Fast DFT Matrices Transform Based on Generalized Prime Factor Algorithm

Ying Guo, Yun Mao, Dong Sun Park, and Moon Ho Lee

Abstract: **Inspired by fast Jacket transforms, we propose simple factorization and construction algorithms for the M-dimensional discrete Fourier transform (DFT) matrices underlying generalized Chinese remainder theorem (CRT) index mappings. Based on successive coprime-order DFT matrices with respect to the CRT with recursive relations, the proposed algorithms are presented with simplicity and clarity on the basis of the yielded sparse matrices. The results indicate that our algorithms compare favorably with the direct-computation approach.**

Index Terms: **Discrete Fourier transform (DFT) matrices, fast Jacket transform, generalized prime factor algorithm (GPFA), Kronecker product, sparse matrices.**

I. INTRODUCTION

It is well known that the Hadamard transform and its generalizations can be used to represent signals and images [1]–[3]. Motivated by the center-weighted Hadamard transform (CWHT) [4], in 1989, Lee proposed *Jacket* matrices with elegant inverse constraints. The interesting orthogonal matrices, such as Hadamard, discrete Fourier transform (DFT), and Slant and Haar matrices, all belong to the *Jacket* matrices family [5]. Because of the simple and efficient calculations of the inverse matrix, the Jacket transform and its reverse transforms have been extensively used [5]–[11]. These transforms are useful for signal processing, communications, cryptography, and image compression [12]–[16].

On the other hand, bounds on generalized prime factor algorithms (GPFA) for fast Fourier transform (FFT) have been widely established [17]–[22]. In information processing, it is important to know the exact structure of the matrix and its decomposition. To achieve this, the fast Jacket transforms are derived using recursive relations based on the Kronecker product of lower-order matrices [9]–[11]. Given this motivation, we further consider the combination of fast Jacket transforms with the GPFA underlying generalized Chinese remainder theorem (CRT) index mappings. In particular, we suggest efficient factorization and construction approaches for M-dimensional DFT matrices.

Since the mapped DFT matrix following an important historical result has close relation with Kronecker product, the M-dimensional DFT matrices can be factorized and constructed with much smaller computation than the previous transforms.

This paper is organized as follows. Section II introduces Jacket matrices and their fast transforms. Section III defines DFT matrices which are class of Jacket matrices which are a class of Jacket matrices. Section IV discusses general fast factorization and construction algorithms for M-dimensional DFT matrices. We then describe in detail the construction approach for 2-D DFT matrices. Finally, a discussions and our conclusions are presented in Section V.

Manuscript received April 15, 2010; approved for publication by Xiang-Gen Xia , Division I Editor, September 17, 2010.

This work was supported by the National Natural Science Foundation of China (60902044), the Ph.D. Programs Foundation of the Ministry of Education of China (20090162120070), the Postdoctoral Science Foundation of China (200801341), the State Key Laboratory of Advanced Optical Communication Systems and Networks (2008SH01), WCU R32-2010-000-20014-0 NRF, Korea, and in part by the Second Stage of the Brain Korea 21 programs, Chonbuk National University, Korea.

Y. Guo and Y. Mao are with the School of Information Science and Engineering, Central South University, Changsha 410083, China, and Y. Mao is the correspondence author, email: {yingguo, yunmao}@csu.edu.cn.

D. S. Park and M. H. Lee are with the Electronics and Information Engineering, Chonbuk National University, Chonju 561-756, Korea, email: {dspark, moonho}@jbnu.ac.kr.

II. JACKET MATRICES AND THEIR TRANSFORMS

In this section, we introduce Jacket matrices and two typical fast Jacket transforms. For clarity, we begin with the Kronecker product.

Definition 1. Let matrix A be $m \times n$ and matrix B $k \times l$. The Kronecker product of A and B is an $mk \times nl$ matrix $mk \times nl$ and is denoted $A \otimes B$, i.e.,

$$A \otimes B = \begin{bmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,n}B \\ a_{2,1B} & a_{2,2}B & \cdots & a_{2,n}B \\ \vdots & \vdots & & \vdots \\ a_{m,1}B & a_{m,2}B & \cdots & a_{m,n}B \end{bmatrix}. \quad (1)$$

Some properties of the Kronecker product [1]–[3] will be useful for the fast constructions of DFT matrices in this paper (assume the matrices involved have appropriate dimensions):

Property 1: $(A \otimes B) \otimes C = A \otimes (B \otimes C)$,

Property 2: $A \otimes (B \otimes C) = (A \otimes B) \otimes C$,

Property 3: $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.

On the other hand, the CWHT was first discovered as a typical case of Jacket matrices whose inverse matrix is found by taking the elementwise inverse. We extend this idea and give a general definition of Jacket matrices [5].

