Lec9B Polynomial Interpolation

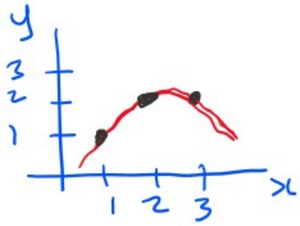
Section 5.7

January 30, 2021 10:44 PM

Let F be a field. Given $n \geq 1$ distinct points $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ (existence) and values $y_1, y_2, \ldots, y_n \in F$ find $f(x) \in F[x]$ s.t. $f(\alpha_i) = y_i$.

Theorem. There exists a unique polynomial $f(x)$ with $\deg(f) \leq n-1$ satisfying $f(\alpha_i) = y_i$.

$\Downarrow$ uniqueness.



$n = 3$

$\alpha_1 = 1, y_1 = 1$

$\alpha_2 = 2, y_2 = 2$

$\alpha_3 = 3, y_3 = 2$

$F = \mathbb{R}$.

$\Rightarrow$ $f(x) = ax^2 + bx + c$

$$\boxed{\begin{aligned} 1 &= a + b + c \\ 2 &= 4a + 2b + c \\ 2 &= 9a + 3b + c \end{aligned}}$$

Solving a linear system of n equations in n unknowns using Gaussian Elimination does $O(n^3)$ arithmetic operations in F.

Two methods that do $O(n^2)$ arith. ops. in F.

Lagrange interpolation: Let $L(x) = (x-\alpha_1)(x-\alpha_2) \cdot \ldots \cdot (x-\alpha_n)$.
and $L_i(x) = L(x)/(x-\alpha_i)$.

Write $f(x) = a_1 \cdot L_1(x) + \cdots + a_i L_i(x) + \cdots + a_n \cdot L_n(x)$.

have degree $n-1$.

$L_1(x) = (x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_n)$

Require $f(\alpha_i) = y_i$.

$f(\alpha_i) = y_i = a_1 \cdot 0 + \cdots + a_i \underbrace{L_i(\alpha_i)}_{\neq 0} + \cdots + a_n \cdot 0$

$\Rightarrow a_i = y_i / L_i(\alpha_i)$

Newton interpolation.

Write $f(x) = b_0 + b_1(x-\alpha_1) + b_2(x-\alpha_1)(x-\alpha_2) + \cdots + b_{n-1}(x-\alpha_1)\cdots(x-\alpha_{n-1})$

deg $=1$ deg $=2$ deg $= n-1$.

Observe $\deg f \leq n-1$.

Require $f(\alpha_i) = y_i$

$f(\alpha_1) = y_1 = b_0 + 0 \Rightarrow b_0 = y_1$

$f(\alpha_2) = y_2 = b_0 + b_1(\alpha_2 - \alpha_1) + 0 \Rightarrow b_1 = (y_2 - b_0)/(\alpha_2 - \alpha_1)$.

$f(\alpha_3) = y_3 = b_0 + b_1(\alpha_3 - \alpha_1) + b_2(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) + 0$

$\Rightarrow b_2 = [y_3 - b_0 - b_1(\alpha_3 - \alpha_1)] / (\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)$.

$f(\alpha_3)$ $y_3 = b_0 + b_1(\alpha_3 - \alpha_1) + b_2(\alpha_3-\alpha_1)(\alpha_3-\alpha_2)$

$\Rightarrow \quad b_2 = \left[y_3 - b_0 - b_1(\alpha_3 - \alpha_1)\right] / (\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2).$

Example. $f(1)=1,\ f(2)=2,\ f(3)=2$ in $\mathbb{Q}[x]$.

