Closed-Form Orthogonal DFT Eigenvectors Generated by Complete Generalized Legendre Sequence

Soo-Chang Pei, *Fellow, IEEE*, Chia-Chang Wen, and Jian-Jiun Ding

***Abstract*—In this paper, we propose a new method for deriving the closed-form orthogonal discrete Fourier transform (DFT) eigenvectors of arbitrary length using the complete generalized Legendre sequence (CGLS). From the eigenvectors, we then develop a novel method for computing the DFT. By taking a specific eigendecomposition to the DFT matrix, after proper arrangement, we can derive a new fast DFT algorithm with systematic construction of an arbitrary length that reduces the number of multiplications needed as compared with the existing fast algorithm. Moreover, we can also use the proposed CGLS-like DFT eigenvectors to define a new type of the discrete fractional Fourier transform, which is efficient in implementation and effective for encryption and OFDM.**

***Index Terms*—Complete generalized Legendre sequence (CGLS), discrete Fourier transform (DFT) eigenvector, discrete fractional Fourier transform (DFRFT), fast Fourier transform (FFT).**

I. Introduction

THE DISCRETE Fourier transform (DFT) is defined as follows:

$$X(k) = \mathbf{F}x(n) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x(n) \exp\left(-i2\pi nk/N\right). \quad (1)$$

Its eigenvalues are 1, -1,i, and $-i$. Their multiplicities (shown in Table I) depend on N[1]–[3]. When $N \geq 4$, as the DFT has repeated eigenvalues, the solution for the DFT eigenvector set is nonunique.

There are several existing methods of deriving the DFT eigenvectors. We describe them as follows.

1) Matrix Manipulation: We can find the eigenvectors by Gaussian elimination to the DFT matrix subtracted by the eigenvalues in the diagonal elements. Since the method requires numerical approach, we can find neither the accurate solution for large N nor the orthogonal solutions very effectively.

2) Linear Combination: Let $\mathbf{s}$ be an arbitrary discrete signal. The linear combination

$$\mathbf{e} = \mathbf{s} + \lambda^{-1}\mathbf{F}\mathbf{s} + \lambda^{-2}\mathbf{F}^2\mathbf{s} + \lambda^{-3}\mathbf{F}^3\mathbf{s}, \qquad (\lambda = \pm 1, \pm i) \quad (2)$$

is an eigenvector of the DFT with eigenvalue λ. Given an arbitrary complete basis, we can generate the eigenvectors, however, we still cannot find the orthogonal eigenvector set by using this method.

TABLE I
MULTIPLICITIES OF THE N-POINT DFT EIGENVALUES

N	1	$-j$	-1	j
$N = 4m$	m+1	m	m	m-1
$N = 4m$+1	m+1	m	m	m
$N = 4m$+2	m+1	m	m+1	m
$N = 4m$+3	m+1	m+1	m+1	m

3) Sampling of Periodic Expansion Hermite Function: In [4] and [5], the eigenvectors were derived by taking the summation of the samples of Hermite functions with periodic expansion. This method leads to closed-form solutions but not orthogonal ones.

4) $\mathbf{S}$ Matrix:

$$\mathbf{S} = \begin{bmatrix} 2 & 1 & 0 & 0 & \cdots & 1 \\ 1 & 2\cos\omega & 1 & 0 & \cdots & 0 \\ 0 & 1 & 2\cos 2\omega & 1 & \cdots & 0 \\ 0 & 0 & 1 & 2\cos 3\omega & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & \cdots & 2\cos(N-1)\omega \end{bmatrix}, \quad \text{where } \omega = 2\pi/N. \quad (3)$$

In [2], the eigenvectors of the specific commuting matrix $\mathbf{S}$ are computed to obtain the DFT eigenvector solution. The formal expression of $\mathbf{S}$ is (3). As $\mathbf{S}$ commutes with the DFT matrix $\mathbf{F}$, i.e., $\mathbf{FS} = \mathbf{SF}$, $\mathbf{S}$ has the same eigenvectors as $\mathbf{F}$ but different eigenvalues. However, we still cannot avoid using the numerical approach to find the eigenvalues of $\mathbf{S}$; thus, the method is still impractical for large N. In [6]–[8], Grünbaum *et al.* also found other matrices that can commute with $\mathbf{F}$ and used them to search for DFT eigenvectors.

5) Symmetry: In [9], the zero forcing (ZF) and the periodic forcing (PF) subspaces were employed to find DFT eigenvectors. Since ZF and PF are dual for the DFT, we can intersect the ZF and PF subspaces to form the DFT-invariant ZPF subspace and use it to find DFT eigenvectors. The solutions can be expressed in a simple exponential form, particularly when N is a power of two. However, the transform length is constrained to $N = rM^2$, and arbitrary length DFT eigenvectors cannot be found by this method.

From the earlier discussion, we realize that finding the complete closed-form orthogonal DFT eigenvectors of arbitrary

Manuscript received March 29, 2007; revised August 17, 2007. First published May 30, 2008; current version published December 12, 2008. This work was supported by the National Science Council, China under Contract 93-2219-E-002-004 and Contract NSC 93-2752-E-002-006-PAE. This paper was recommended by Associate Editor R. Merched.

The authors are with the Department of Electrical Engineering, National Taiwan University, Taipei 10617, Taiwan (e-mail: pei@cc.ee.ntu.edu.tw; djj1@ms63.hinet.net).

Digital Object Identifier 10.1109/TCSI.2008.925353

length is still a state-of-the-art issue, and solving the problem is the main topic of this paper. First, in Section II, we define the complete generalized Legendre sequence (CGLS), which is a generalization of the Legendre sequence defined in literature. Then, in Section III, we use the CGLS to derive the DFT eigenvectors. The proposed eigenvectors have the advantages of closed-form solutions, completeness, orthogonality, being well defined for arbitrary N, and fast expansion. The last advantage comes from the fact that the proposed DFT eigenvectors can be viewed as a permutation and a linear combination of the fewer point DFT basis. This method is helpful for developing some useful fast algorithms. In Section IV.A, we propose algorithms using the proposed DFT eigenvectors to quickly implement the DFT. We can also use the proposed CGLS-like DFT eigenvectors to define a new type of discrete fractional Fourier transform (DFRFT) (Section IV.B).

II. CGLS

The GLS [10], [11] has a wide range of applications; however, the GLS does not generate the complete basis. In order to solve the problem, we redefine the **complete form** of the **GLS** (**CGLS**) in Sections II.B and II.C.

A. Original GLS

The GLS is defined for the case where N equals a power of a prime number, i.e., $N = p^l$.

1) If $p > 2$

$$\eta_{a,l}(n) = \exp(i2\pi\, a(\mathrm{ind}_g n)/\varphi(p^l)), \qquad \text{when } (n,p) = 1$$
$$\eta_{a,l}(n) = 0, \qquad \text{when } (n,p) \neq 1$$
$$a = 0,1,\ldots,\varphi(p^l) - 1,\ n = 0,1,\ldots,p^l - 1 \tag{4}$$

where (n,p) denotes the greatest common divisor (GCD) of the integers n and p. The symbol φ denotes the Euler function, which means the number of integers smaller than p^l and coprime with p^l. Therefore, it is shown that the following equation holds:

$$\varphi(p^l) = p^{l-1}(p-1). \tag{5}$$

The ind_g operator denotes the logarithm over the modulus operation, i.e., $\mathrm{ind}_g(n) = m$ if $n = g^m \bmod (p^l)$[10]. For example, since $2^5 = 32 = 7 \bmod(5^2)$,$\mathrm{ind}_2 7 = 5\bmod(5^2)$. The multiplication property of the logarithm operator that $\mathrm{ind}_g \mathrm{ab} = \mathrm{ind}_g a + \mathrm{ind}_g b$ also holds. The index g is a primitive root modulo p^l, i.e., $g^q \neq 1\bmod(p^l)$ for $0 < q < (\varphi(p^l))$.

2) If $p = 2$, the GLS is defined in another way [10]
   a) When $l = 1$,$\eta_{0,1}(n) = [0\ 1]$.
   b) When

$$l = 2, \eta_{0,l}(n) = [0\ 1\ 0\ 1], \eta_{1,l}(n) = [0\ 1\ 0\ -1]. \tag{6}$$

   c) When $l > 2$, we can find an integer b so that

$$\eta_{a,c,l}(n) = \begin{cases} (-1)^{(n-1)c/2} \exp\left(i2\pi ab/2^{l-2}\right), & n \in \text{odd} \\ 0, & n \in \text{even} \end{cases}$$
$$\text{for } c = 0,1 \quad a = 0,1,\ldots,2^{l-2} - 1 \tag{7}$$

where b is some integer that satisfies the following equation:

$$n \equiv (-1)^{(n-1)c/2} 5^b \mod(2^l) \quad c = 0,1 \quad \text{when } n \text{ is odd.} \tag{8}$$

We list the well-known properties of the GLS as follows.

P1. Symmetry: The GLS is either even or odd symmetric.

P2. Permutation of the sinusoidal function: We can view ind_g as an index permutation operator. Therefore, we can view the GLS as permutation of the sinusoidal function.

P3. Conjugate: The conjugate of a GLS is also a GLS, i.e.,

$$\eta^*_{a,l}(n) = \eta_{\varphi(p^l)-a,l}(n). \tag{9}$$

P4. Orthogonal: The GLS forms the orthogonal set, and the real and imaginary parts are also orthogonal.

P5. Multiplication property: $\eta_{a,l}(mn) = \eta_{a,l}(m)\eta_{a,l}(n)$.

P6. DFT property: If $a \neq 0$ and $(a,p) = 1$,

$$\mathbf{F}\{\eta_{a,l}(n)\} = \lambda \eta^*_{a,l}(n), \qquad |\lambda| = 1 \tag{10}$$

where

$$\lambda = \sqrt{1/N} \sum_{n=0}^{N-1} \exp\{(i2\pi)/(N(p-1)) \times [ap(\mathrm{ind}_g n) - (p-1)n]\}$$

.