Definition 2. Consider a square matrix $[J]_m = [j_{s,t}]_{m \times m}$. If its inverse matrix is obtained simply by taking the element-wise inverse, i.e.,

$$[J]_m^{-1} = \frac{1}{C}[1/j_{s,t}]_{m \times m}^T$$

for $0 \le s, t \le m-1$, where C is a normalized constant, then we call $[J]_m$ a Jacket matrix. That is, we have

$$[J]_m = \begin{bmatrix} j_{0,0} & j_{0,1} & \cdots & j_{0,m-1} \\ j_{1,0} & j_{1,1} & \cdots & j_{1,m-1} \\ \vdots & \vdots & & \vdots \\ j_{m-1,0} & j_{m-1,1} & \cdots & j_{m-1,m-1} \end{bmatrix} \quad (2)$$

and its inverse

$$[J]_m^{-1} = \frac{1}{C}\begin{bmatrix} 1/j_{0,0} & 1/j_{0,1} & \cdots & 1/j_{0,m-1} \\ 1/j_{1,0} & 1/j_{1,1} & \cdots & 1/j_{1,m-1} \\ \vdots & \vdots & & \vdots \\ 1/j_{m-1,0} & 1/j_{m-1,1} & \cdots & 1/j_{m-1,m-1} \end{bmatrix}^T \quad (3)$$

where T denotes the transpose of a matrix. Obviously, from this definition, we have the following relation:

$$\sum_{k=1}^{m} \frac{j_{s,k}}{j_{t,k}} = 0 \quad (4)$$

where $1 \le s,t \le m$, $s \ne t$. It is obvious that because of the special structure of the Jacket matrix, its inverse can be obtained via simple algebra [8], [11], [13].

Given the simplicity of the calculation of the inverse matrix, the Jacket transform and reverse Jacket transform based on Jacket matrices have been widely applied [5]–[11]. We now present the fast Jacket transforms construction and factorization algorithms for large Jacket matrices.

Theorem 1. Suppose J_p and J_q are Jacket matrices, where p and q are prime numbers. Let m and n be non-negative integers. Then, larger Jacket matrices $J_{N=p^m q^n}$ may be constructed in the following way:

$$\begin{aligned} J_N &= \left\{ I_{q^n} \otimes \left(\prod_{i=0}^{m-1} I_{p^{m-i-1}} \otimes J_p \otimes I_{p^i} \right) \right\} \\ &\quad \cdot \left\{ \left(\prod_{i=0}^{n-1} I_{q^{n-i-1}} \otimes J_q \otimes I_{q^i} \right) \otimes I_{p^m} \right\} \\ &= \left\{ I_{q^n} \otimes \left(\prod_{i=1}^{m} I_{p^{m-i}} \otimes J_p \otimes I_{p^{i-1}} \right) \right\} \\ &\quad \cdot \left\{ \left(\prod_{i=1}^{n} I_{q^{n-i}} \otimes J_q \otimes I_{q^{i-1}} \right) \otimes I_{p^m} \right\} \end{aligned} \quad (5)$$

where I_N is the $N \times N$ identity matrix.

Proof: Based on the Jacket matrix J_p for the prime number p and the nonnegative integer m, we construct a larger Jacket matrix J_{p^m} as follows.

$$\begin{aligned} J_{p^m} &= J_{p^{m-1}} \otimes J_p \\ &= \prod_{i=1}^{m} I_{p^{i-1}} \otimes J_p \otimes I_{p^{n-i}}. \end{aligned} \quad (6)$$

By the properties of the Kronecker product, we have

$$\begin{aligned} J_{p^m q^n} &= J_{q^n} \otimes J_{p^m} \\ &= (I_{q^n} J_{q^n}) \otimes (J_{p^m} I_{p^m}) \end{aligned} \quad (7)$$

The larger Jacket matrix $J_{p^m q^n}$ can been constructed using (7). □

If J_N can be factored into J_p and J_q, a decomposition algorithm is possible. The decomposition is the reverse of the construction. Note that the factorizable condition is the same as that for the Kronecker decomposition, i.e., if a matrix

$$C = C_1 \cdots C_i \cdots C_L$$

where C_i can be expressed in a Kronecker form, then C can be factored [10].

Corollary 1. Given a Jacket matrix J_N of order $N = p^m q^n$, if J_N can be factored into J_p and J_q, then the Jacket matrix J_N can be decomposed via (7).

We note that an arbitrary large Jacket matrix can be expressed as a Kronecker product of such matrices using Theorem 1. However, in special cases where the matrix cannot be factored, we must use a special method for the construction and decomposition.

III. CONSTRUCTIONS OF DFT MATRICES

We first introduce the N-point DFT matrix defined by

$$C(k) = \sum_{n=0}^{N-1} x(n) W_N^{nk} \quad (8)$$

where $W_N = e^{-j(2\pi/N)}$ and $k = 0, 1, ..., N-1$.

Definition 3. The $N \times N$ matrix $F_N = [W_N^{st}]$, for $s,t \in \{0, 1, ..., N-1\}$, i.e.,

$$F_N = \begin{bmatrix} W_N^0 & W_N^0 & \cdots & W_N^0 & W_N^0 \\ W_N^0 & W_N^1 & \cdots & W_N^{N-2} & W_N^{N-1} \\ W_N^0 & W_N^2 & \cdots & W_N^{2(N-2)} & W_N^{2(N-1)} \\ W_N^0 & W_N^3 & \cdots & W_N^{3(N-2)} & W_N^{3(N-1)} \\ \vdots & \vdots & & \vdots & \vdots \\ W_N^0 & W_N^{N-1} & \cdots & W_N^{(N-1)(N-2)} & W_N^{(N-1)^2} \end{bmatrix}, \quad (9)$$

is called the N-point DFT matrix. It is a square matrix whose rows and columns are indexed by s and t, respectively, such that the entry in row s and column t is W_N^{st}, for $0 \le s,t \le N-1$. Observe that W_N^N is the complex unit and limits elements in the matrix to a natural circle field of modulo N. One may easily check that the inverse is $F_N^{-1} = \frac{1}{N}[W_N^{-st}]^T$, which satisfies Definition 2. Thus, DFT matrices are a class of Jacket matrices.

