ldots, r_d \implies P(x) = c(x-r_1)(x-r_2)\cdots(x-r_d)$.

Proof Sketch: By induction on number of roots.

Base case (one root r_1): $P(x) = a_0$ can't work unless $a_0 = 0$.
But degree 1 works, with $P(x) = c(x-r_1)$.

Induction Step: $P(x) = (x-r_1)Q(x)$ by Lemma 1.
$Q(x)$ covers remaining $d-1$ roots, $r_2, r_3, \ldots, r_d$
By IH, $Q(x) = c(x-r_2)(x-r_3)\cdots(x-r_d)$
Multiply by $(x-r_1)$ to get $P(x)$... $\square$

So non-zero $P(x)$ with $d+1$ roots $\implies P(x)$ has degree is at least $d+1$.

Contraposition is...
Non-zero $P(x)$ has degree $\leq d \implies P(x)$ has at most d roots.
*The **Roots Theorem**!*

$GF(p)$ and Polynomial Degrees

Proofs generally work for polynomials over $\mathbb{R}$ and over $GF(p)$.

However, some constraints between p and degree of polynomial

Constraint 1 – General $GF(p)$ Polynomial Issue:

From FLT (and special case for $x = 0$), $x^p \equiv x \pmod{p}$

$\Rightarrow$ Degrees $\geq p$ aren't really higher degrees...

If you need degree k polynomials (secret-sharing), make sure $p \geq k$

Constraint 2 – Specific to Secret-Sharing:

For n participants, need secret value at $x = 0$ and n shares at $x = 1, \ldots n$.

$\Rightarrow$ Highest x value mod p is $p - 1$, so need $p \geq n + 1$.

Want to do secret sharing with 5 people?

$\Rightarrow$ Can't use $GF(5)$ – smallest usable is $GF(7)$.

In reality: p is generally much larger than n, so not an issue...

Secret Sharing

Shamir's (k,n)-threshold Scheme: Using prime $p \geq n+1$,

Secret $s \in GF(p)$

1. Choose $a_0 = s$, and random $a_1, \ldots, a_{k-1} \in GF(p)$
2. Let $P(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots a_0$ (with $a_0 = s$)
3. Share i is point $(i, P(i))$ (Remember: evaluate mod p)

Recovery: Any k shares gives secret:
Knowing k pts $\implies$ only one $P(x)$ $\implies$ evaluate $P(0)$.

Secrecy: Any $k-1$ shares give nothing:
Knowing $\leq k-1$ pts $\implies$ any $P(0)$ is possible.

Number Size and Minimality

We need $p \geq n+1$ – how much larger a number do we need?

Bertrand-Chebyshev Theorem: For any $n > 1$, there exists a prime p such that $n < p < 2n$.

Interesting history:

Conjectured by Bertrand
Proved by Chebyshev
More elegantly proven by Erdös (the "proofs from the book" guy)

What it means: We can find and use a prime p "not much larger than n"

$\Rightarrow$ In fact, at most a single bit larger than n

Similarly: For b-bit secret, can find p at most one-bit larger.

Can't really hope to do better than this...

Runtime

Runtime: polynomial in k, n, and $\log p$.

All using $(\log_2 p)$-bit numbers:

Share Creation: Multipoint polynomial evaluation
Evaluate degree $k-1$ polynomial n times

Secret Recovery: Polynomial interpolation
Compute k Δ_i polynomials; multiply by constants and add together

Faster algorithms for multipoint evaluation and interpolation?
More appropriate for an algorithms class...

Summary

Two points make a unique line
Existence: Compute solution: m, b.
Unique: Assume two solutions, show they are the same.

$d+1$ points make a unique degree d polynomial.
Existence: Lagrange interpolation
Unique: Assume two solutions, show they are the same.

If you're careful about limiting degree d or making p large enough...
Proofs work for polynomials over $GF(p)$ just like over $\mathbb{R}$
And over $GF(p)$: values from a finite set – all likely

Secret Sharing:
k points on degree $k-1$ polynomial is all we need!
Can hand out n points on polynomial as shares.