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

Roe Goodman

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

Revised November 3, 2005

1 Inner Products and Unitary Transformations

The formula de£ning the usual inner product and norm on $\mathbb{R}^n$ needs to be modi£ed when we de£ne 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 $\mathrm{i}^2 = -1$. The way around this dif£culty is to use the fact that $\bar{z}z > 0$ if z is a nonzero complex number. Thus we de£ne 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 de£ne 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 de£nition 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 de£ne the *norm* $||\mathbf{u}|| = \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle}$ which measures the total size of a vector with complex components.

De£nition 1.1. Let V be a complex vector space. An *inner product* on V is a complex-valued function $\langle \mathbf{u}, \mathbf{v} \rangle$ de£ned for all $\mathbf{u}, \mathbf{v} \in V$ that satis£es 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 de£ned above satis£es these conditions. Here is another important example.

Example 1.2. Consider the complex vector space V of all complex-valued continuous functions on a £nite 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 £xed real number p.) Given two functions f and g in V, de£ne

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

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 area under the graph of $|f(x)|^2$ is zero. The conjugate symmetry and linearity are obvious.

Let V be a complex vector space with a £xed 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*

$$|\langle \mathbf{u}, \mathbf{v}\rangle| \leq ||\mathbf{u}||\, ||\mathbf{v}|| \tag{2}$$

as in the real case. From the Cauchy-Schwarz inequality we obtain the *triangle inequality*

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

De£nition 1.3. A set of nonzero vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots,$ 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 satis£es $||\mathbf{v}_j|| = 1$ then the set is called *orthonormal*.

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

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

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

$$||\mathbf{u}||^2 = |c_1|^2 + \cdots + |c_n|^2 \tag{Parseval's Formula}$$

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

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

For any vector $\mathbf{v} \in V$ we de£ne

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

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,

$$||\mathbf{v}||^2 = ||P\mathbf{v}||^2 + ||\mathbf{v} - P\mathbf{v}||^2 \tag{3}$$

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 continuous complex-valued functions $f(x)$ de£ned on the interval $0 \le x \le 2\pi$. De£ne an inner product on V by

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

Then the functions $\phi_n(x) = \mathrm{e}^{\,\mathrm{i}\, nx}$, for $n \in \mathbb{Z}$ (the set of all integers), form an orthonormal set. To see this, let $k \neq n$ and calculate

$$\begin{aligned} \langle \phi_n, \phi_k \rangle &= \frac{1}{2\pi} \int_0^{2\pi} \mathrm{e}^{\,\mathrm{i}\,(n-k)x}\, dx \\ &= \left. \frac{\mathrm{e}^{\,\mathrm{i}\,(n-k)x}}{2\pi\,\mathrm{i}\,(n-k)} \right|_{x=0}^{x=2\pi} = 0 \end{aligned}$$

because $\mathrm{e}^{2m\pi\,\mathrm{i}} = 1$ for all integers m. Thus $\phi_n \perp \phi_k$. When $n = k$, we have

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

since $\mathrm{e}^0 = 1$.

If $f \in V$ then the complex numbers

$$\hat{f}(k) = \langle f, \phi_k \rangle = \frac{1}{2\pi} \int_0^{2\pi} f(x)\mathrm{e}^{-2\pi\,\mathrm{i}\,kx}\, dx$$

are called the *Fourier coef£cients* of f. It is an important result of Fourier analysis that the *in£nite series* version of Parseval's formula is valid:

$$\frac{1}{2\pi} \int_0^{2\pi} |f(x)|^2\, dx = \sum_{k \in \mathbb{Z}} |\hat{f}(k)|^2. \tag{4}$$

In particular, the in£nite series on the right side of (4) converges (the proof of (4) for a general continuous function f requires some results from advanced calculus and will not be given in this course).

Let $\mathcal{TP}_n$ be the linear span of the set of functions $\{\phi_k \;:\; |k| \le n\}$. If $f \in \mathcal{TP}_n$ then $\hat{f}(k) = 0$ for $|k| > n$, and the summation on the right side of equation (4) is from $k = -n$ to $k = n$. The function f has the *£nite Fourier series*

$$f = \sum_{k=-n}^{n} \hat{f}(k)\phi_k.$$

Set $z = \mathrm{e}^{2\pi\,\mathrm{i}\,x}$. Then $\phi_k = z^k$, so f is a £nite linear combination of positive and negative powers of z:

$$f = \sum_{k=-n}^{n} c_k z^k, \tag{5}$$

where $c_k = \hat{f}(k)$. Functions of the form (5) are called *Laurent polynomials*.

