01204211 Discrete Mathematics
Lecture 9b: Polynomials (1)[1]

Jittat Fakcharoenphol

October 2, 2023

[1] This section is from Berkeley CS70 lecture notes.

Quick exercise

For any integer $a \neq 1$, $a - 1 | a^2 - 1$.

Quick exercise

For any integer $a \neq 1$, $a - 1 | a^2 - 1$.

For any integer $a \neq 1$ and $n \geq 1$, $a - 1 | a^n - 1$.

Polynomials

A **single-variable polynomial** is a function $p(x)$ of the form

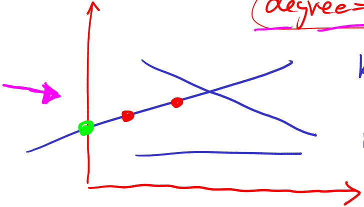
$$p(x) = \underline{a_d x^d} + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0.$$

We call a_i's *coefficients*. Usually, variable x and coefficients a_i's are real numbers. The **degree** of a polynomial is the largest exponent of the terms with non-zero coefficients.

Examples

- $x^{3} - 3x + 1$
- $x + 10$
- 10
- $\boxed{0}$ ← zero polynomial

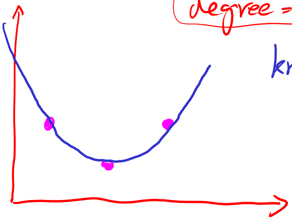
Folklore



degree = 1

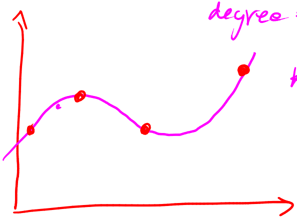
know 2 points ⇒ get f(x)

know < 2 points ⇒ know nothing



degree = 2

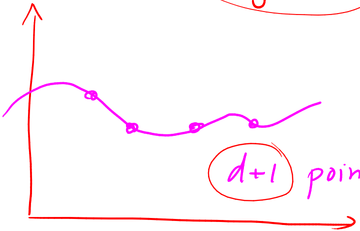
know 3 points → get f(x)



degree = 3

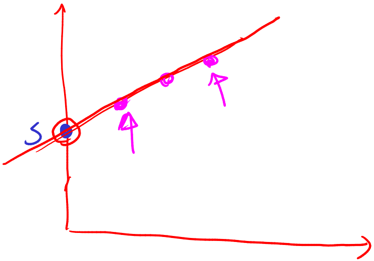
know 4 points.

degree = d



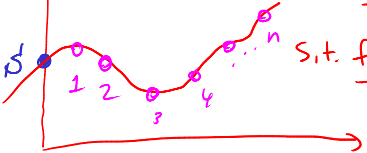
d+1 points

Applications



pick a polynomial of degree $\boxed{k-1}$

$f(x)$



s.t. $f(0)=s$

- Secret sharing

Secret: s

Share s among n people so that any group of k people can recover the secret but any set of < k people know nothing.

$$f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1 x^1 + s$$

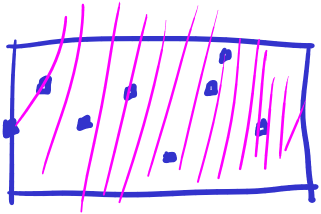
$$x \longrightarrow \boxed{\text{evaluation } f(x)} \longrightarrow f(x)$$

on n points

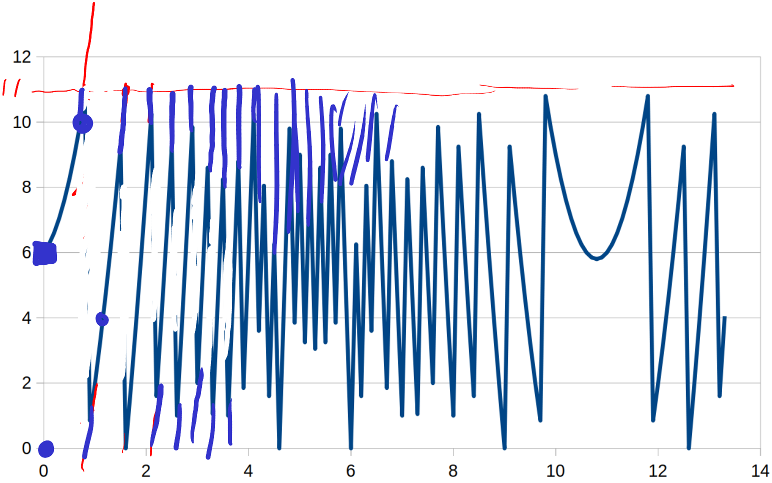
Share a secret to n people, where any group of k people can recover the secret.

