CSC 721 Algorithms Fall 2015

The FFT and the Convolution Theorem

Given two vectors of length n:

$$\begin{aligned} \mathbf{a} &= [\, a_0, a_1, a_2, ..., a_{n-1} \,]^T \\ \mathbf{b} &= [\, b_0, b_1, b_2, ..., b_{n-1} \,]^T \end{aligned}$$

we define $\mathbf{a}_i = \mathbf{b}_i = 0$ whenever $i < 0$ or $i \geq n$. I.e., we extend the support of $\mathbf{a}_i$ and $\mathbf{b}_i$ to all integers i, with the convention that the vectors are zero outside the index range $[\, 0, 1, 2, ..., n-1 \,]$.

We define the **convolution** of $\mathbf{a}$ and $\mathbf{b}$ denoted by $\mathbf{c} = \mathbf{a} \circledast \mathbf{b}$ as a vector of length $2n$ as follows:

$$\mathbf{c}_i \;=\; \sum_{j=0}^{n-1} \mathbf{a}_j \, \mathbf{b}_{i-j} \tag{1}$$

where $0 \leq i < 2n$. Observe that by this definition[1] it will always be the case that $\mathbf{c}_{2n-1} = 0$.

Let $\hat{\mathbf{a}}$ and $\hat{\mathbf{b}}$ denote the vectors $\mathbf{a}$ and $\mathbf{b}$ padded with zeros to make them length $2n$. I.e.,

$$\begin{aligned} \hat{\mathbf{a}} &= [\, a_0, a_1, a_2, ..., a_{n-1}, 0, 0, ..., 0 \,]^T \\ \hat{\mathbf{b}} &= [\, b_0, b_1, b_2, ..., b_{n-1}, 0, 0, ..., 0 \,]^T \end{aligned}$$

Theorem

$$\mathbf{a} \circledast \mathbf{b} \;=\; F^{-1} \left(F\hat{\mathbf{a}} \circ F\hat{\mathbf{b}} \right)$$

where the operation "$\circ$" denotes component-wise multiplication and F denotes the $2n \times 2n$ discrete Fourier transform.

Proof

It suffices to show:

$$F\,(\, \mathbf{a} \circledast \mathbf{b} \,) \;=\; \left(F\hat{\mathbf{a}} \circ F\hat{\mathbf{b}} \right) \tag{2}$$

Let

$$\begin{aligned} F\hat{\mathbf{a}} &= \left[\, a'_0, a'_1, a'_2, ..., a'_{2n-1} \,\right] \\ F\hat{\mathbf{b}} &= \left[\, b'_0, b'_1, b'_2, ..., b'_{2n-1} \,\right] \end{aligned}$$

denote the Fourier transforms of $\hat{\mathbf{a}}$ and $\hat{\mathbf{b}}$ respectively. By definition:

$$\begin{aligned} a'_i &= \textstyle\sum_{j=0}^{2n-1} \; \omega^{ij} \, \hat{\mathbf{a}}_j \\ b'_i &= \textstyle\sum_{k=0}^{2n-1} \; \omega^{ik} \, \hat{\mathbf{b}}_k \end{aligned}$$

[1] We might define define $\mathbf{a} \circledast \mathbf{b}$ to be a sequence of length $2n-1$. In our discussion of the convolution theorem, it will be convenient to define the length of the result $\mathbf{c}$ to be equal to twice the length of the input vectors $\mathbf{a}$ and $\mathbf{b}$.

Multiplying, we have

$$a'_i\, b'_i \;=\; \left(\sum_{j=0}^{2n-1} \omega^{ij}\, \hat{\mathbf{a}}_j \right) \left(\sum_{k=0}^{2n-1} \omega^{ik}\, \hat{\mathbf{b}}_k \right) \tag{3}$$

$$= \sum_{j=0}^{2n-1} \sum_{k=0}^{2n-1} \omega^{i(j+k)}\, \hat{\mathbf{a}}_j\, \hat{\mathbf{b}}_k \tag{4}$$

$$= \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} \omega^{i(j+k)}\, a_j\, b_k \tag{5}$$

Equation (5) follows from equation (4) because $\hat{\mathbf{a}}_j = 0$ whenever $j \geq n$ and $\hat{\mathbf{b}}_k = 0$ whenever $k \geq n$.

