Inverse Fourier Transform, A Justification

Let $n = 2^k$, ω be a primitive n-th root of unity in $\mathbb{C}[x]$ and

$$a(x) = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{C}[x].$$

Let $\mathbf{A} = [a_0, a_1, a_2, \ldots, a_{n-1}]$ and $\mathbf{W} = [a(1), a(\omega), a(\omega^2), \ldots, a(\omega^{n-1})] \in \mathbb{C}^n$ ($\mathbf{W}$ is the result of the "forward" discrete Fourier transform applied at ω).

An alternate to the DFT would be to compute $\mathbf{W}$ naively:

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} a(1) \\ a(\omega) \\ a(\omega^2) \\ \vdots \\ a(\omega^{n-1}) \end{bmatrix}$$

$$\mathbf{V}_\omega \mathbf{A} = \mathbf{W}$$

which requires n^2 multiplications (way worse then DFT). To be more explicit:

$$\text{DFT}(n, a(x), \omega) \equiv \text{ calculating } \mathbf{V}_\omega \mathbf{A}.$$

(Note that $\mathbf{V}_\omega$ is the Vandermode matrix for ω.)

To go in the opposite direction, that is to get $\mathbf{A}$ if $\mathbf{W}$ is known, we can just solve the corresponding linear system: $\mathbf{A} = \mathbf{V}_\omega^{-1}\mathbf{W}$.

Lemma 1.

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \cdots & \omega^{n-1} \\ 1 & \omega^{-2} & \omega^{-4} & \cdots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(n-1)} & \omega^{-2(n-1)} & \cdots & \omega^{-(n-1)(n-1)} \end{bmatrix} = n \cdot \mathbf{I}$$

that is $\mathbf{V}_\omega \mathbf{V}_{\omega^{-1}} = n \cdot \mathbf{I}$.

Proof. If we let $n = 4$ then the product of $\mathbf{V}_\omega$ and $\mathbf{V}_{\omega^{-1}}$ looks like:

$$\mathbf{M} = \begin{bmatrix} 4 & 1+\omega^{-1}+\omega^{-2}+\omega^{-3} & 1+\omega^{-2}+\omega^{-4}+\omega^{-6} & 1+\omega^{-3}+\omega^{-6}+\omega^{-9} \\ 1+\omega+\omega^2+\omega^3 & 4 & 1+\omega^{-1}+\omega^{-2}+\omega^{-3} & 1+\omega^{-2}+\omega^{-4}+\omega^{-6} \\ 1+\omega^2+\omega^4+\omega^6 & 1+\omega+\omega^2+\omega^3 & 4 & 1+\omega^{-1}+\omega^{-2}+\omega^{-3} \\ 1+\omega^3+\omega^6+\omega^9 & 1+\omega^2+\omega^4+\omega^6 & 1+\omega+\omega^2+\omega^3 & 4 \end{bmatrix}$$

From this it is straight forward to discern the general pattern. For any n, the polynomials at any diagonal are given by $1 + \omega^k + \omega^{2k} + \cdots + \omega^{(n-1)k} = s(k)$ for $0 < k < n$.

As $s(k)$ is a geometric series in ω^k

$$s(k) = \sum_{i=0}^{n-1} \left(\omega^k\right)^i = \frac{1 - (\omega^k)^n}{1 - \omega^k} = \frac{1 - 1}{1 - \omega^k} = 0.$$

(recall that $k < n$ so $1 - \omega^k \neq 0$). Therefore we have that $s(k) = 0$ for all $0 < k < n$ if ω is a primitive n-th root of unity.

For $n < k < 0$ recall that $1/\omega$ is also a primitive n-th root of unity and apply the same proof.

For $k = 0$ (diagonal) we have that $s(0) = n$, this gives the desired result. □

An immediate consequence of Lemma 1 is that $\mathbf{V}_\omega^{-1} = \frac{1}{n}\mathbf{V}_{\omega^{-1}}$. So, to interpolate $a(x)$ from $\mathbf{W}$ we do

$$\mathbf{A} = \mathbf{V}_\omega^{-1}\mathbf{W} = \frac{1}{n}\mathbf{V}_{\omega^{-1}}\mathbf{W} = \frac{1}{n}\text{DFT}(n, b(x), \omega^{-1})$$

where $b(x) = \mathbf{W}[1] + \mathbf{W}[2]x + \cdots + \mathbf{W}[n]x^{n-1}$.