Fast circulant block Jacket transform based on the Pauli matrices

Guibo Liu*, Zhan Wang, Dayong Luo and Ying Guo

School of Information Science and Engineering, 
Central South University, 
Changsha 410083, China 
Email: lgbtrs2006@126.com 
Email: 13647498950@yeah.net 
Email: ldycsu@163.com 
Email: yingguo@csu.edu.cn 
*Corresponding author

Moon Ho Lee

Institute of Information and Communication, 
Chonbuk National University, 
Jeonju 561-756, South Korea 
Email: moonho@jbnu.ac.kr

Abstract: Owing to its orthogonality, simplicity of the inversion and fast algorithms, Jacket transform generalising from the Hadamard transform has played important roles in signal and image processing, mobile communication for coding design, cryptography, etc. In this paper, inspired by the emerging block Jacket transform, a new class of circulant block Jacket matrices (CBJMs) are mathematically defined based on the circulant matrix theory. Then the existence conditions for the CBJMs with any size based on the Pauli matrices are explicitly given. Next, by employing the Kroneker product and successive low order basic matrices, the fast algorithms for the construction and decomposition of any high order circulant Pauli block Jacket matrices (CPBJMs) are systematically obtained. Finally, compared to the direct computation (DC), the proposed fast algorithms have a better efficiency, which may be available in many fields, such as signal sequence design, image compression, communication for coding and encoding, quantum signal processing and information theory.

Keywords: circulant block Jacket matrices; CBJMs; Pauli matrices; Jacket transform; Kronecker product; fast algorithms.


Biographical notes: Guibo Liu received his BS and MS in School of Information Science and Engineering from Central South University, China, in 2006 and 2008, respectively. Currently, he is a PhD candidate at the School of Information and Engineering, Central South University. His research interests cover wireless communication, signal and image processing.

Zhan Wang is now a graduate student at the School of Information Science and Engineering, Central South University. His research interests include wireless communication, signal and image processing.

Dayong Luo is a Professor at the School of Information Science and Engineering, Central South University. His research interest covers wireless sensor networks, information fusion, and image processing.

Ying Guo received his BS in 1999 in Qufu Normal University, China, MS in 2003 in Kunming University of Science and Technology, China, and PhD in 2006 in Shanghai Jiaotong University, China. His research interests include quantum information processing, and wireless communication. He is an associate member of IEEE Communication Society. He is currently a Professor in Central South University, China.
Moon Ho Lee received his BS and MS in Electrical Engineering from Chonbuk National University, South Korea, in 1967 and 1976, respectively, and PhD in Electrical Engineering from Chonnam National University in 1984. He also received his PhD in Information Engineering from the University of Tokyo, Tokyo, Japan, in 1990. Currently, he is a Professor in the Department of Electronics and Information Engineering and Head of the Institute of Information and Communication at Chonbuk National University. His research interests include image processing, mobile communications and high-speed communication networks, and information and algebra coding theory.

1 Introduction

Hadamard matrices and their generalisations are orthogonal matrices that play an important roles in the signal sequence transform and data processing (Guo et al., 2011). Jacket matrices motivated by the centre weighted Hadamard matrices (Lee, 1989), whose inverse can be simply obtained by their element-wise (Lee et al., 2013; Jiang et al., 2011), have been extensively investigated and applied in many fields, such as signal processing (Lee et al., 2013), encoding design (Jiang et al., 2011), wireless communication (Lee and Guo, 2012), image compression (Lee et al., 2014), watermarking (Ajay et al., 2010) and cryptography (Ma, 2004; Venkata Kishore and JayaVani, 2011). Particularly, some significant matrices, such as Hadamard, Harr, DFT and slant matrices, all belong to the Jacket matrix family (Song et al., 2010; Dr and Vaishali, 2011). Furthermore, Jacket matrices possess a close association with many interesting matrices, such as unitary matrices and Hermitian matrices which are of potentially vital importance in signal processing, data compression, cryptography, orthogonal code design, mathematics and physics (Hom and Johnson, 1991), and so on.

