Polynomials

GF(p) → work in modulo p

- A degree d polynomial has $\leq d$ real roots
- $d+1$ distinct points uniquely define a polynomial of degree $\leq d$

Coefficients

$$p(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_d x^d$$

evaluation → $p(x_i) = y_i$

Lagrange interpolation ←

Values

(x_0, y_0)
(x_1, y_1)
$\vdots$
(x_d, y_d)

Lagrange Interpolation

(x_0, y_0)
(x_1, y_1)
$\vdots$
(x_d, y_d)

$$\Delta_0 = \frac{(x-x_1)(x-x_2)\cdots(x-x_d)}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_d)}$$

$$\Delta_1 = \frac{(x-x_0)(x-x_2)\cdots(x-x_d)}{(x_1-x_0)(x_1-x_2)\cdots(x_1-x_d)}$$

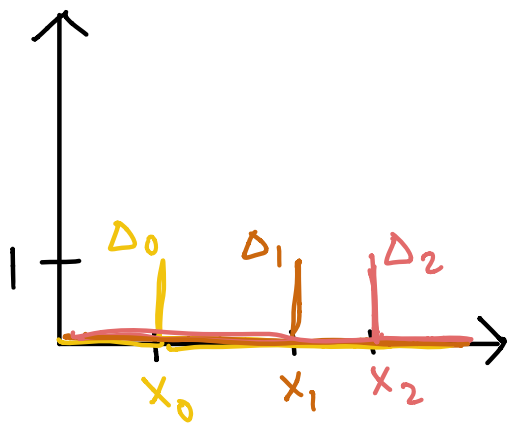
$\vdots$

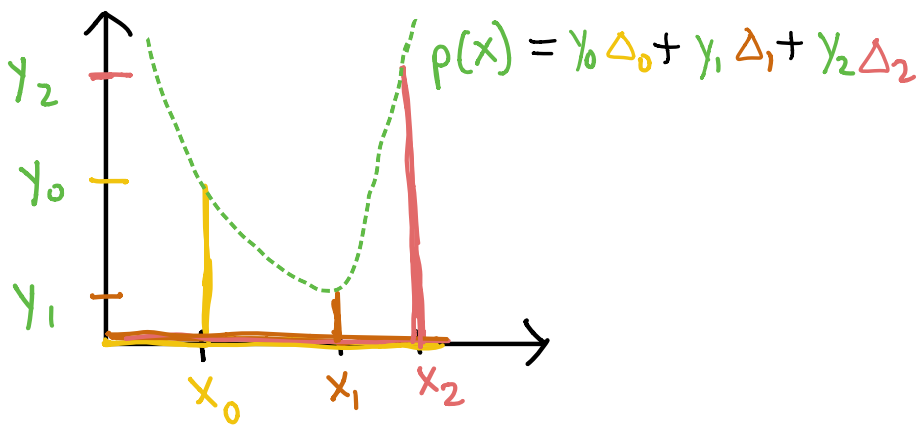
$$\Delta_d = \frac{(x-x_0)(x-x_1)\cdots(x-x_{d-1})}{(x_d-x_0)(x_d-x_1)\cdots(x_d-x_{d-1})}$$

$$\Delta_i(x_i) = 1$$

$$\Delta_i(x_j) = 0 \quad \text{for } i \neq j$$

$$p(x) = y_0\Delta_0 + y_1\Delta_1 + \cdots + y_d\Delta_d$$





CS 70 Discrete Mathematics and Probability Theory
Spring 2021 DIS 4B

Note: This worksheet is on the longer side and your TA may not get through all of the problems during discussion. Nevertheless, you should try to attempt the problems that your TA did not get to on your own.

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

(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 $a \in \{0, 1, \ldots, p-1\}$?

