Gulf Journal of Mathematics
Vol 23, Issue 1 (2026) 1-24

ISSN: 2309-4966
https://doi.org/10.56947/zt9mys24

PARITY OBSTRUCTIONS AND ADDITIVE ORTHOGONAL DECOMPOSITIONS OVER THE RINGS $\mathbb{Z}_{2^r}$

MD MASHUD PARVEZ[1*], MD IBRAHIM KHOLIL[2], KAPILA KOTTEGODA[2], SUJAN PANT[2] and KUBLILAY DAGTOROS[2]

Abstract. We study additive decompositions of matrices over the rings $\mathbb{Z}_{2^r}$ into sums of orthogonal matrices. Unlike the odd-modulus case, where orthogonal matrices generate the full matrix ring, the even-modulus case exhibits parity obstructions due to the non-invertibility of 2. We establish necessary conditions based on reduction modulo 2, trace parity, and row/column balance. In low dimensions, we recover known obstructions and provide explicit constructions when these conditions are satisfied. We further propose a classification framework based on finitely many $\mathbb{Z}_2$-valued invariants and state related conjectures and open problems.

Keywords. Finite rings, modular matrices, orthogonal group, additive decomposition, parity obstruction.
2020 Mathematics Subject Classification. Primary 15A33; Secondary 15B33, 11C20, 13M05

1. Introduction

Matrix decompositions constitute a fundamental component of linear algebra, underpinning both theoretical developments and computational methodologies. Standard matrix factorizations, including LU, QR, and singular value decomposition (SVD), represent matrices as products of structured components and are fundamental tools in numerical analysis, optimization, and applied mathematics; see [3, 6, 9, 18]. These factorizations exploit algebraic and geometric properties of matrix groups and have been extensively studied over fields.

Complementary to multiplicative factorizations, one may consider *additive decompositions*, where a matrix is written as a finite sum of elements from a prescribed class. Such problems arise naturally in the study of additive generation in rings, convexity questions in matrix spaces, and structural investigations of algebraic subsets of $\mathcal{M}_n(R)$. In particular, additive semigroups generated by special matrix classes provide insight into how algebraic constraints influence global structure; see [2, 11, 16, 19].

Date: Received: Apr 16, 2026; Revised: April 29, 2026; Accepted: May 10, 2026.
* Corresponding author

Among structured matrix classes, orthogonal matrices occupy a distinguished position. Over $\mathbb{R}$ and $\mathbb{C}$, the geometry of the orthogonal and unitary groups yields deep connections to spectral theory, operator inequalities, and convex analysis; see [1, 9]. Additive questions involving orthogonal matrices have also been explored in various contexts, including sums of orthogonal matrices and their structural limitations [13].

In contrast, the behavior of orthogonal matrices over rings that are not fields remains comparatively less understood. Let $k \geq 2$ and consider the residue ring $\mathbb{Z}_k$. The matrix ring $\mathcal{M}_n(\mathbb{Z}_k)$ exhibits rich algebraic structure influenced by the arithmetic of $\mathbb{Z}_k$, particularly when k is composite. A matrix $Q \in \mathcal{M}_n(\mathbb{Z}_k)$ is called orthogonal if it satisfies

$$Q^T Q = I_n,$$

and the collection of such matrices forms the group $\mathcal{O}_n(\mathbb{Z}_k)$. For background on classical groups over rings, we refer to [4, 7, 8].

When k is prime, $\mathbb{Z}_k$ is a finite field and the structure of $\mathcal{O}_n(\mathbb{Z}_k)$ is well understood within the theory of finite classical groups [12]. However, when k is composite, the presence of zero divisors fundamentally alters the algebraic landscape. In particular, orthogonality must be understood in the context of bilinear forms over rings, where invertibility conditions and quadratic relations behave differently than over fields [14, 20].

A central phenomenon that arises in this setting is a sharp *odd–even dichotomy*. When k is odd, the element 2 is invertible in $\mathbb{Z}_k$, which allows for flexible manipulation of quadratic expressions and enables a rich supply of orthogonal matrices. In our earlier work [10], we showed that in this case the additive semigroup generated by $\mathcal{O}_n(\mathbb{Z}_k)$ coincides with the entire matrix ring $\mathcal{M}_n(\mathbb{Z}_k)$ for $n \geq 2$.

The situation changes dramatically when k is even. In this case, 2 is a zero divisor, and the orthogonality condition imposes rigid arithmetic constraints. These manifest as parity restrictions on entries, trace conditions, and combinatorial limitations inherited from reduction modulo 2. Even at the base level $\mathbb{Z}_2$, orthogonality encodes nontrivial combinatorial structure, which propagates to higher powers of 2. As a consequence, additive generation fails in general, and explicit obstructions arise.

The purpose of this paper is to undertake a systematic investigation of additive decompositions over the family of rings

$$\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_8, \ldots, \mathbb{Z}_{2^r}.$$

This hierarchy provides a natural framework for analyzing how structural constraints evolve along the 2-adic tower. Reduction maps between these rings allow one to transfer information from $\mathbb{Z}_{2^r}$ to $\mathbb{Z}_2$, where combinatorial methods become effective. At the same time, lifting problems introduce new phenomena arising from nilpotent elements, leading to a layered and intricate structure.

This work makes two primary contributions. First, we identify necessary conditions for additive decomposability arising from parity constraints and reduction invariants. Second, we analyze the extent to which these constraints determine the additive semigroup generated by orthogonal matrices over $\mathbb{Z}_{2^r}$. Our results extend previous work on $\mathbb{Z}_4$ and $\mathcal{M}_3(\mathbb{Z}_2)$ to arbitrary powers of 2, providing a unified structural perspective.

This study also connects to broader questions concerning the generation of rings by special subsets, including idempotents, involutions, and classical group elements; see [5, 11]. The orthogonal case over modular rings presents a particularly rich interaction between algebraic structure and arithmetic constraints.

We begin by establishing the algebraic framework and notation, emphasizing reduction maps and orthogonality over modular rings. We then analyze parity constraints and additive invariants, followed by constructive decompositions and obstruction results. Finally, we develop a classification framework for additive generation over $\mathbb{Z}_{2^r}$.

2. Preliminaries

Throughout this paper, we fix an integer $r \geq 1$ and work over the finite ring $R = \mathbb{Z}_{2^r}$. Unlike fields, the ring R contains nontrivial nilpotent elements and zero divisors when $r \geq 2$, which significantly influences the behavior of matrix equations. In particular, the failure of 2 to be invertible introduces constraints that are central to our analysis.

We write $\mathcal{M}_n(R)$ for the ring of all $n \times n$ matrices with entries in R, endowed with the usual matrix addition and multiplication. The set of units in this ring constitutes the general linear group $\mathrm{GL}_n(R)$. The properties of such matrix rings over finite rings have been extensively explored in algebra and coding theory; see [5, 20].

The collection of all such matrices constitutes the orthogonal group $\mathcal{O}_n(R)$. This definition generalizes the classical notion of orthogonality, but in the present setting it is purely algebraic and must be interpreted within the arithmetic constraints of R. For detailed treatments of orthogonal groups over rings, see [7, 8, 14].

The primary object of investigation is the additive semigroup generated by $\mathcal{O}_n(R)$. We consider matrices representable as sums of a finite number of orthogonal matrices and examine whether such representations generate the full matrix ring $\mathcal{M}_n(R)$. This problem bridges additive algebra and the theory of matrix groups.

A key tool in our analysis is the use of reduction maps. For each $1 \leq s \leq r$, the natural projection

$$\pi_s : \mathbb{Z}_{2^r} \to \mathbb{Z}_{2^s}$$

extends entrywise to matrices:

$$\pi_s : \mathcal{M}_n(\mathbb{Z}_{2^r}) \to \mathcal{M}_n(\mathbb{Z}_{2^s}).$$

In particular, reduction modulo 2 plays a fundamental role. For a matrix $A \in \mathcal{M}_n(R)$, we denote its image in $\mathcal{M}_n(\mathbb{Z}_2)$ by $\overline{A}$.

Orthogonality is preserved under reduction: if $Q \in \mathcal{O}_n(\mathbb{Z}_{2^r})$, then $\overline{Q} \in \mathcal{O}_n(\mathbb{Z}_2)$. This observation allows one to transfer structural properties from $\mathbb{Z}_{2^r}$ to $\mathbb{Z}_2$, where the combinatorial nature of orthogonality becomes more transparent.

