Additive Decompositions of Orthogonal Matrices over Finite Rings

Md Ibrahim Kholil[1], Md Mashud Parvez[2], Sujan Pant[3], Kublilay Dagtoros[4], Md Afsar Ali[5]

[1]Department of Mathematics, Norfolk State University, Norfolk, VA 23504; mikholil@nsu.edu

[2]Department of Mathematics, Dhaka University of Engineering and Technology, Gazipur, 1707, Bangladesh; mmparvez@duet.ac.bd

[3]Department of Mathematics, Norfolk State University, Norfolk, VA 23504; spant@nsu.edu

[4]Department of Mathematics, Norfolk State University, Norfolk, VA 23504; kdagtoros@nsu.edu

[5]Department of Mathematics and Computer Science, Alabama State University, Montgomery, AL 36104; mali2477@alasu.edu

Abstract:

We investigate the problem of expressing matrices over finite rings as additive sums of orthogonal matrices. Working over the modular rings $\mathbb{Z}_k$, we establish a complete positive result for all odd moduli: when $k = 2p + 1$, every matrix in $M_n(\mathbb{Z}_k)$ can be decomposed into a sum of orthogonal matrices, showing that the orthogonal group additively generates the full matrix ring. In contrast, for even moduli the situation changes drastically. We prove that in $M_2(\mathbb{Z}_4)$ strong parity obstructions arise: matrices with odd trace or odd off-diagonal sum cannot admit such decompositions. For $M_3(\mathbb{Z}_2)$ we provide a full characterization, showing that a matrix is a sum of orthogonal matrices precisely when all its row sums and column sums agree in $\mathbb{Z}_2$. These results reveal a sharp dichotomy between odd and even moduli and illustrate how the arithmetic structure of the underlying ring governs additive decomposability into orthogonal components.

1. Introduction

Matrix decompositions are fundamental tools in linear algebra, providing powerful methods for analyzing the structure of matrices and for designing efficient numerical algorithms. Classical factorizations such as the QR decomposition and the singular value decomposition (SVD) express a matrix as a product of structured components—typically orthogonal, triangular, or diagonal matrices (see [3, 10]). These multiplicative decompositions underline a wide range of modern applications, including least-squares problems, low-rank approximation, signal processing, and data analysis.

In contrast to these classical multiplicative representations, the present work investigates a fundamentally different question: when can a matrix be expressed as a sum of orthogonal matrices? Such additive decompositions have been studied over the real and complex fields by Merino [8], who characterized the additive semigroup generated by orthogonal matrices and initiated a broader examination of the algebraic structure of these sums.

Working over finite rings introduces new challenges and phenomena. Orthogonality over $\mathbb{Z}_k$ behaves differently from orthogonality over fields, due in part to the presence of zero divisors and the breakdown of many familiar geometric interpretations. Nevertheless, the algebraic definition,

$$A \in M_n(\mathbb{Z}_k) \text{ is orthogonal if and only if } A^T A = I,$$

extends naturally to modules over commutative rings [1]. The structure of orthogonal groups over finite fields and finite local rings has been investigated in areas such as modular representation

theory, finite geometry, and coding theory (see, for example, Wood [11], Pantoja–De León–Tapia Recillas [9], and Eliahou–Letertre [2]). However, the problem of additively generating matrix rings using orthogonal elements remains largely unexplored in existing literature.

This paper develops a systematic study of when a matrix in $M_n(\mathbb{Z}_k)$ can be written as a sum of orthogonal matrices, and how this property depends on the arithmetic structure of the modulus k. Our results show that decomposability behaves strikingly differently for odd and even moduli: orthogonal matrices are sufficiently abundant to generate the entire matrix ring when k is odd, whereas severe combinatorial and parity obstructions arise when k is even.

We illustrate these phenomena in detail through three cases:

- Over odd moduli $k = 2p + 1$, the orthogonal matrices additively generate the entire ring $M_n(\mathbb{Z}_{2p+1})$ for all $n \geq 2$.
- Over $\mathbb{Z}_4$, trace and parity constraints prevent certain matrices from being decomposed into sums of orthogonal matrices.
- Over $\mathbb{Z}_2$, the scarcity of orthogonal matrices leads to strong combinatorial restrictions; in particular, we prove that $A \in M_3(\mathbb{Z}_2)$ is a sum of orthogonal matrices if and only if all row sums and all column sums of A are equal.

