BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES, Vol. 67, No. 6, 2019
DOI: 10.24425/bpasts.2019.130874

Discrete Fourier transform and permutations

S. HUI[1] and S.H. ŻAK[2*]

[1] Department of Mathematical Sciences, San Diego State University, San Diego, CA 92182, USA
[2] School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907, USA

Abstract. It is well known that the magnitudes of the coefficients of the discrete Fourier transform (DFT) are invariant under certain operations on the input data. In this paper, the effects of rearranging the elements of an input data on its DFT are studied. In the one-dimensional case, the effects of permuting the elements of a finite sequence of length N on its Discrete Fourier transform (DFT) coefficients are investigated. The permutations that leave the unordered collection of Fourier coefficients and their magnitudes invariant are completely characterized. Conditions under which two different permutations give the same DFT coefficient magnitudes are given. The characterizations are based on the automorphism group of the additive group $\mathbb{Z}_N$ of integers modulo N and the group of translations of $\mathbb{Z}_N$. As an application of the results presented, a generalization of the theorem characterizing all permutations that commute with the discrete Fourier transform is given. Numerical examples illustrate the obtained results. Possible generalizations and open problems are discussed. In higher dimensions, results on the effects of certain geometric transformations of an input data array on its DFT are given and illustrated with an example.

Key words: discrete Fourier transform (DFT), DFT invariants, Fourier coefficients, permutations, DFT coefficient magnitudes, circulant matrix, pattern recognition.

1. Introduction

It is well known that the magnitudes of the coefficients of the discrete Fourier transform (DFT) are invariant under certain operations on the input data. We are led to the study of how the rearrangement of a data set affects its discrete Fourier transform (DFT) coefficients by pattern recognition problems [11]. One algorithm that was analyzed uses the unordered magnitudes of the three-dimensional DFT coefficients to extract features from patterns. It is the invariance of the magnitudes of the DFT coefficients under certain geometric transformations that makes them useful.

Permutation of data occur naturally in many application areas. For example, the problem of recognition of permuted data is important in the study of mutation of DNA sequences; see for example [7]. Pairwise relations such as similarities between data points and pattern classification play an important role in many areas of machine learning [10, 13, 22]. Frequency hopping can be considered as the permutation in the frequency domain. An example where this is studied along with signal recognition is in [15]. An application of permutations and the Fourier transform to image encryption can be found in [14]. Our analysis depends heavily on the fact that the DFT commutes with certain subgroups of permutations. The study of operators that commute with the DFT is important in the study of DFT eigenvectors, see for example [21]. A somewhat related problem is the study of data sequences with a small number k of nonzero DFT coefficients, see for example [20]. This can be considered as the study of permutations of a spectrum with nonzero entries at exactly the first k positions.

The rearrangement of a finite sequence is equivalent to composing it with a permutation. The technical definitions of the terms that we use are reviewed in Section 2. This problem has been studied by researchers in matrix theory and signal processing, among other areas. For example, Chao [5] proved that a permutation commutes with the DFT if and only if the permutation is in the automorphism group of integers modulo N and is equal to its own inverse. This theorem is useful in the computation of eigenvalues for certain circulant matrices, see [2, 5]. In this paper, we use our results to generalize this theorem. Other results related to the DFT-permutation commutation problem can be found in [8, 25].

A related problem is that of rearranging the DFT coefficients which is dual to the problem of rearranging the input via the DFT $\leftrightarrow$ IDFT (inverse DFT) duality. The rearrangements of DFT coefficients have been studied in relation to speech signal encryption (see for example [4] and [17]), energy compaction [23], as well as pattern classification [11]. A closely related topic is the use of circulant matrices to encrypt speech signals [16], which is equivalent to multiplying the DFT coefficients by a unimodular sequence, that is, a sequence with modulus 1.

The paper's contributions are:

1. Using the structures of subgroups to analyze the effects of permutations on DFT.
2. We prove that the unordered collection of the DFT coefficients is invariant under a permutation if and only if the permutation is in the group of automorphisms of the integers modulo N. Furthermore, the DFT coefficients are permuted

*e-mail: zak@purdue.edu

Manuscript submitted 2018-09-13, revised 2019-03-11 and 2019-04-02, initially accepted for publication 2019-04-20, published in December 2019

by the inverse of the permutation. This is in Theorem 3 and generalizes the theorem in [5] mentioned above.
3. We show that the unordered collection of the magnitudes of the DFT coefficients is invariant under a permutation if and only if the permutation is in the product of the translation group and the automorphisms of the integers modulo N. This is Theorem 1.
4. We demonstrate that two permutations of a sequence have the same DFT coefficients' magnitudes if and only they are in the same left coset of the product group. This result is the content of Theorem 2. This result fails for right cosets.
5. We show that the unordered collection of the magnitudes of the multidimensional DFT coefficients is invariant when the data array is permuted by elements of a group that includes reflection, rotation, and other common geometric operations.

The paper is organized as follows. In Section 2, we introduce the notation and review the basic concepts. The results on permutations and the amplitudes of the DFT coefficients are presented in Section 3. In Section 4, we characterize the permutations that commute with the DFT. Examples are presented in Section 5. Generalizations for the one-dimensional case are given in Section 6. In Section 7, we present our results on higher dimensional data arrays. Section 8 contains the conclusions.

2. Mathematical preliminaries

In this section, we introduce the background material needed for further analysis. We give the necessary notation and, for the convenience of the reader, a few basic concepts to motivate the development. We refer the reader to [1, 12, 19, 26, 27] for complete details.

2.1. Motivation. The discrete Fourier transform (DFT) transforms a sequence of N complex numbers, $x(0)$, $x(1)$, …, $x(N-1)$ into another sequence of complex numbers, $\hat{x}(0), \hat{x}(1)$, …, $\hat{x}(N-1)$, where

$$\hat{x}(n) = \sum_{k=0}^{N-1} x(k) e^{-2\pi j \frac{kn}{N}} \tag{1}$$

We will use $[x]$ to denote the column vector of the values of $x(k)$, and, $[\hat{x}]$ is the column vector of the values of $\hat{x}(k)$. Let

$$\left[x^{(1)}\right] = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \end{bmatrix}^\top.$$

Applying (1) and then computing the magnitudes of the coefficients of the DFT of $\left[x^{(1)}\right]$, we obtain the set of the DFT coefficient magnitudes

$$A\left(x^{(1)}\right) = \left\{ \begin{matrix} 15.0000 & 4.2533 & 2.6287 & 2.6287 & 4.2533 \end{matrix} \right\}.$$

One can easily check that the magnitudes of the coefficients of the DFT of

$$\left[x^{(2)}\right] = \begin{bmatrix} 5 & 4 & 3 & 2 & 1 \end{bmatrix}^\top,$$

obtained by rearranging the elements of $\left[x^{(1)}\right]$, are the same, that is, $A\left(x^{(1)}\right) = A\left(x^{(2)}\right)$. On the other hand, the magnitudes of the coefficients of the DFT of

$$\left[x^{(3)}\right] = \begin{bmatrix} 5 & 3 & 4 & 1 & 2 \end{bmatrix}^\top,$$

also obtained by rearranging the elements of $\left[x^{(1)}\right]$, are

$$A\left(x^{(3)}\right) = \left\{ \begin{matrix} 15.0000 & 3.6903 & 3.3737 & 3.3737 & 3.6903 \end{matrix} \right\},$$

which differ from the previously computed magnitudes. If we now take

$$\left[x^{(4)}\right] = \begin{bmatrix} 5 & 3 & 4 & 2 & 1 \end{bmatrix}^\top,$$

then we obtain

$$A\left(x^{(4)}\right) = \left\{ \begin{matrix} 15.0000 & 3.3737 & 3.6903 & 3.6903 & 3.3737 \end{matrix} \right\},$$

We say that the sets $A\left(x^{(3)}\right)$ and $A\left(x^{(4)}\right)$ are equivalent because they have the same elements even though the ordering of these elements is different. We refer to the sets $A\left(x^{(i)}\right)$ as the sets of the (unordered) magnitudes of the DFT coefficients.