The orthogonality condition yields a system of quadratic relations among the entries of Q. Writing $Q = [q_{ij}]$, we obtain

$$\sum_{k=1}^{n} q_{ki}q_{kj} = \delta_{ij}, \qquad \sum_{k=1}^{n} q_{ik}q_{jk} = \delta_{ij},$$

for all $1 \leq i, j \leq n$, where δ_{ij} is the Kronecker delta. These identities express the orthogonality of columns and rows, respectively.

Over $\mathbb{Z}_{2^r}$, these relations impose strong parity constraints, particularly through the diagonal conditions $\sum_{k=1}^{n} q_{ki}^2 = 1$. Upon reduction modulo 2, such constraints translate into combinatorial restrictions that govern the structure of orthogonal matrices.

These interactions between orthogonality, reduction, and parity form the foundation of our approach to additive generation in $\mathcal{M}_n(\mathbb{Z}_{2^r})$.

3. Parity constraints over $\mathbb{Z}_{2^r}$

A defining feature of orthogonal matrices over the ring $\mathbb{Z}_{2^r}$ is the presence of strong parity constraints. Unlike the case of odd modulus, where 2 is a unit and orthogonality behaves more flexibly, the failure of invertibility of 2 forces arithmetic restrictions on matrix entries, row and column structures, and global invariants such as the trace. These constraints play a decisive role in determining the structure of the additive semigroup generated by orthogonal matrices.

Let $Q = [q_{ij}] \in O_n(R)$, where $R = \mathbb{Z}_{2^r}$. The defining relation $Q^TQ = I$ yields the identities

$$\sum_{k=1}^{n} q_{ki}q_{kj} = \delta_{ij}, \tag{3.1}$$

$$\sum_{k=1}^{n} q_{ik}q_{jk} = \delta_{ij}, \tag{3.2}$$

for all $1 \leq i, j \leq n$, where δ_{ij} denotes the Kronecker delta.

These relations encode orthogonality of columns and rows, respectively. Over $\mathbb{Z}_{2^r}$, they impose nontrivial arithmetic constraints because squares and cross-products behave differently than over fields.

When $i = j$, equations (3.1) and (3.2) imply that each column and each row satisfies a quadratic norm condition. In particular,

$$\sum_{k=1}^{n} q_{ki}^2 = 1,$$

which forces a parity condition after reduction modulo 2.

We now examine the structure induced by reduction modulo 2, which reveals fundamental combinatorial constraints.

Lemma 3.1 (Odd weight condition)**.** *Let $Q \in O_n(\mathbb{Z}_{2^r})$ and let $\overline{Q}$ denote its reduction modulo 2. Then every row and every column of $\overline{Q}$ has odd Hamming weight.*

Proof. We give a detailed argument based on the orthogonality relations and properties of arithmetic in $\mathbb{Z}_2$.

Since $Q \in O_n(\mathbb{Z}_{2^r})$, by definition we have

$$Q^T Q = I_n \quad \text{in } M_n(\mathbb{Z}_{2^r})\,.$$

Let $\pi_1 : \mathbb{Z}_{2^r} \to \mathbb{Z}_2$ denote the natural reduction map, applied entrywise to matrices. Denote $\overline{Q} = \pi_1(Q)$. Since π_1 is a ring homomorphism, it preserves matrix multiplication and transpose, and hence

$$\overline{Q}^T \overline{Q} = I_n \quad \text{in } M_n(\mathbb{Z}_2)\,.$$

Let $\overline{Q} = [\overline{q}_{ij}]$. Fix a column index j with $1 \le j \le n$. Consider the (j, j)-entry of the matrix product $\overline{Q}^T \overline{Q}$.

Applying the definition of matrix multiplication, we get

$$(\overline{Q}^T \overline{Q})_{jj} = \sum_{k=1}^{n} \overline{q}_{kj}\, \overline{q}_{kj} = \sum_{k=1}^{n} \overline{q}_{kj}^2.$$

Since $\overline{Q}^T \overline{Q} = I_n$, the (j, j)-entry equals 1 in $\mathbb{Z}_2$.

Thus,

$$\sum_{k=1}^{n} \overline{q}_{kj}^2 = 1 \quad \text{in } \mathbb{Z}_2.$$

In the field $\mathbb{Z}_2$, every element satisfies $x^2 = x$ for all $x \in \mathbb{Z}_2$. Indeed, this holds since $\mathbb{Z}_2 = \{0, 1\}$ and $0^2 = 0$, $1^2 = 1$.

Hence,

$$\overline{q}_{kj}^2 = \overline{q}_{kj} \quad \text{for all } k.$$

Substituting into the previous identity gives

$$\sum_{k=1}^{n} \overline{q}_{kj} = 1 \quad \text{in } \mathbb{Z}_2.$$

The quantity $\sum_{k=1}^{n} \overline{q}_{kj}$ in $\mathbb{Z}_2$ represents the sum of the entries in column j modulo 2. Since each entry is either 0 or 1, this sum is equal to the Hamming weight (i.e., the number of nonzero entries) of the column, taken modulo 2.

So,

$$\sum_{k=1}^{n} \overline{q}_{kj} = 1 \quad \Longleftrightarrow \quad \text{column } j \text{ has odd Hamming weight.}$$

A completely analogous argument applies to rows. Since $\overline{Q}^T \overline{Q} = I_n$, it follows that

$$\overline{Q}\, \overline{Q}^T = I_n$$

as well (because $\overline{Q}$ is invertible with inverse $\overline{Q}^T$). Fix a row index i and consider the (i, i)-entry of $\overline{Q}\, \overline{Q}^T$:

$$(\overline{Q}\, \overline{Q}^T)_{ii} = \sum_{k=1}^{n} \overline{q}_{ik}^2 = \sum_{k=1}^{n} \overline{q}_{ik} = 1 \quad \text{in } \mathbb{Z}_2.$$

Therefore, the i-th row also has odd Hamming weight.

We have shown that every column and every row of $\overline{Q}$ contains an odd number of nonzero entries. This completes the proof. □

This lemma shows that $\overline{Q}$ lies in the set of binary matrices with orthonormal rows and columns under the standard dot product over $\mathbb{Z}_2$. However, this condition alone does not force $\overline{Q}$ to be a permutation matrix when $n \geq 3$. The behavior of orthogonal groups defined over finite rings and their reductions has been explored in several contexts, revealing that combinatorial restrictions over $\mathbb{Z}_2$ do not completely describe the structure of the underlying group; see [15, 17].

The conclusion of Lemma 3.1 provides a first indication that orthogonality over $\mathbb{Z}_{2^r}$ is governed by parity considerations at a fundamental level. In particular, the reduction $\overline{Q}$ must lie in the set of binary matrices whose rows and columns each contain an odd number of nonzero entries. This sharply contrasts with the situation over fields of odd characteristic, where no such restriction appears due to the invertibility of 2 and the resulting flexibility in quadratic relations [8, 12].

From a combinatorial perspective, this condition significantly reduces the admissible configurations of $\overline{Q}$. Indeed, each row vector of $\overline{Q}$ belongs to the subset of $\mathbb{Z}_2^n$ consisting of vectors of odd weight, and the same holds for columns. Consequently, orthogonal matrices over $\mathbb{Z}_{2^r}$ project to a highly structured subset of $M_n(\mathbb{Z}_2)$, which can be viewed as a constrained version of the binary orthogonal group. Such combinatorial restrictions are closely related to structural properties of modules over finite rings and their duality behavior, as discussed in [20].

It is worth emphasizing that, while the odd-weight condition is necessary, it is far from sufficient to characterize $O_n(\mathbb{Z}_2)$. Additional orthogonality relations, such as pairwise dot-product constraints, further restrict the structure, as we describe next. These finer constraints reflect the classical theory of bilinear forms and orthogonality in modular settings; see [7, 14].

Lemma 3.2 (Pairwise orthogonality over $\mathbb{Z}_2$)**.** *For $\overline{Q} \in O_n(\mathbb{Z}_2)$, distinct columns (and rows) are orthogonal in the sense that their dot product is zero in $\mathbb{Z}_2$.*

The proof follows directly from the entries of $\overline{Q}^T\overline{Q} = I$ corresponding to $i \neq j$:

$$\sum_{k=1}^{n} \overline{q}_{ki}\overline{q}_{kj} = 0 \quad \text{for } i \neq j.$$

Lemma 3.2 complements the odd-weight condition by imposing pairwise orthogonality among distinct rows and columns. These two properties jointly imply that $\overline{Q}$ defines an orthonormal system in $\mathbb{Z}_2^n$ under the standard bilinear form.