In recent years, block Jacket matrices with their elements substituted by common matrices or block matrices, have been introduced and extensively investigated (Lee et al., 2013; Zeng and Lee, 2008; Jiang and Lee, 2007; Khan et al., 2013). The fast algorithms for one-dimensional and two-dimensional block centre weight Hadamard transform (BCWHT) and block inverse jacket transform are respectively obtained based on the sparse matrix factorisation and the Kroneker products in Lee and Zhang (2007), and Lee and Hou (2006). In Zeng and Lee (2008), generalised inverse block Jacket matrices were extensively investigated, then their fast algorithms were also obtained. Instead of the conventional block-wise inverse Jacket matrix (BIJM), in Mao et al. (2008), the cocyclic block-wise inverse Jacket matrix (CBJIM) was introduced, and corresponding fast algorithms were given subsequently. Besides the afore-mentioned researches emphasising on the theoretical aspect of the block Jacket transforms, there also exist another attempts concentrating on the practical applications of the block Jacket transform, such as non-binary LDPC codes design (Jiang and Lee, 2007), MIMO communication system (Khan et al., 2013), Arikan and Alamouti precoding design (Lee et al., 2013), etc.

Block Jacket matrices have attracted a considerable amount of attention owing to their theoretical value and practical applications. While at the same time, the circulant version of block Jacket transforms just like circulant matrix to the total matrix family, are still absent. The circulant matrices, which are an important component of matrix theory, possess a special structure and useful properties and have been already applied to many engineering fields (Lu and Gu, 2011), so it is necessary to give corresponding focus on the new class of circulant Jacket transform and explore its value. The purpose of this paper firstly is to mathematically define the circulant block Jacket matrix (CBJM). This definition has several essential properties, such as unitary, circulant, block, consistency with Jacket matrix, and so on. After the definition of the CBJM, the existence conditions for the CBJMs based on the Pauli matrices are successfully derived. Since the Pauli matrices are complex orthogonal unitary matrices and actually infinitesimal generators of SU(2) group, the subsequently proposed fast algorithms for the circulant Pauli block Jacket matrices (CPBJMs) may be available in the signal processing, communication, quantum signal processing and information theory (Lee et al., 2012; Guo et al., 2011).

This paper is organised as follows. In Section 2, the definition of the CBJM is mathematically given. In Section 3, the properties of the Pauli matrices are reviewed, and then a general conditions for the existence of the CPBJMs of any size are derived. The fast algorithms for the construction and decomposition of the CPBJMs of any high order are systematically obtained in Section 4, meanwhile some properties and comparisons are also listed. Conclusions are finally drawn in Section 5.

2 Definition of the CBJM

Jacket matrices inspired by the centre weight Hadamard matrices, are kinds of matrices with their inverse being obtained by the element-wise of the matrices. Mathematically, let $A = (a_{ij})$ be a matrix with $A^{-1} = (a_{ij}^T)^T$, then the matrix $A$ is a Jacket matrix, where $T$ denotes the transpose and $(·)$ denotes a matrix. If elements of an $N \times N$ matrix are substituted by $p \times p$ common matrices and there exists $A_{ij} = ((a_{ij}^T)^T$, so the new matrix is called a block Jacket matrix. Meanwhile, circulant matrices as a part of matrix theory have good structure and properties, and also been extensively investigated recently, therefore it is practically valuable to study the new class of the CBJMs. For clarity, before investigating them, it is necessary to give them a scientific unified definition.
Definition 2.1: Let an \( N \times N \) block Jacket matrix 
\[ J_N = (\alpha_i)_{N \times N} \] 
(\( \alpha_i \) are \( p \times p \) matrices with the same size, \( 0 \leq i \leq N - 1 \) and \( p \geq 2 \)), if it has the following form

\[
\begin{pmatrix}
\alpha_0 & \alpha_1 & \cdots & \alpha_{N-1} \\
\alpha_{N-1} & \alpha_0 & \cdots & \alpha_{N-2} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_1 & \alpha_2 & \cdots & \alpha_0 \\
\end{pmatrix}
\]

then we call it a CBJM with size \( N \). When \( \alpha_i \) is replaced by some non-zero numbers, \( J_N \) is just a circulant Jacket matrix.