When f is real-valued, then the Fourier coef£cients have the property

$$\overline{\hat{f}(k)} = \hat{f}(-k),$$

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

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

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

$$f_n = \frac{1}{2\,\mathrm{i}}\phi_n - \frac{1}{2\,\mathrm{i}}\phi_{-n}\,, \qquad g_n = \frac{1}{2}\phi_n + \frac{1}{2}\phi_{-n}\,. \tag{6}$$

We can write these formulas in terms of Laurent polynomials as

$$f_n = \frac{1}{2\,\mathrm{i}}z^n - \frac{1}{2\,\mathrm{i}}z^{-n}\,, \qquad g_n = \frac{1}{2}z^n + \frac{1}{2}z^{-n}\,.$$

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

$$\psi_n(x) = \sum_{k=-n}^{k=n} \hat{f}(k)\mathrm{e}^{2\pi\,\mathrm{i}\,kx}$$

is the function in $\mathcal{TP}_n$ that minimizes $||f - \psi||$ as ψ ranges over all trigonometric polynomials in $\mathcal{TP}_n$, by (3).

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

The matrix U is unitary if and only if

$$\langle U\mathbf{v}, U\mathbf{w}\rangle = \langle \mathbf{v}, \mathbf{w}\rangle \quad \text{for all } \mathbf{v}, \mathbf{w} \in \mathbb{C}^n. \tag{7}$$

To prove this, use the linearity of the inner product in each variable to see that (7) is satis£ed for all vectors $\mathbf{v}, \mathbf{w}$ if and only if it is satis£ed when $\mathbf{v} = \mathbf{e}_j$ and $\mathbf{w} = \mathbf{e}_k$ (the standard basis vectors for $\mathbb{C}^n$). Since the jth column of U is $U\mathbf{e}_j$ and the set $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ is orthonormal, it follows that (7) 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 £nite-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

$$\langle T\mathbf{u}, T\mathbf{v}\rangle = \langle \mathbf{u}, \mathbf{v}\rangle \quad \text{for all vectors } \mathbf{u}, \mathbf{v} \in V. \tag{8}$$

Note that in equation (8) 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

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

relative to the standard basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ of $\mathbb{C}^n$ (where $\mathbf{e}_j$ has 1 in the jth entry and zero elsewhere). Since the standard basis is orthonormal, we see from (8) 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. De£ne a linear transformation T from V to $\mathbb{C}^5$ by

$$Tf = \begin{bmatrix} \hat{f}(-2) \\ \hat{f}(-1) \\ \hat{f}(0) \\ \hat{f}(1) \\ \hat{f}(2) \end{bmatrix}$$

(Tf is the vector whose entries are the Fourier coef£cients of f). Since the Fourier coef£cients depend linearly on f, it is clear that T is a linear transformation. The exponential basis function ϕ_k for $\mathcal{TP}_2$ is tranformed by T into the standard basis vector $\mathbf{e}_{3+k}$ for $k = -2, \ldots, 2$, hence T is unitary. From equation (6) we see that the functions $f_2(x) = \sin(2x)$ and $g_2(x) = \cos(2x)$ have transforms

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

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 continuous complex-valued function $s(x)$ of the real variable x an *analog signal* (think of x as *time* and $s(x)$ as measuring the loudness of a sound). We assume that $s(x)$ is of *£nite duration*, so that is zero outside some interval $a \le x \le b$. We rescale the variable x to make $a = 0$ and $b = 2\pi$. Now choose integers $m < n$ and replace $s(x)$ by the best approximation to $s(x)$ by trigonometric polynomials with frequencies in the range $m \le k < n$:

$$q(x) = \sum_{m \le k < n} \hat{s}(k)\, \mathrm{e}^{\mathrm{i}\,kx}.$$

The *mean square approximation error* is

$$||s - q||^2 = \frac{1}{2\pi}\int_0^{2\pi} |s(x) - q(x)|^2\,dx = \sum_{k<m} |\hat{s}(k)|^2 + \sum_{k \ge n} |\hat{s}(k)|^2 \qquad (9)$$

by Parseval's equality (4). The right side of (9) is the tail of a convergent series, so $q(x)$ will be a good approximation to $s(x)$ (on average) if the frequency band $m \le k < n$ is chosen suf£ciently wide.

