EURASIP Journal on Advances in Signal Processing
a SpringerOpen Journal

RESEARCH Open Access

An explicit construction of fast cocyclic jacket transform on the finite field with any size

Ying Guo[1,2], Moon Ho Lee[2*] and Kyeong Jin Kim[3]

Abstract

An orthogonal cocyclic framework of the block-wise inverse Jacket transform (BIJT) is proposed over the finite field. Instead of the conventional block-wise inverse Jacket matrix (BIJM), we investigate the cocyclic block-wise inverse Jacket matrix (CBIJM), where the high-order CBIJM can be factorized into the low-order sparse CBIJMs with a successive block architecture. It has a recursive fashion that leads to a fast algorithm concerned for reducing computational load. The fast transforms are also developed for the two-dimensional cocyclic block-wise inverse Jacket transform (CBIJT). The present CBIJM may be used for many matrix-based applications, such as the DFT signal processing, combinatorics, and the Reed-Muller code design.

Introduction

The orthogonal transforms, such as the discrete Fourier transform (DFT) and the Walsh-Hadamard transform (WHT), have been widely employed in images processing, feature selection, signal processing, data compressing and coding, and other areas [1-7]. Using orthogonality of the WHT, the interesting orthogonal matrices, such as the element-wise or block-wise inverse Jacket matrices (BIJMs) [8-12], have been developed. More details of these matrices can be referred to [13-19].

Definition 1. An $n \times n$ matrix $J_n = (\alpha_{ij})_{n\times n}$ is called the element-wise inverse Jacket matrix (EIJM) of order n if its inverse matrix J_n^{-1} can be simply obtained by its element-wise inverse, i.e., $J_n^{-1} = \frac{1}{n}(\alpha_{ij}^{-1})^{\mathrm{T}}_{n\times n}$, $\forall\, i,j \in \mathcal{Z}_n := \{0, 1, \ldots, n-1\}$, where the superscript T denotes the transpose.

Many interesting orthogonal matrices, say the Hadamard matrices and the DFT matrices, belong to the Jacket matrix family. With the rapid technological development, different forms of such transforms were improved and generalized. It has been discovered that the newly proposed transforms have been widely used in various signal processing, CDMA, cooperative relay MIMO system [20-28].

Recently, the BIJM $[J]_n$ has been investigated while the complex unit $\exp^{\sqrt{-1}(2\pi/p)}$ of the EIJM J_n is substituted for a suitable matrix unit [15-17]. However, the CBIJM does not attract much attention even though the cocyclic matrix has been very useful for the data coding and processing [5,14,29,30].

Definition 2. If $\mathcal{G}$ is a finite group of order r with operation $\circ$ and $\mathcal{C}$ is a finite Abelian group of order t, a cocycle is a mapping $\phi : \mathcal{G} \times \mathcal{G} \to \mathcal{C}$ satisfying

$$\phi(a, b)\phi(a \circ b, c) = \phi(a, b \circ c)\phi(b, c), \qquad (1)$$

where $a, b, c \in \mathcal{G}$. A square matrix $M(\phi)$ whose row a and column b can be indexed by $\mathcal{G}$ with entry $\phi(a, b) \in \mathcal{C}$ in position (a, b) under some fixed ordering, i.e., $M(\phi) = (\phi(a, b))_{a,b\in\mathcal{G}}$, is called a cocyclic matrix. If $\phi(1, 1) = 1$, then it is the normalized cocyclic matrix for the standard usage [5,29,30].

Definition 3. Let $J_p = (\omega^{\langle i\circ j\rangle_p})_{p\times p}$, $\forall\, i,j \in \mathcal{Z}_p := \{0, 1, \ldots, p-1\}$, be a matrix of order p, where $\omega = \exp(\sqrt{-1}(2\pi/p))$ and $\langle i \circ j\rangle_p = i \times j \mod p$, i.e., the subscript p implies modulo-p arithmetic for the argument. Then the matrix J_p and its s-fold matrix of order p^s

$$J_{p^s} = J_p^{\otimes s} = \underbrace{J_p \otimes J_p \cdots \otimes J_p}_{s}$$

*Correspondence: moonho@chonbuk.ac.kr
[2]Institute of Information and Communication, Chonbuk National University, Jeonju 561-756, Korea
Full list of author information is available at the end of the article

are the conventional cocyclic element-wise inverse Jacket matrices (CEIJM), where $\otimes$ denotes the Kronecker product and p is a prime number.

As a generation of the Hadamard matrix, the BIJM inherits the merits of the Hadamard matrix, at the same time, without the restriction that entries must be '±1'. On the other hand, this matrix has very amicable properties, such as reciprocal orthogonality. The inverse transform can be easily obtained by the reciprocal relationships and the fast algorithms. However, the versions of cocyclic block-wise inverse Jacket matrix (CBIJM) are still absent since the existence of the CEIJM has attracted minor attention in the existing literature [8,21]. The purpose of this article is to develop the CBIJM and its generalizations, instead of the CEIJM. In addition, the present CBIJM has some potential practical applications in signal sequence transforms [1-7], coding design for wireless networks [22,27,28], and cryptography [31].

This article is organized as follows. Section 'Cocyclic block-wise inverse Jacket transforms' presents a simple framework of the fast CBIJT. Section 'Designs of the CBIJM over finite field GF(2^m)' reports the CBIJM over finite field $GF(2^p)$. Section 'Two-dimensional fast CBIJM' proposes the structure of the two-dimensional CBIJM. Finally, conclusions are drawn in Section 'Conclusion'.

Cocyclic block-wise inverse Jacket transforms

In this section, we show that the EIJM can be generalized for the constructions of the CBIJT.

Based on the one-dimensional BIJM $[J]_p$ of order p, which can be partitioned to the $p \times p$ block matrix, we can transform a suitable vector $\mathbf{x}$ into another vector $\mathbf{y}$ through a BIJT, i.e.,

$$\mathbf{y} = [J]_p \, \mathbf{x}. \tag{2}$$

In order to derive the CBIJT, we denote a matrix unit by α such that $\alpha^p = I_p$ for a given prime number p, where I_p denotes the $p \times p$ identity matrix. As an example, let α be a square matrix of size 2×2 defined as

$$\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{3}$$

It is easy to prove that $\alpha^2 = I_2$. Actually, matrix α in (3) has been employed for the existence of the BIJM [15-17]. Fortunately, it will be shown that the s-fold block Jacket matrix $[J]_{2^s} \triangleq \alpha^{\otimes s}$ is also a CBIJM.

In what follows we illustrate the cocyclicity of the BIJM $[J]_{p^s}$ based on the matrix unit α of size $p \times p$. In particular for the given prime number p, we define the matrix unit $\alpha^h = [\, e_{i,j}]_p$, where

$$e_{i,j} = \begin{cases} 1, \text{ for } \ i = \langle j+h \rangle_p; \\ 0, \text{ otherwise,} \end{cases} \tag{4}$$

where $\langle j+h \rangle_p = j+h \bmod p, \forall\, i,j,h \in \mathcal{Z}_p := \{0,1,\ldots,p-1\}$. It can be shown that $\mathcal{A} := \{\alpha^h : h \in \mathcal{Z}_p\}$ forms an Abelian group with the traditional matrix multiplication. Namely, for the given number p, one obtains the matrix units as follows

$$\alpha^0 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}, \alpha^1 = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \cdots$$

$$\alpha^{p-2} = \begin{pmatrix} 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \end{pmatrix}, \alpha^{p-1} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}. \tag{5}$$

Example 1. Let $p = 3$, and we have

$$\alpha^0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \alpha^1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \alpha^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}. \tag{6}$$

