

Finite Fourier Transform, Circulant Matrices, and the Fast Fourier Transform

Roe Goodman

Supplementary Class Notes for Math 642:550 Linear Algebra and Applications
Rutgers, The State University of New Jersey

Revised October 30, 2007

1 Inner Products and Unitary Transformations

The formula defining the usual inner product and norm on \mathbb{R}^n needs to be modified when we define an inner product on \mathbb{C}^n . For a nonzero real number x we always have $x^2 > 0$. But this is not true for complex numbers, since $i^2 = -1$. The way around this difficulty is to use the fact that $\bar{z}z > 0$ if z is a nonzero complex number. Thus we define the *standard inner product* on \mathbb{C}^n to be

$$\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{k=1}^n u_k \bar{v}_k \quad \text{for } \mathbf{u}, \mathbf{v} \in \mathbb{C}^n.$$

Just as in the real case we can write the inner product in terms of matrix multiplication of a row vector ($1 \times n$ matrix) and a column vector ($n \times 1$ matrix). For this we define the *Hermitian transpose* $\mathbf{v}^H = \bar{\mathbf{v}}^T$. Likewise, if A is an $m \times n$ matrix, we write $A^H = \bar{A}^T$. (Note that in MATLAB all matrices are automatically assumed to have complex entries, and A' gives the Hermitian transpose of a matrix A .) Then we can express

$$\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{v}^H \mathbf{u} \quad \text{for } \mathbf{u}, \mathbf{v} \in \mathbb{C}^n.$$

With this definition we have

$$\langle \mathbf{u}, \mathbf{u} \rangle = \sum_{k=1}^n |u_k|^2 = \mathbf{u}^H \mathbf{u},$$

which is positive (unless $\mathbf{u} = 0$, when it is zero). Thus we can define the *norm* $\|\mathbf{u}\| = \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle}$ which measures the total size of a vector with complex components.

Definition 1.1. Let V be a complex vector space. An *inner product* on V is a complex-valued function $\langle \mathbf{u}, \mathbf{v} \rangle$ defined for all $\mathbf{u}, \mathbf{v} \in V$ that satisfies the following conditions:

(Positivity) $\langle \mathbf{u}, \mathbf{u} \rangle \geq 0$ with equality if and only if $\mathbf{u} = 0$.

(Conjugate Symmetry) $\langle \mathbf{u}, \mathbf{v} \rangle = \overline{\langle \mathbf{v}, \mathbf{u} \rangle}$.

(Linearity) $\langle \alpha \mathbf{u} + \beta \mathbf{v}, \mathbf{w} \rangle = \alpha \langle \mathbf{u}, \mathbf{w} \rangle + \beta \langle \mathbf{v}, \mathbf{w} \rangle$ for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ and complex numbers α and β . ■

When $V = \mathbb{C}^n$ then the standard inner product defined above satisfies these conditions. Here is another important example.

Example 1.2. Consider the complex vector space V of all complex-valued continuous functions on a finite interval $[a, b]$. Let $w(x)$ be any continuous function on $[a, b]$ that is strictly positive. (For example, $w(x) = (1 + x^2)^p$ for some fixed real number p .) Given two functions f and g in V , define

$$\langle f, g \rangle = \int_a^b f(x) \overline{g(x)} w(x) dx. \quad (1)$$

To verify that this is an inner product, note that $f(x) \overline{f(x)} \geq 0$, so we have $\langle f, f \rangle \geq 0$. If $\langle f, f \rangle = 0$ then $f(x) = 0$ for all $a \leq x \leq b$, since the function $|f(x)|^2 \geq 0$. The conjugate symmetry and linearity are obvious. ■

Let V be a complex vector space with a fixed inner product. The *norm* associated with an inner product is $\|\mathbf{u}\| = \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle}$, just as in the case of \mathbb{C}^n . Two vectors \mathbf{u} and \mathbf{v} are called *orthogonal* if $\langle \mathbf{u}, \mathbf{v} \rangle = 0$, and we write $\mathbf{u} \perp \mathbf{v}$. For orthogonal vectors we have the *Pythagorean Law* (complex version):

$$\|\mathbf{u} + \mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 \quad \text{when } \mathbf{u} \perp \mathbf{v}$$

with the same proof as in the real case. For any pair of vectors \mathbf{u}, \mathbf{v} with $\mathbf{v} \neq 0$, the *vector projection* of \mathbf{u} onto \mathbf{v} is given by

$$\mathbf{p} = \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\langle \mathbf{v}, \mathbf{v} \rangle} \mathbf{v}$$

just as in the real case. Since $(\mathbf{u} - \mathbf{p}) \perp \mathbf{p}$ and $\mathbf{u} = (\mathbf{u} - \mathbf{p}) + \mathbf{p}$, the Pythagorean Law gives

$$\|\mathbf{u}\|^2 = \|\mathbf{u} - \mathbf{p}\|^2 + \|\mathbf{p}\|^2.$$

Using this equation we obtain the *Cauchy-Schwarz inequality*

$$|\langle \mathbf{u}, \mathbf{v} \rangle| \leq \|\mathbf{u}\| \|\mathbf{v}\| \quad (2)$$

From the Cauchy-Schwarz inequality we obtain the *triangle inequality*

$$\|\mathbf{u} + \mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\| \quad \text{for all vectors } \mathbf{u}, \mathbf{v} \in V.$$

Definition 1.3. A set of nonzero vectors $\mathbf{v}_1, \mathbf{v}_2, \dots$, in an inner product space V is called *orthogonal* if $\mathbf{v}_j \perp \mathbf{v}_k$ for all $j \neq k$. If the set is orthogonal and each vector satisfies $\|\mathbf{v}_j\| = 1$ then the set is called *orthonormal*. ■

An orthonormal set of vectors is always linearly independent. Assume that $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ is a finite orthonormal set. Let U be the subspace of V spanned by this set of vectors. Then $\dim U = n$ and $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ is an *orthonormal basis* for U . Every vector $\mathbf{u} \in U$ can be expressed in terms of this basis as

$$\mathbf{u} = c_1 \mathbf{u}_1 + \dots + c_n \mathbf{u}_n, \quad \text{where } c_j = \langle \mathbf{u}, \mathbf{u}_j \rangle.$$

(The formula for the coefficient c_j follows by taking the inner product of \mathbf{u} with \mathbf{u}_j and using orthonormality.)

Then

$$\|\mathbf{u}\|^2 = |c_1|^2 + \dots + |c_n|^2 \quad (\text{Parseval's Formula})$$

If $\mathbf{v} = d_1 \mathbf{u}_1 + \dots + d_n \mathbf{u}_n$ is another vector in U , then

$$\langle \mathbf{u}, \mathbf{v} \rangle = c_1 \bar{d}_1 + \dots + c_n \bar{d}_n$$

For any vector $\mathbf{v} \in V$ we define

$$P\mathbf{v} = \langle \mathbf{v}, \mathbf{u}_1 \rangle \mathbf{u}_1 + \dots + \langle \mathbf{v}, \mathbf{u}_n \rangle \mathbf{u}_n.$$

Then $P\mathbf{v} \in U$, since it is a linear combination of the vectors \mathbf{u}_k . Furthermore, $\mathbf{v} - P\mathbf{v} \perp U$ since

$$\begin{aligned}\langle \mathbf{v} - P\mathbf{v}, \mathbf{u}_j \rangle &= \langle \mathbf{v}, \mathbf{u}_j \rangle - \sum_{k=1}^n \langle \mathbf{v}, \mathbf{u}_k \rangle \langle \mathbf{u}_k, \mathbf{u}_j \rangle \\ &= \langle \mathbf{v}, \mathbf{u}_j \rangle - \langle \mathbf{v}, \mathbf{u}_j \rangle \langle \mathbf{u}_j, \mathbf{u}_j \rangle = 0\end{aligned}$$

by orthogonality and the fact that $\|\mathbf{u}_j\| = 1$. We call $P\mathbf{v}$ the *orthogonal projection of \mathbf{v} onto the subspace U* . By the Pythagorean Law,

$$\|\mathbf{v}\|^2 = \|P\mathbf{v}\|^2 + \|\mathbf{v} - P\mathbf{v}\|^2 \quad (3)$$

This implies that $P\mathbf{v}$ is the vector in U that is closest to \mathbf{v} .