For a given signal $s(x)$ we £x a *frequency band* $m \le k < n$ so that the approximation error (9) is small. Let $N = n - m$. We replace the functions $s(x)$ and $q(x)$ by

$$f(x) = \mathrm{e}^{-\,\mathrm{i}\,mx} s(x) \quad \text{and} \quad p(x) = \mathrm{e}^{-\,\mathrm{i}\,mx} q(x).$$

This doesn't change the approximation error (9), since $|e^{-\mathrm{i}\,mx}| = 1$. Now we have a frequency range $0 \le k < N$:

$$p(x) = \sum_{0\le k<N} c_k\, e^{\mathrm{i}\,kx}, \quad \text{where } c_k = \hat{f}(k).$$

The coef£cients c_k are obtained from f by integration:

$$c_k = \langle f, \phi_k \rangle = \frac{1}{2\pi} \int_0^{2\pi} f(x) e^{-\mathrm{i}\,kx}\, dx. \tag{10}$$

In signal processing applications there is no formula for $f(x)$, so the integrals (10) must be approximated using some numerical method. To do this, we £rst convert f into a *digital signal* $\mathbf{y} \in \mathbb{C}^N$ by sampling f at the N equal-spaced x values $x_j = 2\pi j/N$, for $j = 0, 1, \ldots, N-1$:

$$\mathbf{y} = \begin{bmatrix} y[0] \\ y[1] \\ \vdots \\ y[N-1] \end{bmatrix} \quad \text{where } y[j] = f(x_j) \text{ for } j = 0, 1, \ldots, N-1. \tag{11}$$

(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 coef£cients that we need to calculate (more coef£cients require a higher sampling rate). With this choice we have

$$\Delta x = x_j - x_{j-1} = 2\pi/N, \qquad \frac{\Delta x}{2\pi} = \frac{1}{N}.$$

Hence we can approximate the integral (10) by the Riemann sum

$$d_k = \frac{1}{N} \sum_{j=0}^{N-1} f(x_j)\, e^{-\mathrm{i}\,kx_j} = \frac{1}{N} \sum_{j=0}^{N-1} y[j]\, \omega_N^{jk} \tag{12}$$

where $\omega_N = e^{-2\pi\,\mathrm{i}/N} = \cos(2\pi\,\mathrm{i}/N) - \mathrm{i}\,\sin(2\pi\,\mathrm{i}/N)$ (note that $(\omega_N)^N = e^{-2N\pi\,\mathrm{i}/N} = 1$). The £nite sequence $\{d_0, d_1, \ldots, d_{N-1}\}$ is called the *discrete Fourier transform* (DFT) of the sampled signal $\{y[0], y[1], \ldots, y[N-1]\}$.

We now write the DFT in matrix form.

De£nition 2.1 (Fourier Matrix)**.** Let F_N be the $N \times N$ matrix with (j,k) entry $\omega_N^{(j-1)(k-1)}$. Every entry in the £rst column of F_N is 1. The second column consists of the powers of ω_N from 0 to $N-1$, the third column consists of the powers of ω_N^2 from 0 to $N-1$, and so on. Since F_N is symmetric, the same description applies to the rows.

For example, since $\omega_2 = e^{-2\pi\,\mathrm{i}/2} = -1$ the 2×2 Fourier matrix is

$$F_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{13}$$

For $N = 4$ we have $\omega_4 = e^{-2\pi\,\mathrm{i}/4} = -\mathrm{i}$, so the 4×4 Fourier matrix is

$$F_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -\mathrm{i} & (-\mathrm{i})^2 & (-\mathrm{i})^3 \\ 1 & (-\mathrm{i})^2 & (\mathrm{i})^4 & (-\mathrm{i})^6 \\ 1 & (-\mathrm{i})^3 & (-\mathrm{i})^6 & (-\mathrm{i})^9 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -\mathrm{i} & -1 & \mathrm{i} \\ 1 & -1 & 1 & -1 \\ 1 & \mathrm{i} & -1 & -\mathrm{i} \end{bmatrix}. \tag{14}$$

Let $\mathbf{d} \in \mathbb{C}^N$ be the vector with components $d_0, d_1, \ldots, d_{N-1}$ given by (12). Then

$$\mathbf{d} = \frac{1}{N} F_N \mathbf{y} \tag{15}$$

Remarks: In MATLAB, the vector $F_N\mathbf{y}$ (without the normalizing factor $1/N$) is obtained by the command `fft(y)`. In Strang's text, however, the *Fourier matrix* is de£ned using $w = \mathrm{e}^{2\pi\,\mathrm{i}/n}$ (with i instead of $-\mathrm{i}$). Thus Strang's version of the Fourier matrix is the complex conjugate of the matrix F_N de£ned here.

