Convolution Notes

Selim Emir Can

April 29, 2024

Contents

Conventions

$*$ denotes the discrete convolution operation.
$\circledast$ denotes the discrete time periodic convolution operation.
$\circ$ denotes the discrete time circular convolution operation.

Preliminary Notes

This document is a small set of notes about discrete convolutions compiled by me while I was taking EC ENGR 113 (Winter Quarter 2022) which was taught by Professor Achuta Kadambi. I have also taken inspiration from Signals and Systems by Alkin Oktay which was the recommended course reading at the time.

1 Types of Convolution

Challenge Questions

1) How does circular convolution relate to linear convolution?
2) What can be done to ensure circular convolution result obtained using the DFT method matches the linear convolution result?

1.1 Linear Convolution

Definition 1.1 (Convolution). Suppose $x \in \mathbb{R}^d, h \in \mathbb{R}^m$. The **convolution** of x with h, or $y \in \mathbb{R}^{(m+d-1)}$, is:

$$y[n] = x[n] * h[n] := \sum_{k=-\infty}^{k=\infty} x[k]h[n-k]$$

Proposition 1.2. The convolution operation is commutative (i.e. $h[n] * x[n] = x[n] * h[n]$)

Proof. We have $x[n] * h[n] = \sum_{k=-\infty}^{k=\infty} x[k]h[n-k]$. Now, define $m = n - k$. Then, $m|_{n=-\infty} = -\infty - k = -\infty$ and $m|_{n=\infty} = \infty - k = \infty$. So, $x[n] * h[n] = \sum_{m=-\infty}^{m=\infty} x[n-m]h[m] = \sum_{m=-\infty}^{m=\infty} h[m]x[n-m] = h[n] * x[n]$. Thus, it follows that $x[n] * h[n] = h[n] * x[n]$. □

Proposition 1.3. The convolution operation is distributive (i.e. $x[n] * (h_1[n] + h_2[n]) = x[n] * h_1[n] + x[n] * h_2[n]$)

Proof. We have $x[n] * (h_1[n] + h_2[n]) = \sum_{k=-\infty}^{k=\infty} x[k](h_1[n-k] + h_2[n-k]) = \sum_{k=-\infty}^{k=\infty} (x[k]h_1[n-k] + x[k]h_2[n-k])$ $= \sum_{k=-\infty}^{k=\infty} x[k]h_1[n-k] + \sum_{k=-\infty}^{k=\infty} x[k]h_2[n-k] = x[n] * h_1[n] + x[n] * h_2[n]$. Thus, it follows that $x[n] * (h_1[n] + h_2[n]) = x[n] * h_1[n] + x[n] * h_2[n]$ □

Proposition 1.4. The convolution operation exhibits the identity property (i.e. $x[n] * \delta[n-m] = x[n-m]$)

Proof. We have $x[n] * \delta[n-m] = \sum_{k=-\infty}^{k=\infty} x[k]\delta[(n-m)-k]$. Since $\delta[(n-m)-k] = \left\{ \begin{array}{ll} 1, & \text{if } k = (n-m) \\ 0, & \text{if } k \neq (n-m) \end{array} \right\}$, we also have $\sum_{k=-\infty}^{k=\infty} x[k]\delta[(n-m)-k] = 0 \times x[0] + ... + 1 \times x[n-m] + ... + 0 \times x[d-1] = x[n-m]$. Thus, it follows that $x[n] * \delta[n-m] = x[n-m]$ □

Exercise. Given $x \in \mathbb{R}^d$ where $x[n] = 0$ for $n < N_1$ or $n \geq (N_1 + d)$ and $h \in \mathbb{R}^m$ where $h[n] = 0$ for $n < N_2$ or $n \geq (N_2 + m)$, show that the convolution of x with h, $y \in \mathbb{R}^{(m+d-1)}$, can be expressed as:

