Interative FFT and Matrix representation

September 8, 2021 10:17 PM

The FFT of $a \in F^n$ is a linear transformation from $F^n \to F^n$.
for $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in F[x]$.

$$\begin{bmatrix} f(1) \\ f(\omega) \\ f(\omega^2) \\ \vdots \\ f(\omega^{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2n-2} \\ & & \vdots & & \\ 1 & \underset{\omega^{-1}}{\underset{\parallel}{\omega^{n-1}}} & \omega^{-2} & \cdots & \omega^{1-n} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix} = Va \in F^n$$

Vandermonde.

FFT1 and FF2 correspond to two different factorizations of V

Exercise. Discover the factorizations for

$n=4$, $\omega = i$; $n=2$, $\omega=-1$; $n=1$; permutation

$$V_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & -1 & \omega^2 \\ 1 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix} = \underline{ABCP} \quad \text{FFT}$$

$$\omega^4 = 1 \qquad\qquad P \qquad\qquad P\,\underline{DEF}$$

FFT1 $\quad [a_0\ a_1\ a_2\ a_3]$

$\quad [a_0\ a_2\ a_1\ a_3]$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} a_0 \\ a_2 \\ a_1 \\ a_3 \end{bmatrix} \qquad P^2 = I.$$

$$V(\omega^{-1}) \cdot V(\omega) = nI$$

$$\underset{\text{FFT1}}{\downarrow} \qquad \underset{\text{FFT2}}{\downarrow}$$

$$ABC\,\cancel{P}\ \cancel{P}\,DEF(\omega) \quad a \quad = a.$$

The permutations in FFT1 and FFT2 can be omitted when we multiply two polynomials. We can then omit T.

The FFT permutation Π.

$A = [a_0, a_1, \ldots\ a_7]$ $\quad$ $O(n)$ moves.

The FFT permutation

$A = [a_0, a_1, \dots, a_7]$

$T = [a_0\ a_4\ a_2\ a_6\ a_1\ a_5\ a_3\ a_7]$.

$O(n)$ moves.

$n=8$

$$
\begin{array}{cccccccccc}
 & 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\
 & (0 & 1 & 2 & 3 & 4 & 5 & 6 & 7) \\
\pi & (0 & 4 & 2 & 6 & 1 & 5 & 3 & 7) \\
 & 000 & 100 & 010 & 110 & 001 & 101 & 011 & 111
\end{array}
$$

Bit reversed permutation.

Question. Why does $FFT^n_{\omega^{-1}}\left(FFT^n_{\omega}(A)\right) = nA$?

$$
\underbrace{\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \omega^{-3} \\ 1 & \omega^{-2} & 1 & \omega^{-2} \\ 1 & \omega^{-3} & \omega^{-2} & \omega^{-1} \end{bmatrix}}_{V(\omega^{-1})}
\underbrace{\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^{2} & \omega^{3} \\ 1 & \omega^{2} & 1 & \omega^{2} \\ 1 & \omega^{3} & \omega^{2} & \omega^{1} \end{bmatrix}}_{V(\omega)}
= \begin{bmatrix} 4 & 0 & & \\ 0 & \boxed{4} & & \\ & & & \\ & & & \end{bmatrix} = 4I
$$

$1 + \omega^{-1}\omega^{1} + \omega^{-2}\cdot\omega^{2} + \omega^{-3}\cdot\omega^{3} = 4$

$1 + \omega + \omega^2 + \omega^3 = 0$