A novel r-circulant block Jacket transform with fast algorithms

Guibo LIU[1, a], Qi LI[1, b], Dayong LUO[1, c], Ying GUO[1, d], Moonho LEE[2, e]

[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, South Korea

[a]email: lgbtrs2006@126.com, [b]email: 931354573@qq.com,
[c]email: yingguo@csu.edu.cn, [d]email: ldycsu@163.com,
[e]email: moonho@jbnu.ac.kr

Keywords: Hadamard transform; Jacket transform; Kronecker product; construction and decomposition; fast algorithm

Abstract. Jacket transform inspired by the well-known Hadamard transform, has been attracting more and more attentions due to its orthogonality, simpleness of its inversion and fast algorithms. It has also been applied to signal processing, image compression, mobile communication, quantum coding, and so on. In this paper, we firstly propose the r-circulant block Jacket transform (r-CBJT) to extend the Jacket transform family, and then we suggest an approach for the elegant construction of the r-circulant block Jacket matrices (r-CBJMs) with any size by using the structure of the permutation matrices. After that, the fast construction and decomposition algorithms for the r-CBJMs can be designed with the Kronecker product of corresponding identity matrices and relative lower order Jacket matrices in a successively iterative form. It has a less computation complexity compared to direct calculation approach, which is vitally important and practical to some real-time applications, such as high-speed mobile wireless communication, instant audio and video transmission, fast encoding and decoding, and so on.

1. Introduction

Jacket transform motivated by the center weighted Hadamard transform [1] [2], is an orthogonal transform with lots of advantages that are very useful in the practical applications involving matrix transform. Also, its corresponding inverse can be derived just by calculating its element-wise or block inverse. Mathematically, given a nonsingular jacket matrix $J_n = (j_{kt})_{n\times n}$, then the (k,t) entry of its inverse matrix is equal to the product of $1/n$ and the inverse of the element in the (t,k) position. In other words,

$$J_n^{-1} = (j_{kt})_{n\times n}^{-1} = \frac{1}{n} J_n^{RT} = \frac{1}{n}(\frac{1}{j_{tk}})_{n\times n} \tag{1}$$

where ‘R’ and ‘T’ denote reciprocal and transpose operations respectively. Jacket transform and its corresponding matrices have been extensively investigated. From the aspect of the matrix transform theory [3], Jacket transforms, such as co-cyclic Jacket transform [4], block Jacket transform [5], center weighted block Jacket transform [6], blind-block parametric Jacket transform [7], Jacket harr transform [8], have been presented and investigated one after another, while from the aspect of the practical applications, there exist literatures relevant with signal processing [9], image compression [10], quantum information system for quantum coding [11], wireless mobile communications for pre-coding, coding and decoding [12] [13] [14], new emerging 3G and 4G MIMO communication [15], encryption and decryption [16], and so on.

Furthermore, lots of widely used transforms, such as WHT [2], DFT [17], DCT, HWT [8], slant transform all belong to the Jacket transform family. In other words, applications that have adopted the above-mentioned transforms can theoretically employ the corresponding Jacket transform. Meanwhile, Jacket matrices have close relation with well-known interesting matrices such as

unitary matrices, hermitian matrices, Hadamard matrices and so on, which are of vital importance in digital signal and image processing, orthogonal code design, cryptography, quantum information systems, mathematics and physics, etc.

Recently, there exist many papers surrounding block Jacket transform and corresponding applications. Fast block inverse Jacket transform was firstly introduced in [18], which proposed one-dimensional and two-dimensional fast algorithms for realizing the block inverse Jacket transform with size of $N = 2^k$ and 3^k. After that, center weighted block Jacket transforms were proposed for weighing the region of mid-spatial frequencies of the signal more than the Hadamard transform in [6], meanwhile, fast algorithms were also derived based on the sparse matrix factorization. Later, based on the well-known Pauli matrices, a generalized block Jacket transform was defined, and also fast algorithms for fast constructing and decomposing block Jacket matrices with any size were derived based on certain recursive relations [19]. Compared to the conventional block inverse Jacket transform, [5] proposed a block-wise inverse Jacket transform and also obtained one-dimensional and two-dimensional fast algorithms with lower complexity. Besides, there also exist associative practical applications, such as quantum coding [11], Arikan and Alamouti code design [9], LDPC [12], pre-coding for Multi-user MIMO broadcast channels [15], and so on.

While unfortunately, as far as we are concerned, just as the circulant matrices to the matrix family, the circulant and even generalized version of block Jacket transform is still absent. So this paper is to fucus on this topic. Contributions of this paper are list as follows, (1) The structure of the r-CBJMs is presented for the first time, meanwhile, based on this elegant structure, some special cases were discussed. (2) Method for constructing the r-CBJMs with any size are extensively studied and successfully derived. (3) Fast algorithms of the r-CBJMs' construction and factorization were found, which has a relatively lower computation complexity than direct computation algorithm and promises a prospect in the practical applications. (4) The proposed construction method and fast algorithms are also applicable to the other r-CBJMs with similar characteristics.