$$y[n] = x[n] * h[n] = \sum_{k=k_1}^{k=k_2} x[k]h[n-k]$$

where $k_2 = min(N_1 + d - 1, n - N_2)$ and $k_1 = max(N_1, n - N_2 - m + 1)$

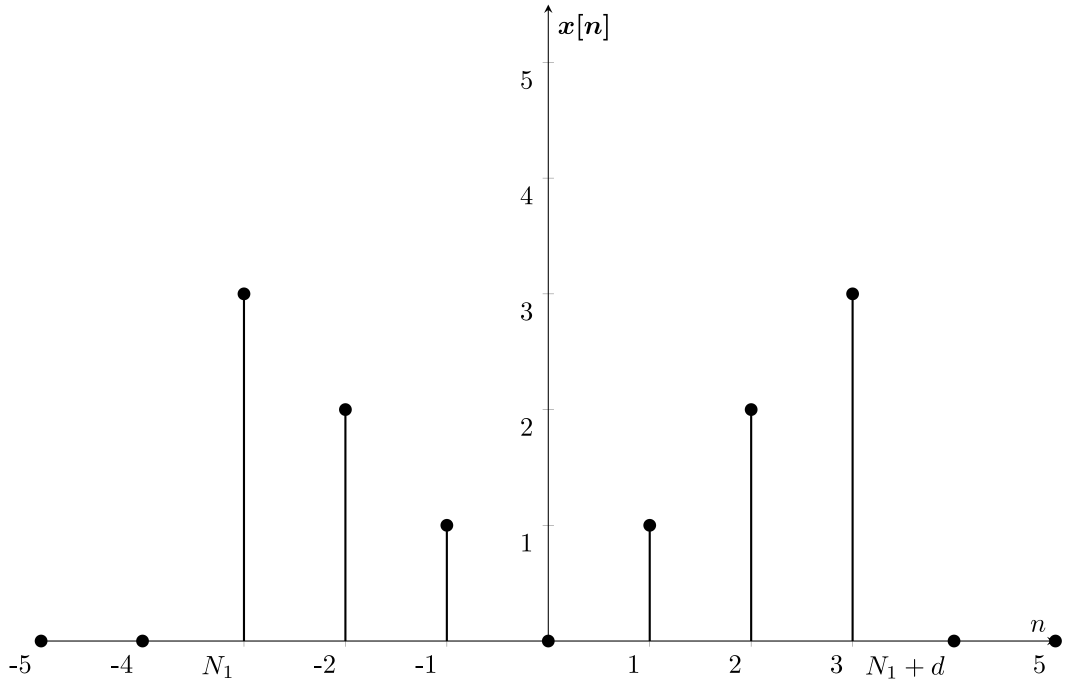

Figure 1: Example signal for exercise 1

Proof. $x[n] * h[n] = \sum_{-\infty}^{\infty} x[k]h[n-k]$. However, notice that $x[k]h[n-k]$ only contributes to the resultant sum if both $x[k]$ and $h[n-k]$ are non-zero simultaneously. We know that $x[k]$ is non-zero for $N_1 \leq k < (N_1+d)$ and $h[n-k]$ is non-zero for $n-(N_2+m) < n-k \leq n-N_2$ (note the order of the bounds since we are subtracting k from n). Now, since these bounds are not equal in general we want **the greatest lower bound** and **the least upper bound** which gives that $x[k]h[n-k]$ is nonzero for $max(N_1, n-(N_2+m)+1) \leq k \leq min(n-N_2, (N_1+d)-1)$. Note that the extra -1 and +1 are both due to our original non-inclusive bounds. This allows us to express the convolution as:

$$y[n] = x[n] * h[n] = \sum_{k=k_1}^{k=k_2} x[k]h[n-k]$$

where $k_2 = min(n-N_2, N_1+d-1)$ and $k_1 = max(N_1, n-N_2-m+1)$, thus completing the proof. $\square$

1.2 Interpretations of Linear Convolution

An equivalent definition for the convolution operator that may be more intuitive for some people is as follows:

Definition 1.5 (Convolution)**.** Suppose $a \in \mathbb{R}^d, b \in \mathbb{R}^m$. The **convolution** of a with b, or $c \in \mathbb{R}^{(m+d-1)}$, is:

$$c[n] = a[n] * b[n] := \sum_{\substack{\text{all } i \text{ and } j \text{ with} \\ i+j=n}} a[i]b[j]$$

This formulation gives way to multiple interpretations. A probabilistic interpretation is as follows: A and B are two discrete random variables such that $P(A=i) = a[i]$ and $P(B=j) = b[j]$ for all i and j. Then, the convolution, $c = a*b$ is equivalent to adding two random variables together such that $c[n] = P(A+B=n)$. Let's set up a theoretical experiment where is A the value of weighted die 1 and B is the value of weighted die 2 after they are both thrown. We can visualize this scenario in a probability distribution function table for a weighted die.

