1.3.2.7.4. *Matrix representation of the discrete Fourier transform (DFT)*

By virtue of definitions (i) and (ii),

$$\mathscr{F}(\mathbf{N})\mathbf{v}_{k^*} = \frac{1}{|\det \mathbf{N}|}\sum_{k} \exp[-2\pi i k^* \cdot (\mathbf{N}^{-1}k)]\mathbf{u}_k$$
$$\bar{\mathscr{F}}(\mathbf{N})\mathbf{u}_k = \sum_{k^*} \exp[+2\pi i k^* \cdot (\mathbf{N}^{-1}k)]\mathbf{v}_{k^*}$$

so that $\mathscr{F}(\mathbf{N})$ and $\bar{\mathscr{F}}(\mathbf{N})$ may be represented, in the canonical bases of $W_{\mathbf{N}}$ and $W^*_{\mathbf{N}}$, by the following matrices:

$$[\mathscr{F}(\mathbf{N})]_{kk^*} = \frac{1}{|\det \mathbf{N}|}\exp[-2\pi i k^* \cdot (\mathbf{N}^{-1}k)]$$
$$[\bar{\mathscr{F}}(\mathbf{N})]_{k^*k} = \exp[+2\pi i k^* \cdot (\mathbf{N}^{-1}k)].$$

When $\mathbf{N}$ is symmetric, $\mathbb{Z}^n/\mathbf{N}\mathbb{Z}^n$ and $\mathbb{Z}^n/\mathbf{N}^T\mathbb{Z}^n$ may be identified in a natural manner, and the above matrices are symmetric.

When $\mathbf{N}$ is diagonal, say $\mathbf{N} = \mathrm{diag}(\nu_1, \nu_2, \ldots, \nu_n)$, then the tensor product structure of the full multidimensional Fourier transform (Section 1.3.2.4.2.4)

$$\mathscr{F}_{\mathbf{x}} = \mathscr{F}_{x_1} \otimes \mathscr{F}_{x_2} \otimes \ldots \otimes \mathscr{F}_{x_n}$$

gives rise to a tensor product structure for the DFT matrices. The tensor product of matrices is defined as follows:

$$\mathbf{A} \otimes \mathbf{B} = \begin{pmatrix} a_{11}\mathbf{B} & \ldots & a_{1n}\mathbf{B} \\ \vdots & & \vdots \\ a_{n1}\mathbf{B} & \ldots & a_{nn}\mathbf{B} \end{pmatrix}.$$

Let the index vectors k and k^* be ordered in the same way as the elements in a Fortran array, *e.g.* for k with k_1 increasing fastest, k_2 next fastest, $\ldots, k_n$ slowest; then

$$\mathscr{F}(\mathbf{N}) = \mathscr{F}(\nu_1) \otimes \mathscr{F}(\nu_2) \otimes \ldots \otimes \mathscr{F}(\nu_n),$$

where

$$[\mathscr{F}(\nu_j)]_{k_j, k_j^*} = \frac{1}{\nu_j}\exp\left(-2\pi i \frac{k_j^* k_j}{\nu_j}\right),$$

and

$$\bar{\mathscr{F}}(\mathbf{N}) = \bar{\mathscr{F}}(\nu_1) \otimes \bar{\mathscr{F}}(\nu_2) \otimes \ldots \otimes \bar{\mathscr{F}}(\nu_n),$$

where

$$[\bar{\mathscr{F}}_{\nu_j}]_{k_j^*, k_j} = \exp\left(+2\pi i \frac{k_j^* k_j}{\nu_j}\right).$$

1.3.2.7.5. *Properties of the discrete Fourier transform*

The DFT inherits most of the properties of the Fourier transforms, but with certain numerical factors ('Jacobians') due to the transition from continuous to discrete measure.

(1) *Linearity* is obvious.

(2) *Shift property*. If $(\tau_a \psi)(k) = \psi(k - a)$ and $(\tau_{a^*}\Psi)(k^*) = \Psi(k^* - a^*)$, where subtraction takes place by modular vector arithmetic in $\mathbb{Z}^n/\mathbf{N}\mathbb{Z}^n$ and $\mathbb{Z}^n/\mathbf{N}^T\mathbb{Z}^n$, respectively, then the following identities hold:

$$\bar{\mathscr{F}}(\mathbf{N})[\tau_k \psi](k^*) = \exp[+2\pi i k^* \cdot (\mathbf{N}^{-1}k)]\bar{\mathscr{F}}(\mathbf{N})[\psi](k^*)$$
$$\mathscr{F}(\mathbf{N})[\tau_{k^*}\Psi](k) = \exp[-2\pi i k^* \cdot (\mathbf{N}^{-1}k)]\mathscr{F}(\mathbf{N})[\Psi](k).$$

