A Kind of Block Inverse Jacket Transform

Dazu Huang, Dan Song, Jianquan Xie and Rongliang Xiao

Department of Information Management, Hunan University of Finance and Economics, Changsha 410205, China.

Keywords: Cocyclic block inverse transform, Orthogonal transforms, Jacket Matrix

Abstract: A novel block inverse Jacket transform is proposed. A cocyclic block inverse Jacket matrix is constructed in which the high-order cocyclic block inverse Jacket matrix can be decomposed into the low-order sparse cocyclic block inverse Jacket matrices with a successive block architecture, instead of the conventional block inverse Jacket matrix (BIJM). It is a fast algorithm by using recursive mode that leads to reducing computational load.

Introduction

The interesting orthogonal matrices, such as the element-wise or block-wise inverse Jacket matrices, have been developed with orthogonal transforms widely employed in images processing, coding, and other areas [1-3]. More details of these matrices can be referred to [4-8].

Definition I: A $n \times n$ 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 obtained by its element-wise inverse.

Many interesting orthogonal matrices belong to the Jacket matrix. 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 [9-13].

Recently, the BIJM $[J_p]$, has been investigated while the complex unit $\exp(\frac{\sqrt{12}\pi}{p})$ of the EIJM $J_n$ is substituted for a suitable matrix unit [7-8]. However, the CBIJM does not attract much attention even though the cocyclic matrix has been very useful for the data coding and processing [14-15].

Definition II: If $\zeta$ is a finite group of order $\gamma$ with operation $\circ$ and $C$ is a finite Abelian group of order $t$, a co-cycle is a mapping $\phi: \zeta \times \zeta \rightarrow C$ satisfying $\phi(a, b)\phi(a \circ b, c) = \phi(a, b \circ c) \phi(b, c)$ where $a, b, c \in \zeta$. A square matrix $M(\phi)$ whose row $a$ and column $b$ can be indexed by $\zeta$ with entry $\phi(a, b) \in \zeta$ in position $(a, b)$ under some fixed ordering, i.e., $M(\phi) = (\phi(a, b))_{a,b \in \zeta}$, is called a cocyclic matrix. If $\phi(1, 1) = 1$, then it is the normalized cocyclic matrix [14-15].

Definition III: Let $J_p = (\omega^{(i,j)})_{p \times p}$, $\forall i, j \in Z_p : = \{0, 1, \cdots, p - 1\}$, be a matrix of order $p$, where $\omega = \exp(\frac{\sqrt{-1}2\pi}{p})$ and $\{i \odot j\}_p = i \times j \mod p$, i.e., the subscript $p$ implies modulo $-p$ arithmetic for the argument. Then the matrix $J_p$ and its $s$-fold matrix of order $p^s$, $J_p^s = J_p \odot J_p \cdots \odot J_p$ are the conventional cocyclic element inverse Jacket matrices (CEIJM), where $\odot$ denotes the Kronecker product and $p$ is a prime number.

As a generation of the Hadamard matrix, BIJM inherits the merits of the Hadamard matrix. The inverse transform can be easily obtained by the reciprocal relationships and the fast algorithms. However, versions of cocyclic block-wise inverse Jacket matrix (CBIJM) are still absent [10]. The purpose of this paper is to develop the CBIJM and its generalizations, instead of the CEIJM.

This paper is organized as follows. Section II presents a framework of the fast CBIJT. Section III reports the $p$-order CBIJM. Section IV discusses the multi-fold CBIJM. Finally, conclusions are drawn in Section V.
Cocyclic Block Inverse Transforms

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

In order to derive the CBIJT, we denote a matrix unit by $\alpha$ 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 $\alpha$ be a square matrix of size $2 \times 2$ defined as

$$\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (1)$$

It is easy to prove that $\alpha^2 = I_2$. Actually, matrix $\alpha$ has been employed for the existence of the BIJM [3]. Fortunately, it will be shown that the $s$-fold block Jacket matrix $[J]_s \Delta \alpha^{ss}$ is also a CBIJM.