This observation allows us to interpret $\overline{Q}$ as a binary analogue of an orthogonal matrix, where the geometry is governed by the arithmetic of $\mathbb{Z}_2$. In particular, each pair of distinct rows (or columns) intersects in an even number of positions where both entries are 1, reflecting the vanishing of their dot product.

The interplay between odd weights and pairwise orthogonality leads to strong combinatorial rigidity. For small dimensions, such as $n = 2$, these conditions completely determine the structure of $O_n(\mathbb{Z}_2)$, forcing $\overline{Q}$ to be a permutation matrix. However, for larger n, more intricate configurations become possible, and a full classification becomes significantly more subtle.

These structural constraints over $\mathbb{Z}_2$ serve as a foundation for understanding the behavior of orthogonal matrices over $\mathbb{Z}_{2^r}$, since every such matrix must reduce to a binary orthogonal matrix satisfying these properties. We now derive stronger restrictions on diagonal entries and traces.

Having established the combinatorial structure of orthogonal matrices modulo 2, we now turn to global invariants that arise from these constraints. Among these, the trace plays a particularly important role, as it captures information about diagonal entries and is additive under matrix summation.

In the context of additive decompositions, trace considerations often yield immediate obstructions. Since the trace is preserved under reduction modulo 2, the behavior of $\mathrm{tr}(\overline{Q})$ provides direct information about $\mathrm{tr}(Q)$ in $\mathbb{Z}_{2^r}$. This connection allows us to transfer structural information from the binary setting to the original ring.

We begin with the simplest nontrivial case, where the dimension is small enough to permit a complete description.

Proposition 3.3 (Trace parity constraint)**.** *Let $Q \in O_n(\mathbb{Z}_{2^r})$ with $r \geq 2$. Then*

$$\mathrm{tr}(Q) \equiv \mathrm{tr}(\overline{Q}) \pmod 2,$$

and in dimension $n = 2$, the trace is always even modulo 2.

Proof. The first statement follows immediately from reduction modulo 2. For $n = 2$, the group $O_2(\mathbb{Z}_2)$ consists of the identity and the swap matrix:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

both of which have trace 0 modulo 2. Hence $\mathrm{tr}(\overline{Q}) \equiv 0$, and the result follows. $\square$

Remark 3.4. This provides an obstruction to additive generation: any sum of orthogonal matrices in $M_2(\mathbb{Z}_{2^r})$ must have even trace modulo 2, excluding half of all matrices.

Proposition 3.5 (Reduction invariance)**.** *If $A \in \mathscr{S}(O_n(\mathbb{Z}_{2^r}))$, then $\overline{A} \in \mathscr{S}(O_n(\mathbb{Z}_2))$.*

Proof. Since $A \in \mathscr{S}(O_n(\mathbb{Z}_{2^r}))$, by definition of the additive semigroup, there exists an integer $m \geq 1$ and matrices $Q_1, \ldots, Q_m \in O_n(\mathbb{Z}_{2^r})$ such that

$$A = \sum_{i=1}^{m} Q_i.$$

Let $\pi_1 : \mathbb{Z}_{2^r} \to \mathbb{Z}_2$ be the natural reduction modulo 2, and extend it entrywise to matrices. Denote $\overline{A} := \pi_1(A)$ and $\overline{Q}_i := \pi_1(Q_i)$.

Since π_1 is a ring homomorphism, it preserves addition.

Therefore,

$$\overline{A} = \pi_1\left(\sum_{i=1}^{m} Q_i\right) = \sum_{i=1}^{m} \pi_1(Q_i) = \sum_{i=1}^{m} \overline{Q}_i.$$

We now show that each $\overline{Q}_i$ is orthogonal over $\mathbb{Z}_2$.

Since $Q_i \in O_n(\mathbb{Z}_{2^r})$, we have

$$Q_i^T Q_i = I_n \quad \text{in } M_n(\mathbb{Z}_{2^r}).$$

Applying the reduction map π_1 to both sides and using multiplicativity, we obtain

$$\pi_1(Q_i^T Q_i) = \pi_1(I_n).$$

Because π_1 respects matrix multiplication and transpose,

$$(\pi_1(Q_i))^T \, \pi_1(Q_i) = I_n \quad \text{in } M_n(\mathbb{Z}_2)\,.$$

Thus,

$$\overline{Q}_i^T \overline{Q}_i = I_n,$$

which shows that $\overline{Q}_i \in O_n(\mathbb{Z}_2)$.

We have expressed $\overline{A}$ as a finite sum of matrices $\overline{Q}_i \in O_n(\mathbb{Z}_2)$:

$$\overline{A} = \sum_{i=1}^{m} \overline{Q}_i.$$

Therefore, by the definition of the additive semigroup,

$$\overline{A} \in \mathscr{S}(O_n(\mathbb{Z}_2))\,.$$

This completes the proof. □

Remark 3.6. Thus, membership in $\mathscr{S}(O_n(\mathbb{Z}_{2^r}))$ imposes necessary conditions at the level of $\mathbb{Z}_2$. This provides a useful obstruction method.

Proposition 3.5 highlights an important functorial property of the additive semigroup generated by orthogonal matrices. In particular, reduction modulo 2 preserves additive decompositions, implying that any obstruction at the level of $\mathbb{Z}_2$ automatically lifts to $\mathbb{Z}_{2^r}$.

This observation provides a powerful method for ruling out possible representations. If $A \in M_n(\mathbb{Z}_{2^r})$ is such that its reduction $\overline{A}$ cannot be represented as a sum of orthogonal matrices over $\mathbb{Z}_2$, then it follows that $A \notin \mathscr{S}(O_n(\mathbb{Z}_{2^r}))$. Thus, the problem of additive generation over $\mathbb{Z}_{2^r}$ is, in part, controlled by the corresponding problem over $\mathbb{Z}_2$.

However, it is important to note that this condition is only necessary and not sufficient. That is, even if $\overline{A} \in \mathscr{S}(O_n(\mathbb{Z}_2))$, it does not follow that $A \in \mathscr{S}(O_n(\mathbb{Z}_{2^r}))$. Additional obstructions arise from higher-order congruences and interactions between entries, which are not visible modulo 2. We now establish a new result that imposes a global restriction on the parity of orthogonal matrices.

While the preceding results focus on local and pairwise constraints, it is natural to ask whether there exist global invariants that govern the additive behavior of orthogonal matrices. Such invariants are particularly useful in understanding the structure of $\mathscr{S}(O_n(\mathbb{Z}_{2^r}))$, as they provide simple criteria for determining whether a given matrix can admit an orthogonal decomposition.

One natural candidate is the total sum of matrix entries, which aggregates information from all rows and columns. At first glance, this quantity appears to be too coarse to yield meaningful restrictions. However, when combined with the parity constraints established earlier, it reveals a surprisingly rigid structure.

The preceding theorem introduces a global invariant that complements the local and pairwise constraints derived earlier. Together, these results form a coherent framework for analyzing the additive structure of orthogonal matrices over $\mathbb{Z}_{2^r}$.

Theorem 3.7 (Global parity constraint)**.** *Let $Q \in O_n(\mathbb{Z}_{2^r})$ with $r \geq 2$. Then the total sum of all entries of Q is congruent to n modulo 2, i.e.,*

$$\sum_{i,j} q_{ij} \equiv n \pmod 2.$$

Consequently, for any $A \in \mathscr{S}(O_n(\mathbb{Z}_{2^r}))$, we have

$$\sum_{i,j} a_{ij} \equiv mn \pmod 2,$$

where m is the number of summands in a decomposition of A.

Proof. We divide the proof into two parts.

Part I: Let $\pi_1 : \mathbb{Z}_{2^r} \to \mathbb{Z}_2$ denote the natural reduction map, extended entrywise to matrices. Set $\overline{Q} = \pi_1(Q)$. Since $Q \in O_n(\mathbb{Z}_{2^r})$, we have

$$Q^T Q = I_n.$$

Applying π_1 and noting that it is a ring homomorphism, yields

$$\overline{Q}^T \overline{Q} = I_n \quad \text{in } M_n(\mathbb{Z}_2)\,.$$

By Lemma 3.1, each row of $\overline{Q}$ has odd Hamming weight. Equivalently, for each $1 \leq i \leq n$,

$$\sum_{j=1}^{n} \overline{q}_{ij} = 1 \quad \text{in } \mathbb{Z}_2.$$

We now compute the total sum of all entries of $\overline{Q}$:

$$\sum_{i,j} \overline{q}_{ij} = \sum_{i=1}^{n} \sum_{j=1}^{n} \overline{q}_{ij}.$$

Using the result from Step 2, each inner sum equals 1 in $\mathbb{Z}_2$, hence

$$\sum_{i,j} \overline{q}_{ij} = \sum_{i=1}^{n} 1 = n \quad \text{in } \mathbb{Z}_2.$$

Since reduction modulo 2 preserves congruence classes, the above identity implies

$$\sum_{i,j} q_{ij} \equiv \sum_{i,j} \overline{q}_{ij} \equiv n \pmod 2.$$

This establishes the first assertion.