These results reveal a rich interaction between algebraic constraints (invertibility of 2 in $\mathbb{Z}_k$), combinatorial constraints (parity patterns of rows and columns), and structural constraints (orthogonal group size) in determining additive decomposability.

This paper provides the first systematic study of sums of orthogonal matrices over finite rings $\mathbb{Z}_k$, extending the real-field analysis of Merino [8] to the modular setting. We show that for every odd modulus $k = 2p + 1$, the orthogonal matrices in $M_n(\mathbb{Z}_{2p+1})$ additively generate the entire matrix ring, establishing that every matrix admits an orthogonal sum decomposition. In contrast, for the even modulus $k = 4$, we identify structural obstructions—particularly those arising from trace and parity constraints—which demonstrate that $M_2(\mathbb{Z}_4)$ is not additively generated by its orthogonal elements. For the smallest even modulus $k = 2$, we give a complete characterization in dimension three, proving that a matrix in $M_3(\mathbb{Z}_2)$ is a sum of orthogonal matrices precisely when all its row sums and all its column sums agree, thereby uncovering a combinatorial criterion reminiscent of incidence structures in design theory. Our approach introduces a unified framework involving conjugation by permutation matrices, scalar reduction modulo k, and parity-based structural analysis, offering tools that extend naturally to higher dimensions and more general finite rings. Collectively, these results reveal how additive orthogonal decomposability over $\mathbb{Z}_k$ is dictated by the arithmetic of the modulus and by combinatorial balancing conditions absent in classical field settings, complementing earlier work on orthogonal groups over finite rings [11, 9, 2].

2. Decomposition of Orthogonal Matrices in $M_2(\mathbb{Z}_k)$

We begin our analysis with the ring $\mathbb{Z}_2$, the field of integers modulo 2. The set $M_2(\mathbb{Z}_2)$ consists of all 2×2 matrices with entries in $\mathbb{Z}_2$. Since each entry has only two possible values $(0\ or\ 1)$, the total number of distinct matrices in $M_2(\mathbb{Z}_2)$ is $2^4 = 16$. This makes it feasible to conduct a complete enumeration and inspection of all matrices in this space.

A matrix $A \in M_2(\mathbb{Z}_2)$ is said to be orthogonal if $A^T A = I$, where A^T denotes the transpose of A, and I is the 2×2 identity matrix. Over $\mathbb{Z}_2$., due to the field's characteristic being 2 $(i.e., 1 + 1 = 0)$, the usual geometric interpretation of orthogonality does not apply. However, the algebraic definition remains valid and provides a useful structural condition.

By direct computation or by referencing standard texts (see [1], [6]), one finds that there are exactly two orthogonal matrices in $M_2(\mathbb{Z}_2)$:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad P = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

These matrices satisfy $A^T A = I$ and are also involutory $(i.e., A = A^{-1})$, which is consistent with orthogonality in fields of characteristic 2.

If we restrict ourselves to using only these two orthogonal matrices and linear combinations $(mod\ 2)$, we find that the only additional matrices constructible through addition are:

$$I + P = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \quad \mathbf{0} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Hence, there are exactly four matrices in $M_2(\mathbb{Z}_2)$ expressible as sums of orthogonal matrices: $I, P, I + P$, and the zero matrix. The remaining twelve matrices cannot be represented in this way. This leaves twelve matrices in $M_2(\mathbb{Z}_2)$ that cannot be expressed as sums of orthogonal matrices. For example, consider the matrix

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

This matrix cannot be written as a linear combination $(mod\ 2)$ of I and P, and hence not as a sum of orthogonal matrices.

In fact, the scarcity of orthogonal matrices over such a small field highlights a key limitation: the set of orthogonal matrices is not additive generating in $M_2(\mathbb{Z}_2)$. Additionally, the ring structure of $\mathbb{Z}_2$ contributes to constraints on matrix decompositions—particularly because scalar diversity and invertibility are minimal.