Example 1.4 (Fourier Series). Let V be the complex vector space of piecewise continuous complex-valued functions $f(x)$ on the interval $0 \leq x \leq 2\pi$. Define an inner product on V by

$$\langle f, g \rangle = \frac{1}{2\pi} \int_0^{2\pi} f(x) \overline{g(x)} dx.$$

The functions $\phi_n(x) = e^{inx}$ for $n \in \mathbb{Z}$ (the set of all integers) are in V , and they are an orthonormal set of functions. To see this, let $k \neq n$ and calculate

$$\langle \phi_n, \phi_k \rangle = \frac{1}{2\pi} \int_0^{2\pi} e^{i(n-k)x} dx = \frac{e^{i(n-k)x}}{2\pi i(n-k)} \Big|_{x=0}^{x=2\pi} = 0$$

because $e^{2m\pi i} = 1$ for all integers m . Thus $\phi_n \perp \phi_k$. Furthermore, since $e^0 = 1$, we have

$$\langle \phi_n, \phi_n \rangle = \frac{1}{2\pi} \int_0^{2\pi} 1 dx = 1$$

Thus $\|\phi_n\| = 1$ and $\{\phi_k : k \in \mathbb{Z}\}$ is an orthonormal set in V .

If $f \in V$ then the complex numbers

$$c_k = \langle f, \phi_k \rangle = \frac{1}{2\pi} \int_0^{2\pi} f(x) e^{-ikx} dx \quad (4)$$

are called the *Fourier coefficients* of f . It is an important result of Fourier analysis that f can be represented by its *Fourier series*:

$$f = \sum_{k \in \mathbb{Z}} c_k \phi_k \quad (5)$$

This is analogous to the representation of a vector in \mathbb{C}^n in terms of an orthonormal basis for \mathbb{C}^n (since $c_k = \langle f, \phi_k \rangle$). Furthermore, the *infinite series* version of Parseval's formula is valid:

$$\frac{1}{2\pi} \int_0^{2\pi} |f(x)|^2 dx = \sum_{k \in \mathbb{Z}} |c_k|^2 \quad (6)$$

In particular, the infinite series on the right side of (6) converges. (The convergence properties of the series (5) and the proof of (6) require results from advanced calculus that will not be discussed in this course).

Let \mathcal{TP}_n be the linear span of the set of functions $\{\phi_k(x) : |k| \leq n\}$. If $f(x) \in \mathcal{TP}_n$ then $c_k = 0$ for $|k| > n$ and the right side of (5) is a *trigonometric polynomial*

$$f(x) = \sum_{-n \leq k \leq n} c_k \phi_k(x)$$

When $f(x)$ is real-valued its Fourier coefficients c_k have the property

$$\overline{c_k} = c_{-k},$$

since $\overline{\phi_k(x)} = \phi_{-k}(x)$. For example, the formulas

$$\sin(nx) = \frac{1}{2i}e^{nix} - \frac{1}{2i}e^{-nix}, \quad \cos(nx) = \frac{1}{2}e^{nix} + \frac{1}{2}e^{-nix}$$

show that the real-valued functions $f_n(x) = \sin(nx)$ and $g_n(x) = \cos(nx)$ are in \mathcal{TP}_n and have Fourier series

$$f_n(x) = \frac{1}{2i}\phi_n(x) - \frac{1}{2i}\phi_{-n}(x), \quad g_n(x) = \frac{1}{2}\phi_n(x) + \frac{1}{2}\phi_{-n}(x) \quad (7)$$

For any function $f \in V$ and positive integer n , the trigonometric polynomial

$$\psi_n(x) = \sum_{-n \leq k \leq n} \langle f, \phi_k \rangle \phi_k(x)$$

is the projection of $f(x)$ onto the subspace \mathcal{TP}_n , since $\{\phi_k(x) : -n \leq k \leq n\}$ is an orthonormal basis for \mathcal{TP}_n . The function $\psi_n(x)$ gives the *best approximation* to $f(x)$ (in the sense of the norm $\|\cdot\|$), since we minimize the norm $\|f - \psi\|$, where ψ is a trigonometric polynomial in \mathcal{TP}_n , by taking $\psi = \psi_n$. ■

Definition 1.5. An $n \times n$ matrix U is said to be a *unitary matrix* if the set $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ of columns of U is orthonormal. ■

The matrix U is unitary if and only if

$$\langle U\mathbf{v}, U\mathbf{w} \rangle = \langle \mathbf{v}, \mathbf{w} \rangle \quad \text{for all } \mathbf{v}, \mathbf{w} \in \mathbb{C}^n. \quad (8)$$

To prove this, use the linearity of the inner product in each variable to see that (8) is satisfied for all vectors \mathbf{v}, \mathbf{w} if and only if it is satisfied when $\mathbf{v} = \mathbf{e}_j$ and $\mathbf{w} = \mathbf{e}_k$ (the standard basis vectors for \mathbb{C}^n). Since the j th column of U is $U\mathbf{e}_j$ and the set $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ is orthonormal, it follows that (8) is equivalent to the statement that the columns of U are an orthonormal set.

An alternate characterization of unitary matrices is that $U^H U = I$, where U^H denotes the conjugate transpose matrix (the proof is the same as for real orthogonal matrices). Hence a unitary matrix is invertible, with inverse $U^{-1} = U^H$.

Now let V and W be finite-dimensional complex inner product spaces of the same dimension, and let T be a linear transformation from V to W . We say that T is a *unitary transformation* if

$$\langle T\mathbf{u}, T\mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle \quad \text{for all vectors } \mathbf{u}, \mathbf{v} \in V. \quad (9)$$

Note that in equation (9) the inner product on the left is for the space W , while the inner product on the right is for the space V . Taking $\mathbf{u} = \mathbf{v}$, we see that $\|T\mathbf{u}\| = \|\mathbf{u}\|$ for all \mathbf{u} . Hence the null space of T is 0. Since V and W have the same dimension, T is represented by a square matrix (relative to a choice of bases for V and W). This matrix has no null space, so it is invertible. Thus every unitary transformation is invertible.

Example 1.6. Let $V = W = \mathbb{C}^n$, and let the linear transformation T have matrix

$$U = [\mathbf{u}_1, \dots, \mathbf{u}_n]$$

relative to the standard basis $\mathbf{e}_1, \dots, \mathbf{e}_n$ of \mathbb{C}^n (where \mathbf{e}_j has 1 in the j th entry and zero elsewhere). Since the standard basis is orthonormal, we see from (9) that T is a unitary transformation if and only if U is a unitary matrix. ■

Example 1.7. Let $V = \mathcal{TP}_2$ be the space of trigonometric polynomials of degree at most 2 with the inner product (1). Then the set of functions $\{\phi_{-2}, \phi_{-1}, \phi_0, \phi_1, \phi_2\}$ is an orthonormal basis for V . If $f \in V$, define

$$Tf = \begin{bmatrix} c_{-2} \\ c_{-1} \\ c_0 \\ c_1 \\ c_2 \end{bmatrix} \quad (10)$$

where c_k are the Fourier coefficients of $f(x)$ defined by equation (4). Notice that there is no variable x displayed in formula (10); Tf is a vector in \mathbb{C}^5 with five numerical components, whereas the continuous function $f(x)$ is considered as a vector in the space V .

