Circulant Matrices: Theory and Application

Roseanna Ferguson 1200579

April 17, 2014

1 Introduction

Remark. For convenience an N-by-N matrix will have rows and columns in the set

$$\{0, 1, \cdots, N-1\}.$$

The notation, $U^* = \overline{U}^T$, is used for the conjugate transpose of a matrix U.

Definition 1.1. Circulant Matrix [12]
An N-by-N matrix whose elements satisfy $a_{m,n} = a_{k,l}$, whenever $n - m \equiv l - k \ modN$, is a circulant matrix.
It follows, a circulant matrix has the form

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}$$

and can be generated by the first row. To generate row r, we place a_i in column c, where $c = i + r \ modN$ and a_i is the element in the i-th column of the zero row. In view of this, we will denote the N-by-N circulant matrix, whose first row consists of the elements $a_0, a_1, a_2, \cdots, a_{N-1}$, by

$$circ(a_0, a_1, a_2, \cdots, a_{N-1}).$$

The structure of circulant matrices and their widespread application, from algebraic geometry to combinatorics, is one motivation to investigate them. In particular, the periodic nature of circulant matrices means they are used in applications such as signal and time series analysis. They display many attributes that are of interest such as; every circulant matrix is diagonalisable by the Fourier matrix and the N-by-N circulant matrices form a commutative ring. This essay is a brief introduction to the theory of circulant matrices.
We shall begin by covering the basic theory of the discrete finite Fourier transform through which it will transpire there exists a close link between the discrete finite Fourier transform and circulant matrices. This link will allow us to utilise the theory of the discrete finite Fourier transform in proving basic results about circulant matrices. We will consider two applications. Firstly, we will look at a general approach for finding roots of polynomials, in one variable, of degree 2, 3 and 4, using circulant matrices. Finally, we consider a method used to solve systems of linear equations whose structure is that of a circulant matrix.

2 Discrete Finite Fourier Transform

Most of the theorems, proofs and definitions in Sections 2 and 3, unless indicated otherwise, are based on those from [11].

[1] Although we approach the Fourier transform in this essay as a tool to facilitate the analysis of circulant matrices, it is a significant area of mathematics and is used in a wide variety of applications. We can describe TV signals, sound waves, mobile phone signals, stock values against time, voltage across a resistor and more using the Fourier transform. It decomposes a waveform into sinusoids, and because any waveform is the sum of sinusoids of different frequencies, the Fourier transform provides another representation of a waveform that is often easier to deal with. Among many other applications the Fourier transform is used to eliminate undesirable noise from signals and to solve differential equations.

Definition 2.1. Discrete Finite Fourier Transform, $\hat{\mathbf{z}} : \mathbb{C}^{\mathbf{N}} \to \mathbb{C}^{\mathbf{N}}$

Let $z = \begin{pmatrix} z(0) \\ z(1) \\ \vdots \\ z(N-1) \end{pmatrix} \in \mathbb{C}^N$. Then $\hat{z} \in \mathbb{C}^N$ is defined by $\hat{z} = \begin{pmatrix} \hat{z}(0) \\ \hat{z}(1) \\ \vdots \\ \hat{z}(N-1) \end{pmatrix}$, where

$$\hat{z}(m) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} z(n) \exp \frac{-2\pi i m n}{N},$$

for $m = 0, 1, \cdots, N-1$.

Remark. The discrete finite Fourier transform is a linear operator.

The discrete finite Fourier transform transforms one function into another. The domain of the discrete finite Fourier transform are functions of the form $f : D \to \mathbb{C}$ where $D = 0, 1, 2, \cdots, N-1$. Equivalently, they are functions defined on a discrete, finite set of points which we can view as being the points evenly distributed around a unit circle. This interpretation provides a natural periodicity, that will be discussed later. Each function can be fully defined by a column vector whose entries are the values of the function. It is therefore sufficient to analyse the effect of the discrete finite Fourier transform on the space $\mathbb{C}^N$.

$$\mathbb{C}^N = \left\{ \begin{pmatrix} z(0) \\ z(1) \\ \vdots \\ z(N-1) \end{pmatrix} : z(n) \in \mathbb{C},\ n = 0, 1, \cdots, N-1 \right\}.$$

2.1 Bases of $\mathbb{C}^{\mathbf{N}}$

A linear operator is uniquely determined by its affect on a basis. In this essay we will consider two bases for $\mathbb{C}^N$, the first of which is familiar.

Definition 2.2. The standard basis $\{\mathbf{e_m}\}_{\mathbf{m=0}}^{\mathbf{N-1}}$

$e_m = \begin{pmatrix} 0 & \cdots & 1 & 0 & \cdots & 0 \end{pmatrix}^T$ is the vector with 1 in the m-th row and zero elsewhere.

Definition 2.3. The Fourier basis $\{\mathbf{F_m}\}_{\mathbf{m=0}}^{\mathbf{N-1}}$

$F_m = \begin{pmatrix} F_m(0) & F_m(1) & \cdots & F_m(N-1) \end{pmatrix}^T$, where $F_m(n) = \dfrac{1}{\sqrt{N}} \exp \dfrac{2\pi imn}{N}$.

Theorem 2.1. *The Fourier basis is an orthonormal basis of $\mathbb{C}^N$.*

Proof. $\mathbb{C}^N$ is a vector space with respect to addition and scalar multiplication of vectors as well as an inner product space.
The inner product (,) is defined by

$$(z, w) = \sum_{n=0}^{N-1} z(n)\overline{w(n)}$$

and

the norm $\|\cdot\|$ is defined by

$$\|z\|^2 = (z, z) = \sum_{n=0}^{N-1} |z(n)|^2.$$

Recall that a set of vectors $\{F_m\}_{m=0}^{N-1}$ of $\mathbb{C}^N$ is orthonormal if:

$$(F_j, F_k) = \delta_{j,k} = \begin{cases} 1 & if\ j = k \\ 0 & if\ j \neq k. \end{cases}$$