This example underscores a deeper phenomenon: in rings with small characteristics, the set of orthogonal matrices is often too limited to generate all matrices additively. Similar phenomena occur in $M_2(\mathbb{Z}_4)$, where trace and parity arguments provide further obstructions to decomposition into orthogonal components. This observation naturally raises the question of when the entire matrix ring $M_2(\mathbb{Z}_n)$can be generated additively by its orthogonal elements. If even one elementary matrix can be expressed as a sum of orthogonal matrices, then by conjugation and scalar combinations, all other matrix units can be obtained, and consequently every element of $M_2(\mathbb{Z}_n)$ can be represented in this way. The following lemma formalizes this key reduction.

Lemma 2.1. Let n $\geq$ 2 be a given integer. Suppose that $E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbb{Z}_n)$ can be written as a sum of orthogonal matrices. Then every matrix in $M_2(\mathbb{Z}_n)$ can be expressed as a sum of orthogonal matrices.

Proof. Assume that E_{11} is a sum of orthogonal matrices. Let $P = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$which is orthogonal since $P^T P = I$. Observe that conjugation by P permutes the positions of the nonzero entries in a matrix. In particular, we have

$$E_{11} P = E_{12}, \quad PE_{11} = E_{21}, \quad PE_{11} P = E_{22}.$$

Because conjugation and multiplication by orthogonal matrices preserve orthogonality, each of the matrices E_{12}, E_{21}, and E_{22} can also be expressed as sums of orthogonal matrices.

Thus, all four standard matrix units

$$E_{11},\ E_{12},\ E_{21},\ E_{22}$$

are sums of orthogonal matrices. Every matrix $A = [a_{ij}] \in M_2(\mathbb{Z}_n)$ can be written as a linear combination:

$$A = a_{11}E_{11} + a_{12}E_{12} + a_{21}E_{21} + a_{22}E_{22},$$

so it remains to show that each scalar multiple aE_{ij} can also be expressed as a sum of orthogonal matrices.

Let $a \in \mathbb{Z}_{\text{n}}$. By the definition of modular arithmetic, a can be represented as a sum of a copies of 1:

$$aE_{ij} = \underbrace{E_{ij} + E_{ij} + \cdots + E_{ij}}_{a\ times}$$

Since E_{ij} is a sum of orthogonal matrices, and the sum of any finite number of orthogonal matrices is again a sum of orthogonal matrices, it follows that aE_{ij} is also a sum of orthogonal matrices.

Therefore, every matrix in $M_2(\mathbb{Z}_n)$, being a linear combination of the matrix units with coefficients from $\mathbb{Z}_n$, can be written as a sum of orthogonal matrices.

We now apply the preceding lemma to the case of odd moduli. The following computation shows explicitly that the hypothesis of the lemma holds when $n = 2p + 1$. Indeed, the standard matrix unit E_{11} can be expressed as a sum of orthogonal matrices, which implies—by the lemma—that all matrices in $M_2(\mathbb{Z}_{2p+1})$ admit such a decomposition.

Now note that the four matrices:

$$E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},\ E_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},\ E_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},\ E_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

are the standard matrix units in $M_2(\mathbb{Z}_n)$ and now known to be sums of orthogonal matrices. Therefore, any matrix in $M_2(\mathbb{Z}_n)$can be constructed by taking linear combinations of these basic matrices with scalars from $\mathbb{Z}_n$.

Now suppose $n = 2p + 1$ for some positive integer p. Consider the matrix

$$\begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Both summands are orthogonal matrices in $M_2(\mathbb{Z}_{2p+1})$. Hence, the matrix $\begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$ is a sum of orthogonal matrices.

Now multiply this matrix by $(p + 1) \in \mathbb{Z}_{2p+1}$:

$$(p + 1)\begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},$$

since $2(p + 1) \equiv 1\ (mod\ 2p + 1)$. Therefore, $\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}$ can be written as a sum of orthogonal matrices, and hence, by the argument above, every matrix in $M_2(\mathbb{Z}_{2p+1})$ can be written as a sum of orthogonal matrices.

The computation above verifies that for odd moduli $n = 2p + 1$, the matrix E_{11} can indeed be expressed as a sum of orthogonal matrices. Hence, the hypothesis of the lemma holds in this case, leading directly to the following corollary.

Corollary 2.2. Let $n = 2p + 1$ be an odd integer. Every matrix in $M_2(\mathbb{Z}_{2p+1})$ can be written as a sum of orthogonal matrices.