It is obvious that $\mathcal{Z}_p$ with the multiplication operation $\langle a \cdot b \rangle_p$ is a finite field of order p. For $\forall\, a, x \in \mathcal{Z}_p$, we define an multiplication function $f_a(x)$ over $\mathcal{Z}_p$, i.e.,

$$f_a(x) := \langle a \cdot x \rangle_p. \tag{7}$$

With the aid of the multiplication function $f_a(x)$, we define a block matrix of size $p \times p^2$ by concatenating p matrices α^{h_i} of size $p \times p$, $\forall\, h_i \in \mathcal{Z}_p$, i.e.,

$$[\,\beta] := \left[\alpha^{h_0}, \alpha^{h_1}, \ldots, \alpha^{h_{p-1}}\right] \tag{8}$$

and hence

$$[\,\beta_a] := \left[\alpha^{f_a(h_0)}, \alpha^{f_a(h_1)}, \ldots, \alpha^{f_a(h_{p-1})}\right]. \tag{9}$$

Lemma 1. For block matrices $[\,\beta_a]$ and $[\,\beta_b]$, $\forall\, a, b \in \mathcal{Z}_p$, we have

$$[\,\beta_a] \cdot [\,\beta_b]^{\mathrm{T}} = \begin{cases} pI, \text{ for } \ \langle a+b \rangle_p = 0; \\ 0, \quad \text{for } \ \langle a+b \rangle_p \neq 0. \end{cases} \tag{10}$$

The proof of Lemma 1 is illustrated in Appendix.

Example 2. Let us consider α with $p = 2$ in (3). It is obvious that $\alpha^2 = I$ is an identity matrix of size 2×2. Let $[\beta] = \left[\alpha^0, \alpha^1\right]$, then we have

$$[\beta_0] = \left[\alpha^0, \alpha^0\right] = \begin{bmatrix} 1\,0\,1\,0 \\ 0\,1\,0\,1 \end{bmatrix}, \tag{11}$$

$$[\beta_1] = \left[\alpha^0, \alpha^1\right] = \begin{bmatrix} 1\,0\,0\,1 \\ 0\,1\,1\,0 \end{bmatrix}. \tag{12}$$

It is straightforward to show that

$$[\beta_0] \cdot [\beta_0]^{\mathrm{T}} = [\beta_1] \cdot [\beta_1]^{\mathrm{T}} = 2I_2. \tag{13}$$

The *p*-order CBIJM

In [15-17], Lee et al. expanded the EIJM to the BIJM.

Definition 4. An $np \times np$ block matrix $[J]_n = ([\alpha_{ij}]_p)_{np\times np}$ is called the BIJM of order n if $[J]_n^{-1} = \frac{1}{c}([\alpha_{ij}]^{-1})^{\mathrm{T}}_{np\times np}$ where c is the normalized value and $[\alpha_{ij}]_{p\times p}$ denotes a matrix unit of size $p \times p$.

Definition 5. For a given prime number p, let α be a $p \times p$ matrix unit such that $\alpha^p = I$ and

$$[\beta] = \left[\alpha^0, \alpha^1, \ldots, \alpha^{p-1}\right]. \tag{14}$$

Define the p-order BIJM $[J]_p$ of size $p^2 \times p^2$ as follows

$$[J]_p := \begin{bmatrix} [\beta_0] \\ [\beta_1] \\ [\beta_2] \\ \vdots \\ [\beta_{p-1}] \end{bmatrix} = \begin{bmatrix} \alpha^0 & \alpha^0 & \cdots & \alpha^0 \\ \alpha^0 & \alpha^1 & \cdots & \alpha^{p-1} \\ \alpha^0 & \alpha^2 & \cdots & \alpha^{2(p-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^0 & \alpha^{p-1} & \cdots & \alpha^{(p-1)(p-1)} \end{bmatrix} \tag{15}$$

and thus its inverse

$$[J]_p^{-1} := \frac{1}{p} \begin{bmatrix} \alpha^0 & \alpha^0 & \cdots & \alpha^0 \\ \alpha^0 & \alpha^{\langle -1\rangle_p} & \cdots & \alpha^{\langle -(p-1)\rangle_p} \\ \alpha^0 & \alpha^{\langle -2\rangle_p} & \cdots & \alpha^{-2(p-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^0 & \alpha^{\langle -(p-1)\rangle_p} & \cdots & \alpha^{\langle -(p-1)(p-1)\rangle_p} \end{bmatrix}. \tag{16}$$

Consequently, we have

$$[J]_p \cdot [J]_p^{-1} = [J]_p^{-1} \cdot [J]_p = I_{p^2\times p^2}. \tag{17}$$

Example 3. Taking $[\beta_0]$ and $[\beta_1]$ for $p = 2$, we have

$$[J]_2 = \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \tag{18}$$

and its inverse

$$[J]_2^{-1} = \frac{1}{2} \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^{\langle -1\rangle_2} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}. \tag{19}$$

Actually, we have

$$[J]_2\,[J]_2^{-1} = \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix} \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 \end{bmatrix} = \begin{bmatrix} I_2 & 0 \\ 0 & I_2 \end{bmatrix}, \tag{20}$$

where $\alpha^0 + \alpha^1 = 0$ since $\alpha^2 = I$ and $\alpha \neq I$ over the finite field.

We note that the above-mentioned BIJM was first proposed by Lee and Hou [13] for the proof of existence of Jacket matrices over the finite field. Next, we illustrate that this BIJM is also a CBIJM in essence.

Theorem 1. Let $\mathcal{G} = \mathcal{Z}_p$ with an operation $a \circ b := \langle a + b\rangle_p, \forall\, a, b \in \mathcal{Z}_p$, and $\mathcal{C} := \{\alpha^i : i \in \mathcal{Z}_p\}$ with the traditional multiplication. The BIJM $[J]_p$ in (15) whose rows and columns are both indexed in $\mathcal{G}$ under the increasing order (i.e., $0 \prec 1 \prec \cdots \prec p-1$) and entries $\phi(a, b)$ in position (a, b) is the normalized CBIJM.

The proof of Theorem 1 is illustrated in Appendix.

Example 4. We consider $p = 3$ with

$$\alpha = \begin{bmatrix} 0\,0\,1 \\ 1\,0\,0 \\ 0\,1\,0 \end{bmatrix}_{3\times 3}.$$

It is easy to verify that $\alpha^3 = I_{3\times 3}$. Let $[\beta] = \left[\alpha^0, \alpha^1, \alpha^2\right]$ be a block matrix of size 3×9. Thus we obtain the three-order BIJM $[J]_3$ of size 9×9 as follows

$$[J]_3 = \begin{bmatrix} \alpha^0 & \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 & \alpha^2 \\ \alpha^0 & \alpha^2 & \alpha^1 \end{bmatrix}, \tag{21}$$

and its inverse

$$[J]_3^{-1} = \begin{bmatrix} \alpha^0 & \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^{\langle -1\rangle_3} & \alpha^{\langle -2\rangle_3} \\ \alpha^0 & \alpha^{\langle -2\rangle_3} & \alpha^{\langle -1\rangle_3} \end{bmatrix}, \tag{22}$$

where $\alpha^{-1} = \alpha^{\langle -1\rangle_3} = \alpha^2$ and $\alpha^{-2} = \alpha^{\langle -2\rangle_3} = \alpha$. Moreover, the indexed BIJM $[J]_3$ can be mapped in Table 1. It shows that the present BIJM $[J]_3$ is a three-order CBIJM in $\mathcal{C} = \{I_3, \alpha, \alpha^2\}$ and $\mathcal{G} = \mathcal{Z}_3$ under the increasing order $0 \prec 1 \prec 2$.

Table 1 Correspondence between indexes and entries of $[J]_3$

$a\backslash b$	0	1	2
0	α^0	α^0	α^0
1	α^0	α^1	α^2
2	α^0	α^2	α^1

The multi-fold CBIJM

In order to derive the high-order recursive CBIJM $[J]_{p^s}$ for any prime number p and nonnegative integer s, let us introduce some lemmas [1-5].