B. CGLS

From the previous section, we can find only $\varphi(p^l) = p^{l-1}(p-1)$ GLSs, and they are not complete for constructing the vector space $\mathbf{V_N}$, where $N = p^l$. Notice that, in (4), the GLS is always zero when n is a multiple of p, which tells us that we can explore the GLSs with length $p^{l-1}, p^{l-2}, \ldots$, and 1 and apply ZF to these sequences to generate the rest basis and construct the complete orthogonal basis over $\mathbf{V_N}$. That is, we **insert**$(p-1)$ zeros between each neighbor element to $\eta_{a,(l-1)}(n)$, then we insert (p^2-1) zeros between each neighbor element to $\eta_{a,(l-2)}(n)$, and so on. In order to express these sequences mathematically and illustrate more clearly the newly defined basis, we define the CGLS by adding the parameter s to the GLS as follows:

$$\chi_{a,l,s}(n) = \eta_{a,(l-s)}(k) \quad \text{for } n = kp^s$$
$$k = 1,2,3,\ldots,p^{l-s} - 1$$
$$(k,p) = 1$$
$$\chi_{a,l,s}(n) = 0, \qquad \text{otherwise} \tag{11}$$

where $a = 0,1,\ldots,\varphi(p^{l-s}) - 1$,$s = 0,1,\ldots,l-1$. When $s = l$, a must be zero and

$$\chi_{0,l,0}(0) = 1 \quad \chi_{0,l,l}(n) = 0, \qquad \text{when } n \neq 0. \tag{12}$$

In the case where $p = 2$ and $s < l - 2$, the equality $\chi_{a,l,s}(n) = \eta_{a,(l-s)}(k)$ in (11) should be changed as $\chi_{a,c,l,s}(n) = \eta_{a,c,(l-s)}(k)$. Moreover, in this case, $a = 0,1,2,\ldots,2^{l-s-2} - 1$ and $c = 0,1$.

The CGLS is a complete basis, since we can verify that the number of the CGLSs we get is

$$\begin{aligned} N' &= \varphi(p^l) + \varphi(p^{l-1}) + \cdots + \varphi(p) + \varphi(1) \\ &= p^l - p^{l-1} + p^{l-1} - p^{l-2} + \cdots + p - 1 + 1 = p^l. \end{aligned} \tag{13}$$

Because the CGLSs are linearly independent, we can generate the entire $\mathbf{V_N}$ with full rank.

The following are examples of CGLS matrices when $N = 8$ and 9:

$$\mathbf{8-pt\ CGLS}:$$
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & -1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 1 & -1 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & -1 & -1 \end{bmatrix}$$
$$\mathbf{9-pt\ CGLS}, (\omega = \exp(j\pi/3)):$$
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 \\ 0 & 0 & 0 & \omega^0 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega^0 & \omega^2 & \omega^4 & \omega^0 & \omega^2 & \omega^4 \\ 0 & 0 & 0 & \omega^0 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega^0 & \omega^4 & \omega^2 & \omega^0 & \omega^4 & \omega^2 \\ 0 & 0 & 0 & \omega^0 & \omega^3 & \omega^0 & \omega^3 & \omega^0 & \omega^3 \end{bmatrix}. \tag{14}$$

In particular, we can see that the last six columns of the 9-pt CGLS is the row-shuffled 6-pt DFT.

The properties **P1** to **P4** also hold for the CGLS. As for **P5** and **P6**, they are modified as follows:

P5. Multiplication: If $m = m'p^s$ and $n = n'p^s$, where $(m', p) = (n', p) = 1$, then

$$\chi_{a,l,s}(mnp^{-s}) = \chi_{a,l,s}(m)\chi_{a,l,s}(n). \tag{15}$$

P6. The most important property of the CGLS is its unique DFT property described as follows. If $a \neq 0$

$$\mathbf{F}\{\chi_{a,l,s}\} = \lambda\chi^*_{ap^{s-r},l,r}, \qquad |\lambda| = 1 \tag{16}$$

where $\chi_{a,l,s}$ and $\chi ap^{s-r}, l, r$ have been normalized such that $\|\chi_{a,l,s}\| = \|\chi_{ap^{s-r},l,r}\| = 1$, where r denotes the order of the GCD between a and p^l so that $(a, p^l) = p^{\cdot}$. From (16), λ can be easily calculated from

$$\lambda = X_{a,l,s}(n)/\chi^*_{ap^{s-r},l,r}(n) \tag{17}$$

where $X_{a,l,s} = \mathbf{F}\{\chi_{a,l,s}\}$ and n is any point that satisfies

$$\chi_{ap^{s-r},l,r}(n) \neq 0. \tag{18}$$

Proof: If $p > 2$

$$\begin{aligned} &\mathrm{F}\{\chi_{a,l,s}(n)\} \\ &= \sqrt{p^{-l}} \sum_{n=o}^{p^l-1} \exp\left[i2\pi a \cdot \mathrm{ind}_g(np^{-s})/\varphi(p^{l-s})\right] \\ &\quad \times \exp(-i2\pi nk/p^l) \\ &= \sqrt{p^{-l}} \sum_{n'=1,(n',p)=1}^{p^{l-s}} \exp\left[\frac{i2\pi ap^{-r}\mathrm{ind}_g n'}{\varphi(p^{l-s-r})}\right] \\ &\quad \times \exp\left(\frac{-i2\pi n'k}{p^{l-s}}\right) \\ &= \sqrt{p^{-l}} \sum_{n'=1,(n',p)=1}^{p^{l-s}} \\ &\quad \times \exp(i2\pi ap^{-r}\mathrm{ind}_g(n'kp^{-r}/kp^{-r})/\varphi(p^{l-s-r})) \\ &\quad \times \exp(-i2\pi n'kp^{-r}/p^{l-s-r}) \\ &= \left\{\sqrt{p^{-l}} \sum_{m=1,(m,p)=1}^{p^{l-s-r}} \exp\left(\frac{i2\pi a \cdot \mathrm{ind}_g m}{\varphi(p^{l-s})}\right)\right. \\ &\quad \left. \times \exp\left(\frac{-i2\pi m}{p^{l-s-r}}\right)\right\} \\ &\quad \times \exp\left(\frac{-i2\pi(ap^{s-r}) \cdot \mathrm{ind}_g(kp^{-r})}{\varphi(p^{l-r})}\right) \\ &= \lambda\chi^*_{ap^{s-r},l,r}. \end{aligned} \tag{19}$$

where λ can be calculated from (17). Please check if Eq. (19) is correctly captured. Here, we set $m = n'kp^{-r}$. If $p = 2$, we can use the same method to prove (16).

For example, if $N = 3^3 = 27$ and $\varphi(N) = 18$, we apply the DFT to $\chi_{1,3,1}(n)$ and get

$$\begin{aligned} &\mathrm{F}\{\chi_{1,3,1}\} \\ &= \mathbf{F}\left[0\,0\,0\,1\,0\,0\,(1-i\sqrt{3})/2\,0\,0\,0\,0\,0\,(-1-i\sqrt{3})/2\,0\,0\right. \\ &\qquad \left. \times (1+i\sqrt{3})/2\,0\,0\,0\,0\,0\,(-1+i\sqrt{3})/2\,0\,0\,-1\,0\,0\right] \\ &= \lambda\left[0\,1\,\frac{1-i\sqrt{3}}{2}\,0\,\frac{-1-i\sqrt{3}}{2}\,\frac{1+i\sqrt{3}}{2}\,0\,\frac{-1+i\sqrt{3}}{2}\right. \\ &\qquad -1\,0\,1\,\frac{1-i\sqrt{3}}{2}\,0\,\frac{-1-i\sqrt{3}}{2} \\ &\qquad \frac{1+i\sqrt{3}}{2}\,0\,\frac{-1+i\sqrt{3}}{2}\,-1\,0\,1\,\frac{1-i\sqrt{3}}{2}\,0\,\frac{-1-i\sqrt{3}}{2} \\ &\qquad \left.\frac{1+i\sqrt{3}}{2}\,0\,\frac{-1+i\sqrt{3}}{2}\,-1\right] \\ &= \lambda\chi^*_{3,3,0}(n) = \lambda\chi_{15,3,0}(n) \\ &\qquad \text{where } \lambda = -0.7660 - i0.6428. \end{aligned} \tag{20}$$

We perform the divisions of 2.4495 and 4.2426 to normalize $\chi_{1,3,1}$ and $\chi_{3,3,0}$, respectively.

When $a = 0$, **P6** does not hold, as the CGLSs are not one-by-one DFT mapping. To compensate for the mismatch,

we apply a linear transformation to $[\chi_{0,l,l},\chi_{0,l,l-1},\ldots,\chi_{0,l,0}]$ by the following:

$$\begin{aligned}\mathbf{e_{1,m}} &= \chi_{0,l,m} + (p^{l/2-m} - p^{l/2-m-1}) \\ &\quad \times [\chi_{0,l,l} + \chi_{0,l,l-1} + \cdots + \chi_{0,l,l-m}] \\ &\quad - p^{l/2-m-1}\chi_{0,l,l-m-1} \qquad (21)\\ \mathbf{e_{-1,m}} &= \chi_{0,l,m} - (p^{l/2-m} - p^{l/2-m-1}) \\ &\quad \times [\chi_{0,l,l} + \chi_{0,l,l-1} + \cdots + \chi_{0,l,l-m}] \\ &\quad + p^{l/2-m-1}\chi_{0,l,l-m-1} \qquad (22)\end{aligned}$$

where $m = 0, 1, \ldots,$ round $[l/2] - 1$.

When l is even, the extra sequence is defined by

$$\mathbf{e_{1,l/2}} = [\chi_{0,l,l} + \chi_{0,l,l-1} + \cdots + \chi_{0,l,l/2}]. \qquad (23)$$

It can be verified that the sequences themselves are directly DFT eigenvectors, and they are also orthogonal. To correspond to **P6** and to solve the DFT eigenvector problem, in subsequence, we transform $[\chi_{0,l,l},\chi_{0,l,l-1},\ldots,\chi_{0,l,0}]$ into $\mathbf{e_{1,m}}$ and $\mathbf{e_{-1,m}}$.