For clarity, examples are given as follows:

Example 2.1: The matrix

\[
\begin{pmatrix}
2 & 2 \\
1 & 1 \\
\end{pmatrix}
\]

is a CBJM with size 2.

We can also check that the following matrices are also CBJMs because there exits \( 144 = 4 \).

\[
\begin{pmatrix}
\alpha & \alpha & \alpha & \alpha \\
\alpha & \alpha & \alpha & \alpha \\
\end{pmatrix}
\]

where \( \alpha \) and \( \beta \) are both non-zero numbers.

3 The existence conditions for the CPBJMs

Pauli matrices are defined as follows:

\[
\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},
\]

where \( i = \sqrt{-1} \) (Zeng and Lee, 2008). Since Pauli matrices are kinds of complex orthogonal unitary matrices, they are very useful in orthogonal and quasi-orthogonal sequence designs, physics and mathematics, and so on. Furthermore, they also belong to Jacket matrices. So in the following subsections, we firstly focus on the existence conditions for CPBJMs with any size.

3.1 CPBJMs with size 2

In this subsection, the existence condition for the CPBJMs with size 2 is directly given.

Theorem 3.1: The circulant Pauli block matrix 
\[ J_2 = \begin{pmatrix} \alpha_0 & \alpha_1 \\ \alpha_1 & \alpha_2 \end{pmatrix} \]

is a Jacket matrix if and only if

\[ \alpha_0 \sigma_2^{-1} + \alpha_1 \sigma_0^{-1} = [0]_2, \]

where \( \alpha_0 \) and \( \alpha_1 \), order of which is 2, are reversible functions of the Pauli matrices. Since the Pauli matrices \( \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\} \) compose a group SU(2), accordingly any 2 by 2 matrices can be denoted using the basis in the group SU(2) (Zeng and Lee, 2008).

Proof: Since \( \alpha_0 \sigma_2^{-1} + \alpha_1 \sigma_0^{-1} = 2I_2 \), we have the following equation.

\[
J_2 J_2^{-1} = \begin{pmatrix} 2I_2 & \alpha_0 \sigma_2^{-1} + \alpha_1 \sigma_0^{-1} \\ \alpha_0 \sigma_2^{-1} + \alpha_1 \sigma_0^{-1} & 2I_2 \end{pmatrix}
\]

Therefore, \( J_2 \) is a CPBJM if and only if \( \alpha_0 \sigma_2^{-1} + \alpha_1 \sigma_0^{-1} = [0]_2 \).

According to (5), some CPBJMs with size 2 × 2 can be illustrated.

Example 3.1: Suppose \( \alpha_0 = \sigma_1 \) and \( \alpha_1 = \sigma_2 \), we can obtain

\[ \alpha_0 \sigma_2^{-1} + \alpha_1 \sigma_0^{-1} = [0]_2. \]

Then the matrix

\[
\begin{pmatrix}
\alpha_0 & \alpha_1 \\
\alpha_1 & \alpha_0 \\
\end{pmatrix}
\]

belongs to the CPBJM family.

3.2 CPBJMs with size 3

In this subsection, based on a permutation matrix, the existence conditions of CPBJMs with size 3 are derived.

Theorem 3.2: The circulant Pauli block matrix

\[
J_3 = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_0 & \alpha_1 \\ \alpha_1 & \alpha_2 & \alpha_0 \end{pmatrix}
\]

is a Jacket matrix if and only if

\[ \alpha_0 \sigma_2^{-1} + \alpha_1 \sigma_0^{-1} + \alpha_2 \sigma_1^{-1} = [0]_3, \]

and

\[ \alpha_0 \sigma_2^{-1} + \alpha_1 \sigma_1^{-1} + \alpha_2 \sigma_0^{-1} = [0]_3, \]

where \( \alpha_i, \ 0 \leq i \leq 2 \), are reversible functions of the Pauli matrices.