Proof. We will show that the hypothesis of the preceding lemma holds for $E_{11} = \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} \in M_2(\mathbb{Z}_{2p+1})$.

Consider the diagonal matrices

$$D_1 = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix},\ I = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}.$$

Both D_1 and I are orthogonal in $M_2(\mathbb{Z}_{2p+1})$ because

$$D_1^T D_1 = diag(1^2, (-1)^2) = diag(1,1) = I, \quad I^T I = I.$$

Their sum equals

$$D_1 + I = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix} + \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} = \begin{bmatrix}2 & 0\\0 & 0\end{bmatrix} = 2E_{11}.$$

Hence $2E_{11}$ is a sum of orthogonal matrices.

In the ring $\mathbb{Z}_{2p+1}$ the element 2 is a unit: its multiplicative inverse is $p + 1$ because

$$2(p + 1) = 2p + 2 \equiv 1\ (mod\ 2p + 1).$$

Therefore

$$E_{11} = (p + 1) \cdot (2E_{11}),$$

and since scalar multiplication by $p + 1$ amounts to adding $2E_{11}$ to itself $p + 1$ times, it follows that E_{11} is a sum of orthogonal matrices as well.

Having established that E_{11} is a sum of orthogonal matrices, the lemma applies: by conjugation with the permutation matrix $P = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ we obtain the other matrix units E_{12}, E_{21}, E_{22} as sums of orthogonal matrices, and scalar multiples aE_{ij} are sums of orthogonal matrices by repeated addition. Hence every element of $M_2(\mathbb{Z}_{2p+1})$ is a sum of orthogonal matrices.

3. Decomposition of Orthogonal Matrices in $M_n(\mathbb{Z}_{2p+1})$

We now turn our attention to the additive generation of matrix rings over odd moduli. The case of $M_2(\mathbb{Z}_{2p+1})$provides the foundation for the general result, showing that the presence of an odd modulus ensures the existence of additive orthogonal decompositions for all matrices.

Theorem 3.1. Let p be a positive integer. Then every matrix in $M_2(\mathbb{Z}_{2p+1})$ can be written as a sum of orthogonal matrices in $M_2(\mathbb{Z}_{2p+1})$.

Proof. Let

$$E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

By Lemma 2.1, if E_{11} can be expressed as a sum of orthogonal matrices, then every 2×2 matrix over $\mathbb{Z}_{2p+1}$ can be expressed similarly.

In $\mathbb{Z}_{2p+1}$, observe that

$$\begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and both summands are orthogonal because

$$\begin{bmatrix} 1 & 0 \\ 0 & \pm 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & \pm 1 \end{bmatrix}^T = I.$$

Multiplying by $(p + 1)$ in $\mathbb{Z}_{2p+1}$ gives

$$(p + 1)\begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = E_{11}.$$

Hence E_{11} is a sum of orthogonal matrices, and therefore every matrix in $M_2(\mathbb{Z}_{2p+1})$ can be expressed as a sum of orthogonal matrices.

Having verified the 2×2 case, we now extend this property to arbitrary dimensions. The next result establishes that the orthogonal matrices over $\mathbb{Z}_{2p+1}$ generate the full matrix ring additively.

Theorem 3.2. Let n and p be positive integers. Then every matrix in $M_n(\mathbb{Z}_{2p+1})$ can be written as a sum of orthogonal matrices in $M_n(\mathbb{Z}_{2p+1})$.

Proof. Let E_{ij} denote the standard matrix unit with 1 in the (i, j) position and 0 elsewhere. From Corollary 2.2, we know that E_{11} can be written as a sum of orthogonal matrices. Since $E_{ij} = P\,E_{11}\,Q$ for suitable permutation matrices P and Q, and permutation matrices are

orthogonal ($P\,P^T = Q\,Q^T = I$), each E_{ij} can likewise be expressed as a sum of orthogonal matrices.

Furthermore, for any $a \in \mathbb{Z}_{2p+1}$, the scalar multiple aE_{ij} is a sum of a copies of E_{ij}, hence also a sum of orthogonal matrices. Since every matrix in $M_n(\mathbb{Z}_{2p+1})$ can be expressed as a $\mathbb{Z}_{2p+1}$-linear combination of the E_{ij}, the result follows.

