ASM Sc. J., 12, Special Issue 5, 2019 for ICoAIMS2019, 72-79

Potential Applications of Hourglass Matrix and its Quadrant Interlocking Factorization

Olayiwola Babarinsa[1*], Arif Mandangan[2] and Hailiza Kamarulhaili[3]

[1]*Department of Mathematical Sciences, Federal University Lokoja, 1154 Kogi State, Nigeria*

[2]*Faculty of Science and Natural Resources, Universiti Malaysia Sabah, 88400 Kota Kinabalu, Malaysia*

[1,2,3]*School of Mathematical Sciences, Universiti Sains Malaysia, 11800 Pulau Pinang, Malaysia*

Hourglass matrix is recently shown to be a subset of Z-matrix which can be obtained from Quadrant Interlocking Factorization (*QIF*) of nonsingular matrix. Unlike Z-matrix, the factorization of hourglass matrix may not exist for every nonsingular matrix. However, the potential applications of hourglass matrix and its *QIF*, such as in statistics (Markov chains), cryptography (GGH encryption scheme) and in graph theory (mixed graph), surpasses the counterpart Z-matrix and its *WZ* factorization. Lastly, hourglass matrix can be partitioned into triangular block matrices having Schur complement.

Keywords: hourglass matrix; z-matrix; quadrant interlocking factorization; markov chains; GGH encryption; mixed graph

I. INTRODUCTION

The appellation word "hourglass matrix" is coined by Demeure (1989) in describing the matrix derived from factorizing a square matrix, predominantly from real symmetric Toeplitz matrix or Hankel matrix by computing the entries column by column via bowtie-hourglass factorization (*WZ* factorization or quadrant interlocking factorization (*QIF*)). However, *WZ* factorization of nonsingular matrix to yield a butterfly (hourglass) shaped dense square matrix called Z-matrix is first posited by D. Evans and Hatzopoulos (1979). WZ factorization has been modified and applied together with its block factorization being discussed, see for examples (B. Bylina, 2018; D. J. Evans, 2002; Rhofi & Ameur, 2016). Z-matrix exists together with W-matrix during *WZ* factorization of non-singular matrix B, such that (B. Bylina, 2003)

$$B = WZ \tag{1}$$

Where the entries in Z as

$$h_{i,j}^{*(k)} = h_{i,j}^{*(k-1)} + w_{i,k}^{*(k)} h_{k,j}^{*(k-1)} + w_{1,n-k+1}^{*(k)} h_{n-k+1,j}^{*(k-1)} \tag{2}$$

and the entries in W are computed from $w_{i.k}^{(k)}$ and $w_{i.n-k+1}^{(k)}$ as

$$\begin{cases} z_{k.k}^{(k-1)} w_{i.k}^{(k)} + z_{n-k+1.k}^{(k-1)} w_{i.n-k+1}^{(k)} = -z_{i.k}^{(k-1)} \\ z_{k.n-k+1}^{(k-1)} w_{i.k}^{(k)} + z_{n-k+1.n-k+1}^{(k-1)} w_{i.n-k+1}^{(k)} = -z_{i.n-k+1}^{(k-1)} \end{cases} \tag{3}$$

For $k = 1, 2, \dots, \frac{n}{2}$; $i, j = k + 1, \dots, n - k$. The necessary and sufficient condition for matrix $B = [b_{j,k}]_{j,k=1}^{n}$ to be factorized is that the central submatrices $B_{n+2-2l}^{c} = [b_{j,k}]_{j,k=1}^{n+1-l}$ are nonsingular, where n is even order of matrix B (the assumption also holds for odd order) and c the centered submatrix of B, for $l = 1, \dots, \frac{n}{2}$ (Rao, 1997). The factorization is known for the adaptability of its direct method to solve $n \times n$ linear systems given as (Heinig & Rost, 2011).

$$Bx = c \tag{4}$$

where
$\det(B) \neq 0$, $x = [x_1, x_2, \dots, x_n]^T$, $x, c \in \mathbb{R}^n, B \in \mathbb{R}^{n\times n}$
$c = [c_1, c_2, \dots, c_n]^T$ $B = \{b_{ij}\}$ $1 \le i, j \le n$.