The remainder of this paper is outlined as follows. Section 2 mathematically proposes the structure of the r-CBJMs, and later, for clarity, some special cases are presented. After that, method for constructing r-CBJMs with any size is extensively investigated and ultimately obtained in Section 3. Section 4 further derives the algorithms for fast constructing and decomposing r-CBJMs. Fast algorithms of r-CBJMs with size 1 to 20 and the complexity analysis for both direct algorithm and fast algorithm are all illustrated in section 5. Section 6 makes a conclusion in the end.

2. The structure of r-CBJMs

After reviewing some concepts and notations, the structure of the r-CBJMs is subsequently presented. An $n \times n$ block matrix $[C]_{n=N/p}$, where $[\cdot]$ denotes block matrix and the subscript means the number of $p \times p$ sub-matrices or blocks in a single row or column throughout this paper, is called as a r-circulant block matrix if it has the following form,

$$[R]_{n=N/p} = \begin{pmatrix} R_p^0 & \cdots & R_p^{n-2} & R_p^{n-1} \\ rR_p^{n-1} & \cdots & R_p^{n-3} & R_p^{n-2} \\ \vdots & \ddots & \vdots & \vdots \\ rR_p^1 & \cdots & rR_p^{n-1} & R_p^0 \end{pmatrix}_{n \times n}, \tag{2}$$

where C_p^i, $i \in \{0,1,\cdots,n-1\}$ are $p \times p$ sub-matrices or blocks of complex or real-valued elements with serial number $i \in \{0,1,\cdots,n-1\}$ and r is a non-zero number. Supposing $p = 1$, the $n \times n$ r-circulant block matrix becomes an $n \times n$ r-circulant matrix.

Besides, for an $N \times N$ matrix J_N, its associative matrix $J_N{}^{RT}$ is formed from the matrix J_N by taking the reciprocal of each element of and exchanging its row and column indices. In other words, entry of the $J_N{}^{RT}$ matrix in the position (k,i) is equal to the reciprocal of the (i,k)

element of the original matrix.

Definition 2.1 An $N \times N$ matrix $J_N = (j_{i,k})_{N \times N}$, $i,k \in \{0,1,\cdots,n-1\}$, is called a Jacket matrix, if J_N is reversible and the (i,k) entry of its inverse matrix is equal to the product of $1/N$ and the inverse of the element in the (k,i) position of J_N.

Definition 2.2 An $n \times n$ r-circulant block matrix $[C]_{n=N/p} = (C_{jk})_{N \times N}$ with $p \times p$ Jacket blocks and $N = np$ is called a r-circulant block Jacket matrix if it is also a Jacket matrix. Especially, supposing $p = 1$, $[C]_{n=N/p}$ is just r-circulant Jacket matrix.

Example 2.1 For a given nonzero number r, the subsequent matrix $J_2 = \begin{pmatrix} \pm\sqrt{|r|}i & 1 \\ r & \pm\sqrt{|r|}i \end{pmatrix}$ is a r-circulant Jacket matrices because of the following constraint

$$J_2^{-1} = \frac{1}{2} J_2^{RT} = \frac{1}{2} \begin{pmatrix} \mp i(|r|)^{-1/2} & 1/r \\ 1 & \mp i(|r|)^{-1/2} \end{pmatrix}. \tag{3}$$

Example 2.2 Let ω be the complex third root of unity. The matrix below

$$J_3 = \begin{pmatrix} 1 & \pm\omega|r| & 1 \\ r & 1 & \pm\omega|r| \\ \pm\omega r|r| & r & 1 \end{pmatrix} \tag{4}$$

is also a r-circulant Jacket matrix, since the following constraint is satisfied,

$$J_3^{-1} = \frac{1}{3} J_3^{RT} = \frac{1}{3} \begin{pmatrix} 1 & 1/r & 1/(\pm\omega r|r|) \\ 1/(\pm\omega|r|) & 1 & 1/r \\ 1 & 1/(\pm\omega|r|) & 1 \end{pmatrix}. \tag{5}$$

The above-mentioned two r-circulant Jacket matrices are special cases of r-circulant block Jacket matrices when $p = 1$. if $r = 1$, the derived two r-circulant Jacket matrices become two circulant

Jacket matrices, simultaneously. While $r = -1$, the two matrices are anti-circulant Jacket matrices.

Subsequently, we further discuss the general form of 4 order r-circulant Jacket matrices. A r-circulant matrix J_4 may be generally denoted as

$$J_4 = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ ra_3 & a_0 & a_1 & a_2 \\ ra_2 & ra_3 & a_0 & a_1 \\ ra_1 & ra_2 & ra_3 & a_0 \end{pmatrix},$$

where $a_i, i \in \{0,1,2,3\}$ are all none zero numbers. Based on the characteristics of jacket matrix, the following equation exists,

$$\left(1 + \frac{ra_1a_3}{a_0^2}\right)\left(1 + \frac{a_0a_1}{a_1^2}\right)\left(1 + \frac{a_0a_1}{ra_2a_3}\right) = 0. \tag{6}$$