We illustrate the cocyclicity of the BIJM $[J]_p$, based on the matrix unit $\alpha$ 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

$$e_{i,j} = \begin{cases} 1, & \text{for } i = \langle j + h \rangle_p; \\ 0, & \text{otherwise,} \end{cases} \quad (2)$$

where $\langle j + h \rangle_p = j + h \mod p, \forall i, j, h \in Z_p = \{0,1,\ldots, p-1\}$. $A := \{\alpha^h : h \in Z_p\}$ forms an Abelian group with the matrix multiplication.

**Example I**: Let $p = 3$, and we have

$$I_3 = \alpha^0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \alpha^1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \alpha^2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \quad (3)$$

Obviously $Z_p$ with the multiplication operation $\langle a \cdot b \rangle_p$ is a finite field of order $p$. For $\forall a, x \in Z_p$, we define an multiplication function $f_a(x)$ over $Z_p$, i.e., $f_a(x) := \langle a \cdot x \rangle_p$. 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 $\alpha^h$ of size $p \times p, \forall h \in Z_p$, i.e., $[\beta] := [\alpha^h, \alpha^{h^2}, \ldots \alpha^{h^{p-1}}]$, and hence

$$[\beta] = [\alpha^{(h_1)}, \alpha^{(h_2)}, \ldots \alpha^{(h_p)}]. \quad (4)$$

**Lemma I**: For block matrices $[\beta_a]$ and $[\beta_b], \forall a, b \in Z_p, we have $[\beta_a] \cdot [\beta_b] = \begin{cases} pI, & \text{for } \langle a + b \rangle_p = 0; \\ 0, & \text{for } \langle a + b \rangle_p \neq 0. \end{cases}$

**Proof**: If $a = b = 0$, then $[\beta_a] = [I, I, \ldots, I]$, and hence $[\beta_a] \cdot [\beta_b] = pI$. If $\langle a + b \rangle_p = 0, \forall a, b \in Z_p, then for \forall h \in Z_p, f_a(h) + f_b(h) = \langle ah \rangle_p + \langle bh \rangle_p = \langle (a + b)h \rangle_p = 0$. Therefore, it is easy to verify that $[\beta_a] \cdot [\beta_b] = \sum_{h=1}^{p-1} \alpha^{(h_1)} \cdot \alpha^{(h_2)} = pI$. But if $\langle a + b \rangle_p \neq 0, \forall 0 < \langle a + b \rangle_p < p$, $\{c(a + b) : c \in Z_p\} = Z_p$. Consequently, we have $[\beta_a] \cdot [\beta_b] = \sum_{i=0}^{p-1} \alpha^i$, which can be proved to be equal to zero since $\alpha^p - I = 0$ but for $\alpha \neq I$.

**Example II**: Let us consider $\alpha$ with $p = 2$ in (1). It is obvious that $\alpha^2 = I$ is an identity matrix of size $2 \times 2$. Let $[\beta] = [\alpha^0, \alpha^1], then [\beta_a] = [\alpha^0, \alpha^1] = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad [\beta_b] = [\alpha^0, \alpha^1] = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$.
It is straightforward to show that
\[
[\beta_0];[\beta_1]^T = [\beta_2];[\beta_1]^T = 2I_2.
\]  

(5)

The \(p\)-order CBIJM

In [7-8], Lee et al. expanded the EIJM to BIJM.

Definition IV: A \(np \times np\) block matrix \([J]_n = ([\alpha_0])_{np \times np}\) is called the BIJM of order \(n\) if \([J]_n^T = \frac{1}{c}([\alpha_0])_{np \times np}^T\), where \(c\) is the normalized value and \([\alpha_0])_{p \times p}\) denotes a matrix unit of size \(p \times p\).