Lemma 2. Let A, B, C, and D are matrices with suitable sizes. Then we have

$$\begin{aligned}&(A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D),\\ &(A \otimes B)^{-1} = (A^{-1} \otimes B^{-1}),\\ &(A \otimes B)^{\mathrm{T}} = (A^{\mathrm{T}} \otimes B^{\mathrm{T}}).\end{aligned} \tag{23}$$

Theorem 2. For a given prime number p, let $[A]_p = [\alpha_{i,j}]_p$ and $[B]_p = [\gamma_{s,t}]_p$, $\forall\, i, j, s, t \in \mathcal{Z}_p$, be two CBIJMs of order p that corresponds to the matrix units α and γ such that $\alpha^p = I$ and $\gamma^p = I$, respectively. Then the two-fold Kronecker product matrix

$$[J]_{p^2} = [A]_p \otimes [B]_p \tag{24}$$

is a two-fold CBIJM of order p^2.

The proof of Theorem 2 is shown in Appendix.

Corollary 1. For any prime number p and non-negative integer number s, let $[J]_{p^s} = [J]_p^{\otimes s}$ be an s-fold block matrix, i.e.,

$$[J]_{p^s} = \underbrace{[J]_p \otimes \cdots [J]_p}_{s}. \tag{25}$$

Then the block matrix $[J]_{p^s}$ is a CBIJM of order p^s.

Example 5. For $p = 2$ and $s = 2$, we consider a matrix unit α of size 2×2 in (3). Thus we have the four-order BIJM $[J]_{2^2}$ given by

$$\begin{aligned}[J]_{2^2} &= [J]_2 \otimes [J]_2\\ &= \begin{bmatrix}\alpha^0 & \alpha^0\\ \alpha^0 & \alpha^1\end{bmatrix}_{4\times 4} \otimes \begin{bmatrix}\alpha^0 & \alpha^0\\ \alpha^0 & \alpha^1\end{bmatrix}_{4\times 4}\\ &= \begin{bmatrix}\alpha^0\alpha^0 & \alpha^0\alpha^0 & \alpha^0\alpha^0 & \alpha^0\alpha^0\\ \alpha^0\alpha^0 & \alpha^0\alpha^1 & \alpha^0\alpha^0 & \alpha^0\alpha^1\\ \alpha^0\alpha^0 & \alpha^0\alpha^0 & \alpha^1\alpha^0 & \alpha^1\alpha^0\\ \alpha^0\alpha^0 & \alpha^0\alpha^1 & \alpha^1\alpha^0 & \alpha^1\alpha^1\end{bmatrix}_{8\times 8}.\end{aligned} \tag{26}$$

Similarly, we have an index order matrix in Table 2, where the row and column index orders are

$$00 \prec 01 \prec 10 \prec 11 \tag{27}$$

and for $\forall\, a_1, b_1, a_2, b_2 \in \mathcal{Z}_2$,

$$a_1a_2 \circ b_1b_2 = \langle a_1 + b_1\rangle_2 \langle a_2 + b_2\rangle_2. \tag{28}$$

As an example, if $a = 2$ and $b = 3$, then we have

$$\alpha^{10\circ 11} = \alpha^{\langle 1+1\rangle_2\langle 0+1\rangle_2} = \alpha^{01} = \alpha.$$

Table 2 Correspondence between indexes and entries of the 2-fold CBIJM $[J]_{2^2}$ based on the basic CBIJM $[J]_2$

$\vec{a}\backslash\vec{b}$	$\circ$	**00**	**01**	**10**	**11**
$\circ$	$a\backslash b$	**0**	**1**	**2**	**3**
00	0	$\alpha^0\alpha^0$	$\alpha^0\alpha^0$	$\alpha^0\alpha^0$	$\alpha^0\alpha^0$
01	1	$\alpha^0\alpha^0$	$\alpha^0\alpha^1$	$\alpha^0\alpha^0$	$\alpha^0\alpha^1$
10	2	$\alpha^0\alpha^0$	$\alpha^0\alpha^0$	$\alpha^1\alpha^0$	$\alpha^1\alpha^0$
11	3	$\alpha^0\alpha^0$	$\alpha^0\alpha^1$	$\alpha^1\alpha^0$	$\alpha^1\alpha^1$

It can be easily verified that the two-fold matrix $[J]_{2^2}$ in (26) is a four-order CBIJM of size 8×8. In addition, using the same index mapping in Table 1, we obtain the index matrix $\mathcal{I}_4$ as follows

$$\mathcal{I}_4 = \begin{bmatrix}0\;0\;0\;0\\ 0\;1\;0\;1\\ 0\;0\;1\;1\\ 0\;1\;1\;0\end{bmatrix}, \tag{29}$$

which is a generator matrix of the first order binary Reed-Muller code [3]. We note that this phenomena exists in the generalized s-fold CBIJM $[J]_{p^s}$ of order p^s for any prime number p.

Actually, the two-fold CBIJM $[J]_{2^2}$ in (26) based on the factorization algorithm can be rewritten as

$$[J]_{2^2} = [J]_2 \otimes [J]_2 = (I_2 \otimes [J]_2)\,([J]_2 \otimes I_2)\,. \tag{30}$$

Namely, we have

$$\begin{aligned}[J]_{2^2} &= \begin{bmatrix}\alpha^0 & \alpha^0 & \alpha^0 & \alpha^0\\ \alpha^0 & \alpha^1 & \alpha^0 & \alpha^1\\ \alpha^0 & \alpha^0 & \alpha^1 & \alpha^1\\ \alpha^0 & \alpha^1 & \alpha^1 & \alpha^0\end{bmatrix}\\ &= \begin{bmatrix}\alpha^0 & \alpha^0 & 0 & 0\\ \alpha^0 & \alpha^1 & 0 & 0\\ 0 & 0 & \alpha^0 & \alpha^0\\ 0 & 0 & \alpha^0 & \alpha^1\end{bmatrix}\begin{bmatrix}\alpha^0 & 0 & \alpha^0 & 0\\ 0 & \alpha^0 & 0 & \alpha^0\\ \alpha^0 & 0 & \alpha^1 & 0\\ 0 & \alpha^0 & 0 & \alpha^1\end{bmatrix}.\end{aligned}$$

The comparison between the direct computation and fast transform in terms of operations (i.e., additions and multiplications) is illustrated in the Table 3. From this table, it is shown that for $N = 4$ if we compute directly there are 12 additions and 16 multiplications, but if we use the fast transform algorithm the numbers of additions and multiplications can be reduced to 8 and 4, respectively. It is obvious that the proposed algorithm has a

Table 3 Complexity of the fast algorithms for $N = p^s$, where ADD and MUL denote additions and multiplications

	Direction method	**Fast algorithms**
ADD	$(N-1)N$	$sp^s(p-1)$
MUL	N^2	$sp^{s-1}(p-1)^2$

greater efficiency for computation than that of the direct approach.