(3) *Differentiation identities*. Let vectors $\boldsymbol{\psi}$ and $\boldsymbol{\Psi}$ be constructed from $\varphi^0 \in \mathscr{E}(\mathbb{R}^n)$ as in Section 1.3.2.7.3, hence be related by the DFT. If $D^{\mathbf{p}}\boldsymbol{\psi}$ designates the vector of sample values of $D^{\mathbf{p}}_{\mathbf{x}}\varphi^0$ at the points of $\Lambda_{\mathbf{B}}/\Lambda_{\mathbf{A}}$, and $D^{\mathbf{p}}\boldsymbol{\Psi}$ the vector of values of $D^{\mathbf{p}}_{\boldsymbol{\xi}}\Phi^0$ at points of $\Lambda^*_{\mathbf{A}}/\Lambda^*_{\mathbf{B}}$, then for all multi-indices $\mathbf{p} = (p_1, p_2, \ldots, p_n)$

$$(D^{\mathbf{p}}\boldsymbol{\psi})(k) = \bar{\mathscr{F}}(\mathbf{N})[(+2\pi i k^*)^{\mathbf{p}}\boldsymbol{\Psi}](k)$$
$$(D^{\mathbf{p}}\boldsymbol{\Psi})(k^*) = \mathscr{F}(\mathbf{N})[(-2\pi i k)^{\mathbf{p}}\boldsymbol{\psi}](k^*)$$

or equivalently

$$\mathscr{F}(\mathbf{N})[D^{\mathbf{p}}\boldsymbol{\psi}](k^*) = (+2\pi i k^*)^{\mathbf{p}}\boldsymbol{\Psi}(k^*)$$
$$\bar{\mathscr{F}}(\mathbf{N})[D^{\mathbf{p}}\boldsymbol{\Psi}](k) = (-2\pi i k)^{\mathbf{p}}\boldsymbol{\psi}(k).$$

(4) *Convolution property*. Let $\boldsymbol{\varphi} \in W_{\mathbf{N}}$ and $\boldsymbol{\Phi} \in W^*_{\mathbf{N}}$ (respectively $\boldsymbol{\psi}$ and $\boldsymbol{\Psi}$) be related by the DFT, and define

$$(\boldsymbol{\varphi} * \boldsymbol{\psi})(k) = \sum_{k' \in \mathbb{Z}^n/\mathbf{N}\mathbb{Z}^n} \boldsymbol{\varphi}(k')\boldsymbol{\psi}(k - k')$$
$$(\boldsymbol{\Phi} * \boldsymbol{\Psi})(k^*) = \sum_{k^{*\prime} \in \mathbb{Z}^n/\mathbf{N}^T\mathbb{Z}^n} \boldsymbol{\Phi}(k^{*\prime})\boldsymbol{\Psi}(k^* - k^{*\prime}).$$

Then

$$\bar{\mathscr{F}}(\mathbf{N})[\boldsymbol{\Phi} * \boldsymbol{\Psi}](k) = |\det \mathbf{N}|\boldsymbol{\varphi}(k)\boldsymbol{\psi}(k)$$
$$\mathscr{F}(\mathbf{N})[\boldsymbol{\varphi} * \boldsymbol{\psi}](k^*) = \boldsymbol{\Phi}(k^*)\boldsymbol{\Psi}(k^*)$$

and

$$\bar{\mathscr{F}}(\mathbf{N})[\boldsymbol{\varphi} \times \boldsymbol{\psi}](k^*) = \frac{1}{|\det \mathbf{N}|}(\boldsymbol{\Phi} * \boldsymbol{\Psi})(k^*)$$
$$\mathscr{F}(\mathbf{N})[\boldsymbol{\Phi} \times \boldsymbol{\Psi}](k) = (\boldsymbol{\varphi} * \boldsymbol{\psi})(k).$$

Since addition on $\mathbb{Z}^n/\mathbf{N}\mathbb{Z}^n$ and $\mathbb{Z}^n/\mathbf{N}^T\mathbb{Z}^n$ is modular, this type of convolution is called *cyclic* convolution.

(5) *Parseval/Plancherel property*. If $\boldsymbol{\varphi}$, $\boldsymbol{\psi}$, $\boldsymbol{\Phi}$, $\boldsymbol{\Psi}$ are as above, then

$$(\mathscr{F}(\mathbf{N})[\boldsymbol{\Phi}], \mathscr{F}(\mathbf{N})[\boldsymbol{\Psi}])_W = \frac{1}{|\det \mathbf{N}|}(\boldsymbol{\Phi}, \boldsymbol{\Psi})_{W^*}$$
$$(\bar{\mathscr{F}}(\mathbf{N})[\boldsymbol{\varphi}], \bar{\mathscr{F}}(\mathbf{N})[\boldsymbol{\psi}])_W = \frac{1}{|\det \mathbf{N}|}(\boldsymbol{\varphi}, \boldsymbol{\psi})_W.$$

