Lecture 9: Polynomials

Why Only Have One Nomial?

What Is a Polynomial?

High school: $p(x) = c_d x^d + c_{d-1} x^{d-1} + ... + c_1 x + c_0$

- $d \in \mathbb{N}$ is the *degree*
- $c_d, ..., c_0$ are the *coefficients*

This is *coefficient representation*
Need $d + 1$ coefficients to define deg d polynomial

Today: see *value representation*
Need $d + 1$ function values to define deg d poly

Today, prove that these are equivalent!

Polynomial Long Division

Theorem: Let $p(x)$, $d(x)$ be polys. Then $\exists$ $q(x)$, $r(x)$ st $p(x) = q(x)d(x) + r(x)$ and $\deg(r) < \deg(p)$.

Same idea as elementary school long division!

$$
\begin{array}{rl}
 & x^2x^2 + 3xx^2 + 3x - 1 \\
x^2 - 1 \,\big) & x^4 + 3x^3 - 2x^2 + 0x + 4 \\
 & -(x^4 + 0x^3 - x^2) \\
 & 3x^3 - x^2 + 0x \\
 & -(3x^3 + 0x^2 - 3x) \\
 & -x^2 + 3x + 4 \\
 & -(-x^2 + 0x + 1) \\
 & 3x + 3
\end{array}
$$

Factoring Roots

Lemma: Suppose $p(a) = 0$. Then can write $p(x) = (x - a)q(x)$ st $\deg(q) = \deg(p) - 1$.

Proof:

- Divide $p(x)$ by $(x - a)$ as before
- $p(x) = (x - a)q(x) + r(x)$
- $0 = p(a) = (a - a)q(a) + r(a) = r(a)$
- $\deg(r) < \deg(x - a) = 1$, so $r(x)$ a constant
- Only possibility: $r(x) = 0$!
- Thus $p(x) = (x - a)q(x)$

Number of Groots

Theorem: Non-zero deg d poly has $\leq d$ roots.

Proof:

- By induction on d.
- Base Case ($d = 0$): constant poly, no roots
- Suppose true for degree k
- Let $p(x)$ have degree $k + 1$
- If p has no roots, done
- Else can factor as $(x - a)q(x)$
- 1 root from $(x - a)$, $\leq k$ from $q(x)$
- Total $\leq k + 1$ roots

Limited Agreement

Theorem: Distinct deg d polys agree on $\leq d$ points

Proof:

- Let $p(x)$ and $q(x)$ be distinct, deg $\leq d$
- $p(x) = q(x)$ iff $p(x) - q(x) = 0$
- Note: $p - q$ is non-zero, deg $\leq d$
- So $p - q$ has $\leq d$ roots
- Means $\leq d$ values of x st $p(x) = q(x)$!

Means $d + 1$ values enough to define polynomial

But do any $d + 1$ points work?

First Interpolation

Want degree 1 poly through $(4, 2)$ and $(7, 0)$

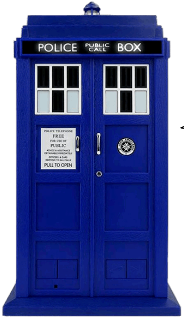
Recall: slope = rise/run
Here: slope $= (0-2)/(7-4) = -\frac{2}{3}$

So $p(x) = -\frac{2}{3}x + c$
Choose c st $p(4) = -\frac{2}{3} \cdot 4 + c = 2$
So $c = 2 + \frac{8}{3} = \frac{14}{3}$

So $-\frac{2}{3}x + \frac{14}{3}$ is unique degree 1 poly!