Since the Fourier coefficients depend linearly on f , it is clear that T is a linear transformation from V to \mathbb{C}^5 . The basis function $\phi_k(x)$ for \mathcal{TP}_2 is transformed by T into the standard basis vector \mathbf{e}_{3+k} for $k = -2, \dots, 2$, hence T is unitary. From equation (7) we see that the functions $f_2(x) = \sin(2x)$ and $g_2(x) = \cos(2x)$ have transforms

$$Tf_2 = \frac{1}{2i} \begin{bmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \quad Tg_2 = \frac{1}{2} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Since T is unitary, it follows that

$$\begin{aligned} \frac{1}{2\pi} \int_0^{2\pi} \sin(2x) \cos(2x) dx &= \langle f_2, g_2 \rangle = \langle Tf_2, Tg_2 \rangle = 0 \\ \frac{1}{2\pi} \int_0^{2\pi} \sin^2(2x) dx &= \langle f_2, f_2 \rangle = \langle Tf_2, Tf_2 \rangle = \frac{1}{2} \end{aligned}$$

The two integrals on the left can be evaluated by double-angle formulas, of course, but this is not necessary because we already know that T is unitary. ■

2 Finite Fourier Transform

We shall call a piecewise continuous complex-valued function $s(t)$ of the real variable t an *analog signal*. We assume that $s(t)$ is of *finite duration*, so that is zero outside some interval $a \leq t \leq b$. We shift and rescale the variable t to make $a = 0$ and $b = 2\pi$. Next, we choose integers $m < n$ and replace $s(t)$ by the best approximation to $s(t)$ by trigonometric polynomials with frequencies in the range $m \leq k < n$:

$$q(t) = \sum_{m \leq k < n} c_k e^{ikt}$$

The Fourier coefficients c_k are obtained by integration:

$$c_k = \frac{1}{2\pi} \int_0^{2\pi} s(t) e^{-ikt} dt$$

The *mean square approximation error* is

$$\|s - q\|^2 = \frac{1}{2\pi} \int_0^{2\pi} |s(t) - q(t)|^2 dt = \sum_{k < m} |c_k|^2 + \sum_{k \geq n} |c_k|^2 \quad (11)$$

by Parseval's equality (6). The right side of (11) is the tail of a convergent series, so $q(t)$ will be a good approximation to $s(t)$ (on average) if the frequency band $m \leq k < n$ is chosen sufficiently wide.

For a given signal $s(t)$ we fix a *frequency band* $m \leq k < n$ so that the approximation error (11) is small. Let $N = n - m$. We replace the functions $s(t)$ and $q(t)$ by

$$f(t) = e^{-imt} s(t) \quad \text{and} \quad p(t) = e^{-imt} q(t)$$

This frequency shift doesn't change the approximation error (11), since $|e^{-imt}| = 1$. Since $e^{-imt} e^{ikt} = e^{i(k-m)t}$, the trigonometric polynomial $p(t)$ has frequencies $0 \leq k < N$:

$$p(t) = \sum_{0 \leq k < N} d_k e^{ikt}$$

Here the Fourier coefficients are

$$d_k = \frac{1}{2\pi} \int_0^{2\pi} f(t) e^{-ikt} dt \quad (12)$$

In signal processing applications there is no formula for $f(t)$, so the integrals (12) must be approximated using some numerical method. The simplest way to do this is to convert f into a *digital signal* $\mathbf{y} \in \mathbb{C}^N$ by sampling f at the N equal-spaced t values $t_j = 2\pi j/N$, for $j = 0, 1, \dots, N-1$:

$$\mathbf{y} = \begin{bmatrix} \mathbf{y}[0] \\ \mathbf{y}[1] \\ \vdots \\ \mathbf{y}[N-1] \end{bmatrix} \quad \text{where } \mathbf{y}[j] = f(t_j) \text{ for } j = 0, 1, \dots, N-1. \quad (13)$$

Here $\mathbf{y}[k]$ denotes the value of the digital signal \mathbf{y} at discrete time k (note that the indexing of the components in \mathbf{y} is different than the usual MATLAB indexing, which would go from 1 to N). We call N the *sampling rate*; the choice of this sampling rate is determined by the number of Fourier coefficients that we need to get a good representation of the signal (more coefficients require a higher sampling rate). With this choice we have

$$\Delta t = t_j - t_{j-1} = 2\pi/N, \quad \frac{\Delta t}{2\pi} = \frac{1}{N}.$$

Hence we can approximate the integral (12) by the Riemann sum

$$d_k \approx \frac{1}{N} \sum_{j=0}^{N-1} f(t_j) e^{-ikt_j} = \frac{1}{N} \sum_{j=0}^{N-1} \mathbf{y}[j] w^{-jk} \quad (14)$$

where $w = e^{2\pi i/N} = \cos(2\pi/N) + i \sin(2\pi/N)$ is a primitive N th root of unity.

Definition 2.1 (Fourier Matrix). Let F_N be the $N \times N$ matrix with (j, k) entry $w^{-(j-1)(k-1)}$, where $w = e^{2\pi i/N}$. The entries in the first column of F_N are all 1. The second column consists of the powers of w^{-1} from 0 to $N-1$, the third column consists of the powers of w^{-2} from 0 to $N-1$, and so on. Since F_N is symmetric, the same description applies to the rows. ■

For example, since $e^{2\pi i/2} = -1$ the 2×2 Fourier matrix is

$$F_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \quad (15)$$

For $N = 4$ we have $w = e^{2\pi i/4} = i$ and $w^{-1} = -i$. Hence the 4×4 Fourier matrix is

$$F_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & (-i)^2 & (-i)^3 \\ 1 & (-i)^2 & (i)^4 & (-i)^6 \\ 1 & (-i)^3 & (-i)^6 & (-i)^9 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix}. \quad (16)$$

Let $\mathbf{d} \in \mathbb{C}^N$ be the vector with components d_0, d_1, \dots, d_{N-1} given by (14). Then

$$\mathbf{d} = \frac{1}{N} F_N \mathbf{y} \quad (17)$$

Theorem 2.2. *The matrix $(1/\sqrt{N})F_N$ is unitary. Hence the matrix $(1/N)F_N$ has inverse \overline{F}_N , and the digital signal vector \mathbf{y} can be reconstructed from the sampled Fourier coefficient vector \mathbf{d} by $\mathbf{y} = \overline{F}_N \mathbf{d}$.*

Proof. To simplify the notation we label the columns of F_N from 0 to $N-1$. The k th column of F_N is then

$$\mathbf{h}_k = [1 \quad w^{-k} \quad w^{-2k} \quad \dots \quad w^{-(N-1)k}]^T$$

Hence the inner product of the j th and k th columns of F_N is

$$\langle \mathbf{h}_j, \mathbf{h}_k \rangle = \mathbf{h}_k^H \mathbf{h}_j = 1 + w^{k-j} + w^{2(k-j)} + \dots + w^{(N-1)(k-j)} \quad (18)$$

since $\overline{w} = w^{-1}$. For $j = k$ this gives $\langle \mathbf{h}_j, \mathbf{h}_j \rangle = N$. Now suppose $j \neq k$ and write $u = w^{k-j}$. Then the right side of (18) is a finite geometric series in powers of u :

$$1 + u + u^2 + \dots + u^{N-1} = \frac{1 - u^N}{1 - u}.$$

(Note that $u \neq 1$ because $0 < |j - k| < N$ and $w^p = 1$ only when p is an integer multiple of N .) But $u^N = w^{N(j-k)} = 1$, so we conclude that $\langle \mathbf{h}_j, \mathbf{h}_k \rangle = 0$ for $j \neq k$. These orthogonality relations can be written in matrix form as

$$F_N (F_N)^H = N I_N, \quad (19)$$

where I_N is the $N \times N$ identity matrix. Since F_N is symmetric, we have $(F_N)^H = \overline{F}_N$. Hence the matrix $(1/N)F_N$ has inverse \overline{F}_N , as claimed. Equation (19) can be rewritten as

$$(1/\sqrt{N})F_N (1/\sqrt{N})\overline{F}_N = I_N$$

which shows that $(1/\sqrt{N})F_N$ is a unitary matrix. ■

Corollary 2.3.