Part II: Let $A \in \mathscr{S}(O_n(\mathbb{Z}_{2^r}))$. Then there exist $m \geq 1$ and matrices $Q_1, \ldots, Q_m \in O_n(\mathbb{Z}_{2^r})$ such that

$$A = \sum_{k=1}^{m} Q_k.$$

The total sum of entries is additive, so

$$\sum_{i,j} a_{ij} = \sum_{i,j} \sum_{k=1}^{m} (Q_k)_{ij} = \sum_{k=1}^{m} \sum_{i,j} (Q_k)_{ij}.$$

From the first part, for each k we have

$$\sum_{i,j} (Q_k)_{ij} \equiv n \pmod{2}.$$

Therefore,

$$\sum_{i,j} a_{ij} \equiv \sum_{k=1}^{m} n = mn \pmod{2}.$$

This proves both statements of the theorem. □

Theorem 3.7 provides a new additive invariant that constrains the image of $\mathscr{S}(O_n(\mathbb{Z}_{2^r}))$. In particular, it follows that matrices whose total parity is incompatible cannot be written as sums of orthogonal matrices. This phenomenon does not arise over rings where 2 is invertible.

The results of this section demonstrate that orthogonality over $\mathbb{Z}_{2^r}$ imposes a hierarchy of constraints, ranging from local conditions on rows and columns to global invariants such as trace and total sum. Collectively, these constraints confine the additive semigroup generated by orthogonal matrices and clarify the pronounced contrast with the odd modulus case.

In the subsequent sections, we will build upon these structural insights to characterize the extent of additive generation and identify precise obstructions in higher dimensions.

4. Constructive decompositions

The structural obstructions identified in the previous section suggest that additive generation by orthogonal matrices over $\mathbb{Z}_{2^r}$ is highly constrained. A natural next step is therefore to investigate *constructive mechanisms* that produce orthogonal matrices and to understand how far such constructions can be leveraged to generate large subsets of $M_n(\mathbb{Z}_{2^r})$.

A guiding principle in this direction is that, although orthogonality imposes strong arithmetic conditions, certain families of matrices—particularly those arising from permutation symmetries and low-rank perturbations—retain sufficient flexibility to serve as building blocks. In this section, we develop explicit constructions, analyze their algebraic properties, and identify both possibilities and limitations for additive decompositions.

Permutation matrices provide the simplest class of orthogonal matrices. Over any ring, they encode the action of the symmetric group and satisfy exact orthogonality relations. Over $\mathbb{Z}_{2^r}$, their structure can be enriched by incorporating sign changes.

Lemma 4.1. *Let P be a permutation matrix in $M_n(\mathbb{Z}_{2^r})$ and let $D = \operatorname{diag}(\epsilon_1, \dots, \epsilon_n)$ with each $\epsilon_i \in \{1, -1\} \subset \mathbb{Z}_{2^r}$. Then $DP \in O_n(\mathbb{Z}_{2^r})$.*

Proof. We verify directly that DP satisfies the defining orthogonality condition. A permutation matrix P is characterized by having exactly one entry equal to 1 in every row and column, with all other entries equal to 0. Therefore, its columns constitute an orthonormal set under the standard dot product over $\mathbb{Z}_{2^r}$. In particular,

$$P^T P = I_n.$$

The matrix $D = \mathrm{diag}(\epsilon_1, \dots, \epsilon_n)$ is diagonal with entries $\epsilon_i \in \{1, -1\}$. Since each $\epsilon_i^2 = 1$ in $\mathbb{Z}_{2^r}$, we obtain

$$D^2 = \mathrm{diag}(\epsilon_1^2, \dots, \epsilon_n^2) = I_n.$$

Moreover, since D is diagonal, we also have $D^T = D$. Hence,

$$D^T D = D^2 = I_n.$$

Using the transpose rule, we obtain

$$(DP)^T = P^T D^T = P^T D.$$

We now compute

$$(DP)^T (DP) = (P^T D)(DP) = P^T (DD) P = I_n.$$

We have shown that DP satisfies the defining condition of orthogonality, and hence

$$DP \in O_n(\mathbb{Z}_{2^r}).$$

□

Lemma 4.1 shows that the subgroup of signed permutation matrices embed naturally into $O_n(\mathbb{Z}_{2^r})$. This subgroup is isomorphic to the hyperoctahedral group and serves as a fundamental discrete skeleton inside the orthogonal group. However, as we will see, this class alone is insufficient for additive generation, particularly in even modulus where parity constraints persist.

To go beyond permutation-type constructions, we introduce a family of orthogonal matrices obtained via a rank-one perturbation. This construction exploits the nilpotent behavior of large powers of 2 in $\mathbb{Z}_{2^r}$.

Proposition 4.2 (Even dimension perturbation)**.** *Let n be even and $r \geq 2$. Let P be a permutation matrix in $M_n(\mathbb{Z}_{2^r})$, let J denote the all-ones matrix, and define $N := 2^{r-1} J$. Then*

$$Q := P + N \in O_n(\mathbb{Z}_{2^r}).$$

Proof. We compute

$$QQ^T = (P + N)(P^T + N^T) = PP^T + PN^T + NP^T + NN^T.$$

Since $PP^T = I$ and $N^T = N$, it remains to analyze the mixed and quadratic terms.

Because P permutes rows and columns, it preserves the all-ones matrix J, hence $PN = NP = N$. Therefore

$$PN^T + NP^T = N + N = 2N = 2^r J \equiv 0 \pmod{2^r}.$$

Furthermore,

$$NN^T = N^2 = (2^{r-1})^2 J^2 = 2^{2r-2} J^2.$$

Since $J^2 = nJ$ and n is even, we have $2^{2r-2} nJ \equiv 0 \pmod{2^r}$. Thus $NN^T \equiv 0$.

Combining these identities yields $QQ^T = I$. □

The requirement that n be even is essential. It ensures that the scalar factor arising from $J^2 = nJ$ vanishes modulo 2^r. This construction highlights a striking dichotomy between even and odd dimensions in the theory of orthogonal matrices over $\mathbb{Z}_{2^r}$.

The preceding constructions suggest that orthogonal matrices over $\mathbb{Z}_{2^r}$ can be partitioned into qualitatively distinct classes: permutation-like elements and perturbative elements. We now formalize how these interact under addition.

Theorem 4.3 (Generation by structured orthogonals)**.** *Let n be even and $r \geq 2$. Then every matrix in the additive semigroup generated by the family*

$$\mathcal{F} := \{DP : P \text{ permutation, } D \text{ diagonal with } \pm 1\} \cup \{P + 2^{r-1}J\}$$

satisfies the global parity constraint

$$\sum_{i,j} a_{ij} \equiv mn \pmod 2,$$

where m is the number of summands.

Proof. By definition, the family $\mathcal{F}$ consists of two types of matrices:

(i) matrices of the form DP, where P is a permutation matrix and D is a diagonal matrix with entries in $\{\pm 1\}$;
(ii) matrices of the form $P + 2^{r-1}J$, where P is a permutation matrix and J is the all-ones matrix.

By Lemma 4.1, every matrix of type (i), namely DP, is in $O_n(\mathbb{Z}_{2^r})$. Similarly, by Proposition 4.2, when n is even, every matrix of type (ii), namely $P + 2^{r-1}J$, is also orthogonal over $\mathbb{Z}_{2^r}$.

Therefore, every element $Q \in \mathcal{F}$ satisfies

$$Q \in O_n(\mathbb{Z}_{2^r}).$$

Let A be any matrix in the additive semigroup generated by $\mathcal{F}$. Then, by definition, there exist matrices $Q_1, \ldots, Q_m \in \mathcal{F}$ such that

$$A = \sum_{k=1}^{m} Q_k.$$

Thus, each Q_k is an orthogonal matrix in $O_n(\mathbb{Z}_{2^r})$.