$\Rightarrow n=3 \Rightarrow \deg(f) \le 2.$

$$f(x) = b_0 + b_1(x-\alpha_1) + b_2(x-\alpha_1)(x-\alpha_2)$$
$$f(x) = b_0 + b_1(x-1) + b_2(x-1)(x-2).$$

$f(1) = 1 = b_0 + b_1 \cdot 0 + b_2 \cdot 0 \Rightarrow b_0 = 1.$

$f(2) = 2 = 1 + b_1(2-1) + 0 \Rightarrow b_1 = 1$

$f(3) = 2 = 1 + 1(3-1) + b_2(3-1)(3-2)$

$2 = 3 + 2b_2 \Rightarrow -1 = 2b_2 \Rightarrow b_2 = -\frac{1}{2}$

$f(x) = 1 + 1(x-1) - \frac{1}{2}(x-1)(x-2).$ ← in Newton form.

$f(x) = -\frac{1}{2}x^2 + \frac{5}{2}x - 1.$

Maple. $F=\mathbb{Q}$ interp([$\alpha_1, \alpha_2, \ldots, \alpha_n$], [$y_1, y_2, \ldots, y_n$], x);

$F=\mathbb{Z}_p$ Interp(" , " , x) mod p;

Example. $f(x,y) = (x^2+1) + (x)\cdot y \in \mathbb{Z}_5[x][y]$

$f(0,y) = 1 + 0 \cdot y$ (0,0)

$f(1,y) = 2 + 1 \cdot y$ (1,1)

$f(2,y) = 0 + 2 \cdot y$ (2,2)

Interpolate x: $(x^2+1) + (x)\cdot y.$

Interp([0,1,2], [1, 2+y, 2y], x) mod 5;

Let $a,b \in \mathbb{Z}_p[x]$. How can we multiply $c = a \times b$?

Idea: $c(x) = a(x) \cdot b(x) \Rightarrow \deg(c) = \deg(a) + \deg(b).$

Interpolate $c(x)$.
$$\left\{\begin{array}{l} c(\alpha_1) = a(\alpha_1) \cdot b(\alpha_1). \\ c(\alpha_2) = a(\alpha_2) \cdot b(\alpha_2) \\ c(\alpha_3) = a(\alpha_3) \cdot b(\alpha_3). \end{array}\right.$$
mults in $\mathbb{Z}_p$.

Evaluation.

Homomorphism Diagram

$$
\begin{tikzcd}[column sep=huge, row sep=huge]
\text{Input } a,b \in \mathbb{Z}_p[x] \arrow[r, "\text{Classical } \times", "O(n^2)."'] \arrow[d, "\phi_{x=\alpha_i}"', "{\substack{i=0,\dots,\deg(a)+\deg(b).\\ \text{where } \alpha_i \in \mathbb{Z}_p.}}"] & \text{Output } c = a \times b. \\
{\substack{a_i = a(\alpha_i)\\ b_i = b(\alpha_i)}} \arrow[r, "c_i = a_i \cdot b_i = c(\alpha_i)"] & c_i \arrow[u, "{\substack{\text{Interpolate } x\\ (\alpha_i, c_i)\\ O(n^2)\\ \text{arith. ops in}\\ \mathbb{Z}_p.}}"']
\end{tikzcd}
$$

$$\deg(c) = \deg(a) + \deg(b) = \underline{2n-2}$$

Evaluation using Horner form.

$$a(x) = a_0 + a_1 x^1 + a_2 \cdot x^2 + \cdots + a_{n-2} x^{n-2} + a_{n-1} \cdot x^{n-1}$$
$$= a_0 + x \cdot (a_1 + x(a_2 + \cdots + x(a_{n-2} + x \cdot a_{n-1}) \cdots)).$$

There are $n-1$ mults and $n-1$ adds therefore evaluating a polynomial of degree $n-1$ does $O(n)$ arith. ops. in $\mathbb{Z}_p$

Total cost of this algorithm is

$$\underbrace{(2n-1)}_{\#\text{ points}} \cdot \underbrace{2}_{a\&b} \cdot \underbrace{O(n)}_{\text{Horner}} + \underbrace{(2n-1)}_{\#\text{points}} \cdot \underbrace{1}_{\times \text{ in } \mathbb{Z}_p} + \underbrace{O((2n-1)^2)}_{\text{Interpolation.}}$$

$$= O(n^2) + O(n) + O(n^2).$$
$$= O(n^2).$$