The pattern is clearer in matrix form. For $N = 2$, $N = 3$, and $N = 4$, we have

$$F_2 = \begin{bmatrix} W_2^0 & W_2^0 \\ W_2^0 & W_2^1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$F_2^{-1} = \frac{1}{2}\begin{bmatrix} W_2^0 & W_2^0 \\ W_2^0 & W_2^{-1} \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$F_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & e^{\frac{-j2\pi}{3}} & e^{\frac{-j4\pi}{3}} \\ 1 & e^{\frac{-j4\pi}{3}} & e^{\frac{-j8\pi}{3}} \end{bmatrix}, F_3^{-1} = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & e^{\frac{j2\pi}{3}} & e^{\frac{j4\pi}{3}} \\ 1 & e^{\frac{j4\pi}{3}} & e^{\frac{j8\pi}{3}} \end{bmatrix},$$

$$F_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -j & -1 & j \\ 1 & -1 & 1 & -1 \\ 1 & j & -1 & -j \end{bmatrix}, F_4^{-1} = \frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & j & -1 & -j \\ 1 & -1 & 1 & -1 \\ 1 & -j & -1 & j \end{bmatrix}. \quad (10)$$

We note that F_2 is the lowest-order Hadamard matrix $[H]_2$; and if we perform row and column permutations of F_4, we can obtain

$$F_4' = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -j & j & -1 \\ 1 & j & -j & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \tag{11}$$

which is the lowest-order center-weighted Hadamard matrix $[WH]_4$ [4]. In fact, the DFT matrix F_N of order $N = 4, 8, 16, \cdots$, can generally be converted to a center-weighted Hadamard matrix $[WH]_N$ via a series of row and column permutations.

Using matrix notation $F\vec{x} = \vec{C}$, we rewrite (8) as

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & W_N^1 & \cdots & W_N^{N-1} \\ 1 & W_N^2 & \cdots & W_N^{2(N-1)} \\ \vdots & \vdots & & \vdots \\ 1 & W_N^{N-1} & \cdots & W_N^{(N-1)^2} \end{bmatrix} \begin{bmatrix} x(0) \\ x(1) \\ x(2) \\ \vdots \\ x(N-1) \end{bmatrix} = \begin{bmatrix} C(0) \\ C(1) \\ C(2) \\ \vdots \\ C(N-1) \end{bmatrix} \tag{12}$$

and obtain the inverse of F_N as follows:

$$F_N^{-1} = \frac{1}{N} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & W_N^{-1} & \cdots & W_N^{-(N-1)} \\ 1 & W_N^{-2} & \cdots & W_N^{-2(N-1)} \\ \vdots & \vdots & & \vdots \\ 1 & W_N^{-(N-1)} & \cdots & W_N^{-(N-1)^2} \end{bmatrix}. \tag{13}$$

IV. FAST JACKET TRANSFORM BASED ON GPFA

This section considers combining fast Jacket transforms and the GPFA underlying the generalized CRT index scheme. An historical result will play an important role in this investigation.

For the one-dimensional DFT defined by (8), assume that N can be factored into mutually prime (i.e., coprime) integers

$$N = N_1 N_2 \cdots N_m. \tag{14}$$

For $m = 2$, Temperton [18] proposed a simple index scheme using the CRT. The indexes become

$$\begin{aligned} n &=< K_1 n_1 + K_2 n_2 >_N, \\ k &=< K_3 k_1 + K_4 k_2 >_N \end{aligned} \tag{15}$$

under the conditions $< K_1 K_3 >_N = N_2$, $< K_2 K_4 >_N = N_1$ and $< K_1 K_4 >_N = < K_2 K_3 >_N = 0$, where the notation $< \cdot >_N$ represents mod N. The result is the two-dimensional DFT transform

$$\begin{aligned} \hat{C}(k_1, k_2) &= \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \hat{x}(n_1, n_2) \\ &\quad \cdot W_N^{K_1 K_3 n_1 k_1} W_N^{K_1 K_4 n_1 k_2} W_N^{K_2 K_3 n_2 k_1} W_N^{K_2 K_4 n_2 k_2} \\ &= \sum_{n_2=0}^{N_2-1} \sum_{n_1=0}^{N_1-1} \hat{x}(n_1, n_2) W_{N_1}^{n_1 k_1} W_{N_2}^{n_2 k_2} \end{aligned} \tag{16}$$

where $0 \le n_1, k_1 \le N_1 - 1$ and $0 \le n_2, k_2 \le N_2 - 1$. Using the more general form of CRT [21], one may obtain an M-dimensional DFT as follows:

Theorem 2. The index mapping

$$\begin{aligned} n &=< K_1 n_1 + K_2 n_2 + \cdots + K_m n_m >_N, \\ k &=< L_1 k_1 + L_2 k_2 + \cdots + L_m k_m >_N \end{aligned} \tag{17}$$

under the conditions

$$< K_i L_i >_N = M_i$$

where $M_i = N/N_i$, for $i = 1, 2, \cdots, m$, and $< K_i L_j >_N = 0$, for $i \neq j$ converts the one-dimensional DFT into an M-dimensional DFT

$$\begin{aligned} \hat{C}(k_1, k_2, \cdots, k_m) &= \sum_{n_m=0}^{N_m-1} \cdots \sum_{n_2=0}^{N_2-1} \sum_{n_1=0}^{N_1-1} \hat{x}(n_1, n_2 \cdots n_m) \\ &\quad \cdot W_{N_1}^{n_1 k_1} W_{N_2}^{n_2 k_2} \cdots W_{N_m}^{n_m k_m} \end{aligned} \tag{18}$$

where

$$\hat{x}(n_1, n_2 \cdots n_m) = x\left(\left\langle \sum_{i=1}^{m} K_i n_i \right\rangle_N\right),$$

$$\hat{C}(k_1, k_2, \cdots, k_m) = C\left(\left\langle \sum_{j=1}^{m} L_i k_i \right\rangle_N\right).$$