Theorem 2.2. *The matrix $(1/\sqrt{N})F_N$ is unitary. Hence the matrix $(1/N)F_N$ has inverse $\bar{F}_N$, and the signal sample vector $\mathbf{y}$ can be reconstructed from the (approximate) Fourier coef£cient vector $\mathbf{d}$ by $\mathbf{y} = \bar{F}_N\mathbf{d}$.*

Proof. To simplify the notation write ω for ω_N and label the columns of F_N from 0 to $N-1$. The kth column of F_N is then

$$\mathbf{h}_k = \begin{bmatrix} 1 & \omega^k & \omega^{2k} & \cdots & \omega^{(N-1)k} \end{bmatrix}^{\mathrm{T}}$$

Hence the inner product of the jth and kth columns of F_N is

$$\langle \mathbf{h}_j, \mathbf{h}_k \rangle = 1 + \omega^{j-k} + \omega^{2(j-k)} + \cdots + \omega^{(N-1)(j-k)} \tag{16}$$

since $\bar{\omega} = \omega^{-1}$. For $j = k$ this gives $\langle \mathbf{h}_j, \mathbf{h}_j \rangle = N$. Now suppose $j \neq k$ and write $u = \omega^{j-k}$. Then $u \neq 1$ because $0 < |j-k| < N$ and $\omega^p = 1$ only when p is an integer multiple of N. In this case the right side of (16) is a £nite geometric series

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

But $u^N = \omega^{N(j-k)} = 1$, 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

$$F_N\big(F_N\big)^H = NI_N\,, \tag{17}$$

where I_N is the $N \times N$ identity matrix. Since F_N is symmetric, we have $\big(F_N\big)^H = \bar{F}_N$. Hence the matrix $(1/N)F_N$ has inverse $\bar{F}_N$, as claimed. Equation (17) can be rewritten as

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

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

Corollary 2.3.

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

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

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

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

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

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

as predicted by Corollary 2.3.

3 Discrete Periodic Signals and Convolution

Consider a digital signal y of £nite duration with N values, say $y[0], y[1], \ldots, y[N-1]$. In the previous section we viewed y as a column vector

$$\mathbf{y} = \begin{bmatrix} y[0] \\ y[1] \\ \vdots \\ y[N-1] \end{bmatrix} \in \mathbb{C}^N. \tag{18}$$

and calculated the discrete Fourier transform (DFT) $\mathbf{d} = (1/N)F_N\mathbf{y}$ of $\mathbf{y}$. In this section we consider y as a function de£ned on the set $\{0, 1, \ldots, N-1\}$ and we will obtain one of the main applications of the DFT.

A basic operation in signal processing is to take a *moving average* of the signal. For example, we can replace each value $y[j]$ by the average of the values $y[j-1]$ and $y[j+1]$. This gives a new signal z with

$$z[j] = \frac{1}{2}(y[j-1] + y[j+1]). \tag{19}$$

There is a bug in formula (19), however. To calculate $z[0]$ or $z[N-1]$ we need the values $y[-1]$ and $y[N]$, which aren't available. We will solve this problem by using the *periodic extension* of y:

$$y[j+kN] = y[j] \quad \text{for } j = 0, 1, \ldots, N-1 \text{ and all integers } k \tag{20}$$

Thus we set $y[-1] = y[N-1]$ and $y[N] = y[0]$, since $-1 = N-1+N$ and $N = 0+N$. In terms of *modular arithmetic*, we have $y[m] = y[j]$ when $m \equiv j \pmod N$. Now formula (19) is well-de£ned. It can be written in a more cumbersome case-by-case way as

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

and

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

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

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

Formula (19) has two fundamental properties:

(linearity) The output signal z depends linearly on the input signal y.

(shift invariance) If the input signal y is shifted by t (with periodic extension), then the output signal z is also shifted by t (with periodic extension):

$$z[j+t] = \frac{1}{2}(y[j+t-1] + y[j+t+1])$$

for any £xed integer t and all integer values of j.

We will now analyze all linear transformations of signals that have these two properties. We assume that all signals are periodic of a £xed period N. De£ne the *shift operator* S by

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

Here $Sy[0] = y[N-1]$, since y is periodic. It is clear from the de£nition that S is linear and shift invariant. The operator S is invertible:

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

Thus formula (19) can be written as

$$z = \frac{1}{2}(S + S^{-1})y. \tag{21}$$

We shall prove that every linear shift-invariant transformation C can be expressed as a linear combination of powers of the shift operator S. We £rst observe that the property of shift-invariance for C is the same as

