

Contents

1 Lemma:	$V_{\omega}^{-1} = \frac{1}{n} V_{\omega^{-1}}$	1
2 Definitions		1
3 Theorem:	$\text{DFT}_{\omega}(f * g) = \text{DFT}_{\omega}(f) \cdot \text{DFT}_{\omega}(g)$	2
4 Result		2
5 Finite Field Extension Containing Nth Roots of Unity		2
6 FFT Algorithm Recursive Compute		2
6.1	Algorithm	3
6.2	Even Values	3
6.3	Odd Values	3
7 Example		4
8 Comparing Evaluations for $f(X)$ and $r(X), s(X)$		4
8.1	Even Values	4
8.2	Odd Values	5

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

$$fg = \sum_{i+j < 2n-2} a_i b_j x^{i+j}$$

Complexity: $O(n^2)$

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

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

$$\text{DFT}_{\omega} : \mathbb{F}^n \rightarrow \mathbb{F}^n$$

$$\text{DFT}_{\omega}(f) = (f(\omega^0), f(\omega^1), \dots, f(\omega^{n-1}))$$

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

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

since vandermonde multiplication is simply evaluation of a polynomial.

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

Use $1 + \omega + \dots + \omega^{n-1}$ 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

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

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

$$\begin{aligned} fg &= q'(x^n - 1) + f * g \\ \Rightarrow f * g &= fg + q(x^n - 1) \\ \deg fg &\leq 2n - 2 \end{aligned}$$

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

4 Result

$$\begin{aligned} f, g &\in \mathbb{F}_{<n/2}[x] \\ fg &= f * g \\ \text{DFT}_\omega(f * g) &= \text{DFT}_\omega(f) \cdot \text{DFT}_\omega(g) \\ fg &= \frac{1}{n} \text{DFT}_{\omega^{-1}}(\text{DFT}_\omega(f) \cdot \text{DFT}_\omega(g)) \end{aligned}$$

5 Finite Field Extension Containing Nth Roots of Unity

$$\begin{aligned} \mu_N &= \langle \omega \rangle, |\mathbb{F}_{p^N}^\times| = p^N - 1 \\ \text{ord}(\omega) &= n |p^N - 1| \end{aligned}$$

but $\mathbb{F}_{p^N}^\times$ is cyclic.

For all $d | p^N - 1$, there exists $x \in \mathbb{F}_{p^N}^\times$ with $\text{ord}(x) = d$.

Finding $n | p^N - 1$ is sufficient for $\omega \in \mathbb{F}_{p^N}$

$$n | p^N - 1 \Leftrightarrow \text{ord}(p) = (\mathbb{Z}/n\mathbb{Z})^\times$$

6 FFT Algorithm Recursive Compute

We recurse to a depth of $\log n$. Since each recursion uses ω^i , then in the final step $\omega^i = 1$, and we simply return f^T .

We only need to prove a single step of the algorithm produces the desired result, and then the correctness is inductively proven.

$$\begin{aligned} f(X) &= a_0 + a_1X + a_2X^2 + \dots + a_{n-1}X^{n-1} \\ &= g(X) + X^{n/2}h(X) \end{aligned}$$

6.1 Algorithm

Algorithm 1 Discrete Fourier Transform

```

1: function DFT( $n = 2^d, f(X)$ )
2:   if  $n = 1$  then
3:     return  $f(X)$ 
4:   end if
5:    $f(X) = g(X) + X^{n/2}h(X)$  ▷ Write  $f(X)$  as the sum of two polynomials with equal degree
6:   Let  $\mathbf{g}, \mathbf{h}$  be the vector representations of  $g(X), h(X)$ 
7:
8:    $\mathbf{r} = \mathbf{g} + \mathbf{h}$ 
9:    $\mathbf{s} = (\mathbf{g} - \mathbf{h}) \cdot (\omega^0, \dots, \omega^{n/2-1})$ 
10:  Let  $r(X), s(X)$  be the polynomials represented by the vectors  $\mathbf{r}, \mathbf{s}$ 
11:
12:  Compute  $(r(\omega^0), \dots, r(\omega^{n/2})) = \text{DFT}_{\omega^2}(n/2, r(X))$ 
13:  Compute  $(s(\omega^0), \dots, s(\omega^{n/2})) = \text{DFT}_{\omega^2}(n/2, s(X))$ 
14:
15:  return  $(r(\omega^0), s(\omega^0), r(\omega^2), s(\omega^2), \dots, r(\omega^{n/2}), s(\omega^{n/2}))$ 
16: end function