(6) *Period* 4. When $\mathbf{N}$ is symmetric, so that the ranges of indices k and k^* can be identified, it makes sense to speak of powers of $\mathscr{F}(\mathbf{N})$ and $\bar{\mathscr{F}}(\mathbf{N})$. Then the 'standardized' matrices $(1/|\det \mathbf{N}|^{1/2})\mathscr{F}(\mathbf{N})$ and $(1/|\det \mathbf{N}|^{1/2})\bar{\mathscr{F}}(\mathbf{N})$ are *unitary* matrices whose fourth power is the identity matrix (Section 1.3.2.4.3.4); their eigenvalues are therefore ± 1 and $\pm i$.

1.3.3. Numerical computation of the discrete Fourier transform

1.3.3.1. *Introduction*

The Fourier transformation's most remarkable property is undoubtedly that of turning convolution into multiplication. As distribution theory has shown, other valuable properties – such as the shift property, the conversion of differentiation into multiplication by monomials, and the duality between periodicity and sampling – are special instances of the convolution theorem.

This property is exploited in many areas of applied mathematics and engineering (Campbell & Foster, 1948; Sneddon, 1951; Champeney, 1973; Bracewell, 1986). For example, the passing of a signal through a linear filter, which results in its being convolved with the response of the filter to a δ-function 'impulse', may be modelled as a multiplication of the signal's transform by the transform of the impulse response (also called transfer function). Similarly, the solution of systems of partial differential equations may be turned by Fourier transformation into a division problem for distributions. In both cases, the formulations obtained after Fourier transformation are considerably simpler than the initial ones, and lend themselves to constructive solution techniques.

Whenever the functions to which the Fourier transform is applied are band-limited, or can be well approximated by band-limited functions, the discrete Fourier transform (DFT) provides a means of constructing explicit numerical solutions to the problems at hand. A great variety of investigations in physics, engineering and applied mathematics thus lead to DFT calculations, to such a degree that, at the time of writing, about 50% of all supercomputer CPU time is alleged to be spent calculating DFTs.

The straightforward use of the defining formulae for the DFT leads to calculations of size N^2 for N sample points, which become unfeasible for any but the smallest problems. Much ingenuity has therefore been exerted on the design and implementation of faster algorithms for calculating the DFT (McClellan & Rader, 1979; Nussbaumer, 1981; Blahut, 1985; Brigham, 1988). The most famous is that of Cooley & Tukey (1965) which heralded the age of digital signal processing. However, it had been preceded by the prime factor algorithm of Good (1958, 1960), which has lately been the basis of many new developments. Recent historical research (Goldstine, 1977, pp. 249–253; Heideman *et al.*, 1984) has shown that Gauss essentially knew the Cooley–Tukey algorithm as early as 1805 (before Fourier's 1807 work on harmonic analysis!); while it has long been clear that Dirichlet knew of the basis of the prime factor algorithm and used it extensively in his theory of multiplicative characters [see *e.g.* Chapter I of Ayoub (1963), and Chapters 6 and 8 of Apostol (1976)]. Thus the computation of the DFT, far from being a purely technical and rather narrow piece of specialized numerical analysis, turns out to have very rich connections with such central areas of pure mathematics as number theory (algebraic and analytic), the representation theory of certain Lie groups and coding theory – to list only a few. The interested reader may consult Auslander & Tolimieri (1979); Auslander, Feig & Winograd (1982, 1984); Auslander & Tolimieri (1985); Tolimieri (1985).

One-dimensional algorithms are examined first. The Sande mixed-radix version of the Cooley–Tukey algorithm only calls upon the additive structure of congruence classes of integers. The prime factor algorithm of Good begins to exploit some of their multiplicative structure, and the use of relatively prime factors leads to a stronger factorization than that of Sande. Fuller use of the multiplicative structure, *via* the group of units, leads to the Rader algorithm; and the factorization of short convolutions then yields the Winograd algorithms.

Multidimensional algorithms are at first built as tensor products of one-dimensional elements. The problem of factoring the DFT in several dimensions simultaneously is then examined. The section ends with a survey of attempts at formalizing the interplay between algorithm structure and computer architecture for the purpose of automating the design of optimal DFT code.

It was originally intended to incorporate into this section a survey of all the basic notions and results of abstract algebra which are called upon in the course of these developments, but time limitations have made this impossible. This material, however, is adequately covered by the first chapter of Tolimieri *et al.* (1989) in a form tailored for the same purposes. Similarly, the inclusion of numerous detailed examples of the algorithms described here has had to be postponed to a later edition, but an abundant supply of such examples may be found in the signal processing literature, for instance in the books by McClellan & Rader (1979), Blahut (1985), and Tolimieri *et al.* (1989).