Example 6. From Equation (23), we have $p = 3$, $s = 2$ and

$$\alpha^0 = \begin{bmatrix} 1&0&0\\0&1&0\\0&0&1 \end{bmatrix}, \alpha^1 = \begin{bmatrix} 0&0&1\\1&0&0\\0&1&0 \end{bmatrix}, \alpha^2 = \begin{bmatrix} 0&1&0\\0&0&1\\1&0&0 \end{bmatrix},$$

then we can derive the two-fold CBIJM $[J]_{3^2} = [J]_3 \otimes [J]_3$, i.e.,

$$[J]_{3^2} = \begin{bmatrix} \alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0&\alpha^0\\ \alpha^0&\alpha^1&\alpha^2&\alpha^0&\alpha^1&\alpha^2&\alpha^0&\alpha^1&\alpha^2\\ \alpha^0&\alpha^2&\alpha^1&\alpha^0&\alpha^2&\alpha^1&\alpha^0&\alpha^2&\alpha^1\\ \alpha^0&\alpha^0&\alpha^0&\alpha^1&\alpha^1&\alpha^1&\alpha^2&\alpha^2&\alpha^2\\ \alpha^0&\alpha^1&\alpha^2&\alpha^1&\alpha^2&\alpha^0&\alpha^2&\alpha^0&\alpha^1\\ \alpha^0&\alpha^2&\alpha^1&\alpha^1&\alpha^0&\alpha^2&\alpha^2&\alpha^1&\alpha^0\\ \alpha^0&\alpha^0&\alpha^0&\alpha^2&\alpha^2&\alpha^2&\alpha^1&\alpha^1&\alpha^1\\ \alpha^0&\alpha^1&\alpha^2&\alpha^2&\alpha^0&\alpha^1&\alpha^1&\alpha^2&\alpha^0\\ \alpha^0&\alpha^2&\alpha^1&\alpha^2&\alpha^1&\alpha^0&\alpha^1&\alpha^0&\alpha^2 \end{bmatrix}_{27\times 27}, \quad (31)$$

which can be factorized as

$$[J]_{3^2} = [J]_3 \otimes [J]_3 = (I_3 \otimes [J]_3)([J]_3 \otimes I_3)$$

$$= \begin{bmatrix} \alpha^0&\alpha^0&\alpha^0&0&0&0&0&0&0\\ \alpha^0&\alpha^1&\alpha^2&0&0&0&0&0&0\\ \alpha^0&\alpha^2&\alpha^1&0&0&0&0&0&0\\ 0&0&0&\alpha^0&\alpha^0&\alpha^0&0&0&0\\ 0&0&0&\alpha^0&\alpha^1&\alpha^2&0&0&0\\ 0&0&0&\alpha^0&\alpha^2&\alpha^1&0&0&0\\ 0&0&0&0&0&0&\alpha^0&\alpha^0&\alpha^0\\ 0&0&0&0&0&0&\alpha^0&\alpha^1&\alpha^2\\ 0&0&0&0&0&0&\alpha^0&\alpha^2&\alpha^1 \end{bmatrix}_{27\times 27}$$

$$\times \begin{bmatrix} \alpha^0&0&0&\alpha^0&0&0&\alpha^0&0&0\\ 0&\alpha^0&0&0&\alpha^0&0&0&\alpha^0&0\\ 0&0&\alpha^0&0&0&\alpha^0&0&0&\alpha^0\\ \alpha^0&0&0&\alpha^1&0&0&\alpha^2&0&0\\ 0&\alpha^0&0&0&\alpha^1&0&0&\alpha^2&0\\ 0&0&\alpha^0&0&0&\alpha^1&0&0&\alpha^2\\ \alpha^0&0&0&\alpha^2&0&0&\alpha^1&0&0\\ 0&\alpha^0&0&0&\alpha^2&0&0&\alpha^1&0\\ 0&0&\alpha^0&0&0&\alpha^2&0&0&\alpha^1 \end{bmatrix}_{27\times 27}. \quad (32)$$

with the signal flow graph in Figure 1. It is obvious that $I_3 \otimes [J]_3$ and $[J]_3 \otimes I_3$ are both sparse matrices, and the two-fold matrix $[J]_{3^2}$ is a nine-order CBIJM of size 27×27. The index matrix $\mathcal{I}_9$ of $[J]_{3^2}$ is given by

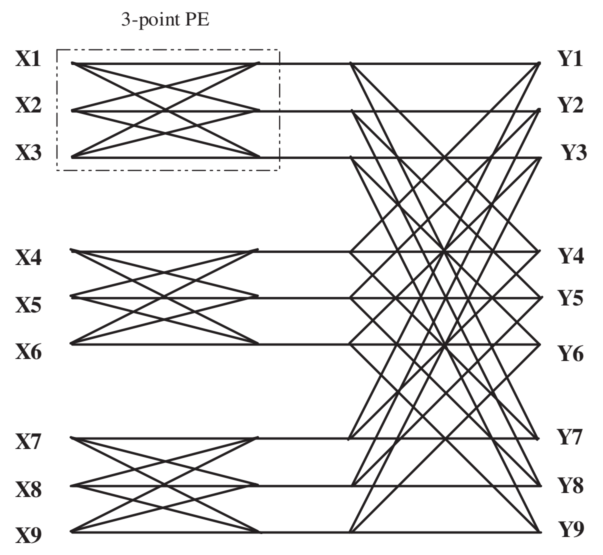


Figure 1 Signal flow graph for the two-fold CBIJM $[J]_{3^2}$ of order nine.

$$\mathcal{I}_9 = \begin{bmatrix} 0&0&0&0&0&0&0&0&0\\ 0&1&2&0&1&2&0&1&2\\ 0&2&1&0&2&1&0&2&1\\ 0&0&0&1&1&1&2&2&2\\ 0&1&2&1&2&0&2&0&1\\ 0&2&1&1&0&2&2&1&0\\ 0&0&0&2&2&2&1&1&1\\ 0&1&2&2&0&1&1&2&0\\ 0&2&1&2&1&0&1&0&2 \end{bmatrix}_{9\times 9}$$

which can be used for the generalization of the first order 3-ary Reed-Muller code [3].

Consequently, the s-fold CBIJM $[J]_{p^s}$ of order p^s can be generated from the following factorization algorithm

$$[J]_{p^s} = [J]_{p^{s-1}} \otimes [J]_p = \prod_{i=1}^{s} \left(I_{p^{s-i}} \otimes [J]_p \otimes I_{p^{i-1}} \right) \quad (33)$$

where I_{p^i} denotes the identity matrix of size $p^i \times p^i$ and $I_{p^0} = 1$ for the simple description.

Corollary 2. Based on the p-order CBIJM $[J]_p$ for any number p, the s-fold CBIJM $[J]_{p^s}$ of order p^s can be constructed with the recursive formula

$$[J]_{p^s} = \prod_{i=1}^{s} \left(I_{p^{s-i}} \otimes [J]_p \otimes I_{p^{i-1}} \right), \quad (34)$$

where p is any prime number and s is a nonnegative integer number.

The proof of Corollary 2 is shown in Appendix.

In order to show the factorization of the generalized CBIJM $[J]_n$ of order p^s with any prime number p, we propose several construction approaches in Table 4. In this table, the second column is the decomposition for the numbers (order) of the CBIJM, and the third column is the construction for CBIJM. It shows that the large-order CBIJM can be designed on the basis of the lower order CBIJM $[J]_p$ with sparse matrices in the successive architecture.

Low-density of the CBIJM

In what follows, we consider the density of 1's in the s-fold CBIJM $[J]_{p^s}$.

According to the afore-mentioned CBIJM $[J]_p$, it is known that matrix $[J]_p$ whose matrix unit is α in (4) is a $p^2 \times p^2$ binary matrix. The total number of 1's is p in each matrix unit α^h, $\forall\, h \in \mathcal{Z}_p$. Then the density of 1's in α^h is

$$\rho(\alpha^h) = \frac{p}{p^2} = \frac{1}{p}. \qquad (35)$$

Therefore the density of 1's in $[J]_p$ is calculated as

$$\rho([J]_p) = \rho(\alpha^h) = \frac{1}{p}, \qquad (36)$$

and the density of 1's in the s-fold matrix $[J]_{p^s}$ is

$$\rho([J]_{p^s}) = \rho([J]_p) = \frac{1}{p}, \qquad (37)$$

which shows that the larger matrix order p means the lower density of 1's in both $[J]_p$ and $[J]_{p^s}$.

As an example, we consider the CBIJM $[J]_2$ in Example 3 and the two-fold CBIJM $[J]_{2^2}$ in Example 5 with matrix unit $\alpha = [e_{i,j}]_{2\times 2}$ in (4). It is easy to verify that the densities of 1's in $[J]_2$, and $[J]_{2^2}$ are all 1/2, i.e., $\rho([J]_{2^2}) = \rho([J]_2) = 1/2$. Generally, for any prime number p we have $\rho([J]_{p^2}) = \rho([J]_p) = \rho(\alpha) = 1/p$, as shown in Table 5.