(a) *Let $\{\mathbf{e}_1, \dots, \mathbf{e}_N\}$ be the standard basis for \mathbb{C}^N . Set $\mathbf{u}_j = (1/\sqrt{N})F_N \mathbf{e}_j$. Then $\{\mathbf{u}_1, \dots, \mathbf{u}_N\}$ is an orthonormal basis for \mathbb{C}^N , called the Fourier basis.*

(b) *Let $\mathbf{y} \in \mathbb{C}^N$ and set $\mathbf{d} = (1/N)F_N \mathbf{y}$. Then $\frac{1}{N} \|\mathbf{y}\|^2 = \|\mathbf{d}\|^2$.*

Proof. (a): Note that \mathbf{u}_j is the j th column of the unitary matrix $(1/\sqrt{N})F_N$.

(b): Since $\sqrt{N}\mathbf{d} = (1/\sqrt{N})F_N \mathbf{y}$ and $(1/\sqrt{N})F_N$ is a unitary matrix, the vectors $\sqrt{N}\mathbf{d}$ and \mathbf{y} have the same norm. ■

Example 2.4. Suppose $N = 4$. The Fourier basis for \mathbb{C}^4 is

$$\mathbf{u}_1 = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \quad \mathbf{u}_2 = \frac{1}{2} \begin{bmatrix} 1 \\ -i \\ -1 \\ i \end{bmatrix}, \quad \mathbf{u}_3 = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}, \quad \mathbf{u}_4 = \frac{1}{2} \begin{bmatrix} 1 \\ i \\ -1 \\ -i \end{bmatrix}.$$

If we think of the standard basis \mathbf{e}_j as a sampled version of a signal, then the signal is *localized* in time, since only one component of \mathbf{e}_j is nonzero. By contrast, all the entries in \mathbf{u}_j are nonzero, so the Fourier matrix removes the time localization.

Let $\mathbf{y} = [1, 2, -1, 0]^T$. Then

$$\mathbf{d} = \frac{1}{4}F_4\mathbf{y} = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ -1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1/2 \\ (1-i)/2 \\ -1/2 \\ (1+i)/2 \end{bmatrix}.$$

In this case $\frac{1}{4}\|\mathbf{y}\|^2 = \frac{1}{4}[1 + 2^2 + (-1)^2] = 2/3$ and

$$\|\mathbf{d}\|^2 = \frac{1}{4}[1^2 + (1-i)(1+i) + (-1)^2 + (1+i)(1-i)] = 2/3,$$

as predicted by Corollary 2.3. ■

3 Discrete Periodic Signals and Convolution

Consider a finite digital signal \mathbf{y} with N values, say $\mathbf{y}[0], \mathbf{y}[1], \dots, \mathbf{y}[N-1]$. In the previous section we viewed \mathbf{y} as a column vector

$$\mathbf{y} = \begin{bmatrix} \mathbf{y}[0] \\ \mathbf{y}[1] \\ \vdots \\ \mathbf{y}[N-1] \end{bmatrix} \in \mathbb{C}^N. \quad (20)$$

We will also think of digital signals as functions. A basic operation in signal processing is to take a *moving average* of the signal. For example, we can replace each value $\mathbf{y}[j]$ by the average of the values $\mathbf{y}[j-1]$ and $\mathbf{y}[j+1]$. This gives a new signal \mathbf{z} with

$$\mathbf{z}[j] = \frac{1}{2}(\mathbf{y}[j-1] + \mathbf{y}[j+1]). \quad (21)$$

There is a bug in formula (21), however. To calculate $\mathbf{z}[0]$ or $\mathbf{z}[N-1]$ we need the values $\mathbf{y}[-1]$ and $\mathbf{y}[N]$, which aren't available. We will solve this problem by using the *periodic extension* of \mathbf{y} :

$$\mathbf{y}[j+kN] = \mathbf{y}[j] \quad \text{for } j = 0, 1, \dots, N-1 \text{ and all integers } k \quad (22)$$

Thus we set $\mathbf{y}[-1] = \mathbf{y}[N-1]$ and $\mathbf{y}[N] = \mathbf{y}[0]$, since $-1 = N-1 + N$ and $N = 0 + N$. In terms of *modular arithmetic*, we have $\mathbf{y}[m] = \mathbf{y}[j]$ when $m \equiv j \pmod{N}$. Now formula (21) is well-defined. It can be written in a more cumbersome case-by-case way as

$$\mathbf{z}[0] = \frac{1}{2}(\mathbf{y}[N-1] + \mathbf{y}[1]), \quad \mathbf{z}[N-1] = \frac{1}{2}(\mathbf{y}[N-2] + \mathbf{y}[0]),$$

and

$$\mathbf{z}[j] = \frac{1}{2}(\mathbf{y}[j-1] + \mathbf{y}[j+1]) \quad \text{for } j = 1, \dots, N-2.$$

For example, if $\mathbf{y} = [1, 2, -1, 0]^T$ as in Example 2.4, then

$$\mathbf{z}[0] = (0 + 2)/2, \quad \mathbf{z}[1] = (1 - 1)/2, \quad \mathbf{z}[2] = (2 + 0)/2, \quad \mathbf{z}[3] = (-1 + 1)/2.$$

Define the *shift operator* S on periodic signals \mathbf{y} of period N by

$$S\mathbf{y}[j] = \mathbf{y}[j-1] \quad \text{for } j = 0, 1, \dots, N-1.$$

Here $S\mathbf{y}[0] = \mathbf{y}[N-1]$, since \mathbf{y} is periodic. It is clear from the definition that S is linear and invertible:

$$S^{-1}\mathbf{y}[j] = \mathbf{y}[j+1].$$

We can write formula (21) as

$$\mathbf{z} = \frac{1}{2}(S + S^{-1})\mathbf{y}. \quad (23)$$

It follows that formula (21) has satisfies the following:

(linearity) The output signal \mathbf{z} depends linearly on the input signal \mathbf{y} .

(shift invariance) If the input signal \mathbf{y} is replaced by $S\mathbf{y}$, then the output signal \mathbf{z} is also replaced by $S\mathbf{z}$.