Bigger Interpolation

Want degree 2 through $(0, -1)$, $(2, 9)$, $(-1, -3)$
Rise/run trick only works for degree 1...



$$\Delta_0(x) = -\tfrac{1}{2}x^2 + \tfrac{1}{2}x + 1$$
$$\Delta_2(x) = \tfrac{1}{6}x^2 + \tfrac{1}{6}x$$
$$\Delta_{-1}(x) = \tfrac{1}{3}x^2 - \tfrac{2}{3}x$$

Take $p(x) = -1\Delta_0(x) + 9\Delta_2(x) - 3\Delta_{-1}(x)$
Works out to $(\frac{1}{2} + \frac{3}{2} - 1)x^2 + (-\frac{1}{2} + \frac{3}{2} + 2)x - 1$
So $p(x) = x^2 + 3x - 1$

Finidng Δ

Goal: $\Delta_0(x)$ st $\Delta_0(0) = 1$, $\Delta_0(2) = \Delta_0(-1) = 0$

Last two easy: take $q_0(x) = (x-2)(x+1)$
Note: $q_0(0) = (0-2)(0+1) = -2$
Take $\Delta_0(x) = -\frac{1}{2}q_0(x)$
Gives $\Delta_0(x) = -\frac{1}{2}(x^2 - x - 2) = -\frac{1}{2}x^2 + \frac{1}{2}x + 1$

For 2, take $q_2(x) = (x-0)(x+1) = x^2 + x$
$\Delta_2(x) = \frac{q_2(x)}{q_2(2)} = \frac{x^2+x}{6} = \frac{1}{6}x^2 + \frac{1}{6}x$

For -1, take $q_{-1} = (x-0)(x-2) = x^2 - 2x$
$\Delta_{-1}(x) = \frac{q_{-1}(x)}{q_{-1}(-1)} = \frac{x^2-2x}{3} = \frac{1}{3}x^2 - \frac{2}{3}x$

Lagrange Interpolation

Theorem: Given points $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$, can construct deg (at most) d poly through them.

Proof:

- Suppose have polys $\Delta_i(x)$ st
  - $\Delta_i(x_i) = 1$
  - $\Delta_i(x_j) = 0$ for $j \neq i$
- Take $p(x) = y_1\Delta_1(x) + \ldots + y_{d+1}\Delta_{d+1}(x)$
- To construct $\Delta_i(x)$:
  - Take $q_i(x) = \prod_{j \neq i}(x - x_j)$
  - Let $\Delta_i(x) = \frac{q_i(x)}{q_i(x_i)}$

Note similarities to CRT!

Lagrange Example

Find deg 2 poly through $(1,6)$, $(6,1)$, $(7,0)$

$$\Delta_1(x) = \frac{(x-6)(x-7)}{(1-6)(1-7)} = \frac{1}{30}x^2 - \frac{13}{30}x + \frac{42}{30}$$

$$\Delta_6(x) = \frac{(x-1)(x-7)}{(6-1)(6-7)} = -\frac{1}{5}x^2 + \frac{8}{5}x - \frac{7}{5}$$

$$\Delta_7(x) = \frac{(x-1)(x-6)}{(7-1)(7-6)} = \frac{1}{6}x^2 - \frac{7}{6}x + 1$$

So take $p(x) = 6\Delta_1(x) + 1\Delta_6(x) + 0\Delta_7(x)$
$6\Delta_1(x) = \frac{1}{5}x^2 - \frac{13}{5}x + \frac{42}{5}$
$p(x) = (\frac{1}{5}x^2 - \frac{13}{5}x + \frac{42}{5}) + (-\frac{1}{5}x^2 + \frac{8}{5}x - \frac{7}{5}) = -x + 7$

Notice: doesn't have to be degree *exactly* 2!

Break

Break time! Talk to your neighbors!

Today's Discussion Question:
What is your favorite breakfast food?

Get Real

So far, working with polynomials in $\mathbb{R}$

Calculations tend to get messy
Issues with finite precision on computers!

What properties of $\mathbb{R}$ did we actually use?

- Ability to add, multiply, subtract
- Division by non-zero numbers
- Product of non-zero numbers is non-zero

These properties hold in any *field*
Numbers modulo a prime is a field!

