

Cycle structures of orthomorphisms extending partial orthomorphisms of Boolean groups

Nichole L. Schimanski

Dept. of Mathematics and Statistics
Portland State University
Portland, Oregon, U.S.A.

nls@pdx.edu

John S. Caughman IV

Dept. of Mathematics and Statistics
Portland State University
Portland, Oregon, U.S.A.

caughman@pdx.edu

Submitted: Oct 12, 2015; Accepted: Aug 18, 2016; Published: Sep 2, 2016

Mathematics Subject Classifications: 05A05, 05B15, 20B99, 68P25

Abstract

A *partial orthomorphism* of a group G (with additive notation) is an injection $\pi : S \rightarrow G$ for some $S \subseteq G$ such that $\pi(x) - x \neq \pi(y) - y$ for all distinct $x, y \in S$. We refer to $|S|$ as the *size* of π , and if $S = G$, then π is an *orthomorphism*. Despite receiving a fair amount of attention in the research literature, many basic questions remain concerning the number of orthomorphisms of a given group, and what cycle types these permutations have.

It is known that conjugation by automorphisms of G forms a group action on the set of orthomorphisms of G . In this paper, we consider the additive group of binary n -tuples, \mathbb{Z}_2^n , where we extend this result to include conjugation by translations in \mathbb{Z}_2^n and related compositions. We apply these results to show that, for any integer $n > 1$, the distribution of cycle types of orthomorphisms of the group \mathbb{Z}_2^n that extend any given partial orthomorphism of size two is independent of the particular partial orthomorphism considered. A similar result holds for size one. We also prove that the corresponding result does not hold for orthomorphisms extending partial orthomorphisms of size three, and we give a bound on the number of cycle-type distributions for the case of size three. As a consequence of these results, we find that all partial orthomorphisms of \mathbb{Z}_2^n of size two can be extended to complete orthomorphisms.

1 Introduction

Let G be a finite group written with additive notation. A *partial orthomorphism* of G is an injection $\pi : S \rightarrow G$ such that $\pi(x) - x = \pi(y) - y$ implies $x = y$ for all $x, y \in S \subseteq G$. The *size* of a partial orthomorphism is the cardinality of the domain S . If $S = G$, then π is an *orthomorphism*. An orthomorphism σ is said to *extend* a partial orthomorphism π

whenever σ agrees with π everywhere on the domain of π . A partial orthomorphism (or orthomorphism) is *canonical* if $\pi(0) = 0$.

Orthomorphisms grew out of the study of mutually orthogonal Latin squares, initiated by Euler in [4]. The concept of orthomorphism was further developed by Johnson, et al. in [8], motivated by the study of mutually orthogonal Latin squares. Since then, results on the number of orthomorphisms of some small groups have been computed and an upper bound on the maximum number of orthomorphisms for a group of a given size has been proved. See [14] for an exposition of the current state of research in the context of Latin squares. Further, in the context of Latin squares, the existence of extensions of partial orthomorphisms of various sizes for the group \mathbb{Z}_n has been studied [1, 7, 13].

Applications of orthomorphisms of the group \mathbb{Z}_2^n to cryptography are found in the construction of block ciphers and hash functions—most famously in the Lai-Massey scheme [15], but also in the less well-known FOX family of block ciphers [9]. More recently, orthomorphisms have been used to strengthen the Even-Mansour block cipher against a cryptographic attack which makes use of the non-uniformity of $p(x) - x$ when p is a random permutation [5].

Interest in the algebraic structure of orthomorphisms, of the group \mathbb{Z}_2^n specifically, can be found in [10] where Mitternath shows that a permutation is an orthomorphism if and only if it maps every maximal subgroup half into itself and half into its complement. Further mathematical research on orthomorphisms of the group \mathbb{Z}_2^n can be found in [2] and [6].

Since orthomorphisms are permutations, it is natural to consider their cycle types. Although the number of different cycle types for a permutation of a set with m elements is given by the number of integer partitions of m , we find that for orthomorphisms of \mathbb{Z}_2^n , the number of possible cycle types is significantly reduced. For example, it is elementary to show that orthomorphisms of \mathbb{Z}_2^n must have exactly one fixed point and can have no cycles of length two. These constraints alone dramatically limit the number of cycle types possible for orthomorphisms. Our results extend these elementary observations and offer further information concerning the permissible cycle types.

