Univariate Interpolation

November 23, 2023 9:18 AM

Newton interpolation.

Let $f \in F[x]$, F a field and $d = \deg(f)$.
Let $\alpha_0, \alpha_1, \ldots, \alpha_d, \ldots$ be distinct points in F.
The Newton basis for f is

$$\{ \overset{0}{1}, \overset{1}{x-\alpha_0}, \overset{2}{(x-\alpha_0)(x-\alpha_1)}, \ldots, \overset{d}{(x-\alpha_0)\cdots(x-\alpha_{d-1})} \}.$$

There exist unique $v_0, v_1, \ldots, v_d, v_{d+1}, \ldots$ s.t.

$$f(x) = \underbrace{\boxed{v_0 + v_1(x-\alpha_0) + \cdots + v_{k-1}(x-\alpha_0)\cdots(x-\alpha_{k-2})}}_{g_{k-1}} + v_k \underbrace{\boxed{(x-\alpha_0)\cdots(x-\alpha_{k-1})}}_{m(\alpha_k)}$$
$$+ \cdots + v_d \underbrace{(x-\alpha_0)\cdots(x-\alpha_{d-1})}_{\deg d} + v_{d+1} \underbrace{(x-\alpha_0)\cdots(x-\alpha_d)}_{\deg d+1}.$$

$\deg(f) = d \Rightarrow v_{d+1} = 0$, $v_d \neq 0$, but $v_0, \ldots, v_{d-1}$ could be 0.

E.g. $f(x) = 2(x-1)(x-2)$, $\alpha_0 = 1, \alpha_1 = 2, \alpha_2 = 3$

$$f(x) = \underset{0}{\underset{\shortparallel}{v_0}} + \underset{0}{\underset{\shortparallel}{v_1}}(x-1) + \underset{2}{\underset{\shortparallel}{v_2}}(x-1)(x-2).$$

Suppose we have a black-box $B: F \to F$ for $f \in F[x]$, F a field. How can we compute $d = \deg(f)$?

Algorithm GetDegree
Input $B: F \to F$ a black box for $f \in F[x]$.
Output $\deg(f)$ with high probability.

Let S be a large finite subset of F.
E.g. if $F = \mathbb{Z}_p$, $S = \mathbb{Z}_p$.

$g_{-1} \leftarrow 0$; $k \leftarrow 0$; $m \leftarrow 1$;
while true do
  pick $\alpha_k \in S$ <u>at random</u> s.t. $m(\alpha_k) \neq 0$. // new α.
  $u_k \leftarrow B(\alpha_k)$ # $y_k = f(\alpha_k)$.

pick $\alpha_k \in S$ <u>at random</u> s.t. $M(\alpha_k) \neq 0$.

$y_k \leftarrow B(\alpha_k)$ # $y_k = f(\alpha_k)$.

$v_k \leftarrow (y_k - g_{k-1}(\alpha_k))/M(\alpha_k)$.

if $v_k = 0$ return $k-1$. # $k-1 = \deg(g_{k-1})$.

$g_k = g_{k-1} + v_k \cdot M$

$M = M \cdot (x - \alpha_k)$.

k++;

od;

This works correctly iff $v_0 \neq 0 \wedge v_1 \neq 0 \wedge \dots \wedge v_{d-1} \neq 0$.

$$v_k = 0 \iff y_k = g_{k-1}(\alpha_k) \iff h(\alpha_k) = 0.$$

α_k is a root of h.

Let $h(x) = f(x) - g_{k-1}(x) \leftarrow \deg g_{k-1} = k-1$.

$\deg h = d$ $y_k = f(\alpha_k)$ $\deg f = d$

Since a polynomial of degree d in $F[x]$ can have at most d roots and $\deg(h) = d$ and there are $|S| - k$ choices for α_k ($\alpha_k \notin \{\alpha_0, \alpha_1, \dots, \alpha_{k-1}\}$)

$$\Pr[v_k = 0] = \Pr[h(\alpha_k) = 0] \leq \frac{d}{|S| - k}.$$

$$\Rightarrow \Pr[v_0 = 0 \text{ or } v_1 = 0 \text{ or} \dots \text{or } v_{d-1} = 0]$$
$$\leq \underbrace{\frac{d}{|S|} + \frac{d}{|S|-1} + \dots + \frac{d}{|S|-d}}_{d \text{ terms.}} \leq \frac{d^2}{|S| - d}$$

How does this work in practice?

If $F = \mathbb{Z}_p$ and p is a 63 bit prime $\Rightarrow 2^{62} < p < 2^{63}$.

If $d = 2^{10}$ then

$$\Pr[v_0 = 0 \text{ or} \dots \text{or } v_{d-1} = 0] \leq \frac{d^2}{|S| - d} = \frac{2^{20}}{\underline{2^{63} - 2^{10}}} \sim \frac{1}{2^{43}}.$$

How could we reduce the probability of error?

How could we reduce the probability of error?

Require $v_{k-1}=0$ and $v_k=0$ before returning $k-2$.

$$\Pr[\underbrace{v_0=v_1=0 \text{ or } v_1=v_2=0 \text{ or} \cdots \text{or}}_{d-1} v_{d-2}=v_{d-1}=0] < \left(\frac{d}{|S|-d}\right)\cdot\left(\frac{d}{|S|-d}\right)\cdot(d-1).$$

$$\le \left(\frac{2^{10}}{2^{63}-2^{10}}\right)^2\cdot(2^{10}-1) \approx \frac{2^{30}}{2^{126}} = \frac{1}{2^{96}}.$$

What if $F = \mathbb{F}_2$?

Pick $\alpha_k \in \mathbb{F}_2^{100} \cong \mathbb{F}_2[z]/m(z)$.