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

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 (18). 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 y corresponds to the standard basis vector $\mathbf{e}_k$. Then $y[j] = 1$ if $j + 1 = k$, and otherwise $y[j] = 0$ (note the index shift by one). Since $Sy[j] = y[j-1]$, we see that $Sy[j] = 1$ if $j = k$ and $Sy[j] = 0$ 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 £rst column of C be $[c_0, c_1, \dots, c_{N-1}]^T$. Then*

$$C = c_0 I + c_1 S + c_2 S^2 + \cdots + c_{N-1} S^{N-1}, \tag{22}$$

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

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

$$C\mathbf{e}_1 = c_0\mathbf{e}_1 + c_1\mathbf{e}_2 + \cdots + c_{N-1}\mathbf{e}_N\,. \tag{23}$$

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 (23) by S^{k-1} and use the property $S^{k-1}\mathbf{e}_1 = \mathbf{e}_k$, we obtain

$$\begin{aligned} C\mathbf{e}_k &= CS^{k-1}\mathbf{e}_1 \\ &= S^{k-1}C\mathbf{e}_1 \\ &= c_0 S^{k-1}\mathbf{e}_1 + c_1 S^{k-1}\mathbf{e}_2 + c_2 S^{k-1}\mathbf{e}_3 + \cdots + c_{N-1}S^{k-1}\mathbf{e}_N \\ &= c_0\mathbf{e}_k + c_1 S\mathbf{e}_k + c_2 S^2\mathbf{e}_k + \cdots + c_{N-1}S^{N-1}\mathbf{e}_k\,. \end{aligned}$$

This shows that the kth column of the matrix C is the same as the kth column of the matrix $c_0 I + c_1 S + c_2 S^2 + \cdots + c_{N-1}S^{N-1}$ for $k = 1, \dots, N$. Hence the two matrices are equal. ■

Example 3.3. Suppose $N = 3$ and $C = c_0 I + c_1 S + c_2 S^2$ 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 £rst column. Matrices of this form are called *circulant matrices*. For example, when $N = 4$ the averaging operation from (19) 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 $F_N = [\,\mathbf{h}_0\ \mathbf{h}_1\ \cdots\ \mathbf{h}_{N-1}\,]$ be the $N \times N$ Fourier matrix with columns

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

These column vectors are obtained by applying F_N to the standard basis:

$$\mathbf{h}_j = F_N\mathbf{e}_{j+1}.$$

Since S gives a circular permutation of the standard basis, we have

$$F_N S\mathbf{e}_j = F_N\mathbf{e}_{j+1} = \mathbf{h}_j.$$

But we can write

$$\mathbf{h}_j = \begin{bmatrix} 1 \\ \omega\,\omega^{j-1} \\ \omega^2\,\omega^{2(j-1)} \\ \vdots \\ \omega^{N-1}\,\omega^{(N-1)(j-1)} \end{bmatrix} = D_N \mathbf{h}_{j-1} = D_N F_N \mathbf{e}_j \,,$$

where

$$D_N = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \omega & 0 & \cdots & 0 \\ 0 & 0 & \omega^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \omega^{N-1} \end{bmatrix} \tag{24}$$

is a diagonal matrix with the consecutive powers of ω on the diagonal. This calculation shows that

$$F_N S \mathbf{e}_j = D_N F_N \mathbf{e}_j \quad \text{for } j = 1, \dots, N.$$

The vector on the left side of this equation in the jth column of $F_N S$, while the vector on the right side is the jth column of $D_N F_N$. Since these vectors are equal for $j = 1, \dots, N$, we obtain

$$F_N S = D_N F_N. \tag{25}$$

By Theorem 2.2 the Fourier matrix is invertible. Hence multiplying the right side of (25) on the right by F_N^{-1}, we obtain

$$F_N S F_N^{-1} = D_N. \tag{26}$$

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 and has eigenvalues the N complex numbers ω^k for $k = 0, 1, \dots, N-1$ (the Nth 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*

$$C = c_0 I + c_1 S + c_2 S^2 + \cdots + c_{N-1} S^{N-1}$$

and de£ne the polynomial $p(z) = c_0 + c_1 z + c_2 z^2 + \cdots + c_{N-1} z^{N-1}$. Let $p(D_N)$ be the diagonal matrix obtained by substituting D_N for z. Then C is diagonalized by the Fourier matrix:

$$F_N C F_N^{-1} = p(D_N). \tag{27}$$

Hence the eigenvalues of C are $p(\omega^k)$ for $k = 0, 1, \dots, N-1$.