$f(x_0) = 0$ $\quad (x - x_0)\, \tilde{f}(x)\, g(x)$

$(f \cdot g)(x_0) = 0$

GF(3)

$f(0) = 0$ $\quad g(0) = 1$

$f(1) = 1$ $\quad g(1) = 0$

$f(2) = 1$ $\quad g(2) = 0$

$f+g(0) = 0$

$f+g(1) = 0$

$f \cdot g(2) = 0$

$f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_d x^d$ $\quad f(0) = c_0 = a$

$= a$ (1) $\quad \{0, 1, 2, \ldots, p-1\}$ (p) $\quad \neq 0$ $\quad \{1, 2, 3, \ldots, p-1\}$ (p-1)

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

(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?

$$\Delta_0 = (x-2)(x-4)\left((0-2)(0-4)\right)^{-1}$$
$$\Delta_1 = (x-0)(x-4)\left((2-0)(2-4)\right)^{-1}$$
$$\Delta_2 = (x-0)(x-2)\left((4-0)(4-2)\right)^{-1}$$

$\Delta_0(0)=1 \quad \Delta_1(0)=0 \quad \Delta_2(0)=0$
$\Delta_0(2)=0 \quad \Delta_1(2)=1 \quad \Delta_2(2)=0$
$\Delta_0(4)=0 \quad \Delta_1(4)=0 \quad \Delta_2(4)=1$

$$f(x) = 1\cdot\Delta_0 + 2\cdot\Delta_1 + 0\cdot\Delta_2$$
$$= 1\cdot(x-2)(x-4)\cdot 2 + 2\cdot(x-0)(x-4)\cdot 1$$
$$= 4x^2+1$$

(0,1) → 5 ways
(1,)
(2,2)
(3,) → 5 ways
(4,0)

5 × 5 = 25

2 Interpolation Practice

Find the lowest degree polynomial with coefficients in $\mathbb{R}$ that passes through the points $(0,0), (1,2)$, and $(2,-1)$. Now do it again in, with coefficients in GF(3).

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 order to make the others believe that the secret is s'?

$$p(x) = y_1 \Delta_1(x) + y_2 \Delta_2(x) + \cdots + y_{n+1} \Delta_{n+1}(x)$$

$$s = p(0) = y_1 \cdot \Delta_1(0) + y_2 \Delta_2(0) + \cdots + y_{n+1} \Delta_{n+1}(0)$$

$$s' = z_1 \cdot \Delta_1(0) + y_2 \Delta_2(0) + \cdots + y_{n+1} \Delta_{n+1}(0)$$

$$y_1 \Delta_1(0) - z_1 \Delta_1(0) = s - s'$$

$$z_1 = \boxed{-(s-s')\Delta_1^{-1}(0) + y_1}$$

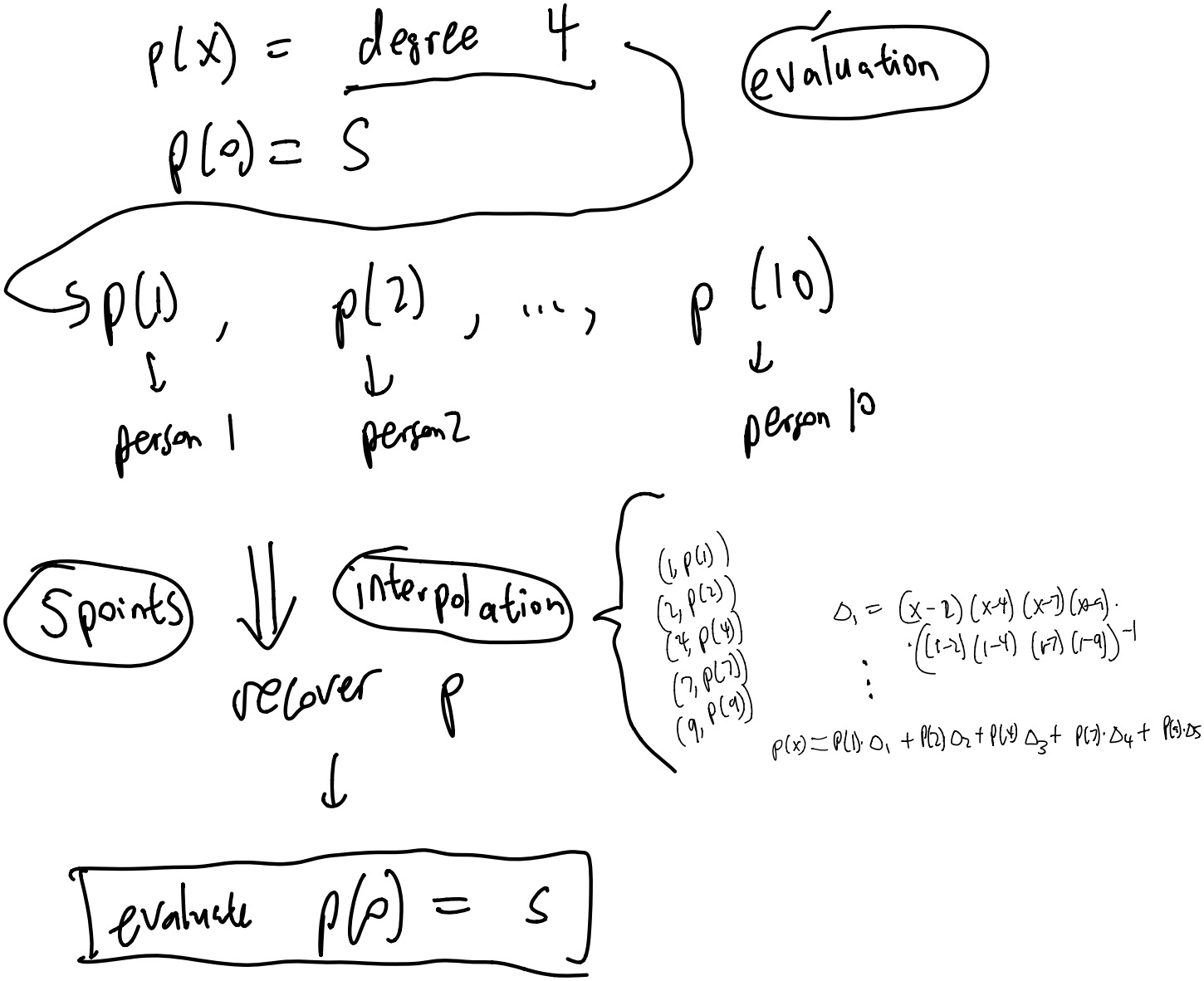
$$\Delta_1(x) = \begin{cases} 1 & \text{at } x = 1 \\ 0 & \text{at } x = 2, 3, 4, \ldots, n+1 \\ \neq 0 & \text{at } 0 \end{cases}$$