Finite Fields

Numbers mod p often denoted $GF(p)$[1]

Note: is important that p is a prime!

Ex: Consider $(x-2)(x-3)$ modulo 6

- Degree two polynomial
- But four roots: 0, 2, 3, 5!

Ex: No deg 1 poly through $(0,0)$ and $(3,1)$ mod 6

- Go through $(0,0)$ means $c_0 = 0$
- Go through $(3,1)$ means $c_1 \cdot 3 \equiv 1 \pmod 6$

---

[1] "GF" stands for "Galois Field"

Finite Field Lagrange

Want deg 2 poly mod 7 through $(0,3)$, $(2,2)$, $(3,0)$

$q_0(x) = (x-2)(x-3) = x^2 - 5x + 6 \equiv x^2 + 2x + 6$
$q_0(0) = 6$, so $q_0(0)^{-1} \equiv 6 \pmod 7$
$\Delta_0(x) \equiv 6(x^2 + 2x + 6) \equiv 6x^2 + 5x + 1 \pmod 7$

$q_2(x) = (x-0)(x-3) = x^2 - 3x \equiv x^2 + 4x \pmod 7$
$q_2(2) = -2 \equiv 5 \pmod 7$, so $q_2(2)^{-1} \equiv 3 \pmod 7$
$\Delta_2(x) \equiv 3(x^2 + 4x) \equiv 3x^2 + 5x \pmod 7$

Don't have to calculate $\Delta_3(x)$ — multiplied by zero!

Take $p(x) = 3\Delta_0(x) + 2\Delta_2(x) + 0\Delta_3(x)$
$\equiv (4x^2 + x + 3) + (6x^2 + 3x) \equiv 3x^2 + 4x + 3 \pmod 7$

Counting Polynomials

Suppose I know $p(1) = 5$ and $p(2) = 3$.
How many deg ≤ 2 polynomials could p be?

Polynomial fully defined by 3rd point
Equiv: how many possible values for $p(0)$?

In $\mathbb{R}$, infinitely many...not too interesting
In $GF(q)$, q possibilities!

Shhh, It's a Secret

The password to my computer is 1234.

If something bad happens, want staff to unlock it
But dangerous to just give out my password

Idea: if k of n staff members agree, can unlock
If fewer than k, unable to

Shamir's Secret Sharing Scheme:

- Choose random deg $k-1$ poly st $p(0) = 1234$
  - Can choose points and interpolate
  - Or can choose coefficients
- Distribute $p(i)$ to ith staff member $(1 \leq i \leq n)$

Shhh-amir Properties

Claim: k staff members can recover password

Proof:

- Any k points on p fully define polynomial
- Use Lagrange to interpolate; evaluate $p(0)$

Claim: Only $k - 1$ staff members get nothing

Proof:

- Have $k - 1$ known points
- Any value of $p(0)$ gives potential polynomial
- All values consistent with known points!

Secret Sharing Example

Suppose my secret is 4.
Want to make sure any 3 of the 12 TAs can find it.

What prime should I work modulo?
Eventually give out $p(1)$, $p(2)$, ..., $p(12)$
To ensure distinct, need prime 13 or larger!
(Also need prime bigger than secret)

Choose polynomial $x^2 + 4 \pmod{13}$
Give out $p(1) = 5$, $p(2) = 8$, ..., $p(12) = 5$

Exercise: choose 3 pts, check Lagrange gives $x^2 + 4$

Hierarchical Secret Sharing

Can modify protocol for more complicated setups

Ex: Need Elizabeth $+ k$ TAs to unlock

Idea: have nested secret sharing

- Password is root of degree 1 poly $p(x)$
- $p(1)$ given to Elizabeth
- $p(2)$ is secret shared by TAs!
- Give TAs points on $q(x)$ st $q(0) = p(2)$

See more examples of this in discussion

Fin

Next time: error correcting codes!