Proof. Since (26) implies that $F_N S^k F_N^{-1} = D_N^k$ for all integers k, the matrix C satis£es the corresponding equation

$$F_N C F_N^{-1} = c_0 I + c_1 D_N + c_2 D_N^2 + \cdots + c_{N-1} D_N^{N-1}.$$

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 $1, \mathrm{i}, -1, -\mathrm{i}$, the eigenvalues of C are

$$p(1) = 1, \quad p(\mathrm{i}) = (1/2)(\mathrm{i} + \mathrm{i}^3) = 0,$$
$$p(-1) = (1/2)(-1 + (-1)^3) = -1, \quad p(-\mathrm{i}) = (1/2)(-\mathrm{i} + (-\mathrm{i})^3) = 0.$$

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 $c_0, \ldots, c_{N-1}$ so that

$$C = c_0 I + c_1 S + c_2 S^2 + \cdots + c_{N-1} S^{N-1}.$$

If we apply C to a periodic signal y, then we get the signal

$$Cy[j] = c_0 y[j] + c_1 y[j-1] + c_2 y[j-2] + \cdots + c_{N-1} y[j-N+1] \tag{28}$$

for $j = 0, 1, \ldots, N-1$. This shows that Cy is a *moving average* of the original signal y, generalizing the special case of (19). De£ne the function $f[k] = c_k$ for $k = 0, 1, \ldots, N-1$. Then (28) can be written as

$$Cy[j] = \sum_{k=0}^{N-1} f[k] y[j-k]. \tag{29}$$

We call the function Cy the *convolution* ("folding") of f and y and we write $Cy = f * y$. An alternate statement of Theorem 3.2 is the following:

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

We can now obtain the linear-£lter version of Theorem 3.5.

De£nition 3.7 (Fourier Transform)**.** If y is a periodic signal (of period N), then the *Fourier transform* of y is the signal $\hat{y}$ de£ned by

$$\hat{y}[k] = \sum_{j=0}^{N-1} y[j] \omega^{jk},$$

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

The £lter f corresponding to the circulant matrix C in (22) is de£ned by $f[k] = c_k$ for $k = 0, 1, \ldots, N-1$. The matrix-vector product $C\mathbf{y}$ becomes the convolution $f * y$ 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 $Cy = f * y$ be the convolution operator* (29) *on signals y that are periodic of period N. Then the Fourier transform of Cy is the pointwise product $\hat{f}\hat{y}$:*

$$\widehat{Cy}[k] = \hat{f}[k]\hat{y}[k] \quad \textit{for } k = 0, 1, \ldots, N-1. \tag{30}$$

Proof. Since equation (29) is the same as (28), we know that

$$C = f[0]I + f[1]S + f[2]S^2 + \cdots + f[N-1]S^{N-1}.$$

Now apply Theorem 27. In this case the polynomial

$$p(z) = f[0] + f[1]z + f[2]z^2 + \cdots + f[N-1]z^{N-1}.$$

Hence $p(\omega^k) = \hat{f}[k]$, by de£nition of the Fourier transform. It follows that the diagonal matrix $p(D_N)$ acts on the standard basis by

$$p(D_N)\mathbf{e}_k = \hat{f}[k-1]\mathbf{e}_k \quad \text{for } k = 1, 2, \ldots, N.$$

If y is a signal, then the Fourier transform $\widehat{Cy}$ corresponds to the vector

$$\begin{aligned} F_N C\mathbf{y} &= p(D_N)F_N\mathbf{y} \\ &= p(D_N)(\hat{y}[0]\mathbf{e}_1 + \hat{y}[1]\mathbf{e}_2 + \cdots + \hat{y}[N-1]\mathbf{e}_N) \\ &= \hat{f}[0]\hat{y}[0]\mathbf{e}_1 + \hat{f}[1]\hat{y}[1]\mathbf{e}_2 + \cdots + \hat{f}[N-1]\hat{y}[N-1]\mathbf{e}_N. \end{aligned}$$

The coef£cient of $\mathbf{e}_{k+1}$ in $F_N C\mathbf{y}$ is $\widehat{Cy}[k]$. The last equation shows that this coef£cient is $\hat{f}[k]\hat{y}[k]$ for $k = 0, 1, \ldots, N-1$. This proves (30). ■

Example 3.9. Consider the averaging operator (19) from the beginning of this Section:

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

where y is a periodic signal of length N. We can write this as $Cy = f * y$, where

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

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 $\hat{f}[k] = (1/2)(\omega^k + \omega^{-k})$. Thus

$$\widehat{Cy}[k] = \frac{1}{2}(\omega^k + \omega^{-k})\hat{y}[k] \quad \text{for } k = 0, 1, \ldots, N-1.$$

4 Fast Fourier Transform

The effectiveness of the 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

$$F_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad F_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -\mathrm{i} & -1 & \mathrm{i} \\ 1 & -1 & 1 & -1 \\ 1 & \mathrm{i} & -1 & -\mathrm{i} \end{bmatrix}.$$