x	$P(A=x), a[x]$
1	1/16
2	2/16
3	3/16
4	4/16
5	4/16
6	2/16

x	$P(B=x), b[x]$
1	1/16
2	4/16
3	2/16
4	3/16
5	3/16
6	3/16

$P(A) \times P(B)$	$P(B=1)$	$P(B=2)$	$P(B=3)$	$P(B=4)$	$P(B=5)$	$P(B=6)$
$P(A=1)$	1/256	4/256	2/256	3/256	3/256	3/256
$P(A=2)$	2/256	8/256	4/256	6/256	6/256	6/256
$P(A=3)$	3/256	12/256	6/256	9/256	9/256	9/256
$P(A=4)$	4/256	16/256	8/256	12/256	12/256	12/256
$P(A=5)$	4/256	16/256	8/256	12/256	12/256	12/256
$P(A=6)$	2/256	8/256	4/256	6/256	6/256	6/256

Now, we are able to see a pattern confirming our intuition:

$c[0] = 0 = P(A+B=0)$

$c[1] = 0 = P(A+B=1)$

$c[2] = a[1]b[1] = \frac{1}{256} = P(A+B=2)$

$c[3] = a[2]b[1] + a[1]b[2] = \frac{6}{256} = P(A+B=3)$

$c[4] = a[3]b[1] + a[2]b[2] + a[1]b[3] = \frac{13}{256} = P(A+B=4)$

$c[5] = a[4]b[1] + a[3]b[2] + a[2]b[3] + a[1]b[4] = \frac{23}{256} = P(A+B=5)$

$$\vdots$$

Another perspective we can take is viewing the convolution as polynomial multiplication. If a and b are the coefficients of polynomials $p(x) = a[0] + a[1] \cdot x + ... + a[d-1] \cdot x^{d-1}$ and $q(x) = b[0] + b[1] \cdot x + ... + b[m-1] \cdot x^{m-1}$, then $c = a * b$ gives the coefficients of the product polynomial $p(x)q(x) = c[0] + c[1] \cdot x + ... + c[m+d-2] \cdot x^{m+d-2}$.

Proof. We know that $p(x)q(x) = (a[0] + ... + a[d-1] \cdot x^{d-1})(b[0] + ... + b[m-1] \cdot x^{m-1})$. But instead of writing out each term, lets make a product table of the coefficients of a and b indexed by the order of x. The $(n+1)^{th}$ anti-diagonal of this table will give us all the terms of order n, which when summed, gives us the n^{th} coefficient of $p(x)q(x)$.

order of x	$\mathbf{a[0]}$	$\mathbf{a[1]}$	$\mathbf{a[2]}$	...	$\mathbf{a[d-2]}$	$\mathbf{a[d-1]}$
$\mathbf{b[0]}$	$a[0]b[0]$	$a[1]b[0]$	$a[2]b[0]$	...	$a[d-2]b[0]$	$a[d-1]b[0]$
$\mathbf{b[1]}$	$a[0]b[1]$	$a[1]b[1]$	$a[2]b[1]$	...	$a[d-2]b[1]$	$a[d-1]b[1]$
$\mathbf{b[2]}$	$a[0]b[2]$	$a[1]b[2]$	$a[2]b[2]$	...	$a[d-2]b[2]$	$a[d-1]b[2]$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
$\mathbf{b[m-2]}$	$a[0]b[m-2]$	$a[1]b[m-2]$	$a[2]b[m-2]$	...	$a[d-2]b[m-2]$	$a[d-1]b[m-2]$
$\mathbf{b[m-1]}$	$a[0]b[m-1]$	$a[1]b[m-1]$	$a[2]b[m-1]$	...	$a[d-2]b[m-1]$	$a[d-1]b[m-1]$

Now, using this table, we can see that the 2^{nd} anti-diagonal (line from **b[2]** to **a[2]**) which corresponds to the 1^{st} order coefficients of $p(x)q(x)$ gives:

1^{st} order terms $= a[0]b[1] + b[1]a[0] = c[1]$

Looking at the 3^{rd} anti-diagonal (line from **b[3]** to **a[3]**) which corresponds to the 2^{nd} order coefficients of $p(x)q(x)$ gives:

2^{st} order terms $= a[0]b[2] + b[1]a[1] + b[2]a[0] = c[2]$

It is left as an exercise to the reader to confirm that higher order terms, and the zeroth order term matches that of the problem statement. For rigor, we give an algebraic proof below:

$p(x)q(x) = (a[0] + ... + a[d-1] \cdot x^{d-1})(b[0] + ... + b[m-1] \cdot x^{m-1}) = (\sum_{i=0}^{i=d-1} a[i]x^i)(\sum_{j=0}^{j=m-1} b[j]x^j) = \sum_{i=0}^{i=d-1}\sum_{j=0}^{j=m-1} a[i]x^i b[j]x^j = \sum_{i=0}^{i=d-1}\sum_{j=0}^{j=m-1} a[i]b[j]x^{i+j}$. Now, to simplify the problem, assume $i+j=n$ for some constant $n \in \mathbb{N}$. Then, the n^{th} order term of the product polynomial is $\sum_{i=0}^{i=d-1}\sum_{j=n-i} a[i]b[n-i]x^n = \sum_{i=1}^{i=d} a[i]b[n-i]x^n = (a[n] * b[n])x^n = c[n]x^n$ where we eliminated the sum $\sum_{j=n-i}$ because the summand doesn't depend on j. Note that $n \in \{0, m+d-2\}$. Thus, it follows that $p(x)q(x) = c[0] + c[1] \cdot x + ... + c[m+d-2] \cdot x^{m+d-2}$.

□

Lastly, the simplest interpretation of convolution is viewing it as a moving average of $b \in \mathbb{R}^m$, for the special case that our filter $a \in \mathbb{R}^d$ is a signal such that $\sum_{i=0}^{d-1} a[i] = 1$. For example, let $a = [\frac{1}{3}, \frac{1}{3}, \frac{1}{3}]$, b $= [0, 2, 5]$, and $c = a * b$. Then,

$$c = [\tfrac{1}{3}, \tfrac{1}{3}, \tfrac{1}{3}] * [0, 2, 5] = [(0 \times \tfrac{1}{3}), (0 \times \tfrac{1}{3} + 2 \times \tfrac{1}{3}), (0 \times \tfrac{1}{3} + 2 \times \tfrac{1}{3} + 5 \times \tfrac{1}{3}), (2 \times \tfrac{1}{3} + 5 \times \tfrac{1}{3}), (5 \times \tfrac{1}{3})] = [0, \tfrac{2}{3}, \tfrac{7}{3}, \tfrac{7}{3}, \tfrac{5}{3}].$$

Notice that we are taking the average of b in the small window defined by a as we slide it across b; starting from the intersection of $a[3]$ and $b[1]$, ending at the intersection of $a[1]$ and $b[3]$. As a sanity check, it is easy to confirm that $\sum_{i=0}^{2} b[i] = \sum_{i=0}^{4} c[i] =$ window length $\times$ average of $b = 7$.

1.3 Periodic Convolution

Definition 1.6 (Periodic Convolution). Suppose $\tilde{x}$ and $\tilde{h}$ are periodic signals with a period of N. The **periodic convolution** of $\tilde{x}$ with $\tilde{h}$, or $\tilde{y}$, is:

$$\tilde{y}[n] = \tilde{x}[n] \circledast \tilde{h}[n] := \sum_{k=0}^{k=N-1} \tilde{x}[k]\tilde{h}[n-k]$$

1.4 Circular Convolution

Definition 1.7 (Circular Convolution). Suppose x and h are signals of length N. The **circular convolution** of x with h, or y, is:

$$y[n] = x[n] \circ h[n] := \sum_{k=0}^{k=N-1} x[k]h[n-k]_{mod(N)}$$

for $n = 0, ..., N-1$

Notice that the definition for the circular convolution is a special case of the periodic convolution. Both formulations are nearly identical even though are formulated slightly differently. It is left as an exercise to the reader to confirm this. The challenge questions below provide an example where we compute a circular convolution.

1.5 Challenge Questions

1) How does circular convolution relate to linear convolution?