Case of $\mathbb{Z}_4$:

We now turn our attention to the case of even modulus, beginning with matrices over $\mathbb{Z}_4$. Unlike the situation for odd moduli, where additive decomposability is unrestricted, the presence of zero divisors in $\mathbb{Z}_4$ introduces new algebraic constraints on orthogonality. In particular, parity conditions emerge as key obstructions to expressing arbitrary matrices as sums of orthogonal matrices. To analyze these structural limitations, we first examine the necessary conditions on the entries of an orthogonal matrix in $M_2(\mathbb{Z}_4)$. The following lemma establishes simple yet fundamental parity relations that all such matrices must satisfy.

Lemma 3.3. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}_4)$ be orthogonal. Then $a + b, b + d, c + d$, and $a + c$ are all odd.

Proof. Since A is orthogonal, we have $A^T A = I$. Compute:

$$A^T A = \begin{bmatrix} a^2 + c^2 & ac + bd \\ ac + bd & c^2 + d^2 \end{bmatrix}.$$

So, we have $a^2 + c^2 = 1$, which implies $a + c$ is odd in $\mathbb{Z}_4$ (only one of them is odd). Similarly, $b^2 + d^2 = 1$ implies $b + d$ is odd.

Now compute AA^T:

$$AA^T = \begin{bmatrix} a^2 + b^2 & ac + bd \\ ac + bd & c^2 + d^2 \end{bmatrix}.$$

This gives $a^2 + b^2 = 1$ and $c^2 + d^2 = 1$, hence $a + b$ and $c + d$ are also odd.

Lemma 3.3 establishes that orthogonality in $M_2(\mathbb{Z}_4)$ imposes strict parity constraints on adjacent entries of the matrix. These local parity relations already hint that orthogonal matrices over $\mathbb{Z}_4$ occupy a highly restricted subset of the full matrix space. To understand the global consequences of these constraints, it is natural to examine how they affect key matrix invariants such as the trace and the sum of the off-diagonal entries. The following theorem formalizes this observation by showing that, for any orthogonal matrix in $M_2(\mathbb{Z}_4)$, both the trace and the sum of the off-diagonal elements must be even. This result further illustrates how parity structure fundamentally governs orthogonality in rings with nontrivial zero divisors.

Theorem 3.4. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}_4)$ be orthogonal. Then the trace $tr(A) = a + d$ is even, and $b + c$ is also even.

Proof. From Lemma 3.3, $a + b$ and $b + d$ are odd, so $a + d + 2b$ is even, implying $a + d$ is even. Similarly, $a + c$ and $c + d$ being odd implies $b + c$ is even.

Now let $A \in M_2(\mathbb{Z}_4)$ be given. If A is a sum of orthogonal matrices, say

$$A = Q_1 + Q_2 + \cdots + Q_k,$$

then

$$tr(A) = \sum_{m=1}^{k} tr(Q_m)$$

is a sum of even numbers, hence even. But consider the matrix

$$B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

Its trace is 1, which is odd, so it cannot be a sum of orthogonal matrices.

Corollary 3.5. There exists a matrix in $M_2(\mathbb{Z}_4)$ that cannot be written as a sum of orthogonal matrices in $M_2(\mathbb{Z}_4)$.

Matrix decompositions into sums of orthogonal matrices are well understood over fields such as $\mathbb{R}$ and $\mathbb{C}$, where orthogonal and unitary matrices play a central role in numerous applications. However, over commutative rings with zero divisors, such as $\mathbb{Z}_4$, these classical results often fail. The ring $\mathbb{Z}_4$ is neither a field nor an integral domain, and its algebraic structure significantly restricts the set of orthogonal and invertible matrices.

Corollary 3.5 illustrates this limitation by showing that there exists a matrix in $M_2(\mathbb{Z}_4)$ that cannot be written as a sum of orthogonal matrices. This failure is rooted in the presence of zero divisors and the resulting constraints on matrix behavior. As noted by Wood [11], such structural properties affect module duality and orthogonality over finite rings. Further analysis by Pantoja, De León, and Tapia-Recillas [9] confirms that orthogonal matrices over finite local rings are subject to

stricter conditions, reinforcing the conclusion that orthogonal decompositions are fundamentally limited in $M_2(\mathbb{Z}_4)$.