From (16), after applying the DFT to a CGLS, we can obtain the conjugation of another CGLS. For example, when $N = 3^3 = 27$, we can find the conjugate transform pairs of the DFT as given by (24), shown at the bottom of this page.

C. CGLS for Arbitrary Length

In this section, we extend our discussion to arbitrary length $N = p_1^{l_1}p_2^{l_2},\ldots,p_k^{l_k}$. The composite length CGLS is defined by multiplying the CGLS defined for each $p_i^{l_i}$ as

$$\begin{aligned}&\chi_{a_1,a_2,\ldots,a_k,l_1,l_2,\ldots,l_k,s_1,s_2,\ldots,s_k}(n) \\ &\quad = \chi_{a_1,l_1,s_1}(n)\chi_{a_2,l_2,s_2}(n),\ldots,\chi_{a_k,l_k,s_k}(n). \qquad (25)\end{aligned}$$

Note that, in (25), $\chi_{a_i,l_i,s_i}(n)$ is repeated $(p_1^{l_1}p_2^{l_2},\ldots,p_k^{l_k}/p_i^{l_i})$ times. The CGLS defined in (25) also obeys rules **P1** to **P4** but **P5** does not hold any more. As for the DFT property **P6**, we describe it as follows.

Theorem 2.1: Let $h_1(n)$,$h_2(n)$ be two periodic m_1-point and m_2-point sequences, where $(m_1, m_2) = 1$. Let $H(k)$ be the m_1m_2-point DFT of $h(n) = h_1(n)h_2(n)$. We can show that $H(k) = H_1(k)H_2(k)$, where $H_1(k)$ is the m_1-point DFT of $h_1(m_2n)$ repeating m_2 times, and $H_2(k)$ is the m_2-point DFT of $h_2(m_1n)$ repeating m_1 times.

Proof: Applying the DFT to $h(n)$, we get

$$\begin{aligned}H(k) = \mathbf{F}[h(n)] &= \frac{1}{\sqrt{m_1m_2}} \\ &\quad \times \sum_{n=0}^{m_1m_2-1} h(n)\exp\left(\frac{-i2\pi nk}{m_1m_2}\right). \qquad (26)\end{aligned}$$

Let $n = m_1n_2 + m_2n_1 \bmod (m_1m_2)$, where $0 \le n_1 \le m_1 - 1$ and $0 \le n_2 \le m_2 - 1$. Since $(m_1, m_2) = 1$, we can rewrite (26) in double summation form with index n_1, n_2 as follows:

$$\begin{aligned}&H(k) \\ &= \frac{1}{\sqrt{m_1m_2}}\sum_{n_1=0}^{m_1-1}\sum_{n_2=0}^{m_2-1} h_1(m_2n_1 + m_1n_2) \\ &\quad \times h_2(m_2n_1 + m_1n_2)\exp\left(\frac{-i2\pi(m_1n_2 + m_2n_1)k}{m_1m_2}\right) \\ &= \frac{1}{\sqrt{m_1m_2}}\sum_{n_1=0}^{m_1-1}\sum_{n_2=0}^{m_2-1} h_1(m_2n_1) \\ &\quad \times h_2(m_1n_2)\exp\left(\frac{-i2\pi n_2k}{m_2}\right)\exp\left(\frac{-i2\pi n_1k}{m_1}\right) \\ &= \left[\frac{1}{\sqrt{m_1}}\sum_{n_1=0}^{m_1-1} h_1(m_2n_1)\exp\left(\frac{-i2\pi n_1k}{m_1}\right)\right] \\ &\quad \times \left[\frac{1}{\sqrt{m_2}}\sum_{n_2=0}^{m_2-1} h_2(m_1n_2)\exp\left(\frac{-i2\pi n_2k}{m_2}\right)\right]. \qquad (27)\end{aligned}$$

Moreover, in this case, the DFT of the CGLS is

$$\begin{aligned}&\mathbf{F}\{\chi_{a_1,a_2,\ldots,a_k,l_1,l_2,\ldots,l_k,s_1,s_2,\ldots,s_k}\} \\ &\quad = \lambda\chi^*_{a_1p_1^{s_1-r_1},a_2p_2^{s_2-r_2},\ldots,a_kp_k^{s_k-r_k},l_1,l_2,\ldots,l_k,r_1,r_2,\ldots,r_k} \qquad (28)\end{aligned}$$

where $\lambda = \lambda_1\lambda_2\cdots\lambda_k\chi_{a_1,l_1,s_1}(Np_1^{s_1-l_1})\chi_{a_2,l_1,s_2}(Np_2^{s_2-l_2})\cdots$

$$\chi_{a_k,l_1,s_k}(Np_k^{s_k-l_k}). \qquad (29)$$

Proof: By (27), we can get the following:

$$\begin{aligned}\mathbf{F}(\chi) &= \left[p_1^{-l_1/2}\sum_{n=0}^{p_1^{l_1}-1}\chi_{a_1,l_1,s_1}\left(Np_1^{-l_1}n\right)\exp\left(\frac{-i2\pi nk}{p_1^{l_1}}\right)\right] \\ &\quad \times \left[\left(\frac{N}{p_1^{l_1}}\right)^{-1/2}\sum_{n=0}^{\left(N/p_1^{l_1}\right)-1}\chi_{a_2,\ldots,a_k,l_2,\ldots,l_k,s_2,\ldots,s_k}\left(p_1^{l_1}n\right)\right. \\ &\quad \left.\times\exp\left(\frac{-i2\pi nkp_1^{l_1}}{N}\right)\right]. \qquad (30)\end{aligned}$$

By **P5**, we can decompose $\chi_{a_1,l_1,s_1}(Np_1^{-l_1}n)$ as $\chi_{a_1,l_1,s_1}(Np_1^{s_1-l_1}n) \times \chi_{a_1,l_1,s_1}(n)$; therefore, we can express the first bracket of the right-hand side of (30) as $\chi_{a_1,l_1,s_1}(Np_1^{s_1-l_1}n)\mathrm{FT}[\chi_{a_1,l_1,s_1}(n)]$. With iterative decomposition of the right-hand side of (30), we obtain

$$\begin{aligned}\mathbf{F}(\chi) &= \left[\chi_{a_1,l_1,s_1}\left(Np_1^{s_1-l_1}\right)\mathbf{F}\{\chi_{a_1,l_1,s_1}\}\right] \\ &\quad \times \left[\chi_{a_2,l_2,s_2}\left(Np_2^{s_2-l_2}\right)\mathbf{F}\{\chi_{a_2,l_2,s_2}\}\right] \\ &\quad \cdots\left[\chi_{a_k,l_k,s_k}\left(Np_k^{s_k-l_k}\right)\mathbf{F}\{\chi_{a_k,l_k,s_k}\}\right]\end{aligned}$$

$$\left\{\begin{array}{c}[\chi_{1,3,0},\chi_{17,3,0}],[\chi_{2,3,0},\chi_{16,3,0}],[\chi_{3,3,0},\chi_{5,3,1}],[\chi_{4,3,0},\chi_{14,3,0}] \\ [\chi_{5,3,0},\chi_{13,3,0}],[\chi_{6,3,0},\chi_{4,3,1}],[\chi_{7,3,0},\chi_{11,3,0}],[\chi_{8,3,0},\chi_{10,3,0}] \\ [\chi_{9,3,0},\chi_{1,3,2}],[\chi_{12,3,0},\chi_{2,3,1}],[\chi_{15,3,0},\chi_{1,3,1}],\chi_{3,3,1} \\ \mathbf{e_{1,0}},\mathbf{e_{1,1}},\mathbf{e_{-1,0}},\mathbf{e_{-1,1}}\end{array}\right\} \qquad (24)$$

$$
\begin{aligned}
&= \chi_{a_1,l_1,s_1}\left(Np_1^{s_1-l_1}\right)\chi_{a_2,l_2,s_2}\left(Np_2^{s_2-l_2}\right)\\
&\quad\times\cdots\chi_{a_k,l_k,s_k}(Np_k^{s_k-l_k})\\
&\quad\times\lambda_1\lambda_2\cdots\lambda_k\chi^*_{a_1p_1^{s_1-r_1},l_1,s_1}\\
&\quad\bullet\,\chi^*_{a_2p_2^{s_2-r_2},l_2,s_2}\bullet\cdots\chi^*_{a_kp_k^{s_k-r_k},l_k,s_k}\\
&= \lambda\chi^*_{a_1p_1^{s_1-r_1},a_2p_2^{s_2-r_2},\ldots,a_kp_k^{s_k-r_k},r_1,r_2,\ldots,r_k}.
\end{aligned}
$$

We now perform a DFT pair example where $N = 3^2 \times 5 = 45$. To clarify the expression, let $\chi_{a,l,s}$ and $\kappa_{u,m}$ (for $a = 0$) be the 9-pt CGLS and $\xi_{a,l,s}$ and $\theta_{u,m}$ (for $a = 0$) be the 5-pt CGLS. The 45-pt DFT pairs are shown in (31) at the bottom of this page.

III. Deriving DFT Eigenvectors

From DFT pairs property **P6** (illustrated in (16) and (28)) in Section II.B, let

$$\mathbf{G_S} = \left[\chi_{A,L,S}, \chi^*_{A,L,S}, \chi_{AP^{S-R},L,R}, \chi^*_{AP^{S-R},L,R}\right] \tag{32}$$

form an orthogonal CGLS set. We can then derive the complete DFT eigenvector set from linear combinations of $\mathbf{G_s}$ as follows.