The objective of this paper to characterize the transformations that leave the unordered collection of Fourier coefficients and their magnitudes invariant.

2.2. Permutations. We first define some basic notation and review certain fundamental notions from abstract algebra. Let $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ denote the natural numbers (positive integers), the integers, the real numbers, and the complex numbers, respectively.

Let $N \in \mathbb{N}$ be fixed. For $a, b \in \mathbb{Z}$, we say that a is *congruent* to b modulo N if N divides $a - b$ and denote this by $a = b \bmod N$. Note that by simple arithmetic, we have that for every integer $a \in \mathbb{Z}$, there is a unique integer $b \in \{0, \ldots, N-1\}$ such that $a = b \bmod N$. For each $N \in \mathbb{N}$, let $\mathbb{Z}_N$ denote the collection of integers $\{0, \ldots, N-1\}$. Let $m, n \in \mathbb{Z}_N$. Then by the above, there are unique elements $u, v \in \mathbb{Z}_N$ such that

$$m + n = u \mod N \quad \text{and} \quad mn = v \mod N.$$

We follow the convention (and an abuse of notation) of using $m + n$ and mn to denote u and v in $\mathbb{Z}_N$, respectively. Thus defined, $\mathbb{Z}_N$ has an addition operation and a multiplication operation, which is commonly referred to as *modular arithmetic*. The usual properties of arithmetic on $\mathbb{Z}$ carry over to modular arithmetic on $\mathbb{Z}_N$ with two key exceptions:

1. If N is not a prime number, then there are nonzero elements m, n of $\mathbb{Z}_N$ whose product is zero in $\mathbb{Z}_N$, which is equivalent to the fact that mn is an integer multiple of N.
2. If $p \in \mathbb{Z}_N$ is relatively prime to N, then it has a multiplicative inverse in $\mathbb{Z}_N$ in the sense that for some $q \in \mathbb{Z}_N$, we have $pq = 1$ in $\mathbb{Z}_N$. This follows from the fact the since p is relatively prime to N, then there are integers q, $0 < q < N$, and s such that $pq + sN = 1$ (see [26]).

It follows that if $p \in \mathbb{Z}_N$ is relatively prime to N, then it has a multiplicative inverse in $\mathbb{Z}_N$ and the inverse is q as given above.

The set of integers in $\mathbb{Z}_N$ relatively prime to N is denoted $\mathbb{Z}_N^*$. It is easy to see that if $m, n \in \mathbb{Z}_N^*$, then $mn \in \mathbb{Z}_N^*$.

A *group* $(G, \cdot)$ is a nonempty set G along with a binary operation $\cdot$ with the following properties:

1. If $a, b \in G$, then $a \cdot b \in G$.
2. If $a, b, c \in G$, then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. There is a unique element $e \in G$ such that for every $a \in G$, $a \cdot e = e \cdot a = a$. The element e is called the *identity* of the group G.
4. For each element $a \in G$, there is an element $a^{-1} \in G$ such that $a \cdot a^{-1} = e$. The element a^{-1} is called the *inverse* of a.

If we have in addition to the above that $a \cdot b = b \cdot a$ for all $a, b \in G$, then $(G, \cdot)$ is called an *abelian group*. As an example, we note that $(\mathbb{Z}_N, +)$ is an abelian group. If the operation $\cdot$ on a set G is clearly specified, it is common practice to use G to denote the group $(G, \cdot)$. A subset $F \subset G$ forms a *subgroup* of the group G if F along with the operation $\cdot$ is itself a group. The following well known result is useful for showing that a subset is a subgroup:

Lemma 1. A subset F of a group G is a subgroup if and only if the following conditions hold:

1. If $a, b \in F$, then $a \cdot b \in F$.
2. For all $a \in F$, $a^{-1} \in F$.

Proof. See page 32 of [12]. □

If F is a subgroup of G and $a \in G$, then the subset

$$a \cdot F = \{a \cdot f : f \in F\}$$

is called a *left coset* of G and

$$F \cdot a = \{f \cdot a : f \in F\}$$

is called a *right coset* of G. A subgroup F of G is said to be *normal* if $a \cdot F = F \cdot a$ for all $a \in G$.

A *permutation* on $\mathbb{Z}_N$ is a bijection (or equivalently, one-to-one and onto) function from $\mathbb{Z}_N$ to $\mathbb{Z}_N$. Let S_N denote the collection of all permutations on $\mathbb{Z}_N$. We use $\circ$ to denote composition on S_N. That is, if $\rho, \xi \in S_N$, then $(\rho \circ \xi)(n) = \rho(\xi(n))$ for each $n \in \mathbb{Z}_N$. It follows that if $\rho, \xi \in S_N$, then $(\rho \circ \xi) \in S_N$ and thus $\circ$ defines a binary operation on S_N. It can be shown that $(S_N, \circ)$ is a group, called the *permutation group* of $\mathbb{Z}_N$. We note that it is not an abelian group in general. The identity element of this group is the identity map from $\mathbb{Z}_N$ to $\mathbb{Z}_N$ and the inverse of an element ρ of S_N is the inverse function ρ^{-1}.

Let $p \in \mathbb{Z}_N^*$. We define a function $\mu_p : \mathbb{Z}_N \to \mathbb{Z}_N$ by

$$\mu_p(k) = pk \mod N.$$

We have the following.

Lemma 2. We have $\mu_p \in S_N$ and $\mu_p^{-1} = \mu_{p^{-1}}$.

Proof. Let $p \in \mathbb{Z}_N^*$ and let q be its multiplicative inverse in $\mathbb{Z}_N$. Then for each $k \in \mathbb{Z}_N$,

$$k = k(qp) = (kq)p \mod N.$$

It follows that $\mu_p(kq) = k$ and since $k \in \mathbb{Z}_N$ is arbitrary, we conclude that μ_p in onto. Since every onto function from a finite set to itself is one-to-one, we conclude that μ_p is a bijection. Hence μ_p is a permutation of $\mathbb{Z}_N$ when p is in $\mathbb{Z}_N^*$, which completes the proof of the first part.

To see the second part, note that by definition, we have $\mu_q(k) = qk$. We have shown above that $\mu_p(qk) = k$. Therefore $\mu_p^{-1} = \mu_q = \mu_{p^{-1}}$. □

An *automorphism* on the group $\mathbb{Z}_N$ is a permutation $\xi \in S_N$ such that $\xi(m + n) = \xi(m) + \xi(n)$ for all $m, n \in \mathbb{Z}_N$. We let $\mathrm{Aut}(\mathbb{Z}_N)$ denote the collection of all automorphisms on $(\mathbb{Z}_N, +)$. Then by definition $\mathrm{Aut}(\mathbb{Z}_N) \subset S_N$ and is a subgroup of S_N:

Lemma 3. $(\mathrm{Aut}(\mathbb{Z}_N), \circ)$ is a group and it is the collection of the functions μ_p with p in $\mathbb{Z}_N^*$.

Proof. See [1]. □

For each $r \in \mathbb{Z}_N$, let

$$\alpha_r(k) = k + r \mod N.$$

Then α_r is a permutation on $\mathbb{Z}_N$ and the collection

$$T = \{\alpha_r : r \in \mathbb{Z}_N\}$$

is a subgroup of S_N. To see that T is a subgroup of S_N, we note that $\alpha_r \circ \alpha_s = \alpha_{r+s} \in T$ and $\alpha_r^{-1} = \alpha_{-r} \in T$ and apply Lemma 1. We refer to T as the *group of translations*. It follows that for $p \in \mathbb{Z}_N^*$ and $r \in \mathbb{Z}_N$, the function $\sigma_{p,r}$ defined by

$$\sigma_{p,r}(k) = \alpha_r \circ \mu_p(k) = pk + r \text{ in } \mathbb{Z}_N$$

is a permutation.