$$\| \quad (x-2)(x-3)\cdots(x-(n+1)) \left((1-2)(1-3)\cdots(1-(n+1)) \right)^{-1}$$

3 When the imposter is sus

10 crewmates in Among Us are deciding whether or not to eject an accused impostor (not one of the 10 crewmates) from their spaceship. The ejection mechanism has a password that is protected by a secret sharing scheme that will only allow the crewmates to eject the accused impostor if certain conditions are met. In the following parts, you will explore different secret sharing schemes to fulfill certain requirements.

(a) Design a secret sharing scheme that will allow the crewmates to eject the accused impostor if and only if at least 5 of the crewmates agree to.



(b) Now, 7 of the crewmates have finished their tasks and 3 of the crewmates have not finished their tasks and you are more inclined to trust the judgement of crewmates who have finished their tasks. Design a secret sharing scheme that will allow the crewmates to eject the accused impostor if and only if **either** at least 3 of the crewmates who finished their tasks agree **or** at least 5 out of all the crewmates agree. Assume that you know which crewmates have finished their tasks and which ones have not beforehand.

$F(x)$ = degree 2 polynomial

$F(0) = S$

distribute $F(1), F(2), \ldots, F(7)$

$E(x)$ = degree 4 polynomial

$E(0) = S$

distribute $E(1), E(2), \ldots, E(10)$

(c) The crewmates have decided to split up into groups as they wander around their spaceship to more effectively keep tabs on when the imposter is sus. In particular, 4 of them go to Electrical, 5 of them go to Communications, and 1 stays in Admin. Design a secret sharing scheme that will allow the crewmates to eject the accused impostor if and only if all of the crewmates in one group agree **and** at least one crewmate from another group agrees.

$E(x) = \deg 4$ poly $\rightarrow$ E(1) (C(6) A(2)
E(2) (C(6) A(2)
E(3) (C(6) A(2)
E(4) C(6) A(2)

$S = E(0)$ is the secret

$C(x) = \deg 5$ poly

$S = C(0)$ is the secret $\rightarrow$ C(1) E(5) A(2)
C(2) E(5) A(2)
C(3) E(5) A(2)
C(4) E(5) A(2)
C(5) E(5) A(2)

$A(x) = \deg 1$ poly

$S = A(0)$ is the secret $\rightarrow$ A(1) E(5) C(6)