Appendix A

Some More Definitions, Theorems, Lemmas, and Corollaries

A.1 The Modulus Operator

Let $n \in Z$ then

$$n = pq + r \tag{A.1}$$

where p, q, $r \in Z$. We denote q the quotient of n divided by p and r is the remainder of that division. The q and r not uniquely determined from p and n but given p, n we speak of the uniquely equivalence class consisting of all values of r fulfilling (A.1) with $q \in Z$. However, one representative of this equivalence stands out. It is called the principal remainder and it is defined as

$$r = n \mod p = n - p\left[\frac{n}{p}\right] \tag{A.2}$$

where [.] denotes the nearest integer towards zero.

This is the way modulus is implemented in many programming languages such as Matlab. While mathematically correct, it has the inherent inconvenience that a negative r is chosen for $n < 0$. In many applications such as periodic convolution, we think of r as being the index of an array or a vector. Therefore, we wish to choose a representative where $r \in [0, p-1]$ for all $n \in Z$. This can be accomplished by defining

$$r = \langle n \rangle_p = n - p\left\lfloor\frac{n}{p}\right\rfloor \tag{A.3}$$

where $\lfloor n/p \rfloor$ denotes the nearest integer below n/p. We have introduced the notation $\langle n \rangle_p$ in order to avoid confusion, and we note that

$$\langle n \rangle_p = n \mod pforn > 0, p > 1. \tag{A.4}$$

For practical purpose $\langle n \rangle_p$ should not be implemented as in (A.2); rather, it should be written using the built-in modulus function modifying the result whenever needed.

Definition A.1.1 *Let n be given as in (A.1). If $r = 0$, we say that p is a divisor of n and we write*

$$p \mid n \tag{A.5}$$

It follows that for all p, q, n, $r \in \mathbf{Z}$, we have

$$p \mid (n - r) \tag{A.6}$$

and

$$q \mid (n - r) \tag{A.7}$$

Lemma A.1.1 *Let n_1, n_2, $q \in \mathbf{Z}$. Then*

$$\langle n_1 \pm n_2 \rangle_q = \langle n_1 \pm \langle n_2 \rangle_q \rangle_q \tag{A.8}$$

$$\langle n_1 n_2 \rangle_q = \langle n_1 \langle n_2 \rangle_q \rangle_q \tag{A.9}$$

Proof: See [Nie98].

Lemma A.1.2 *Let k, n, $q \in \mathbf{Z}$. Then*

$$k\langle n \rangle_q = \langle kn \rangle_{kq} \tag{A.10}$$

Proof: See [Nie98].

A.2 Moments of Scaling Functions

Consider the problem of computing the moments as given in (1.40):

$$M_l^p = \int_{-\infty}^{\infty} x^p \phi(x - l)dx, \quad l, p \in \mathbf{Z}. \tag{A.11}$$

By the normalization (1.11), we note first that

$$M_l^p = 1, \quad l \in \mathbf{Z}. \tag{A.12}$$

Let $l = 0$. The dilation equation (1.31) then yields

$$\begin{aligned} M_0^p &= \int_{-\infty}^{\infty} x^p \phi(x) dx \\ &= \sqrt{2} \sum_{k=0}^{D-1} a_k \int_{-\infty}^{\infty} x^p \phi(2x-k) dx \\ &= \frac{\sqrt{2}}{2^{p+1}} \sum_{k=0}^{D-1} a_k \int_{-\infty}^{\infty} y^p \phi(y-k) dy, \quad y = 2x \\ &= \frac{\sqrt{2}}{2^{p+1}} \sum_{k=0}^{D-1} a_k M_k^p. \end{aligned} \tag{A.13}$$

To reduce the number of unknowns in (A.13), we will eliminate M_k^p for $k \neq 0$. Using the variable transformation $y = x - l$ in (A.11), we get

$$\begin{aligned} M_l^p &= \int_{-\infty}^{\infty} (y+l)^p \phi(y) dy \\ &= \sum_{n=0}^{p} \binom{p}{n} l^{p-n} \int_{-\infty}^{\infty} y^n \phi(y) dy \end{aligned}$$

or

$$M_l^p = \sum_{n=0}^{p} \binom{p}{n} l^{p-n} M_0^n. \tag{A.14}$$

Substituting (A.14) into (A.13), we obtain

$$\begin{aligned} M_0^p &= \frac{\sqrt{2}}{2^{p+1}} \sum_{k=0}^{D-1} a_k \sum_{n=0}^{p} \binom{p}{n} k^{p-n} M_0^n \\ &= \frac{\sqrt{2}}{2^{p+1}} \sum_{n=0}^{p-1} \binom{p}{n} M_0^n \sum_{k=0}^{D-1} a_k k^{p-n} + \frac{\sqrt{2}}{2^{p+1}} M_0^p \sum_{k=0}^{D-1} a_k. \end{aligned}$$