Let

$$H = \{\sigma_{p,r} : p \in \mathbb{Z}_N^* \text{ and } r \in \mathbb{Z}_N\}. \tag{2}$$

A simple computation shows that

$$\sigma_{p_1,r_1} \circ \sigma_{p_2,r_2} = \sigma_{p_1p_2,\, p_1r_2+r_1} \in H$$

and

$$\sigma_{p,r}^{-1} = \sigma_{p^{-1},\, -p^{-1}r} \in H.$$

Thus it follows from Lemma 1 that H is a subgroup of the group S_N. The elements of H are often called affine permutations. Note that $H = T \circ \mathrm{Aut}(\mathbb{Z}_N)$ is a product of the group of translations and the automorphism group of $\mathbb{Z}_N$.

2.3. Discrete Fourier transform (DFT). In this subsection, we introduce the notation and definitions related to the DFT that we use in the paper. Introductions to the DFT can be found in many

books, including [3, 18, 24]. The book [24] contains a nice discussion of DFT on $\mathbb{Z}_N$ and other abelian groups. The relation of the DFT and circulant matrices can be found in [6, 9].

For $x : \mathbb{Z}_N \to \mathbb{C}$, the DFT of x is defined by

$$\hat{x}(n) = \sum_{k \in \mathbb{Z}_N} x(k) e^{-2\pi j \frac{kn}{N}}. \tag{3}$$

Let

$$F(x) = \{\hat{x}(n) : n \in \mathbb{Z}_N\}$$

denote the collection of (unordered) DFT coefficients of x and

$$A(x) = \{|\hat{x}(n)| : n \in \mathbb{Z}_N\}$$

denote the (unordered) collection of their magnitudes.

Recall that the DFT matrix W is defined by

$$W_{n,m} = e^{-2\pi j \frac{mn}{N}}$$

for $0 \leq m, n \leq N-1$ and gives $[\hat{x}] = W[x]$, where $[x]$ and $[\hat{x}]$ are the column vectors of the values of $x(k)$ and $\hat{x}(k)$, respectively.

A circulant matrix is a square matrix such that each row, other than the first row, is a cyclic right shift of the previous row. It is well known (see for example [9]) that a matrix C is circulant if and only if

$$C = WDW^*, \tag{4}$$

where W^* denotes the conjugate transpose of W, and D is a diagonal matrix. In other words, the DFT diagonalizes all circulant matrices. Furthermore, the first row of C is precisely the DFT of the function formed by the diagonal elements of D.

For a vector (or any ordered finite sequence of numbers) v, we use $C(v)$ and $D(v)$ to denote, respectively, the circulant matrix and the diagonal matrix obtained by using the entries of v as the first row and the diagonal, respectively. With this notation, equation (4) gives

$$C(\hat{x}) = WD(x)W^*$$

3. Permutations and magnitudes of the DFT coefficients

In this section, we present our results on permutations and the magnitudes of the DFT coefficients. The following technical result is fundamental to the proofs of our other results.

Lemma 4. Let $x : \mathbb{Z}_N \to \mathbb{C}$ and let $\sigma_{p,r} \in H$. Then for $n \in \mathbb{Z}_N$,

$$\widehat{x \circ \sigma_{p,r}}(n) = e^{2\pi j \frac{rn}{pN}} \hat{x} \circ \sigma_{p^{-1},0}(n) = e^{2\pi j \frac{rn}{pN}} \hat{x} \circ \mu_p^{-1}(n),$$

where p^{-1} denotes the multiplicative inverse of p in $\mathbb{Z}_N$. In particular, if $r = 0$, then

$$\widehat{x \circ \mu_p} = \hat{x} \circ \mu_p^{-1}.$$

Furthermore, if $p^2 = 1 \bmod N$, then

$$\widehat{x \circ \mu_p} = \hat{x} \circ \mu_p.$$

Proof. Let $x : \mathbb{Z}_N \to \mathbb{C}$ and let $\sigma_{p,r} \in H$. Let $q = p^{-1}$ in $\mathbb{Z}_N$. Then for $m, n \in \mathrm{Z}_N$, we have $(mp)(qn) = mn$ in $\mathbb{Z}_N$. It follows that

$$\begin{aligned}
\widehat{x \circ \sigma_{p,r}}(n) &= \sum_{m \in \mathbb{Z}_N} x(mp + r) e^{-2\pi j \frac{mn}{N}} \\
&= e^{2\pi j \frac{rqn}{N}} \sum_{m \in \mathbb{Z}_N} x(mp + r) e^{-2\pi j \frac{(mp+r)qn}{N}} \\
&= e^{2\pi j \frac{rqn}{N}} \sum_{k \in \mathbb{Z}_N} x(k) e^{-2\pi j \frac{kqn}{N}} \\
&= e^{2\pi j \frac{rqn}{N}} \hat{x}(qn) \\
&= e^{2\pi j \frac{rp^{-1}n}{N}} \hat{x} \circ \mu_{p^{-1}}(n) \\
&= e^{2\pi j \frac{rn}{pN}} \hat{x} \circ \mu_p^{-1}(n).
\end{aligned}$$

In the above manipulations, we used the substitution $k = mp + r$ and the fact that $p\mathbb{Z}_N + r = \mathbb{Z}_N$ in $\mathbb{Z}_N$. □

The following corollary is now immediate.

Corollary 1. Let $\phi \in S_N$ be an arbitrary permutation. Then for each permutation σ in the coset $\phi \circ H$, there exist complex numbers $\xi_0, \ldots, \xi_{N-1}$ of absolute value 1 and $q \in \mathbb{Z}_N^*$ such that for $n \in \mathbb{Z}_N$,

$$\widehat{x \circ \sigma}(n) = \xi_n \widehat{x \circ \phi} \circ \mu_q(n).$$

In particular, $A(x \circ \sigma)$ is independent of the choice of σ in the coset.

Proof. Let $\phi \in S_N$ be and let $\sigma \in \phi \circ H$. Then there is $\sigma_{p,r} \in H$ such that $\sigma \in \phi \circ \sigma_{p,r}$. By Lemma 4,

$$\begin{aligned}
\widehat{x \circ \sigma}(n) &= e^{2\pi j \frac{rn}{pN}} \widehat{x \circ \phi} \circ \mu_p^{-1}(n) \\
&= \xi_n \widehat{x \circ \phi} \circ \mu_q(n).
\end{aligned}$$

where $\xi_n = e^{2\pi j \frac{rn}{pN}}$ and $q = p^{-1}$ in $\mathbb{Z}_N$. □

The next result characterizes the permutations that leave invariant the magnitudes of the DFT coefficients.

Theorem 1. Let σ be a permutation of $\mathbb{Z}_N$. Then $A(x \circ \sigma) = A(x)$ for all $x : \mathbb{Z}_N \to \mathbb{C}$ if and only if $\sigma \in H$.

Proof. By letting ϕ be the identity in Corollary 1, we see that if $\sigma \in H$, then $A(x \circ \sigma) = A(x)$ for all $x : \mathbb{Z}_N \to \mathbb{C}$.

Conversely, suppose $A(x\circ\sigma)=A(x)$ for all $x:\mathbb{Z}_N\to\mathbb{C}$. We first consider the case of $N=2$. The only possible rearrangements of a two element sequence $x=\{x(1),x(2)\}$ are $x=\{x(1),x(2)\}$ and $y=\{x(2),x(1)\}$. It is elementary that the DFT coefficients of the sequences x and y have the same magnitude. Thus $A(x\circ\sigma)=A(x)$ holds for all σ in the group S_2. Now observe that $H=\{\sigma_{1,0},\sigma_{1,1}\}=S_2$.

