Lec10B The Inverse Fourier Transform Section 4.6

February 10, 2021 11:49 PM

Let $a(x) = \sum_{i=0}^{n-1} a_i x^i \in F[x]$, $n = 2^k$ and ω is a pnru.

Let $A = [a_0, a_1, \ldots, a_{n-1}]^T \in F^n$ and
$B = [a(1), a(\omega), \ldots, a(\omega^{n-1})]^T \in F^n$ (Fourier transform of $a(x)$).

Consider

$$\begin{array}{cc} & n \\ n & \underbrace{\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ \vdots & & & & \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)^2} \end{bmatrix}}_{V_\omega} \end{array} \underbrace{\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix}}_{A} = \underbrace{\begin{bmatrix} a(1) \\ a(\omega) \\ \\ \\ a(\omega^{n-1}) \end{bmatrix}}_{B}$$

One way to compute B is $V_\omega \cdot A \Rightarrow n^2$ mults in F.
One way to interpolate $a(x)$ given B is to solve $V_\omega A = B$ for A.
Another way is to compute V_ω^{-1} then $A = V_\omega^{-1} \cdot B$. This costs $O(n^3)$.

Lemma 2. Let ω be a pnru. Then $\omega^{-1} = \omega^{n-1}$ and ω^{-1} is also a pnru.

Proof. $\omega^n = 1 \Rightarrow \omega \cdot \omega^{n-1} = 1 \Rightarrow \omega^{-1} = \omega^{n-1}$

TAC Suppose $(\omega^{-1})^k = 1$ for some $0 < k < n$.
Then $\omega^n \cdot \omega^{-k} = 1 \Rightarrow \omega^{n-k} = 1$ $\boxtimes$

Lemma 3. $V_\omega \cdot V_{\omega^{-1}} = nI \Rightarrow V_\omega^{-1} = \frac{1}{n} \cdot V_{\omega^{-1}}$

Proof.

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 \cdots & \omega^{n-1} \\ \vdots & & & \\ 1 & \omega^{n-1} & \cdots & \omega^{(n-1)^2} \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \omega^{-2} \cdots & \omega^{-(n-1)} \\ 1 & \omega^{-2} & & \\ \vdots & & & \\ 1 & \omega^{-(n-1)} & \cdots & \omega^{-(n-1)^2} \end{bmatrix} = \begin{bmatrix} \boxed{n} & \boxed{0} & \\ \boxed{0} & \boxed{n.} & \\ & & \end{bmatrix}$$

$(1+\omega^{-1}+\omega^{-2}+\cdots+\omega^{-(n-1)})$

$1+\omega+\omega^2+\cdots\omega^{n-1} = 0$

$1 + \omega\omega^{-1} + \omega^2 \cdot \omega^{-2} + \cdots + \omega^{n-1} \cdot \omega^{-(n-1)}$
$= 1 + \omega^0 + \omega^0 + \cdots + \omega^0 = n.$

$\omega^n(1+\omega^{-1}+\omega^{-2}+\cdots+\omega^{-(n-1)})$
$= \omega^n + \omega^{n-1} + \omega^{n-2} + \cdots + \omega^1 = 1+\omega+\omega^2+\cdots+\omega^{n-1} = 0.$

$\shortparallel$

To interpolate $A = [a_0, a_1, \ldots, a_{n-1}]$ from $B = [a(1), a(\omega), \ldots, a(\omega^{n-1})]$

$$A = V_\omega^{-1} \cdot B = \frac{1}{n} V_{\omega^{-1}} \cdot B = \frac{1}{n} \cdot \mathrm{DFFT}(n, B, \omega^{-1}) \in F^n$$

scalar × $\quad$ $O(n \log n)$ $\quad$ pnru.

4.7 Algorithm FFT Multiplication

Input $a, b \in F[x]$, F a field.
Output $c = a \times b$.

Let $n = 2^k > \deg(c) = \underset{e}{\deg(a)} + \underset{m}{\deg(b)}$.

Find $\omega \in F$ a pnru.

$A \leftarrow [a_0, a_1, \ldots, a_e, 0, 0, \ldots, 0] \in F^n$

$B \leftarrow [b_0, b_1, \ldots, b_m, 0, 0, \ldots, 0] \in F^n$

$c(x) = a(x) \cdot b(x)$
$c(\omega^i) = a(\omega^i) \cdot_F b(\omega^i)$

$A \leftarrow DFFT(n, A, \omega)$	$[a(1), a(\omega), \ldots, a(\omega^{n-1})]$
$B \leftarrow DFFT(n, B, \omega)$	$[b(1), b(\omega), \ldots, b(\omega^{n-1})]$
$C \leftarrow [A_1 \cdot B_1, A_2 \cdot B_2, \ldots, A_n \cdot B_n]$	$[\underbrace{a(1) \cdot b(1)}_{=c(1)}, \underbrace{a(\omega) \cdot b(\omega)}_{=c(\omega)}, \ldots]$
$C \leftarrow DFFT(n, C, \omega^{-1})$	$[n \cdot c_0, n \cdot c_1, \ldots]$
$C \leftarrow \frac{1}{n} \cdot C$	
Output $\sum_{i=0}^{n-1} c_i \cdot x^i$	$= c(x)$.

Total $\approx$ 3 DFFT calls $+ 2n$ mults. $= 3 \cdot O(n \log n) + 2n = O(n \log n)$

Computing pnru 4.8

Does a $n = 2^k$th pnru exist in F?

For $F = \mathbb{R}$ no.

For $F = \mathbb{C}$ yes. In $\mathbb{C}$ $e^{i\pi} = -1 \Rightarrow e^{2i\pi} = 1 \Rightarrow \omega = e^{2i\pi/n}$.

For $F = \mathbb{Z}_p$ yes iff $n | p-1$. $\quad$ $p - 1 = n \cdot q$

(i) Let α be a primitive element in $\mathbb{Z}_p$.

$\Rightarrow \boxed{\alpha^{p-1} = 1} \Rightarrow \alpha^{n \cdot q} = 1 = (\underset{\omega}{\alpha^q})^n = 1$

Maple. `alpha := numtheory[primroot](p);`

We need $n = 2^k$ and $n > \deg a + \deg b$.

Need $p = n \cdot s + 1$. Two such primes are

$p = 2^{30} \cdot 3 + 1 < 2^{32}$

$p = 2^{59} \cdot 27 + 1 < 2^{64}$