According to Eq.(6), there exist three cases. Case 1, if $\left(1 + \frac{ra_1a_3}{a_0^2}\right) = 0$, J_4 can be denoted as,

$$J_4 = \begin{pmatrix} a_0 & \pm a_0 r^{-\frac{1}{4}} & a_0 r^{-\frac{1}{2}} & \mp a_0 r^{-\frac{3}{4}} \\ \mp a_0 r^{\frac{1}{4}} & a_0 & \pm a_0 r^{-\frac{1}{4}} & a_0 r^{-\frac{1}{2}} \\ a_0 r^{\frac{1}{2}} & \mp a_0 r^{\frac{1}{4}} & a_0 & \pm a_0 r^{-\frac{1}{4}} \\ \pm a_0 r^{\frac{3}{4}} & a_0 r^{\frac{1}{2}} & \mp a_0 r^{\frac{1}{4}} & a_0 \end{pmatrix} or \begin{pmatrix} a_0 & \pm i a_0 r^{-\frac{1}{4}} & -a_0 r^{-\frac{1}{2}} & \pm i a_0 r^{-\frac{3}{4}} \\ \pm i a_0 r^{\frac{1}{4}} & a_0 & \pm i a_0 r^{-\frac{1}{4}} & -a_0 r^{-\frac{1}{2}} \\ -a_0 r^{\frac{1}{2}} & \pm i a_0 r^{\frac{1}{4}} & a_0 & \pm i a_0 r^{-\frac{1}{4}} \\ \pm i a_0 r^{\frac{3}{4}} & -a_0 r^{\frac{1}{2}} & \pm i a_0 r^{\frac{1}{4}} & a_0 \end{pmatrix}. \tag{7}$$

Case 2, if $\left(1+\frac{a_0a_1}{a_1^2}\right)=0$, J_4 can be calculated as,

$$J_4=\begin{pmatrix} a_0 & \pm ia_0r^{-\frac{1}{4}} & a_0r^{-\frac{1}{2}} & \mp ia_0r^{-\frac{3}{4}} \\ \mp ia_0r^{\frac{1}{4}} & a_0 & \pm ia_0r^{-\frac{1}{4}} & a_0r^{-\frac{1}{2}} \\ a_0r^{\frac{1}{2}} & \mp ia_0r^{\frac{1}{4}} & a_0 & \pm ia_0r^{-\frac{1}{4}} \\ \pm ia_0r^{\frac{3}{4}} & a_0r^{\frac{1}{2}} & \mp ia_0r^{\frac{1}{4}} & a_0 \end{pmatrix} or \begin{pmatrix} a_0 & \pm ia_0r^{-\frac{1}{4}} & -a_0r^{-\frac{1}{2}} & \pm ia_0r^{-\frac{3}{4}} \\ \pm ia_0r^{\frac{1}{4}} & a_0 & \pm ia_0r^{-\frac{1}{4}} & -a_0r^{-\frac{1}{2}} \\ -a_0r^{\frac{1}{2}} & \pm ia_0r^{\frac{1}{4}} & a_0 & \pm ia_0r^{-\frac{1}{4}} \\ \pm ia_0r^{\frac{3}{4}} & -a_0r^{\frac{1}{2}} & \pm ia_0r^{\frac{1}{4}} & a_0 \end{pmatrix}. \tag{8}$$

Case 3, if $\left(1+\frac{a_0a_1}{ra_2a_3}\right)=0$, J_4 can be changed to,

$$J_4=\begin{pmatrix} a_0 & a_1 & \pm a_0r^{-\frac{1}{2}} & \mp a_1r^{-\frac{1}{2}} \\ \mp a_1r^{\frac{1}{2}} & a_0 & a_1 & \pm a_0r^{-\frac{1}{2}} \\ \pm a_0r^{\frac{1}{2}} & \mp a_1r^{\frac{1}{2}} & a_0 & a_1 \\ ra_1 & \pm a_0r^{\frac{1}{2}} & \mp a_1r^{\frac{1}{2}} & a_0 \end{pmatrix}. \tag{9}$$

From the above three cases, J_4 conforms to the following form,

$$J_4=\begin{pmatrix} a_0 & a_1 & r^{-\frac{1}{2}}a_0 & -r^{-\frac{1}{2}}a_1 \\ -r^{\frac{1}{2}}a_1 & a_0 & a_1 & r^{-\frac{1}{2}}a_0 \\ r^{\frac{1}{2}}a_0 & -r^{\frac{1}{2}}a_1 & a_0 & a_1 \\ ra_1 & r^{\frac{1}{2}}a_0 & -r^{\frac{1}{2}}a_1 & a_0 \end{pmatrix} or \begin{pmatrix} a_0 & a_1 & -r^{-\frac{1}{2}}a_0 & r^{-\frac{1}{2}}a_1 \\ r^{\frac{1}{2}}a_1 & a_0 & a_1 & -r^{-\frac{1}{2}}a_0 \\ -r^{\frac{1}{2}}a_0 & r^{\frac{1}{2}}a_1 & a_0 & a_1 \\ ra_1 & -r^{\frac{1}{2}}a_0 & r^{\frac{1}{2}}a_1 & a_0 \end{pmatrix}. \tag{10}$$

This section has been presented the structure of r-CBJMs, meanwhile, some special cases are also illustrated for clarity. In the following section, we will discuss the method for constructing r-CBJMs with any size.