We now show that every shift-invariant linear transformation C can be expressed as a linear combination of powers of the shift operator S . We first observe that the property of shift-invariance for C is the same as

$$CS = SC. \quad (\text{Shift Invariance})$$

In particular, any linear combination of powers of S is shift invariant. To prove the converse, we identify the periodic signals of period N with \mathbb{C}^N by (20). Then S becomes a linear transformation of \mathbb{C}^N . We calculate its matrix relative to the standard basis of \mathbb{C}^N as follows: Suppose the signal \mathbf{y} corresponds to the standard basis vector \mathbf{e}_k . Then $\mathbf{y}[j] = 1$ if $j + 1 = k$, and otherwise $\mathbf{y}[j] = 0$ (note the index shift by one). Since $S\mathbf{y}[j] = \mathbf{y}[j - 1]$, we see that $S\mathbf{y}[j] = 1$ if $j = k$ and $S\mathbf{y}[j] = 0$ if $j \neq k$. This shows that

$$S\mathbf{e}_k = \mathbf{e}_{k+1} \quad \text{for } k = 1, 2, \dots, N$$

(for this formula to be valid we must label the basis vectors circularly modulo N : $\mathbf{e}_{N+1} = \mathbf{e}_1$, $\mathbf{e}_{N+2} = \mathbf{e}_2$ and so on). We see that S acts as a *circular permutation* of the standard basis vectors.

Example 3.1. Suppose $N = 3$. Then $S\mathbf{e}_1 = \mathbf{e}_2$, $S\mathbf{e}_2 = \mathbf{e}_3$, and $S\mathbf{e}_3 = \mathbf{e}_1$, so the matrix of the shift operator S relative to the standard basis for \mathbb{C}^3 is

$$S = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Notice that $S^2\mathbf{e}_1 = \mathbf{e}_3$, $S^2\mathbf{e}_2 = \mathbf{e}_1$, and $S^2\mathbf{e}_3 = \mathbf{e}_2$. Also $S^3 = I$. Thus

$$S^{-1} = S^2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = S^T.$$

We have $S^{-1} = S^T$ since $\{S\mathbf{e}_1, S\mathbf{e}_2, S\mathbf{e}_3\}$ is an orthonormal basis for \mathbb{C}^3 . ■

The general features of Example 3.1 are valid for the shift operator for any value of N . Namely, $S^N = I_N$ and $S^{-1} = S^{N-1}$. The matrix of S relative to the standard basis for \mathbb{C}^N is real and orthogonal, so in matrix form $S^{-1} = S^T$.

Theorem 3.2. Let S be the shift operator, viewed as an $N \times N$ matrix relative to the standard basis for \mathbb{C}^N . Suppose C is any shift-invariant linear transformation of N -periodic signals. View C as an $N \times N$ matrix relative to the standard basis for \mathbb{C}^N and let the first column of C be $[c_0, c_1, \dots, c_{N-1}]^T$. Then

$$C = c_0I + c_1S + c_2S^2 + \dots + c_{N-1}S^{N-1}, \quad (24)$$

where I denotes the $N \times N$ identity matrix.

Proof. The first column of C is the vector $C\mathbf{e}_1$, so this vector can be written in terms of the standard basis as

$$C\mathbf{e}_1 = c_0\mathbf{e}_1 + c_1\mathbf{e}_2 + \dots + c_{N-1}\mathbf{e}_N. \quad (25)$$

Now we calculate the columns $C\mathbf{e}_k$ of C for $k = 2, \dots, N$. Since C is shift-invariant we have $S^{k-1}C = CS^{k-1}$. Thus if we multiply both sides of (25) by S^{k-1} and use the property $S^{k-1}\mathbf{e}_1 = \mathbf{e}_k$, we obtain

$$\begin{aligned} C\mathbf{e}_k &= CS^{k-1}\mathbf{e}_1 \\ &= S^{k-1}C\mathbf{e}_1 \\ &= c_0S^{k-1}\mathbf{e}_1 + c_1S^{k-1}\mathbf{e}_2 + c_2S^{k-1}\mathbf{e}_3 + \dots + c_{N-1}S^{k-1}\mathbf{e}_N \\ &= c_0\mathbf{e}_k + c_1S\mathbf{e}_k + c_2S^2\mathbf{e}_k + \dots + c_{N-1}S^{N-1}\mathbf{e}_k. \end{aligned}$$

This shows that the k th column of the matrix C is the same as the k th column of the matrix $c_0I + c_1S + c_2S^2 + \dots + c_{N-1}S^{N-1}$ for $k = 1, \dots, N$. Hence the two matrices are equal. ■

Example 3.3. Suppose $N = 3$ and $C = c_0I + c_1S + c_2S^2$ is a 3×3 shift-invariant matrix. From Example 3.1 we have

$$C = c_0 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + c_1 \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} c_0 & c_2 & c_1 \\ c_1 & c_0 & c_2 \\ c_2 & c_1 & c_0 \end{bmatrix}.$$

Hence the successive columns of C are obtained by circular permutation of the first column. Matrices of this form are called *circulant matrices*. For example, when $N = 4$ the averaging operation from (21) is given by the circulant matrix

$$C = \frac{1}{2}(S + S^{-1}) = \frac{1}{2} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

■

We now obtain the connection between shift-invariant linear transformations and the Fourier matrix. Let $F_N = [\mathbf{h}_0 \ \mathbf{h}_1 \ \dots \ \mathbf{h}_{N-1}]$ be the $N \times N$ Fourier matrix with columns

$$\mathbf{h}_j = \begin{bmatrix} 1 \\ w^{-j} \\ w^{-2j} \\ \vdots \\ w^{-(N-1)j} \end{bmatrix}, \quad \text{where } w = e^{2\pi i/N}.$$

Since S shifts the entries in \mathbf{h}_j down one place, with the last entry moved to the top, we have

$$S\mathbf{h}_j = \begin{bmatrix} w^{-(N-1)j} \\ 1 \\ w^{-j} \\ \vdots \\ w^{-(N-2)j} \end{bmatrix} = w^j \begin{bmatrix} w^{-Nj} \\ w^{-j} \\ w^{-2j} \\ \vdots \\ w^{-(N-1)j} \end{bmatrix} = w^j \mathbf{h}_j.$$

Define a diagonal matrix with the N th roots of 1 on the diagonal:

$$D_N = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & w & 0 & \dots & 0 \\ 0 & 0 & w^2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & w^{N-1} \end{bmatrix} \quad (26)$$

The calculation just made shows that

$$SF_N = [\mathbf{h}_0 \quad w\mathbf{h}_1 \quad w^2\mathbf{h}_2 \quad \cdots \quad w^{N-1}\mathbf{h}_{N-1}] = F_N D_N. \quad (27)$$

By Theorem 2.2 the Fourier matrix is invertible. Hence multiplying (27) on the left by F_N^{-1} , we obtain

$$F_N^{-1}SF_N = D_N. \quad (28)$$

We can summarize these calculations as follows:

Theorem 3.4. *The $N \times N$ shift matrix S is diagonalized by the Fourier matrix F_N . The columns of F_N are eigenvectors of S , and the eigenvalues of S are the N complex numbers w^j for $j = 0, 1, \dots, N-1$ (the N th roots of unity).*

Combining the last two theorems gives us the main result of this section:

Theorem 3.5 (Diagonalization of Circulant Matrices). *Suppose that C is a $N \times N$ shift-invariant (circulant) matrix. Write*

$$C = c_0I + c_1S + c_2S^2 + \cdots + c_{N-1}S^{N-1}$$

and define the polynomial $p(z) = c_0 + c_1z + c_2z^2 + \cdots + c_{N-1}z^{N-1}$. Then \mathbf{h}_j is an eigenvector for C , with eigenvalue $p(w^j)$, for $j = 0, 1, \dots, N-1$. Hence C is diagonalized by the Fourier matrix:

$$F_N^{-1}CF_N = p(D_N) = \begin{bmatrix} p(1) & 0 & 0 & \cdots & 0 \\ 0 & p(w) & 0 & \cdots & 0 \\ 0 & 0 & p(w^2) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & p(w^{N-1}) \end{bmatrix} \quad (29)$$