4 Decomposition of Orthogonal Matrices in $M_3(\mathbb{Z}_2)$

Let $n \geq 2$ and $k \geq 2$ be integers and consider $M_n(\mathbb{Z}_k)$, the ring of $n \times n$ matrices over the ring $\mathbb{Z}_k$. A fundamental class of orthogonal matrices in this context arises from permutation matrices. A matrix $P \in M_n(\mathbb{Z}_k)$ is a permutation matrix if it contains exactly one entry equal to 1 in each row and each column, with all other entries equal to 0. These matrices satisfy $P\,P^T = I$, and are thus orthogonal in the standard sense that $A^T A = I$ (see [6]).

Let $J \in M_n(\mathbb{Z}_k)$ denote the matrix in which all entries are 1. When $k = 2$ and n is even, interesting structural identities emerge due to the arithmetic of $\mathbb{Z}_2$. Specifically, $J^2 = 0$, since in $\mathbb{Z}_2$the sum of any even number of 1s is 0. Moreover, J is symmetric, so $J^T = J$.

Now let $Q \in M_n(\mathbb{Z}_2)$ be a permutation matrix. Since permutation matrices preserve the all-ones vector under multiplication, we observe that $Q\,J^T = J\,Q^T = J$. Consider the matrix $Q + J$. We compute:

$$(Q + J)(Q + J)^T = Q\,Q^T + Q\,J^T + J\,Q^T + J^2 = I + J + J + 0 = I.$$

Hence, $Q + J$ is orthogonal. For $n \geq 4$, such matrices are not themselves permutation matrices. This reveals that the class of orthogonal matrices in $M_n(\mathbb{Z}_2)$ extends beyond permutations when n is even and sufficiently large.

When $n = 2$, however, the situation is more restrictive. The only orthogonal matrices in $M_2(\mathbb{Z}_2)$are the identity and the flip matrix, i.e., the two permutation matrices. This fact aligns with earlier classifications of matrix behavior over small finite fields (cf. [9], [11]).

The case $n = 3$ introduces additional complexity. In this case, $J^2 = J$, and so the argument used for even n fails. Consider a matrix $A = [a_{ij}] \in M_3(\mathbb{Z}_2)$. If A is orthogonal, then $A\,A^T = I$, which implies that the dot product of each row with itself is 1. Because $a^2 = a$ for all $a \in \mathbb{Z}_2$, we find that:

$$a_{i1}^2 + a_{i2}^2 + a_{i3}^2 = a_{i1} + a_{i2} + a_{i3} = 1,$$

for each $i = 1, 2, 3$. Thus, each row of A contains exactly one entry equal to 1 and two entries equal to 0. A similar argument applied to $A^T A = I$ shows that each column must satisfy the same condition.

It follows that the orthogonal matrices in $M_3(\mathbb{Z}_2)$ are precisely the 3×3 permutation matrices. This result illustrates how the field structure of $\mathbb{Z}_2$, combined with matrix dimension, governs the extent of orthogonality and its deviation from richer field behaviors. These findings are consistent with structural results on orthogonality and matrix decomposition over finite local rings and finite fields as discussed in [9], [11], and [6].

The preceding results in lower-dimensional settings illustrate how orthogonality over modular rings imposes strong combinatorial and arithmetic restrictions on matrix entries. To further explore this phenomenon, we now turn to the case of $M_3(\mathbb{Z}_2)$, where the binary nature of the ring introduces additional structural symmetry. In this setting, orthogonality translates into precise conditions on the distribution of ones within rows and columns. The next theorem provides a complete characterization of these conditions, showing that every orthogonal matrix in $M_3(\mathbb{Z}_2)$ must have exactly one entry equal to~1 in each row and each column—a property reminiscent of permutation matrices.

Theorem 4.1. Let $Q \in M_3(\mathbb{Z}_2)$ be orthogonal. Then each row and each column of Q has exactly one entry equal to 1. In particular, the sum of the entries in each row and in each column is 1.

Proof. Assume that $Q \in M_3(\mathbb{Z}_2)$ is orthogonal. Then, by definition, we have

$$Q\,Q^T = I,$$

where I is the 3×3 identity matrix. Let q_1, q_2, q_3 denote the row vectors of Q. The matrix product $Q\,Q^T$ has (i,j)-entry equal to the dot product $q_i \cdot q_j$ for all $i,j \in \{1,2,3\}$. Therefore,

$$q_i \cdot q_j = \delta_{ij}$$

where δ_{ij} is the Kronecker delta.