For $j, k = 0, 1, \cdots, N-1$,

$$\begin{aligned} (F_j, F_k) &= \sum_{n=0}^{N-1} F_j(n)\overline{F_k(n)} \\ &= \sum_{n=0}^{N-1} \frac{1}{\sqrt{N}} \exp \frac{2\pi ijn}{N} \overline{\frac{1}{\sqrt{N}} \exp \frac{2\pi ikn}{N}} \\ &= \sum_{n=0}^{N-1} \frac{1}{\sqrt{N}} \exp \frac{2\pi ijn}{N} \frac{1}{\sqrt{N}} \exp \frac{-2\pi ikn}{N} \\ &= \frac{1}{N} \sum_{n=0}^{N-1} \left(\exp \frac{2\pi i(j-k)}{N} \right)^n. \end{aligned} \tag{1}$$

So if $j = k$, then (1) $\Rightarrow$

$$\|F_j\|^2 = (F_j, F_j) = \frac{1}{N} \sum_{n=0}^{N-1} 1 = 1.$$

If $j \neq k$, then $0 < |j-k| < N \Rightarrow \exp \dfrac{2\pi i(j-k)}{N} \neq 1$.
Observing (1) is a geometric series $\Rightarrow$

$$(F_j, F_k) = \frac{1}{N} \frac{1 - \left(\exp \frac{2\pi i(j-k)}{N} \right)^N}{1 - \exp \frac{2\pi i(j-k)}{N}}.$$

But

$$\left(\exp\frac{2\pi i(j-k)}{N}\right)^N = \exp 2\pi i(j-k) = (\exp \pi i)^{2(j-k)} = \left(-1^2\right)^{(j-k)} = 1$$

$$\Rightarrow (F_j, F_k) = 0.$$

$\{F_m\}_{m=0}^{N-1}$ are N orthonormal vectors therefore it follows the Fourier basis is an orthonormal basis of $\mathbb{C}^N$. $\square$

2.2 Matrix Representation of The Finite Fourier Transform, $\hat{\mathbf{z}} : \mathbb{C}^\mathbf{N} \to \mathbb{C}^\mathbf{N}$

The discrete finite Fourier transform is a linear operator and hence it can be expressed as a matrix. Suppose $z \in \mathbb{C}^N$. For $m = 0, 1, \cdots, N-1$,

$$\hat{z}(m) = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} z(n)\exp\frac{-2\pi imn}{N} = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} z(n)\left(\exp\frac{-2\pi i}{N}\right)^{mn} = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} z(n)\omega_N^{mn},$$

where $\omega_N = \exp\dfrac{-2\pi i}{N}$. So we have the following definition.

Definition 2.4. The N-by-N Fourier Matrix

$$\Omega_N = \frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \omega_N^2 & \cdots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \cdots & \omega_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix} \text{ where } \hat{z} = \Omega_N z.$$

Remark. The Fourier matrix:

- Is symmetric and unitary, so it follows it is non-singular.
- Is a Vandermonde matrix, hence [8]

$$det(\Omega_N) = \frac{1}{\sqrt{N}}\prod_{1\le i<j\le n-1}(\omega_N^j - \omega_N^i) \neq 0.$$

- Is the change of basis matrix from the standard basis to the Fourier basis.
- Has at most N distinct entries as $\omega_N^{mn} = \omega_N^{mn\ modN}$ but contains no zeros. The calculation $\hat{z} = \Omega_N z$ involves N^2 complex multiplications, so has complexity $O(N^2)$.

2.3 Inverse Fourier Transform

Definition 2.5. The Inverse Fourier Transform, $\check{\mathbf{z}} : \mathbb{C}^{\mathbf{N}} \to \mathbb{C}^{\mathbf{N}}$

Let $z = \begin{pmatrix} z(0) \\ z(1) \\ \vdots \\ z(N-1) \end{pmatrix} \in \mathbb{C}^N$. Then $\check{z} \in \mathbb{C}^N$ is defined by $\check{z} = \begin{pmatrix} \check{z}(0) \\ \check{z}(1) \\ \vdots \\ \check{z}(N-1) \end{pmatrix}$, where

$$\check{z}(m) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} z(n) \exp \frac{2\pi imn}{N},$$

for $m = 0, 1, \cdots, N-1$.

Matrix Representation of the Inverse Fourier Transform

Suppose $z \in \mathbb{C}^N$. Then for $m = 0, 1, \cdots, N-1$,

$$\check{z}(m) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} z(n) \exp \frac{2\pi imn}{N} = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} z(n) \left(\exp \frac{2\pi i}{N} \right)^{mn} = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} z(n) \overline{\left(\exp \frac{-2\pi i}{N} \right)^{mn}}.$$

It follows $\check{z} = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} z(n) \overline{\omega_N^{mn}}$ $(= \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} z(n) \overline{\omega_N^{nm}})$. Therefore $\overline{\Omega_N}$ is the matrix of $\check{z}$ where $\overline{\Omega_N}$ is the matrix obtained by taking complex conjugate of each entry of Ω_N. $\frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} z(n) \overline{\omega_N^{nm}}$ is the formula for the inverse of a unitary matrix, so to obtain this result we could have just observed Ω_N is unitary and symmetric.

Example 2.1. Use the Fourier matrix to calculate $\hat{z}$ for $z = \begin{pmatrix} 1 & -i & i & 1 \end{pmatrix}^T$. Then verify the inverse Fourier matrix by applying the formula $z = \overline{\Omega_N} \hat{z}$ to your answer, (Definitions 2.1 and 2.5 are an alternative method to using matrices).
Using the formula $\hat{z} = \Omega_N z$,

$$\hat{z} = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix} \begin{pmatrix} 1 \\ -i \\ i \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ i \\ 1-i \end{pmatrix}.$$

For the second part of the example,

$$\check{\hat{z}} = z = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ i \\ 1-i \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 \\ -2i \\ 2i \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ -i \\ i \\ 1 \end{pmatrix}.$$

2.4 Translation-Invariant Linear Operators

Before introducing the translation invariant linear operator, we need to extend the domain of the functions we are considering. We will now consider functions, $f : D \to \mathbb{C}$, where $D = \mathbb{Z}$. In addition, f is periodic with period N. Hence any function f we consider satisfies: $f(n+N) = f(n)$, $\forall\ n \in \mathbb{Z}$.