Equation (5) is our final expression for the right hand side of equation (2). We now consider the left hand side of equation (2). The theorem will be proven when we show that the two sides are equal.

Recall $\mathbf{c} = \mathbf{a} \circledast \mathbf{b}$ and let

$$F\mathbf{c} \;=\; \left[\, c'_0, c'_1, c'_2, ..., c'_{2n-1} \,\right]$$

denote the Fourier transform of $\mathbf{c}$. By definition of the Fourier transform we have:

$$c'_i \;=\; \sum_{\ell=0}^{2n-1} \omega^{i\ell}\, \mathbf{c}_\ell \tag{6}$$

Applying definition (1) to $\mathbf{c}_i$ in equation (6), we have:

$$c'_i \;=\; \sum_{\ell=0}^{2n-1} \omega^{i\ell} \sum_{j=0}^{n-1} \mathbf{a}_j\, \mathbf{b}_{\ell-j} \tag{7}$$

Distributing, and exchanging the order of summation:

$$c'_i \;=\; \sum_{j=0}^{n-1} \sum_{\ell=0}^{2n-1} \omega^{i\ell}\, \mathbf{a}_j\, \mathbf{b}_{\ell-j} \tag{8}$$

We now perform a change-of-variable substitution in the inner summation in equation (8). Let $k = \ell - j$. To make the substitution, we can replace the expression $\ell - j$ by k, and we can replace the variable ℓ by $k + j$. We also need to adjust the limits of summation since k is the new index variable in the summation. If $\ell = 0$, then $k = -j$. If $\ell = 2n - 1$, then $k = 2n - 1 - j$. Therefore:

$$c'_i \;=\; \sum_{j=0}^{n-1} \sum_{k=-j}^{2n-1-j} \omega^{i(j+k)}\, \mathbf{a}_j\, \mathbf{b}_k \tag{9}$$

Notice when we finish our change-of-variable substitution, the variable ℓ is no longer present in equation (9).

In equation (9), notice that for any negative values of k, each term will have a factor of zero, since $\mathbf{b}_k = 0$ whenever $k < 0$. Therefore we can adjust the lower limit of the summation and write:

$$c'_i \;=\; \sum_{j=0}^{n-1} \sum_{k=0}^{2n-1-j} \omega^{i(j+k)}\, \mathbf{a}_j\, \mathbf{b}_k \tag{10}$$

We are almost done. We now need to lower the upper limit of the inner summation to $n-1$, but we need to prove that by doing so, we are not changing the value of the sum. We accomplish this by considering the range of j and doing some simple math.

From the limits of the outer summation, we know:

$$0 \;\leq\; j \;\leq\; n-1 \quad . \tag{11}$$

Multiplying inequality (11) by -1, mindful of the properties of inequalities, we have:

$$-n+1 \;\leq\; -j \;\leq\; 0 \quad . \tag{12}$$

Adding $2n-1$ to each expression in inequality (12) we obtain:

$$\begin{aligned} 2n-1-n+1 \quad &\leq \quad 2n-1-j \quad \leq \quad 2n-1 \\ n \quad &\leq \quad 2n-1-j \quad \leq \quad 2n-1 \end{aligned} \tag{13}$$

Inequality (13) shows that the upper limit in the inner summation in equation (10) is always greater than $n-1$. However, $\mathbf{b}_k = 0$ for all values of k greater than $n-1$. Therefore, we can safely lower the upper bound on the inner summation of equation (10) to $n-1$, since all the newly excluded terms are zero. We obtain:

$$c'_i \;=\; \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} \omega^{i(j+k)}\, \mathbf{a}_j\, \mathbf{b}_k \tag{14}$$

The right hand side of equation (14) exactly matches the right hand side of equation (5). Therefore we have:

$$c'_i \;=\; a'_i\, b'_i \tag{15}$$

and the theorem is proven.

∎