1) When $\mathbf{G_s}$ is an even symmetric CGLS set

$$[\mathbf{e_{1a}e_{-1a}e_{1b}e_{-1b}}] = \mathbf{G_sA_s}$$

where

$$\mathbf{A_s} = \begin{bmatrix} 1 & -1 & -i & i \\ 1 & -1 & i & -i \\ \lambda^* & \lambda^* & i\lambda^* & i\lambda^* \\ \lambda & \lambda & -i\lambda & -i\lambda \end{bmatrix}/2. \tag{33}$$

2) When $\mathbf{G}_s$ is an odd symmetric CGLS set

$$[\mathbf{e_{ia}e_{-ia}e_{ib}e_{-ib}}] = \mathbf{G_sA_s}$$

where

$$\mathbf{A_s} = \begin{bmatrix} 1 & -1 & -i & i \\ 1 & -1 & i & -i \\ i\lambda^* & i\lambda^* & -\lambda^* & -\lambda^* \\ -i\lambda & -i\lambda & -\lambda & -\lambda \end{bmatrix}/2. \tag{34}$$

The suffixes 1, -1,i, and $-i$ denote the corresponding eigenvalues, and the meaning of λ is illustrated in (17). The notations A, S, P, L, and R denote vectors of $[a_1, a_2, \ldots, a_k]$, $[s_1,s_2,\ldots,s_k]$,$[p_1,p_2,\ldots,p_k]$,$[l_1,l_2,\ldots,l_k]$, and $[r_1,r_2,\ldots,r_k]$ to represent the CGLS as in (25) when $N = p_1^{l_1}p_2^{l_2},\ldots,p_k^{l_k}$. The results of (33) and (34) are useful when we need to construct a novel DFT fast algorithm in the next section.

The DFT eigenvectors obtained using our method have the following properties:

1) complete;
2) closed-form solution;
3) well defined for any length N;
4) orthogonality;
5) fast expansion (i.e., the eigenvector expansion operation has a fast algorithm).

Proofs of 4 and 5: From orthogonal property **P4** and the fact that $\mathbf{A_s}$ in (33) and (34) are orthogonal transform matrices, $[\mathbf{e_{1a}e_{-1a}e_{1b}e_{-1b}}]$ and $[\mathbf{e_{ia}e_{-ia}e_{ib}e_{-ib}}]$ are orthogonal.

Suppose that there is a vector $\mathbf{x}$ and we want to express it as the linear combination of the DFT eigenvectors derived in (33) and (34), i.e.,

$$\mathbf{x} = \mathbf{Ez} \tag{35}$$

where each column of the N by N matrix $\mathbf{E}$ is a DFT eigenvector and $\mathbf{z}$ is an N-length column vector whose entries are expansion coefficients. We can compute $\mathbf{z}$ from

$$\mathbf{z} = \mathbf{E}^{-1}\mathbf{x} = \mathbf{CE}^{\mathrm{H}}\mathbf{x} \tag{36}$$

where $\mathbf{C} = (\mathbf{E}^{\mathrm{H}}\mathbf{E})^{-1}$ is a diagonal matrix and $^{\mathrm{H}}$ means Hermitian (transpose + conjugation). We can implement (35) by fast algorithms. In (33) to (34), the eigenvectors are derived from the linear combination of CGLSs. Thus, we can decompose $\mathbf{E}$ as

$$\mathbf{E} = \mathbf{GA} \tag{37}$$

where each column of $\mathbf{G}$ is a CGLS and $\mathbf{A}$ is a sparse matrix containing no more than two N nonzero elements derived from (33) and (34). We can view the CGLSs as permutations of sinusoidal functions (**P2**, see Section II). Therefore, we can implement $\mathbf{G}$ in (37) by several sub-DFTs so that the eigenvector expansion in (35) has fast algorithms.

Although we can use other ways to derive the DFT, until now, no other efficient algorithm can obtain the DFT eigenvectors that satisfy all the five properties (completeness, orthogonality, closed-form solution, suitability for any N, and fast expansion) as does our proposed algorithm. We compare the proposed method and the existing eigenvector derivation methods in Tables II and III. The symbol O means that the property applies, X means that the property does not apply, and Δ means that the property applies in theory but is not practical due to the limitation of accuracy in the numerical approach for large N.

The CGLS-like DFT eigenvectors can be connected with the AM–FM transform [12]

$$x[n] = \sum A_k[n]\exp\{j\Omega_k[n]\}. \tag{38}$$

$$\left\{\begin{array}{c} [\chi_{1,2,0}\xi_{1,1,0}, \chi_{5,2,0}\xi_{3,1,0}], [\chi_{2,2,0}\xi_{1,1,0}, \chi_{4,2,0}\xi_{3,1,0}], [\chi_{3,2,0}\xi_{1,1,0}, \chi_{1,2,1}\xi_{3,1,0}], \\ [\chi_{4,2,0}\xi_{1,1,0}, \chi_{2,2,0}\xi_{3,1,0}], [\chi_{1,2,0}\xi_{2,1,0}, \chi_{5,2,0}\xi_{2,1,0}], [\chi_{2,2,0}\xi_{2,1,0}, \chi_{4,2,0}\xi_{2,1,0}], \\ [\chi_{3,2,0}\xi_{2,1.0}, \chi_{1,2.1}\xi_{2,1.0}], [\chi_{1,2.0}\theta_{1,0}, \chi_{5,2.0}\theta_{1,0}], [\chi_{3,2.0}\theta_{1,0}, \chi_{1,2.1}\theta_{1,0}], \\ [\chi_{1,2.0}\theta_{-1,0}, \chi_{5,2.0}\theta_{-1,0}], [\chi_{2,2,0}\theta_{-1,0}, \chi_{4,2,0}\theta_{-1,0}], [\chi_{3,2,0}\theta_{-1,0}, \chi_{1,2,1}\theta_{-1,0}] \\ [\kappa_{1,0}\theta_{1,0}], [\kappa_{1,0}\theta_{-1,0}], [\kappa_{1,0}\xi_{1,1,0}, \kappa_{1,0}\xi_{3,1,0}] \quad , \quad [\kappa_{1,1}\xi_{2,1,0}], [\kappa_{1,1}\theta_{1,0}], \\ [\kappa_{1,1}\theta_{-1,0}], [\kappa_{-1,0}\xi_{2,1,0}], [\kappa_{-1,0}\theta_{1,0}], [\kappa_{-1,0}\theta_{-1,0}], [\kappa_{-1,0}\xi_{1,1,0}, \kappa_{-1,0}\xi_{3,1,0}], \\ [\chi_{1,2,1}\xi_{1,1,0}, \chi_{3,2,0}\xi_{3,1,0}], [\chi_{5,2,0}\xi_{1,1,0}, \chi_{1,2,0}\xi_{3,1,0}], [\chi_{2,2,0}\theta_{1,0}, \chi_{4,2,0}\theta_{1,0}], \\ [\kappa_{1,0}\xi_{2,1,0}] \quad , \quad [\kappa_{1,1}\xi_{1,1,0}, \kappa_{1,1}\xi_{3,1,0}] \end{array}\right\} \tag{31}$$

TABLE II
COMPARISON OF THE DIFFERENT METHODS TO GET DFT EIGENVECTORS

	L.C. *	S.P.E.H.*	S *	Sym *	CGLS *
Complete	Δ	O	O	O	O
Orthogonal	X	X	O	O	O
Closed-Form	O	O	X	O	O ***
Fast expansion	X	X	X	O	O
Arbitrary length	O	O	Δ **	X	O
Hermite-like	X	O	O	X	X

* L.C.— by linear combination, S.P.E.H.— by sampling of periodic expansion Hermite function S— by S matrix, Sym— by Symmetry, CGLS— by the complete generalized Legendre sequence as proposed.

** In theory, we can use the **S** matrix method to derive DFT eigenvectors for arbitrary length *N*. However, due to the truncation error in the numerical approach, the two algorithms are impractical for very large *N*.

*** The value of λ may be calculated from (17).

TABLE III
COMPARISON OF THE DFRFTS BASED ON THE EIGENVECTORS DERIVED FROM THE **S** MATRIX AND THE CGLS-LIKE DFT EIGENVECTOR

	S matrix DFRFT	CGLS-like DFRFT
Eigenvector form	Discrete version of the Hermite function	Linear combination, repeating, and permutation of the lower-point DFT basis
Physical meaning	Rotate the discrete Wigner distribution function clockwise by an angle of $\alpha\pi/2$	Lack of physical meaning
Energy distribution	Concentrated on low-frequency region	More uniform, "white" spread spectrum
Complexity	$O(N^2)$	$O(N\log_2 N)$, since we can use the DFT fast algorithm to compute the DFRFT
Suitable Applications	Filter design, time-frequency analysis, beam-forming, image restoration, etc	Encryption, watermark embedding, CDMA, OFDM, etc

This is useful for spectral analysis. There are many ways of choosing $A_k[n]$ and $\Omega_k[n]$. For example, in [12], Pattichis *et al.* found that, after permuting the signal according to its histogram, the spectrum becomes more concentrated. This type of AM–FM transform can be viewed as the permutation of the DFT.

Similarly, the proposed CGLS-like eigenvectors can also be viewed as a permutation of the DFT basis with the insertion of zeros. Note that, in (11), ind_g is equivalent to performing the permutation for n. Comparing with (38), we find that, when $N = p^l$, the CGLS is a special form of the AM–FM transform where

$$\begin{aligned}\Omega_k[n] &= 2\pi a \cdot \mathrm{ind}_g(np^{-s})/\varphi(p^{l-s}),\\ A_k[n] &= \sum_{r,r=bp^s,\quad (b,m)=1} \exp\{-j\Omega_k[r]\}x[r]\\ &\qquad \text{when } n = mp^s \quad \text{where } (m,p)=1,\\ A_k[n] &= 0 \quad \text{otherwise.}\end{aligned} \tag{39}$$

When $N \neq p^l$, from (25), the CGLS can still be viewed as a product of the permuting DFT. Thus, the CGLS-like eigenvector is similar to the DFT-permuting type AM–FM transform in [12].