More so, it was further elucidated that hourglass matrix is the same as Z-matrix which can be partitioned into blocks structured Z-system (J. Bylina & Bylina, 2016; Heinig & Rost, 2005). Unfortunately, there are changes in structure of Z-matrix from WZ factorization or QIF which depend on the type of matrix (Toeplitz, Hankel, Hermitian, centrosymmetric, diagonally dominant or tridiagonal matrix) being factorized. Nevertheless, Z-matrix may not

*Corresponding author's e-mail: babs3in1@gmail.com

always imply hourglass matrix nor their applications are always indistinguishable. Consequently, the synonymity between hourglass matrix and Z-matrix dwindles over time without a cogent reason. Recently, Babarinsa and Kamarulhaili (2018) gave meticulous details of hourglass matrix and its quadrant interlocking factorization by restricting the computed entries of the factorization to be nonzero in comparison with the shape of hourglass device. This led them to conclude that hourglass matrix is a subset of Z-matrix. Thus, in Section II, we give the review of hourglass matrix and its factorization. While in Section III, the potential applications of hourglass matrix and its factorization are highlighted with some results.

II. HOURGLASS MATRIX

Definition 1. (Babarinsa & Kamarulhaili, 2018) Let H be an hourglass matrix of order $n(n \geq 3)$ with strictly nonzero elements $h_{i,j} \in \mathbb{R}$, defined as

$$H = \begin{cases} h_{i,j} & 1 \leq i \leq \left\lfloor \frac{n+1}{2} \right\rfloor \quad i \leq j \leq n+1-i; \\ h_{i,j} & \left\lceil \frac{n+2}{2} \right\rceil \leq i \leq n \quad n+1-i \leq j \leq i; \\ 0, & \text{otherwise.} \end{cases}$$

In other words, an hourglass matrix (H-matrix) is a nonsingular matrix of order n $(n \geq 3)$ with nonzero entries from the ith to the $(n-i+1)$ element of the ith and $(n-i+1)$ row of the matrix, 0's otherwise for $i = 1, 2, \ldots, \left\lceil \frac{n+1}{2} \right\rceil$ (Babarinsa & Kamarulhaili, 2018). The authors referred quadrant interlocking factorization of nonsingular matrix to yield hourglass matrix as WH factorization, whereas Z-matrix is obtained from WZ factorization. Though the factorization of H-matrix and Z-matrix are quite similar, WH factorization restricts the computed entries to be nonzero at every stage during the factorization. Unlike WZ factorization, WH factorization specifies the number of times row-interchange can be applied at each stage of the factorization. The WZ factorization exists for every nonsingular matrix often with pivoting while WH factorization may fail to exist even if the matrix is nonsingular. WZ and WH factorization require W-matrix to be computed during the factorization process. Unlike the factorization of Z-matrix, the factorization for an hourglass matrix from a nonsingular matrix may not be from a symmetric positive definite or diagonally dominant matrix but definitely not from a tridiagonal matrix. Unlike Z-matrix, hourglass matrix of order n has $\frac{(n^2+2n-|(n+1) mod\, 2-1|)}{2}$ nonzero entries and $\frac{(n^2-2n+|(n+1) mod\, 2-1|)}{2}$ zero entries. Therefore, the WH factorization gives

$$B = WH \tag{5}$$

Proposition 1. (Babarinsa & Kamarulhaili, 2018) Let H be an hourglass matrix of order $n(n \geq 3)$. Then, the determinant of hourglass matrix is

$$det(H) = \begin{cases} \displaystyle\prod_{i=1}^{\left\lceil \frac{n-1}{2} \right\rceil} \begin{vmatrix} h_{i,i}^{(i-1)} & h_{i,n+i-1}^{(i-1)} \\ h_{n+i-1,i}^{(i-1)} & h_{n+i-1,n+i-1}^{(i-1)} \end{vmatrix} & if\ n\ is\ even \\ h_{\frac{n+1}{2},\frac{n+1}{2}}^{\frac{n+1}{2}} \displaystyle\prod_{i=1}^{\left\lceil \frac{n-1}{2} \right\rceil} \begin{vmatrix} h_{i,i}^{(i-1)} & h_{i,n+i-1}^{(i-1)} \\ h_{n+i-1,i}^{(i-1)} & h_{n+i-1,n+i-1}^{(i-1)} \end{vmatrix} & if\ n\ is\ odd \end{cases}$$

Partitioning of hourglass matrix of order n $(n > 3)$ into block triangular matrices gives $Hsystem$, with each block containing $\left\lfloor \frac{n}{2} \right\rfloor \times \left\lfloor \frac{n}{2} \right\rfloor$matrices, see Equation (6). The partition gives exactly four blocks of triangular matrices if n is even dimension while additional column vector, $\tilde{x}$, position at $\frac{n+1}{2}$ th column of the matrix if n is odd dimension. The column vector $\tilde{x}$ can be further partitioned into x_1, x and x_2, where x_1 and x_2 have dimension of $\frac{n-1}{2} \times 1$, and x an epicenter element (unit vector). Moreover, the major difference between Z_{system} and H_{system} is that each block in H_{system} has specific number of zero and nonzero entries, unlike Z_{system}

$$H_{system} = \begin{bmatrix} H_{1,1} & H_{1,2} \\ H_{2,1} & H_{2,2} \end{bmatrix} \tag{6}$$