Definition 2.6. $\mathbf{R_k z}$ The translation of z by k
For $k \in \mathbb{Z}$, let $R_k z : \mathbb{Z} \to \mathbb{Z}$ be defined by $(R_k z)(n) = z(n-k)$, $\forall\ n \in \mathbb{Z}$.

The matrix representation of R_k is P^k, where P is the permutation matrix in Definition 2.7 below. A geometrical interpretation of the translations is to take the N-th roots of unity. These satisfy $z(n+N) = z(n)$, $\forall\ n \in \mathbb{Z}$ and applying R_k is equivalent to rotating this circle of points.

Definition 2.7. P
P is a permutation matrix [9], such that column c_i is column $c_{i-1\ modN}$ from I_N

$$P = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Remark. $P^{-1} = P^T$.

Example 2.2.

$$R_3 z = \begin{pmatrix} z(0-3) \\ z(1-3) \\ \vdots \\ z(N-1-3) \end{pmatrix} = \begin{pmatrix} z(-3) \\ z(-2) \\ \vdots \\ z(N-4) \end{pmatrix} = \begin{pmatrix} z(N-3) \\ z(N-2) \\ \vdots \\ z(N-4) \end{pmatrix}.$$

We now introduce the notion of the translation invariant linear operator.

Definition 2.8. Translation Invariant Linear Operator A $: \mathbb{C}^{\mathbf{N}} \to \mathbb{C}^{\mathbf{N}}$
A is a translation invariant linear operator if, $\forall z, w \in \mathbb{C}^N$ and $\forall \alpha \in \mathbb{C}$ it satisfies:

i $A(z+w) = Az + Aw$,

ii $A(\alpha z) = \alpha Az$,

iii $AR_k = R_k A \quad \forall\ k \in \mathbb{Z}$, where R_k is the translation by k on $\mathbb{C}^N$.

Remark. (iii) is equivalent to $AR_1 = R_1 A$. Each R_k is equivalent to applying R_1, k times so if A commutes with R_1 it does so $\forall\ k \in \mathbb{Z}$.

Theorem 2.2. *Let $A : \mathbb{C}^N \to \mathbb{C}^N$ be a translation invariant linear operator, then F_m is an eigenvector of A, for $m = 0, 1, \cdots, N-1$.*

Proof. Consider any vector from the Fourier basis and apply A to get AF_m. We know the Fourier basis $\{F_j\}_{j=0}^{N-1}$ is a basis of $\mathbb{C}^N$ which means we can express AF_m as a linear combination of the Fourier basis and $\exists\ \alpha_0, \alpha_1, \cdots, \alpha_{N-1}$ such that $AF_m = \sum_{k=0}^{N-1} \alpha_k F_k$.

Thus for $n = 0, 1, \cdots, N-1$,

$$(R_1 AF_m)(n) = \sum_{k=0}^{N-1} \alpha_k F_k(n-1) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \alpha_k \exp \frac{2\pi ik(n-1)}{N} = \sum_{k=0}^{N-1} \alpha_k \exp \frac{-2\pi ik}{N} F_k(n). \tag{2}$$

For $n = 0, 1, \cdots, N-1$,

$$(R_1 F_m)(n) = F_m(n-1) = \frac{1}{\sqrt{N}} \exp \frac{2\pi i m(n-1)}{N} = \exp \frac{-2\pi i m}{N} F_m(n).$$

Then using linearity of A,

$$(AR_1 F_m)(n) = \exp \frac{-2\pi i m}{N} (AF_m)(n) = \sum_{k=0}^{N-1} \alpha_k \exp \frac{-2\pi i m}{N} F_k(n). \tag{3}$$

Because A is translation invariant $(AR_1 F_m)(n) = (R_1 A F_m)(n)$. By comparing the coefficients in (2) and (3) we can see that for $k = 0, 1, \cdots, N-1$,

$$\alpha_k \exp \frac{-2\pi i m}{N} = \alpha_k \exp \frac{-2\pi i k}{N},$$

which can only be true if $\alpha_k = 0$ whenever $m \neq k$ and this implies $AF_m = \alpha_m F_m$. Therefore F_m is an eigenvector of A. $\square$

Theorem 2.3. *Let $A : \mathbb{C}^N \to \mathbb{C}^N$ be a translation invariant linear operator. The matrix of A with respect to the Fourier basis, $F = \{F_m\}_{m=0}^{N-1}$ of $\mathbb{C}^N$, is diagonal. Furthermore, the elements along the diagonal, λ_m for $m = 0, 1, \cdots, N-1$, are the eigenvalues of A corresponding to eigenvectors F_m.*

Proof. From Theorem 2.2, $AF_m = \lambda_m F_m$

$$\left.\begin{aligned} AF_0 &= \lambda_0 F_0 + 0F_1 + 0F_2 + \cdots + 0F_{N-1} \\ AF_1 &= 0F_0 + \lambda_1 F_1 + 0F_2 + \cdots + 0F_{N-1} \\ &\vdots \\ AF_{N-1} &= 0F_0 + 0F_1 + 0F_2 + \cdots + \lambda_{N-1} F_{N-1} \end{aligned}\right\} \Rightarrow \mathrm{A} = \begin{pmatrix} \lambda_0 & 0 & 0 & \cdots & 0 \\ 0 & \lambda_1 & 0 & \cdots & 0 \\ 0 & 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_{N-1} \end{pmatrix}.$$

$\square$

3 Circulant Matrices and the Fourier Transform

We are now equipped with sufficient theory to observe the link between circulant matrices and the discrete finite Fourier transform. First, recall Definition 1.1 of an N-by-N circulant matrix whose elements, $A = (a_{m,n})$, satisfy:

$$a_{m+N,n} = a_{m,n}, \qquad a_{m,n+N} = a_{m,n}, \qquad a_{m+1,n+1} = a_{m,n}.$$

Where the indices are the residues modulo N.