Proof: To prove Theorem 3.2, we firstly consider the permutation matrix

\[
P = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}
\]

which is known as the basic circulant matrix of order 3. Then \( J_3 \) and \( J_3^{-1} \) can be calculated as follows:

\[
J_3 = I_3 \oplus \alpha_0 + P \oplus \alpha_1 + P^2 \oplus \alpha_2,
\]

and

\[
J_3^{-1} = I_3 \oplus \alpha_0^{-1} + P \oplus \alpha_1^{-1} + P^2 \oplus \alpha_2^{-1},
\]

where \( \oplus \) denotes the Kronecker product. So we can obtain \( J_3 J_3^{-1} = I_3 \oplus (3I_3) \), therefore, Theorem 3.2 holds.
Example 3.2: Let \( \alpha_0 = \sigma_1 \) and \( \alpha_2 = \alpha_1 = \frac{1+i\sqrt{5}}{2} \sigma_1 \) in equation (8) and equation (9), we can easily check that the above two equations hold. Therefore, the constructed block matrix

\[
J_3 = \begin{pmatrix}
\alpha_0 & \alpha_1 & \alpha_2 \\
\alpha_1 & \alpha_0 & \alpha_2 \\
\alpha_1 & \alpha_2 & \alpha_0
\end{pmatrix}
\] (13)

is a CPBJM.

3.3 CPBJMs with size \( N \)

In this subsection, a method is presented to get general conditions for the CPBJMs with size \( N \).

Theorem 3.3: Let \( \alpha_i, i \in \{0, 1, \ldots, N-1\} \), be reversible functions of the Pauli matrices, then the circulant Pauli block matrix with size \( N \)

\[
J_N = \begin{pmatrix}
\alpha_0 & \alpha_1 & \ldots & \alpha_{N-1} \\
\ldots & \ldots & \ldots & \ldots \\
\alpha_{N-1} & \alpha_0 & \ldots & \alpha_{N-2}
\end{pmatrix}
\] (14)

is a Jacket matrix if and only if for \( \alpha_i, i \in \{0, 1, 2, \ldots, N-1\} \), it has the following constraint

\[
\sum_{j=0}^{N-1} [\alpha_j \alpha_{(N-i+j)\mod N}] = [0]_2.
\] (15)

where \( \mod \) denotes the modulo operation.

Proof: Suppose an \( N \)-order permutation matrix

\[
P = \begin{pmatrix}
0 & 1 & 0 & \ldots & 0 \\
0 & 0 & 1 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 0 & 0 & \ldots & 0
\end{pmatrix},
\] (16)

then \( J_N \) and \( J_N^{-1} \) can be calculated as follows,

\[
J_N = I_N \otimes \alpha_0 + \sum_{i=1}^{N-1} (P^i \otimes \alpha_i),
\] (17)

and

\[
J_N^{-1} = I_N \otimes \alpha_0^{-1} + \sum_{i=1}^{N-1} (P^{-i} \otimes \alpha_i^{-1}),
\] (18)

where \( I \) denotes the identity matrix. Therefore, the equation

\[
J_N J_N^{-1} = I_N \otimes \alpha_0 + \sum_{i=1}^{N-1} (P^i \otimes \alpha_i) 
\times \left[ I_N \otimes \alpha_0^{-1} + \sum_{i=1}^{N-1} (P^{-i} \otimes \alpha_i^{-1}) \right]
= I_N \otimes \sum_{i=0}^{N-1} (\alpha_i \alpha_i^{-1})
+ \sum_{i=1}^{N-1} \left[ P^i \otimes \sum_{j=0}^{N-1} [\alpha_j \alpha_{(N-i+j)\mod N}] \right]
= I_N \otimes (N \mathbb{I})
\] (19)

holds if and only if it satisfies the following constraint

\[
\sum_{j=0}^{N-1} [\alpha_j \alpha_{(N-i+j)\mod N}] = [0]_2.
\] (20)

By using Theorem 3.3, we can construct CPBJMs with size \( N \).