Proof. Since (28) implies that $F_N^{-1}S^kF_N = D_N^k$ for all integers k , the matrix C satisfies the corresponding equation:

$$F_N^{-1}CF_N = c_0I + c_1D_N + c_2D_N^2 + \cdots + c_{N-1}D_N^{N-1}.$$

The right side of this equation is $p(D_N)$. ■

Example 3.6. Consider the 4×4 circulant matrix $C = \frac{1}{2}(S + S^{-1}) = \frac{1}{2}(S + S^3)$ from Example 3.3 (note that $S^{-1} = S^3$ since $S^4 = I$). Then $p(z) = \frac{1}{2}z + \frac{1}{2}z^3$. Since the fourth roots of 1 are $1, i, -1, -i$, the eigenvalues of C are

$$\begin{aligned} p(1) &= 1, & p(i) &= (1/2)(i + i^3) = 0, \\ p(-1) &= (1/2)(-1 + (-1)^3) = -1, & p(-i) &= (1/2)(-i + (-i)^3) = 0. \end{aligned}$$
■

Now we return to the digital signal point of view. Let C be a linear shift-invariant operator on signals periodic of period N . Then by Theorem 3.2 there are complex numbers c_0, \dots, c_{N-1} so that

$$C = c_0I + c_1S + c_2S^2 + \cdots + c_{N-1}S^{N-1}.$$

If we apply C to a periodic signal \mathbf{y} , then we get the signal

$$C\mathbf{y}[j] = c_0\mathbf{y}[j] + c_1\mathbf{y}[j-1] + c_2\mathbf{y}[j-2] + \cdots + c_{N-1}\mathbf{y}[j-N+1] \quad (30)$$

for $j = 0, 1, \dots, N - 1$. This shows that $C\mathbf{y}$ is a *moving average* of the original signal \mathbf{y} , generalizing the special case of (21). Define the function $\mathbf{f}[k] = c_k$ for $k = 0, 1, \dots, N - 1$. Then (30) can be written as

$$C\mathbf{y}[j] = \sum_{k=0}^{N-1} \mathbf{f}[k]\mathbf{y}[j-k]. \quad (31)$$

We call the function $C\mathbf{y}$ the *convolution* (folding) of \mathbf{f} and \mathbf{y} and we write $C\mathbf{y} = \mathbf{f} * \mathbf{y}$. An alternate statement of Theorem 3.2 is the following:

(Linear Shift-Invariant Filters) Every linear transformation of N -periodic signals \mathbf{y} that is shift invariant is given by the convolution (moving average) operation $\mathbf{y} \mapsto \mathbf{f} * \mathbf{y}$ for some function \mathbf{f} on the set $\{0, 1, \dots, N - 1\}$ (the *filter*).

We can now obtain the linear filter version of Theorem 3.5.

Definition 3.7 (Discrete Fourier Transform). If \mathbf{y} is a periodic digital signal (of period N), then the *Fourier transform* of \mathbf{y} is the function

$$\hat{\mathbf{y}}[k] = \sum_{j=0}^{N-1} \mathbf{y}[j]w^{-jk} \quad \text{for } k = 0, 1, \dots, N - 1,$$

where $w = e^{2\pi i/N}$ (note that the function $\hat{\mathbf{y}}$ is also periodic of period N). Thus if \mathbf{y} is viewed as a column vector in \mathbb{C}^N , then $\hat{\mathbf{y}}$ is the column vector $F_N\mathbf{y}$. ■

The filter \mathbf{f} corresponding to the circulant matrix C in (24) is defined by $\mathbf{f}[k] = c_k$ for $k = 0, 1, \dots, N - 1$. The matrix-vector product $C\mathbf{y}$ becomes the convolution $\mathbf{f} * \mathbf{y}$ in the signal-processing picture. We can restate the result of Theorem 3.4 in terms of the Fourier transform and convolution as follows:

Theorem 3.8 (Diagonalization of Convolution Operators). Let $C\mathbf{y} = \mathbf{f} * \mathbf{y}$ be the convolution operator (31) on signals \mathbf{y} that are periodic of period N . Then the Fourier transform of $C\mathbf{y}$ is the pointwise product:

$$\widehat{C\mathbf{y}}[k] = \hat{\mathbf{f}}[k]\hat{\mathbf{y}}[k] \quad \text{for } k = 0, 1, \dots, N - 1. \quad (32)$$

Proof. The columns of the Fourier matrix are eigenvectors for the circulant matrix C , and the eigenvalues are the scalars $\hat{\mathbf{f}}[k]$. Thus when a vector is expressed in terms of the Fourier basis, C acts on the k th component by multiplying by the eigenvalue $\hat{\mathbf{f}}[k]$.

We can give a direct proof of this result, without using Theorem 3.4, as follows. By definition of the finite Fourier transform, we have

$$\widehat{\mathbf{f} * \mathbf{y}}[k] = \sum_{j=0}^{N-1} (\mathbf{f} * \mathbf{y})[j]w^{-jk} = \sum_{j=0}^{N-1} \sum_{l=0}^{N-1} \mathbf{f}[j-l]\mathbf{y}[l]w^{-jk}$$

for $k = 0, 1, \dots, N - 1$. Making the substitution $m = j - l$ and using the periodicity of \mathbf{f} and \mathbf{y} so that the range of summation is $0 \leq m < N$ and $0 \leq l < N$, we obtain

$$\begin{aligned} \widehat{\mathbf{f} * \mathbf{y}}[k] &= \sum_{m=0}^{N-1} \sum_{l=0}^{N-1} \mathbf{f}[m]\mathbf{y}[l]w^{-(m+l)k} = \sum_{m=0}^{N-1} \mathbf{f}[m]w^{-mk} \sum_{l=0}^{N-1} \mathbf{y}[l]w^{-lk} \\ &= \hat{\mathbf{f}}[k]\hat{\mathbf{y}}[k] \end{aligned}$$

This proves (32). ■

Example 3.9. Consider the averaging operator (21) from the beginning of this Section:

$$C\mathbf{y}[j] = \frac{1}{2}(\mathbf{y}[j-1] + \mathbf{y}[j+1]),$$

where \mathbf{y} is a periodic signal of length N . We can write this as $C\mathbf{y} = \mathbf{f} * \mathbf{y}$, where

$$\mathbf{f}[1] = 1/2, \quad \mathbf{f}[N-1] = 1/2, \quad \text{and } \mathbf{f}[j] = 0 \text{ for } j \neq 1, N-1,$$

since $C = (1/2)(S + S^{-1})$ as in Example 3.6. In this case the polynomial $p(z) = (1/2)(z + z^{-1})$ and $\hat{\mathbf{f}}[k] = (1/2)(w^k + w^{-k})$. Thus

$$\widehat{C\mathbf{y}}[k] = \frac{1}{2}(w^k + w^{-k})\hat{\mathbf{y}}[k] \quad \text{for } k = 0, 1, \dots, N-1.$$

■

4 Fast Fourier Transform

The effectiveness of the discrete Fourier transform (DFT) as a computational tool depends on a remarkable *fast algorithm* for calculating the matrix-vector product $F_n \mathbf{v}$ when $n = 2^k$ is a power of 2 (similar fast algorithms exist for every *highly composite* number n , such as $n = 2^k 3^m$). The Fast Fourier Transform (FFT) algorithm is based on the observation that the Fourier matrix F_{2n} can be written as product of a permutation matrix (which has no arithmetic computational cost) and a 2×2 *block matrix*, where the blocks are F_n or a diagonal matrix multiplying F_n .