Solving for M_0^p yields

$$M_0^p = \frac{\sqrt{2}}{2(2^p - 1)} \sum_{n=0}^{p-1} \binom{p}{n} M_0^n \sum_{k=0}^{D-1} a_k k^{p-n}. \tag{A.15}$$

Equation (A.15) can now be used to determine the p^{th} moment of $\phi(x)$, M_0^p for any $p > 0$. For $p = 0$, use (A.12). The translated moments M_l^p are then obtained from (A.14).

A.3 Circulant Matrices and the DFT

Definition A.3.1 ***Circulant Matrix:*** *Let* $\mathbf{A}$ *be an* $N \times N$ *matrix and let* $\mathbf{a} = [a_0, a_1, a_2, \cdots, a_{N-1}]^T$ *be the first column of* $\mathbf{A}$. *Then* $\mathbf{A}$ *is* ***circulant*** *if*

$$[\mathbf{A}]_{m,n} = a_{\langle m-n \rangle_N}, \quad m, n = 0, 1, \cdots, N-1.$$

Definition A.3.2 ***Discrete Convolution:*** *Let* $\mathbf{x} = [x_0, x_1, x_2, \cdots, x_{N-1}]^T$ *and define* $\mathbf{y}$ *and* $\mathbf{z}$ *similarly. Then*

$$\mathbf{z} = \mathbf{x} * \mathbf{y}$$

is the (cyclic) convolution defined by

$$z_m = \sum_{n=0}^{N-1} x_n y_{\langle m-n \rangle_N}, \quad m = 0, 1, 2, \cdots, N-1. \tag{A.16}$$

Definition A.3.3 ***Discrete Fourier Transform:*** *Let* $\{x_l\}_{l=0}^{N-1}$ *be a sequence of* N *complex numbers. The sequence* $\{\hat{x}_k\}_{k=0}^{N-1}$ *defined by*

$$\hat{x}_k = \sum_{l=0}^{N-1} x_l \omega_N^{-kl}, \quad k = 0, 1, 2, \cdots, N-1, \tag{A.17}$$

where $\omega_N = e^{i2\pi/N}$, *is the discrete Fourier transform of* $\{x_l\}_{l=0}^{N-1}$.

Definition A.3.4 ***Inverse Discrete Fourier Transform:*** *Let* $\{x_l\}_{l=0}^{N-1}$ *and* $\{\hat{x}_k\}_{k=0}^{N-1}$ *be given as in Definition A.3.3. Then the discrete Fourier transform (IDFT) is defined by*

$$x_l = \frac{1}{N} \sum_{k=0}^{N-1} \hat{x}_k \omega_N^{kl}, \quad l = 0, 1, 2, \cdots, N-1. \tag{A.18}$$

Both the DFT and the IDFT can be computed in $O(N \log_2 N)$ steps using the fast Fourier transform algorithm (FFT). The link between DFT and convolution is embodied in the **convolution theorem**, which we state as follows:

Theorem A.3.1 ***Convolution Theorem:***

$$\mathbf{z} = \mathbf{x} * \mathbf{y} \Leftrightarrow \hat{\mathbf{z}} = diag\ (\hat{\mathbf{x}})\hat{\mathbf{y}}.$$

Proof: See [Nie98].

Corollary A.3.2

$$\mathbf{x} * \mathbf{y} = \mathbf{y} * \mathbf{x}.$$

Proof: See [Nie98].

Lemma A.3.3 *Let* A *and* **a** *be defined as in Definition A.3.1 and* $\mathbf{x} \in R^N$ *then*

$$\mathbf{Ax} = \mathbf{a} * \mathbf{x}$$

Proof: See [Nie98].

Theorem A.3.4 **A** *is circulant* $\Leftrightarrow \mathbf{A} = \mathbf{F}_N^{-1} \mathbf{\Lambda}_a \mathbf{F}_N,\ \mathbf{\Lambda}_a = diag(\hat{\mathbf{a}})$.

Proof: See [Nie98].

Theorem A.3.5 *Circulant matrices with the same dimensions commute.*

Proof: See [Nie98].

Theorem A.3.6 **A** *is circulant* $\Leftrightarrow \mathbf{A}^{-1}$ *is circulant.*

Proof: See [Nie98].