We next consider the case when $N\geq 3$. We first consider the case when $\sigma(0)=0$ and show that $\sigma=\mu_p$ for some $p\in\mathbb{Z}_N^*$. Let $p=\sigma(1)$. Fix $m\in\mathbb{Z}_N$, $m\neq=0,1$. Define $x:\mathbb{Z}_N\to\mathbb{C}$ by

$$x(k)=\begin{cases}e^{2\pi jk/N} & \text{if } k=0,\ p,\sigma(m)\\ 0 & \text{otherwise.}\end{cases}$$

Then it is clear that $\hat{x}(1)=3$. We have

$$\begin{aligned}\widehat{x\circ\sigma}(n) &= \sum_{k\in\mathbb{Z}_N} x\circ\sigma(k)e^{-2\pi j\frac{kn}{N}}\\ &= 1+e^{2\pi j\frac{p}{N}}e^{-2\pi j\frac{n}{N}}+e^{2\pi j\frac{\sigma(m)}{N}}e^{-2\pi j\frac{mn}{N}}\\ &= 1+e^{2\pi j\frac{p-n}{N}}+e^{2\pi j\frac{\sigma(m)-mn}{N}}.\end{aligned}$$

It follows that $\left|\widehat{x\circ\sigma}(n)\right|\leq 3$. Since $A(x\circ\sigma)=A(x)$ by assumption and $\hat{x}(1)=3$, we must have $\left|\widehat{x\circ\sigma}(n)\right|=3$ for some n, which is only possible if

$$e^{2\pi j\frac{p-n}{N}}=1 \text{ and } e^{2\pi j\frac{\sigma(m)-mn}{N}}=1$$

simultaneously. The first equality gives $n=p \bmod N$ and the second equality gives $\sigma(m)=mn \bmod N$. Therefore $\sigma(m)=mp \bmod N$. Since $m\neq 0,1$ is arbitrary, and $\sigma(0)=0$ and $\sigma(1)=p$ by assumption, we conclude that $\sigma(m)=mp$ for all $m\in\mathbb{Z}_N^*$. Since σ is a permutation on $\mathbb{Z}_N$, we must have $p\in\mathbb{Z}_N^*$ because $p\mathbb{Z}_N\neq\mathbb{Z}_N$ otherwise.

We next consider the general case. Suppose $r=\sigma(0)$. Let $\alpha(k)=k-r$ in $\mathbb{Z}_N$. Then α is a permutation on $\mathbb{Z}_N$ and thus $x\circ\alpha$ is a complex valued function on $\mathbb{Z}_N$. By assumption, $A(x\circ\alpha\circ\sigma)=A(x\circ\alpha)$. By Lemma 4, or by a simple computation, we see that $A(x\circ\alpha)=A(x)$. We have by definition that $\alpha\circ\sigma(0)=r-r=0$ and so the special case we proved above applies to show that $\alpha\circ\sigma=\mu_p$ for some $p\in\mathbb{Z}_N$ in $\mathbb{Z}_N^*$. It follows that $\sigma(m)=\alpha^{-1}\circ\mu_p(m)=mp+r$ for $m\in\mathbb{Z}_N$. The proof is complete. □

Note that each permutation σ can also be considered as a sequence $[\sigma(0)\cdots\sigma(N-1)]$. Then the above theorem shows that for every $\sigma\in H$,

$$A(\sigma)=A(\sigma^2)=A(\sigma^3)=\cdots, \tag{5}$$

where σ^n denotes the permutation obtained by composing σ with itself N times. However, the condition in equation (5) is in general not sufficient to guarantee that $\sigma\in H$. (See Conjecture 1 in Section 6.) The following theorem contains Theorem 1 as a special case (when σ_2 is the identity permutation) but its proof requires Theorem 1.

Theorem 2. Let σ_1 and σ_2 be permutations on $\mathbb{Z}_N$. Then $A(x\circ\sigma_1)=A(x\circ\sigma_2)$ for all $x:\mathbb{Z}_N\to\mathbb{C}$ if and only if σ_1 and σ_2 are in the same left coset of H in S_N.

Proof. We have from Corollary 1 that if σ_1 and σ_2 are in the same coset of H in S_N, then $A(x\circ\sigma_1)=A(x\circ\sigma_2)$. To prove the converse, we apply the assumption to the function $x\circ\sigma_1^{-1}$ to obtain $A(x\circ\sigma_1^{-1}\circ\sigma_2)=A(x)$. Then by Theorem 1, $\sigma_1^{-1}\circ\sigma_2\in H$ and it follows that both σ_1 and σ_2 are in $\sigma_1\in H$.

Remark 1. The above theorem fails for right cosets. See Section 5 for an example.

4. Permutations that commute with the DFT

In this Section, we give conditions under which the collection of DFT coefficients is invariant. Then we will use these to generalize a theorem (Theorem 1 in [5]) that characterizes permutation matrices that commute with the DFT matrix. Their proofs use the following fact:

Lemma 5. Let σ_1 and σ_2 be permutations on $\mathbb{Z}_N$. Then $\sigma_1=\sigma_2$ if and only if $y\circ\sigma_1=y\circ\sigma_2$ for all $y:\mathbb{Z}_N\to\mathbb{C}$.

Proof. Clearly if $\sigma_1=\sigma_2$, then $y\circ\sigma_1=y\circ\sigma_2$ for all $y:\mathbb{Z}_N\to\to\mathbb{C}$. Conversely, suppose $y\circ\sigma_1=y\circ\sigma_2$ for all $y:\mathbb{Z}_N\to\to\mathbb{C}$. Fix $m\in\mathbb{Z}_N$. Define y be setting $y(\sigma_1(m)))=1$ and y equal to 0 at the other coordinates. If $\sigma_2(m)\neq\sigma_1(m)$, then $y(\sigma_2(m)))=0$, which contradicts the assumption and so we must have $\sigma_2(m)=\sigma_1(m)$. □

Theorem 3. Let σ_1 and σ_2 be permutations on $\mathbb{Z}_N$. Then $\widehat{x\circ\sigma_2}=\hat{x}\circ\sigma_1$ for all $x:\mathbb{Z}_N\to\mathbb{C}$ if and only if σ_1 and σ_2 belong to $\mathrm{Aut}(\mathbb{Z}_N)$ and $\sigma_1=\sigma_2^{-1}$.

Proof. Suppose σ_1 and σ_2 belong to $\mathrm{Aut}(\mathbb{Z}_N)$ and $\sigma_2=\sigma_1^{-1}$. We have from Lemma 4 that if $\sigma_2\in\mathrm{Aut}(\mathbb{Z}_N)$, then $\widehat{x\circ\sigma_2}=\hat{x}\circ\sigma_2^{-1}$ for all $x:\mathbb{Z}_N\to\mathbb{C}$. Since $\sigma_1=\sigma_2^{-1}$ by assumption, we have $\hat{x}\circ\sigma_1=\widehat{x\circ\sigma_2}$.

Conversely, suppose $\hat{x}\circ\sigma_1=\widehat{x\circ\sigma_2}$ for all $x:\mathbb{Z}_N\to\mathbb{C}$. Then clearly $A(x\circ\sigma_2)=A(x)$ for all $x:\mathbb{Z}_N\to\mathbb{C}$ since $\hat{x}\circ\sigma_1$ merely rearranges the values of $\hat{x}$. Thus by Theorem 1, $\sigma_2=\sigma_{p,r}\in H$. By the assumption and Lemma 4,

$$\hat{x}\circ\sigma_1(n)=\widehat{x\circ\sigma_{p,r}}(n)=e^{2\pi j\frac{rn}{pN}}\hat{x}\circ\mu_p^{-1}(n).$$

By choosing x such that $\hat{x}(n)$ is real for all $n\in\mathbb{Z}_N$, we conclude that $e^{2\pi j\frac{rn}{pN}}=1$ for all $n\in\mathbb{Z}_N$, which is only possible if $r=0$ in $\mathbb{Z}_N$. Thus $\sigma_2=\sigma_{p,0}=\mu_p\in\mathrm{Aut}(\mathbb{Z}_N)$ and by Lemma 5, $\sigma_1=\mu_p^{-1}$. The proof is complete. □

Corollary 2. Let σ be a permutation on $\mathbb{Z}_N$. Then $F(x\circ\sigma)=$ $=F(x)$ for all $x:\mathbb{Z}_N\to\mathbb{C}$ if and only $\sigma\in\mathrm{Aut}(\mathbb{Z}_N)$.