In above formula, N is given by (14) based on m mutually prime factors N_i for $i = 1, 2, \cdots, m$. The details of these maps are given in [18] and [21]. Other index schemes [18]–[20], [22] can also achieve this result.

For two-dimensional DFT, Temperton noted that combining Ruritanian and CRT leads to true 2-D DFTs ($F_{N_1} \otimes F_{N_2}$) that require no "twiddle factors." This combination mapping is not unique in eliminating twiddle factors, as observed by Lun and Siu in 1993, but any mapping that eliminates twiddle factors must belong to the set of CRT maps. This result also holds for M-dimensional DFT [22]. It is somewhat tedious to show that the twiddle factors disappear. Here, we present only an important historical result. Using matrix notation, $F\vec{x} = \vec{C}$ becomes $P_O^{-1} E P_I \vec{x} = \vec{C}$, where P_O^{-1} and P_I are the output/input map permutation matrices, and $E = F_{N_1} \otimes F_{N_2} \otimes \cdots \otimes F_{N_m}$. Thus, we write

$$P_O^{-1}(F_{N_1} \otimes F_{N_2} \otimes \cdots \otimes F_{N_m}) P_I \vec{x} = \vec{C}. \tag{19}$$

This gives

$$F_N = P_O^{-1}(F_{N_1} \otimes F_{N_2} \otimes \cdots \otimes F_{N_m}) P_I \tag{20}$$

which implies that after row/column permutations, F_N can be represented as the Kronecker product of successive coprime-order DFT matrices. It is obvious that F_N can be factored.

Our goal is to explore fast factorization/construction transforms for the DFT matrix in (20). Note that P_O^{-1} (or P_I^{-1}) may not be representable as a linear form modulo N. There is no 3-D or higher-dimensional CRT mapping with linear inverses,

and only some 2-D CRT mapping has a linear inverse [22]. Fortunately, in practice this does not significantly enhance the computational complexity. Therefore, we consider the construction of the combined matrix $E = F_{N_1} \otimes F_{N_2} \otimes \cdots \otimes F_{N_m}$. For convenience, we denote E as $F_N^{'}$ from now on. If a fast transform for matrix $F_N^{'}$ is available, we can achieve our goal via suitable permutation maps. In the following, we omit the permutation maps that have no impact on our results.

A. Fast Factorization Transform for Multi-Dimensional DFT Matrices

In this subsection we show that the DFT matrices are a class of Jacket matrices, which implies that the fast Jacket transform may be applied. Furthermore, we propose a generalized factorization transform for mapped M-dimensional DFT matrix. This regular decomposition is based on a sparse-matrix factorization of the prime-order DFT matrices in Kronecker product form of the identity matrices and successive prime-order DFT matrices.

Theorem 3. Suppose that N is product of coprime numbers, i.e., $N = p_1 p_2 \cdots p_m$ for $p_i = N_i$, $1 \le i \le m$. Let F_{p_i} be a DFT matrix of order p_i. The factorization of the matrix $F_N^{'} = F_{p_1} \otimes F_{p_2} \otimes \cdots \otimes F_{p_m}$ may be expressed as

$$F_N^{'} = C_{p_1}^1 C_{p_2}^2 \cdots C_{p_m}^m \tag{21}$$

where

$$\begin{aligned} C_{p_i}^i = {} & I_{p_1} \otimes I_{p_2} \cdots \otimes I_{p_{i-1}} \otimes F_{p_i} \\ & \otimes I_{p_{i+1}} \otimes I_{p_{i+2}} \cdots \otimes I_{p_m}. \end{aligned} \tag{22}$$

Proof: When $p_1 = p_2 = \cdots = p_m = p$, we obtain

$$C_{p_i}^i = C_{p^m}^i = I_{p^{i-1}} \otimes F_p \otimes I_{p^{m-i}}$$

and

$$F_N^{'} = \prod_{i=1}^{m} (I_{p^{i-1}} \otimes F_p \otimes I_{p^{m-i}}). \tag{23}$$

Assume that the hypothesis holds for m, we show that it must be true for $m+1$. For $1 \le i \le m$, we have the following formula from the hypothesis [11]:

$$\begin{aligned} C_{p^{m+1}}^i &= I_{p^{i-1}} \otimes F_p \otimes I_{p^{m+1-i}} \\ &= I_{p^{i-1}} \otimes F_p \otimes (I_{p^{m-i}} \otimes I_p) \\ &= (I_{p^{i-1}} \otimes F_p \otimes I_{p^{m-i}}) \otimes I_p \\ &= C_{p^m}^i \otimes I_p, \end{aligned} \tag{24}$$

so

$$C_{p^{m+1}}^{m+1} = I_{p^m} \otimes F_p \otimes I_{p^0} = I_{p^m} \otimes F_p. \tag{25}$$