By Theorem 3.7, every orthogonal matrix $Q_k \in O_n(\mathbb{Z}_{2^r})$ satisfies

$$\sum_{i,j} (Q_k)_{ij} \equiv n \pmod 2.$$

Summing over all $k = 1, \ldots, m$ and using additivity of the total sum, we obtain

$$\sum_{i,j} a_{ij} = \sum_{k=1}^{m} \sum_{i,j} (Q_k)_{ij} \equiv \sum_{k=1}^{m} n = mn \pmod 2.$$

Hence, every matrix in the additive semigroup generated by $\mathcal{F}$ satisfies the stated global parity constraint. $\square$

The theorem 4.3 shows that even highly nontrivial constructions remain subject to the same global parity obstruction. Thus, while constructive families enlarge the pool of available orthogonal matrices, they do not bypass the intrinsic arithmetic constraints imposed by the ring $\mathbb{Z}_{2^r}$.

We now revisit the case $n = 2$, where the constraints become especially rigid.

Proposition 4.4 (Persistent obstruction in dimension two)**.** *Let $r \geq 2$. The matrix E_{11} in $M_2(\mathbb{Z}_{2^r})$ does not belong to $\mathscr{S}(O_2(\mathbb{Z}_{2^r}))$.*

Proof. We argue by contradiction. Suppose that $E_{11} \in \mathscr{S}(O_2(\mathbb{Z}_{2^r}))$. Then, by definition of the additive semigroup generated by orthogonal matrices, there exist orthogonal matrices

$$Q_1, Q_2, \ldots, Q_m \in O_2(\mathbb{Z}_{2^r})$$

such that

$$E_{11} = \sum_{k=1}^{m} Q_k.$$

We now analyze the trace of both sides of this equation. Recall that the trace function

$$\mathrm{tr} : M_2(\mathbb{Z}_{2^r}) \to \mathbb{Z}_{2^r}$$

is additive. Hence,

$$\mathrm{tr}(E_{11}) = \sum_{k=1}^{m} \mathrm{tr}(Q_k).$$

Next, we reduce this identity modulo 2. Let $\overline{A}$ denote reduction modulo 2. Since reduction is a ring homomorphism, it preserves addition and trace, and therefore

$$\mathrm{tr}(\overline{E_{11}}) = \sum_{k=1}^{m} \mathrm{tr}(\overline{Q_k}) \quad \text{in } \mathbb{Z}_2.$$

We now evaluate both sides explicitly.

The matrix E_{11} is given by

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

so its trace is

$$\mathrm{tr}(E_{11}) = 1.$$

Reducing modulo 2, we obtain

$$\mathrm{tr}(\overline{E_{11}}) \equiv 1 \pmod 2.$$

For each k, since $Q_k \in O_2(\mathbb{Z}_{2^r})$, its reduction $\overline{Q_k}$ lies in $O_2(\mathbb{Z}_2)$. The orthogonal group $O_2(\mathbb{Z}_2)$ consists precisely of the two permutation matrices

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Both of these matrices have trace equal to 0 in $\mathbb{Z}_2$. Therefore,

$$\mathrm{tr}(\overline{Q_k}) \equiv 0 \pmod 2 \quad \text{for every } k = 1, \ldots, m.$$

Summing over k, we obtain

$$\sum_{k=1}^{m} \operatorname{tr}(\overline{Q_k}) \equiv 0 \pmod 2.$$

Thus,

$$\operatorname{tr}(\overline{E_{11}}) \equiv 0 \pmod 2.$$

However, we also have

$$\operatorname{tr}(\overline{E_{11}}) \equiv 1 \pmod 2.$$

This is a contradiction.

The assumption that $E_{11} \in \mathscr{S}(O_2(\mathbb{Z}_{2^r}))$ is not true.

Therefore,

$$E_{11} \notin \mathscr{S}(O_2(\mathbb{Z}_{2^r}))\,.$$

□

This obstruction illustrates that additive generation fails dramatically in small dimensions. In fact, the trace condition excludes exactly half of all matrices in $M_2(\mathbb{Z}_{2^r})$, demonstrating that $\mathscr{S}(O_2(\mathbb{Z}_{2^r}))$ is a proper subset with nontrivial codimension.

We now present a new result that strengthens the understanding of additive generation in even dimensions.

Theorem 4.5 (Parity class decomposition)**.** *Let n be even and $r \geq 2$. Then $\mathscr{S}(O_n(\mathbb{Z}_{2^r}))$ is contained in the subset*

$$\mathcal{P}_n := \left\{ A \in M_n(\mathbb{Z}_{2^r}) : \sum_{i,j} a_{ij} \equiv 0 \pmod 2 \right\}.$$

Moreover, $\mathcal{P}_n$ is closed under addition and contains all sums of an even number of orthogonal matrices.

Proof. Let $Q \in O_n(\mathbb{Z}_{2^r})$. By Theorem 3.7 (global parity constraint), we have

$$\sum_{i,j} q_{ij} \equiv n \pmod 2.$$

Since n is assumed to be even, it follows that

$$\sum_{i,j} q_{ij} \equiv 0 \pmod 2.$$

Thus, every orthogonal matrix Q belongs to $\mathcal{P}_n$.

Let $A \in \mathscr{S}(O_n(\mathbb{Z}_{2^r}))$. By definition, there exist orthogonal matrices

$$Q_1, Q_2, \ldots, Q_m \in O_n(\mathbb{Z}_{2^r})$$

such that

$$A = \sum_{k=1}^{m} Q_k.$$

Using the additivity of the total sum of entries, we obtain

$$\sum_{i,j} a_{ij} = \sum_{k=1}^{m} \sum_{i,j} (Q_k)_{ij}.$$

Reducing modulo 2 and applying Step 1 to each Q_k, we find

$$\sum_{i,j} a_{ij} \equiv 0 \pmod 2.$$

Hence $A \in \mathcal{P}_n$, proving that

$$\mathscr{S}(O_n(\mathbb{Z}_{2^r})) \subseteq \mathcal{P}_n.$$

Let $A, B \in \mathcal{P}_n$. Then

$$\sum_{i,j} a_{ij} \equiv 0 \pmod 2, \qquad \sum_{i,j} b_{ij} \equiv 0 \pmod 2.$$

Therefore,

$$\sum_{i,j} (a_{ij} + b_{ij}) \equiv 0 \pmod 2.$$

This shows that $A + B \in \mathcal{P}_n$, and hence $\mathcal{P}_n$ is closed under addition.

Let $Q_1, \dots, Q_{2m} \in O_n(\mathbb{Z}_{2^r})$ and set

$$A = \sum_{k=1}^{2m} Q_k.$$

Applying Theorem 3.7 to each summand, we obtain

$$\sum_{i,j} (Q_k)_{ij} \equiv n \pmod 2 \quad \text{for each } k.$$

Summing over k gives

$$\sum_{i,j} a_{ij} \equiv \sum_{k=1}^{2m} n = 2m \cdot n \equiv 0 \pmod 2,$$

since $2m \cdot n$ is even. Thus $A \in \mathcal{P}_n$.

We have shown that every element of $\mathscr{S}(O_n(\mathbb{Z}_{2^r}))$ lies in $\mathcal{P}_n$, that $\mathcal{P}_n$ is closed under addition, and that it contains all sums of an even number of orthogonal matrices. □

Theorem 4.5 shows that, in even dimensions, the additive semigroup $\mathscr{S}(O_n(\mathbb{Z}_{2^r}))$ is confined to a strict parity class. This provides a global invariant that sharply restricts the range of possible decompositions.

The results above suggest a deeper structural phenomenon governing additive generation.

Conjecture 4.6 (Even modulus classification)**.** Let $n \geq 2$ and $r \geq 2$. Then

$$\mathscr{S}(O_n(\mathbb{Z}_{2^r})) = \left\{ A \in M_n(\mathbb{Z}_{2^r}) : \overline{A} \in \mathscr{S}(O_n(\mathbb{Z}_2)),\ \sum_{i,j} a_{ij} \equiv 0 \pmod 2 \right\}.$$

Remark 4.7. This conjecture asserts that the obstructions identified in Section 3—namely, reduction modulo 2 and global parity—are not only necessary but also sufficient. Establishing this would yield a complete classification of additive generation by orthogonal matrices over $\mathbb{Z}_{2^r}$. The conjecture is consistent with all known low-dimensional cases and aligns with the behavior observed in the odd modulus setting, where no such obstructions arise [10, 13]. Its resolution would provide a unified framework bridging both regimes and would complement existing structural results on orthogonal groups over finite rings [15, 17].