```

6.2 Even Values

$$r(X) = g(X) + h(X)$$

$$\begin{aligned}
f(\omega^{2i}) &= g(\omega^{2i}) + (\omega^{2i})^{n/2} h(\omega^{2i}) \\
&= g(\omega^{2i}) + h(\omega^{2i}) \\
&= (g + h)(\omega^{2i})
\end{aligned}$$

So then we can now compute $\text{DFT}_{\omega}(f)_{k=2i} = \text{DFT}_{\omega^2}(r)$ for the even powers of $f(\omega^{2i})$.

6.3 Odd Values

For odd values $k = 2i + 1$

$$s(X) = (g(X) - h(X)) \cdot (\omega^0, \dots, \omega^{n/2-1})$$

$$\begin{aligned}
f(X) &= a_0 + a_1 X + a_2 X^2 + \dots + a_{n-1} X^{n-1} \\
&= g(X) + X^{n/2} h(X) \\
f(\omega^{2i+1}) &= g(\omega^{2i+1}) + (\omega^{2i+1})^{n/2} h(\omega^{2i+1})
\end{aligned}$$

But observe that for any n th root of unity $\omega^n = 1$ and $\omega^{n/2} = -1$

$$(\omega^{2i+1})^{n/2} = \omega^{in} \omega^{n/2} = \omega^{n/2} = -1$$

$$\begin{aligned}
\Rightarrow f(\omega^{2i+1}) &= g(\omega^{2i+1}) - h(\omega^{2i+1}) \\
&= (g - h)(\omega^{2i+1})
\end{aligned}$$

Let $\mathbf{s} = (\mathbf{g} - \mathbf{h}) \cdot (\omega^0, \dots, \omega^{n/2-1})$ be the representation for $s(X)$. Then we can see that $s(\omega^{2i+1}) = (g - h)(\omega^{2i+1})$ as desired.

So then we can now compute $\text{DFT}_{\omega}(f)_{k=2i+1} = \text{DFT}_{\omega^2}(s)$ for the odd powers of $f(\omega^{2i+1})$.

7 Example

Let $n = 8$

$$\begin{aligned}
f(X) &= (a_0 + a_1X + a_2X^2 + a_3X^3) + (a_4X^4 + a_5X^5 + a_6X^6 + a_7X^7) \\
&= (a_0 + a_1X + a_2X^2 + a_3X^3) + X^4(a_4 + a_5X + a_6X^2 + a_7X^3) \\
&= g(X) + X^{n/2}h(X) \\
g(X) &= a_0 + a_1X + a_2X^2 + a_3X^3 \\
h(X) &= a_4 + a_5X + a_6X^2 + a_7X^3
\end{aligned}$$

Now vectorize $g(X), h(X)$

$$\begin{aligned}
\mathbf{g} &= (a_0, a_1, a_2, a_3) \\
\mathbf{h} &= (a_4, a_5, a_6, a_7)
\end{aligned}$$

Compute reduced polynomials in vector form

$$\begin{aligned}
\mathbf{r} &= \mathbf{g} + \mathbf{h} \\
&= (a_0 + a_4, a_1 + a_5, a_2 + a_6, a_3 + a_7) \\
\mathbf{s} &= (\mathbf{g} - \mathbf{h}) \cdot (1, \omega, \omega^2, \omega^3) \\
&= (a_0 - a_4, a_1 - a_5, a_2 - a_6, a_3 - a_7) \cdot (1, \omega, \omega^2, \omega^3) \\
&= (a_0 - a_4, \omega(a_1 - a_5), \omega^2(a_2 - a_6), \omega^3(a_3 - a_7))
\end{aligned}$$

Convert them to polynomials from the vectors. We also expand them out below for completeness.

$$\begin{aligned}
r(X) &= r_0 + r_1X + r_2X^2 + r_3X^3 \\
&= (a_0 + a_4) + (a_1 + a_5)X + (a_2 + a_6)X^2 + (a_3 + a_7)X^3 \\
s(X) &= s_0 + s_1X + s_2X^2 + s_3X^3 \\
&= (a_0 - a_4) + \omega(a_1 - a_5)X + \omega^2(a_2 - a_6)X^2 + \omega^3(a_3 - a_7)X^3
\end{aligned}$$