Thus,

$$\begin{aligned} F_{p^{m+1}} &= C_{p^{m+1}}^1 C_{p^{m+1}}^2 \cdots C_{p^{m+1}}^m C_{p^{m+1}}^{m+1} \\ &= (C_{p^m}^1 \otimes I_p)(C_{p^m}^2 \otimes I_p) \cdots (C_{p^m}^m \otimes I_p)(I_{p^m} \otimes F_p) \\ &= (C_{p^m}^1 C_{p^m}^2 \cdots C_{p^m}^m I_{p^m}) \otimes F_p \\ &= F_{p^m} \otimes F_p. \end{aligned} \tag{26}$$

Since $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$ [24], (26) is verified completely. Therefore, by substituting $I_{p_1} \otimes I_{p_2} \cdots \otimes I_{p_{i-1}}$ for $I_{p^{i-1}}$, and $I_{p_{i+1}} \otimes I_{p_{i+2}} \cdots \otimes I_{p_m}$ for $I_{p^{m-i}}$, we can easily obtain (31). Hence, the theorem is proved. □

Example 1: Let $N = 30 = 2 \cdot 3 \cdot 5$, and $p_1 = 2$, $p_2 = 3$, and $p_3 = 5$. In this case, the DFT matrix F_{30} of size 30 can be decomposed as

$$\begin{aligned} F_{30}^{'} &= C_2^1 C_3^2 C_5^3 \\ &= (F_2 \otimes I_3 \otimes I_5)(I_2 \otimes F_3 \otimes I_5)(I_2 \otimes I_3 \otimes F_5) \\ &= \begin{bmatrix} C_0 & 0 & 0 & C_0 & 0 & 0 \\ 0 & C_0 & 0 & 0 & C_0 & 0 \\ 0 & 0 & C_0 & 0 & 0 & C_0 \\ C_0 & 0 & 0 & C_1 & 0 & 0 \\ 0 & C_0 & 0 & 0 & C_1 & 0 \\ 0 & 0 & C_0 & 0 & 0 & C_1 \end{bmatrix} \\ &\quad \cdot \begin{bmatrix} D_0 & D_0 & D_0 & 0 & 0 & 0 \\ D_0 & D_1 & D_2 & 0 & 0 & 0 \\ D_0 & D_2 & D_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & D_0 & D_0 & D_0 \\ 0 & 0 & 0 & D_0 & D_1 & D_2 \\ 0 & 0 & 0 & D_0 & D_2 & D_1 \end{bmatrix} \\ &\quad \cdot \begin{bmatrix} E_0 & 0 & 0 & 0 & 0 & 0 \\ 0 & E_0 & 0 & 0 & 0 & 0 \\ 0 & 0 & E_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & E_0 & 0 & 0 \\ 0 & 0 & 0 & 0 & E_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & E_0 \end{bmatrix} \end{aligned} \tag{27}$$

where

$$C_i = \begin{bmatrix} W_2^i & 0 & 0 & 0 & 0 \\ 0 & W_2^i & 0 & 0 & 0 \\ 0 & 0 & W_2^i & 0 & 0 \\ 0 & 0 & 0 & W_2^i & 0 \\ 0 & 0 & 0 & 0 & W_2^i \end{bmatrix},$$

$$D_j = \begin{bmatrix} W_3^j & 0 & 0 & 0 & 0 \\ 0 & W_3^j & 0 & 0 & 0 \\ 0 & 0 & W_3^j & 0 & 0 \\ 0 & 0 & 0 & W_3^j & 0 \\ 0 & 0 & 0 & 0 & W_3^j \end{bmatrix},$$

$$E_0 = \begin{bmatrix} W_5^0 & W_5^0 & W_5^0 & W_5^0 & W_5^0 \\ W_5^0 & W_5^1 & W_5^2 & W_5^3 & W_5^4 \\ W_5^0 & W_5^2 & W_5^4 & W_5^1 & W_5^3 \\ W_5^0 & W_5^3 & W_5^1 & W_5^4 & W_5^2 \\ W_5^0 & W_5^4 & W_5^3 & W_5^2 & W_5^1 \end{bmatrix} \tag{28}$$

for $i = 0, 1$ and $j = 0, 1, 2$.

The signal flowchart corresponding to (27) is shown in Fig. 1, where the symbols X_i and Y_i, for $1 \le i \le 30$ represent input and output signals, respectively. It is easy to see that the fast transform for a matrix of order $N = 30$ requires 210 additions and 300 multiplications.whereas direct computation requires 870 additions and 900 multiplications. Obviously, the fast transform is faster than the direct approach. We note that the permutation mapping for the input/output signals has not been shown, because for three or more dimensions, the linear inverse of the permutation matrix is unrepresentable.