3. Construction method for the r-CBJMs

Before studying the general method for forming the r-CBJMs with any size, let's firstly discuss the constructing method for r-CBJMs with the lowest size.

3.1. Method for constructing the r-CBJMs with size 2

Theorem 3.1 Let a r-circulant block matrix with size 2 be $[R]_2=\begin{pmatrix} R_p^0 & R_p^1 \\ rR_p^1 & R_p^0 \end{pmatrix}$, where $R_p^i, i\in\{0,1\}$ are both Jacket matrices, then $[R]_2$ is a Jacket matrix if and only if the subsequent condition is satisfied,

$$R_p^0(R_p^1)^{RT}+rR_p^1(R_p^0)^{RT}=0. \tag{11}$$

Proof Since $R_p^i, i\in\{0,1\}$ are both Jacket matrices, there exists $R_p^i(R_p^i)^{RT}=pI_p, i\in\{0,1\}$. Also there exists,

$$\begin{aligned}[R]_2[R]_2^{RT}&=\begin{pmatrix} R_p^0 & R_p^1 \\ rR_p^1 & R_p^0 \end{pmatrix}\begin{pmatrix} R_p^0 & R_p^1 \\ rR_p^1 & R_p^0 \end{pmatrix}^{RT}=\begin{pmatrix} R_p^0(R_p^0)^{RT}+R_p^1(R_p^1)^{RT} & R_p^0(rR_p^1)^{RT}+R_p^1(R_p^0)^{RT} \\ rR_p^1(R_p^0)^{RT}+R_p^0(R_p^1)^{RT} & rR_p^1(R_p^1)^{RT}+R_p^0(R_p^0)^{RT} \end{pmatrix} \\ &=\begin{pmatrix} 2pI_p & \frac{1}{r}R_p^0(R_p^1)^{RT}+R_p^1(R_p^0)^{RT} \\ rR_p^1(R_p^0)^{RT}+R_p^0(R_p^1)^{RT} & 2pI_p \end{pmatrix}.\end{aligned} \tag{12}$$

So $[R]_2$ is a Jacket matrix, if and only if $rR_p^1(R_p^0)^{RT}+R_p^0(R_p^1)^{RT}=0$ exists.

Example 3.1.1 Supposing $r=16$, $R_p^0=\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $R_p^1=\begin{pmatrix} \frac{1}{4} & -\frac{1}{4} \\ -\frac{1}{4} & -\frac{1}{4} \end{pmatrix}$. It is simple to check

that Eq.(11) holds, then $[R]_2 = \begin{pmatrix} R_p^0 & R_p^1 \\ rR_p^1 & R_p^0 \end{pmatrix}$ is a r-CBJM with size 2

3.2. Method for constructing the r-CBJMs with size 3

Theorem 3.2 Let a r-circulant block matrix with size 3 be $[R]_3 = \begin{pmatrix} R_p^0 & R_p^1 & R_p^2 \\ rR_p^2 & R_p^0 & R_p^1 \\ rR_p^1 & rR_p^2 & R_p^0 \end{pmatrix}$, where $R_p^i,\ i \in \{0,1,2\}$ are both jacket matrices, then $[R]_3$ is a Jacket matrix if and only if the subsequent conditions are both satisfied,

$$R_p^0 (R_p^2)^{RT} + rR_p^1 (R_p^0)^{RT} + rR_p^2 (R_p^1)^{RT} = 0 \tag{13}$$

$$R_p^0 (R_p^1)^{RT} + R_p^1 (R_p^2)^{RT} + rR_p^2 (R_p^0)^{RT} = 0. \tag{14}$$

Proof Let elementary matrix with size 3 be $\Pi_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ r & 0 & 0 \end{pmatrix}$, then the new proposed matrix and its associative matrix can be respectively written as, $[R]_3 = I_3 \otimes R_p^0 + \Pi_3 \otimes R_p^1 + {\Pi_3}^2 \otimes R_p^2$ and $[R]_3{}^{RT} = I_3 \otimes (R_p^0)^{RT} + \frac{1}{r}{\Pi_3}^2 \otimes (R_p^1)^{RT} + \frac{1}{r}\Pi_3 \otimes (R_p^2)^{RT}$. Then, $[R]_3[R]_3{}^{RT}$ can be further calculated as,

$$\begin{aligned} [R]_3[R]_3{}^{RT} &= \left(I_3 \otimes R_p^0 + \Pi_3 \otimes R_p^1 + {\Pi_3}^2 \otimes R_p^2\right) \times \left\{I_3 \otimes (R_p^0)^{RT} + \frac{1}{r}{\Pi_3}^2 \otimes (R_p^1)^{RT} + \frac{1}{r}\Pi_3 \otimes (R_p^2)^{RT}\right\} \\ &= I_3 \otimes 3pI_p + \Pi_3 \otimes \left\{\frac{1}{r}R_p^0 (R_p^2)^{RT} + R_p^1 (R_p^0)^{RT} + R_p^2 (R_p^1)^{RT}\right\} \\ &\quad + {\Pi_3}^2 \otimes \left\{\frac{1}{r}R_p^0 (R_p^1)^{RT} + \frac{1}{r}R_p^1 (R_p^2)^{RT} + R_p^2 (R_p^0)^{RT}\right\}. \end{aligned} \tag{15}$$

Therefore, $[R]_3[R]_3{}^{RT} = I_3 \otimes 3pI_p$ holds if and only if $R_p^0 (R_p^2)^{RT} + rR_p^1 (R_p^0)^{RT} + rR_p^2 (R_p^1)^{RT} = 0$ and $R_p^0 (R_p^1)^{RT} + R_p^1 (R_p^2)^{RT} + rR_p^2 (R_p^0)^{RT} = 0$ are both satisfied. So theorem 3.2 is tenable.