Table 4 Decompositions of orders for the CBIJM $[J]_{p^s}$ with density $1/p$

Order	Decomposition	CBIJM	Density
2	$2 = 2$	$[J]_2 = [J]_2$	1/2
3	$3 = 3$	$[J]_3 = [J]_3$	1/3
4	$2^2 = 2 \times 2$	$[J]_4 = [J]_2^{\otimes 2}$	1/2
5	$5 = 5$	$[J]_5 = [J]_5$	1/5
7	$7 = 7$	$[J]_7 = [J]_7$	1/7
8	$2^3 = 2^2 \times 2$	$[J]_8 = [J]_2^{\otimes 3}$	1/2
9	$3^2 = 3 \times 3$	$[J]_9 = [J]_3^{\otimes 2}$	1/3
11	$11 = 11$	$[J]_{11} = [J]_{11}$	1/11
13	$13 = 13$	$[J]_{13} = [J]_{13}$	1/13
16	$2^4 = 2^3 \times 2$	$[J]_{16} = [J]_2^{\otimes 4}$	1/2
17	$17 = 17$	$[J]_{17} = [J]_{17}$	1/17
19	$19 = 19$	$[J]_{19} = [J]_{19}$	1/19
23	$23 = 23$	$[J]_{23} = [J]_{23}$	1/23
25	$5^2 = 5 \times 5$	$[J]_{25} = [J]_5^{\otimes 2}$	1/5

Designs of the CBIJM over finite field GF(2^m)

In this section, we consider the generalized CBIJM over finite field GF(2^m) and derive the high-order CBIJM for $p = 2^m - 1$.

Let α be a matrix unit of size $p \times p$ over GF(2^m) such that $\alpha^{2^m-1} = I$ and $\alpha \neq I$. Then we obtain the $(2^m - 1)$-order CBIJM $[J]_{2^m-1}$ as follows.

Theorem 3. Let

$$[J]_{2^m-1} \triangleq [\alpha^{ij}]_{2^m-1}$$

be a $(2^m - 1)$-order block matrix over GF(2^m), $\forall\, i,j \in \mathcal{Z}_{2^m-1}$, where α is a matrix unit of size $(2^m - 1) \times (2^m - 1)$ satisfying $\alpha^{2^m-1} = I$ and $\alpha \neq I$. Then block matrix $[J]_{2^m-1}$ is a CBIJM.

The proof of Theorem 3 are shown in Appendix.

Example 7. We consider the seven-order block matrix $[J]_{2^3-1}$ with the primitive polynomial $x^3 + x + 1 = 0$ over GF(2^3). Let α be an arbitrary matrix unit such that $\alpha^7 = I$ and $\alpha \neq I$. Then any matrix element β over GF(2^3) can be represented as a binary vector (b_0, b_1, b_2), $\forall\, b_i \in \mathcal{Z}_2$ and $i \in \{0, 1, 2\}$, such that

$$\beta = b_0 + b_1\alpha + b_2\alpha^2.$$

By the Table 6, it is straightforward that Theorem 3 is true over GF(2^3). Then we obtain the BIJM $[J]_7$ and its inverse $[J]_7^{-1}$, i.e.,

$$[J]_7 = \begin{bmatrix} \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ \alpha^0 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 \\ \alpha^0 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \\ \alpha^0 & \alpha^4 & \alpha^1 & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\ \alpha^0 & \alpha^5 & \alpha^3 & \alpha^1 & \alpha^6 & \alpha^4 & \alpha^2 \\ \alpha^0 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 \end{bmatrix}, \qquad (38)$$

Table 5 Densities of the matrix units α, CBIJM $[J]_p$, and s-fold CBIJM $[J]_{p^s}$

	2	3	5	7	11
α	1/2	1/3	1/5	1/7	1/11
$[J]_p$	1/2	1/3	1/5	1/7	1/11
$[J]_{p^s}$	1/2	1/3	1/5	1/7	1/11

Table 6 Binary representation of β over GF(2^3)

Elements	Binary representation
0	(0 0 0)
α^0	(1 0 0)
α^1	(0 1 0)
α^2	(0 0 1)
α^3	(1 1 0)
α^4	(0 1 1)
α^5	(1 1 1)
α^6	(1 0 1)

and

$$[J]_7^{-1} = \frac{1}{7}\begin{bmatrix} \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 \\ \alpha^0 & \alpha^5 & \alpha^3 & \alpha^1 & \alpha^6 & \alpha^4 & \alpha^2 \\ \alpha^0 & \alpha^4 & \alpha^1 & \alpha^5 & \alpha^6 & \alpha^2 & \alpha^3 \\ \alpha^0 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \\ \alpha^0 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 \\ \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{bmatrix}. \qquad (39)$$

Actually, according to the index mapping of the present matrix in Table 7, it can be shown that matrix $[J]_7$ in (38) is a seven-order CBIJM over GF(2^3).

Two-dimensional fast CBIJM

In the previous section, we consider the one-dimensional CBIJT based on the CBIJM. Now we extend it to the version of the two-dimensional CBIJT.

The fast two-dimensional CBIJM can be similarly derived from the two-dimensional Jacket transform [15]

$$Y = [J]_{p^s} X [J]_{p^s}^{\mathrm{T}},$$

which can be expressed by the transformation of the column-wise stacking vector X as

$$\mathrm{vec}(Y) = ([J]_{p^s} \otimes [J]_{p^s})\mathrm{vec}(X).$$

Namely, if $X = (\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{p^s-1})$, then $\mathrm{vec}(X) = (\mathbf{x}_0^{\mathrm{T}}, \mathbf{x}_1^{\mathrm{T}}, \ldots, \mathbf{x}_{p^s-1}^{\mathrm{T}})^{\mathrm{T}}$, where $\mathbf{x}_i$ denotes the ith column of X, $\forall\ i \in \mathcal{Z}_{p^s}$. It shows that the fast algorithm of the two-dimensional CBIJM can be designed from the two-fold one-dimensional CBIJM, i.e.,

$$[J]_{p^{2s}} = [J]_{p^s} \otimes [J]_{p^s}.$$

Table 7 Index mapping of CBIJM $[J]_7$ over GF(2^3)

$g \setminus h$	0	1	2	3	4	5	6
0	α^0	α^0	α^0	α^0	α^0	α^0	α^0
1	α^0	α^1	α^2	α^3	α^4	α^5	α^6
2	α^0	α^2	α^4	α^6	α^1	α^3	α^5
3	α^0	α^3	α^6	α^2	α^5	α^1	α^4
4	α^0	α^4	α^1	α^5	α^2	α^6	α^3
5	α^0	α^5	α^3	α^1	α^6	α^4	α^2
6	α^0	α^6	α^5	α^4	α^3	α^2	α^1

Based on the fast algorithm of $[J]_{p^s} \otimes [J]_{p^s}$, we have the fast algorithm of two-dimensional CBIJM $[J]_{p^{2s}}$ in the recursive fashion expressed in (40). It illustrates that the two-dimension CBIJM can be concerned with the sparse matrix factorizations based on the factorizations of one-dimensional CBIJM. A successive architecture for reducing the computational load can also be developed in the similar fast algorithms as that of one-dimensional CBIJM while factorizing two-dimensional CBIJM into the lower order sparse matrices with low complexities.