Proof. Note that $F(x \circ \sigma) = F(x)$ if and only if the set of DFT coefficients of $x \circ \sigma$ is a rearrangement of the DFT coefficients of x, which is equivalent to the existence of a permutation α such that $\widehat{x \circ \sigma} = \hat{x} \circ \alpha$. Then by Theorem 3, $\sigma \in \mathrm{Aut}(\mathbb{Z}_N)$.

Conversely, if $\sigma \in \mathrm{Aut}(\mathbb{Z}_N)$, then by Lemma 4, $F(x \circ \sigma) = F(x)$. □

We now show that our results generalize the theorem in [5] that characterizes the permutation matrices that commute with the DFT matrix. We first introduce the required notation. Let σ be a permutation on $\mathbb{Z}_N$. The permutation matrix P^σ corresponding to σ is defined entry-wise by

$$P^\sigma_{m,n} = \begin{cases} 1 & \text{if } n = \sigma(m) \\ 0 & \text{otherwise,} \end{cases}$$

where $0 \le m, n \le N-1$. It is clear from the definition of P^σ that

$$[x \circ \sigma] = P^\sigma [x].$$

In matrix notation, we have

$$[\hat{x} \circ \sigma] = P^\sigma W[x] \text{ and } [\widehat{x \circ \sigma}] = WP^\sigma [x]. \tag{6}$$

Observe that by equation (6), $P^{\sigma_1} W = WP^{\sigma_2}$ is equivalent to $\hat{x} \circ \sigma_1 = \widehat{x \circ \sigma_2}$ for all $x : \mathbb{Z}_N \to \mathbb{C}$. Thus Theorem 3 can be restated as

Theorem 4. Let σ_1 and σ_2 be permutations on $\mathbb{Z}_N$. Then $P^{\sigma_1} W = WP^{\sigma_2}$ if and only if σ_1 and σ_2 belong to $\mathrm{Aut}(\mathbb{Z}_N)$ and $\sigma_1 = \sigma_2^{-1}$.

Theorem 4 generalizes the following theorem proved in [5] that characterizes the permutation matrices that commute with the DFT matrix.

Theorem 5. (Chao) Let σ be a non-identity permutation on $\mathbb{Z}_N$. Then $P^\sigma W = WP^\sigma$ if and only if σ belongs to the automorphism group, $\mathrm{Aut}(\mathbb{Z}_N)$, of the additive group of the integers module N, and σ is of order two.

To see that Theorem 3 implies Theorem 5, suppose $\sigma \in \mathrm{Aut}(\mathbb{Z}_N)$ and σ^2 is the identity. Then $\sigma^{-1} = \sigma$ and we can apply Theorem 4 to conclude that $P^\sigma W = WP^\sigma$. Conversely, if $P^\sigma W = WP^\sigma$, then Theorem 4 gives $\sigma \in \mathrm{Aut}(\mathbb{Z}_N)$ and $\sigma^{-1} = \sigma$, which is equivalent to the fact that σ^2 is the identity.

Since $P^{\sigma^{-1}} = [P^\sigma]^{-1}$, we have the following corollary of Theorem 4:

Corollary 3. For every $\sigma \in \mathrm{Aut}(\mathbb{Z}_N)$, $P^\sigma W P^\sigma = W$. Also, if P, Q are permutation matrices, then $PWQ = W$ if and only if $P \in \mathrm{Aut}(\mathbb{Z}_N)$ and $Q = P$.

5. Examples and discussion

In this Section, we give examples to illustrate our results and to show that Theorem 2 fails for right cosets of H. We discuss possible generalizations of the results in Section 6.

Example 1. In this example, we give an illustration of Corollary 2. Rather than giving sequences in $\mathbb{C}$ and their DFT, we provide a short MATLAB script that can be used by the interested reader to generate numerical examples. The script will generate all possible rearrangements of the input sequence by the automorphism group $\mathrm{Aut}(\mathbb{Z}_N)$ as columns of a matrix. In addition, we give one random permutation of the input sequence as the last column to illustrate the failure of the conclusion when the permutation is not given by $\mathrm{Aut}(\mathbb{Z}_N)$. To keep the script simple, we do not check that the randomly generated permutation is not in the $\mathrm{Aut}(\mathbb{Z}_N)$. However, the probability that a randomly generated permutation is in $\mathrm{Aut}(\mathbb{Z}_N)$ is at most $1/(N-1)!$. The script uses a random complex-valued (column) sequence of length 8 as input, which can be changed to an arbitrary sequence.

```
% Input sequence
x=randn([8 1])+j*randn([8 1]);
% Length of the sequence
N=length(x);
y=[]; % Initialize the matrix of
% rearrangements of x
% Generate all rearrangements
% of x given by the automorphism group
for k=1:N
   if gcd(k,N)==1
         y=[y x(mod(k*[0:N-1],N)+1)];
   end
end
%
% Append one random rearrangement of x
y=[y x(randperm(N))];
Input_and_rearrang=y
% Compute DFT
DFT_of_Rearrang=fft(Input_and_rearrang)
% Sort magnitudes
Sorted_mags=sort(abs(DFT_of_Rearrang))
```

Example 2. In this example, we illustrate Theorem 1. We use $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ to keep the length manageable. The elements 1 and 3 are relatively prime to 4 and so $\mathbb{Z}_4^* = \{0, 3\}$. It follows that the subgroup $H = \{\sigma_{1,0}, \ldots, \sigma_{1,3}\} \cup \{\sigma_{3,0}, \ldots, \sigma_{3,3}\}$ has eight elements. Since the S_4 has 24 elements and H has eight elements, H has three cosets, one of which being H itself (see [12, page 39]). We generate the left and right cosets of H by a simple computation, which are shown in Table 1 and Table 2, respectively. The elements corresponding to $\{\sigma_{1,0}, \ldots, \sigma_{1,3}\}$ and $\{\sigma_{3,0}, \ldots, \sigma_{3,3}\}$ are separated by horizontal lines in the tables. The permutations are listed in the form $[\sigma(0)\sigma(1)\sigma(2)\sigma(3)]$. For example, the 4-number group $[0\ 2\ 3\ 1]$ stands for the permutation $\sigma(0) = 0$, $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$. By inspection, one can see that the left cosets and the right cosets are distinct. (This implies that the group H is not normal.) The two permutations in small boxes in the first column of Table 1 form $\mathrm{Aut}(\mathbb{Z}_N)$. The permutations listed under each of these permutations are the translations of the permutations in the small boxes. The second and

Table 1
The group H and its left cosets in S_4

Left Coset 1 = H	Left Coset 2	Left Coset 3
0 1 2 3	1 0 2 3	0 3 1 2
1 2 3 0	0 2 3 1	3 1 2 0
2 3 0 1	2 3 1 0	1 2 0 3
3 0 1 2	3 1 0 2	2 0 3 1
0 3 2 1	1 3 2 0	0 2 1 3
1 0 3 2	0 1 3 2	3 0 2 1
2 1 0 3	2 0 1 3	1 3 0 2
3 2 1 0	3 2 0 1	2 1 3 0

Table 2
The group H and its right cosets in S_4

Right Coset 1 = H	Right Coset 2	Right Coset 3
0 1 2 3	1 0 2 3	0 2 3 1
1 2 3 0	2 1 3 0	1 3 0 2
2 3 0 1	3 2 0 1	2 0 1 3
3 0 1 2	0 3 1 2	3 1 2 0
0 3 2 1	3 0 2 1	0 2 1 3
1 0 3 2	0 1 3 2	1 3 2 0
2 1 0 3	1 2 0 3	2 0 3 1
3 2 1 0	2 3 1 0	3 1 0 2

the third columns of Table 1 are the cosets $[1\ 0\ 2\ 3] \circ H$ and $[0\ 3\ 1\ 2] \circ H$, respectively.