Theorem 3.1. *Let $A : \mathbb{C}^N \to \mathbb{C}^N$ be a translation invariant linear operator. The matrix of A with respect to the standard basis, $\{e_i\}_{i=0}^{N-1}$, is circulant.*

Proof. Note that the indices are the residues modulo N. We want to show that the elements of $A = (a_{j,k})$ satisfy $a_{m+1,n+1} = a_{m,n}$. $Ae_{n+1} = A \begin{pmatrix} 0 & \cdots & 1 & 0 & \cdots & 0 \end{pmatrix}^T$. Where 1 is in

the $n+1$-th position. $Ae_{n+1} = \begin{pmatrix} a_{0,n+1} \\ a_{1,n+1} \\ \vdots \\ a_{N-1,n+1} \end{pmatrix}$.
Finally, using the translation invariance of A, $AR_1 = R_1 A$, we obtain for all $m, n \in \mathbb{Z}$,

$$a_{m+1,n+1} = (Ae_{n+1})_{m+1,0} = (AR_1 e_n)_{m+1,0} = (R_1 A e_n)_{m+1,0} = (Ae_n)_{m,0} = a_{m,n}.$$

Hence A is circulant. □

Remark. By definition, a translation invariant linear operator commutes with R_k, for any k. P is the matrix representation of R_k and the matrix representation of a translation invariant linear operator is circulant in the standard basis. So from Theorem 3.1 it follows that any circulant matrix commutes with P, and hence all powers of P.

Theorem 3.2. *A linear operator, A, is translation invariant $\Leftrightarrow$ the matrix of A with respect to the standard basis is circulant.*

Proof. [4] In Theorem 3.1, we saw a translation invariant linear operator expressed as a matrix in the standard basis is circulant. It follows from the one-one correspondence between linear maps and matrices, that this matrix is unique.
Conversely, let $A = (\alpha_{i,j})$ be a circulant matrix. A linear map is uniquely determined by its action on a basis. Therefore, there is only one linear map where $Ae_j = \sum_{i=0}^{N-1} \alpha_{i,j} e_i$, for $j = 0, 1, \cdots, N-1$ such that $\alpha_{i,j}$ corresponds to the elements of the circulant matrix A.
It remains to show that $AR_k = R_k A \;\; \forall$ k $\in \mathbb{Z}$, where R_k is the translation by k on $\mathbb{C}^N$. If this holds for each of the standard basis vectors then it holds for all vectors in $\mathbb{C}^N$.
For $n = 0, 1, \cdots, N-1$, for $m = 0, 1, \cdots, N-1$,

$$AR_k e_n = \sum_{r=0}^{N-1} \alpha_{r,n} R_k e_r \qquad \text{so} \qquad AR_k e_n(m) = \alpha_{m+k,n}$$

$$\text{and} \qquad R_k A e_n = R_k \sum_{r=0}^{N-1} \alpha_{r,n} e_r \qquad \text{so} \qquad R_k A e_n(m) = \alpha_{m+k,n}.$$

So $AR_k = R_k A$ and the unique linear map corresponding to the circulant matrix is indeed a translation invariant linear operator. □

4 Eigenvalues and Eigenvectors of Circulant Matrices

Definition 4.1. [10] A matrix U is unitary if $U^{-1} = U^*$.
A matrix A is normal if $AA^* = A^*A$.

Theorem 4.1. *[3] Every N-by-N circulant Matrix is diagonalisable by the N-by-N Fourier matrix.*

Proof. Let A be a translation invariant linear operator. Let C be the matrix representing A with respect to the standard basis which is circulant, (Theorem 3.1). Let B be the matrix representing A with respect to the Fourier basis which is diagonal (Theorem 2.3). Finally, the Fourier matrix is the change of basis matrix from the standard basis to the Fourier basis, so

$$\Omega_N C \Omega_N^{-1} = B.$$

□

Remark. The Fourier matrix is unitary and symmetric, therefore it follows $\Omega_N^{-1} = \overline{\Omega_N}^T = \overline{\Omega_N}$. Hence, the above expression can be written $\Omega_N C \overline{\Omega_N} = B$.

Circulant matrices are similar to a diagonal matrix and similar matrices have the same eigenvalues and eigenvectors. Furthermore, the eigenvalues of a diagonal matrix are the elements along the diagonal.

Corollary. *All circulant Matrices are normal.*

Proof. From Theorem 3.25 in [10], A is normal $\Leftrightarrow$ A is diagonalisable by a unitary matrix. All circulant matrices are diagonalisable by the Fourier matrix by Theorem 4.1 and as previously remarked, the Fourier matrix is unitary. Therefore, all circulant matrices are normal. □

Theorem 4.2. *Let $A = circ(a_0, a_1, \cdots, a_{N-1})$, then $\lambda_m = \sum_{u=0}^{N-1} (\omega_N^m)^u a_{N-u \ modN}$ are the eigenvalues of A with corresponding eigenvectors F_m, for $m = 0, 1, \cdots, N-1$.*

Proof. Let the matrix $B = diag(\lambda_0, \lambda_1, \cdots, \lambda_{N-1})$ be the diagonal matrix of A with respect to the Fourier basis. From Theorem 4.1, $\Omega_N A \overline{\Omega_N} = B$.
The elements of the j-th row of $\Omega_N A$, for $k = 0, 1, \cdots, N-1$ are,

$$(\Omega_N A)_{j,k} = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \omega_N^{jn} a_{N-n+k \ modN}.$$

By multiplying the j-th row of $\Omega_N A$ by the j-th column of $\overline{\Omega_N}$ we obtain,

$$\lambda_j = \frac{1}{N} \sum_{k=0}^{N-1} \omega_N^{-kj} \sum_{n=0}^{N-1} \omega_N^{jn} a_{N-n+k \ modN} = \frac{1}{N} \sum_{k=0}^{N-1} \sum_{n=0}^{N-1} \omega_N^{j(n-k)} a_{N-(n-k) \ modN}.$$

Note $\omega_N^{j(n-k)} = \omega_N^{j(n-k) \ modN}$ and in the sum above each $n - k \equiv u \ modN$ occurs N times. Therefore,

$$\lambda_j = \frac{1}{N} \sum_{k=0}^{N-1} \sum_{n=0}^{N-1} \omega_N^{j(n-k)} a_{N-(n-k) \ modN} = \frac{1}{N} N \sum_{u=0}^{N-1} \omega_N^{ju} a_{N-u \ modN} = \sum_{u=0}^{N-1} \omega_N^{ju} a_{N-u \ modN}.$$