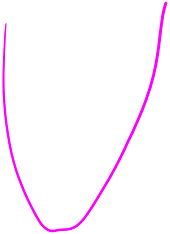
$$(x, f(x)), \ldots (- -)$$
$$\downarrow$$
$$\boxed{\text{interpolation}} \longrightarrow f(x)$$

Applications

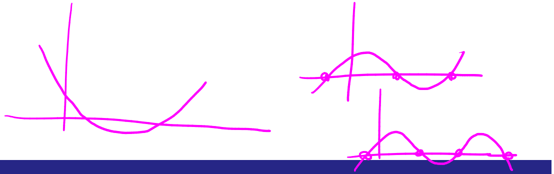


- Secret sharing
- Error-correcting codes





Basic facts



Definition

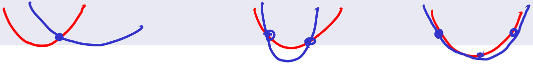
a is a **root** of polynomial $f(x)$ if $f(a) = 0$.

Properties

Property 1: A non-zero polynomial of degree d has at most d roots.
Property 2: Given $d+1$ pairs $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ with distinct x_i's, there is a *unique* polynomial $p(x)$ of degree at most d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

Lemma 1 *

If two polynomials $\underline{f(x)}$ *and* $\underline{g(x)}$ *of degree at most* d *that share* $\underline{d+1}$ *points* $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$*, where all* x_i*'s are distinct, i.e.,* $f(x_i) = g(x_i) = y_i$*, then* $\boxed{f(x) = g(x)}$*.*

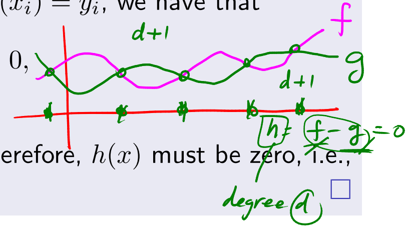


Proof.

Suppose that $\underline{f(x)} = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ and $\underline{g(x)} = b_d x^d + b_{d-1} x^{d-1} + \cdots + b_0$.
Let $\boxed{h(x)} = \underline{f(x) - g(x)}$, i.e., let $h(x) = c_d x^d + c_{d-1} x^{d-1} + \cdots + c_0$, where $c_i = a_i - b_i$. Note that $h(x)$ is also a polynomial of degree (at most) d.
We claim that $h(x)$ has $d+1$ roots. Note that since $f(x_i) = g(x_i) = y_i$, we have that

$$h(x_i) = f(x_i) - g(x_i) = y_i - y_i = 0,$$

i.e., every x_i is a root of $h(x)$.
From **Property 1**, if $h(x)$ is non-zero it has at most d roots; therefore, $h(x)$ must be zero, i.e., $f(x) - g(x) = 0$ or $f(x) = g(x)$ as required. □

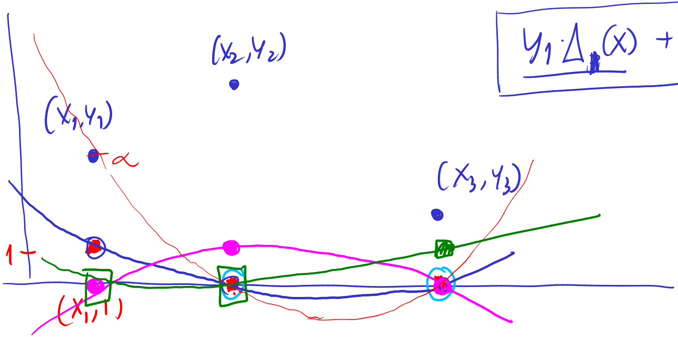


Polynomial interpolation - ideas

- polynomial degree $\boxed{2}$

$$\boxed{y_1 \cdot \Delta_1(x) + y_2 \cdot \Delta_2(x) + y_3 \cdot \Delta_3(x)}$$

(y_1, y_2, y_3)