As an illustration, we compute the DFT of the function x on $\mathbb{Z}_4$ defined by $x(k) = k + 1$, or informally, $x = [1, 2, 3, 4]$. Note that $x(3) = 4$. We obtain for each $\sigma \in H$ that (to two decimal places)

$$A(x \circ \sigma) = \{10.00, 2.83, 2.00, 2.83\}.$$

For each σ in Left Coset 2,

$$A(x \circ \sigma) = \{10.00, 3.16, 0.00, 3.16\},$$

and for each σ in Left Coset 3,

$$A(x \circ \sigma) = \{10.00, 1.41, 4.00, 1.41\}.$$

This example illustrates the fact that each permutation in a left coset gives the same DFT coefficient magnitudes and that the DFT coefficient magnitudes are different for different cosets in general.

Note that $\sigma = [1\ 0\ 2\ 3]$ and $\sigma = [0\ 3\ 1\ 2]$ are both in Right Coset 2 but $\sigma = [1\ 0\ 2\ 3]$ is in Left Coset 2 while $\sigma = [0\ 3\ 1\ 2]$ is in Left Coset 3. Since the permutations in Left Coset 2 and Left Coset 3 give different DFT magnitudes as we have seen, we conclude that permutations in the right cosets of H do not necessarily give the same DFT magnitudes and this is an illustration that Theorem 2 fails for right cosets of H.

6. Generalizations

In this section, we discuss the possibility of generalizing the results of Section 3. More specifically, it would be useful to know how x and y are related if $|\hat{x}| = |\hat{y}|$ or $A(x) = A(y)$. Is there a subclass of functions on $\mathbb{Z}_N$ such that $|\hat{x}| = |\hat{y}|$ or $A(x) = A(y)$ implies that x and y are permutations of each other? This has important implications if speech signals are encrypted by transforming the signal with a unitary circulant matrix. We have the following very general result:

Theorem 6. Let $x, y : \mathbb{Z}_N \to \mathbb{C}$. Then $|\hat{x}| = |\hat{y}|$ if and only if there is a unitary circulant matrix U_c such that $[y] = U_c[x]$.

Proof. Suppose $[y] = U_c[x]$, where U_c is unitary and circulant. Then by equation (4), U_c can be expressed as $U_c = W\Lambda W^*$, where Λ is a diagonal matrix with unimodular entries on the diagonal. Then $[\hat{y}] = \Lambda[\hat{x}]$ and so $|\hat{x}| = |\hat{y}|$.

Now suppose $|\hat{x}| = |\hat{y}|$. Then $[\hat{y}] = \Lambda[\hat{x}]$, where Λ is a diagonal matrix with unimodular entries on the diagonal. It then follows that $[y] = (W\Lambda W^*)[x]$. It is clear that $W\Lambda W^*$ is unitary and circulant. □

We see that transforming a signal with a unitary circulant matrix changes the phase but not the magnitude of the DFT coefficients. Thus if additional information about the original signal can be obtained from the encrypted signal by knowing the magnitudes of the DFT coefficients, the integrity of the encryption may be compromised. Since there are uncountably many unitary circulant transformations, Theorem 6 is of limited use because without further assumptions the most one can say is that when $|\hat{x}| = |\hat{y}|$, then $[y] = U_c[x]$, where U_c is unitary and circulant (see Example 3). On the other hand, we have the following very specialized result, which states that a nonnegative sequence cannot have a flat amplitude spectrum unless it is a translation of a simple pulse. This hints at the possibility that if the original comes from a known special class of functions, one may be able to say more.

For each $n \in \mathbb{Z}_N$, define e_n on $\mathbb{Z}_N$ by setting $e_n(n) = 1$ and $e_n(m) = 0$ for all other $m \in \mathbb{Z}_N$.

Theorem 7. Let $x : \mathbb{Z}_N \to \mathbb{C}$ be nonnegative and let $a \geq 0$. Then $|\hat{x}(n)| = a$ for all $n \in \mathbb{Z}_N$ if and only if $x = ae_n$ for some $n \in \mathbb{Z}_N$.

Proof. Let $x : \mathbb{Z}_N \to \mathbb{C}$ be nonnegative and $|\hat{x}(n)| = a$ for all $n \in \mathbb{Z}_N$. Without loss of generality, let $a = 1$. Then $|\hat{x}| = |\hat{e_0}|$. By Theorem 6, there is a unitary circulant matrix U_c such that $[x] = U_c[e_0]$. Thus the first column of U_c is nonnegative. Since U_c is circulant, all entries of U_c are nonnegative. Since U_c is also unitary, the dot products of the distinct columns of U_c are 0 and contain all possible combinations of $x(m)x(n)$ for $m \neq n$. It follows that $x(m)x(n) = 0$ for $m \neq n$. Since $\hat{x}$ is nonzero, there is at least one $x(n) \neq 0$, which implies that $x(m) = 0$ for all $m \neq n$. Because $x(n) \geq 0$ and $|\hat{x}(m)| = 1$ for all m by assumption, we must have $x(n) = 1$ and it follows that $x = e_n$. The converse is obvious. □

Remark 2. Note that Theorem 7 fails if x is not non-negative. It is easy to verify that

$$[x] = \frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ -1 \\ -1 \end{bmatrix} \Leftrightarrow [\hat{x}] = \begin{bmatrix} -1 \\ 1 \\ 1 \\ 1 \end{bmatrix}.$$

The following result is contained in the proof of Theorem 7 but is also a simple consequence of it.

Corollary 4. A nonnegative matrix is unitary and circulant if and only if it is a permutation matrix corresponding to a translation.

Proof. Clearly, a permutation matrix that corresponds to a translation is nonnegative, unitary, and circulant. For the converse, we only have to note the first column of a matrix U is given by $U[e_0]$. If U is a nonnegative unitary circulant matrix, then by Theorem 7, its first column is $[e_n]$ for some $n \in \mathbb{Z}_N$. □

The following example shows that there is no straightforward generalization of Theorem 7 to the case of non-negative x, y such that $|\hat{x}| = |\hat{y}|$.

Example 3. Let

$$U_c = \frac{1}{2}\begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \text{ and } [x] = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

Then U_c is unitary and circulant and

$$[y] = U_c[x] = \begin{bmatrix} 1 \\ 1 \\ 3 \\ 1 \end{bmatrix}.$$

Thus $|\hat{x}| = |\hat{y}|$ by Theorem 6 but obviously x and y are not related by a permutation or any simple geometric transformation of the coordinates. One can also easily verify that

$$[\hat{x}] = \begin{bmatrix} 3 \\ 1 \\ -1 \\ 1 \end{bmatrix} \text{ and } [\hat{y}] = \begin{bmatrix} 3 \\ -1 \\ 1 \\ -1 \end{bmatrix}.$$

Based on some experimentation results, we conjecture the following:

Conjecture 1. If N is prime, then $\sigma \in H$ if and only if

$$A(\sigma) = A(\sigma^2) = A(\sigma^3) = \cdots.$$

Conjecture 2. Let $x, y : \mathbb{Z}_N \to \{0, 1\}$. Then
1. $|\hat{x}| = |\hat{y}|$ if and only if there is $\sigma \in T$ such that $y = x \circ \sigma$;
2. $A(x) = A(y)$ if and only if there is $\sigma_{p,r} \in H$ such that $y = x \circ \sigma_{p,r}$.

7. Permutations and magnitudes of the DFT coefficients in higher dimensions

Some of the results we obtained so far carry over to higher dimensional input data, that is, data arrays. To present the main ideas without the more complicated notation for the higher dimensions, we only state and prove the results on the magnitudes of a 2-dimensional DFT coefficients when the entries of a 2-dimensional data array are permuted. The same results hold for higher dimensions with similar proofs. The results we have are not as complete as the one dimensional case but they are useful in image pattern classification problems. For example, we show later in this section that our results contain as special cases that the set of magnitudes of a 2-dimensional DFT coefficients of an image are invariant when the image is reflected, rotated, or cyclically shifted.