IV. APPLICATIONS

A. DFT Implementation by CGLS-Like DFT Eigenvectors

It is well known that, when $N = 2^k$, we can use the radix-2 fast Fourier transform algorithm to implement the DFT in a very efficient way. However, when $N \neq 2^k$, particularly for the case where N is a prime number, the implementation of DFT is much more complex than the case where $N = 2^k$. In this section, we propose a method that uses the CGLS-like DFT eigenvectors to implement the DFT, particularly when N is a prime number or a product of distinct prime numbers, to improve the efficiency of the DFT implementation. For an N-point DFT matrix $\mathbf{F}$, we can express its eigendecomposition form as follows:

$$\mathbf{Fx} = \mathbf{EDE^{-1}x} \tag{40}$$

where the columns of $\mathbf{E}$ are the CGLS-like DFT eigenvectors and $\mathbf{D}$ is a diagonal matrix whose diagonal entries are eigenvalues of the DFT. From (36) and (37)

$$\mathbf{Fx} = \mathbf{EDE^{-1}x} = \mathbf{G}(\mathbf{ADCA^H})\mathbf{G^Hx} = \mathbf{GBG^Hx} \quad \text{where } \mathbf{B} = \mathbf{ADCA}^{\mathrm{H}} \tag{41}$$

and we change the coordinate into the CGLS basis. From the permutation property of the CGLD (**P2** in Section II), we can implement $\mathbf{G}$ by the combination of sub-DFT block matrices.

Then, we discuss the implementation of $\mathbf{B}$. Note that $\mathbf{B} = \mathbf{ADCA}^{\mathrm{H}}$ and that $\mathbf{A}$ is a canonical matrix whose diagonal is a series of the 4×4 (or 2×2, 1×1) submatrices that have the form as in (33) and (34). This makes $\mathbf{B}$ also a canonical matrix. When $\chi_{a,l,s}$ is even, the 4×4 submatrix of $\mathbf{B}$ (denoted by $\mathbf{B}_s$) that corresponds to the CGLS of $[\chi_{A,L,S}, \chi^*_{A,L,S}, \chi_{AP^{S-R},L,R}, \chi^*_{AP^{S-R},L,R}]$ has the form

$$\mathbf{B}_s = \mathbf{A}_s\mathbf{D}_s\mathbf{C}_s\mathbf{A}_s^{\mathrm{H}} \tag{42}$$

where $\mathbf{A}_s$ is defined in (33), $\mathbf{C}_s = r^{-1}\mathbf{I}$, where $r = \langle \chi_{A,L,S}, \chi_{A,L,S}\rangle$. Moreover, since the eigenvalues corresponding to $\mathbf{e}_{1a}\mathbf{e}_{-1a}\mathbf{e}_{1b}\mathbf{e}_{-1b}$ in (33) are 1, −1, 1, and −1, the eigenvalue matrix $\mathbf{D}_s$is

$$\mathbf{D_s} = \begin{bmatrix} 1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1 \end{bmatrix}. \tag{43}$$

from (33). By direct computation, we can show that

$$\mathbf{B_s} = \begin{bmatrix} 0 & 0 & 0 & r^{-1}\lambda^*\\ 0 & 0 & r^{-1}\lambda & 0\\ 0 & r^{-1}\lambda^* & 0 & 0\\ r^{-1}\lambda & 0 & 0 & 0 \end{bmatrix}. \tag{44}$$

When $\chi_{A,LS}$ is odd, in a similar way, we can also prove that $\mathbf{B}_s$ is also an antidiagonal matrix. Therefore, the rows of $\mathbf{B}$ that correspond to the eigenvector generated from $\chi_{A,L,S}$ have only one nonzero element. For the rows that correspond to the eigenvector generated from $\mathbf{e}_{\pm 1,\mathbf{m}}$, from (21), (22), and (23), there are more than one nonzero entry. However, with proper implementation, there are only two multiplications for each pair of rows

[i.e., $p^{1/2-m} - p^{1/2-m-1}$ and $-p^{1/2-m-1}$ in (21) and (22)]. Therefore, $\mathbf{B}$ can be decomposed as

$$\mathbf{B} = \mathbf{UV} \tag{45}$$

where $\mathbf{V}$ is a diagonal matrix and $\mathbf{U}$ is a sparse integer matrix that corresponds to the permutations to form the antidiagonal matrix in (44) and the addition operations in (21), (22), and (23). Thus, $\mathbf{B}$ can be implemented efficiently with no more than N floating-point multiplications.

For example, for $N = 65 = 5 \times 13, \mathbf{B}_{65}$ is presented in Appendix B. Moreover, in this case, according to (12) and (29), $p_1 = 5, p_2 = 13, l_1 = l_2 = 1$, and we can generate $\mathbf{G}_{65}$ by (46), (47), (48), (49), and (50), shown at the bottom of this page. The superscript ind_g is used to distinguish the operations over different modulo. With proper rearrangement, we can express the CGLS matrix $\mathbf{G}_{65}$ as follows:

$$\mathbf{G_{65}} = \mathbf{P}_{65} \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{F_4} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{F_{12}} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{F_{12}} & \mathbf{F_{12}} & \mathbf{F_{12}} & \mathbf{F_{12}} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{F_{12}} & -j\mathbf{F_{12}} & -\mathbf{F_{12}} & j\mathbf{F_{12}} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{F_{12}} & -\mathbf{F_{12}} & \mathbf{F_{12}} & -\mathbf{F_{12}} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{F_{12}} & j\mathbf{F_{12}} & -\mathbf{F_{12}} & j\mathbf{F_{12}} \end{bmatrix} \tag{51}$$

where $\mathbf{P}_{65}$ is the permutation operator (see Appendix B). Moreover, we can further decompose (51) as

$$\mathbf{G_{65}} = \mathbf{PD_1P_BD_2} \tag{52}$$

where

$$\mathbf{D_1} = \begin{bmatrix} \mathbf{I_5} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{F}_{12} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{F}_{12} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{F}_{12} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{F}_{12} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{F}_{12} \end{bmatrix}$$

$$\mathbf{D_2} = \begin{bmatrix} \mathbf{I_{13}} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{F_4} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{F_4} & \cdots & \mathbf{0} & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{F_4} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{F_4} \end{bmatrix}$$

$\mathbf{P}_A, \mathbf{P}_B$, and $\mathbf{P}_C$ are permutation matrices and $\mathbf{I}_N$ means the N by N identity matrix. Furthermore, we can decompose the 12-pt DFT matrix $\mathbf{F}_{12}$ in (52) as follows:

$$\mathbf{F_{12}} = \mathbf{G_{12}B_{12}G_{12}^H}$$

where

$$\mathbf{G_{12}} = \mathbf{P}_{12} \begin{bmatrix} \mathbf{F_2} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{F_2} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{F_2} & \mathbf{F_2} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{F_2} & -\mathbf{F_2} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{F_2} & \mathbf{F_2} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{F_2} & -\mathbf{F_2} \end{bmatrix}$$

$$\mathbf{F_2} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{53}$$

$$\begin{aligned} \mathrm{B}_{12}[1,1] &= 1 \quad \mathrm{B}_{12}[2,3] = 1 \\ \mathrm{B}_{12}[1,5] &= 1 \quad \mathrm{B}_{12}[8,10] = -i\sqrt{3}/2 \\ \mathrm{B}_{12}[5,1] &= 1 \quad \mathrm{B}_{12}[7,3] = 1 \\ \mathrm{B}_{12}[4,11] &= i \quad \mathrm{B}_{12}[11,11] = -i/2 \\ \mathrm{B}_{12}[3,2] &= 1 \quad \mathrm{B}_{12}[4,4] = i \\ \mathrm{B}_{12}[5,5] &= -1/2 \quad \mathrm{B}_{12}[6,6] = -i\sqrt{3}/2 \\ \mathrm{B}_{12}[3,7] &= 1 \quad \mathrm{B}_{12}[11,4] = i \\ \mathrm{B}_{12}[9,7] &= -1/2 \quad \mathrm{B}_{12}[10,8] = -i\sqrt{3}/2 \\ \mathrm{B}_{12}[9,1] &= 1 \quad \mathrm{B}_{12}[2,9] = 1 \\ \mathrm{B}_{12}[7,9] &= -1/2 quad \mathrm{B}_{12}[12,12] = \sqrt{3}/2. \end{aligned} \tag{54}$$

The rest of $\mathbf{B}_{12}[m,n]$ are zero, and $\mathbf{P}_{12}$ is a sparse matrix that has element one in $[(1,1),(9,2),(8,3),(4,4),(5,5),(10,6),(2,7),(11,8),(6,9),(3,10),(7,11),(12,12)]$ with the others being zeros.

$$\chi_{a_1,a_2,1,1,0,0}(n) = \begin{cases} \exp(i2\pi a_1(\mathrm{ind}_2 n)_5/4)\exp(i2\pi a_2(\mathrm{ind}_2 n)_{13}/12), & \text{for } (n,5)=1,(n,13)=1 \\ 0, & \text{otherwise} \end{cases}$$

$$\text{for } a_1 = 0,1,2,3,\ a_2 = 0,1,\ldots,11, \tag{46}$$

$$\text{where } (\mathrm{ind}_g n)_m = \mathrm{ind}_g n_1 \bmod m \text{ and } n_1 = n \bmod m \tag{47}$$

$$\chi_{0,a_3,1,1,1,0}(n) = \begin{cases} \exp(i2\pi a_3(\mathrm{ind}_2 n)_{13}/12), & (n,5) > 1 \\ 0, & \text{otherwise} \end{cases}$$

$$\text{for } a_3 = 0,1,\ldots,11 \tag{48}$$

$$\begin{aligned} \chi_{a_4,0,1,1,0,1}(n) &= \exp(i2\pi a_4(\mathrm{ind}_2 n)_5/4) \\ &\quad (n,13) > 1, \quad \text{for } a_4 = 0,1,2,3, \\ \chi_{a_4,0,1,1,0,1}(n) &= 0, \quad \text{otherwise} \end{aligned} \tag{49}$$

$$\begin{aligned} \chi_{0,0,1,1,1,1}(n) &= 1, \quad \text{when } n = 0, \chi_{0,0,1,1,1,1}(n) \\ &= 0, \quad \text{otherwise.} \end{aligned} \tag{50}$$

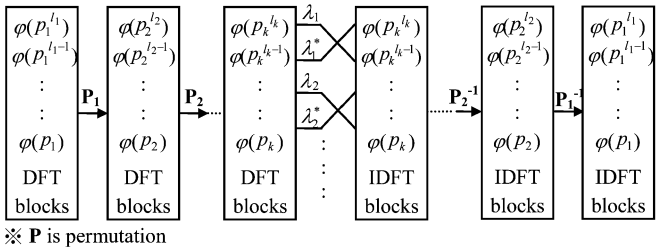

Fig. 1. DFT implementation process for $N = p_1^{l_1} p_2^{l_2}, \ldots, p_k^{l_k}$.