The constructive results of this section reveal both the richness and the limitations of orthogonal matrices over $\mathbb{Z}_{2^r}$. While explicit families can be produced via permutation structures and nilpotent perturbations, the additive semigroup they generate remains fundamentally constrained by arithmetic invariants. These findings reinforce the central theme of this work: that parity phenomena play a decisive role in shaping additive decompositions over even modulus rings. Such behavior is closely tied to the arithmetic structure of finite rings and the theory of quadratic forms, where the failure of invertibility of 2 imposes intrinsic restrictions absent in the odd modulus case [8, 14, 20].

We now provide partial theoretical evidence supporting Conjecture 4.6 by showing that the proposed invariants are not only necessary but, under mild structural assumptions, essentially sufficient up to controlled lifting.

Theorem 4.8 (Partial classification via parity lifting)**.** *Let $n \geq 2$ and $r \geq 2$. Suppose that $A \in M_n(\mathbb{Z}_{2^r})$ satisfies:*

(i) $\overline{A} \in \mathscr{S}(O_n(\mathbb{Z}_2))$,

(ii) $\displaystyle\sum_{i,j} a_{ij} \equiv 0 \pmod 2$.

Then there exists a matrix $B \in \mathscr{S}(O_n(\mathbb{Z}_{2^r}))$ such that

$$A \equiv B \pmod{2^{r-1}}.$$

In particular, every such matrix A can be approximated modulo 2^{r-1} by a sum of orthogonal matrices.

Proof. By assumption (i), the reduction $\overline{A} \in M_n(\mathbb{Z}_2)$ lies in the additive semigroup generated by orthogonal matrices over $\mathbb{Z}_2$. Therefore, there exist matrices

$$\widetilde{Q}_1, \widetilde{Q}_2, \ldots, \widetilde{Q}_m \in O_n(\mathbb{Z}_2)$$

such that

$$\overline{A} = \sum_{k=1}^{m} \widetilde{Q}_k.$$

We now lift each $\widetilde{Q}_k$ from $\mathbb{Z}_2$ to $\mathbb{Z}_{2^r}$. By structural results on orthogonal groups over finite local rings (see [15, 17]), every orthogonal matrix over $\mathbb{Z}_2$ admits a lift to an orthogonal matrix over $\mathbb{Z}_{2^r}$. That is, for each k, there exists

$$Q_k \in O_n(\mathbb{Z}_{2^r})$$

such that

$$\overline{Q}_k = \widetilde{Q}_k.$$

Define

$$B := \sum_{k=1}^{m} Q_k.$$

By construction, each Q_k is orthogonal over $\mathbb{Z}_{2^r}$, hence

$$B \in \mathscr{S}(O_n(\mathbb{Z}_{2^r}))\,.$$

Reducing modulo 2, we obtain

$$\overline{B} = \sum_{k=1}^{m} \overline{Q}_k = \sum_{k=1}^{m} \widetilde{Q}_k = \overline{A}.$$

From the identity $\overline{A} = \overline{B}$, it follows that

$$A - B \equiv 0 \pmod{2}.$$

Hence there exists a matrix $C \in M_n(\mathbb{Z}_{2^r})$ such that

$$A - B = 2C.$$

We now analyze the structure of C. Taking the total sum of entries on both sides, we obtain

$$\sum_{i,j}(a_{ij} - b_{ij}) = 2\sum_{i,j} c_{ij}.$$

Reducing modulo 2, the right-hand side vanishes, and thus

$$\sum_{i,j} a_{ij} \equiv \sum_{i,j} b_{ij} \pmod{2}.$$

By assumption (ii), the left-hand side is 0 modulo 2. On the other hand, since B is a sum of orthogonal matrices, Theorem 3.7 implies that

$$\sum_{i,j} b_{ij} \equiv mn \pmod{2}.$$

In particular, this is also 0 modulo 2 whenever n is even or m is even. Hence, the parity condition is consistent, and no contradiction arises.

More importantly, the relation $A - B = 2C$ shows that each entry of $A - B$ is divisible by 2, so C is well-defined modulo 2^{r-1}.

Since $A - B = 2C$, it follows immediately that

$$A \equiv B \pmod{2^{r-1}},$$

because multiplication by 2 annihilates one power in the modulus.

We have constructed a matrix $B \in \mathscr{S}(O_n(\mathbb{Z}_{2^r}))$ such that $A \equiv B \pmod{2^{r-1}}$. This shows that any matrix satisfying conditions (i) and (ii) can be approximated modulo 2^{r-1} by a sum of orthogonal matrices, completing the proof. □

Theorem 4.8 shows that the obstructions in Conjecture 4.6 control additive generation up to one level in the 2-adic filtration. In particular, it reduces the full classification problem to a lifting problem from $\mathbb{Z}_{2^{r-1}}$ to $\mathbb{Z}_{2^r}$. This is analogous to classical lifting phenomena in the theory of quadratic forms and orthogonal groups over local rings [8, 14].

Corollary 4.9 (Exact classification for $r = 2$)**.** *For $r = 2$, Conjecture 4.6 holds if and only if every matrix $C \in M_n(\mathbb{Z}_2)$ with $\overline{C} \in \mathscr{S}(O_n(\mathbb{Z}_2))$ admits a lift preserving orthogonality sums.*

Remark 4.10. The corollary highlights that the case $r = 2$ (i.e., $\mathbb{Z}_4$) serves as the critical base case for the conjecture. This is consistent with previous results where $\mathbb{Z}_4$ exhibits the first nontrivial obstructions to additive generation [10]. Establishing a complete lifting theory in this case would likely resolve the conjecture in full generality.

5. A classification over $\mathbb{Z}_{2^r}$

The preceding sections reveal that additive decompositions over $\mathbb{Z}_{2^r}$ are governed by a collection of subtle parity constraints arising from the failure of 2 to be invertible. These constraints manifest themselves through invariants that persist under addition and reduction modulo 2. The goal of this section is to formalize these invariants and to outline a pathway toward a classification of the additive semigroup $\mathscr{S}(O_n(\mathbb{Z}_{2^r}))$.

A key observation is that many obstructions to decomposability are already visible after reduction modulo 2. This motivates the introduction of $\mathbb{Z}_2$-valued invariants that capture essential combinatorial features of matrices.

Definition 5.1 (Parity invariants)**.** For $A = [a_{ij}] \in M_n(\mathbb{Z}_{2^r})$, define:

- the trace parity: $\tau(A) := \operatorname{tr}(\overline{A}) \in \mathbb{Z}_2$,
- the row-sum vector modulo 2: $r(A) := \overline{A}\,\mathbf{1} \in (\mathbb{Z}_2)^n$,
- the column-sum vector modulo 2: $c(A) := \overline{A}^T\mathbf{1} \in (\mathbb{Z}_2)^n$,

where $\mathbf{1} = (1, \dots, 1)^T$.

The invariants $\tau(A)$, $r(A)$, and $c(A)$ capture both global and local parity information associated with the matrix A. They will play a central role in identifying necessary conditions for membership in the additive semigroup generated by orthogonal matrices.

More specifically, these invariants encode, respectively, the diagonal behavior and the global balance properties of rows and columns. In particular, the vectors $r(A)$ and $c(A)$ measure the parity of row and column sums, thereby reflecting the distribution of nonzero entries modulo 2. Such parity constraints are fundamental in the study of orthogonal matrices over $\mathbb{Z}_{2^r}$ and will be used extensively in the structural analysis that follows.

Lemma 5.2. *The maps $A \mapsto \tau(A)$, $A \mapsto r(A)$, and $A \mapsto c(A)$ are additive invariants modulo 2. That is, for all $A, B \in M_n(\mathbb{Z}_{2^r})$, one has*

$$\tau(A+B) = \tau(A) + \tau(B), \quad r(A+B) = r(A) + r(B), \quad c(A+B) = c(A) + c(B),$$

where all operations are taken in $\mathbb{Z}_2$.

Proof. Let $A, B \in M_n(\mathbb{Z}_{2^r})$. We verify additivity for each invariant separately.