Where

$$H_{1,1} = \begin{cases} h_{i,j} & 1 \leq i \leq \left\lceil \frac{n-1}{2} \right\rceil, \quad i \leq j \leq \left\lceil \frac{n-1}{2} \right\rceil; \\ 0, & \text{otherwise.} \end{cases}$$

$$H_{1,2} = \begin{cases} h_{i,j} & 1 \leq i \leq \left\lceil \frac{n-1}{2} \right\rceil, \quad \left\lfloor \frac{n+3}{2} \right\rfloor \leq j \leq n+1-i; \\ 0, & \text{otherwise.} \end{cases}$$

$$H_{2,1} = \begin{cases} h_{i,j} & \left\lfloor \frac{n+3}{2} \right\rfloor \leq i \leq n, \quad \left\lfloor \frac{n+3}{2} \right\rfloor \leq j \leq i; \\ 0, & \text{otherwise.} \end{cases}$$

$$H_{2,1} = \begin{cases} h_{i,j} & \left\lfloor \frac{n+3}{2} \right\rfloor \leq i \leq n, \quad n+1-i \leq j \leq \left\lceil \frac{n-1}{2} \right\rceil; \\ 0, & \text{otherwise.} \end{cases}$$

The major difference between Z_{system} and H_{system} is that each block in H_{system} has specific number of zero and nonzero entries, unlike Z_{system}. Like Z_{system}, the determinant of $Hsystem$ can easily be calculated from its blocks. We will concentrate on the even order of H_{system}. Then, the Schur complement of a matrix block in Equation (6) is defined as follows

$$H_{system}/H_{1,1} = H_{2,2} - H_{2,1}{H_{1,1}}^{-1}H_{1,2} \tag{7}$$

Theorem 1. Schur complement exists in Hsystem only if H-matrix is nonsingular.

Proof

For the existence of H-matrix like Z-matrix, the necessary and sufficient condition for WH factorization is that matrix B must be centro-nonsingular. First, let H-matrix of even order being factorized from nonsingular matrix B be

$$H = \begin{bmatrix} \alpha_{k,k} & \cdots & \cdots & \alpha_{k,\frac{n}{2}} & \vdots & \beta_{k,\frac{n}{2}+1} & \cdots & \cdots & \beta_{k,n} \\ & \ddots & H_{1,1} & \vdots & \vdots & \vdots & H_{1,2} & \iddots & \\ & & \ddots & \vdots & \vdots & \vdots & \iddots & & \\ & & & \alpha_{k,k} & \cdots & \beta_{k,l} & & & \\ \cdots & \cdots & \cdots & \vdots & & \vdots & \cdots & \cdots & \cdots \\ & & & \gamma_{l,k} & \cdots & \delta_{l,l} & & & \\ & & \iddots & \vdots & \vdots & \vdots & \ddots & & \\ & \iddots & H_{2,1} & \vdots & \vdots & \vdots & H_{2,2} & \ddots & \\ \gamma_{n,k} & \cdots & \cdots & \gamma_{n,\frac{n}{2}} & \vdots & \delta_{n,\frac{n}{2}+1} & \cdots & \cdots & \delta_{n,n} \end{bmatrix} \tag{8}$$

Where $k = 1,2,\ldots,\frac{n}{2}$; $l = n - k + 1$.. Then, the determinant of H-matrix is

$$\det(H) = det\begin{bmatrix} \alpha_{k,k} & \cdots & \beta_{k,l} \\ \vdots & \ddots & \vdots \\ \gamma_{l,k} & \cdots & \delta_{l,l} \end{bmatrix}_{1\le k\le\frac{n}{2};\, l=n-k+1}$$

$$\prod_{k=1}^{\frac{n}{2}} \left(\alpha_{k,k}\delta_{l,l} - \beta_{k,l}\gamma_{l,k}\right)_{l=n-k+1} \neq 0 \tag{9}$$

Next, partition Equation (8) into H_{system} of 2×2 triangular block matrices as

$$H_{system} = \begin{bmatrix} H_{1,1} & H_{1,2} \\ H_{2,1} & H_{2,2} \end{bmatrix} \tag{10}$$

