Circular Convolution and Discrete Fourier Transform

Frank the Giant Bunny

January 2, 2016

Consider three vectors $a, b, c \in \mathbb{C}^n$ where c is a *circular convolution* of a and b:

$$c_i = \sum_{k=0}^{n-1} a_k b_{\langle i-k \rangle_n} \quad \text{for } i \in \{0, 1, \cdots, n-1\}$$

where $\langle \ell \rangle_n$ is a modulo operator. Define another vectors α, β, and γ as the *Discrete Fourier Transform* (DFT) of a, b, and c

$$\alpha_j = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} a_i \overline{\omega}^{ij}, \quad \beta_j = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} b_i \overline{\omega}^{ij}, \quad \text{and} \quad \gamma_j = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} c_i \overline{\omega}^{ij},$$

where $\omega = e^{\iota 2\pi/n}$ is the *primitive* n^{th} *root of unity* and $\overline{\omega}$ is its complex conjugate. Then the *circular convolution property* states that γ is obtained by the entry-wise product of α and β. This is easily seen by rearranging terms in summations.

$$\begin{aligned}
\gamma_j &= \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} c_i \overline{\omega}^{ij} && \text{by definition of DFT} \\
&= \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} \left(\sum_{k=0}^{n-1} a_k b_{\langle i-k \rangle_n} \right) \overline{\omega}^{ij} && \text{by definition of } c_i \\
&= \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} a_k \left(\sum_{i=0}^{n-1} b_{\langle i-k \rangle_n} \right) \overline{\omega}^{ij} && \text{by rearranging terms} \\
&= \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} a_k \overline{\omega}^{kj} \left(\sum_{i=0}^{n-1} b_{\langle i-k \rangle_n} \overline{\omega}^{(i-k)j} \right) && \text{by decomposing } \overline{\omega}^{ij} \\
&= \alpha_j \left(\sum_{i=0}^{n-1} b_{\langle i-k \rangle_n} \overline{\omega}^{(i-k)j} \right) && \text{by definition of DFT} \\
&= \alpha_j \left(\sum_{i=0}^{n-1} b_{\langle i-k \rangle_n} \overline{\omega}^{\langle i-k \rangle_n j} \right) && \overline{\omega}^n = 1 \\
&= \sqrt{n} \alpha_j \left(\frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} b_{\langle i-k \rangle_n} \overline{\omega}^{\langle i-k \rangle_n j} \right) && \text{by decomposing 1} \\
&= \sqrt{n} \alpha_j \beta_j && \text{by definition of DFT}
\end{aligned}$$