By definition 5.1,

$$\tau(A) = \operatorname{tr}(\overline{A}), \qquad \tau(B) = \operatorname{tr}(\overline{B}),$$

where $\overline{A}$ and $\overline{B}$ denote reductions modulo 2. Since reduction modulo 2 is a ring homomorphism, we have

$$\overline{A+B} = \overline{A} + \overline{B}.$$

Using the linearity of the trace over $\mathbb{Z}_2$, it follows that

$$\tau(A+B) = \operatorname{tr}(\overline{A+B}) = \operatorname{tr}(\overline{A} + \overline{B}) = \operatorname{tr}(\overline{A}) + \operatorname{tr}(\overline{B}) = \tau(A) + \tau(B).$$

From the definition 5.1,

$$r(A) = \overline{A}\,\mathbf{1}, \qquad r(B) = \overline{B}\,\mathbf{1},$$

where $\mathbf{1} = (1, \dots, 1)^T \in (\mathbb{Z}_2)^n$. Using that reduction modulo 2 is a homomorphism, we obtain

$$r(A+B) = \overline{A+B}\,\mathbf{1} = (\overline{A} + \overline{B})\mathbf{1}.$$

By distributivity of matrix multiplication,

$$(\overline{A} + \overline{B})\mathbf{1} = r(A) + r(B).$$

Similarly, by definition,

$$c(A) = \overline{A}^T\mathbf{1}, \qquad c(B) = \overline{B}^T\mathbf{1}.$$

Then

$$c(A+B) = \overline{(A+B)}^T\mathbf{1} = (\overline{A} + \overline{B})^T\mathbf{1}.$$

Using the linearity of transpose,

$$(\overline{A} + \overline{B})^T = \overline{A}^T + \overline{B}^T,$$

and hence

$$c(A+B) = (\overline{A}^T + \overline{B}^T)\mathbf{1} = c(A) + c(B).$$

All three maps are additive after reduction modulo 2, and therefore define additive invariants with values in $\mathbb{Z}_2$. $\square$

Remark 5.3. Lemma 5.2 shows that these quantities descend to homomorphisms

$$M_n(\mathbb{Z}_{2^r}) \longrightarrow \mathbb{Z}_2 \quad \text{or} \quad (\mathbb{Z}_2)^n,$$

and therefore provide necessary conditions for membership in $\mathscr{S}(O_n(\mathbb{Z}_{2^r}))$. In particular, any obstruction detected by these invariants cannot be removed by adding orthogonal matrices.

We now record the behavior of these invariants on orthogonal matrices.

Proposition 5.4 (Invariant structure of orthogonal matrices)**.** *Let $Q \in O_n(\mathbb{Z}_{2^r})$. Then:*

(1) $r(Q) = c(Q) = \mathbf{1}$ in $(\mathbb{Z}_2)^n$,
(2) $\tau(Q) = \operatorname{tr}(\overline{Q})$ satisfies dimension-dependent constraints (e.g., $\tau(Q) = 0$ for $n = 2$).

Proof. Reducing the relation $Q^T Q = I$ modulo 2, we obtain $\overline{Q}^T \overline{Q} = I$ in $M_n(\mathbb{Z}_2)$. By Lemma 3.1, each row and each column of $\overline{Q}$ has odd Hamming weight. It follows immediately that

$$r(Q) = \overline{Q}\,\mathbf{1} = \mathbf{1} \quad \text{and} \quad c(Q) = \overline{Q}^T \mathbf{1} = \mathbf{1}$$

in $(\mathbb{Z}_2)^n$, proving the first assertion.

For the second statement, the trace parity $\tau(Q) = \operatorname{tr}(\overline{Q})$ is determined entirely by the structure of the binary orthogonal group $O_n(\mathbb{Z}_2)$. In particular, in low dimensions this group is explicitly known; for instance, when $n = 2$, it consists only of permutation matrices, each having trace 0 in $\mathbb{Z}_2$. This establishes the stated constraint. $\square$

Proposition 5.4 shows that orthogonal matrices occupy a highly structured subset of $M_n(\mathbb{Z}_{2^r})$ when viewed through the lens of parity invariants. In particular, all such matrices share the same row and column parity profile.

We now combine these invariants to obtain a unified obstruction.

Theorem 5.5 (Parity obstruction criterion)**.** *Let $A \in \mathscr{S}(O_n(\mathbb{Z}_{2^r}))$. Then there exists an integer $m \geq 1$ such that*

(i) $r(A) \equiv m\mathbf{1} \pmod 2$,
(ii) $c(A) \equiv m\mathbf{1} \pmod 2$,
(iii) $\tau(A) \equiv \sum_{k=1}^m \tau(Q_k) \pmod 2$,

where $A = \sum_{k=1}^m Q_k$ with $Q_k \in O_n(\mathbb{Z}_{2^r})$.

Proof. Since $A \in \mathscr{S}(O_n(\mathbb{Z}_{2^r}))$, there exist orthogonal matrices $Q_1, \dots, Q_m \in O_n(\mathbb{Z}_{2^r})$ such that

$$A = \sum_{k=1}^m Q_k.$$

By Lemma 5.2, the invariants τ, r, and c are additive modulo 2. Therefore,

$$r(A) = \sum_{k=1}^m r(Q_k), \qquad c(A) = \sum_{k=1}^m c(Q_k), \qquad \tau(A) = \sum_{k=1}^m \tau(Q_k)$$

in $\mathbb{Z}_2$.

By Proposition 5.4, each orthogonal matrix satisfies $r(Q_k) = c(Q_k) = \mathbf{1}$. Hence,

$$r(A) = \sum_{k=1}^m \mathbf{1} = m\mathbf{1}, \qquad c(A) = \sum_{k=1}^m \mathbf{1} = m\mathbf{1}$$

in $(\mathbb{Z}_2)^n$, which proves (i) and (ii).

For statement (iii), recall that $\tau(A) = \operatorname{tr}(\overline{A})$ is defined via reduction modulo 2 followed by taking the trace. Since both reduction modulo 2 and the trace map are linear operations, it follows that τ is additive over $\mathbb{Z}_2$. More precisely, we have

$$\overline{A} = \overline{\sum_{k=1}^m Q_k} = \sum_{k=1}^m \overline{Q_k},$$

and therefore,

$$\tau(A) = \sum_{k=1}^{m} \operatorname{tr}(\overline{Q_k}) = \sum_{k=1}^{m} \tau(Q_k)$$

in $\mathbb{Z}_2$, where we use the linearity of the trace. This establishes (iii). □

This theorem shows that decomposability forces strong alignment conditions on row and column sums. In particular, not every binary pattern can arise from a sum of orthogonal matrices.

The preceding results suggest that parity invariants capture all essential obstructions to additive generation.

Conjecture 5.6 (Mod 2 invariants determine decomposability)**.** Fix $r \geq 2$ and $n \geq 2$. There exists a finite set of $\mathbb{Z}_2$-valued linear invariants $\mathcal{I}_n$ on $M_n(\mathbb{Z}_{2^r})$ such that

$$A \in \mathscr{S}(O_n(\mathbb{Z}_{2^r})) \quad \Longleftrightarrow \quad \overline{A} \in \mathscr{S}(O_n(\mathbb{Z}_2)) \;\text{ and }\; I(A) = 0 \text{ for all } I \in \mathcal{I}_n.$$

Moreover, one may take $\mathcal{I}_n$ to be generated by trace parity together with a minimal collection of row/column balance invariants.

Conjecture 5.6 proposes that the classification problem reduces entirely to linear algebra over $\mathbb{Z}_2$. If true, this would provide a complete and computable characterization of $\mathscr{S}(O_n(\mathbb{Z}_{2^r}))$, reducing a nonlinear problem over $\mathbb{Z}_{2^r}$ to a finite-dimensional problem over $\mathbb{Z}_2$.

The conjecture is supported by all known low-dimensional cases and aligns with the philosophy that obstructions over rings with noninvertible 2 are fundamentally parity-driven. A proof would likely require a detailed analysis of lifting properties and combinatorial structure of $O_n(\mathbb{Z}_2)$.

A central technical challenge underlying the conjecture is the ability to lift orthogonal matrices from $\mathbb{Z}_2$ to $\mathbb{Z}_{2^r}$.

Problem 5.7 (Orthogonal lifting)**.** Given $\widetilde{Q} \in O_n(\mathbb{Z}_2)$, determine whether there exists $Q \in O_n(\mathbb{Z}_{2^r})$ such that $\overline{Q} = \widetilde{Q}$. If so, characterize the set of lifts and provide explicit constructions.

We provide a partial resolution in the following result.

Theorem 5.8 (Existence of lifts for permutation matrices)**.** *Let $\widetilde{Q} \in O_n(\mathbb{Z}_2)$ be a permutation matrix. Then there exists a matrix $Q \in O_n(\mathbb{Z}_{2^r})$ such that*

$$\overline{Q} = \widetilde{Q},$$

where $\overline{Q}$ denotes the reduction of Q modulo 2.