Definition V: For a given prime number \(p\), let \(\alpha\) be a \(p \times p\) matrix unit such that \(pI_\alpha = 0\) and \(\alpha_0, \alpha_1, \ldots, \alpha_{p-1}\). Define the \(p\)-order BIJM \([J]_p\) of size \(p^2 \times p^2\) as follows

\[
[J]_p := [\begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_{p-1} \end{pmatrix}] = [\begin{pmatrix} \alpha_0^0 & \alpha_0^1 & \ldots & \alpha_0^{p-1} \\ \alpha_0^1 & \alpha_0^2 & \ldots & \alpha_0^{2(p-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{p-1} & \alpha_0^{2(p-1)} & \ldots & \alpha_0^{(p-1)(p-1)} \end{pmatrix}]
\]  

(6)

and thus its inverse

\[
[J]_p^{-1} := \frac{1}{p} [\begin{pmatrix} \alpha_0^0 & \alpha_0^{-(p-1)} & \ldots & \alpha_0^{-(p-1)(p-1)} \\ \alpha_0^1 & \alpha_0^{-2(p-1)} & \ldots & \alpha_0^{-(p-1)(p-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{p-1} & \alpha_0^{-2(p-1)} & \ldots & \alpha_0^{-(p-1)(p-1)} \end{pmatrix}]
\]  

(7)

Consequently, we have \([J]_p \cdot [J]_p^{-1} = [J]_p^T \cdot [J]_p = I_{p^4} \cdot p^2\).

Example III: Taking \([\beta_0]\) and \([\beta_1]\) for \(p = 2\), we have

\[
[J]_2 = [\begin{pmatrix} \alpha_0^0 & \alpha_0^1 \\ \alpha_0^1 & \alpha_0^2 \end{pmatrix}] = [\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}],
\]  

(8)

and its inverse

\[
[J]_2^{-1} = \frac{1}{2} [\begin{pmatrix} \alpha_0^0 & \alpha_0^1 \\ \alpha_0^1 & \alpha_0^{-(p-1)} \end{pmatrix}] = [\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}].
\]  

(9)

Actually, we have

\[
[J]_2[J]_2^{-1} = [\begin{pmatrix} \alpha_0^0 & \alpha_0^1 \\ \alpha_0^1 & \alpha_0^2 \end{pmatrix}][\begin{pmatrix} \alpha_0^0 & \alpha_0^1 \\ \alpha_0^1 & \alpha_0^2 \end{pmatrix}] = [\begin{pmatrix} I_2 & 0 \\ 0 & I_2 \end{pmatrix}],
\]  

(10)

where \(\alpha_0 + \alpha_1 = 0\) since \(\alpha^2 = l\) and \(\alpha \neq l\) over the finite field.

We note that the above-mentioned BIJM was first proposed by Lee and Hou [7] 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 Ⅰ: Let $\varsigma = \mathbb{Z}_p$ with an operation $a \circ b := \langle a + b \rangle_p$, $\forall a, b \in \mathbb{Z}_p$ and $C := \{\alpha^i : i \in Z_p\}$ with the traditional multiplication. The BIJM $[J]_p$ in (6) whose rows and columns are both indexed in $\varsigma$ under the increasing order (i.e., $0 < 1 < \cdots < p - 1$) and entries $\phi(a, b)$ in position $(a, b)$ is the CBIJM.

Proof: According to the defined BIJM $[J]_p$ in (6), we have $\phi(a, b) := \alpha^i_j$. For $\forall c \in Z_p$, we have
\[
\phi(a, b)\phi(a \circ b, c) = \alpha^{(a \circ b)}_j \cdot \alpha^{(a \circ b)\circ c}_{ij} = \alpha^{(a \circ b + a \circ c)}_{ij},
\]
(11)
On the other hand,
\[
\phi(a, b \circ c)\phi(b, c) = \alpha^{(a \circ c)}_j \cdot \alpha^{(a \circ c)}_{ij} = \alpha^{(a \circ c + b \circ c)}_{ij},
\]
(12)
Combining (11) and (12), we have
\[
\phi(a, b)\phi(a \circ b, c) = \phi(a, b \circ c)\phi(b, c).
\]
(13)
Thus the BIJM $[J]_p$ is also a CBIJM.

