Polynomials

Questions

- functions
  - single var
  - → coefficients → $P(x) = a_d x^d + a_{d-1} x^{d-1} \cdots a_0 x^0$
    - d → max degree
    - $2x^{(d+1)}$ ... d
    - ↓ unique
- [degree → largest power d]
- ($P(x)$ of deg d)
  - $x^2 + x + 1$ → $(1,1,1)$
  - ↳ $d = 2$

Proof in notes

- Reps
  - → coefficients → $d+1$ coefficients > [Uniquely] define P
  - → points → $d+1$ points
  - → roots → $= d$ roots at most
    - $(x-a)(x-b) \ldots$
    - ↳ [values st $P(x) = 0$ ↳ x]
    - ↓ zero roots, $d = 2$

$x^2 + x + 1$ → $(0,1)$, $(1,3)$, $(2,7)$

→ switch between $P(1)$, $P(2)$

- coefficients → points
  - evaluate $(P(1))$
- points → coefficients
  - [lagrange interpolation]
  - mechanically → notes

Galois Fields

↳ evaluate $(P(x) \bmod p)$ → $G(p)$ ↳ mod p — large prime

→ properties

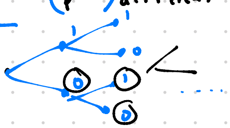
1. ↳ $a_i \in [\{0, \ldots p-1\}]$ $\forall i$
2. → polynomials can be degree at most $p-1$ → [uniquely]
   - $G(5)$ → at most $d = 4$

↳ Counting

- number of options for each coef p
- for a deg $d < p$ → ($d+1$ coeff)
- $\Rightarrow (p^{d+1})$ different polynomials $[G(p)]$
  - ↓ p^{d+1}

$p = 2$

$G(2)$



$[2^{d+1}]$

a_0 a_1 → a_d

Counting 2 4 2^{d+1}

↓ $d+1$ choices

Secret Sharing

[Some group $n > k$] (50 workers, $G(p)$ only 5 needed) ↳ gets s

↳ secret $s \in \{0 \cdots p-1\}$

1. share st if k people or greater group up ⇒ uncover s
2. if $< k$ no info → Proof
   - ↳ s is prime
   - s is odd etc
   - ↳ missile codes

↳ **Algorithm** → p large prime

1. under $G(p)$
   - ↳ make [deg $k-1$] polynomial
   - → st $(P(0) = s)$ → secret
     - ↳ can count # of options based on k and p
     - arbitrary
   - ↳ assign $[P(1) \cdots P(n)]$ to n people
   - ↳ to get $P(0)$ deg $[k-1]$
     - ↳ k people need to interpolate P → $P(0) = s$
     - (deg $k-1$ poly uniquely k pts)
   - Know [x get y] (x, y)

CS 70 Summer 2021 — Discrete Mathematics and Probability Theory — DIS 3B

1 Polynomial Practice

(a) If f and g are non-zero real polynomials, how many roots do the following polynomials have at least? How many can they have at most? (Your answer may depend on the degrees of f and g.)

→ no roots → has root → 1

(i) $f+g$ $\quad [(x^2+1) + (x^3 + x^2 + x + 1)]$ → 1

(ii) $f \cdot g$ $\quad x^2 \quad 1 \to x^2+1$

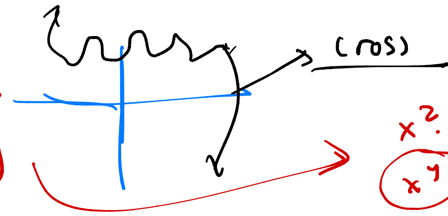
(iii) f/g, assuming that f/g is a polynomial

roots max d $\quad$ d odd

i) min 0 $\quad$ max → max(deg)

ii) min 0 $\quad$ max → deg f + deg g

iii) min 0 $\quad$ max → deg f − deg g



cross

$x^2 \cdot x^2$ $\quad x^4$

(b) Now let f and g be polynomials over GF(p), where p is prime.

(i) We say a polynomial $f = 0$ if $\forall x, f(x) = 0$. If $f \cdot g = 0$, is it true that either $f = 0$ or $g = 0$? $\quad$ → $f: x \to 0$ $\quad$ T or F

(ii) How many f of degree *exactly* $d < p$ are there such that $f(0) = a$ for some fixed $a \in \{0, 1, \ldots, p-1\}$? $\quad$ [Counting] $\quad$ what are possible options for $a_0\ a_1\ a_2 \cdots a_d$ (mod p)

$\binom{p}{d}$ → other term

① $a_0 = a$ → ① $\quad$ p options $\quad$ GF(p) → property of coefficients

[$f(0) = a_0 = a$] $\quad a_1$

② $a_d \neq 0$ $\quad$ exclude zero $\quad p \cdot p \quad a_2$

$a_0 \quad a_d \quad [a_1 - a_{d-1}] \quad p \to a_d$

$[1 \cdot (p-1) \cdot p^{d-1}]$ $\quad$ → $d-1$

zeroth rule $\quad$ think

option counts

$(|A| \quad |B|)$

Permutations

Combination

$1 \cdot (p-1) \quad |A| \cdot |B| \to$

$\quad p \quad p$

(c) Find a polynomial f over GF(5) that satisfies $f(0) = 1, f(2) = 2, f(4) = 0$. How many such polynomials are there?