Therefore, we decompose $\mathbf{F}_{65}$ into $\mathbf{F}_4$ and $\mathbf{F}_{12}$. Moreover, $\mathbf{F}_{12}$ can be further decomposed into a combination of $\mathbf{F}_2$. Thus, with iterative decomposition of the DFT matrix, we can find the fast algorithm for computing the DFT.

From (54), $\mathbf{F}_{12}$ needs four real floating-point multiplications. Therefore, from (51), (52), and Appendix B, the 65-pt DFT $\mathbf{F}_{65}$ requires only $10{*}4$ (from $\mathbf{F}_{12}$) $+ 7$ (from $\mathbf{B}_{65}$) $= 47$ real and 56 (from $\mathbf{B}_{65}$) complex floating-point multiplications. Since we can implement each complex multiplication by three real multiplications, only 215 real floating-point multiplications are required. In contrast, if we use the popular prime-factor algorithm to implement the 65-pt DFT, we require $72 * 5 + 8 * 13 = 464$ complex floating-point multiplications, i.e., 1392 real floating-point multiplications.

Generally speaking, for $N = p_1 p_2$, when using the proposed method, the total number of multiplications is about $(N + 2(p_1 N_2 + p_2 N_1))$, where N_1 and N_2 are the numbers of floating-point multiplications required for the $(p_1 - 1)$ and $(p_2 - 1)$-pt DFTs. In comparison with the prime-factor algorithm, because the numbers of the floating-point multiplications for the $(p_1 - 1)$ and $(p_2 - 1)$-pt DFTs are much less than those of p_1 and p_2-pt DFTs, using the proposed method for implementing the DFT is more efficient than using the prime-factor algorithm. For example, when $N = 91 = 13 * 7$, using the proposed method, we need only to use 398 real multiplications to realize the DFT. In contrast, if we use the prime-factor algorithm, 2214 real multiplications are needed. Thus, using the proposed algorithm can greatly improve the efficiency of DFT implementation when N is a prime number or a product of distinct prime numbers.

The general DFT implementation process for the N-point DFT $(N = p_1^{l_1} p_2^{l_2}, \ldots, p_k^{l_k})$ using sub-DFT blocks is shown in Fig. 1, which shows that we can easily combine the DFT blocks on hand to design any higher order DFT module. For example, we can **use only radix-2 DFT modules to design the 65-pt DFT** as in the earlier example [see (51)(52)(53)). In fact, we have the following theorem.

Theorem 1: Since $\varphi(\varphi(\varphi(\cdots)))$ will eventually converge to powers of two [1], [2], **it is possible to implement an arbitrary length DFT with only radix-2 DFT blocks**. For example, when $N = 107$

$$\varphi(107) = 106 = 2 \times 53 \quad \varphi(53) = 52 = 2^2 \times 13$$
$$\varphi(13) = 12 = 2^2 \times 3 \quad \varphi(3) = 2. \tag{55}$$

Thus, we can use butterfly structures to implement the DFT for any N.

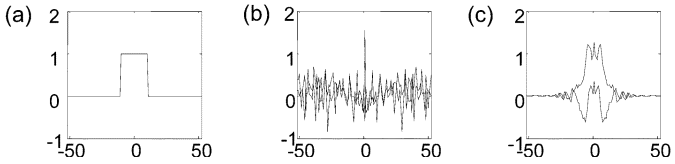

Fig. 2. (a) Input rectangular function. (b) Results of the DFRFT $(\alpha = 0.25)$ based on the proposed CGLS-like eigenvectors. (c) Results of the DFRFT $(\alpha = 0.25)$ based on the eigenvectors derived form $\mathbf{S}$ matrix.

B. DFRFT Based on CGLS-Like DFT Eigenvectors

Pei *et al.*[13], [14] and Candan *et al.*[3] used the eigenvectors derived from the $\mathbf{S}$ matrix [see (3)] to define the DFRFT, which is a generalization of the DFT. In [15] and [16], Vargas-Rubio and Santhanam used another DFT eigenvector set, which is derived from the Grünbaum commuter [6]–[8] to define the DFRFT and use it for chirp signal analysis and speech processing. The DFRFT is defined as

$$\mathbf{F}^{\alpha}\mathbf{x} = \mathbf{E_S}\mathbf{D}^{\alpha}\mathbf{E_S^H}\mathbf{x}$$
$$\mathbf{E}_S : \text{the eigenvectors of } \mathbf{S}$$
$$\alpha : \text{the order of the DFRFT} \tag{56}$$
$$\mathbf{D^{\alpha}} = \text{diag}\{1,\ e^{-j\alpha\pi/2}, \ldots, e^{-j(N-2)\alpha\pi/2}, e^{-jN_1\alpha\pi/2}\} \tag{57}$$

where $N_1 = N - 1$ for odd N and $N_1 = N$ for even N. Since the eigenvectors derived from the $\mathbf{S}$ matrix and the Grünbaum commuter are similar to the samples of the noncentered and the centered continuous Hermite function, respectively, [3], [6]–[8] the performances of the DFRFTs defined in [3], [13]–[16] are very similar to those of the continuous FRFT.

However, if we do not consider whether the DFRFT is similar to the continuous FRFT, we can use the CGLS-like DFT eigenvectors we derived to define a new type of DFRFT (i.e., in (69), $\mathbf{E}_s$ is replaced by the CGLS-like eigenvector set).

An example is shown in Fig. 2 for transforming a 105-point rectangular function using the proposed DFRFT and comparing this with the original DFRFT. Although the DFRFT derived from the proposed eigenvectors does not resemble the continuous FRFT, it is useful for the application of data encryption and watermarks because the outputs of the proposed DFRFT are usually "white-noise-like." Moreover, owning to orthogonality and the wide-spectrum property, it can also be applied in CDMA, OFDM, etc.

In Fig. 3, an example is shown that uses the DFRFT based on the $\mathbf{S}$ matrix and the DFRFT based on the proposed CGLS-like eigenvectors for image encryption. We first perform the DFRFT with order α for the input image to encrypt it. Then, the order α can be treated as the "key." When performing the decryption, we must know the value of α and apply the DFRFT with order $-\alpha$ to recover the original image. If α is wrong, the original image cannot be retrieved.

In Fig. 3(b), (c), and (d), we show the results that of using the DFRFT based on the proposed CGLS-like eigenvectors for image encryption. If we use the correct value of α, as shown in Fig. 3(c), the original image is recovered. When we use a wrong value of α, even if it differs only slightly from the correct one,

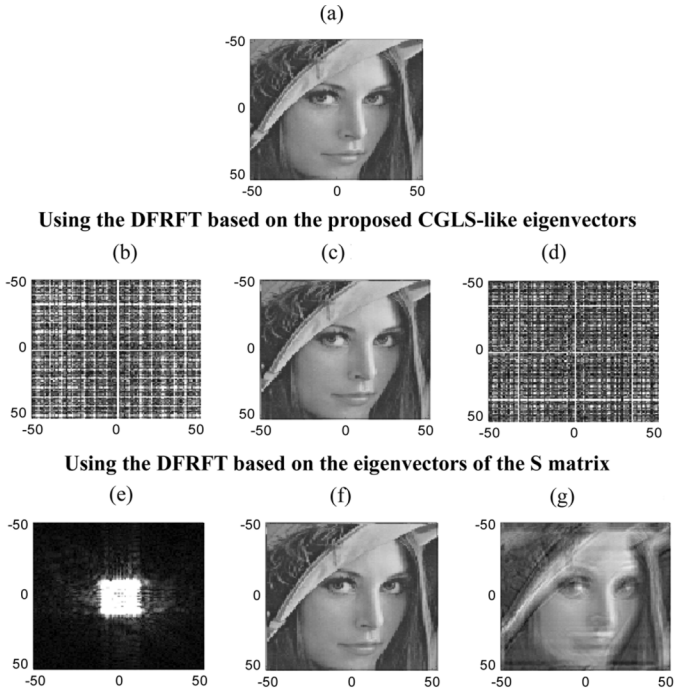

Fig. 3. Image encryption (b), (c), and (d) using DFRFT based on the proposed CGLS-like eigenvectors and (e), (f), and (g) using DFRFT based on the $\mathbf{S}$ matrix. Using DFRFT based on the proposed CGLS-like eigenvectors (a), input image (b), encrypted by DFRFT ($\alpha = 0.75$), (c) recovered image using correct α, (d) recovered image using wrongα, $\alpha = 0.7$ **and using the DFRFT based on the eigenvectors of the S matrix.** (e) Encrypted by DFRFT ($\alpha = 0.75$),. (f) Recovered image. (g) Recovered image using correct α, using wrong α, and $\alpha = 0.7$.

we cannot recover the original image, as shown in Fig. 3(d) (in Fig. 3(d), we use $\alpha = 0.7$, and the correct value of α is 0.75).

In contrast, when using the DFRFT based on the $\mathbf{S}$ matrix, from Fig. 3(g), it can be seen that, if the value of α is wrong, we can still retrieve many features of the original image. To enhance the security, we should ensure that the original data cannot be retrieved when the key is wrong. According to the results shown in Fig. 3(d) and (g), the DFRFT derived from CGLS-like eigenvectors is more effective for encryption.