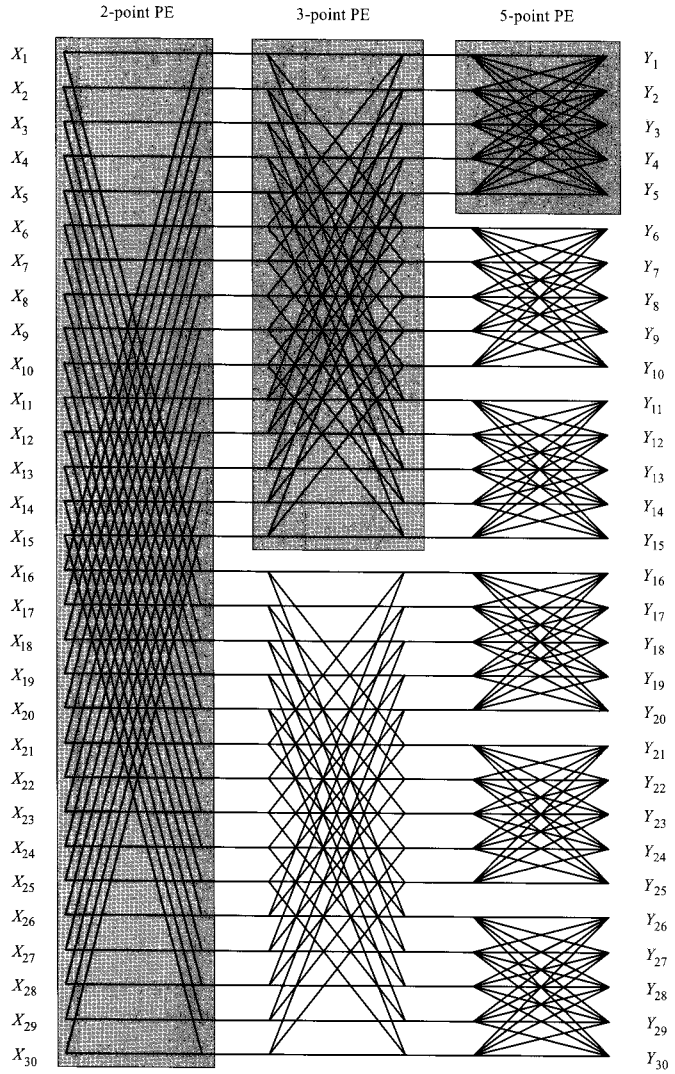

Fig. 1. Signal graph for DFT matrices transform of size 30.

B. *Fast Construction Transform for M-Dimensional DFT Matrices*

This subsection concentrates on fast construction of mapped M-Dimensional DFT matrices. In paricular, the construction of a 2-D DFT matrix is described in detail.

In Theorem 3, we show that the formula

$$F_N^{'} = \prod_{i=1}^{m} (I_{p^{i-1}} \otimes F_p \otimes I_{p^{m-i}}) \tag{29}$$

plays a key role in the construction and decomposition of a complex matrix. By Theorem 1, we modify this formula as

$$F_N^{'} = \prod_{i=1}^{m} (I_{p^{m-i}} \otimes F_p \otimes I_{p^{i-1}}) \tag{30}$$

which is the reverse procedure of the construction.

Theorem 4. Let F_{p_i} be a DFT matrix of order p_i, $1 \le i \le m$. The construction for the matrix $F_N^{'} = F_{p_1} \otimes F_{p_2} \otimes \cdots \otimes F_{p_m}$ may be expressed as

$$F_N^{'} = D_{p_1}^1 D_{p_2}^2 \cdots D_{p_m}^m \tag{31}$$

where

$$D_{p_i}^i = I_{p_{i+1}} \otimes I_{p_{i+2}} \cdots \otimes I_{p_m} \otimes F_{p_i} \otimes I_{p_1} \otimes I_{p_2} \cdots \otimes I_{p_{i-1}}. \tag{32}$$

Proof: By substituting (30) for (23) and following the proof of Theorem 3, we can easily prove this theorem. □

For a comparison with example 1, we again consider $N = 2 \times 3 \times 5$. By Theorem 4, the fast construction of F_{30} is

$$\begin{aligned} F_{30}^{'} &= D_2^1 D_3^2 D_5^3 \\ &= (I_3 \otimes I_5 \otimes F_2)(I_5 \otimes F_3 \otimes I_2)(F_5 \otimes I_2 \otimes I_3) \end{aligned}$$

which indicates that both the construction and decomposition are only minimally related to the sparse matrices.

For 2-D linear maps ($N = p_1 p_2$), Schatzman suggested that only some CRT maps have linear inverse maps. For clarity, we note the CRT maps for $n \to (n_1, n_2)$, i.e., $K_1 = a_1 p_2$, $K_2 = a_2 p_1$, $\gcd(a_1, p_1) = 1$ and $\gcd(a_2, p_2) = 1$, where a_1 and a_2 are integers. In particular, the CRT maps given by $a_1 = p_2^{-1} \bmod p_1$, $a_2 = (z p_1) \bmod p_2$, and $z = \lfloor a_1 p_2 / p_1 \rfloor$ is the unique CRT maps that has a linear inverse, which is its own inverse. Clearly, we have

$$F_N = P_O^{-1}(F_{p_1} \otimes F_{p_2}) P_I = P_O(F_{p_1} \otimes F_{p_2}) P_I \tag{33}$$

which can easily be constructed via Theorem 4 with the available permutation maps.