Answer.
To build intuition let's define $x[n] = \{1, 3, 2, -4, 6\}$ and $h[n] = \{5, 4, 3, 2, 1\}$. Let's compute the linear convolution defined by $y_l[n] = \sum_{k=-\infty}^{k=\infty} x[k]h[n-k]$

$h[n-k]\backslash x[k]$	$x[0]$	$x[1]$	$x[2]$	$x[3]$	$x[4]$
$h[0-k]$	$5\cdot 1$	0	0	0	0
$h[1-k]$	$4\cdot 1$	$5\cdot 3$	0	0	0
$h[2-k]$	$3\cdot 1$	$4\cdot 3$	$5\cdot 2$	0	0
$h[3-k]$	$2\cdot 1$	$3\cdot 3$	$4\cdot 2$	$5\cdot(-4)$	0
$h[4-k]$	$1\cdot 1$	$2\cdot 3$	$3\cdot 2$	$4\cdot(-4)$	$5\cdot 6$
$h[5-k]$	0	$1\cdot 3$	$2\cdot 2$	$3\cdot(-4)$	$4\cdot 6$
$h[6-k]$	0	0	$1\cdot 2$	$2\cdot(-4)$	$3\cdot 6$
$h[7-k]$	0	0	0	$1\cdot(-4)$	$2\cdot 5$

adding up the elements of the n^{th} row to compute $y_l[n]$ gives $y_l[n] = \{5, 19, 25, 1, 27, 19, 12, 8, 6\}$. Now let's compute the circular convolution defined by $y_c[n] = \sum_{k=-\infty}^{k=\infty} x[k]h[n-k]_{mod(N)}$

$h[n-k]\backslash x[k]$	$x[0]$	$x[1]$	$x[2]$	$x[3]$	$x[4]$
$h[0-k]$	$5\cdot 1$	$(1\cdot 3)$	$(2\cdot 2)$	$(3\cdot(-4))$	$(4\cdot 6)$
$h[1-k]$	$4\cdot 1$	$5\cdot 3$	$(1\cdot 2)$	$(2\cdot(-4))$	$(3\cdot 6)$
$h[2-k]$	$3\cdot 1$	$4\cdot 3$	$5\cdot 2$	$(1\cdot(-4))$	$(2\cdot 6)$
$h[3-k]$	$2\cdot 1$	$3\cdot 3$	$4\cdot 2$	$5\cdot(-4)$	$(1\cdot 6)$
$h[4-k]$	$1\cdot 1$	$2\cdot 3$	$3\cdot 2$	$4\cdot(-4)$	$5\cdot 6$

adding up the elements of the n^{th} row to compute $y_c[n]$ gives $y_c[n] = \{24, 31, 33, 5, 276\}$. Now, notice that both tables are very similar. In fact, the only difference in the circular convolution table are the new terms that are in parentheses. Upon a closer look, we notice that the new terms in the row labeled by $h[0-k]$ on the circular convolution table are the same as that in the row $h[5-k]$ on the linear convolution table. Then it follows that $y_c[0] = y_l[0] + y_l[5]$. Upon further examination it easy to deduce $y_c[n] = y_l[n] + y_l[n+5]$. Generalizing this, we have

$$y_c[n] = \sum_{m=-\infty}^{\infty} y_l[n+mN]$$

□

2) What can be done to ensure circular convolution result obtained using the DFT method matches the linear convolution result?

Answer. There must be enough samples of the DFT to obtain the linear convolution without corrupting it as the circular convolution length does not always match that of the linear convolution (due to the $mod(N)$ constraint). More precisely, both signals x and h need to be long enough to accommodate all samples of y_l without any overlaps. Given $x[n]$ and $h[n]$ with length N_x and N_h, $y_l[n] = x[n]*h[n]$ can be computed using the DFT method as follows:

1. length of y_l will be $N_y = N_x + N_h - 1$, so extend each signal using zero padding.

$$x_p[n] = \left\{ \begin{array}{ll} x[n], & \text{if } n = 0, ..., N_x - 1 \\ 0, & \text{if } n = N_x, .., N_y - 1 \end{array} \right\}$$

$$h_p[n] = \left\{ \begin{array}{ll} h[n], & \text{if } n = 0, ..., N_h - 1 \\ 0, & \text{if } n = N_h, .., N_y - 1 \end{array} \right\}$$

2. Compute DFTs of x_p and h_p

$X_p[k] = DFT\{x_p[n]\}$
$H_p[k] = DFT\{h_p[n]\}$

3. Multiply DFTs to obtain $Y_p[k]$

$Y_p[k] = X_p[k]H_p[k]$ (We assume that the reader knows the fact: $x[n] \circ h[n] \xleftrightarrow{DFT} X[k]H[k]$)

4. Compute IDFT

$y_p[n] = IDFT\{Y_p[k]\}$

The result is the same as the linear convolution. Namely, $y_p[n] = y_l[n]$ for $n = 0, ..., N_y - 1$ □