If each 2×2 triangular block matrix is singular (or $H_{1,1}H_{2,2} = H_{1,2}H_{2,1}$), then H_{system} is not invertible which contradicts Equation (9). Thus, there exist at least two nonsingular triangular block matrices in H_{system}. If $H_{1,1}$ is invertible as well as $H_{2,2}$ (this is also true for $H_{1,2}$ and $H_{2,1}$), then the Schur complement of the block $H_{1,1}$ in H_{system} is given as

$$H_{2,2} - H_{2,1}{H_{1,1}}^{-1}H_{1,2} \tag{11}$$

The determinant of Equation (11) is nonsingular because $H_{2,2} - H_{2,1}{H_{1,1}}^{-1}H_{1,2}$ is a lower triangular invertible matrix and

$$\frac{\det\left(H_{2,2} - H_{2,1}{H_{1,1}}^{-1}H_{1,2}\right)}{\det(H_{1,1})} \neq 0.$$

Thus,

$$\det(H_{system}) = \det(H_{1,1})\det(H_{2,2} - H_{2,1}{H_{1,1}}^{-1}H_{1,2}).$$

This shows that the Schur complement of H_{system} depends on the existence of H-matrix.

III. POTENTIAL APPLICATIONS OF HOURGLASS MATRIX AND ITS QIF ALGORITHM

A. Statistics: Markov chains

WZ factorization has been applied to find the numerical solutions of Markov chains, see (B. Bylina & Bylina, 2004, 2009). However, we can replace WZ factorization with WH factorization in modeling with Markov chains. Markov models are the most useful ones to describe queueing models. A homogeneous continuous-time Markov chain can be described with one singular matrix

$$Q = (q_{ij})_{i,j=1,2,\ldots,n} \tag{12}$$

called the transition rate matrix given by

$$q_{ij} = \lim_{\Delta t\to 0} \frac{p_{ij}(\Delta t)}{\Delta t} \tag{13}$$

and by

$$q_{ii} = -\sum_{i\neq j} q_{ij} \tag{14}$$

for $i \neq j$.

We need to find $x = \pi^T$ the vector of the stationary probabilities π_i that the system is in the state i at the time t from:

$$Q^T x = 0, \qquad x \geq 0, \qquad x^T e = 1 \tag{15}$$

where Q is an $n \times n$ transition rate matrix (with dominant diagonal and rank $(n-1)$, x a vector of state probabilities and $e = (1, 1, \ldots, 1)^T$. The most intuitive approach to solve a homogenous linear system Equation (15) is to replace an arbitrary equation of that system with the normalization equation $x^T e = 1$. Let Q_p be the matrix Q with the pth column replaced with the vector e, then the system can be written as $Q_p^T x = e_p$, where $e_p = (\rho_{ip})$ for $i = 1, \ldots, n$. Let $Q_p^T = WZ$. Solving Equation (4) with WZ factorization to have

$$\begin{cases} Wy = c \\ Zx = y \end{cases}$$

we can set $Zx = y$ in the system $WZx = e_p$ to get $Wy = e_p$. From which it is obvious that $y = e_p$ bacause W is unimodular matrix, where we can now solve the system $Zx = e_p$. However, we may apply WH factorization instead of the classical WZ factorization in the Markov chains by letting $Q_p^T = WH$. Now, we set $Hx = y$ in the system $WHx = e_p$ to get $Wy = e_p$ and then solve the system $Hx = e_p$. Preconditioning prevents the problem of convergence of the coefficient matrix Q of the linear system. Since Q is ill-conditioned matrix, then Equation (15) can be transformed by preconditioning it as

$$M^{-1}Q^T x = 0, \qquad x \geq 0, \qquad x^T e = 1 \tag{16}$$

where M is a nonsingular matrix. However, Equation (15) and Equation (16) have the same solution but different condition number with accuracy $\|M^{-1}Q^T x - 0\|$.

B. Cryptography: Goldreich-Goldwasser-Halevi encryption scheme

Cryptography is a science of information security which aims to achieve security goals such as confidentiality, authentication, data integrity and nonrepudiation (Schneier, 2007). Most of the available cryptographic schemes widely deployed today lying in their security on the hardness of number theoretic hard problems such as integer factorization problem (IFP), discrete logarithm problem (DLP) and elliptic curve discrete logarithm problem (ECDLP). The most establish cryptographic schemes which rely on these problems are Rivest-Shamir-Adleman (RSA), El-Gamal and elliptic curve cryptosystems. However, the security of these schemes can be compromised due to the existence of powerful algorithm known as Shor's quantum algorithm which can solve these problems in reasonable amount of time (Shor, 1994). Unfortunately, the algorithm requires a fully functioning quantum computer to be executed effectively. Therefore, it is prudent to find alternatives to avoid global security threats once the fully functioning quantum computer is being established.