Another important advantage of the DFRFT based on CGLS-like eigenvectors is that its complexity is $O(Nlog_2N)$, which is the same as that of the DFT. In contrast, the complexity of the DFRFT based on the $\mathbf{S}$ matrix is $O(N^2)$. Thus, for the applications of encryption, watermarks, CDMA, and OFDM, we can use the proposed DFRFT instead of the DFRFT based on the $\mathbf{S}$ matrix to increase efficiency.

V. Conclusion

In this paper, we have proposed a systematic method for deriving the orthogonal DFT eigenvectors based on the CGLS for any length N. Since they have closed-form solutions, it is possible to find the DFT eigenvectors accurately even for very large N. Moreover, since the eigenvector expansion operation can be implemented by a fast algorithm, we can use the proposed eigenvectors to improve the efficiency of the DFT, particularly for the case where N is prime or a product of prime numbers. We believe that there are a variety of applications for our proposed closed-form orthogonal DFT eigenvectors.

Appendix A

11-pt real DFT eigenvectors (denoted by $E_k[n]$) derived from the CGLS are

$$
\begin{aligned}
E_0[0] &= 11^{1/2} - 11^{-1/2} \\
E_0[n] &= 1 - 11^{-1/2} \text{ for } n \neq 0 \\
E_1[0] &= -11^{1/2} + 11^{-1/2} \\
E_1[n] &= 1 + 11^{-1/2} \text{ for } n \neq 0 \\
E_k[n] &= \operatorname{Im}\Big[\exp\left(j2\pi a \cdot \operatorname{ind}_2 n/10\right) \\
&\qquad - j\lambda_a \cdot \exp\left(-j2\pi a \cdot \operatorname{ind}_2 n/10\right)\Big] \\
&\quad \text{when } k = 2, 6, a = k/2 (a = 1, 3) \\
E_k[n] &= \operatorname{Im}\Big[\exp\left(j2\pi a \cdot \operatorname{ind}_2 n/10\right) \\
&\qquad + j\lambda_a \cdot \exp(-j2\pi a \cdot \operatorname{ind}_2 n/10)\Big] \\
&\quad \text{when } k = 3, 7, a = (k-1)/2 (a = 1, 3), \\
E_k[n] &= \operatorname{Im}\Big[\exp(j2\pi a \cdot \operatorname{ind}_2 n/10) \\
&\qquad + \lambda_a \cdot \exp(-j2\pi a \cdot \operatorname{ind}_2 n/10)\Big] \\
&\quad \text{when } k = 4, 8, a = k/2 (a = 2, 4) \\
E_k[n] &= \operatorname{Im}\Big[\exp(j2\pi a \cdot \operatorname{ind}_2 n/10) \\
&\qquad - \lambda_a \cdot \exp(-j2\pi a \cdot \operatorname{ind}_2 n/10)\Big] \\
&\quad \text{when } k = 5, 9, a = (k-1)/2 (a = 2, 4) \\
E_{10}[n] &= [1, -1, 1, 1, 1, -1, -1, -1, 1, -1], \\
\lambda_a &= \sqrt{11}^{-1} \sum_{m=1}^{10} \exp\left[i2\pi a \cdot \operatorname{ind}_2 m/10\right] \exp(-i2\pi m/11).
\end{aligned}
$$

In the case where $k = 2$ to 9, we can also take the real part instead of the imaginary part.

Appendix B

We can express $\mathbf{B}_{65}$ in (45) by an integer matrix $\mathbf{U}$ and a diagonal matrix $\mathbf{V}$, i.e., $\mathbf{B}_{65} = \mathbf{UV}$.

$$
\begin{aligned}
U[1,1] &= 1 \quad U[11,25] = 4 \quad U[24,12] = 4 \\
U[43,53] &= 1 \quad U[1,2] = 1 \quad U[12,12] = 4 \\
U[24,24] &= -1 \quad U[44,52] = 1 \quad U[1,6] = 3 \\
U[12,24] &= 4 \quad U[25,11] = 4 \quad U[45,51] = 1 \\
U[1,18] &= 3 \quad U[13,11] = 4 \quad U[25,23] = -1 \\
U[46,50] &= 1 \quad U[2,1] = 1 \quad U[13,23] = 4 \\
U[26,10] &= 4 \quad U[47,49] = 1 \quad U[2,2] = -1/4 \\
U[14,10] &= 4 \quad U[26,22] = -1 \quad U[48,48] = 1 \\
U[2,6] &= 3 \quad U[14,22] = 4 \quad U[27,9] = 4 \\
U[49,47] &= 1 \quad U[2,18] = -1/4 \quad U[15,9] = 4 \\
U[27,21] &= -1] \quad U[50,46] = 1 \quad U[3,5] = 4 \\
U[15,21] &= 4 \quad U[28,8] = 4 \quad U[51,45] = 1 \\
U[3,54] &= 4 \quad U[16,8] = 4 \quad U[28,20] = -1 \\
U[52,44] &= 1 \quad U[4,4] = 4 \quad U[16,20] = 4 \\
U[29,7] &= 4 \quad U[53,43] = 1 \quad U[4,42] = 4]
\end{aligned}
$$

$$
\begin{aligned}
U[17,7] &= 4 \quad U[29,19] = -1 \quad U[54,3] = 4 \\
U[5,3] &= 4 \quad U[17,19] = 4 \quad U[30,5] = 4 \\
U[54,30] &= -1 \quad U[5,30] = 4 \quad U[18,1] = 1 \\
U[30,54] &= -1 \quad U[55,41] = 1 \quad U[6,1] = 1 \\
U[18,2] &= -1/4 \quad U[31,65] = 1 \quad U[56,40] = 1 \\
U[6,2] &= 1 \quad U[18,6] = -1/4 \quad U[32,64] = 1 \\
U[57,39] &= 1 \quad U[6,6] = -1/4 \quad U[18,18] = 1/16 \\
U[33,63] &= 1 \quad U[58,38] = 1 \quad U[6,18] = -1/4 \\
U[19,17] &= 4 \quad U[34,62] = 1 \quad U[59,37] = 1 \\
U[7,17] &= 4 \quad U[19,29] = -1 \quad U[35,61] = 1 \\
U[60,36] &= 1 \quad U[7,29] = 4 \quad U[20,16] = 4 \\
U[36,60] &= 1 \quad U[61,35] = 1 \quad U[8,16] = 4 \\
U[20,28] &= -1 \quad U[37,59] = 1 \quad U[62,34] = 1 \\
U[8,28] &= 4 \quad U[21,15] = 4 \quad U[38,58] = 1 \\
U[63,33] &= 1 \quad U[9,15] = 4 \quad U[21,27] = -1 \\
U[39,57] &= 1 \quad U[64,32] = 1 \quad U[9,27] = 4 \\
U[22,14] &= 4 \quad U[40,56] = 1 \quad U[65,31] = 1 \\
U[10,14] &= 4 U[22,26] = -1 \quad U[41,55] = 1 \\
U[10,26] &= 4 \quad U[23,13] = 4 \quad U[42,4] = 4 \\
U[11,13] &= 4 \quad U[23,25] = -1 \quad U[42,42] = -1
\end{aligned}
$$

The rest of $U[m,n] = 0$.

$$
\begin{aligned}
V[1,1] &= 1 \quad V[2,2] = 1 \quad V[3,3] = -0.0396 - 0.0245j \\
V[4,4] &= -0.0466 \quad V[5,5] = 0.0396 - 0.0245j \\
V[6,6] &= 1/3 \quad V[7,7] = -0.0392 - 0.0641j \\
V[8,8] &= -0.0646 - 0.0384j \quad V[9,9] = 0.0218 + 0.0719j \\
V[10,10] &= 0.0190 + 0.0727j \quad V[11,11] = 0.0029 + 0.0751j \\
V[12,12] &= -0.0751 \quad V[13,13] = -0.0029 + 0.0751j \\
V[14,14] &= 0.0190 - 0.0727j \quad V[15,15] = -0.0218 + 0.0719j \\
V[16,16] &= -0.0646 + 0.0384j \quad V[17,17] = 0.0392 - 0.0641j \\
V[18,18] &= 1/3 \quad V[19,19] = -0.0392 - 0.0641j \\
V[20,20] &= -0.0646 - 0.0384j \quad V[21,21] = 0.0218 + 0.0719j \\
V[22,22] &= 0.0190 + 0.0727j \quad V[23,23] = 0.0029 + 0.0751j \\
V[24,24] &= -0.0751 \quad V[25,25] = -0.0029 + 0.0751j \\
V[26,26] &= 0.0190 - 0.0727j \quad V[27,27] = -0.0218 + 0.0719j \\
V[28,28] &= -0.0646 + 0.0384j \quad V[29,29] = 0.0392 - 0.0641j \\
V[30,30] &= -0.0396 - 0.0245j \quad V[31,31] = -0.0007 + 0.1680j \\
V[32,32] &= 0.0777 + 0.1489j \quad V[33,33] = 0.0431 - 0.1623j \\
V[34,34] &= 0.0493 - 0.1606j \quad V[35,35] = 0.0827 - 0.1462j \\
V[36,36] &= 0.1429 + 0.0833j \quad V[37,37] = 0.0938 - 0.1394j \\
V[38,38] &= -0.1215 + 0.1159j \quad V[39,39] = 0.1259 - 0.1112j \\
V[40,40] &= 0.1679 + 0.0029j \quad V[41,41] = -0.1499 + 0.0757j \\
V[42,42] &= -0.0466 \quad V[43,43] = 0.0877 + 0.1423j \\
V[44,44] &= 0.1444 + 0.0858j \quad V[45,45] = -0.0487 - 0.1608j \\
V[46,46] &= -0.0424 - 0.1625j \quad V[47,47] = -0.0065 - 0.1678j \\
V[48,48] &= 0.1680 \quad V[49,49] = 0.0065 - 0.1678j \\
V[50,50] &= -0.0424 + 0.1625j \quad V[51,51] = 0.0487 - 0.1608j \\
V[52,52] &= 0.1444 - 0.0858j \quad V[53,53] = -0.0877 + 0.1432j \\
V[54,54] &= 0.0396 - 0.0245j \quad V[55,55] = -0.1499 - 0.0757j \\
V[56,56] &= -0.1679 + 0.0029j \quad V[57,57] = 0.1259 + 0.1112j \\
V[58,58] &= 0.1215 + 0.1159j \quad V[59,59] = 0.0938 + 0.1394j \\
V[60,60] &= -0.1429 + 0.0883j \quad V[61,61] = 0.0827 + 0.1462j \\
V[62,62] &= -0.0493 - 0.1606j \quad V[63,63] = 0.0431 + 0.1623j \\
V[64,64] &= -0.0777 + 0.1489j \quad V[65,65] = -0.0007 - 0.1680j
\end{aligned}
$$

The rest of $V[m,n] = 0$.