Example 3.2.1 Suppose $r = -i$, $R_2^0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $R_2^1 = \frac{\sqrt{3}+i}{2}R_2^0$ and $R_2^2 = \frac{1-\sqrt{3}i}{2}R_2^0$, so we can check that Eq.(13) and Eq.(14) hold. Then $[R]_3 = \begin{pmatrix} R_2^0 & R_2^1 & R_2^2 \\ rR_2^2 & R_2^0 & R_2^1 \\ rR_2^1 & rR_2^2 & R_2^0 \end{pmatrix}$ is a r-CBJM with size 3.

3.3. Method for constructing the r-CBJMs with any size

Theorem 3.3 Let a r-circulant block matrix with size n be as follows,

$$[R]_{n=N/p} = \begin{pmatrix} R_p^0 & \cdots & R_p^{n-2} & R_p^{n-1} \\ rR_p^{n-1} & \cdots & R_p^{n-3} & R_p^{n-2} \\ \vdots & \ddots & \vdots & \vdots \\ rR_p^1 & \cdots & rR_p^{n-1} & R_p^0 \end{pmatrix}_{n \times n}, \tag{16}$$

where $R_p^i,\ i \in \{0,1,\cdots,n-1\}$ are all jacket matrices, then $[R]_n$ is a Jacket matrix if and only if the subsequent condition is satisfied,

$$\sum_{j=0}^{n-1} \left\{ \left(r^{floor\left\lfloor \frac{n+j-i}{n} \right\rfloor} \right) R_p^j \left(R_p^{(n+j-i) \bmod n} \right)^{RT} \right\} = 0,\ i \in \{1,2,\cdots,n-1\}. \tag{17}$$

Proof Let an $n\times n$ elementary matrix be $\Pi=\begin{pmatrix}0&1&\cdots&0\\ \vdots&\vdots&\ddots&\vdots\\ 0&0&\cdots&1\\ r&0&\cdots&0\end{pmatrix}$, then $\Pi^0=I_n$ and $\Pi^n=rI_n$.

$[R]_n$ and $[R]_n^{RT}$ can be respectively denoted as

$$[R]_n=\sum_{i=0}^{n-1}(\Pi^i\otimes R_p^i),\ [R]_n^{RT}=\tfrac{1}{r}\sum_{j=0}^{n-1}\left(\Pi^{n-j}\otimes(R_p^j)^{RT}\right).$$

So $[R]_n[R]_n^{RT}$ can be further transformed as,

$$\begin{aligned}[R]_n[R]_n^{RT}&=\left(\sum_{i=0}^{n-1}\Pi^i\otimes R_p^i\right)\times\left(\frac{1}{r}\sum_{j=0}^{n-1}\Pi^{(n-j)}\otimes(R_p^j)^{RT}\right)\\&=I_n\otimes npI_p+\Pi\otimes\left\{\frac{1}{r}R_p^0(R_p^{(n-1)})^{RT}+\sum_{j=1}^{n-1}(R_p^j)(R_p^{(j-1)})^{RT}\right\}+,\cdots,+\Pi^i\otimes\left\{\frac{1}{r}\sum_{j=0}^{i-1}R_p^j(R_p^{(n-i+j)})^{RT}+\sum_{j=i}^{n-1}(R_p^j)(R_p^{(j-i)})^{RT}\right\}.\quad(18)\\&\quad+,\cdots,+\Pi^{n-1}\otimes\left\{\frac{1}{r}\sum_{j=0}^{n-2}(R_p^j)(R_p^{n-i+j})^{RT}+R_p^{n-1}(R_p^0)^{RT}\right\}\end{aligned}$$

Therefore, $[R]_n[R]_n^{RT}=I_n\otimes npI_p$ if and only if

$$\sum_{j=0}^{n-1}\left\{\left(r^{floor\left\lfloor\frac{n+j-i}{n}\right\rfloor}\right)R_p^j\left(R_p^{(n+j-i)\bmod n}\right)^{RT}\right\}=0,i\in\{1,\cdots,n-1\}.$$

Example 3.3.1 Supposing $r=-1$, $p=2$, $C_2^0=\begin{pmatrix}a&b\\a&-b\end{pmatrix},C_2^i=C_2^1=\begin{pmatrix}a&a\\-b&b\end{pmatrix},i\in\{2,3,\cdots,n-1\}$ and $a=\left((n-2)\pm\left(n^2-4n+5\right)^{1/2}\right)b,ab\neq0$, so we can check $[C]_n=\begin{pmatrix}C_2^0&C_2^1&\cdots&C_2^1\\ \vdots&\vdots&\ddots&\vdots\\ -C_2^1&-C_2^1&\cdots&C_2^1\\ -C_2^1&-C_2^1&\cdots&C_2^0\end{pmatrix}$ is a r-CBJM with size n.