De£ne

$$\widetilde{D}_2 = \begin{bmatrix} 1 & 0 \\ 0 & -\mathrm{i} \end{bmatrix}, \quad P_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then F_4 can be factored as a 4×4 matrix in the following block form:

$$F_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -\mathrm{i} & \mathrm{i} \\ 1 & 1 & -1 & -1 \\ 1 & -1 & \mathrm{i} & -\mathrm{i} \end{bmatrix} P_4 = \begin{bmatrix} F_2 & \widetilde{D}_2 F_2 \\ F_2 & -\widetilde{D}_2 F_2 \end{bmatrix} P_4.$$

Note that right multiplication by P_4 interchanges columns 2 and 3, and left multiplication by $\widetilde{D}_2$ multiplies the second row of F_2 by $-\,\mathrm{i}$. Let $\mathbf{c} = \begin{bmatrix} c[0] & c[1] & c[2] & c[3] \end{bmatrix}^{\mathrm{T}} \in \mathbb{C}^4$. Then

$$P_4\mathbf{c} = \begin{bmatrix} c[0] \\ c[2] \\ c[1] \\ c[3] \end{bmatrix} = \begin{bmatrix} \mathbf{c}_{\text{even}} \\ \mathbf{c}_{\text{odd}} \end{bmatrix} \quad \text{where} \quad \mathbf{c}_{\text{even}} = \begin{bmatrix} c[0] \\ c[2] \end{bmatrix}, \quad \mathbf{c}_{\text{odd}} = \begin{bmatrix} c[1] \\ c[3] \end{bmatrix}.$$

Hence

$$F_4\mathbf{c} = \begin{bmatrix} F_2 & \widetilde{D}_2F_2 \\ F_2 & -\widetilde{D}_2F_2 \end{bmatrix} \begin{bmatrix} \mathbf{c}_{\text{even}} \\ \mathbf{c}_{\text{odd}} \end{bmatrix} = \begin{bmatrix} F_2\mathbf{c}_{\text{even}} + \widetilde{D}_2F_2\mathbf{c}_{\text{odd}} \\ F_2\mathbf{c}_{\text{even}} - \widetilde{D}_2F_2\mathbf{c}_{\text{odd}} \end{bmatrix}. \tag{31}$$

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

$$\mathbf{c} = \begin{bmatrix} c[0] & c[1] & \ldots & c[2n-2] & c[2n-1] \end{bmatrix}^{\mathrm{T}}$$

of length $2n$. Let

$$\mathbf{c}_{\text{even}} = \begin{bmatrix} c[0] & c[2] & \ldots & c[2n-2] \end{bmatrix}^{\mathrm{T}}, \qquad \mathbf{c}_{\text{odd}} = \begin{bmatrix} c[1] & c[3] & \ldots & c[2n-1] \end{bmatrix}^{\mathrm{T}}.$$

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

Write $\omega = \mathrm{e}^{-2\pi\,\mathrm{i}\,/2n} = \mathrm{e}^{-\pi\,\mathrm{i}\,/n}$ and $z = \omega^2 = \mathrm{e}^{-2\pi\,\mathrm{i}\,/n}$. Then

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

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

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

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

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

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

$$\widetilde{D}_n = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \omega & 0 & \cdots & 0 \\ 0 & 0 & \omega^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \omega^{n-1} \end{bmatrix} \quad \text{(caution: } \omega^n = -1\text{)}. \tag{32}$$

Note that the diagonal of $\widetilde{D}_n$ only contains half of the $2n$th roots of 1; it is not the same as the matrix D_N in equation (24) which has all Nth roots of 1. Let P_{2n} be the permutation matrix that splits $\mathbf{c}$ into its even and odd components:

$$P_{2n}\mathbf{c} = \begin{bmatrix} \mathbf{c}_{\mathrm{even}} \\ \mathbf{c}_{\mathrm{odd}} \end{bmatrix}.$$

Then the equations for $F_{2n}\mathbf{c}$ can be written as

$$F_{2n}\mathbf{c} = \begin{bmatrix} F_n\mathbf{c}_{\mathrm{even}} + \widetilde{D}_n F_n \mathbf{c}_{\mathrm{odd}} \\ F_n\mathbf{c}_{\mathrm{even}} - \widetilde{D}_n F_n \mathbf{c}_{\mathrm{odd}} \end{bmatrix} = \begin{bmatrix} F_n & \widetilde{D}_n F_n \\ F_n & -\widetilde{D}_n F_n \end{bmatrix} P_{2n}\mathbf{c} \tag{33}$$

The *Fast Fourier Transform* algorithm calculates F_N when N is a power of 2 by iterating formula (33). For example, when $N = 256 = 2^8$ then (33) expresses $F_{256}\mathbf{c}$ in terms of F_{128} applied to signals of length 128. To calculate these Fourier transforms, we use (33) 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.