The Multi-fold CBIJM

In order to derive the high-order recursive CBIJM $[J]_p^r$ for any prime number $p$ and nonnegative integer $s$, let us introduce some lemmas [1-2].

Lemma Ⅱ: Let $A, B, C, D$ are matrices with suitable sizes. We have $(A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$, $(A \otimes B)^{-1} = (A^{-1} \otimes B^{-1})(A \otimes B)^T = (A^T \otimes B^T)$.

Theorem 2: For a given prime number $p$, let $[A]_p = [\alpha_{i,j}]_p$ and $[B]_p = [\gamma_{i,j}]_p$, $\forall i, j, s, t \in Z_p$, be two CBIJMs of order $p$ that correspond to the matrix units $\alpha$ and $\gamma$ such that $\alpha^p = I$ and $\gamma^p = I$, respectively. Then the 2-fold Kronecker product matrix $[J]_p^r = [A]_p \otimes [B]_p$ is a 2-fold CBIJM of order $p^2$.

Proof: Since $[A]_p = [\alpha_{i,j}]_p$ and $[B]_p = [\gamma_{i,j}]_p$ are both BIJM, we have the inverse
\[
[A]_p^{-1} = \frac{1}{p} [\alpha_{i,j}]_p^{-1}, \quad [B]_p^{-1} = \frac{1}{p} [\gamma_{i,j}]_p^{-1},
\]
(14)
Let $[A]_p \otimes [B]_p = [\sigma_{i,j,s,t}]_p$; where $\sigma_{i,j,s,t} = \alpha_{i,j} \cdot \gamma_{s,t}$ denotes the traditional multiplication of two matrices. Therefore, we have the inverse matrix $[J]_p^{-1}$ that can be calculated directly from the block inverse of the original block matrix $[J]_p$, i.e.,
\[
[J]_p^{-1} = ([A]_p \otimes [B]_p)^{-1} = ([A]_p^{-1} \otimes [B]_p^{-1}) = \frac{1}{p^2} [\alpha^{-1}_{i,j} \cdot \gamma^{-1}_{s,t}]_p,
\]
(15)
It implies that $[J]_p$ is a block Jacket matrix.

Next, we show that matrix $[J]_p$ 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 $Z_p$, respectively
\[
\begin{align*}
\alpha_{ij} \prec \alpha_{ij} \prec \cdots \prec \alpha_{ij}, & \quad \text{for} \ a_{ij} \in Z_p, \ \forall j \in Z_p; \\
\beta_{kj} \prec \beta_{kj} \prec \cdots \prec \beta_{kj}, & \quad \text{for} \ b_{kj} \in Z_p, \ \forall k \in Z_p;
\end{align*}
\]
(16)
where $s \in \{r, c\}$, $a_{ij}$ and $b_{kj}$ denote the $j^{th}$ row and the $j^{th}$ column index of block matrix $[A]_p$, $b_{kj}$ and $b_{kj}$ denote the $k^{th}$ row and the $k^{th}$ column index of block matrix $[B]_p$, and $\prec$ denotes the increasing order. Then for the $p^2$-order block matrix $[J]_p$ over $Z_p$, the row and column index order can be defined as follows.
\[ a_y b_x < a_z b_w, \text{ if } \begin{cases} a_y < a_w; \\ a_y = a_w, b_x < b_w. \end{cases} \] (17)

Also the entries of \([J]_{p^r}\) are defined on the basis of \([J]_p\) as \(\phi_{p^r}(a_y b_w, a_z b_w) = \phi_p(a_w, a_z) \cdot \phi_p(b_w, b_w)\). As for the entries \(\phi_p(a_i, a_i)\) and \(\phi_p(b_h, b_h)\) of \([A]_p\) and \([B]_p\), \forall a_i, a_i, a_i \in Z_p\) and \forall b_h, b_h, b_h \in Z_p, we have

\[
\phi_p(a_i, a_i) \phi_p(a_i, a_i) = \phi_p(a_i, a_i) \cdot \phi_p(a_i, a_i),
\]
(18)

\[
\phi_p(b_h, b_h) \phi_p(b_h, b_h) = \phi_p(b_h, b_h) \cdot \phi_p(b_h, b_h),
\]
(19)