4. Fast algorithms

Based on the above section, r-CBJMs with any size can be successfully constructed. While there is another problem whether there exist fast algorithms for more efficiently constructing and factorizing r-CBJMs. The following section will focus on the subject, which is of vitally theoretic and practical importance concerning with relatively larger size matrix transform.

4.1. Fast construction algorithms

Theorem 4.1 A r-CBJM with size $[R]_{n=q^kp^j}$, where p and q are co-prime numbers, can be efficiently constructed in the following way,

$$[R]_{n=q^kp^j}=\left\{[I]_{q^k}\otimes\left(\prod_{i=1}^{j}[I]_{p^{j-i}}\otimes[R]_p\otimes[I]_{i-1}\right)\right\}\left\{\left(\prod_{i=1}^{k}[I]_{p^{k-i}}\otimes[R]_p\otimes[I]_{i-1}\right)\otimes[I]_{p^j}\right\},\quad(19)$$

where lower order r-CBJMs $[R]_p$ and $[R]_q$ can be obtained from the above sections.

Proof There are two steps to prove the above theorem. Firstly, by using inductive method to derive the following equation,

$$[R]_{n=q^k}=\prod_{i=1}^{k}[I]_{q^{k-i}}\otimes[R]_q\otimes[I]_{q^{i-1}}.\quad(20)$$

If $k=1$, $[R]_{n=q^k}$ can be transformed as $[R]_{n=q^1}=\prod_{i=1}^{1}[I]_{q^0}\otimes[R]_q\otimes[I]_{q^0}=[R]_q$. Next, if $k=L$, $[R]_{n=q^L}=\prod_{i=1}^{L}[I]_{q^{L-i}}\otimes[R]_q\otimes[I]_{q^{i-1}}$ can be obtained. Subsequently, when $k=L+1$, Eq.(20) can be written as,

$$\begin{aligned}[R]_{n=q^{L+1}}&=\left([I]_q\otimes[R]_{q^L}\right)\left([R]_q\otimes[I]_{q^L}\right)\\&=\left\{[I]_q\otimes\left(\prod_{i=1}^{L}[I]_{q^{L-i}}\otimes[R]_q\otimes[I]_{q^{i-1}}\right)\right\}\times\left([R]_q\otimes[I]_{q^L}\right).\\&=\prod_{i=1}^{L+1}[I]_{q^{L+1-i}}\otimes[R]_q\otimes[I]_{q^{i-1}}\end{aligned}\tag{21}$$

So, Eq.(20) is proved. Similarly, $[R]_{n=p^j}=\prod_{i=1}^{j}[I]_{p^{j-i}}\otimes[R]_p\otimes[I]_{p^{i-1}}$ exists. Secondly, $[R]_{n=q^kp^j}$ can be obtained by,

$$\begin{aligned}[R]_{n=q^kp^j}&=\left([I]_{q^k}\otimes[R]_{p^j}\right)\times\left([R]_{q^k}\otimes[I]_{p^j}\right)\\&=\left\{[I]_{q^k}\otimes\left(\prod_{i=1}^{j}[I]_{p^{j-i}}\otimes[R]_p\otimes[I]_{p^{i-1}}\right)\right\}\times\left\{\left(\prod_{i=1}^{k}[I]_{q^{k-i}}\otimes[R]_q\otimes[I]_{q^{i-1}}\right)\otimes[I]_{p^j}\right\}.\end{aligned}\tag{22}$$

So theorem 4.1 is proved. This theorem suggests a fast algorithm for construction of r-CBJMs. When $j=0$ or $k=0$, r-CBJMs with size $n=2^m$, $n=3^m$, $n=5^m$ and so on, can be efficiently constructed, meanwhile $[R]_{6^m}=[R]_{2^m3^m}$ can also be fast constructed based on the relatively lower order Jacket matrices $[R]_2$ and $[R]_3$ using $[R]_6=([R]_2\otimes[I]_3)\times([R]_3\otimes[I]_2)$ with $k=j=m$, $q=2$ and $p=3$.

4.2. Fast decomposition algorithms

The above section surrounded the algorithm for fast constructing r-CBJMs, while in this section, attention will be paid to how to efficiently decompose r-CBJMs, which is also of the same theoretical and practical importance to the corresponding matrix transform.

Theorem 4.2 Supposing a r-CBJM $[R]_{n=q^jp^k}$, if $[R]_n$ is factorable until $[R]_q$ and $[R]_p$. Then $[R]_n$ can be decomposed according to Eq.(19).

Proof If $[R]_n$ is factorable until $[R]_q$ and $[R]_p$, the decomposition algorithm is feasible. This procedure is a reverse one of its construction. Thus, the proof is obvious. For example, supposing a r-CBJM $[R]_{15}$, then its corresponding decomposition signal flow graph is shown as in Figure 1 with $[R]_{n=3\times4}=([I]_2\otimes[R]_3\otimes[I]_2)([I]_2\otimes[R]_2\otimes[I]_3)([I]_3\otimes[R]_2\otimes[I]_2)$. Meanwhile, in practice such as signal processing, the employed matrices with large size are always factorable. For some special cases, in which $[R]_n$ is not factorable, one should use other special way to process.

