Fast Multipoint Evaluation in F[x]

October 17, 2023 9:17 AM

Modern Computer Algebra Ch 10.

Let $f \in F[x]$, $\alpha_1, \alpha_2, \ldots, \alpha_n$ where $n = 2^k$ and $\deg(f) < n$.

How fast can we compute $f(\alpha_i)$ for $1 \le i \le n$?

Horner's method does $\le n \cdot (n-1) \in O(n^2)$ mults and adds.

Consider

The product tree Π_n for $n = 8$

Degree

$1 = n/8$ $\quad x-\alpha_1 \quad x-\alpha_2 \quad x-\alpha_3 \quad x-\alpha_4 \quad x-\alpha_5 \quad x-\alpha_6 \quad x-\alpha_7 \quad x-\alpha_8.$

$2 = n/4$ $\quad (x-\alpha_1)(x-\alpha_2) \quad (x-\alpha_3)(x-\alpha_4) \quad (x-\alpha_5)(x-\alpha_6) \quad (x-\alpha_7)(x-\alpha_8)$

$\quad M_4 \quad M_5 \quad M_6 \quad M_7$

$4 = n/2$ $\quad M_2 = M_4 M_5 \qquad M_3 = M_6 \cdot M_7$

$8 = n$ $\quad M_1 = M_2 \cdot M_3$

Compute $r_2 = f \bmod M_2$ (remainder) $\qquad r_3 = f \bmod M_3$

$r_4 = r_2 \bmod M_4 \qquad r_5 = r_2 \bmod M_5$

$r_8 = r_4 \bmod x-\alpha_1 = f(\alpha_1)$? $\qquad r_{10} = r_5 \bmod x-\alpha_3 = f(\alpha_3)$?

$r_9 = r_4 \bmod x-\alpha_2 = f(\alpha_2)$? $\qquad r_{11} = r_5 \bmod x-\alpha_4 = f(\alpha_4)$.?

Claim.

Let $T(n)$ be the # arith ops of all the divisions.

Suppose $D(n) \le 4M(n)$.

$$
\begin{aligned}
T(n) &= 2D(\tfrac{n}{2}) + 4D(\tfrac{n}{4}) + \cdots + nD(1) \\
&\le 4\left(2M(\tfrac{n}{2}) + 4M(\tfrac{n}{4}) + \cdots + nM(1)\right) \\
&< 4\left(M(n) + 2M(\tfrac{n}{2}) + \cdots + \tfrac{n}{2}M(2)\right) \\
&< 4\left(M(n) + M(n) + \cdots + M(n).\right) \\
&= 4M(n)\log_2 n \in O(M(n)\log n).
\end{aligned}
$$

Assume $2M(\frac{n}{2}) < M(n)$.

What if $\deg(f) \ge n$?

one more division, one more mult.

Compute $r_1 = f \bmod M_1 = M_2 M_3 = \prod_{i=1}^{n}(x-\alpha_i)$

Lemma. Let $f, g, h \in F[x]$ where $g \mid h$. $=$ $(x-\alpha_1)(x-\alpha_2)$

Then $f \bmod g = (f \bmod h) \bmod g$.

$(x-\alpha_1)$

Proof. $f \div h$: $f = qh + r$ where $r=0$ or $\deg r < \deg h$.

$\Rightarrow f \bmod h = r$.

Also if $g \mid h$ then $h = g \cdot a$ for some $a \in F[x]$.

Now $f \bmod g = (qh + r) \bmod g$

$= (q \cdot g \cdot a + r) \bmod g$.

$= r \bmod g$.

$= (f \bmod h) \bmod g$.

Suppose we use the FFT for every multiplication in $F[x]$ in the product tree Π_n. If $\deg(fg) < n = 2^k$ we can multiply $f \cdot g$ using 3 FFTs of size n. But in Π_n $\deg(f \cdot g) = n = 2^k$. We need 3 FFTs of size $2n$.

Exercise: Show how to do this using 3 FFTs of size n.

Let $T(n)$ be the # arith. ops in F needed to compute Π_n.
Let $M(n)$ be " " " " " " to multiply two polys of degree n.

$$T(n) < \frac{n}{2}M(1) + \frac{n}{4}M(2) + \cdots + 4M\left(\frac{n}{8}\right) + 2M\left(\frac{n}{4}\right)$$
$$< \frac{n}{4}M(2) + \frac{n}{2}M(4) + \cdots + 2M\left(\frac{n}{4}\right) + M\left(\frac{n}{2}\right)$$
$$< M\left(\frac{n}{2}\right) + M\left(\frac{n}{2}\right) + \cdots + M\left(\frac{n}{2}\right) + M(n/2)$$
$$= M\left(\frac{n}{2}\right)(\log_2 n - 1) \in O(M(n) \log n).$$

Assume $2M\left(\frac{n}{2}\right) < M(n)$.

So the total cost to compute $f(\alpha_i)$ for $1 \le i \le n = 2^k$ is $2\,O(M(n)\log n) = O(M(n)\log n)$.

$O(M(n))$ — Division, $\sqrt{f(x)}$.

$O(M(n)\log n)$ — Multipoint Evaluation, Interpolation, $\mathrm{Gcd}(a,b)$