Example 2: Consider $N = 3 \cdot 5$. If we choose K_1, since $a_1 = 5^{-1} \bmod 3 = 2$, $K_1 = 2 \cdot 5 = 10$. For $z = \lfloor (2 \cdot 5)/3 \rfloor = 3$ and $a_2 = (3 \cdot 3) \bmod 5 = 4$, $K_2 = 4 \cdot 3 = 12$. Therefore, the permutation maps can be uniquely represented in a signal flowchart. By Theorem 4, we have

$$F_{15} = P_O((I_5 \otimes F_3)(F_5 \otimes I_3)) P_I. \tag{34}$$

Given the DFT matrices F_3 and F_5, i.e.,

$$F_3 = \begin{bmatrix} W_3^0 & W_3^0 & W_3^0 \\ W_3^0 & W_3^1 & W_3^2 \\ W_3^0 & W_3^2 & W_3^1 \end{bmatrix} \tag{35}$$

and

$$F_5 = \begin{bmatrix} W_5^0 & W_5^0 & W_5^0 & W_5^0 & W_5^0 \\ W_5^0 & W_5^1 & W_5^2 & W_5^3 & W_5^4 \\ W_5^0 & W_5^2 & W_5^4 & W_5^1 & W_5^3 \\ W_5^0 & W_5^3 & W_5^1 & W_5^4 & W_5^2 \\ W_5^0 & W_5^4 & W_5^3 & W_5^2 & W_5^1 \end{bmatrix}, \tag{36}$$

we construct the desirable matrix F_{15} via (34). The factor graph for the above equation is plotted in Fig. 2. The permutation maps are shown at the left and right, respectively. This transform requires 90 additions and 120 multiplications. whereas direct computation requires 210 additions and 225 multiplications. Thus, our approach is faster than the existing algorithms.

Table 1 presents a comparison of direct computation and fast factorization/construction algorithms for M-dimensional DFT matrices. From this table, we can see that our algorithms are more efficient.

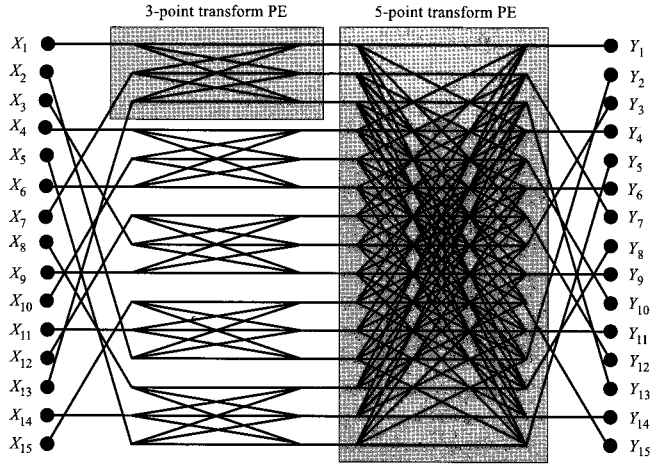

Fig. 2. Signal flow graph for DFT transform of size 15.

Table 1. Computational complexity of different algorithms. DCA, FAS, ADD, and MUL indicate direct computation, fast algorithm, number of additions, and number of multiplications, respectively.

	DCA	FAS for $N = p_1 p_2 \cdots p_m$
ADD	$(N-1)N$	$\sum_{i=1}^{m}(p_i - 1)N$
MUL	N^2	$\sum_{i=1}^{m} p_i N$

V. DISCUSSION AND CONCLUSION

We remark that the proposed Jacket matrices F_n of order n can be used for the construction of error-correcting detection codes or error-correction codes. Consider a pair of n-symbol blocks $f_1 = (f_{11}, f_{12}, \cdots, f_{1n})$ and $f_2 = (f_{21}, f_{22}, \cdots, f_{2n})$, which are any two rows of the yield matrix F_n of length n. The Hamming distance between two blocks f_1 and f_2, called the code word, is the number of coordinates in which the two blocks differ, i.e.,

$$\begin{aligned} d_H(f_1, f_2) &= d_H(f_2, f_1) \\ &= |\{i | f_{1i} \neq f_{1i}, i = 0, 1, \cdots, n-1\}|. \end{aligned} \quad (37)$$

Let C be the set $\{f_i | 1 \leq i \leq c\}$. The minimum distance, denoted d_e, of C is the minimum Hamming distance between all distinct pairs of code words in C. Undetectable errors are those that cause the transmitted code word to look like another code word. A transmitted code word is guaranteed to differ in at least d_e coordinates from any other code word. For an error to be undetectable, it must change the symbol values in the transmitted code words in at least d_e coordinates. A code C with minimum distance d_e can detect all errors of weight less than or equal to $d_e - 1$. We say that it has error-detection ability d_e and error-correction ability $t = (d_e - 1)/2$.

Based on the Jacket matrix F_n, we select a set that has the maximum number of rows such that it has the minimum Hamming distance d_e. We say that this matrix F_n has error-correcting ability $t = (d_e - 1)/2$. Using our fast construction of the Jacket matrix F_n, we can construct a suitable error-correction code. This shows one advantage of our approach: It can be used for the construction of codes for error correction.

In conclusion, we have developed fast algorithms for M-dimensional DFT matrices by combining the GPFA with fast Jacket transforms. Using these methods, we can easily decompose and construct M-dimensional DFT matrices in Kronecker product form of identity matrices and successive coprime-order DFT matrices. Compared with direct computation, our algorithms decrease the computational complexity, and they can be applied to, for example, encoding, sequence signal processing, and information theory.

REFERENCES

[1] N. Ahmed and K. R. Rao, *Orthogonal Transform for Digital Signal Processing*. Berlin, Germany: Springer Verlag, 1975.

[2] R. E. Blahut, *Algebraic Codes for Data Transmission*. Cambridge, UK: 2003.

[3] K. Y. Rao and J. E. Hershey, *Hadamard Matrix Analysis and Synthesis*. Norwell, MA: Kluwer, 1997.