$$\begin{aligned} [J]_{p^{2s}} &= \left([J]_{p^s} \otimes I_{p^s}\right)\left(I_{p^s} \otimes [J]_{p^s}\right) \\ &= \left[\left([J]_{p^{s-1}} \otimes [J]_p\right) \otimes I_{p^s}\right]\left[I_{p^s} \otimes \left([J]_{p^{s-1}} \otimes [J]_p\right)\right] \\ &= \left\{\left[\left([J]_{p^{s-1}} \otimes I_p\right)\left(I_{p^{s-1}} \otimes [J]_p\right)\right] \otimes I_{p^s}\right\} \\ &\quad \times \left\{I_{p^s} \otimes \left[\left([J]_{p^{s-1}} \otimes I_p\right)\left(I_{p^{s-1}} \otimes [J]_p\right)\right]\right\} \\ &= \left([J]_{p^{s-1}} \otimes I_p \otimes I_{p^s}\right)\left(I_{p^{s-1}} \otimes [J]_p \otimes I_{p^s}\right) \\ &\quad \times \left(I_{p^s} \otimes [J]_{p^{s-1}} \otimes I_p\right)\left(I_{p^s} \otimes I_{p^{s-1}} \otimes [J]_p\right). \end{aligned} \qquad (40)$$

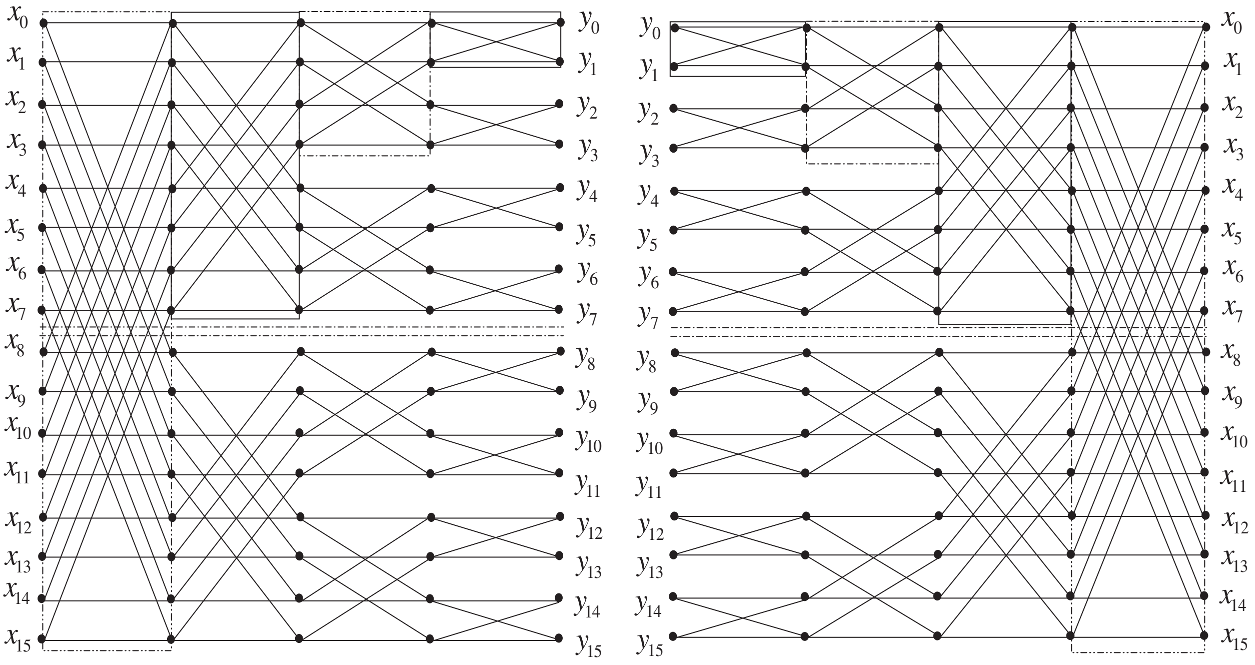
Example 8. We consider the two-dimensional four-order CBIJM

$$\begin{aligned} [J]_{2^4} &= [J]_{2^2} \otimes [J]_{2^2} \\ &= ([J]_2 \otimes I_2 \otimes I_4)\,(I_2 \otimes [J]_2 \otimes I_4) \cdot \\ &\quad \times (I_4 \otimes [J]_2 \otimes I_2)\,(I_4 \otimes I_2 \otimes [J]_2). \end{aligned} \qquad (41)$$

It is shown in the previous section that block matrix $[J]_{2^2}$ is a four-order CBIJM that can be constructed in the recursive fashion on the basis of $[J]_2$ with fast algorithm. Therefore, the two-dimensional CBIJM $[J]_{2^4}$ can be similarly designed in the recursive fashion with fast algorithm based on two-fold four-order CBIJT $[J]_{2^2}$, as shown in Figure 2. Compared with the fast algorithm of the one-dimensional CBIJM $[J]_{3^2}$ in Figure 1, the present fast algorithm needs four steps for calculations, instead of two steps for the factorizing decomposition.

Conclusion

A simple method of developing the fast CBIJM is proposed over finite field. This method is presented for its simplicity and clarity, which decomposes the high-order CBIJM into multiple sparse matrices with the lower-order CBIJMs, instead of the conventional BIJMs or EIJMs. This factorization algorithm is valid for the generalized s-fold CBIJM of order p^s over finite field with a suitable matrix unit α of size $p \times p$. Also, the present CBIJM is useful for developing the fast two-dimensional CBIJM based on



(a) Forward 2-Dimentional Fast CBJIM Algorithm

(b) Inverse 2-Dimentional Fast CBJIM Algorithm

Figure 2 Signal flow graph for the two-dimensional two-fold four-order CBIJM $[J]_{16}$ based on $[J]_2$, i.e., $[J]_{16} = [J]_{2^2} \otimes [J]_{2^2}$.

sparse matrices in the recursive forms. It may have potential applications in combinatorial designs (CD) [8], space-time block codes [23,27], and odd-order code design [20] thanks to its successive architecture.

Appendix

Proof of Lemma 1

If $a = b = 0$, then $[\beta_0] = [I, I, \ldots, I]$, and hence $[\beta_0] \cdot [\beta_0]^{\mathrm{T}} = pI$. If $\langle a + b \rangle_p = 0$, $\forall\, a, b \in \mathcal{Z}_p$, then for $\forall\, h_i \in \mathcal{Z}_p$,

$$f_a(h_i) + f_b(h_i) = \langle ah_i \rangle_p + \langle bh_i \rangle_p = \langle (a+b)h_i \rangle_p = 0. \tag{42}$$

Therefore, it is easy to verify that

$$[\beta_a] \cdot [\beta_b]^{\mathrm{T}} = \sum_{i=1}^{p} \alpha^{f_a(h_i) + f_b(h_i)} = pI.$$

But if $\langle a + b \rangle_p \neq 0$, then for $0 < \langle a + b \rangle_p < p$,

$$\left\{ \langle c(a+b) \rangle_p : c \in \mathcal{Z}_p \right\} = \mathcal{Z}_p. \tag{43}$$

Consequently, we have

$$[\beta_a] \cdot [\beta_b]^{\mathrm{T}} = \sum_{i=0}^{p-1} \alpha^i, \tag{44}$$

which can be proved to be equal to zero over the finite field since $\alpha^p - I = 0$ but for $\alpha \neq I$.

Proof of Theorem 1

According to the defined BIJM $[J]_p$ in (15), we have $\phi(a, b) := \alpha^{\langle a \cdot b \rangle_p}$. For $\forall\, c \in \mathcal{Z}_p$, we have

$$\phi(a, b)\phi(a \circ b, c) = \alpha^{\langle a \cdot b \rangle_p} \cdot \alpha^{\langle (a+b)c \rangle_p} = \alpha^{\langle a \cdot b + (a+b) \cdot c \rangle_p}. \tag{45}$$

On the other hand,

$$\phi(a, b \circ c)\phi(b, c) = \alpha^{\langle a \cdot (b+c) \rangle_p} \cdot \alpha^{\langle b \cdot c \rangle_p} = \alpha^{\langle a \cdot (b+c) + b \cdot c \rangle_p}. \tag{46}$$

Combining (45) and (46), we have

$$\phi(a, b)\phi(a \circ b, c) = \phi(a, b \circ c)\phi(b, c). \tag{47}$$

Thus the BIJM $[J]_p$ is also a CBIJM.