Compute

$$\text{DFT}_{\omega^2}(4, r(X)), \text{DFT}_{\omega^2}(4, s(X))$$

The values returned will be

$$(r(1), s(1), r(\omega^2), s(\omega^2), r(\omega^4), s(\omega^4), r(\omega^6), s(\omega^6)) = (f(1), f(\omega), f(\omega^2), f(\omega^3), f(\omega^4), f(\omega^5), f(\omega^6), f(\omega^7))$$

Which is the output we return.

8 Comparing Evaluations for $f(X)$ and $r(X), s(X)$

We can see the evaluations are correct by substituting in ω^i .

We expect that $s(X)$ on the domain $(1, \omega^2, \omega^4, \omega^6)$ produces the values $(f(1), f(\omega^2), f(\omega^4), f(\omega^6))$, while $r(X)$ on the same domain produces $(f(\omega), f(\omega^3), f(\omega^5), f(\omega^7))$.

8.1 Even Values

Let $k = 2i$, be an even number. Then note that k is a multiple of 2, so $4k$ is a multiple of $n \Rightarrow \omega^{4k} = 1$,

$$\begin{aligned}
r(X) &= (a_0 + a_4) + (a_1 + a_5)X + (a_2 + a_6)X^2 + (a_3 + a_7)X^3 \\
r(\omega^{2i}) &= (a_0 + a_4) + (a_1 + a_5)\omega^{2i} + (a_2 + a_6)\omega^{4i} + (a_3 + a_7)\omega^{6i} \\
f(\omega^k) &= (a_0 + a_1\omega^k + a_2\omega^{2k} + a_3\omega^{3k}) + \omega^{4k}(a_4 + a_5\omega^k + a_6\omega^{2k} + a_7\omega^{3k}) \\
&= (a_0 + a_1\omega^k + a_2\omega^{2k} + a_3\omega^{3k}) + (a_4 + a_5\omega^k + a_6\omega^{2k} + a_7\omega^{3k}) \\
&= (a_0 + a_4) + (a_1 + a_5)\omega^k + (a_2 + a_6)\omega^{2k} + (a_3 + a_7)\omega^{3k} \\
&= f(\omega^{2i}) \\
&= (a_0 + a_4) + (a_1 + a_5)\omega^{2i} + (a_2 + a_6)\omega^{4i} + (a_3 + a_7)\omega^{6i} \\
&= r(\omega^{2i})
\end{aligned}$$

8.2 Odd Values

For $k = 2i + 1$ odd, we have a similar relation where $4k = 8i + 4$, so $\omega^{4k} = \omega^4$. But observe that $\omega^4 = -1$.

$$\begin{aligned}
s(X) &= (a_0 - a_4) + \omega(a_1 - a_5)X + \omega^2(a_2 - a_6)X^2 + \omega^3(a_3 - a_7)X^3 \\
s(\omega^{2i}) &= (a_0 - a_4) + (a_1 - a_5)\omega^{2i+1} + (a_2 - a_6)\omega^{4i+2} + (a_3 - a_7)\omega^{6i+3} \\
f(\omega^k) &= (a_0 + a_1\omega^k + a_2\omega^{2k} + a_3\omega^{3k}) + \omega^{4k}(a_4 + a_5\omega^k + a_6\omega^{2k} + a_7\omega^{3k}) \\
&= (a_0 + a_1\omega^k + a_2\omega^{2k} + a_3\omega^{3k}) - (a_4 + a_5\omega^k + a_6\omega^{2k} + a_7\omega^{3k}) \\
&= f(\omega^{2i+1}) \\
&= (a_0 + a_1\omega^{2i+1} + a_2\omega^{4i+2} + a_3\omega^{6i+3}) - (a_4 + a_5\omega^{2i+1} + a_6\omega^{4i+2} + a_7\omega^{6i+3}) \\
&= (a_0 - a_4) + (a_1 - a_5)\omega^{2i+1} + (a_2 - a_6)\omega^{4i+2} + (a_3 - a_7)\omega^{6i+3} \\
&= s(\omega^{2i})
\end{aligned}$$