Indeed, although the set of orthomorphisms of \mathbb{Z}_2^n for the $n \leq 4$ cases can be easily generated with a computer, it turns out that, as of the date of this writing, even the cardinality of this set is unknown for any $n \geq 5$. When $n = 1$, there are no orthomorphisms. When $n = 2$, it is easily shown that all 8 orthomorphisms have cycle type 1,3, that is, they have precisely one fixed point and one cycle of length three. Similarly, when $n = 3$, all 384 orthomorphisms have cycle type 1,7. When $n = 4$, however, we find that there are a total of 244,744,192 orthomorphisms, and they are distributed among exactly 16 cycle types. This is out of 231 total partitions of the number $2^4 = 16$, and out of just 17 that have a single fixed point and no cycles of length two.

To investigate these cycle structures further, we will consider a number of group actions on the set of orthomorphisms. These group actions lead to a uniformity in the cycle types of orthomorphisms that extend certain partial orthomorphisms. Specifically, we show that, for any integer $n > 1$, the distribution of cycle types of orthomorphisms of the group \mathbb{Z}_2^n that extend any given partial orthomorphism of size two is independent of the

particular partial orthomorphism considered. A similar result holds for size one. However, we also prove that the corresponding result does not hold for orthomorphisms extending partial orthomorphisms of size three, and we give a bound on the number of cycle type distributions for the case of size three.

2 Bijective, cycle-preserving maps

In this section, we introduce a class of bijective cycle-type preserving functions defined on sets of orthomorphisms. The basic functions in this class are conjugations by automorphisms $g \in \text{Aut}(\mathbb{Z}_2^n)$, conjugations by translations

$$T_k(x) = x + k,$$

for $x, k \in \mathbb{Z}_2^n$, and the inverse map. In particular, we consider all functions of the form $C_h(\pi) = h\pi h^{-1}$ where h is a finite composition of automorphisms and translations, and π is an orthomorphism. As conjugations, the functions C_h are obviously bijective and cycle-type preserving. Similarly, the inverse map is bijective and cycle-type preserving. The critical point, in all cases, is to verify that these functions map orthomorphisms to orthomorphisms.

Lemma 1. [8, p.361] *For any $g \in \text{Aut}(\mathbb{Z}_2^n)$ and any orthomorphism π of \mathbb{Z}_2^n ,*

$$C_g(\pi) = g\pi g^{-1}$$

is an orthomorphism of \mathbb{Z}_2^n .

Proof. Since g, π are permutations of \mathbb{Z}_2^n , it suffices to show that the map $x \mapsto g\pi g^{-1}(x) - x$ is a permutation. Since π is an orthomorphism, the map $\sigma : x \mapsto \pi(x) - x$ is a permutation. Therefore

$$\begin{aligned} g\pi g^{-1}(x) - x &= g(\pi(g^{-1}(x))) - g(g^{-1}(x)) \\ &= g(\pi(g^{-1}(x)) - g^{-1}(x)) \\ &= g\sigma g^{-1}(x), \end{aligned}$$

and $g\sigma g^{-1}$ is a permutation. □

We note that, as the proof above shows, Lemma 1 is generally true for any group G , not just \mathbb{Z}_2^n . Next we consider conjugating by translations.

Lemma 2. *For any $k \in \mathbb{Z}_2^n$ and any orthomorphism π of \mathbb{Z}_2^n , the map*

$$C_{T_k}(\pi) = T_k\pi T_k^{-1}$$

is an orthomorphism of \mathbb{Z}_2^n .

Proof. Since T_k, π are permutations of \mathbb{Z}_2^n , it suffices to show the map $x \mapsto T_k \pi T_k^{-1}(x) - x$ is a permutation. Since π is an orthomorphism, the map $\sigma : x \mapsto \pi(x) - x$ is a permutation. Therefore,

$$\begin{aligned} T_k \pi T_k^{-1}(x) - x &= T_k(\pi(x - k)) - x \\ &= \pi(x - k) + k - x \\ &= \pi(x - k) - (x - k) \\ &= \sigma T_k^{-1}(x) \end{aligned}$$

is also a permutation. \square

We note that, as the above proof shows, if G is an arbitrary group, then Lemma 2 holds.