Finally, by Theorem 2.3 F_j is the corresponding eigenvector of λ_j. □

Example 4.1. Find the eigenvalues and eigenvectors of $circ(1, 2, 3, 4)$, using Theorem 4.2 and $\omega_4 = \exp \frac{-2\pi i}{4}$

$\lambda_0 = \sum_{u=0}^{3} a_{4-u \ mod4} = 10$ and $\lambda_1 = \sum_{u=0}^{3} (\exp \frac{-2\pi i}{4})^u a_{4-u \ mod4} = 10$

and $\lambda_2 = \sum_{u=0}^{3} (\exp \frac{-4\pi i}{4})^u a_{4-u \ mod4} = a_0 - a_3 + a_2 - a_1 = -2$

and $\lambda_3 = \sum_{u=0}^{3} (\exp \frac{-6\pi i}{4})^u a_{4-u \ mod4} = a_0 + ia_3 - a_2 - ia_1 = -2 + 2i$,

with corresponding eigenvectors F_0, F_1, F_2, F_3.

5 General Theory

Theorem 5.1. *[5] An N-by-N matrix, A, is circulant $\Leftrightarrow P^T AP = A$.*

Proof. Need to show that i, j-th element of A is the i, j-th element of $P^T AP$.
For $i, k = 0, 1, \cdots, N-1$,

$$(PA)_{i,k} = \sum_{j=0}^{N-1} P_{i,j}(A)_{j,k} = (A)_{i+1mod(N),k}.$$

For $i, k = 0, 1, \cdots, N-1$,

$$(PAP^T)_{i,k} = \sum_{j=0}^{N-1} (PA)_{i,j}(P^T)_{j,k} = (PA)_{i-1mod(N),k} = (A)_{i+1-1,k} = (A)_{i,k}.$$

Therefore $P^T AP = A$. $\square$

Remark. An N-by-N matrix is circulant $\Leftrightarrow AP = PA$. This is equivalent to Theorem 5.1 and follows from observing $P^{-1} = P^T$.

Theorem 5.2. *[5] The Inverse of a non-singular N-by-N circulant Matrix is also an N-by-N circulant Matrix.*

Proof. Let A be a non-singular N-by-N circulant matrix. By Theorem 5.1, A satisfies $AP = PA$. Multiplying both sides of this identity on the left by A^{-1} it follows,

$$A^{-1}AP = A^{-1}PA \Rightarrow P = A^{-1}PA.$$

Multiplying on the right by A^{-1} we get,

$$A^{-1}P = A^{-1}PAA^{-1} \Rightarrow A^{-1}P = A^{-1}P.$$

Therefore, by Theorem 5.1, the inverse of A is circulant.

$\square$

Remark. When finding the inverse of a circulant matrix only the first row needs to be computed.

Corollary. *The determinant of a square matrix is equal to the product of its eigenvalues.*

Proof. Let A be an N-by-N Matrix with eigenvalues $\lambda_0, \lambda_1, \cdots, \lambda_{N-1}$ then it follows,

$$det(A - xI) = (\lambda_0 - x)(\lambda_1 - x) \cdots (\lambda_{N-1} - x).$$

So setting x = 0,

$$det(A) = \lambda_0 \lambda_1 \cdots \lambda_{N-1}.$$

$\square$

Theorem 5.3. *[8] Let $C = circ(a_0, a_1, a_2, \cdots, a_{N-1})$, then*

$$det(C) = \prod_{m=0}^{N-1} \left(\sum_{u=0}^{N-1} (\omega_N^m)^u a_{N-u \ modN} \right).$$

Proof. From the previous corollary, the determinant of a square matrix is equal to the product of its eigenvalues. Let $C = circ(a_0, a_1, a_2, \cdots, a_{N-1})$. By Theorem 4.2, C has eigenvalues $\lambda_m = \sum_{u=0}^{N-1} (\omega_N^m)^u a_{N-u \ modN}$ for $m = 0, 1, \cdots, N-1$.
Therefore, $det(C) = \prod_{m=0}^{N-1} \left(\sum_{u=0}^{N-1} (\omega_N^m)^u a_{N-u \ modN} \right)$. □

Theorem 5.4. *[3] For $a_1, \cdots, a_{N-1} \in \mathbb{C}$ a general circulant matrix $circ(a_0, a_1, a_2, \cdots, a_{N-1})$ can be expressed as a polynomial in P.*

$$q(P) = a_0 I_N + a_1 P + a_2 P^2 + \cdots + a_{N-1} P^{N-1}.$$

Proof. First, I make the claim that elements, $(P^i)_{s,t}$, of the N-by-N matrix P^i are non-zero and equal one if and only if they satisfy $t - s \equiv i \ modN$. We prove this by induction on i. For $i = 0$, $P^0 = I_N$. Elements $(P^0)_{s,t}$ are non-zero when $s = t$ and hence $t - s \equiv 0 \ modN$. Assume the only non-zero elements of P^i satisfy $(P^i)_{s,t}$ where $t - s \equiv i \ modN$. Clearly, $P^{i+1} = PP^i$. For $r, q \in \{0, 1, \cdots, N-1\}$,

$$(PP^i)_{r,q} = \sum_{j=0}^{N-1} P_{r,j}(P^i)_{j,q} = (P^i)_{r+1 \ modN, q}.$$

By the induction hypothesis $(PP^i)_{r,q}$ is non-zero when $q - (r+1) \equiv i \ modN$ and so it follows when $(PP^i)_{r,q}$ is non-zero when r, q satisfy $q - r \equiv i + 1 \ modN$. Therefore by the principle of induction our the claim is true.
Take the general form of an N-by-N circulant matrix $C = circ(a_0, a_1, a_2, \cdots, a_{N-1})$ as in Definition 1.1. C is equivalent to the addition of N, N-by-N matrices, $M_0, M_1, \cdots, M_{N-1}$ where the elements in M_i are either a_i or 0 and the r, q-th element is non zero in at most one of the N matrices. In particular, $(M_i)_{s,t}$ is a_i when $t - s \equiv i \ modN$ otherwise it is zero. a_i occur precisely in the positions of the ones of the N-by-N permutation matrix P^i, therefore M_i is just a scalar multiple of P^i. We conclude that any circulant matrix can be written as the above polynomial. □

