The Inverse Transform

October 4, 2023 5:25 PM

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

Let $A = [a_0, a_1, \ldots, a_{n-1}] \in F^n$ and
$B = [a(1), a(\omega^1), a(\omega^2), \ldots, a(\omega^{n-1})] \in F^n$.

Observe

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

interpolation

$a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{n-1}\omega^{n-1}$

One way to compute B is $V_\omega \cdot A$ but this does n^2 mults. in F. ✓

One way to compute A (interpolate $a(x)$) is to solve $V_\omega A = B$ for A.

Another way to compute A is to compute V_ω^{-1} then $A = V_\omega^{-1} \cdot B$.

But these cost $O(n^3)$ mults in F ☹

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

$\Rightarrow \omega^n \cdot (\omega^{-1})^k = \omega^n$

$\Rightarrow \omega^{n-k} = 1 \quad \Rightarrow 1 \le n-k < n. \quad \boxtimes$

Therefore ω^{-1} is a pnru.

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

Proof.

$$\underbrace{\begin{array}{cc} & n \\ n & \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 \cdots & \omega^{n-1} \\ \vdots & & & \\ 1 & \omega^{n-1} & \cdots & \omega^{(n-1)^2} \end{bmatrix} \end{array}}_{V_\omega} \underbrace{\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \omega^{-2} \cdots & \omega^{1-n} \\ 1 & \omega^{-2} & & \\ \vdots & & & \\ 1 & \omega^{1-n} & \cdots & \omega^{-(n-1)^2} \end{bmatrix}}_{V_{\omega^{-1}}} = \begin{bmatrix} n & 0 & & \\ 0 & n & & \\ & & & \\ & & & \end{bmatrix}$$

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

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

$\omega^n = 1 \quad 1 = \omega^n, \omega^{n-1}, \omega^{n-2}, \ldots + \omega^1$

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

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

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

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

L1. $= 0$

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

$$A = V_\omega^{-1}\cdot B = \frac{1}{n} V_{\omega^{-1}}\cdot B = \frac{1}{n}\cdot \text{DFFT}(n, B, \omega^{-1}).$$

$$B = V_\omega A = \text{DFFT}(n, A, \omega)$$

Algorithm FFT Multiplication

Input $a, b \in F[x]$, F a field. $\qquad d_a = \deg a = 7$, $\quad n = 2^5 = 32$.

Output $c = a \times b$. $\qquad d_b = \deg b = 20$. $\deg c = 27$.

Let $n = 2^k$ be the first power of 2 $> \deg(c) = \deg(a) + \deg(b)$.

Find $\omega \in F$ a pnru.

$A \leftarrow [a_0, a_1, \ldots, a_{d_a}, 0, 0, \ldots, 0] \in F^n$ $\qquad c(x) = a(x)\cdot b(x)$.

$B \leftarrow [b_0, b_1, \ldots, b_{d_b}, 0, 0, \ldots, 0] \in F^n$. $\qquad c(\omega^i) = a(\omega^i)\cdot b(\omega^i)$.

$A \leftarrow \text{DFFT}(n, A, \omega) \in F^n$ // $[a(1), a(\omega), a(\omega^2), \ldots, a(\omega^{n-1})]$

$B \leftarrow \text{DFFT}(n, B, \omega) \in F^n$ // $[b(1), b(\omega), \ldots, b(\omega^{n-1})]$

$C \leftarrow [\underset{c(1)}{A_1\cdot B_1}, \underset{c(\omega)}{A_2\cdot B_2}, \ldots, \underset{c(\omega^n)}{A_n\cdot B_n}]$.

// We have $c(\omega^i)$. We need to interpolate $c(x)$

$C \leftarrow \text{DFFT}(n, C, \omega^{-1}) \in F^n$

$C \leftarrow \frac{1}{n}\cdot C$

Output $\sum_{i=0}^{n-1} C_i x^i$.

Cost 3 DFFTs of size $n = 2^k > \deg c$. $\qquad \frac{n}{2}$ for $[1, \omega, \omega^2, \ldots, \omega^{n/2-1}]$

and $n + n$. $\qquad \frac{n}{2}$ for $[1, \omega^{-1}, \omega^{-2}, \ldots]$.

$= \frac{3}{2} n \log_2 n + 2n + n.$

$\in O(n \log n)$. mults in F.

Computing pnru.

In $\mathbb{C}$ $e^{i\pi} = -1 \Rightarrow e^{2i\pi} = 1 \Rightarrow \omega = e^{2i\pi/n}$ satisfies

$\omega^n = 1$ and it's a pnru.

In $\mathbb{Z}_p$ ω exists iff $2^k = n \mid p-1$.

Two such primes $p = 3 \cdot 2^{30} + 1 < 2^{32}$.

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

① Let α be a primitive element i.e. $\alpha^{p-1} = 1$
and $\alpha^k \neq 1$ for $1 \leq k < p-1$.

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

② $\alpha^{p-1} = 1 \Rightarrow \alpha^{nq} = 1 \Rightarrow (\underbrace{\alpha^q}_{\omega.})^n = 1.$

$n \mid p-1 \Rightarrow p-1 = n \cdot q$ for some $q \in \mathbb{Z}$.