To determine the computational cost of the FFT algorithm, let $n = 2^k$, and de£ne $\phi(k)$ be the number of scalar multiplications needed to evaluate $F_n\mathbf{c}$ 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 $\mathbf{c}$ is a signal of length $2n = 2^{k+1}$, then calculating $F_{2n}\mathbf{c}$ using (33) requires $2\phi(k)$ multiplications to obtain $F_n\mathbf{c}_{\mathrm{even}}$ and $F_n\mathbf{c}_{\mathrm{odd}}$, followed by 2^k multiplications to obtain $\widetilde{D}_n F_n \mathbf{c}_{\mathrm{odd}}$. We are using the fact that $\tilde{D}_n$ is a diagonal matrix, so it only requires n multiplications to calculate $\widetilde{D}_n\mathbf{b}$ for any vector $\mathbf{b}$. The matrix P_{2n} just sorts the entries of $\mathbf{c}$; no arithmetic is needed to calculate $P_{2n}\mathbf{c}$. Thus

$$\phi(k+1) = 2\phi(k) + 2^k \tag{34}$$

We can calculate $\phi(k)$ recursively from (34), 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

$$\phi(k) = (k-1)2^{k-1} \quad \text{for all positive integers } k = 1, 2, 3, \ldots. \tag{35}$$

This formula, which we have just shown true for $k = 2$, 3, and 4, is easily veri£ed by induction: assuming it true for k and using (34), 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 (35), note that direct evaluation of $F_n\mathbf{c}$ as a matrix-vector product requires $n^2 = 2^{2k}$ scalar multiplications (n for each of the n components of $\mathbf{c}$). Take $k = 10$ and $n = 2^{10} = 1024$. Then direct evaluation of $F_n\mathbf{c}$ 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

1. Let N be a positive integer and set $\omega = \mathrm{e}^{-2\pi\,\mathrm{i}/N}$. View the columns of the Fourier matrix F_N as the functions $h_0, \ldots, h_{N-1}$ de£ned by $h_k[j] = \omega^{jk}$ (note that with this de£nition h_k is automatically periodic of period N.) Verify directly that each function h_k is an eigenfunction for the shift operator S, and determine the eigenvalue. Recall that S acts on a periodic function f by $Sf[j] = f[j-1]$.

2. Let C be the linear shift-invariant transformation $Cy[j] = y[j-1] - 2y[j] + y[j+1]$ for y a function periodic of period N.

   (a) Find the function f such that $Cy = f * y$. (HINT: Write C in terms of the shift operator.)

   (b) Find the Fourier transform of the function f in (a).

   (c) Suppose $N = 4$ and y corresponds to the vector $\mathbf{y} = [2\,3\,1\,5]^T \in \mathbb{C}^4$. Calculate the vectors corresponding to Cy and $\widehat{Cy}$.

3. 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 $C = \begin{bmatrix} 4 & * & * \\ 7 & * & * \\ 5 & * & * \end{bmatrix}$ satis£es $CS = SC$.

   (a) Write C as a polynomial in S. Use this to £ll in the missing entries in C:

$$C = \begin{bmatrix} 4 & \underline{\quad\quad} & \underline{\quad\quad} \\ \\ 7 & \underline{\quad\quad} & \underline{\quad\quad} \\ \\ 5 & \underline{\quad\quad} & \underline{\quad\quad} \end{bmatrix}$$

   (b) View vectors in $\mathbb{C}^3$ as periodic functions y on the integers: $y[j] = y[j+3]$ for all integers j. Let T be the linear transformation on such functions corrsponding to the matrix C above. Give explicit formulas (in terms of $y[0]$, $y[1]$, and $y[2]$) for $Ty[j]$ for $j = 0, 1, 2$.

   (c) Let F be the 3×3 Fourier matrix, and let $\omega = \mathrm{e}^{-2\pi\,\mathrm{i}/3}$. Let C be the matrix above. Find complex numbers λ_0, λ_1, and λ_2 so that $FCF^{-1} = \begin{bmatrix} \lambda_0 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{bmatrix}$.

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

4. Let $n = 2^k$. De£ne $\psi(k)$ 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.

   (a) Show that $\psi(1) = 2$ and that $\psi(k+1) = 2\psi(k) + 2(2^k - 1)$.

   (b) Use the recursion in (a) to calculate $\psi(k)$ for $k = 2, 3, 4$.

   (c) Prove by induction that $\psi(k) \le k2^k$ for all positive integers k.

   (d) 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 $(3/2)k2^k$.