Polynomials

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$$

Properties

1. A nonzero polynomial of degree d has at most d roots.
2. Given $d+1$ points $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$ where all the x_i are distinct, there is a unique polynomial $p(x)$ of degree at most d such that $p(x_i) = y_i$ for all i.

Finite Fields $GF(p)$

All operations are done in $(\bmod\ p)$.

Interpolation

Given points $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$, find a polynomial of degree at most d that fits all of the given points.

Ex: $(0, 2), (1, 1), (2, 4)$ $\quad\quad \deg(p) \le 2$

Method 1: System of Linear Equations

$$p(x) = ax^2 + bx + c$$

$$\begin{aligned} p(0) &= \phantom{4a + 2b + {}} c = 2 \\ p(1) &= a + b + c = 1 \\ p(2) &= 4a + 2b + c = 4 \end{aligned}$$

Method 2: Lagrange Interpolation – shown in worksheet

CS 70	Discrete Mathematics and Probability Theory	
Spring 2022	Koushik Sen and Satish Rao	DIS 4B

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.)

(i) $f+g$

(ii) $f \cdot g$

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

(i) min: 0
max: max(deg f, deg g)

Exception: If $f+g=0$, then there are ∞ roots.

(ii) min: 0
max: deg(f) + deg(g)

(iii) min: 0
max: deg f − deg g

(b) Now let f and g be polynomials over GF(p).

(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 $g = 0$?

(ii) How many f of degree *exactly* $d < p$ are there such that $f(0) = a$ for some fixed $a \in \{0, 1, \ldots, p-1\}$?

(i) No. Consider $f(x) = x(x-1)(x-2)$ and $g(x) = (x-3)(x-4)$ in GF(5).

(ii) $$f(x) = \underset{\substack{\uparrow \\ p-1 \text{ choices}}}{a_d} x^d + \underset{\substack{\uparrow \\ p \text{ choices}}}{a_{d-1}} x^{d-1} + \ldots + \underset{\substack{\uparrow \\ p \text{ choices}}}{a_1} x + a$$

$$(p-1) \cdot p \cdot \ldots \cdot p = (p-1)p^{d-1}$$

(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?

Skipped. See official solutions.

2 Lagrange Interpolation in Finite Fields

Find a unique polynomial $p(x)$ of degree at most 3 that passes through points $(-1,3)$, $(0,1)$, $(1,2)$, and $(2,0)$ in modulo 5 arithmetic using the Lagrange interpolation.

(a) Find $p_{-1}(x)$ where $p_{-1}(0) \equiv p_{-1}(1) \equiv p_{-1}(2) \equiv 0 \pmod 5$ and $p_{-1}(-1) \equiv 1 \pmod 5$.

$$p_{-1}(x) \equiv 4x(x-1)(x-2) \equiv 4x^3+3x^2+3x$$

(b) Find $p_0(x)$ where $p_0(-1) \equiv p_0(1) \equiv p_0(2) \equiv 0 \pmod 5$ and $p_0(0) \equiv 1 \pmod 5$.

$$p_0(x) \equiv 3(x+1)(x-1)(x-2) \equiv 3x^3+4x^2+2x+1$$

(c) Find $p_1(x)$ where $p_1(-1) \equiv p_1(0) \equiv p_1(2) \equiv 0 \pmod 5$ and $p_1(1) \equiv 1 \pmod 5$.

$$p_1(x) \equiv 2x(x+1)(x-2) \equiv 2x^3-2x^2+x$$

(d) Find $p_2(x)$ where $p_2(-1) \equiv p_2(0) \equiv p_2(1) \equiv 0 \pmod 5$ and $p_2(2) \equiv 1 \pmod 5$.

$$p_2(x) \equiv x(x+1)(x-1) \equiv x^3-x$$

(e) Construct $p(x)$ using a linear combination of $p_{-1}(x)$, $p_0(x)$, $p_1(x)$ and $p_2(x)$.

$$\begin{aligned} p(x) &\equiv 3p_{-1}(x) + p_0(x) + 2p_1(x) \\ &\equiv 3(4x^3+3x^2+3x) + (3x^3+4x^2+2x+1) + 2(2x^3-2x^2+x) \\ &\equiv 4x^3+4x^2+3x+1 \pmod 5 \end{aligned}$$

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.

(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.

$P(x)$ = degree 192 polynomial where $P(0) = s$ give each country a point $P(i)$

$Q(x)$ = degree 1 polynomial where $Q(0) = s$ give $Q(1)$ to Secretary-General

$R(x)$ = degree 54 polynomial where $R(0) = Q(2)$ give each country a point $R(i)$

(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.

See official solutions.

4 To The Moon!

A secret number s is required to launch a rocket, and Alice distributed the values $(1, p(1)), (2, p(2)), \ldots, (n+1, p(n+1))$ of a degree n polynomial p to a group of \$GME holders $\text{Bob}_1, \ldots, \text{Bob}_{n+1}$. As usual, she chose p such that $p(0) = s$. Bob_1 through Bob_{n+1} now gather to jointly discover the secret. However, Bob_1 is secretly a partner at Melvin Capital and already knows s, and wants to sabotage $\text{Bob}_2, \ldots, \text{Bob}_{n+1}$, making them believe that the secret is in fact some fixed $s' \neq s$. How could he achieve this? In other words, what value should he report (in terms variables known in the problem, such as s', s or y_1) in order to make the others believe that the secret is s'?

See official solutions.