Contents

1 **Lemma:** $V_\omega^{-1} = \frac{1}{n} V_{\omega^{-1}}$ **1**

2 **Definitions** **1**

3 **Theorem:** $\mathbf{DFT}_\omega(f * g) = \mathbf{DFT}_\omega(f) \cdot \mathbf{DFT}_\omega(g)$ **1**

4 **Result** **2**

$$f(x)g(x) \in \mathbb{F}_{<2n}[x]$$
$$fg = \sum_{i+j<2n-2} a_i b_j x^{i+j}$$

Complexity: $O(n^2)$

Suppose $\omega \in \mathbb{F}$ is an nth root of unity.

Recall: if $\mathbb{F} = \mathbb{F}_{p^k}$ then $\exists N : \mathbb{F}_{p^N}$ contains all nth roots of unity.

$$\mathrm{DFT}_\omega : \mathbb{F}^n \to \mathbb{F}^n$$
$$\mathrm{DFT}_\omega(f) = (f(\omega^0), f(\omega^1), ..., f(\omega^{n-1}))$$

$$V_\omega = \begin{pmatrix} 1 & 1 & 1 & ... & 1 \\ 1 & \omega^1 & \omega^2 & ... & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & ... & \omega^{2(n-1)} \\ \vdots & & & & \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & ... & \omega^{(n-1)^2} \end{pmatrix}$$

$$\mathrm{DFT}_\omega(f) = V_\omega \cdot f^T$$

since vandermonde multiplication is simply evaluation of a polynomial.

1 Lemma: $V_\omega^{-1} = \frac{1}{n} V_{\omega^{-1}}$

Use $1 + \omega + \cdots + \omega^{n-1}$ and compute $V_\omega V_{\omega^{-1}}$

Corollary: DFT_ω is invertible.

2 Definitions

1. Convolution $f * g = fg \mod (x^n - 1)$
2. Pointwise product

$$(a_0, ..., a_{n-1}) \cdot (b_0, ..., b_{n-1}) = (a_0 b_0, ..., a_{n-1} b_{n-1}) \in \mathbb{F}^n \to \mathbb{F}_{<n}[x]$$

3 Theorem: $\mathbf{DFT}_\omega(f * g) = \mathbf{DFT}_\omega(f) \cdot \mathbf{DFT}_\omega(g)$

$$fg = q'(x^n - 1) + f * g$$
$$\Rightarrow f * g = fg + q(x^n - 1)$$
$$\deg fg \le 2n - 2$$

$$\begin{aligned}(f * g)(\omega^i) &= f(\omega^i) g(\omega^i) + q(\omega^i)(\omega^{in} - 1) \\ &= f(\omega^i) g(\omega^i)\end{aligned}$$

4 Result

$$f, g \in \mathbb{F}_{<n/2}[x]$$

$$fg = f * g$$

$$\mathrm{DFT}_\omega(f * g) = \mathrm{DFT}_\omega(f) \cdot \mathrm{DFT}_\omega(g)$$

$$fg = \frac{1}{n}\mathrm{DFT}_{\omega^{-1}}(\mathrm{DFT}_\omega(f) \cdot \mathrm{DFT}_\omega(g))$$