One of the most promising candidates to replace the number theoretic-based cryptographic schemes is lattice-based cryptography (Schneier, 2007). The idea behind the lattice-based cryptography is to exploit the immunity of some lattice problems such as the shortest vector problem (SVP) and closest vector problem (CVP) against the Shor's quantum algorithm (Ekert & Jozsa, 1996). Another selling point of the lattice-based cryptography is the establishment of relationship between the worst case and average case hardness of these lattice problems. The earliest lattice-based encryption scheme which was considered as the most practical scheme is Goldreich-Goldwasser-Halevi encryption scheme or GGH scheme. Through various empirical results, Goldreich, Goldwasser, and Halevi (1997) analysed the security of the GGH scheme and conjectured that the scheme was intractable in practice for a lattice dimension above 300. However, the key size of the GGH scheme is larger than those cryptosystems since the public and private keys of the GGH scheme are the lattice bases. Due to the attack on the GGH Scheme, Nguyen (1999) discovered that the main weaknesses of the scheme are due to its key generation process. The generated public basis B allowed his attack to succeed in simplifying the underlying lattice CVP instance into its simpler form. Although Nguyen's attack successfully decrypted the published GGH internet challenges up to lattice dimension of 350. The security of GGH scheme can still be upgraded by improving the key generation processes to address the weaknesses exploited by Nguyen's attack. The improvement is not only on the security aspect to make the GGH Scheme stronger than its original version, but also in efficiency aspect. The size of the bases should be reduced to allow larger lattice dimension to be implemented while keeping the scheme practical. Suppose that $B, H \in \mathbb{R}^{n \times n}$ be nonsingular with linearly independent vectors $\vec{b}_1, \vec{b}_2 \ldots, \vec{b}_n$ and $\vec{h}_1, \vec{h}_2 \ldots, \vec{h}_n$ as their columns respectively. The lattice $L(B) \subset \mathbb{R}^n$ that spanned by the basis B is defined as follow

$$L(B) = \left\{ \sum_{i,j=1}^{n} \mu_{i,j} \vec{b}_i \,\middle|\, \vec{b}_i \in B \text{ and } \mu_{i,j} \in \mathbb{Z}, \forall i, j = 1, \ldots, n \right\}$$

and the lattice $L(H) \subset \mathbb{R}^n$ that spanned by the basis H is defined as follow

$$L(H) = \left\{ \sum_{i,j=1}^{n} \tau_{i,j} \vec{h}_i \,\middle|\, \vec{h}_i \in H \text{ and } \tau_{i,j} \in \mathbb{Z}, \forall i,j = 1, \dots, n \right\}$$

To ensure that the bases B and H are spanning the same lattice, i.e., $L(B) = L(H)$, the matrix W is required to be a unimodular matrix with $\det(W) = \pm 1$.

Proposition 2: Let $B, H \in \mathbb{R}^{n \times n}$ be two non-singular square matrices such that $B = HW$ where $W \in \mathbb{Z}^{n \times n}$. If W is a unimodular matrix, the B and H are bases that spanning the same lattice, i.e., $L(B) = L(H)$.

Proof

Suppose the matrices $B, H \in \mathbb{R}^{n \times n}$ are the basis of the lattice $L(B)$ and $L(H)$ respectively. This implies that, the basis vectors $\vec{b}_1, \vec{b}_2 \dots, \vec{b}_n \in L(B)$ and $\vec{h}_1, \vec{h}_2 \dots, \vec{h}_n \in L(H)$. Given that $B = HW$. Then we have,

$$\begin{bmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,n} \end{bmatrix}$$

$$= \begin{bmatrix} h_{1,1} & h_{1,2} & \cdots & h_{1,n} \\ h_{2,1} & h_{2,2} & \cdots & h_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n,1} & h_{n,2} & \cdots & h_{n,n} \end{bmatrix} \begin{bmatrix} w_{1,1} & w_{1,2} & \cdots & w_{1,n} \\ w_{2,1} & w_{2,2} & \cdots & w_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ w_{n,1} & w_{n,2} & \cdots & w_{n,n} \end{bmatrix}$$

$$[\vec{b}_1 \quad \vec{b}_2 \quad \cdots \quad \vec{b}_n] = [\vec{h}_1 \quad \vec{h}_2 \quad \cdots \quad \vec{h}_n][\vec{w}_1 \quad \vec{w}_2 \quad \cdots \quad \vec{w}_n]$$