Proof of Theorem 2

Since $[A]_p = [\alpha_{i,j}]_p$ and $[B]_p = [\gamma_{s,t}]_p$ are both BIJM, we have the inverse

$$[A]_p^{-1} = \frac{1}{p} [\alpha_{i,j}^{-1}]_p^{\mathrm{T}}, \;\; [B]_p^{-1} = \frac{1}{p} [\gamma_{s,t}^{-1}]_p^{\mathrm{T}}. \tag{48}$$

Let

$$[A]_p \otimes [B]_p = \left[\sigma_{ip+s, jp+t} \right]_{p^2},$$

where $\sigma_{ip+s,jp+t} = \alpha_{i,j} \cdot \gamma_{s,t}$ denotes the traditional multiplication of two matrices. Therefore, we have the inverse matrix $[J]_{p^2}^{-1}$ that can be calculated directly from the block-wise inverse of the original block matrix $[J]_{p^2}$ in (24), i.e.,

$$\begin{aligned} {}_{p^2}^{-1} &= \left([A]_p \otimes [B]_p\right)^{-1} = \left([A]_p^{-1} \otimes [B]_p^{-1}\right) \\ &= \frac{1}{p^2}\left[\alpha_{i,j}^{-1} \cdot \gamma_{s,t}^{-1}\right]_{p^2}^{\mathrm{T}} = \frac{1}{p^2}\left[\sigma_{ip+s,jp+t}^{-1}\right]_{p^2}^{\mathrm{T}}. \end{aligned} \tag{49}$$

It implies that $[J]_{p^2}$ is a block Jacket matrix.

Next, we show that matrix $[J]_{p^2}$ is a CBIJM under the indexed row and column. Assume that $[A]_p$ and $[B]_p$ are both CBIJMs under the row and column index over $\mathcal{Z}_p$, respectively,

$$\begin{cases} a_{s1} \prec a_{s1} \prec \cdots \prec a_{sp}, \text{ for } a_{sj} \in \mathcal{Z}_p, \ \forall\, j \in \mathcal{Z}_p; \\ b_{s1} \prec b_{s1} \prec \cdots \prec b_{sp}, \text{ for } b_{sk} \in \mathcal{Z}_p, \ \forall\, k \in \mathcal{Z}_p, \end{cases} \tag{50}$$

where $s \in \{r, c\}$, a_{rj} and a_{cj} denote the jth row and the jth column index of block matrix $[A]_p$, b_{rk} and b_{ck} denote the kth row and the kth column index of block matrix $[B]_p$, and $\prec$ denotes the increasing order. Then for the p^2-order block matrix $[J]_{p^2}$ over $\mathcal{Z}_{p^2}$, the row and column index order can be defined as follows

$$a_{sj}b_{sk} \prec a_{si}b_{sh} \text{ if } \begin{cases} a_{sj} \prec a_{si}; \\ a_{sj} = a_{si}, b_{sk} \prec b_{sh}. \end{cases} \tag{51}$$

Also the entries of $[J]_{p^2}$ are defined on the basis of $[J]_p$ as

$$\phi_{p^2}(a_{ri}b_{rh}, a_{cj}b_{ck}) = \phi_p(a_{ri}, a_{cj}) \cdot \phi_p(b_{rh}, b_{ck}). \tag{52}$$

As for the entries $\phi_p(a_i, a_j)$ and $\phi_p(b_h, b_k)$ of $[A]_p$ and $[B]_p$, $\forall\, a_i, a_j, a_l \in \mathcal{Z}_p$ and $\forall\, b_h, b_k, b_t \in \mathcal{Z}_p$, we have

$$\phi_p(a_i, a_j)\phi_p(a_i \circ a_j, a_l) = \phi_p(a_i, a_j \circ a_l)\phi_p(a_j, a_l), \tag{53}$$

$$\phi_p(b_h, b_k)\phi_p(b_h \circ b_k, b_t) = \phi_p(b_h, b_k \circ b_t)\phi_p(b_k, b_t). \tag{54}$$

Therefore, it can be easily verified that

$$\begin{aligned} &\phi_{p^2}(a_ib_h, a_jb_k)\phi_{p^2}(a_ib_h, a_jb_k \circ a_lb_t) \\ &\quad = \phi_{p^2}(a_ib_h, a_jb_k \circ a_lb_t)\phi_{p^2}(a_jb_k, a_lb_t). \end{aligned} \tag{55}$$

It shows that block matrix $[J]_{p^2}$ is also a CBIJM under the indexed order in (51). This completes the proof of this theorem.

Proof of Corollary 2

We deploy induction on index s. If $s = 1$, then it is clearly true, i.e., $[J]_{p^1} = [J]_p$. In what follows, we assume the hypothesis is true for s. Namely, for $\forall\, i \in \{1, 2, \ldots, s\}$ we have the following hypothesis:

$$[J]_{p^s} = \prod_{i=1}^{s}\left(I_{p^{s-i}} \otimes [J]_p \otimes I_{p^{i-1}}\right). \tag{56}$$

Then we show it must therefore hold for $s+1$. Actually, by induction based on properties of the Kronecker product we have

$$\begin{aligned} [J]_{p^{s+1}} &= [J]_p \otimes [J]_{p^s} \\ &= \left([J]_p \cdot I_p\right) \otimes \left(I_{p^s} \cdot [J]_{p^s}\right) \\ &= \left([J]_p \otimes I_{p^s}\right)\left(I_p \otimes [J]_{p^s}\right). \end{aligned} \tag{57}$$

Combining (56) and (58), we obtain

$$[J]_{p^{s+1}} = \prod_{i=1}^{s+1}\left(I_{p^{s-i}} \otimes [J]_p \otimes I_{p^{i-1}}\right). \tag{58}$$

This completes the proof of this corollary.

Proof of Theorem 3

In order to prove Theorem 3, we introduce a lemma as follows.

Lemma 3.

$$\sum_{i=0}^{2^m-2} \alpha^{ir} = \begin{cases} (2^m - 1)I, & \text{for } r = 0; \\ 0, & \text{for } 1 \le r \le 2^m - 2. \end{cases} \tag{59}$$

Proof. It is evident that $\sum_{i=0}^{2^m-2} \alpha^{ir}$ contains $2^m - 1$ terms. If $r = 0$, then $\sum_{i=0}^{2^m-2} \alpha^{ir}$ is a sum of $2^m - 1$ identity matrices. Thus the first equation is proved. We now consider the case of $1 \le r \le 2^m - 2$ such that $\alpha^r \ne I$, i.e., $\alpha^r - I \ne 0$. Since $\alpha^{2^m-1} = I$, then we have $\alpha^{r(2^m-1)} = I$ and

$$0 = \alpha^{r(2^m-1)} - I = \left(\alpha^r - I\right)\sum_{i=0}^{2^m-2} \alpha^{ir},$$

from which we obtain

$$\sum_{i=0}^{2^m-2} \alpha^{ir} = 0.$$

Then the proof is completed. □

With the aid of Lemma 3, we show the existence of CBIJM for Theorem 3.