Proof. Let $\widetilde{Q} = [\widetilde{q}_{ij}] \in O_n(\mathbb{Z}_2)$ be a permutation matrix. By definition, each row and each column of $\widetilde{Q}$ contains exactly one entry equal to 1, with all other entries equal to 0. In particular, $\widetilde{Q}$ represents a permutation $\sigma \in S_n$, so that

$$\widetilde{q}_{ij} = \begin{cases} 1, & \text{if } j = \sigma(i), \\ 0, & \text{otherwise.} \end{cases}$$

We construct a matrix $Q = [q_{ij}] \in M_n(\mathbb{Z}_{2^r})$ by taking the same entries as $\widetilde{Q}$, but now viewed in $\mathbb{Z}_{2^r}$. That is, we define

$$q_{ij} = \widetilde{q}_{ij} \in \{0,1\} \subset \mathbb{Z}_{2^r}.$$

Clearly, reducing Q modulo 2 yields $\widetilde{Q}$, i.e.,

$$\overline{Q} = \widetilde{Q}.$$

It remains to verify that Q is orthogonal over $\mathbb{Z}_{2^r}$. To this end, we compute

$$(Q^T Q)_{ij} = \sum_{k=1}^{n} q_{ki} q_{kj}.$$

Because every column of Q has precisely one nonzero entry, namely 1, there is a unique index k for which $q_{ki} = 1$, and all remaining entries in that column vanish. Similarly for column j. Thus:

If $i = j$, then exactly one term in the sum is equal to 1, and all others are zero. Hence

$$(Q^T Q)_{ii} = 1.$$

If $i \neq j$, then the positions of the 1's in columns i and j occur in different rows, since $\widetilde{Q}$ is a permutation matrix. Therefore, for every k, at least one of q_{ki} or q_{kj} is zero, and hence

$$q_{ki} q_{kj} = 0.$$

It follows that

$$(Q^T Q)_{ij} = 0.$$

Combining these cases, we obtain

$$Q^T Q = I_n$$

in $M_n(\mathbb{Z}_{2^r})$, which shows that $Q \in O_n(\mathbb{Z}_{2^r})$.

Thus, Q is an orthogonal matrix over $\mathbb{Z}_{2^r}$ whose reduction modulo 2 is precisely $\widetilde{Q}$, completing the proof. □

The difficulty of the lifting problem lies in the fact that not all elements of $O_n(\mathbb{Z}_2)$ admit lifts preserving orthogonality. This reflects the failure of Hensel-type lifting in the absence of nondegeneracy conditions.

A full solution to the lifting problem would likely involve a deformation-theoretic analysis of the equation $Q^T Q = I$ over $\mathbb{Z}_{2^r}$, viewed as a system of quadratic congruences. This perspective may provide a pathway toward resolving Conjecture 5.6.

The classification of $\mathscr{S}(O_n(\mathbb{Z}_{2^r}))$ appears to be governed by a delicate interplay between linear invariants over $\mathbb{Z}_2$ and nonlinear lifting phenomena. The results of this section lay the groundwork for a systematic theory, reducing the problem to a finite collection of parity constraints and lifting conditions.

The results developed in this work highlight a sharp structural contrast between odd and even moduli in the context of additive generation by orthogonal matrices. When the modulus is odd, the invertibility of 2 enables a high degree of algebraic flexibility, ultimately allowing the additive semigroup generated by orthogonal matrices to coincide with the entire matrix ring. In contrast, the even-modulus setting reveals a fundamentally different landscape, where arithmetic constraints impose rigid limitations. These constraints, already apparent at the level of reduction modulo 2, manifest through parity conditions on rows, columns, traces, and global sums. As demonstrated throughout the paper, such invariants act as genuine obstructions, preventing full additive generation and giving rise to a highly structured and restricted semigroup. This dichotomy underscores the deep interplay between the arithmetic of the base ring and the algebraic behavior of matrix groups defined over it.

Looking ahead, several natural directions emerge for further investigation. A primary objective is to obtain a complete characterization of $\mathscr{S}(O_n(\mathbb{Z}_2))$ for general n, which would serve as the foundational layer for understanding all higher powers of 2. Closely related is the development of a systematic lifting theory, addressing when orthogonal matrices and their additive decompositions can be extended from $\mathbb{Z}_{2^s}$ to $\mathbb{Z}_{2^{s+1}}$. Such results would clarify how obstructions propagate along the 2-adic tower. Another important direction is to establish the sufficiency of a finite and explicitly describable set of parity invariants, thereby confirming whether these conditions fully determine additive decomposability. Achieving this would lead to a definitive classification theorem for $\mathscr{S}(O_n(\mathbb{Z}_{2^r}))$, completing the program initiated in this work and providing a unified framework for additive generation over modular rings.

References

[1] Bhatia, R. (1997). *Matrix analysis*. Springer. https://doi.org/10.1007/978-1-4612-0653-8 https://link.springer.com/book/10.1007/978-1-4612-0653-8

[2] Charkani, M. E., & Najim, A. (2019). Presentation matrices of torsion modules over polynomial rings. *Gulf Journal of Mathematics, 7*(1). https://doi.org/10.56947/gjom.v7i1.15

[3] DeFranza, J., & Gagliardi, D. (2009). *Introduction to linear algebra with applications*. McGraw-Hill. https://www.abebooks.com/Introduction-Linear-Algebra-Applications-Jim-DeFranza/32250978109/bd

[4] Dieudonné, J. (1971). *La géométrie des groupes classiques*. Springer. https://doi.org/10.1007/BF00969144

[5] Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra* (3rd ed.). Wiley. https://www.wiley.com/en-us/Abstract+Algebra%2C+3rd+Edition-p-9780471433347

[6] Golub, G. H., & Van Loan, C. F. (2013). *Matrix computations* (4th ed.). Johns Hopkins University Press. https://doi.org/10.56021/9781421407944

[7] Grove, L. C. (2002). *Classical groups and geometric algebra*. American Mathematical Society. https://doi.org/10.1090/gsm/039

[8] Hahn, A. J., & O'Meara, O. T. (1989). *The classical groups and K-theory*. Springer.

[9] Horn, R. A., & Johnson, C. R. (2013). *Matrix analysis* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781139020411

[10] Kholil, M. I., Parvez, M. M., Pant, S., Dagtoros, K., & Ali, M. A. (2025). Additive decompositions of orthogonal matrices over finite rings. *Journal of Computational Analysis and Applications, 34*(12), 515–528. https://eudoxuspress.com/index.php/pub/article/view/4425

[11] Lam, T. Y. (2001). *A first course in noncommutative rings* (2nd ed.). Springer. https://books.google.sh/books?id=2PwGCAAAQBAJ&printsec=copyright#v=onepage&q&f=false

[12] Lidl, R., & Niederreiter, H. (1994). *Introduction to finite fields and their applications*. Cambridge University Press. https://doi.org/10.1017/CBO9781139172769

[13] Merino, D. I. (2012). The sum of orthogonal matrices. *Linear Algebra and Its Applications, 436*(7), 1960–1968. https://doi.org/10.1016/j.laa.2011.10.011

[14] O'Meara, O. T. (1963). *Introduction to quadratic forms*. Springer. https://doi.org/10.1007/978-3-642-62031-7

[15] Prasad, A., Singla, P., & Spallone, S. (2015). Similarity of matrices over local rings of length two. *Indiana Univ. Math. J. 64, 471-514*, 147–172. https://doi.org/10.48550/arXiv.1212.6157

[16] Roman, S. (2008). *Advanced linear algebra* (3rd ed.). Springer. https://doi.org/10.1007/978-0-387-72831-5

[17] *Sison, V. P., & Repizo, C. R. (2021). One-Sided K-Orthogonal Matrices Over Finite Semi-Local Rings And Their Codes. arXiv:2103.05592.* https://doi.org/10.48550/arXiv.2103.05592

[18] Trefethen, L. N., & Bau, D. (1997). *Numerical linear algebra*. SIAM. https://doi.org/10.1137/1.9780898719574

[19] Velazco-Velazco, J. A., & Tapia-Recillas, H. (2023). Vector-circulant matrices and codes over rings. *Gulf Journal of Mathematics, 15*(2), 160–165. https://doi.org/10.56947/gjom.v15i2.1412

[20] Wood, J. A. (1999). Duality for modules over finite rings and applications to coding theory. *American Journal of Mathematics, 121*(3), 555–575. https://doi.org/10.1353/ajm.1999.0024

[1] Department of Mathematics, Dhaka University of Engineering and Technology (DUET), Gazipur, Gazipur-1707, Bangladesh.

Email address: mmparvez@duet.ac.bd

[2] Department of Mathematics, Norfolk State University, Norfolk, VA 23504, USA.

Email address: mikholil@nsu.edu
Email address: kkottegoda@nsu.edu
Email address: spant@nsu.edu
Email address: kdagtoros@nsu.edu