Note that, each of the $\vec{b}_j$ vectors can be represented as follows

$$\vec{b}_j = w_{1,j}\vec{h}_1 + w_{2,j}\vec{h}_2 + \cdots + w_{n,j}\vec{h}_n$$

for all $j = 1, \dots, n$. Assume that, W is a unimodular matrix. Then, the scalars $w_{i,j} \in \mathbb{Z}$ for all $w_{i,j} \in W$. This implies that, the basis vectors $\vec{b}_1, \vec{b}_2 \dots, \vec{b}_n \in L(H)$. Hence, we have

$$L(B) \subset L(H)$$

Since W is a unimodular matrix, then $\det(W) = \pm 1$. That means, there exists W^{-1} such that $WW^{-1} = I$. For simplicity, we let $W^{-1} = U$. From $B = HW$, now we have

$$H = BW^{-1}$$
$$H = BU$$

$$\begin{bmatrix} h_{1,1} & h_{1,2} & \cdots & h_{1,n} \\ h_{2,1} & h_{2,2} & \cdots & h_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n,1} & h_{n,2} & \cdots & h_{n,n} \end{bmatrix}$$

$$= \begin{bmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,n} \end{bmatrix} \begin{bmatrix} u_{1,1} & u_{1,2} & \cdots & u_{1,n} \\ u_{2,1} & u_{2,2} & \cdots & u_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ u_{n,1} & u_{n,2} & \cdots & u_{n,n} \end{bmatrix}$$

$$[\vec{h}_1 \quad \vec{h}_2 \quad \cdots \quad \vec{h}_n] = [\vec{b}_1 \quad \vec{b}_2 \quad \cdots \quad \vec{b}_n][\vec{u}_1 \quad \vec{u}_2 \quad \cdots \quad \vec{u}_n]$$

Note that, each of the $\vec{h}_j$ vectors can be represented as follows

$$\vec{h}_j = u_{1,j}\vec{b}_1 + u_{2,j}\vec{b}_2 + \cdots + u_{n,j}\vec{b}_n$$

for all $j = 1, \dots, n$. Since W is a unimodular matrix, then $W^{-1} = U$ is also a unimodular matrix. That means, the scalars $u_{i,j} \in \mathbb{Z}$ for all $u_{i,j} \in U$. This implies that, the basis vectors $\vec{h}_1, \vec{h}_2 \dots, \vec{h}_n \in L(B)$. Hence, we have

$$L(H) \subset L(B)$$

Since $L(B) \subset L(H)$ and $L(H) \subset L(B)$, therefore we have shown that

$$L(B) = L(H)$$

when W is a unimodular matrix.

Based on the structure of hourglass matrix, the matrix could be potentially used as the key (basis) in the GGH encryption scheme. The usage of hourglass matrix is expected to be able to reduce the size of bases, especially the public key. Almost half of the entries of the hourglass matrix are zero entries, which means the size of public key can be reduced if the public key is generated in the form of hourglass matrix. This reduction will allow the GGH Scheme to be implemented in higher lattice dimension while still being able to be efficient and practical. Hourglass matrix has linearly independent columns forming the basis of a lattice, which makes it suitable for GGH scheme. In addition, the generation of hourglass matrix from *QIF* processes can be executed in polynomial time. This give more advantages in terms of efficiency.

C. Graph theory: Mixed graph

A simple graph $G = (V, E)$ is an ordered pair consisting of a set of vertices $V = \{ v_1, v_2 \dots v_n \}$ and a set of undirected edges $E = \{ e_1, e_2 \dots e_n \}$, no loop or multiple edges permitted (Rosen & Krithivasan, 2015). A directed graph or digraph is a graph that contains only set of directed arcs with the set of vertices $V = \{ v_1, v_2 \dots v_n \}$ (Rosen & Krithivasan, 2015)A mixed graph $G = (V, E, A)$ is an ordered triple consisting a set of vertices $V = \{ v_1, v_2 \dots v_n \}$, a set of undirected edges $E = \{ e_1, e_2 \dots e_n \}$ and a set of directed arcs A (Arumugam, Brandstädt, Nishizeki, & Thulasiraman, 2016). The unweighted mixed adjacency matrix of a mixed graph G is defined as $M = M(G) = [m_{ij}]$ as an $n \times n$. matrix indexed by the vertices $\{ v_1, v_2 \dots v_n \}$, where $m_{ij} = 1$ if $v_i v_j \in E$, $m_{ij} = -1$ if $v_i v_j \in A$, and $m_{ij} = 0$ otherwise; see for instance (Adiga, Rakshith, & So, 2016; Guo & Mohar, 2015).