5. Complexity analysis of r-CBJMs

In the section 4, fast algorithms of r-CBJMs with any size have been obtained in an elegant form. This section gives a comparison between the direct computation algorithm and the fast algorithms.

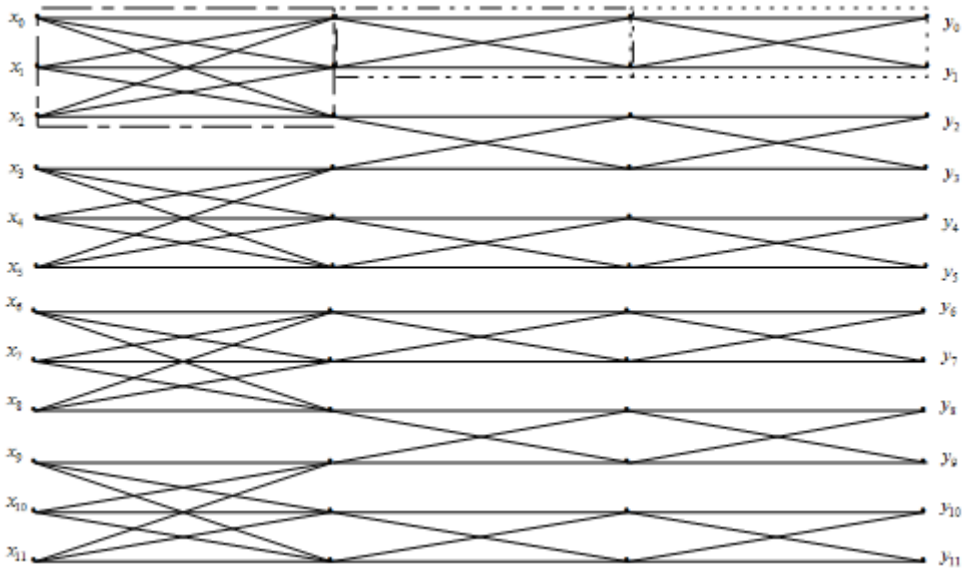

Fig.1. Signal flow graph for fast decomposing r-CBJM with size 12

Before making a research on the complexity analysis of fast algorithms, Table I lists construction and decomposition approaches for r-CBJMs $[R]_i,\ i \in \{1,2,\cdots,20\}$. The second column of the table denotes the prime factor decomposition methods for these numbers while the fast algorithms are shown in the third column. Compared to direct computation algorithms, fast algorithms require less number of mathematical operations. Table II illustrates the differences between them in details, where $N = \prod_{i=1}^{n} p_i^{k_i}$ denotes the prime factor factorization of the matrix size and $p_i, k_i, i \in \{1,2,...,n\}$ denote corresponding prime factors and its power order. From the table, we can check that when $N = 27$, direct computation algorithms needs 702 additions and 729 multiplications, respectively, but by using fast algorithm, the numbers of additions and multiplications can be reduced to 162 and 108, respectively. Thus, compared to the direct computation, the proposed fast algorithms have less computation complexity, and are especially more suitable for some applications with high request for real-time performance.

Table I Prime factor decompositions of numbers and corresponding r-CBJMs

SN	Numbers	r-CBJMs
1	$1=1$	$[R]_1 = [R]_1$
2	$2 = 2$	$[R]_2 = [R]_2$
3	$3=3$	$[R]_3 = [R]_3$
4	$4 = 2^2$	$[R]_4 = [R]_2^{\otimes 2}$
5	$5=5$	$[R]_5 = [R]_5$
6	$6 = 2\times 3$	$[R]_6 = [R]_2 \otimes [R]_3$
7	$7=7$	$[R]_7 = [R]_7$
8	$8 = 2^3$	$[R]_8 = [R]_2^{\otimes 3}$
9	$9 = 3^2$	$[R]_9 = [R]_3^{\otimes 2}$
10	$10 = 2\times 5$	$[R]_{10} = [R]_2 \otimes [R]_5$
11	$11 = 11$	$[R]_{11} = [R]_{11}$
12	$12 = 2^2\times 3$	$[R]_{12} = [R]_2^{\otimes 2} \otimes [R]_3$
13	$13 = 13$	$[R]_{13} = [R]_{13}$
14	$14 = 2\times 7$	$[R]_{14} = [R]_2 \otimes [R]_7$

15	$15 = 3 \times 5$	$[R]_{15} = [R]_3 \otimes [R]_5$
16	$16 = 2^4$	$[R]_{16} = [R]_2^{\otimes 4}$
17	$17 = 17$	$[R]_{17} = [R]_{17}$
18	$18 = 2 \times 3^2$	$[R]_{18} = [R]_3^{\otimes 2} \otimes [R]_2$
19	19 = 19	$[\mathrm{R}]_{19} = [R]_{19}$
20	$20 = 2^2 \times 5$	$[R]_{20} = [R]_2^{\otimes 2} \otimes [R]_5$

Table II Complexity analysis of FR-CBJT. (DCA and FR-CBJT denote direct computation algorithm and fast algorithms of r-CBJT, respectively.)