$(0,1,0)$

$$\Delta_2(x) = \frac{(x-x_1)(x-x_3)}{(x_2-x_1)(x_2-x_3)}$$

$$\Delta_1(x) = \frac{(x-x_2)(x-x_3)}{(x_1-x_2)(x_1-x_3)}$$

$(1,0,0)$

$$\Delta_3(x) = \frac{(x-x_1)(x-x_2)}{(x_3-x_1)(x_3-x_2)}$$

$(0,0,1)$

Lagrange polynomial

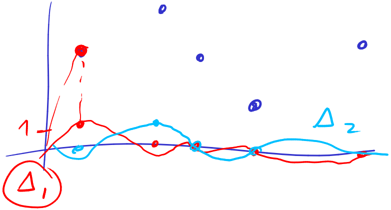
For $\underline{d+1}$ points $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$ where all x_i's are distinct, let

$$\Delta_i(x) = \frac{(x - x_1)(x - x_2)\cdots(x - x_{i-1})(x - x_{i+1})\cdots(x - x_{d+1})}{(x_i - x_1)(x_i - x_2)\cdots(x_i - x_{i-1})(x_i - x_{i+1})\cdots(x_i - x_{d+1})}.$$

Note that $\boxed{\Delta_i(x)}$ is a polynomial of degree d

↳ is 1 at x_i ✓

↳ is 0 at other x_j $j \neq i$ ✓



Lagrange polynomial

For $d+1$ points $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$ where all x_i's are distinct, let

$$\Delta_i(x) = \frac{(x - x_1)(x - x_2)\cdots(x - x_{i-1})(x - x_{i+1})\cdots(x - x_{d+1})}{(x_i - x_1)(x_i - x_2)\cdots(x_i - x_{i-1})(x_i - x_{i+1})\cdots(x_i - x_{d+1})}.$$

Note that $\Delta_i(x)$ is a polynomial of degree d. Also we have that

- For $j \neq i$, $\Delta_i(x_j) =$

Lagrange polynomial

For $d+1$ points $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$ where all x_i's are distinct, let

$$\Delta_i(x) = \frac{(x - x_1)(x - x_2)\cdots(x - x_{i-1})(x - x_{i+1})\cdots(x - x_{d+1})}{(x_i - x_1)(x_i - x_2)\cdots(x_i - x_{i-1})(x_i - x_{i+1})\cdots(x_i - x_{d+1})}.$$

Note that $\Delta_i(x)$ is a polynomial of degree d. Also we have that

- For $j \neq i$, $\Delta_i(x_j) = 0$, and
- $\Delta_i(x_i) =$

Lagrange polynomial

For $d + 1$ points $(x_1, y_1), (x_2, y_2), \dots, (x_{d+1}, y_{d+1})$ where all x_i's are distinct, let

$$\Delta_i(x) = \frac{(x - x_1)(x - x_2)\cdots(x - x_{i-1})(x - x_{i+1})\cdots(x - x_{d+1})}{(x_i - x_1)(x_i - x_2)\cdots(x_i - x_{i-1})(x_i - x_{i+1})\cdots(x_i - x_{d+1})}.$$

Note that $\Delta_i(x)$ is a polynomial of degree d. Also we have that

- For $j \neq i$, $\Delta_i(x_j) = 0$, and
- $\Delta_i(x_i) = 1$.

Lagrange polynomial

For $d+1$ points $(x_1, y_1), (x_2, y_2), \ldots, (x_{d+1}, y_{d+1})$ where all x_i's are distinct, let

$$\Delta_i(x) = \frac{(x-x_1)(x-x_2)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_{d+1})}{(x_i-x_1)(x_i-x_2)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_{d+1})}.$$

Note that $\Delta_i(x)$ is a polynomial of degree d. Also we have that

- For $j \neq i$, $\Delta_i(x_j) = 0$, and
- $\Delta_i(x_i) = 1$.

We can use $\Delta_i(x)$ to construct a degree-d polynomial

$$\boxed{p(x) = y_1 \cdot \Delta_1(x) + y_2 \cdot \Delta_2(x) + \cdots y_{d+1} \cdot \Delta_{d+1}(x).}$$

What can you say about $p(x_i)$?

Property 2 *

Given $\boxed{d+1}$ pairs $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ with distinct x_i's, there is a *unique* polynomial $p(x)$ of degree at most d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

Proof of Property 2.

Using Lagrange interpolation, we know that there exists a polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for all $1 \leq i \leq d+1$.

For uniqueness, assume that there exists another polynomial $g(x)$ of degree d also satifying the condition. Since $p(x)$ and $g(x)$ agrees on more than d points, $p(x)$ and $g(x)$ must be equal from Lemma 1. □