Example 3.3: Let \( N = 4, \alpha_2 = \pm \alpha_0 \) and \( \alpha_3 = \mp \alpha_0 \), one can check that

\[
J_4 = \begin{pmatrix}
\alpha_0 & \alpha_1 & \pm \alpha_0 & \mp \alpha_0 \\
\mp \alpha_0 & \alpha_0 & \alpha_1 & \pm \alpha_0 \\
\pm \alpha_0 & \mp \alpha_0 & \alpha_0 & \alpha_1 \\
\alpha_0 & \pm \alpha_0 & \mp \alpha_0 & \alpha_0
\end{pmatrix}
\] (21)

is also a CPBJM.

Example 3.4: Let \( \alpha_0 = \sigma_1 \) and \( \alpha_i = \alpha_i, i \in \{2, 3, \ldots, N-1\} \) in equation (15), then equation (15) is changed as follows:

\[
\alpha_0 \alpha_1^{-1} + \alpha_0 \alpha_0^{-1} + (N-2)J_2 = [0]_2.
\] (22)

Suppose \( \alpha_i = m \sigma_1 \), so we have

\[
m + \frac{1}{m} + N - 2 = 0,
\] (23)

that is to say,

\[
m = -\frac{(N-2) \pm \sqrt{N^2 - 4N}}{2}.
\] (24)

Therefore, when \( \alpha_0 = \sigma_1 \) and

\[
\alpha_1 = \frac{-\alpha_1 \pm \sqrt{N^2 - 4N}}{\alpha_1}
\] (25)

the matrix \( J_3 \) is a CPBJM.

Example 3.5: Let

\[
\alpha_0 = \sigma_1, \quad \alpha_1 = m (\sigma_1 + \sigma_3),
\] (26)
\[ \alpha_2 = \frac{(m-1)}{2} (\sigma_0 + \sigma_3) + \frac{(m+1)}{2} \sigma_1 + \frac{(m-1)}{2} i \sigma_2, \]  
(27)

where \( \hat{r} = -1 \), and \( \alpha_i = \alpha_2, i \in \{3, 4, \ldots, N-1\} \) in equation (15), if the constraint
\[ m = -\frac{(N-2) \pm \sqrt{N^2 - 4N}}{2} \]  
(28)

is met, then the constructed matrix \( J_n \) is a CPBJM.

4 The fast algorithms

In the Subsection 3.3, we have proved that CPBJMs with size \( N \) (\( N \geq 2 \)) can be obtained based on the basic Pauli matrices just with certain conditions satisfied. In this section, we first investigate the fast algorithm to construct CPBJMs with high order.

4.1 The fast construction algorithm

Theorem 4.1: A CPBJM with size \( J_{N=2^p q^m} \) (\( p \) and \( q \) are coprime numbers.) can be efficiently constructed in the following way,
\[ J_N = \left[ I_{2^p} \otimes \left( \prod_{i=1}^{m} I_{q^{m-1}} \otimes J_p \otimes I_{p^{i-1}} \right) \right] \]
\[ \times \left[ \prod_{i=1}^{m} I_{q^{m-i}} \otimes J_q \otimes I_{q^{i-1}} \right] \otimes I_{p^{m}}, \]  
(29)

where lower order CPBJMs \( J_p \) and \( J_q \) (lower order: compared to the original matrix \( J_N \)) can be obtained as Subsection 3.3 suggests.