1.3.3.2. *One-dimensional algorithms*

Throughout this section we will denote by $e(t)$ the expression $\exp(2\pi i t)$, $t \in \mathbb{R}$. The mapping $t \longmapsto e(t)$ has the following properties:

$$\begin{aligned} e(t_1 + t_2) &= e(t_1)e(t_2) \\ e(-t) &= \overline{e(t)} = [e(t)]^{-1} \\ e(t) &= 1 \Leftrightarrow t \in \mathbb{Z}. \end{aligned}$$

Thus e defines an isomorphism between the additive group $\mathbb{R}/\mathbb{Z}$ (the reals modulo the integers) and the multiplicative group of complex numbers of modulus 1. It follows that the mapping $\ell \longmapsto e(\ell/N)$, where $\ell \in \mathbb{Z}$ and N is a positive integer, defines an isomorphism between the one-dimensional residual lattice $\mathbb{Z}/N\mathbb{Z}$ and the multiplicative group of Nth roots of unity.

The DFT on N points then relates vectors $\mathbf{X}$ and $\mathbf{X}^*$ in W and W^* through the linear transformations:

$$\begin{aligned} F(N): \quad & X(k) = \frac{1}{N} \sum_{k^* \in \mathbb{Z}/N\mathbb{Z}} X^*(k^*) e(-k^* k/N) \\ \bar{F}(N): \quad & X^*(k^*) = \sum_{k \in \mathbb{Z}/N\mathbb{Z}} X(k) e(k^* k/N). \end{aligned}$$

1.3.3.2.1. *The Cooley–Tukey algorithm*

The presentation of Gentleman & Sande (1966) will be followed first [see also Cochran *et al.* (1967)]. It will then be reinterpreted in geometric terms which will prepare the way for the treatment of multidimensional transforms in Section 1.3.3.3.

Suppose that the number of sample points N is composite, say $N = N_1 N_2$. We may write k to the base N_1 and k^* to the base N_2 as follows:

$$\begin{aligned} k &= k_1 + N_1 k_2 \quad k_1 \in \mathbb{Z}/N_1\mathbb{Z}, \quad k_2 \in \mathbb{Z}/N_2\mathbb{Z} \\ k^* &= k_2^* + k_1^* N_2 \quad k_1^* \in \mathbb{Z}/N_1\mathbb{Z}, \quad k_2^* \in \mathbb{Z}/N_2\mathbb{Z}. \end{aligned}$$

The defining relation for $\bar{F}(N)$ may then be written:

$$\begin{aligned} X^*(k_2^* + k_1^* N_2) = \sum_{k_1 \in \mathbb{Z}/N_1\mathbb{Z}} \sum_{k_2 \in \mathbb{Z}/N_2\mathbb{Z}} & X(k_1 + N_1 k_2) \\ & \times e\left[\frac{(k_2^* + k_1^* N_2)(k_1 + N_1 k_2)}{N_1 N_2}\right]. \end{aligned}$$

The argument of $e[.]$ may be expanded as

$$\frac{k_2^* k_1}{N} + \frac{k_1^* k_1}{N_1} + \frac{k_2^* k_2}{N_2} + k_1^* k_2,$$

and the last summand, being an integer, may be dropped:

$$\begin{aligned} & X^*(k_2^* + k_1^* N_2) \\ & \quad = \sum_{k_1} \left\{ e\left(\frac{k_2^* k_1}{N}\right) \left[\sum_{k_2} X(k_1 + N_1 k_2) e\left(\frac{k_2^* k_2}{N_2}\right) \right] \right\} \\ & \qquad \times e\left(\frac{k_1^* k_1}{N_1}\right). \end{aligned}$$

This computation may be decomposed into five stages, as follows:

(i) form the N_1 vectors $\mathbf{Y}_{k_1}$ of length N_2 by the prescription

$$Y_{k_1}(k_2) = X(k_1 + N_1 k_2), \quad k_1 \in \mathbb{Z}/N_1\mathbb{Z}, \quad k_2 \in \mathbb{Z}/N_2\mathbb{Z};$$

(ii) calculate the N_1 transforms $\mathbf{Y}_{k_1}^*$ on N_2 points:

$$\mathbf{Y}_{k_1}^* = \bar{F}(N_2)[\mathbf{Y}_{k_1}], \quad k_1 \in \mathbb{Z}/N_1\mathbb{Z};$$

(iii) form the N_2 vectors $\mathbf{Z}_{k_2^*}$ of length N_1 by the prescription

$$\mathbf{Z}_{k_2^*}(k_1) = e\left(\frac{k_2^* k_1}{N}\right) Y_{k_1}^*(k_2^*), \quad k_1 \in \mathbb{Z}/N_1\mathbb{Z}, \quad k_2^* \in \mathbb{Z}/N_2\mathbb{Z};$$

references