2 Rational Root Theorem

The rational root theorem states that for a polynomial

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

$a_0, \cdots, a_n \in \mathbb{Z}$, if $a_0, a_n \neq 0$, then for each rational solution $\frac{p}{q}$ such that $\gcd(p,q) = 1$, $p|a_0$ and $q|a_n$. Prove the rational root theorem.

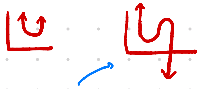
3 Secrets in the United Nations

A vault in the United Nations can be opened with a secret combination $s \in \mathbb{Z}$. In only two situations should this vault be opened: (i) all 193 member countries must agree, or (ii) at least 55 countries, plus the U.N. Secretary-General, must agree. hint → can give any number of pts to anyone

(a) Propose a scheme that gives private information to the Secretary-General and all 193 member countries so that the secret combination s can only be recovered under either one of the two specified conditions.

(b) The General Assembly of the UN decides to add an extra level of security: each of the 193 member countries has a delegation of 12 representatives, all of whom must agree in order for that country to help open the vault. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary-General and to each representative of each country.

Answers



1) a i → $f+g$

min : 0 (1) → if $f+g$ has odd deg

max : $\max(\deg f, \deg g)$

max roots for deg d polynomial $= d$

ii → $f \cdot g$

mult

↳ min : as above

max : $\deg f + \deg g$

iii → f/g

↳ min : as above

max : $\deg f - \deg g$

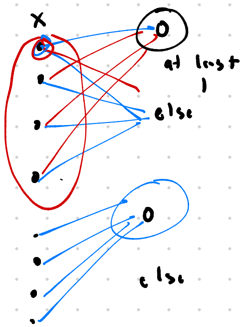
[f | t] f g

b i) False

↳ $[f \cdot g = 0] \rightarrow [(\forall x \in S)[f(x) = 0 \lor g(x) = 0]]$

[not as strong as]

$(\forall x \in S, f(x) = 0) \lor (\forall x \in S, g(x) = 0)$



b ii) Counting

↳ $f = \deg d \Rightarrow d+1$ coefficients

↳ $c_d \neq 0$ and $c_0 = a = f(0)$

↳ under $GP(p) \longrightarrow p$ possible values $\{0, \dots p-1\}$

↳ $c_0 \quad c_d \quad$ rest

$1 \cdot (p-1) \cdot p^{(d+1)-2}$ possible

c) reps

↳ polynomial → $d+1$ coefficients

GF(p) → under field coefficients and powers

↳ max deg $(p-1)$

max deg $= 4$

$\Rightarrow$ determined by 5 points $(d+1)$ → 3 done ↓

↳ lagrange interpolation

↳ 2 others options

5 each → choose x

$5 \cdot 5 = 25$ ↳ (possible y)

2 $\frac{p}{q}$ → root

$$\Rightarrow p\left(\frac{p}{q}\right) = 0 = a_n \cdot \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} \dots + a_1\left(\frac{p}{q}\right) + a_0$$

↳ $\cdot q^n$ $\quad a_n \cdot p^n + a_{n-1} \cdot q \cdot p^{n-1} + \cdots a_0 \cdot q^n = 0$

$p(a_n \cdot p^{n-1} + a_{n-1} \cdot q p^{n-2} \cdots) = -a_0 \cdot q^n$

show $p \mid a_0$

↳ $p \mid a_0 q^n$

$\gcd(p, q) = 1$

$\Rightarrow p \mid a_0$

3 a) $n, s < q$

↳ prime

↳ under $GF(q)$ — deg k, n

→ create $p(0) = s$ — give n people $P(1) \dots P(n)$

↳ deg

↳ 142 polynomial → [takes 143 pts]

→ [assign points to each country and assign 138 pts to sec gen]

↳ [$138 = 193 - 55$]

↳ cont

sec — get the p

$s = P(0)$

193 agree or 55 + one lady ↳ (193 − 55) → 193

3 b) encode each countries key → values part a

↳ (deg 11 poly) ($f(0) = $ key) → 12 needed

→ need 12 pts → can generate as many as I like

[→ each country for key to part a]