Now, fix $i \in \{1,2,3\}$. Since $q_i \cdot q_j = 1$, the dot product of the i-th row with itself is equal to 1 in $\mathbb{Z}_2$. Note that in $\mathbb{Z}_2$, each element satisfies $a^2 = a$ and $a + a = 0$. Hence, for $q_i = (q_{i1}, q_{i2}, q_{i3}) \in \mathbb{Z}_2^3$, we have

$$q_i \cdot q_i = q_{i1}^2 + q_{i2}^2 + q_{i3}^2 = q_{i1}, + q_{i2} + q_{i3} = 1.$$

.

Thus, the sum of the entries in each row is 1.

A similar argument applies to the columns of Q. Since Q is orthogonal, we also have $Q^T Q = I$. Denoting the columns of Q by c_1, c_2, c_3, the same reasoning shows that

$$c_j \cdot c_j = 1 \ for\ all\ j \in \{1,2,3\},$$

which implies that the sum of entries in each column is also 1.

Therefore, every row and every column of Q contain exactly one entry equal to 1, and the remaining entries are 0.

Let $A \in M_3(\mathbb{Z}_2)$ be a sum of orthogonal matrices, say $A = Q_1 + \cdots + Q_k$, where each Q_i is orthogonal. If k is even, the row and column sums of A are all 0. If k is odd, the row and column sums of A are all 1.

Let $Q \in M_3(\mathbb{Z}_2)$ be orthogonal. Then each row and column contains either one or three entries equal to 1. If there is exactly one 1 in each row and column, then Q is a permutation matrix.

Suppose Q has a row of all 1s. Multiply Q by a permutation matrix P so that the first row of PQ is [1 1 1]. The second row must contain either one 1 or three 1s. If the second row is also all 1s, then the sum of the columns is 2, which is not valid. So, the second row must have exactly one 1. Multiply on the left by a permutation S so that the second row becomes [1 0 0]. Then:

$$P\,Q\,S = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

is not orthogonal.

Therefore, the only orthogonal matrices in $M_3(\mathbb{Z}_2)$ are the permutation matrices:

$$Q_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ Q_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, Q_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix},$$

$$Q_4 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, Q_5 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},\ Q_6 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

From the above argument, it becomes evident that any attempt to construct an orthogonal matrix in $M_3(\mathbb{Z}_2)$ containing a row of all ones inevitably leads to inconsistency with the orthogonality condition. The inner product structure in $\mathbb{Z}_2$ imposes strong combinatorial restrictions: each row must contain an odd number of ones, yet mutual orthogonality requires that the pairwise dot products of distinct rows vanish. This tension rules out configurations with rows of weight three, leaving only those with exactly one entry equal to one in each row. Consequently, any orthogonal matrix over $\mathbb{Z}_2$ of order three must have precisely one 1 per row and per column, that is, it must

be a permutation matrix. The six possible such matrices are listed above. This reasoning leads directly to the following fundamental characterization.

Theorem 4.2. Let $Q \in M_3(\mathbb{Z}_2)$. Then Q is orthogonal if and only if Q is a permutation matrix.

Proof. Suppose Q is orthogonal, i.e., $Q\,Q^T = I$. This implies that the rows of Q form an orthonormal set in the vector space $(\mathbb{Z}_2)^3$, equipped with the standard dot product. Since $\mathbb{Z}_2$ has characteristic 2, we have $a^2 = a$ and $a + a = 0$ for all $a \in \mathbb{Z}_2$. Hence, for any vector $v = (v_1, v_2, v_3) \in (\mathbb{Z}_2)^3$, the dot product with itself satisfies

$$\langle v, v\rangle = v_1^2 + v_2^2 + v_3^2 = v_1 + v_2 + v_3$$

Therefore, the dot product of each row of Q with itself equals the sum of its entries, which must be 1. Thus, each row contains exactly one or three entries equal to 1.

Now consider the pairwise orthogonality of distinct rows. Suppose one row of Q is $(1, 1, 1)$; then the dot product with any other row is also 1 (since all entries are 1), violating orthogonality. Hence, no row can contain three 1s. Thus, each row of Q must contain exactly one 1. A similar argument applied to the columns of Q (using $Q^T\,Q = I$) shows that each column must also contain exactly one 1.