Example 4. In Fig. 1 we show a sample image and the images transformed by a combination of the transformations covered under our results. The original color image contains 300×200 pixels, which we consider as a 300×200×3 data array. The transformed image is obtained by applying in sequence the following operations:
1. flip the image upside down;
2. shift the image up cyclically by 110 pixels;

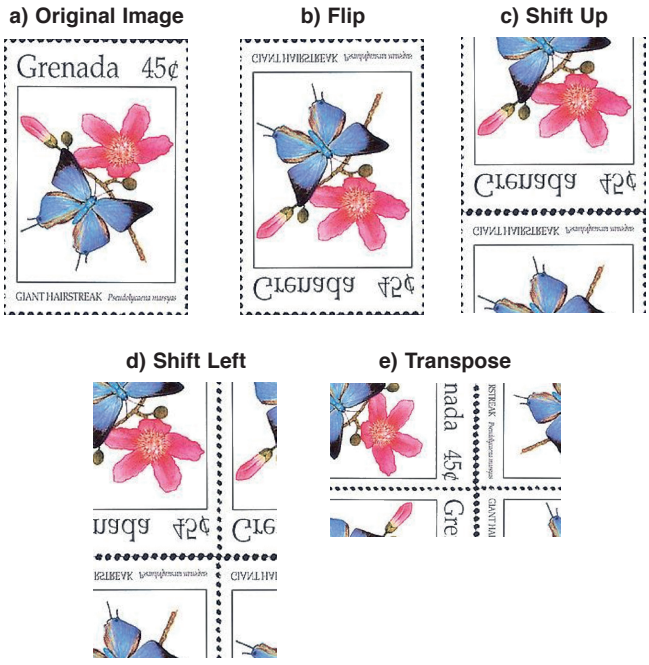

Fig. 1. Illustration of image transformations of Example 4. Each of five images has different DFT but the same set of the DFT coefficient magnitudes

3. shift the image left by 63 pixels;
4. transpose the image.

We note that each of five images has the same set of the DFT coefficient magnitudes. □

Let a 2-dimensional input data array be represented by a complex-valued $M\times N$ matrix x. We consider the matrix x as a function $x:\mathbb{Z}_M\times\mathbb{Z}_N\to\mathbb{C}$, where $x(m,n)$ is the entry located in row $m+1$ and column $n+1$. The 2-dimensional DFT (2d-DFT) of x is defined by

$$\hat{x}(a,b)=\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}x(m,n)e^{-2\pi j(am/M+bn/N)}, \tag{7}$$

where $a\in\mathbb{Z}_M$ and $b\in\mathbb{Z}_N$. Let $S_{M,N}$ denote the collection of all bijections

$$\rho:\mathbb{Z}_M\times\mathbb{Z}_N\to\mathbb{Z}_M\times\mathbb{Z}_N.$$

Note that $S_{M,N}$ is a group when it is equipped with the composition operator as in the 1-dimensional case. As before, let

$$A(x)=\{|\hat{x}(a,b)|:a\in\mathbb{Z}_M,b\in\mathbb{Z}_N\}$$

denote the set of values of the DFT coefficient magnitudes of x, that is, the amplitude spectrum of x. We show that $A(x)=A(x\circ\gamma)$ for γ in a subgroup of $S_{M,N}$.

We use the following lemmas to introduce the permutations that are used to generate the subgroup and prove the invariance of the set of the 2d-DFT coefficient magnitudes when an input data array is permuted by one of these permutations.

Lemma 6. Let $\eta_1(m,n)=(M-m,n)$ for $m\in\mathbb{Z}_M$ and $n\in\mathbb{Z}_N$. Then for each $x:\mathbb{Z}_M\times\mathbb{Z}_N\to\mathbb{C}$,

$$\widehat{x\circ\eta_1}=\hat{x}\circ\eta_1.$$

It follows that $A(x\circ\eta_1)=A(x)$. Note that $M-m$ is the additive inverse of m in $\mathbb{Z}_m$.

Proof. We have

$$\begin{aligned}
\widehat{x\circ\eta_1}(a,b) &= \sum_{m=0}^{M-1}\sum_{n=0}^{N-1}(x\circ\eta_1)(m,n)e^{-2\pi j(am/M+bn/N)}\\
&= \sum_{m=0}^{M-1}\sum_{n=0}^{N-1}x(M-m,n)e^{-2\pi j(am/M+bn/N)}\\
&= \sum_{k=M}^{1}\sum_{n=0}^{N-1}x(k,n)e^{-2\pi j(a(M-k)/M+bn/N)}\\
&= \sum_{k=0}^{M-1}\sum_{n=0}^{N-1}x(k,n)e^{-2\pi j(a(-k)/M+bn/N)}\\
&= \hat{x}(-a,b)\\
&= (\hat{x}\circ\eta_1)(a,b).
\end{aligned}$$

□

Analogously, we have.

Lemma 7. Let $\eta_2(m,n)=(m,N-n)$ for $m\in\mathbb{Z}_M$ and $n\in\mathbb{Z}_N$. Then for each $x:\mathbb{Z}_M\times\mathbb{Z}_N\to\mathbb{C}$,

$$\widehat{x\circ\eta_2}=\hat{x}\circ\eta_2.$$

In particular, $A(x\circ\eta_2)=A(x)$. Note that $N-n$ is the additive inverse of N in $\mathbb{Z}_N$.

Lemma 8. Let $\theta_1(m,n)=(m+1,n)$ for $m\in\mathbb{Z}_M$ and $n\in\mathbb{Z}_N$. Then for each $x:\mathbb{Z}_M\times\mathbb{Z}_N\to\mathbb{C}$,

$$\widehat{x\circ\theta_1}(a,b)=e^{2\pi ja/M}\hat{x}(a,b).$$

In particular, $A(x\circ\theta_1)=A(x)$. Note that $M=0 \bmod M$ and that $x\circ\theta$ cyclically shifts the rows of x up by one row.

Proof. We have

$$\begin{aligned}
\widehat{x\circ\theta_1}(a,b) &= \sum_{m=0}^{M-1}\sum_{n=0}^{N-1}(x\circ\theta_1)(m,n)e^{-2\pi j(am/M+bn/N)}\\
&= \sum_{m=0}^{M-1}\sum_{n=0}^{N-1}x(m+1,n)e^{-2\pi j(am/M+bn/N)}\\
&= \sum_{k=1}^{M}\sum_{n=0}^{N-1}x(k,n)e^{-2\pi j(a(k-1)/M+bn/N)}\\
&= e^{2\pi ja/M}\sum_{k=0}^{M-1}\sum_{n=0}^{N-1}x(k,n)e^{-2\pi j(ak/M+bn/N)}\\
&= e^{2\pi ja/M}\hat{x}(a,b).
\end{aligned}$$

□

Analogously, we have.

Lemma 9. Let $\theta_2(m,n)=(m,n+1)$ for $m\in\mathbb{Z}_M$ and $n\in\mathbb{Z}_N$. Then for each $x:\mathbb{Z}_M\times\mathbb{Z}_N\to\mathbb{C}$,

$$\widehat{x\circ\theta_2}(a,b)=e^{2\pi jb/N}\hat{x}(a,b).$$

It follows that $A(x\circ\theta_2)=A(x)$. Note that $N=0 \bmod N$ and that $x\circ\theta_2$ cyclically shifts the columns of x to the left by one column.

We now define the subgroup of permutations that we use. Let ι be the identity function on $\mathbb{Z}_M\times\mathbb{Z}_N$. Let $G=\{\iota,\nu_1,\nu_2,\theta_1,\theta_2\}$ and let Γ be the subgroup of $S_{M,N}$ generated by G. That is, Γ is the collection of all possible finite compositions of the functions in Γ. The main result of this section now follows immediately from the above lemmas.

Theorem 8. For all $\gamma\in\Gamma$, $A(x\circ\gamma)=A(x)$.

We next note that some common geometric operations on 2-d images can be considered as elements of the group Γ. For example, let an $M\times N$ matrix x be the digitization of an image. Then

1. $\theta_1\circ\eta_1=$ reflection of the image across the horizontal median;
2. $\theta_2\circ\eta_2=$ reflection of the image across the vertical median;

3. $\theta_1 \circ \eta_1 \circ \theta_2 \circ \eta_2 = \theta_2 \circ \eta_2 \circ \theta_1 \circ \eta_1 =$ rotation of the image by 180°.