Example 5.1. To visualise this take the case when $N = 4$ and $C = circ(b_0, b_1, \cdots, b_3)$

$$C = \begin{pmatrix} b_0 & 0 & 0 & 0 \\ 0 & b_0 & 0 & 0 \\ 0 & 0 & b_0 & 0 \\ 0 & 0 & 0 & b_0 \end{pmatrix} + \begin{pmatrix} 0 & b_1 & 0 & 0 \\ 0 & 0 & b_1 & 0 \\ 0 & 0 & 0 & b_1 \\ b_1 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & b_2 & 0 \\ 0 & 0 & 0 & b_2 \\ b_2 & 0 & 0 & 0 \\ 0 & b_2 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & b_3 \\ b_3 & 0 & 0 & 0 \\ 0 & b_3 & 0 & 0 \\ 0 & 0 & b_3 & 0 \end{pmatrix}$$

$$= b_0 I_N + b_1 P + b_2 P^2 + b_3 P^3$$

Remark. Clearly the set of N-by-N circulant matrices form a vector space. We can say something stronger than this theorem, that is, as well as spanning the vector space of circulant matrices over the complex field, the collection of matrices $\{P^0 = I_N, P^1, P^2, \cdots, P^{N-1}\}$ is a basis of the N-by-N circulant matrices over $\in \mathbb{C}$.

Theorem 5.5. *[5] The set of N-by-N Circulant Matrices forms a commutative ring with respect to addition and multiplication of matrices.*

Proof. To show the set of N-by-N circulant matrices S, is a ring, we just need to show S is a sub-ring of the N-by-N matrices, R. By Proposition 2.2 from [6], $(S,+)$ is a subgroup of $(R,+)$. This is because the additive identity, the N-by-N zero matrix, satisfies $P0 = 0P = 0$ and hence by Theorem 5.1 is circulant. In addition, if A, B are N-by-N circulant matrices then they satisfy $AP = PA$ and $BP = PB$ by Theorem 5.1. So $(A + B)P = AP + BP = PA + PB = P(A + B)$ by distributivity of N-by-N matrices and again by Theorem 5.1, as $(A + B)P = P(A + B)$, $A + B$ is circulant and we have closure of addition.
It follows from Proposition 6.7 from [6], to show S is a sub-ring of R we now only need to check closure of multiplication and that the identity of N-by-N matrices is circulant.
As the N-by-N identity matrix I_N satisfies $I_N P = PI_N$ by Theorem 5.1 the identity matrix is circulant. To show closure we observe from Theorem 5.1, $P^T AP = A \Leftrightarrow A$ is circulant.

$$AB = P^T APP^T BP = P^T ABP$$

Therefore

$$AB = P^T ABP$$

and hence AB is circulant by Theorem 5.1. Therefore the set of N-by-N circulant matrices is closed under multiplication and it is therefore a sub-ring of the N-by-N matrices and hence a ring. To show the set of N-by-N matrices is a commutative ring it just remains to show multiplication of circulant matrices is commutative.
By Theorem 5.4 a general circulant matrix $circ(a_0, a_1, a_2, \cdots, a_{N-1})$ can be expressed as a polynomial in P, $q(P) = a_0 I_N + a_1 P + a_2 P^2 + \cdots + a_N - 1P^{N-1}$. From Theorem 5.1 we know that circulant matrices commute with the permutation matrix P, and hence it follows it commutes with powers of P. Therefore given two N-by-N circulant matrices A and B, expressing $A = q(P)$ and using the distributivity of matrix multiplication and addition we get,

$$\begin{aligned}
Bq(P) &= B(a_0 I_N + a_1 P + a_2 P^2 + \cdots + a_N - 1P^{N-1}) \\
&= a_0 BI_N + a_1 BP + a_2 BP^2 + \cdots + a_N - 1BP^{N-1} \\
&= a_0 I_N B + a_1 PB + a_2 P^2 B + \cdots + a_N - 1P^{N-1} B \\
&= (a_0 I_N + a_1 P + a_2 P^2 + \cdots + a_N - 1P^{N-1})B \\
&= q(P)B.
\end{aligned}$$

Therefore $AB = BA$.
Hence the set of N-by-N circulant matrices is commutative with respect to multiplication and is a commutative ring. □

Theorem 5.6. *[7] If $Pv = \overline{\lambda} v$. Then $q(P)v = q(\overline{\lambda})v$, where q is the polynomial in Theorem 5.5.*

Proof. By Theorem 4.2 the eigenvalues of a circulant matrix $C = circ(a_0, a_1, a_2, \cdots, a_{N-1})$ are given by: $\lambda_m = \sum_{u=0}^{N-1} (\omega_N^m)^u a_{N-u \ modN}$ for $m = 0, 1, \cdots, N - 1$. So the eigenvalues for $P = Circ(0, 1, 0, \cdots, 0)$ are $\overline{\lambda}_m = \exp \dfrac{-2\pi im}{N}$. Therefore, it is clear the eigenvalues for the general circulant matrix C, for $m = 0, 1, \cdots, N - 1$, are given by

$$\lambda_m = a_0 + a_1(\omega_N)^m + a_2(\omega_N)^{2m} + \cdots + a_N - 1(\omega_{Nm})^{N-1} = q(\overline{\lambda}_m)$$

Therefore $q(\lambda_m)$ is an eigenvalue of $C = q(P)$ with corresponding eigenvector F_m. □

Remark. Theorem 5.6 is true for general square matrices. For convenience, I have chosen to prove this specific case only.

6 Application 1: Solving Polynomials

[7] The applications of circulant matrices are numerous. It is because the concept of solving polynomials is so elementary and hence so accessible that this particular application is so appealing. The appearance of circulant matrices in this topic demonstrates how they can arise in the foundations of mathematics and hence must permeate through the rest of mathematics. Circulant matrices provide a more unified approach to solving polynomials. To demonstrate this method we will look at the process involved in solving general polynomials of degree 2, 3 and 4. The general idea is to find the circulant whose characteristic polynomial is the polynomial whose roots we wish to find. Once we have determined the elements of this particular circulant matrix we can calculate its eigenvalues and hence the roots of our original polynomial using Theorem 4.2.