Proof: First by using inductive method to prove the following two equations,
\[ J_{p^n} = \sum_{i=1}^{n} I_{p^{\mu_i}} \otimes J_p \otimes I_{p^{\mu_i-1}}, \]  
(30)

and
\[ J_{q^n} = \prod_{i=1}^{n} I_{q^{\mu_i}} \otimes J_q \otimes I_{q^{\mu_i-1}}. \]  
(31)

Since both have the same proof procedures, so just one is given as follow:
\[ J_{p^1} = \prod_{i=1}^{1} I_{p^{\mu_i}} \otimes J_p \otimes I_{p^{\mu_i-1}}, \]  
(32)

where \( m = 1 \). Now suppose that \( m = K \), the equation still holds,
\[ J_{p^K} = \prod_{i=1}^{K} I_{p^{\mu_i}} \otimes J_p \otimes I_{p^{\mu_i-1}}. \]  
(33)

Subsequently, when \( m = K + 1 \), \( J_{p^{K+1}} \) can be derived as follows,
\[ J_{p^{K+1}} = J_p \otimes J_{p^K} = (I_p \times J_p) \otimes (J_{p^K} \times I_{p^{K}}) \]
\[ = \left( I_p \otimes \left( \prod_{i=1}^{K} I_{p^{\mu_i}} \otimes J_p \otimes I_{p^{\mu_i-1}} \right) \right) \otimes J_{p^K} \]  
(34)

\[ = \prod_{i=1}^{K+1} I_{p^{\mu_i+1}} \otimes J_p \otimes I_{p^{\mu_i-1}}. \]

So (30) and (31) all hold. Combined with these derived results, \( J_N \) can be further calculated as follows:
\[ J_N = J_{q^m} \otimes J_{p^n} \]
\[ = (I_{q^m} \otimes J_{p^n}) \left( I_{q^m} \otimes I_{p^n} \right) \]
\[ = I_{q^m} \otimes \left( \prod_{i=1}^{m} I_{q^{m-i}} \otimes J_q \otimes I_{q^{i-1}} \right) \]
\[ \times \left( \prod_{i=1}^{n} I_{p^{\mu_i+1}} \otimes J_p \otimes I_{p^{\mu_i-1}} \right) \]  
(35)

so the Theorem 4.1 holds.

Here, we note that \( \otimes \) denotes the Kronecker product of block matrices, i.e., let \( J_1 = \begin{pmatrix} \alpha_0 & \alpha_1 \\ \alpha_1 & \alpha_0 \end{pmatrix} \) and \( J_2 = \begin{pmatrix} \beta_0 & \beta_1 \\ \beta_1 & \beta_0 \end{pmatrix} \) be two CPBJMs with size 2, then
\[ J_1 \otimes J_2 = \begin{pmatrix} \alpha_0 \beta_0 & \alpha_0 \beta_1 & \alpha_1 \beta_0 & \alpha_1 \beta_1 \\ \alpha_1 \beta_0 & \alpha_1 \beta_1 & \alpha_0 \beta_0 & \alpha_0 \beta_1 \\ \beta_0 \alpha_0 & \beta_0 \alpha_1 & \beta_1 \alpha_0 & \beta_1 \alpha_1 \\ \beta_1 \alpha_0 & \beta_1 \alpha_1 & \beta_0 \alpha_0 & \beta_0 \alpha_1 \end{pmatrix} \]  
(36)

According to Theorem 4.1, we can construct CPBJMs with large size in a recursive way. In the following parts, some examples are illustrated.

4.1.1 CPBJMs with size \( 2^a \)

In Subsection 3.1, we have constructed CPBJMs with size 2, a general CPBJMs \( J_{N=2^a} \) can be obtained using (29) with \( p = 2, m = n \). So we may construct the CPBJMs with size \( 2^a \) based on CPBJMs with size 2.

Example 4.1: Let a CPBJM \( J_2 = \begin{pmatrix} \sigma_2 \\ \sigma_3 \end{pmatrix} \), then a CPBJM \( J_4 \) may be constructed in the following way \( J_4 = J_2 \otimes J_2 \).