Of course, many more transformations of an image can be generated using the group Γ.

Unless an image is represented by a square matrix, a 90° rotation of the image will not be given by a permutation of $\mathbb{Z}_M \times \mathbb{Z}_N$. Instead, it will be a function from $\mathbb{Z}_M \times \mathbb{Z}_N$ to $\mathbb{Z}_N \times \mathbb{Z}_M$. Let $S'_{M,N}$ denote the collection of all bijections

$$\rho' : \mathbb{Z}_N \times \mathbb{Z}_M \to \mathbb{Z}_M \times \mathbb{Z}_N.$$

As in the case of $S_{M,N}$, $S'_{M,N}$ is a group when it is equipped with the composition operator. Note that if x is an $M \times N$ matrix, then $x \circ \rho'$ in an $N \times M$ matrix.

Lemma 10. Let $\tau'(n, m) = (m, n)$ for $m \in \mathbb{Z}_M$ and $n \in \mathbb{Z}_N$. Then for each $x : \mathbb{Z}_M \times \mathbb{Z}_N \to \mathbb{C}$,

$$\widehat{x \circ \tau'} = \hat{x} \circ \tau',$$

that is,

$$\widehat{x \circ \tau'}(b, a) = (\hat{x} \circ \tau')(b, a)$$

for $a \in \mathbb{Z}_M$ and $b \in \mathbb{Z}_N$. Note that $x \circ \tau'$ is the transpose of x and thus the 2d-DFT commutes with transposition. In particular, we have $A(x \circ \tau') = A(x)$.

Proof. Let $a \in \mathbb{Z}_M$ and $b \in \mathbb{Z}_N$. Then we have

$$\begin{aligned}
\widehat{x \circ \tau'}(b,a) &= \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} (x \circ \tau')(n,m) e^{-2\pi j (bn/N + am/M)} \\
&= \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} x(m,n) e^{-2\pi j (bn/N + am/M)} \\
&= \hat{x}(a,b) \\
&= (\hat{x} \circ \tau')(b,a)
\end{aligned}$$

□

For example, we have

1. $\tau' \circ \theta_1 \circ \eta_1 =$ rotation of the image 90° clockwise;
2. $\tau' \circ \theta_2 \circ \eta_2 =$ rotation of the image 90° counterclockwise.

Again, there are many more transformations of an image that can be generated by the elements of Γ and τ'.

Theorem 8 and Lemma 10 show that the set of the 2d-DFT coefficient magnitudes of the 2d-DFT of a rectangular image is invariant under the operations in Γ and τ'. This property makes possible the use of the amplitudes of the 2d-DFT in the design of image recognition algorithms that are robust against the operations in Γ and τ', including rotation, reflection, and many others. However, we cannot use the magnitude of the 2d-DFT directly as it is not invariant under the operations in Γ and τ', only the unordered values are.

8. Conclusions

In this paper, we analyzed how rearrangements of a finite sequence affect its DFT coefficients. In addition to its intrinsic mathematical interest, this problem has applications in matrix theory and signal processing. We completely characterized the permutations that leave the collection of the DFT coefficients and their magnitudes invariant. We also gave a more general form of the theorem that gives conditions on a permutation under which it commutes with the DFT operation. We gave examples to illustrate the results obtained. For multidimensional data arrays, we proved that the set of magnitudes of the DFT coefficients are invariant under a subgroup of the permutation group that contains many of the usual geometric transformations. We also discussed possible generalizations and open problems.

References

[1] W.A. Adkins and S.H.Weintraub, *Algebra: An Approach via Module Theory*, Springer-Verlag, New York, 1992.
[2] C. Aitken, Two notes on matrices, *Proceedings of the Glasgow Mathematical Association* 5(3), 109–113, January 1962.
[3] E. Oran Brigham, *The Fast Fourier Transform And Its Applications*, Prentice-Hall, New York, 1988.
[4] S. E. Borujeni, "Speech encryption based on fast Fourier transform permutation", *Proceedings of the 7th IEEE International Conference on Electronics, Circuits and Systems* 1, 290–293, 2000.
[5] C.-Y. Chao, "On a type of circulants", *Linear Algebra and its Applications* 6, 241–248, 1973.
[6] P. J. Davis, Circulant Matrices, Wiley, New York, 1979.
[7] F. Farnoud (Hassanzadeh) and O. Milenkovic, "Sorting of permutations by cost-constrained transpositions", *IEEE Transactions on Information Theory* 58(1), 3–23, January 2012.
[8] P. Ferreira, "A group of permutations that commute with the discrete Fourier transform", *IEEE Transactions on Signal Processing* 42(2), 444–445, 1994.
[9] R.M. Gray, "Toeplitz and circulant matrices: A review", *Foundations and Trends in Communications and Information Theory* 2(3), 155–239, 2006.
[10] F. Horn and K.-R. Muller, "Predicting pairwise relations with neural similarity encoders", *Bull. Pol. Ac.: Tech.* 66(6), 821–830, 2018.
[11] S. Hui and S.H. Żak, "Discrete Fourier transform based pattern classifiers", *Bull. Pol. Ac.: Tech.* 62(1), 15–22, 2014.
[12] T.W. Hungerford, Algebra, Springer-Verlag, New York, 1974.
[13] J. Kurek, B. Swiderski, S. Osowski, M. Kruk, and W. Barhoumi, "Deep learning versus classical neural approach to mammogram recognition", *Bull. Pol. Ac.: Tech.* 6(6), 831–840, 2018.
[14] J. Lang, "Color image encryption based on color blend and chaos permutation in the reality-preserving multipleparameter fractional Fourier transform domain", *Optics Communications* 338, 181–192, 2015.
[15] S. Liu, Y. D. Zhang, and T. Shan, "Detection of weak astronomical signals with frequency-hopping interference suppression", *Digital Signal Processing* 72, 1–8, 2018.
[16] G. Manjunath and G.V. Anand, "Speech encryption using circulant transformations", *Proceedings of the 2002 IEEE International Conference on Multimedia and Expo*, ICME 2002, 1, 26–29, 2002.
[17] A. Matsunaga, K. Koga, and M. Ohkawa, "An analog speech scrambling system using the FFT technique with high-level security", *IEEE Journal on Selected Areas in Communications* 7(4), 540–547, 1989.

[18] A.V. Oppenheim and R.W. Schafer, *Discrete-Time Signal Processing*, Prentice-Hall, New York, 1989.
[19] D. Passman, *Permutation Groups, Benjamin*, New York, 1968.
[20] S. Pawar and K. Ramchandran, "R-FFAST: A robust sub-linear time algorithm for computing a sparse DFT", *IEEE Transactions on Information Theory* 64(1), 451–466, January 2018.
[21] S.-C. Pei, C.-C. Wen, and J.-J. Ding, "Closed-form orthogonal DFT eigenvectors generated by complete generalized Legendre Sequence", *IEEE Transactions on Circuits and Systems— I: Regular Papers* 55(11), 3469–3479, December 2008.
[22] Y. Qiu, G. Zhou, Q. Zhao, and A. Cichocki, "Comparative study on the classification methods for breast cancer diagnosis", *Bull. Pol. Ac.: Tech.* 6(6), 841–848, 2018.
[23] N.D. Sidiropoulos, M.S. Pattichis, A.C. Bovik, and J.W. Havlicek, "COPERM: Transform-domain energy compaction by optimal permutation", *IEEE Transactions on Signal Processing* 47(6), 1679–1688, 1999.
[24] E.M. Stein and R. Shakarchi, *Fourier Analysis*, Princeton University Press, Princeton, 2003.
[25] R. Urbanke, Q. Li, and B. Rimoldi, "On the cardinality of the group of permutations that commute with the Discrete Fourier Transform", *32nd Allerton Conf. on Communication, Control, and Computing*, Monticello, IL, Sept. 28–30, 1994.
[26] A.Weil, *Number Theory for Beginners*, Springer-Verlag, New York, 1985.
[27] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.