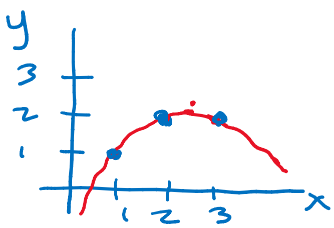
Polynomial Interpolation in F[x]

September 19, 2023 9:04 AM

Let F be a field. Given $n \geq 1$ distinct points $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ 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 $f(x) \in F[x]$ with $\deg(f) \leq n-1$ satisfying $\boxed{f(\alpha_i) = y_i.}$



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

$n = 3$

$\alpha_1 = 1 \quad y_1 = 1 \Rightarrow$
$\alpha_2 = 2 \quad y_2 = 2 \Rightarrow$
$\alpha_3 = 3 \quad y_3 = 2 \Rightarrow$

$$\boxed{\begin{aligned} y_1 &= a \cdot 1 + b \cdot 1 + c \\ y_2 &= 4a + 2b + c \\ y_3 &= 9a + 3b + c. \end{aligned}}$$

Solving a linear system, $n \times n$, using Gaussian elimination does $O(n^3)$ arithmetic ops. in F.

Two $O(n^2)$ methods

Lagrange interpolation

Let $L(x) = (x - \alpha_1)(x - \alpha_1) \cdots (x - \alpha_n)$.

Let $L_i(x) = L(x)/(x - \alpha_i)$ for $1 \leq i \leq n$.

Write $f(x) = a_1 \cdot L_1(x) + a_2 \cdot L_2(x) + \cdots + a_n \cdot L_n(x)$.

have degree $n-1$.

Require $f(\alpha_i) = y_i$.

$$y_i = f(\alpha_i) = a_1 \cdot 0 + \cdots + a_i \cdot \overset{\neq 0}{L_i(\alpha_i)} + 0 \cdot L_{i+1}(\alpha_i) + \cdots + a_n \cdot 0$$

$\Rightarrow a_i = y_i / L_i(\alpha_i)$. (this proves existence.)

Newton interpolation.

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

Require $f(\alpha_i) = y_i$.

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

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

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

Example. $f(1)=1,\ f(2)=2,\ f(3)=2.$ $n=3$, $\deg(f)\le 2$.

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

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

$$1 = f(1) = b_0 + 0 + 0 \Rightarrow b_0 = 1$$

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

$$2 = f(3) = 1 + 1\cdot 2 + b_2(2)(1)$$

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

$$f(x) = 1 + 1(x-1) - \tfrac{1}{2}(x-1)(x-2). \leftarrow \text{Newton form}$$

$$f(x) = -\tfrac{1}{2}x^2 + \tfrac{5}{2}x - 1 \leftarrow \text{Standard form.}$$

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

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

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

$$f(0,y) = 1 + 0\cdot y$$
$$f(1,y) = 2 + 1\cdot y$$
$$f(2,y) = 0 + 2\cdot y$$

$$f(x,y) \qquad x^2+1 \qquad x\cdot y$$

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

Proof of uniqueness:

Let $f(x)$ and $g(x)$ that satisfy the conditions of the theorem. Then

$$f(\alpha_i) = y_i = g(\alpha_i)$$

$$\Rightarrow \underbrace{f(\alpha_i) - g(\alpha_i)} = 0$$

$$\Rightarrow x - \alpha_i \mid f(x) - g(x). \text{ for } 1 \le i \le n.$$

$$\Rightarrow (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \mid f(x) - g(x) = 0.$$

$\uparrow$ degree n $\qquad$ degree $n-1$.

$(x-1)(x-2) \mid h(x)$

$(x-1)(x-3) \mid h(x)$

$(x-1)(x-2)(x-3) \mid h(x)$

So what? Interpolation is a key tool for speeding up algorithms.

Let $a, b \in \mathbb{Z}_p[x]$ p large.

How can we multiply $c = a \times b$?

Idea:

$$c(x) = a(x) \cdot b(x) \qquad \deg(c) = \deg(a) + \deg(b).$$

$$\Rightarrow \quad \text{Interpolate} \left\{ \begin{array}{l} c(\alpha_1) = a(\alpha_1) \cdot b(\alpha_1) \\ c(\alpha_2) = a(\alpha_2) \cdot b(\alpha_2) \\ \vdots \\ c(\alpha_n) = a(\alpha_n) \cdot b(\alpha_n). \end{array} \right.$$

Need $n = \deg(c) + 1$ points

Horner.