A butterfly graph (hourglass graph) is a is a planar undirected graph formed by at least two triangles intersecting in a single vertex, especially from 5-vertex graph of two $k3$'s or from friendship graph $F2$, see (Alikhani, Brown, & Jahari, 2016; Liu, Zhu, Shan, & Das, 2017; Ponraj, Narayanan, & Ramasamy, 2015). However, the hourglass graph discusses here is a mixed complete graph coined from the name of its mixed adjacency matrix which is obtained from hourglass matrix. A direct representation of hourglass matrix to weighted hourglass-adjacency matrix will produce a weighted mixed hourglass graph with loops and with or without multiple arcs and undirected edges. There are conditions to be met if the weighted mixed hourglass graph of weighted mixed hourglass-adjacency matrix is to be represented, such as taking absolute value of negative weights and making all entries on the anti-diagonal the same to avoid multiple arcs and produce edges instead. However, the nature of the entries in hourglass matrix solely depends on the factorization and it is responsible for the weight in the graph. The inconsistence in the representation can be avoided if we consider mixed hourglass-adjacency matrix from the weighted mixed hourglass-adjacency matrix. To do this, we replace the nonzero entries (weights) of the weighted mixed hourglass-adjacency matrix with 1's if there exists an undirected edge, -1's if there exists an arc or loop and 0's otherwise, see (Babarinsa & Kamarulhaili, 2019). In order to avoid loops, we assign 0's to the diagonal of the mixed hourglass-adjacency matrix $M(\mathcal{G})$ to obtain mixed hourglass graph $\mathcal{G}$ with an edge joining v_i and $v_{(n+1-i)}$; for $i = 1, 2, \dots, \lceil \frac{n-1}{2} \rceil$. With this, the mixed energy, spanning subgraph, Zagreb index and k-factorization of the graph can be obtained from mixed hourglass graph.

Definition 2. (Babarinsa & Kamarulhaili, 2019) A mixed hourglass-adjacency matrix $M(\mathcal{G})$ of a mixed hourglass graph $\mathcal{G}$ is the $n \times n (n \geq 3)$ matrix $M(\mathcal{G}) = (h_{i,j})_{n \times n}$ defined by

$$M(\mathcal{G}) = \begin{cases} 1 & \text{if } v_i v_J \text{ is an edge;} \\ -1 & \text{if } (v_i, v_J) \text{ is an arc;} \\ 0 & otherwise. \end{cases}$$

Proposition 3. Let $\mathcal{G}$ be a mixed hourglass graph and let $\det(M(\mathcal{G}))$ be the determinant of mixed hourglass-adjacency matrix $M(\mathcal{G})$ of order n. Then

$$det(M(\mathcal{G})) = \begin{cases} 0 & if\ n\ is\ odd \\ -1 & if\ n = 2k\ where\ k\ is\ odd \\ 1 & if\ n = 2k\ where\ k\ is\ even. \end{cases}$$

Proof

We let $det(M(\mathcal{G})) = cos\left(\frac{\pi n}{2}\right)$ because $-1 \leq cos\left(\frac{\pi n}{2}\right) \leq 1$ irrespective of the value of n. Noticeably, when n is odd then $cos\left(\frac{\pi n}{2}\right) = 0$. If n is even, then $n = 2k$ for $k \in \mathbb{N}$. We have,

$$cos\left(\frac{\pi n}{2}\right) = \cos(\pi k) = (-1)^k$$

Thus,

$$(-1)^k = \begin{cases} 1 & if\ k\ is\ even \\ -1 & if\ k\ is\ odd. \end{cases}$$

Therefore,

$$cos\left(\frac{\pi n}{2}\right) = \begin{cases} 0 & if\ n\ is\ odd \\ (-1)^k = \left\{ \begin{matrix} 0 & if\ n\ is\ odd \\ -1 & if\ n = 2k\ where\ k\ is\ odd \\ 1 & if\ n = 2k\ where\ k\ is\ even. \end{matrix} \right\} & if\ n\ is\ even \end{cases}$$

IV. CONCLUSION

Results on hourglass matrix and its quadrant interlocking factorization hasbeen discussed. The applications of the matrix and its factorization has been highlighted. We conclude that WH factorization may not exist for every nonsingular matrix even if the matrix can be factorized from WZ factorization. However, the advantages of hourglass matrix go beyond scientific computing and surpass its counterpart Z-matrix.