Corollary 3. *If π is an orthomorphism and h is any composition of a finite number of automorphisms and translations of \mathbb{Z}_2^n , then $C_h(\pi)$ is an orthomorphism. Moreover, the cycle type of $C_h(\pi)$ is the same as that of π .*

Proof. An immediate consequence of Lemmas 1 and 2. The cycle type of any permutation is preserved by conjugation [3, p. 125]. \square

The final cycle-type preserving function on orthomorphism sets we describe in this paper will be used in Section 7. Once again, as the proof shows, the result is generally true for any group G .

Lemma 4. *For any orthomorphism π of \mathbb{Z}_2^n , the map*

$$R(\pi) = \pi^{-1}$$

is an orthomorphism of \mathbb{Z}_2^n with the same cycle type as π .

Proof. Since π^{-1} is a permutation with the same cycle-type as π , it suffices to show $x \mapsto \pi^{-1}(x) - x$ is injective. Let $x, y \in \mathbb{Z}_2^n$. Since π is bijective, there exists unique $x', y' \in \mathbb{Z}_2^n$ such that $\pi(x') = x$ and $\pi(y') = y$. The following are equivalent,

$$\begin{aligned} \pi^{-1}(x) - x &= \pi^{-1}(y) - y \\ \pi^{-1}(\pi(x')) - \pi(x') &= \pi^{-1}(\pi(y')) - \pi(y') \\ x' - \pi(x') &= y' - \pi(y'), \end{aligned}$$

thus, since π is an orthomorphism, $x' = y'$. Further, since π is well-defined, $x = y$. \square

We observe that the group \mathbb{Z}_2^n may be viewed as an n -dimensional vector space over the field with two elements. So, the following theorem is fundamental to most of the arguments in Sections 4 and 5.

Theorem 5. *For any $n \in \mathbb{N}$, the automorphism group of \mathbb{Z}_2^n satisfies the following properties.*

1. $\text{Aut}(\mathbb{Z}_2^n) \cong \text{GL}_n(\mathbb{Z}_2)$, the group of invertible $n \times n$ matrices.
2. Each element of $g \in \text{Aut}(\mathbb{Z}_2^n)$ can be represented by a matrix in $\text{GL}_n(\mathbb{Z}_2)$ and its action on \mathbb{Z}_2^n corresponds to matrix multiplication.
3. Let g be an element of $\text{Aut}(\mathbb{Z}_2^n)$. Any $x_1, \dots, x_k \in \mathbb{Z}_2^n$ satisfies a dependence relation

$$c_1x_1 + \dots + c_kx_k = 0 \quad (c_1, \dots, c_k \in \mathbb{Z}_2)$$

if and only if $g(x_1), \dots, g(x_k)$ satisfies the same relation.

4. In particular, if $g \in \text{Aut}(\mathbb{Z}_2^n)$ then any $x_1, \dots, x_k \in \mathbb{Z}_2^n$ are linearly dependent (independent) if and only if $g(x_1), \dots, g(x_k)$ are linearly dependent (independent).

Proof. For more about these standard results from linear algebra, we refer the interested reader to the excellent texts [3, Chapter 11] and [12]. \square

3 Notation

Definition 6. If π is a partial orthomorphism of size one with a domain in \mathbb{Z}_2^n such that $\pi(r) = i$, then we write π as (i_r) . If π is a partial orthomorphism of size two such that $\pi(r) = i$ and $\pi(s) = j$ for distinct r, s , then we write π as (i_r, j_s) . Further, if π is a partial orthomorphism of size three such that $\pi(r) = i$, $\pi(s) = j$, and $\pi(t) = k$, then we write π as (i_r, j_s, k_t) .

Note that in the partial orthomorphism (i_r, j_s) , the elements i and j are distinct since the partial orthomorphism is injective; and $i + r \neq j + s$ which follows from the definition of partial orthomorphism.