N	OP	DCA	FR-CBJT
$N = p^k$	ADD	$(N-1)N$	$kp^k(p-1)$
	MUL	N^2	$kp^{k-1}(p-1)^2$
$N = \prod_{i=1}^{n} p_i^{k_i}$	ADD	$(N-1)N$	$\sum_{i=1}^{n} k_i p_i^{k_i}(p_i - 1)$
	MUL	N^2	$\sum_{i=1}^{n} \left\{ \frac{k_i}{p_i} p_i^{k_i} (p_i - 1)^2 \right\}$

6. Conclusion

In this paper, we firstly proposed a generalized circulant block Jacket transform named by r-CBJT, and then investigated its elegant structures. After that, we further explored existence condition for the r-CBJTs' matrices with any size, which suggests a construction method for the r-CBJTs. Subsequently, algorithms for fast constructing and decomposing r-CBJMs were successfully derived based on the Kronecker product of the permutation matrices and corresponding lower order block Jacket matrices with a successively recursive forms. Compared to direct computation algorithms, the proposed fast algorithms possess a lower computation complexity. The further study will surround other fast algorithms of r-CBJTs, parametric or factional Jacket transforms or certain an actual application of Jacket transform.

Acknowledgement

In this paper, the research was sponsored by the National Natural Science Foundation of China (61379153, 61272495), the New Century Excellent Talents in University, China (NCET-11-0510), and partly by the World Class University (R32-2010-000-20014-0), and Fundamental Research (2010-0020942, 2012-002521) NRF, Korea.

References

[1] Sundar Rajan B, Lee M H and Park J Y. A generalized reverse jacket transform [J]. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 2001, 48(7):684-690.

[2] Lee M H. The center weighted Hadamard transform [J]. Circuits and Systems, IEEE Transactions on, 1989, 36(9):1247-1249.

[3] Hom R A and Johnson C R. Topics in matrix analysis. Cambridge Univ. Press, Cambridge, U. K., 1991.

[4] Chen Z, Lee M H, Song W, et al. Fast co-cyclic Jacket transform based on DFT [J].

Communications, 2008. ICC ’08. IEEE International Conference on, 2008:458-462.
[5] Zeng G H and Lee M H. A generalized reverse block Jacket transform [J]. Accepted IEEE Trans. Circuits Syst.-I, 2008, 55(6):1589-1600.
[6] Lee M H and Zhang X D. Fast block center weighted Hadamard transform [J]. IEEE Trans. Circuits and Systems-I: Regular Papers, 2007, 54:2741-2745.
[7] Bouguezel S, Ahmad M O and Swamy M N S. A new blind block reciprocal parametric transform [J]. Circuits and Systems, 2008. ISCAS 2008. IEEE International Symposium on, 2008:3102-3105.
[8] Ding J, Pei S and Wu P. Jacket haar transform [J]. Circuits and Systems (ISCAS), 2011 IEEE International Symposium on, 2011, 19(5):1520-1523.
[9] Lee M H, Khan H M A and Kim K J. Arikan and alamouti matrices based on fast block-wise inverse Jacket transform [J]. EURASIP J. Adv. Sig. Proc. 2013, 37:247-124.
[10] Lee M H, Khan M H A, Kim K J, et al. A fast hybrid Jacket-hadamard matrix based diagonal block-wise transform [J]. Sig. Proc.: Image Comm., 2014, 29:49-65.
[11] Shi R, Guo Y and Lee M H. Quantum codes based on fast Pauli block transforms in the finite field [J]. Quantum Information Processing, 2010, 9(5):611-628.
[12] Jiang X Q and Lee M H. A new class of non-binary LDPC codes design based on inverse block Jacket matrices [J]. Wireless, Mobile and Sensor Networks, 2007, 07:954-957.
[13] Song W, Lee M H, Matalgah M M, et al. Quasi-orthogonal space-time block codes designs based on Jacket transform [J]. Journal of Communications and Networks, 2010, 12:240-245.
[14] Jiang X Q, Lee M H, Guo Y, et al. Ternary codes from modified Jacket matrices [J], Journal of Communications and Networks, 2011, 13:12-16.
[15] Khan M H, Cho K M, Lee M H, et al. A simple block diagonal precoding for multi-user MIMO broadcast channels [J]. EURASIP Journal on Wireless Communications and Networking, 2014, 2014(1): 95.
[16] Ma W P. The Jacket Matrix and Cryptography [D]. Chonbuk National University, Chonju, Korea, 2004.
[17] Guo Y, Mao Y, Park D S, et al. Fast DFT matrices transform based on generalized prime factor algorithm [J]. Journal of Communications and Networks, 2011, 13:449-455.
[18] Lee M H and Hou J. Fast block inverse Jacket transform [J]. IEEE Signal Process. Lett., 2006, 13:461-464.
[19] Mao Y, Guo Y and Lee M H. Fast co-cyclic block-wise inverse Jacket transform over the finite field [J]. IEEE Trans. Circuits and Systems, 2008, 55:1589-1599.