Therefore, it can be easily verified that

\[
\phi_{p^r}(a_i b_h, a_i b_h) \phi_{p^r}(a_i b_h, a_i b_h) = \phi_{p^r}(a_i b_h, a_i b_h) \cdot \phi_{p^r}(a_i b_h, a_i b_h).
\]
(20)

It shows that block matrix \([J]_{p^r}\) is also a CBIJM under the indexed order in (17). This completes the proof of this theorem.

**Corollary I**: For any prime number \(p\) and non-negative integer number \(s\), let \([J]_{p^s} = [J]_p \otimes \cdots \otimes [J]_p\) be an \(s\)-fold block matrix, i.e., \([J]_{p^s} = \prod_{i=1}^{s} [J]_p\). Then the block matrix \([J]_{p^s}\) is a CBIJM of order \(p^s\).

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

\[
[J]_{p^s} = [J]_{p^{s-1}} \otimes [J]_p = \prod_{i=1}^{s} ([I]_{p^{s-i}} \otimes [J]_p \otimes [I]_{p^{i-1}})
\]
(21)

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 II**: 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

\[
[J]_{p^s} = \prod_{i=1}^{s} ([I]_{p^{s-i}} \otimes [J]_p \otimes [I]_{p^{i-1}}),
\]
(22)

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

**Proof**: 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 \(\forall i \in \{1, 2, \cdots, s\}\) we have

\[
[J]_{p^i} = \prod_{i=1}^{i} ([I]_{p^{s-i}} \otimes [J]_p \otimes [I]_{p^{i-1}}).
\]
(23)

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

\[
[J]_{p^{s+1}} = [J]_p \otimes [J]_{p^s} = ([J]_p \otimes [I]_p) \otimes ([I]_{p^s} \otimes [J]_p) = ([J]_p \otimes [I]_p) ([I]_{p^s} \otimes [J]_p) = \prod_{i=1}^{s+1} ([I]_{p^{s-i}} \otimes [J]_p \otimes [I]_{p^{i-1}})
\]
(24)

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 1. 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.
Conclusion

A simple method of developing the CBIJM is proposed. 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.

Table 1 Decomposition of Order for the CBJM $[J]_p$.

<table>
<thead>
<tr>
<th>Order</th>
<th>Decomposition</th>
<th>CBIJM</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$2 \times 2$</td>
<td>$[J]_2 = [J]_1$</td>
</tr>
<tr>
<td>3</td>
<td>$3 = 3$</td>
<td>$[J]_3 = [J]_3$</td>
</tr>
<tr>
<td>4</td>
<td>$2^2 = 2 \times 2$</td>
<td>$[J]_4 = [J]_5^{2 \times 2}$</td>
</tr>
<tr>
<td>5</td>
<td>$5 = 5$</td>
<td>$[J]_5 = [J]_5$</td>
</tr>
<tr>
<td>7</td>
<td>$7 = 7$</td>
<td>$[J]_7 = [J]_7$</td>
</tr>
<tr>
<td>8</td>
<td>$2^3 = 2 \times 2 \times 2$</td>
<td>$[J]_8 = [J]_6^{2 \times 2}$</td>
</tr>
<tr>
<td>9</td>
<td>$3^2 = 3 \times 3$</td>
<td>$[J]_9 = [J]_5^{2 \times 3}$</td>
</tr>
</tbody>
</table>

Acknowledgement

This work was supported by Research Plan Projects of Science-Technology Department of Hunan Province, also was supported in part by the construct program of the key discipline in Hunan province.

References