Therefore, Q has exactly one entry equal to 1 in each row and column, and the remaining entries are 0. This is precisely the definition of a permutation matrix.

Conversely, every permutation matrix is known to satisfy $Q^T Q = I$, since permuting rows or columns of the identity matrix preserves orthogonality. Thus, any permutation matrix is orthogonal.

We conclude that Q is orthogonal if and only if Q is a permutation matrix.

5. Result, Discussion and Conclusion

The characterization established in Theorem 3.4 highlights a unifying principle in the study of additive orthogonal decompositions over finite rings: the possibility of expressing a matrix as a sum of orthogonal matrices depends intricately on both algebraic and combinatorial constraints. Specifically, for $M_3(\mathbb{Z}_2)$, the equality of all row and column sums provides a complete and elegant criterion for additive decomposability. This result demonstrates how structural restrictions inherent in $\mathbb{Z}_2$ govern orthogonality and matrix decomposition behavior, showing that orthogonal summability in modular settings arises from the interplay between algebraic orthogonality and combinatorial uniformity inherent to finite arithmetic.

These findings fit naturally into the broader framework established in earlier sections. In Theorem 3.2, we proved that every matrix in $M_n(\mathbb{Z}_{2p+1})$, where $2p+1$ is an odd prime power, can be written as a sum of orthogonal matrices, thereby showing that orthogonal matrices in this setting generate the entire matrix ring additively. In contrast, Corollary 3.5 revealed a structural limitation

in $M_2(\mathbb{Z}_4)$: not every matrix can be decomposed into orthogonal summands due to parity restrictions and the presence of zero divisors in $\mathbb{Z}_4$.

Theorem 3.4 complements these results by showing that for $M_3(\mathbb{Z}_2)$, additive decomposability is characterized precisely by a parity-based invariant—namely, the uniformity of row and column sums. This provides a combinatorial analogue of the algebraic constraints identified in Corollary 3.5, reinforcing that the arithmetic structure of the underlying ring, particularly its parity and zero-divisor properties, governs orthogonal decomposition behavior.

Together, Lemma 3.3, Theorem 3.4 and Corollary 3.5 illustrate a rich dichotomy between odd and even moduli: over odd moduli such as $\mathbb{Z}_{2p+1}$, additive orthogonal completeness holds universally, while over even moduli such as $\mathbb{Z}_2$ and $\mathbb{Z}_4$, additional parity conditions restrict the decomposability of matrices.

Future research will aim to extend these results to higher dimensions, particularly $M_n(\mathbb{Z}_k)$, with $n > 3$ and even moduli k, where more complex behavior is anticipated due to the abundance of zero divisors and nontrivial idempotent elements. Additionally, exploring connections with coding theory, design theory, and modular orthogonal groups may reveal deeper structural parallels between algebraic decompositions and combinatorial constructions over finite rings.

References

[1] J. DeFranza and D. Gagliardi. Introduction to Linear Algebra with Applications. First Edition, McGraw-Hill, New York, NY, 2009.

[2] S. Eliahou and F. Letertre, Orthogonal matrices over finite local rings of length two, Linear Algebra and its Applications, 659, 147–172, 2023.

[3] G. H. Golub and C. F. Van Loan, Matrix Computations, Fourth Edition, Johns Hopkins University Press, 2013.

[4] R. A. Horn and C. R. Johnson, Matrix Analysis, Second Edition, Cambridge University Press, 2013.

[5] D. C. Lay, Linear Algebra and Its Applications, 4th Edition, Pearson, 2011.

[6] R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, 1994.

[7] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1977.

[8] D. I. Merino, The sum of orthogonal matrices, Linear Algebra and its Applications, 436(7), 0024-3795, 2012.

[9] J. A. Pantoja, H. A. De León, and H. Tapia-Recillas, Orthogonal matrices over finite local rings, Linear Algebra and its Applications, 478, 73–90, 2015.

[10] L. N. Trefethen and D. Bau, Numerical Linear Algebra. SIAM, Philadelphia, 1997.

[11] J. A. Wood, Duality for modules over finite rings and applications to coding theory, American Journal of Mathematics, 121(3), 555–575, 1999.