[4] M. H. Lee, "The center weighted Hadamard transform," *IEEE Trans. Circuits Syst.*, vol. 36, pp. 1247–1249, Sept. 1989.

[5] M. H. Lee, "A new reverse Jacket transform and its fast algorithm," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process*, vol. 47, no. 1, pp. 39–47, Jan. 2000.

[6] M. H. Lee and Y. L. Borissov, "A proof of non-existence of bordered Jacket matrices of odd order over some field," *Electron. Lett.*, vol. 46, pp. 349–351, Mar. 2010.

[7] M. H. Lee, B. S. Rajan, and J. Y. Park, "A generalized reverse Jacket transform," *IEEE Trans. Circuits Syst.*, vol. 48, pp. 684–688, July 2001.

[8] M. H. Lee and J. Hou, "Fast block inverse Jacket transform," *IEEE Signal Process. Lett.*, vol. 13, no. 4, pp. 461–464, 2006.

[9] M. H. Lee and G. Zeng, "Family of fast Jacket transform algorithms," *Electron. Lett.*, vol. 43, no. 11, pp. 651–651, 2007.

[10] G. Zeng and M. H. Lee, "A generalized reverse block Jacket transform," *IEEE Trans. Circuits and Syst.*, vol. 55, pp. 1589–1599, July 2008.

[11] Z. Chen, M. H. Lee, and G. Zeng, "Fast cocyclic Jacket transform," *IEEE Trans. Signal Process.*, vol. 56, no. 5, pp. 2143–2148, 2008.

[12] M. H. Lee and K. Finlayson, "A simple element inverse Jacket transform coding," in *Proc. IEEE ITW*, New Zealand, vol. 14, 2006, pp. 1–4.

[13] X. J. Jiang and M. H. Lee, "Higher dimensional Jacket code for mobile communications," in *Proc. APW*, Sapporo, Japan, Aug. 2005, pp. 4–5.

[14] M. G. Parker and M. H. Lee, "Optimal bipolar sequence for the complex reverse-Jacket transform," in *Proc. ISITA*, Honolulu, USA, Nov. 2000, pp. 5–8.

[15] J. Hou and M. H. Lee, *Cocyclic Jacket Matrices and Its Application to Cryptography Systems*. Berlin, Germany: Springer, vol. 3391, 2005.

[16] W. Song, M. H. Lee, and G. Zeng, "Orthogonal space-time block codes design using Jacket transform for MIMO transmission system," in *Proc. IEEE ICC*, May 2008, pp. 766–769.

[17] S. Winograd, "On computing the discrete Fourier transform," in *Proc. Nat. Acad. Sci.*, USA, vol. 73, no. 4, Apr. 1976, pp. 1005–1006.

[18] C. Temperton, "Implementation of a self-sorting, in-place prime factor FFT algorithm," *J. Computat. Physics*, vol. 58, pp. 283–299, 1985.

[19] C. S. Burrus, "Index mapping for multidimensional formulation of the DFT and convolution," *IEEE Trans. Acoust. Speech, Signal Process.*, vol. 25, no. 3, pp. 239–242, June 1977.

[20] C. S. Burrus and P. W. Eschenbacher, "An in-place, in-order prime factor for FFT algorithm," *IEEE Trans. Acoust. Speech, Signal Process.*, vol. 29, no. 4, pp. 806–817, Aug. 1981.

[21] Z. Wang, "Index mapping for one to multidimensional," *Electron. Lett.*, vol. 25, no. 12, pp. 781–782, June 1989.

[22] J. C. Schatzman, "Index mapping for the fast Fourier transform," *IEEE Trans. Signal Process.*, vol. 44, no. 3, pp. 717–719, Mar. 1996.

[23] H. Neudecker, "A note on Kronecker matrix products and matrix equation systems," *SIAM J. Appl. Mathematics*, vol. 17, no. 3, pp. 603–606, May 1969.

[24] R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis*. New York: Cambridge Univ. Press, 1991.

Ying Guo received his B.S. in 1999 in Qufu Normal University, China, M.S., in 2003 in Kunming University of Science and Technology, China, and Ph.D. degrees in 2006 in the Shanghai Jiaotong University, China. His research interests include Quantum information processing, wireless Communication. He is an Association Member of IEEE Communication Society. He is now a Associate Professor in Central South University, China.

Yun Mao received the B.S. degree in Changan University, China, in 1999. She received the M.S. degree in Kunming University of Science and Technology, China, in 2004. She began working toward the Ph.D. degree in traffic information and control engineering in 2009 at the Central South University. He worked as a Lecturer in 2006 in Central South University. Her research efforts focus on mobile communications and high-speed communication networks.

Dong Sun Park received his B.S. in Korea University, Korea and M.S., Ph.D. degrees in the University of Missouri, USA. His research interests include image processing, pattern recognition, computer vision, and artificial intelligence. He is an Association Member of IEEE Computer Society. He is now a Professor in Chonbuk National University, Korea.

Moon Ho Lee received his B.S. and M.S. degrees in Electrical Engineering from Chonbuk National University, South Korea, in 1967 and 1976 respectively, and his Ph.D. degree in Electrical Engineering from Chonnam National University in 1984. He also received a Ph.D. degree in Information Engineering from the University of Tokyo, Tokyo, Japan, in 1990. Currently, he was a Professor in the Department of Electronics and Information Engineering and Head of the Institute of Information and Communication at Chonbuk National University. His research interests include image processing, mobile communications and high-speed communication networks, and information and algebra coding theory.