Example 4.1. Consider $n = 2$. Recall that

$$F_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad F_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} = [\mathbf{h}_0 \quad \mathbf{h}_1 \quad \mathbf{h}_2 \quad \mathbf{h}_3].$$

Let $\mathbf{y} \in \mathbb{C}^4$. By the definition of matrix-vector multiplication we can write

$$F_4 \mathbf{y} = \mathbf{y}[0] \mathbf{h}_0 + \mathbf{y}[1] \mathbf{h}_1 + \mathbf{y}[2] \mathbf{h}_2 + \mathbf{y}[3] \mathbf{h}_3$$

as a linear combination of the columns of the Fourier matrix. Rearrange this sum according to the even and odd indices:

$$\mathbf{y}[0] \mathbf{h}_0 + \mathbf{y}[2] \mathbf{h}_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \\ 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \mathbf{y}[0] \\ \mathbf{y}[2] \end{bmatrix}, \quad \mathbf{y}[1] \mathbf{h}_1 + \mathbf{y}[3] \mathbf{h}_3 = \begin{bmatrix} 1 & 1 \\ -i & i \\ -1 & -1 \\ i & -i \end{bmatrix} \begin{bmatrix} \mathbf{y}[1] \\ \mathbf{y}[3] \end{bmatrix}. \quad (33)$$

Define

$$\mathbf{y}_{\text{even}} = \begin{bmatrix} \mathbf{y}[0] \\ \mathbf{y}[2] \end{bmatrix}, \quad \mathbf{y}_{\text{odd}} = \begin{bmatrix} \mathbf{y}[1] \\ \mathbf{y}[3] \end{bmatrix}, \quad \tilde{D}_2 = \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix}.$$

Then, using block multiplication of matrices, we can write the formulas (33) as

$$\mathbf{y}[0] \mathbf{h}_0 + \mathbf{y}[2] \mathbf{h}_2 = \begin{bmatrix} F_2 \\ F_2 \end{bmatrix} \mathbf{y}_{\text{even}}, \quad \mathbf{y}[1] \mathbf{h}_1 + \mathbf{y}[3] \mathbf{h}_3 = \begin{bmatrix} \tilde{D}_2 F_2 \\ -\tilde{D}_2 F_2 \end{bmatrix} \mathbf{y}_{\text{odd}}.$$

The splitting of \mathbf{y} into even/odd vectors of half length can be accomplished by the permutation matrix

$$P_4 = \begin{bmatrix} \mathbf{e}_1 & \mathbf{e}_3 & \mathbf{e}_2 & \mathbf{e}_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad P_4 \mathbf{y} = \begin{bmatrix} \mathbf{y}_{\text{even}} \\ \mathbf{y}_{\text{odd}} \end{bmatrix}.$$

The calculations above show that

$$F_4 \mathbf{y} = \begin{bmatrix} F_2 \mathbf{y}_{\text{even}} + \tilde{D}_2 F_2 \mathbf{y}_{\text{odd}} \\ F_2 \mathbf{y}_{\text{even}} - \tilde{D}_2 F_2 \mathbf{y}_{\text{odd}} \end{bmatrix} = \begin{bmatrix} F_2 & \tilde{D}_2 F_2 \\ F_2 & -\tilde{D}_2 F_2 \end{bmatrix} P_4 \mathbf{y}.$$

Hence the 4×4 Fourier matrix F_4 can be written in 2×2 block form:

$$F_4 = \begin{bmatrix} F_2 & \tilde{D}_2 F_2 \\ F_2 & -\tilde{D}_2 F_2 \end{bmatrix} P_4. \quad \blacksquare$$

The same splitting into even and odd components works for the DFT of a signal

$$\mathbf{y} = \begin{bmatrix} \mathbf{y}[0] & \mathbf{y}[1] & \dots & \mathbf{y}[2n-2] & \mathbf{y}[2n-1] \end{bmatrix}^T$$

of length $2n$. Let

$$\mathbf{y}_{\text{even}} = \begin{bmatrix} \mathbf{y}[0] & \mathbf{y}[2] & \dots & \mathbf{y}[2n-2] \end{bmatrix}^T, \quad \mathbf{y}_{\text{odd}} = \begin{bmatrix} \mathbf{y}[1] & \mathbf{y}[3] & \dots & \mathbf{y}[2n-1] \end{bmatrix}^T.$$

Here we are using the terms *even* and *odd* because we view \mathbf{y} as a function on $\{0, 1, \dots, 2n-1\}$; the vector \mathbf{y}_{even} contains components $1, 3, \dots, 2n-1$ of the vector \mathbf{y} when we use the MATLAB indexing convention. The splitting of \mathbf{y} into \mathbf{y}_{even} and \mathbf{y}_{odd} of half length is called *downsampling*.

Write $w = e^{2\pi i/2n} = e^{\pi i/n}$ and $z = w^2 = e^{2\pi i/n}$. Then

$$\begin{aligned} F_{2n} \mathbf{y}[j] &= \sum_{k=0}^{2n-1} w^{-jk} \mathbf{y}[k] \\ \text{(split into even-odd)} &= \sum_{k=0}^{n-1} w^{-j(2k)} \mathbf{y}[2k] + \sum_{k=0}^{n-1} w^{-j(2k+1)} \mathbf{y}[2k+1] \\ &= \sum_{k=0}^{n-1} z^{-jk} \mathbf{y}_{\text{even}}[k] + w^{-j} \sum_{k=0}^{n-1} z^{-jk} \mathbf{y}_{\text{odd}}[k] \end{aligned}$$

for $j = 0, 1, 2, \dots, 2n-1$. This shows that

$$F_{2n} \mathbf{y}[j] = F_n \mathbf{y}_{\text{even}}[j] + w^{-j} F_n \mathbf{y}_{\text{odd}}[j] \quad \text{for } j = 0, 1, \dots, n-1.$$

Since $w^n = -1$ and $z^n = 1$, we have $w^{-(n+j)} = -w^{-j}$ and $z^{-(n+j)k} = z^{-jk}$. Furthermore, the functions $F_n \mathbf{y}_{\text{even}}$ and $F_n \mathbf{y}_{\text{odd}}$ are periodic of period n . Thus

$$F_{2n} \mathbf{y}[n+j] = F_n \mathbf{y}_{\text{even}}[j] - w^{-j} F_n \mathbf{y}_{\text{odd}}[j] \quad \text{for } j = 0, 1, \dots, n-1.$$

We can write these formulas in block-matrix form, just as in the case $n = 2$. Let

$$\tilde{D}_n = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & w^{-1} & 0 & \dots & 0 \\ 0 & 0 & w^{-2} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & w^{-(n-1)} \end{bmatrix} \quad \text{(caution: } w^n = -1). \quad (34)$$

Note that the diagonal of \tilde{D}_n only contains half of the $2n$ th roots of 1; it is not the same as the matrix D_N in equation (26) which has all N th roots of 1. Let P_{2n} be the permutation matrix that splits \mathbf{y} into its even and odd components:

$$P_{2n} = \begin{bmatrix} \mathbf{e}_1 & \mathbf{e}_3 & \dots & \mathbf{e}_{2n-1} & \mathbf{e}_2 & \mathbf{e}_4 & \dots & \mathbf{e}_{2n} \end{bmatrix}^T, \quad P_{2n}\mathbf{y} = \begin{bmatrix} \mathbf{y}_{\text{even}} \\ \mathbf{y}_{\text{odd}} \end{bmatrix}.$$

Then, just as in the case $n = 2$, the equations for $F_{2n}\mathbf{y}$ can be written as

$$F_{2n}\mathbf{y} = \begin{bmatrix} F_n\mathbf{y}_{\text{even}} + \tilde{D}_n F_n\mathbf{y}_{\text{odd}} \\ F_n\mathbf{y}_{\text{even}} - \tilde{D}_n F_n\mathbf{y}_{\text{odd}} \end{bmatrix} = \begin{bmatrix} F_n & \tilde{D}_n F_n \\ F_n & -\tilde{D}_n F_n \end{bmatrix} P_{2n}\mathbf{y} \quad (35)$$

The *Fast Fourier Transform* algorithm calculates F_N when N is a power of 2 by iterating formula (35). For example, when $N = 256 = 2^8$ then (35) expresses $F_{256}\mathbf{y}$ in terms of F_{128} applied to signals of length 128. To calculate these Fourier transforms, we use (35) again to express F_{128} in terms of F_{64} applied to signals of length 64, and so on until we are down to F_2 (see Figure 3.12 on page 195 of Strang's book).