According to the definition of the $(2^m - 1)$-order block matrix $[J]_{2^m-1}$, we let

$$[J]_{2^m-1}^{-1} = \frac{1}{2^m - 1}[\alpha^{\langle -ij \rangle_{2^m-1}}]_{2^m-1}^{\mathrm{T}}.$$

By the simple calculation, it can be verified that

$$[J]_{2^m-1}[J]_{2^m-1}^{-1} = [J]_{2^m-1}^{-1}[J]_{2^m-1} = I_{2^m-1}.$$

It shows that block matrix $[J]_{2^m-1}$ is a BIJM. In order to prove that it is a CBIJM, we let $\phi(i, j)$ be an entry in position (i, j), where the order of rows and columns is from

0 to $2^m - 2$ over $\mathcal{Z}_{2^m-1}$. Consequently, for $i, j, h, k \in \mathcal{Z}_{2^m-1}$ we have

$$\begin{aligned}
&\phi(i,j) = \alpha^{\langle i\cdot j\rangle_{2^m-1}},\\
&\phi(i,j\circ h) = \alpha^{\langle i\cdot(j+h)\rangle_{2^m-1}},\\
&\phi(i,j)\phi(h,k) = \alpha^{\langle i\cdot j+h\cdot k\rangle_{2^m-1}}.
\end{aligned} \tag{60}$$

Then we achieve

$$\phi(i,j\circ k)\phi(j,k) = \alpha^{\langle i\cdot(j+k)\rangle_{2^m-1}}\alpha^{\langle j\cdot k\rangle_{2^m-1}} = \alpha^{\langle i\cdot j+i\cdot k+j\cdot k\rangle_{2^m-1}}, \tag{61}$$

and

$$\phi(i,j)\phi(i\circ j,k) = \alpha^{\langle i\cdot j\rangle_{2^m-1}}\alpha^{\langle (i+j)\cdot k\rangle_{2^m-1}} = \alpha^{\langle i\cdot j+i\cdot k+j\cdot k\rangle_{2^m-1}}. \tag{62}$$

It is obvious to verify

$$\phi(i,j\circ k)\phi(j,k) = \phi(i,j)\phi(i\circ j,k), \tag{63}$$

which implies that the BIJM $[J]_{2^m-1}$ is a CBIJM over GF(2^m).

Competing interests
The authors do not have competing interests.

Acknowledgements
We acknowledge useful suggestions and valuable comments from referees. This study was supported by the National Natural Science Foundation of China (60902044, 610711096, 61111140391, 61272495), the New Century Excellent Talents in University of China (NCET-11-0510), and partly by the World Class University R32-2010-000-20014-0 NRF, and BSRP 2010-0020942 NRF, Korea, MEST 2012-002521, NRF, Korea, and 2011 Korea-China International Cooperative Research Project (Grant Nos. D00066, I00026). This work was done when Dr. Kyeong Jin Kim was working this work in Inha University, Korea.

Author details
[1]School of Information Science and Engineering, Central South University, Changsha 410083, China. [2]Institute of Information and Communication, Chonbuk National University, Jeonju 561-756, Korea. [3]Mitsubishi Electric Research Laboratories, 201 Broadway, Cambridge, MA 02139, USA.

Received: 10 February 2012 Accepted: 17 July 2012
Published: 24 August 2012

References

1. NU Ahmed, KR Rao, *Orthogonal Transforms for Digital Signal Processing* (Springer-Verlag, Inc., New York, 1975)
2. SS Agaian, *Hadamard Matrices and Their Applications,* (Lecture Notes in Mathematics) (Springer, Berlin, 1985)
3. SB Wicker, *Error Control Systems for Digital Communication and Storage* (Prentice-Hall, New Jersey, 1995)
4. RK Yarlagadda, JE Hershey, *Hadamard Matrix Analysis and Synthesis With Applications to Communications Signal/Image Processing* (Kluwer Academic Publishers, Dordrecht, 1997)
5. KJ Horadam, *Hadamard Mastrices and Their Applications* (Princeton University Press, Princeton, 2006)
6. RE Blahut, *Algebraic Codes for Data Transmission* (Cambridge Press, Cambridge, 2003)
7. AT Butson, Generalized Hadamard matrices. Proc. Am. Math. Soc. **13**, 894–898 (1962)
8. GL Feng, MH Lee, in *5th Shanghai Conference in Combinatorics*. An explicit construction of co-cyclic Jacket matrices with any size (Shanghai, China, 2005)
9. MH Lee, The center weighted Hadamard transform. IEEE Trans. Circ. Syst. **CAS-36**, 1247–1252 (1989)
10. MH Lee, YL Borrisov, On Jacket transforms over finite fields. Int. Symp. Inf. Theory, Seoul, Korea, 2803–2807 (2009)
11. MH Lee, A new reverse jacket transform and its fast algorithm. IEEE Trans. Circ. Syst. II, Analog Digit. Signal Process. **47**(1), 39–47 (2000)
12. MH Lee, BS Rajan, JY Park, A generalized reverse Jacket transform. IEEE Trans. Circ. Syst. **48**, 684–688 (2001)
13. MH Lee, Y Guo, A novel construction of Jacket matrix from characters on finite Abelian group. Electron. Lett. **46**, 1199–1200 (2010)
14. Z Chen, MH Lee, Fast cocyclic Jacket transform. IEEE Trans. Signal Process. **56**(5), 2143–2148 (2008)
15. MH Lee, J Hou, Fast block inverse Jacket transform. IEEE Signal Process. Lett. **13**(4), 461–464 (2006)
16. GH Zeng, MH Lee, A generalized reverse block Jacket transform. IEEE Trans. Circ. Syst. **55**, 1589–1599 (2008)
17. MH Lee, XD Zhang, Fast block center weighted Hadamard transform. IEEE Trans. Circ. Syst. **54**(12), 2741–2745 (2007)
18. MH Lee, K Finlayson, A simple element inverse Jacket transform coding. IEEE Signal Process. Lett. **14**(5), 325–328 (2007)
19. Jacket matrix http://en.wikipedia.org/wiki/Jacket_matrix; Category: Matrix http://en.wikipedia.org/wiki/; Category: Matrices Leejacket http://en.wikipedia.org/wiki/leejacket
20. B Yuri, SM Dodunekov, MH Lee, in *12th Algebraic and Combinatorial Coding Theory*. On odd order Jacket matrices over finite character fields, (Novosibirsk, Russi, 2010)
21. Z Chen, MH Lee, W Song, in *IEEE Int. Conference on Communication*. Fast cocyclic, Jacket transform based on DFT, (2008), pp. 766–769
22. MH Lee, MM Matalgah, W Song, Fast method for precoding and decoding of distributive MIMO channels in relay-based decode-and-forward cooperative wireless networks. IET Commun. **4**(2), 144–153 (2010)
23. W Song, MH Lee, MM Matalgah, Y Guo, Quasi-orthogonal space-time block codes designs based on jacket transform. J. Commun. Netw. **12**(3), 766–769 (2010)
24. MH Lee, YL Borissov, SM Dodunekov, Class of jacket matrices over finite characteristic fields. Electron. Lett. **46**(13), 916–918 (2010)
25. MH Lee, YL Borissov, A proof of non-existence of bordered jacket matrices of odd order over some fields. Electron. Lett. **46**(5), 349–351 (2010)
26. MH Lee, XD Zhang, W Song, in *IET Conference on Wireless, Mobiloe and Sensor Networks,* vol. 12. A note on Eigenvlaue decomposition on Jacket transform, (2007), pp. 987–990
27. W Song, MH Lee, GH Zeng, in *IEEE Int. Conf. Commun*. Orthogonal space-time block codes design using Jacket transform for MIMO transmission system, (2008), pp. 766–769
28. XQ Jiang, MH Lee, Y Guo, YE Yan, SA Latif, Ternary codes from modified Jacket matrices. J. Commun. Netw. **13**(1), 12–16 (2011)
29. KJ Horadam, P Udaya, Cocyclic Hadamard codes. IEEE Trans. Inf. Theory. **46**(4), 1545–1550 (2000)
30. AAI Perera, KJ Horadam, Cocyclic generalised hadamard matrices and central relative difference sets. J. Designs Codes Crypt. **15**(2), 187–200 (1998)
31. J Hou, MH Lee, Cocyclic Jacket matrices and its application to cryptography systems. Lecture Notes Comput. Sci. **3391**, 662–668 (2005)

doi:10.1186/1687-6180-2012-184
Cite this article as: Guo *et al.*: **An explicit construction of fast cocyclic jacket transform on the finite field with any size.** *EURASIP Journal on Advances in Signal Processing* 2012 **2012**:184.