Definition 7. If π is a partial orthomorphism of size one with a domain in \mathbb{Z}_2^n such that $\pi(r) = i$, then the set of all orthomorphisms that extend π is denoted $\mathcal{S}(i_r)$. If (i_r, j_s) is a partial orthomorphism of size two then the set of all orthomorphisms that extend it is denoted $\mathcal{S}(i_r, j_s)$. Further, if (i_r, j_s, k_t) is a partial orthomorphism then the set of all orthomorphisms that extend it is denoted $\mathcal{S}(i_r, j_s, k_t)$.

We now define a sequence that encodes the distribution of orthomorphisms among the possible cycle types.

Definition 8. For a fixed n , let \mathcal{C}_n be the set of all possible cycle types of permutations of \mathbb{Z}_2^n . Then, for any partial orthomorphism (i_r, j_s) , we define

$$\vec{\mathbf{d}}(i_r, j_s) = (n_t)_{t \in \mathcal{C}_n}$$

to be the $|\mathcal{C}_n|$ -tuple of nonnegative integers, indexed by \mathcal{C}_n , whose entries n_t equal the number of elements of $\mathcal{S}(i_r, j_s)$ with the given cycle type t . For partial orthomorphisms of size one (and three), we define $\vec{\mathbf{d}}(i_r)$ (and $\vec{\mathbf{d}}(i_r, j_s, k_t)$) similarly.

4 Cycle type distributions and partial orthomorphisms of size one

In this section we show that the set of orthomorphisms that extend any partial orthomorphism of size one has a cycle-type distribution which does not depend on the particular partial orthomorphism of size one chosen.

We begin by considering some canonical partial orthomorphisms of size one and two.

Lemma 9. *Suppose $(0_0, i_r)$ is a partial orthomorphism of \mathbb{Z}_2^n and $n > 1$. Then*

$$\vec{\mathbf{d}}(0_0) = (2^n - 2)\vec{\mathbf{d}}(0_0, i_r).$$

Proof. Partitioning the set of canonical orthomorphisms $\mathcal{S}(0_0)$ according to the partial orthomorphisms of size two on $\{0, r\}$ they extend, we have

$$\vec{\mathbf{d}}(0_0) = \sum_{j \neq 0, r} \vec{\mathbf{d}}(0_0, j_r).$$

For any $i, j \in \mathbb{Z}_2^n \setminus \{0, r\}$, the sets $\{r, i\}$ and $\{r, j\}$ are linearly independent. So, by Theorem 5, there exists an automorphism g of \mathbb{Z}_2^n such that $g(r) = r$ and $g(i) = j$. Then the function C_g maps $\mathcal{S}(0_0, i_r)$ onto $\mathcal{S}(0_0, j_r)$ bijectively, showing that $\vec{\mathbf{d}}(0_0, i_r) = \vec{\mathbf{d}}(0_0, j_r)$. It follows that each of the $2^n - 2$ terms in the sum shares the common value $\vec{\mathbf{d}}(0_0, i_r)$, so

$$\vec{\mathbf{d}}(0_0) = \sum_{j \neq 0, r} \vec{\mathbf{d}}(0_0, j_r) = (2^n - 2)\vec{\mathbf{d}}(0_0, i_r),$$

as desired. □

Lemma 10. *Suppose (i_s, t_t) is a partial orthomorphism of \mathbb{Z}_2^n and $n > 1$. Then*

$$\vec{\mathbf{d}}(i_s) = (2^n - 2)\vec{\mathbf{d}}(i_s, t_t).$$

Proof. First note that i, s, t must be distinct since (i_s, t_t) is a partial orthomorphism. Indeed, observe that any $x \in \mathbb{Z}_2^n$ is a fixed point of an orthomorphism π if and only if $\pi(x) - x = 0$. So, if r and s are fixed points of π then

$$\pi(r) - r = 0 = \pi(s) - s,$$

but the map $x \mapsto \pi(x) - x$ is a permutation when π is an orthomorphism. So, by injectivity, every orthomorphism of \mathbb{Z}_2^n has at most 1 fixed point; and by surjectivity, some x must satisfy $\pi(x) - x = 0$, so every orthomorphism has at least 1 fixed point. Therefore, every orthomorphism of \mathbb{Z}_2^n has precisely one fixed point. So, we can partition the set of orthomorphisms $\mathcal{S}(i_s)$ so that:

$$\vec{\mathbf{d}}(i_s) = \sum_{j \neq i, s} \vec{\mathbf{d}}(i_s, j_j).$$

For any $j, t \in \mathbb{Z}_2^n \setminus \{i, s\}$, the sets $\{i + s, t + s\}$ and $\{i + s, j + s\}$ are linearly independent. So, by Theorem 5, there exists an automorphism g of \mathbb{Z}_2^n such that $g(i + s) = i + s$ and $g(t + s) = j + s$. Set $h = T_s g T_s$, and note that the function C_h maps $\mathcal{S}(i_s, t_t)$ onto $\mathcal{S}(i_s, j_j)$ bijectively, showing that $\vec{\mathbf{d}}(i_s, t_t) = \vec{\mathbf{d}}(i_s, j_j)$. It follows that all $2^n - 2$ terms in the above sum are equal, so

$$\vec{\mathbf{d}}(i_s) = (2^n - 2)\vec{\mathbf{d}}(i_s, t_t),$$

as desired. \square

With the lemmas above, we are now ready to prove our result concerning size one partial orthomorphisms.

Theorem 11. *For any integer $n > 1$, the distribution of cycle types of orthomorphisms of the group \mathbb{Z}_2^n that extend any given partial orthomorphism of size one is independent of the particular partial orthomorphism considered.*

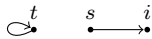
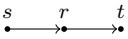

Proof. Let $i, s, i', s' \in \mathbb{Z}_2^n$. If $i = s$ and $i' = s'$ then C_h maps $\mathcal{S}(i_s)$ onto $\mathcal{S}(i'_{s'})$ bijectively when $h = T_{s+s'}$. If $i \neq s$ and $i' \neq s'$, we can instead use the map $h = T_{s'} g T_s$, where g is any automorphism satisfying $g(i + s) = i' + s'$. We are left to show that $\mathcal{S}(0_0)$ has the same cycle type distribution as $\mathcal{S}(i_s)$ for some $i \neq s$. From Lemmas 9 and 10, we can write

$$\vec{\mathbf{d}}(0_0) = (2^n - 2)\vec{\mathbf{d}}(i_s, 0_0) = \vec{\mathbf{d}}(i_s),$$

and the statement is proved. \square

5 Cycle type distributions and partial orthomorphisms of size two

Investigating partial orthomorphisms of size two leads to the consideration of three basic types of cycle structures. We will explore each of these cases separately by first proving cycle distribution uniformity within each category. Then we complete the argument by establishing uniformity across the cases. Note that the 2-cycle and two 1-cycles are not partial orthomorphisms, so cases related to them are not considered.

Case	Orthomorphism Set	Digraph Representation
1	$\mathcal{S}(t_t, i_s)$	
2	$\mathcal{S}(t_r, r_s)$	
3	$\mathcal{S}(t_r, i_s)$	

Regarding Cases 1 and 2, notice that if (t_t, i_s) is a partial orthomorphism then $i, s, t \in \mathbb{Z}_2^n$ are distinct. Similarly, if (t_r, r_s) is a partial orthomorphism then r, s, t are distinct. This pattern does not continue for the partial orthomorphism (t_r, i_s) . To distinguish Case 3 from the others, we make the additional assumption that $i, r, s, t \in \mathbb{Z}_2^n$ are distinct.

Lemma 12 (Case 1). Suppose (t_t, i_s) and $(t'_{t'}, i'_{s'})$ are partial orthomorphisms of \mathbb{Z}_2^n and $n > 1$. Then

$$\vec{\mathbf{d}}(t_t, i_s) = \vec{\mathbf{d}}(t'_{t'}, i'_{s'}).$$

Proof. By Lemma 10 and Theorem 11, we have

$$\vec{\mathbf{d}}(t_t, i_s) = \left(\frac{1}{2^n-2}\right) \vec{\mathbf{d}}(i_s) = \left(\frac{1}{2^n-2}\right) \vec{\mathbf{d}}(i'_{s'}) = \vec{\mathbf{d}}(t'_{t'}, i'_{s'}). \quad \square$$