The elements of $\mathbf{P}_{65}$ in (64) are as follows:

$$
\begin{aligned}
P[1,1] &= 1 \quad P[56,14] = 1 \quad P[22,27] = 1 \\
P[44,40] &= 1 \quad P[55,53] = 1 \quad P[27,2] = 1 \\
P[61,15] &= 1 \quad P[57,28] = 1 \quad P[29,41] = 1 \\
P[28,54] &= 1 \quad P[14,3] = 1 \quad P[31,16] = 1 \\
P[42,29] &= 1 \quad P[15,42] = 1 \quad P[8,55] = 1 \\
P[40,4] &= 1 \quad P[16,17] = 1 \quad P[54,30] = 1 \\
P[60,43] &= 1 \quad P[63,56] = 1 \quad P[53,5] = 1 \\
P[2,18] &= 1 \quad P[34,31] = 1 \quad P[50,44] = 1 \\
P[58,57] &= 1 \quad P[41,6] = 1 \quad P[47,19] = 1 \\
P[24,32] &= 1 \quad P[45,45] = 1 \quad P[23,58] = 1 \\
P[21,7] &= 1 \quad P[37,20] = 1 \quad P[19,33] = 1 \\
P[10,46] &= 1 \quad P[38,59] = 1 \quad P[11,8] = 1 \\
P[32,21] &= 1 \quad P[49,34] = 1 \quad P[25,47] = 1 \\
P[13,60] &= 1 \quad P[6,9] = 1 \quad P[62,22] = 1 \\
P[64,35] &= 1 \quad P[65,48] = 1 \quad P[33,61] = 1 \\
P[36,10] &= 1 \quad P[12,23] = 1 \quad P[39,36] = 1 \\
P[20,49] &= 1 \quad P[43,62] = 1 \quad P[51,11] = 1 \\
P[52,24] &= 1 \quad P[59,37] = 1 \quad P[30,50] = 1 \\
P[48,63] &= 1 \quad P[26,12] = 1 \quad P[7,25] = 1 \\
P[4,38] &= 1 \quad P[35,51] = 1 \quad P[18,64] = 1 \\
P[46,13] &= 1 \quad P[17,26] = 1 \quad P[9,39] = 1 \\
P[5,52] &= 1 \quad P[3,65] = 1.
\end{aligned}
$$

The rest of $P[m,n] = 0$.

REFERENCES

[1] J. H. McClellan, "Eigenvalue and eigenvector decomposition of the discrete Fourier transform," *IEEE Trans. Audio Electroacoust.*, vol. 20, no. 1, pp. 66–74, Mar. 1972.

[2] B. W. Dickinson and K. Steiglitz, "Eigenvectors and functions of the discrete Fourier transform," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. 30, no. 1, pp. 25–31, Feb. 1982.

[3] C. Candan, M. A. Kutay, and H. M. Ozaktas, "The discrete fractional Fourier transform," *IEEE Trans. Signal Process.*, vol. 48, no. 5, pp. 1329–1337, May 2000.

[4] N. M. Atakishiyev, L. E. Vicent, and K. B. Wolf, "Continuous versus discrete fractional Fourier transforms," *J. Comput. Appl. Math.*, vol. 107, no. 1, pp. 73–95, Jul. 1999 .

[5] M. L. Mehta, "Eigenvalues and eigenvectors of the finite Fourier transform," *J. Math. Phys.*, vol. 28, no. 4, pp. 781–785, Apr. 1987.

[6] F. A. Grünbaum, "The eigenvectors of the discrete Fourier transform: A version of the Hermite functions," *J. Math. Anal. Appl.*, vol. 88, no. 2, pp. 355–363, 1982.

[7] S. Clary and D. H. Mugler, "Shifted Fourier matrices and their tridiagonal commuters," *SIAM J. Matrix Anal. Appl.*, vol. 24, no. 3, pp. 809–821, Mar. 2003.

[8] D. H. Mugler and S. Clary, "Discrete Hermite functions and the fractional Fourier transform," in *Proc. Int. Conf. Sampling Theory Appl.*, 2001, pp. 303–308.
[9] T. Erseghe and G. Cariolaro, "An orthonormal class of exact and simple DFT eigenvectors with a high degree of symmetry," *IEEE Trans. Signal Process.*, vol. 51, no. 10, pp. 2527–2539, Oct. 2003.
[10] L. G. Hua, *Introduction to Number Theory*. New York: Springer-Verlag, 1997, ch. 7.
[11] M. R. Schroeder, *Number Theory in Science and Communications*. Berlin, Germany: Springer-Verlag, 1997.
[12] M. S. Pattichis, A. C. Bovik, J. W. Havlicek, and N. D. Sidiropoulos, "Multidimensional orthogonal FM transforms," *IEEE Trans. Image Process.*, vol. 10, no. 3, pp. 448–464, Mar. 2001.
[13] S. C. Pei and M. H. Yeh, "Discrete fractional Fourier transform," in *Proc. IEEE Int. Symp. Circuits Syst*, May 1996, pp. 536–539.
[14] S. C. Pei, M. H. Yeh, and C. C. Tseng, "Discrete fractional Fourier transform based on orthogonal projections," *IEEE Trans. Signal Process.*, vol. 47, no. 5, pp. 1335–1348, May 1999.
[15] J. G. Vargas-Rubio and B. Santhanam, "On the multiangle centered discrete fractional Fourier transform," *IEEE Signal Process. Lett.*, vol. 12, no. 4, pp. 273–276, Apr. 2005.
[16] J. G. Vargas-Rubio and B. Santhanam, "An improved spectrogram using the multiangle centered discrete fractional Fourier transform," in *Proc. ICASSP*, 2005, vol. 4, pp. 505–508.
[17] S. C. Pei and J. J. Ding, "Eigenfunctions of Fourier and fractional Fourier transforms with complex offsets and parameters," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 54, no. 7, pp. 1599–1611, Jul. 2007.
[18] C. Candan, "On higher order approximations for Hermite–Gaussian functions and discrete fractional Fourier transforms," *IEEE Signal Process. Lett.*, vol. 14, no. 10, pp. 699–702, Oct. 2007.
[19] C. C. Yang, "Modified Legendre sequence for optical-CDMA based passive optical networks," *IEEE Commun. Lett.*, vol. 10, no. 5, pp. 393–395, May 2006.
[20] M. Wang, "On factor prime factorizations for n-D polynomial matrices," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 54, no. 6, pp. 1398–1405, Jun. 2007.

Soo-Chang Pei (SM'89–F'00) was born in Soo-Auo, Taiwan, in 1949. He received the B.S.E.E. degree from the National Taiwan University (NTU), Taipei, Taiwan, in 1970 and the M.S.E.E. and Ph.D. degrees from the University of California, Santa Barbara (UCSB), Santa Barbara, in 1972 and 1975, respectively.

He was an Engineering Officer with the Chinese Navy Shipyard from 1970 to 1971. From 1971 to 1975, he was a Research Assistant with UCSB. He was a Professor and the Chairman with the Electrical Engineering Department, Tatung Institute of Technology, Taipei, and NTU, from 1981 to 1983 and 1995 to 1998, respectively. He is currently the Dean of the Electrical Engineering and Computer Science College and a Professor with the Electrical Engineering Department, NTU. His research interests include digital signal processing, image processing, optical information processing, and laser holography.

Dr. Pei is a member of Eta Kappa Nu and the Optical Society of America. He was the recipient of the National Sun Yet-Sen Academic Achievement Award in Engineering in 1984, the Distinguished Research Award from the National Science Council from 1990 to 1998, the outstanding Electrical Engineering Professor Award from the Chinese Institute of Electrical Engineering in 1998, the Academic Achievement Award in Engineering from the Ministry of Education in 1998, the Pan Wen-Yuan Distinguished Research Award in 2002, and the National Chair Professor Award from the Ministry of Education in 2002. He was the President of the Chinese Image Processing and Pattern Recognition Society in Taiwan from 1996 to 1998. He became an IEEE Fellow in 2000 for contributions to the development of digital eigenfilter design, color image coding and signal compression, and electrical engineering education in Taiwan.

Chia-Chang Wen was born in Taipei, Taiwan. He received the B.S. and M.S. degrees in electrical engineering from National Taiwan University (NTU), Taipei, in 2000 and 2002, respectively.

He is currently the Chief Technician with NTU Hospital Information System Office. His research interests include number theory, digital signal processing, digital image processing, bioinformatics, and hospital information system design.

Jian-Jiun Ding was born in Taiwan in 1973. He received the B.S., M.S., and Ph.D. degrees in electrical engineering from the National Taiwan University (NTU), Taipei, Taiwan, in 1995, 1997, and 2001, respectively.

From 2001 to 2005, he was a Postdoctoral Researcher with the Department of Electrical Engineering, NTU, where he is currently an Assistant Professor. His current research areas are in time-frequency analysis, fractional Fourier transforms, linear canonical transforms, image processing, orthogonal polynomials, fast algorithms, quaternion algebra, pattern recognition, filter design, etc.