4.1.2 CPBJMs with size \( 3^a \)

A method is presented to construct CPBJMs with size 3 in Subsection 3.2, then we can obtain CPBJMs \( J_{N=3^a} \) using (29) with \( p = 3 \) and \( m = n \).

Example 4.2: Let
one can check that \( J_3 \) is a CPBJM. Then we may obtain a
CPBJM with size \( 3^3 \) in the following way
\[
J_{N=3^3} = J_3 \otimes J_3 \otimes J_3.
\]

\subsection*{4.1.3 CPBJMs with size \( 5^i \)} Similarly, the CPBJM \( J_5 \) is needed to construct the CPBJMs
\( J_{N=5^i} \). Inspired by the Example 3.4, let
\[
\alpha_i = \frac{-3 + i\sqrt{5}}{2},
\]
i \in \{1, 2, 3, 4\}, then we obtain a CPBJM \( J_5 \). So a CPBJM
with size \( 5^2 \) can be formed in the following way
\( J_{n=5^2} = J_5 \otimes J_5 \).

\subsection*{4.1.4 CPBJMs with size \( 6^i \)} Since \( 6^i = 2^a \times 3^b \), based on the (29) with \( p = 2, q = 3 \) and
\( m = n \), the matrices \( J_{N=6^i} \) can be directly constructed as
\( J_6 = (J_2 \otimes I_3)(I_2 \otimes J_3) \).

\subsection*{4.2 The fast factorisation algorithm} In the Subsection 4.1, we focus on the fast construction of
CPBJMs with large size, while in this subsection we
investigate their fast factorisation algorithms, which also
have a recursive form.

\textbf{Theorem 4.2:} Suppose a CPBJM \( J_{N=p_1q_1} \) if \( J_N \) is
factorable until \( J_p \) and \( J_q \). Then \( J_N \) can be decomposed
according to (29).

\textbf{Proof:} It is obvious that the decomposition is a reverse
procedure of the construction. So the proof is
straightforward. Theorem 4.2 gives a method to decompose
high order CPBJMs.

\textbf{Example 4.3:} For example, we consider the case with \( p = 3, \)
\( q = 5 \) and \( n = m = 1 \). Since \( J_3 \) and \( J_5 \) can not be decomposed,
the block matrix with size 15 can be denoted as
\( J_{15} = (J_3 \otimes I_5)(I_3 \otimes J_5) \). The decomposition graph corresponding to the
factorisation is shown in Figure 1.

For more examples, Table 1 lists some construction and
decomposition approaches for CPBJMs \( J_i \) (\( i = 1, 2, \ldots, 20 \)).
In this table, the second column denotes the decomposition
approaches for these numbers meanwhile the construction
approaches are shown in the third column.

Compared to direct computation (abbreviated as DC),
fast circulant block Jacket transforms require less numbers
of additions (abbreviated as ADD) and multiplications
(abbreviated as MUL). Table 2 illustrates the differences
between them in detail. The first column contains two
operations of ADD and MUL, meanwhile the computation
complexity of DC is presented in the second column. While
the remaining two columns denote the computation
complexity of DC is presented in the second column. While
the remaining two columns denote the computation
complexity of DC is presented in the second column. While
the remaining two columns denote the computation
complexity of DC is presented in the second column. While
the remaining two columns denote the computation
complexity of DC is presented in the second column. While
the remaining two columns denote the computation
complexity of DC is presented in the second column. While
the remaining two columns denote the computation
5 Conclusions

In this paper, CBJMs based on the Pauli matrices with any size are derived to extend the Jacket matrix and the circulant matrix families. We have firstly investigated the existence conditions of CPBJMs with any size. Then, fast efficient construction and decomposition algorithms based on the Kronecker product and sparse matrices decomposition have been extensively investigated. Compared to the DC, the fast algorithms have a greater efficiency for computation. Some properties and original results are also presented in the form of tables at the end, which may be applied to many fields such as signal transform, image processing, cryptography, mobile communication, and so on.

References