To determine the computational cost of the FFT algorithm, let $n = 2^k$, and define $\phi(k)$ be the number of scalar multiplications needed to evaluate $F_n\mathbf{y}$ for a signal of length $n = 2^k$ using the FFT algorithm. When $k = 1$ then the entries in F_2 are ± 1 , so no multiplications are needed (just sign changes). Hence $\phi(1) = 0$. If \mathbf{y} is a signal of length $2n = 2^{k+1}$, then calculating $F_{2n}\mathbf{y}$ using (35) requires $2\phi(k)$ multiplications to obtain $F_n\mathbf{y}_{\text{even}}$ and $F_n\mathbf{y}_{\text{odd}}$, followed by 2^k multiplications to obtain $\tilde{D}_n F_n\mathbf{y}_{\text{odd}}$. We are using the fact that \tilde{D}_n is a diagonal matrix, so it only requires n multiplications to calculate $\tilde{D}_n \mathbf{b}$ for any vector \mathbf{b} . The matrix P_{2n} just sorts the entries of \mathbf{y} ; no arithmetic is needed to calculate $P_{2n}\mathbf{y}$. Thus

$$\phi(k+1) = 2\phi(k) + 2^k \quad (36)$$

We can calculate $\phi(k)$ recursively from (36), starting with $\phi(1) = 0$:

$$\phi(2) = 2\phi(1) + 2 = 2, \quad \phi(3) = 2\phi(2) + 2^2 = 2 \cdot 2^2, \quad \phi(4) = 2\phi(3) + 2^3 = 3 \cdot 2^3$$

This suggests that

$$\phi(k) = (k-1)2^{k-1} \quad \text{for all positive integers } k = 1, 2, 3, \dots \quad (37)$$

This formula, which we have just shown true for $k = 2, 3$, and 4, is easily verified by induction: assuming it true for k and using (36), we get

$$\phi(k+1) = 2(k-1)2^{k-1} + 2^k = k2^k - 2^k + 2^k = k2^k,$$

so the formula is true for $k+1$.

To appreciate the consequences of (37), note that direct evaluation of $F_n\mathbf{y}$ as a matrix-vector product requires $n^2 = 2^{2k}$ scalar multiplications (n for each of the n components of \mathbf{y}). Take $k = 10$ and $n = 2^{10} = 1024$. Then direct evaluation of $F_n\mathbf{y}$ as a matrix-vector product requires $n^2 = 2^{20} = 1,048,576$ multiplications, whereas evaluation using the FFT only requires $9 \cdot 2^9 = 4608$ multiplications. This is a speedup by a factor of

$$\frac{2^{20}}{9 \cdot 2^9} = 228.$$

If we go to longer signals, such as $n = 2^{20} = 1,048,576$, then the speedup is by a factor of

$$\frac{2^{40}}{19 \cdot 2^{19}} = 110,376$$

(more than one hundred thousand times faster). The same sort of counting of the number of scalar addition operations needed in the FFT shows a similar dramatic improvement over calculations using the standard matrix-vector product. Without the FFT algorithm digital signal processing would be impractical.

5 Exercises

- Let N be a positive integer and set $w = e^{2\pi i/N}$. View the columns of the Fourier matrix F_N as the functions $\mathbf{h}_0, \dots, \mathbf{h}_{N-1}$ defined by $\mathbf{h}_k[j] = w^{-jk}$ (note that with this definition \mathbf{h}_k is automatically periodic of period N .) Verify directly that each function \mathbf{h}_k is an eigenfunction for the shift operator S , and determine the eigenvalue. Recall that S acts on a periodic function \mathbf{f} by $S\mathbf{f}[j] = \mathbf{f}[j-1]$.
- Let C be the linear shift-invariant transformation $C\mathbf{y}[j] = \mathbf{y}[j-1] - 2\mathbf{y}[j] + \mathbf{y}[j+1]$ for \mathbf{y} a function periodic of period N .
 - Find the function \mathbf{f} such that $C\mathbf{y} = \mathbf{f} * \mathbf{y}$. (HINT: Write C in terms of the shift operator.)
 - Find the Fourier transform of the function \mathbf{f} in (a).
 - Suppose $N = 4$ and \mathbf{y} corresponds to the vector $\mathbf{y} = [2\ 3\ 1\ 5]^T \in \mathbb{C}^4$. Calculate the vectors corresponding to $C\mathbf{y}$ and $\widehat{C\mathbf{y}}$.

- Let $S = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ be the matrix for the shift operator relative to the standard basis for \mathbb{C}^3 . Suppose the matrix $C = \begin{bmatrix} 4 & * & * \\ 7 & * & * \\ 5 & * & * \end{bmatrix}$ satisfies $CS = SC$.
 - Write C as a polynomial in S . Use this to fill in the missing entries in C :

$$C = \begin{bmatrix} 4 & \text{---} & \text{---} \\ 7 & \text{---} & \text{---} \\ 5 & \text{---} & \text{---} \end{bmatrix}$$

- View vectors in \mathbb{C}^3 as periodic functions \mathbf{y} on the integers: $\mathbf{y}[j] = \mathbf{y}[j+3]$ for all integers j . Let T be the linear transformation on such functions corresponding to the matrix C above. Give explicit formulas (in terms of $\mathbf{y}[0]$, $\mathbf{y}[1]$, and $\mathbf{y}[2]$) for $T\mathbf{y}[j]$ for $j = 0, 1, 2$.
- Let F be the 3×3 Fourier matrix, and let $w = e^{2\pi i/3}$. Let C be the matrix in part (a). Find complex numbers λ_0 , λ_1 , and λ_2 so that $F^{-1}CF = \begin{bmatrix} \lambda_0 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{bmatrix}$.

Express your answer in terms of w and w^2 (no complex arithmetic is needed).

- Let $n = 2^k$. Define $\psi(k)$ to be the number of scalar additions (or subtractions) needed to calculate $F_n \mathbf{c}$ by the Fast Fourier Transform (FFT) algorithm. Note that the product of a row vector and a column vector, each with n components, needs $n-1$ additions.
 - Show that $\psi(1) = 2$ and that $\psi(k+1) = 2\psi(k) + 2(2^k - 1)$.
 - Use the recursion in (a) to calculate $\psi(k)$ for $k = 2, 3, 4$.
 - Prove by induction that $\psi(k) \leq k2^k$ for all positive integers k .
 - Use the result in the notes and (c) to show that the total number of arithmetic operations (multiplications and additions) required for the FFT on vectors of size 2^k is less than $(3/2)k2^k$.