V. ACKNOWLEDGEMENT

This research is funded by RU (Research University) Grant, Universiti Sains Malaysia, Grant number 1001/PMATHS/811337.

VI. REFERENCES

Adiga, C Rakshith, B & So, W 2016, "On the mixed adjacency matrix of a mixed graph" *Linear Algebra and its Applications, 495*, pp. 223-241.

Alikhani, S Brown, J & Jahari, S 2016 "On the domination polynomials of friendship graphs" *Filomat, 30*(1), pp. 169-178.

Arumugam, S Brandstädt, A Nishizeki, T & Thulasiraman, K 2016. *Handbook of graph theory, combinatorial optimization, and algorithms*: Chapman and Hall/CRC.

Babarinsa, O & Kamarulhaili, H 2018 *Quadrant interlocking factorization of hourglass matrix*. Paper presented at the AIP Conference Proceedings, Kuantan.

Babarinsa, O & Kamarulhaili, H 2019 "Mixed Energy of a Mixed Hourglass Graph" *Communications in Mathematics and Applications, 10*(1), pp. 45-53.

Bylina, B 2003 "Solving linear systems with vectorized WZ factorization" *Annales UMCS, Informatica, 1*(1), pp. 1-9.

Bylina, B 2018 "The block WZ factorization" *Journal of Computational and Applied Mathematics, 331*, pp. 119-132.

Bylina, B & Bylina, J 2004 "*The Vectorized and Parallelized Solving of Markovian Models for Optical Networks"* Paper presented at the International Conference on Computational Science.

Bylina, B & Bylina, J 2009 "Influence of preconditioning and blocking on accuracy in solving Markovian models" *International Journal of Applied Mathematics and Computer Science, 19*(2), pp. 207-217.

Bylina, J & Bylina, B 2016 "*Parallelizing nested loops on the Intel Xeon Phi on the example of the dense WZ factorization"* Paper presented at the Computer Science and Information Systems (FedCSIS), 2016 Federated Conference on.

Demeure, C 1989 "Bowtie factors of Toeplitz matrices by means of split algorithms. *IEEE Transactions on Acoustics, Speech, and Signal Processing, 37*(10), pp.1601-1603.

Ekert, A & Jozsa, R 1996 "Quantum computation and Shor's factoring algorithm" *Reviews of Modern Physics, 68*(3), 733.

Evans, D & Hatzopoulos, M 1979 "A parallel linear system solver" *International Journal of Computer Mathematics, 7*(3), pp. 227-238.

Evans, D 2002 "The QIF singular value decomposition method" *International Journal of Computer Mathematics, 79*(5), pp. 637-645.

Goldreich, O Goldwasser, S & Halevi, S 1997 "*Public-key cryptosystems from lattice reductionproblems"* Paper presented at the Annual International Cryptology Conference.

Guo, K & Mohar, B 2015 "Hermitian adjacency matrix of digraphs and mixed graphs" *Journal of Graph Theory, 85*(1), pp. 217-248.

Heinig, G & Rost, K 2005 "Schur-type algorithms for the solution of Hermitian Toeplitz systems via factorization" *Recent advances in operator theory and its applications* pp. 233-252, Springer.

Heinig, G & Rost, K 2011 "Fast algorithms for Toeplitz and Hankel matrices" *Linear Algebra and its Applications, 435*(1), pp. 1-59.

Liu, M Zhu, Y Shan, H & Das, K 2017 "The spectral characterization of butterfly-like graphs" *Linear Algebra and its Applications, 513*, pp. 55-68.

Nguyen, P 1999 "*Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from crypto'97"* Paper presented at the Annual International Cryptology Conference.

Ponraj, R Narayanan, S & Ramasamy, A "2015" Total mean cordiality of umbrella, butterfly and dumbbell graphs" *Jordan J. Math. and Stat.(JJMS), 8*(1), pp. 59-77.

Rao, S 1997 "Existence and uniqueness of WZ factorization" *Parallel Computing, 23*(8), pp. 1129-1139.

Rhofi, M & Ameur, A 2016 "Double power method iteration for parallel eigenvalue problem"*International Journal of Pure and Applied Mathematics, 108*(4), pp. 945-955.

Rosen, K & Krithivasan, K 2015 "*Discrete mathematics and its applications*"

Schneier, B 2007 *Applied cryptography: protocols, algorithms, and source code in C*: john wiley & sons.

Shor, P 1994 "*Algorithms for quantum computation:Discrete logarithms and factoring*. Paper presented at the Proceedings 35th annual symposium on foundations of computer science.