Quadratic Polynomials

In this section we will solve a general quadratic equation and hence produce the quadratic formula. This simple case demonstrates the method of solving polynomials using circulant matrices which will then be generalised for the cases of degree 3 and 4.
Consider the general monic quadratic polynomial $t^2 + \alpha t + \beta$ and a 2 x 2 circulant matrix $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ with characteristic polynomial $x^2 - 2ax + a^2 - b^2$. We want to find the elements, a and b, in terms of the coefficients of the general polynomial and hence find the circulant matrix whose characteristic polynomial is equal to the general polynomial. Therefore, equating the coefficients of the general polynomial and the characteristic polynomial it follows,

$$\left.\begin{aligned} -2a &= \alpha \\ a^2 - b^2 &= \beta \end{aligned}\right\} \qquad \text{Solving this} \Rightarrow \qquad \begin{aligned} a &= \frac{-\alpha}{2} \\ b &= \pm\sqrt{\frac{\alpha^2}{4} - \beta}. \end{aligned}$$

Both solutions of b produce the same roots, so taking the positive square root of b and substituting a and b into our general circulant matrix, we get

$$C = \begin{pmatrix} \dfrac{-\alpha}{2} & \sqrt{\dfrac{\alpha^2}{4} - \beta} \\ \sqrt{\dfrac{\alpha^2}{4} - \beta} & \dfrac{-\alpha}{2} \end{pmatrix}.$$

From Theorem 4.2 the formula, $q(t) = \dfrac{-\alpha}{2} + t\sqrt{\dfrac{\alpha^2}{4} - \beta}$, where t is a square root of unity, generates the eigenvalues of C and hence the roots of the general quadratic equation. So we have,

$$q(1) = \frac{-\alpha}{2} + \sqrt{\frac{\alpha^2}{4} - \beta} \qquad \text{and} \qquad q(-1) = \frac{-\alpha}{2} - \sqrt{\frac{\alpha^2}{4} - \beta},$$

the quadratic formula.

For finding the roots of polynomials of degree $n > 2$ we shall use the following result in order to simplify a general polynomial.

Theorem 6.1. *[7] In general for $p(x) = x^n + \alpha_{n-1}x^{n-1} + \alpha_{n-2}x^{n-2} + \cdots$ we can eliminate the term of degree $n-1$ by making the linear change of variable $y = x - \dfrac{\alpha_{n-1}}{n}$.*

Cubic Polynomials

The approach used to find the roots of a quadratic polynomial generalises to finding the roots of cubic polynomials.
Consider the monic cubic polynomial $t^3 + \alpha t^2 + \beta t + \gamma$. By Theorem 6.1, it is possible to make a linear change of variable in the general cubic polynomial so that it is written as $t^3 + \beta t + \gamma$, with no t^2 term.
So we consider a general 3-by-3 circulant matrix, whose characteristic polynomial is $x^3 - b^3 - c^3 - 3bcx$ with no x^2 term.

$$\begin{pmatrix} 0 & b & c \\ c & 0 & b \\ b & c & 0 \end{pmatrix}.$$

As in the quadratic case we equate the coefficients of the characteristic equation with the general polynomial to identify the elements b and c of the relevant circulant matrix.

$$\left.\begin{aligned} b^3 + c^3 &= -\gamma \\ 3bc &= -\beta \end{aligned}\right\} \quad \Rightarrow \quad \begin{aligned} b^3 + c^3 &= -\gamma \\ b^3c^3 &= \frac{-\beta^3}{27}. \end{aligned}$$

Observe that $b^3 + c^3$ and b^3c^3 are solutions to the quadratic $x^2 + \gamma - \dfrac{\beta^3}{27}$ which has solutions

$$x = \frac{-\gamma \pm \sqrt{\gamma^2 + \dfrac{4\beta^3}{27}}}{2}.$$

Set $b = x$ and $c = \dfrac{-\beta}{sb}$ and use the polynomial $q(t) = ct^2 + bt$ to generate the eigenvalues of C (the roots of the general cubic polynomial). Note all choices of b result in the same roots.

Quartic Polynomials

Consider the monic quartic polynomial $t^4 + \alpha t^3 + \beta t^2 + \gamma t + \delta$. We make a change of variables (Theorem 6.1) such that the t^3 term disappears and we obtain the general quartic $t^4 + \beta t^2 + \gamma t + \delta$.
Assuming there is not a change of variable such that β, γ and δ all vanish. Consider a general 4-by-4 circulant matrix.

$$\begin{pmatrix} 0 & b & c & d \\ d & 0 & b & c \\ c & d & 0 & b \\ b & c & d & 0 \end{pmatrix}.$$

With characteristic polynomial

$$x^4 - (4bd + 2c^2)x^2 - 4c(b^2 + d^2)x + c^4 - b^4 - d^4 - 4bdc^2 + 2b^2d^2.$$

This equals the general polynomial if the following hold.

$$4bd + 2c^2 = -\beta \qquad \text{and} \qquad 4c(b^2 + d^2) \qquad \text{and} \qquad c^4 - b^4 - d^4 - 4bdc^2 + 2b^2d^2 = \delta.$$

Observe the first two equations give us b^2d^2 and $b^2 + d^2$ in terms of c. By substituting into the third we obtain a cubic polynomial in c^2,

$$c^6 + \frac{\beta}{2}c^4 + (\frac{\beta^2}{16} - \frac{\delta}{4})c^2 - \frac{\gamma^2}{64} = 0.$$

We can solve this by using our circulant matrix for a general cubic equation, which we found in the last section, to solve for the roots of this polynomial and find c. We then generate the eigenvalues of the circulant matrix using $q(t) = bt + ct^2 + dt^3$ giving:

$$q(\exp\frac{-2\pi i0}{N}) = q(1) = b + c + d \qquad \text{and} \qquad q(\exp\frac{-2\pi i}{4}) = q(-i) = -b + c - d$$
$$q(\exp\frac{-4\pi i}{4}) = q(-1) = -c + i(b - d) \qquad \text{and} \qquad q(\exp\frac{-6\pi i}{4}) = q(i) = -c - i(b - d).$$

7 Application 2: Solving Systems of Linear Equations using the Fast Fourier Transform

Most of the theorems, proofs and definitions in this section, unless indicated otherwise are based on those from [11]. Being armed with the theory of circulant matrices allows us to increase the efficiency with which computers solve equations that exhibit a particular structure.

7.1 Fast Fourier Transform

Before applying the theory of circulant matrices to solving a system of equations, we need to cover some of the basics of the fast Fourier transform. To simplify this overview we will assume that we are considering Ω_N where N is a power of two. This will allow us to use the Cooley-Tukey formula.

Definition 7.1. Cooley-Tukey formula

$$\Omega_N = \begin{pmatrix} I_{\frac{N}{2}} & D_{\frac{N}{2}} \\ I_{\frac{N}{2}} & D_{\frac{N}{2}} \end{pmatrix} \begin{pmatrix} \Omega_{\frac{N}{2}} & 0 \\ 0 & \Omega_{\frac{N}{2}} \end{pmatrix} K_N.$$

$I_{\frac{N}{2}}$ is the $\frac{N}{2}$x$\frac{N}{2}$ identity matrix and $D_{\frac{N}{2}}$ is the diagonal matrix $\text{diag}(1, \omega_N, \omega_N^2, \cdots, \omega_N^{\frac{N-2}{2}})$ and K_N is the permutation matrix which puts even rows before odd. We can then decompose further to $\Omega_{\frac{N}{4}}$ then $\Omega_{\frac{N}{8}}$ and so on.

7.2 How does the fast Fourier transform affect the order of complexity?

As mentioned previously, the Fourier matrix contains no zeros and there are N^2 complex multiplications involved in the calculation $\hat{z} = \Omega_N z$. For large N, this calculation takes a significant amount of computer power and time. Therefore, it is of interest to reduce the number of complex multiplications in order to speed up the process of finding a solution.

Theorem 7.1. *Let $N = 2^l$. The number of complex multiplications using the fast Fourier transform is at most $\frac{N}{2} log_2 N$.*

Proof. By induction. Let $l = 1$ and $z = \begin{pmatrix} z(0) \\ z(1) \end{pmatrix}$. Then

$$\hat{z} = \Omega_N z = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} z(0) \\ z(1) \end{pmatrix} = \begin{pmatrix} z(0) + z(1) \\ z(1) - z(1) \end{pmatrix}$$

and no multiplication is required. Assume the theorem is true for l and proceed by induction. The number of complex multiplications required for a matrix of size $N = 2^l$ is at most $\dfrac{2^l l}{2}$. Using the Cooley-Tukey formula we need 2^l products using diagonal Ds to put together the half size products from the matrix of size $N = 2^l$. So we need at most $2^l + 2^l l = \dfrac{2^{l+1}(l+1)}{2}$ complex multiplications. Therefore the theorem follows by induction. □

7.3 Using Fast Fourier Transform to Solve Systems of Linear Equations

[2] Consider the system of equations

$$Cx = b$$

Where $C = circ(a_0, a_1, \cdots, a_{N-1})$ is an N-by-N circulant matrix. As we have ascertained earlier.

$$\overline{\Omega_N} diag(\lambda_0, \lambda_1, \cdots, \lambda_{N-1}) \Omega_N = C.$$

For $m = 0, 1, \cdots, N-1$

$$\lambda_m = \sum_{u=0}^{N-1} (\omega_N^m)^u a_{N-u \ modN}$$

are the eigenvalues of C.
If C is non singular then the inverse of C is also circulant (Theorem 5.2) and the Fourier Matrix is unitary.

$$C^{-1} = \overline{\Omega_N} diag(\lambda_0^{-1}, \lambda_1^{-1}, \cdots, \lambda_{N-1}^{-1}) \Omega_N.$$

So the solution is,

$$x = \overline{\Omega_N} diag(\lambda_0^{-1}, \lambda_1^{-1}, \cdots, \lambda_{N-1}^{-1}) \Omega_N b.$$

Therefore we can use the fast Fourier transform to find the solution using less complex multiplications. We must first use the fast Fourier transform to transform $\tilde{b} = \Omega_N b$. Then compute the eigenvalues of C using the fast Fourier transform. Calculate $\bar{b} = diag(\lambda_0^{-1}, \lambda_1^{-1}, \cdots, \lambda_{N-1}^{-1})\tilde{b}$ and finally, transform the vector $\bar{b}$ using the fast Fourier transform to obtain the solution $x = \overline{\Omega_N} \bar{b}$. We use the fast Fourier transform 3 times to obtain the solution therefore this is an algorithm with complexity $O(N log_2 N)$.

To conclude this essay I use the following quote.

> *Some mathematical topics, circulant matrices, in particular, are pure gems that cry out to be admired and studied with different techniques or perspectives in mind.* [8]

Whilst researching this topic, I found many interesting applications that involve circulant matrices and more advanced results than have been included in this essay and with further study circulant matrices could reveal much more than I have been able to cover.

References

[1] P J Bevel. The fourier transform. http://www.thefouriertransform.com/.

[2] Mingkui Chen. On the solution of circulant linear systems. *SIAM journal on numerical analysis*, 24(3):668–683, 1987.

[3] Philip J Davis. *Circulant Matrices*. John Wiley and Sons, 1979.

[4] Agelos Georgakopoulos and Daan Krammer. Ma106 linear algebra lecture notes, 2013.

[5] Franklin A Graybill. *Matrices with Applications in Statistics*. Wadsworth Inc., 1983.

[6] Derek Holt. Ma249 algebra ii lecture notes, 2014.

[7] Dan Kalman and James E White. Polynomial equations and circulant matrices. *The American Mathematical Monthly*, 108(9):821–840, 2001.

[8] Erwin Kra and Santiago R. Simanca. On circulant matrices.

[9] H Lütkepohl. *Handbook of Matrices*. John Wiley and Sons, 1996.

[10] Damiano Testa. Algebra i: Advanced linear algebra (ma251) lecture notes, 2013.

[11] Man Wah Wong. *Discrete Fourier Analysis*, volume 5. Springer Basel AG, 2011.

[12] Alun Wyn-jones. Circulants (extract).