Lemma 13 (Case 2). Suppose (t_r, r_s) and $(t'_{r'}, r'_{s'})$ are partial orthomorphisms of \mathbb{Z}_2^n and $n > 1$. Then

$$\vec{\mathbf{d}}(t_r, r_s) = \vec{\mathbf{d}}(t'_{r'}, r'_{s'}).$$

Proof. Observe that the sets $\{r+s, t+s\}$ and $\{r'+s', t'+s'\}$ are linearly independent whenever (t_r, r_s) and $(t'_{r'}, r'_{s'})$ are partial orthomorphisms. So, by Theorem 5, there exists an automorphism g of \mathbb{Z}_2^n that satisfies $g(r+s) = r'+s'$ and $g(t+s) = t'+s'$. Finally, apply C_h where $h = T_{s'}gT_s$ to $\mathcal{S}(t_r, r_s)$ to prove the statement of the lemma. \square

We make note of the following corollary, which relates Case 2 for partial orthomorphisms of size two back to the distributions for partial orthomorphisms of size one.

Corollary 14. For distinct $r, s, t \in \mathbb{Z}_2^n$, and $n > 1$,

$$\vec{\mathbf{d}}(t_r) = (2^n - 2)\vec{\mathbf{d}}(t_r, r_s).$$

Proof. By Lemma 13, we have $\vec{\mathbf{d}}(t_r, r_s) = \vec{\mathbf{d}}(t_r, r_{s'})$ for all $s' \in \mathbb{Z}_2^n \setminus \{r, t\}$. So,

$$\begin{aligned} \vec{\mathbf{d}}(t_r) &= \sum_{s' \neq r, t} \vec{\mathbf{d}}(t_r, r_{s'}) \\ &= (2^n - 2)\vec{\mathbf{d}}(t_r, r_s). \end{aligned} \quad \square$$

We now turn to Case 3.

Lemma 15 (Case 3). Suppose (t_r, i_s) and $(t'_{r'}, i'_{s'})$ are partial orthomorphisms of \mathbb{Z}_2^n and $n > 1$ where $i, r, s, t \in \mathbb{Z}_2^n$ are distinct and $i', r', s', t' \in \mathbb{Z}_2^n$ are distinct. Then

$$\vec{\mathbf{d}}(t_r, i_s) = \vec{\mathbf{d}}(t'_{r'}, i'_{s'}).$$

Proof. To begin, note that the set $\{t+r, i+r, s+r\}$ is linearly independent whenever (t_r, i_s) is a partial orthomorphism with distinct elements. Similarly, the set $\{t'+r', i'+r', s'+r'\}$ is linearly independent. Then by Theorem 5, there exists an automorphism g of \mathbb{Z}_2^n such that $g(t+r) = t'+r'$, $g(i+r) = i'+r'$, and $g(s+r) = s'+r'$. Setting $h = T_{r'}gT_r$, the map C_h defines a cycle-type preserving bijection from $\mathcal{S}(t_r, i_s)$ onto $\mathcal{S}(t'_{r'}, i'_{s'})$. \square

Again we make note of a relationship between Case 3 for partial orthomorphisms of size two and the distributions for partial orthomorphisms of size one.

Corollary 16. For distinct $r, s, t \in \mathbb{Z}_2^n$ and $n > 1$,

$$\vec{\mathbf{d}}(t_r) = (2^n - 2)\vec{\mathbf{d}}(t_r, i_s)$$

for all $i \in \mathbb{Z}_2^n \setminus \{r, s, t, t + r + s\}$.

Proof. Given that $r, t \in \mathbb{Z}_2^n$ and $r \neq t$, we have

$$\vec{\mathbf{d}}(t_r) = \sum_{i \neq t, t+r+s} \vec{\mathbf{d}}(t_r, i_s).$$

Using Lemma 15, Corollary 14, and Lemma 10, we see that, for some $i \in \mathbb{Z}_2^n \setminus \{r, s, t, r + s + t\}$,

$$\begin{aligned} \vec{\mathbf{d}}(t_r) &= (2^n - 4)\vec{\mathbf{d}}(t_r, i_s) + \vec{\mathbf{d}}(t_r, r_s) + \vec{\mathbf{d}}(t_r, s_s) \\ &= (2^n - 4)\vec{\mathbf{d}}(t_r, i_s) + \left(\frac{1}{2^n - 2}\right) \vec{\mathbf{d}}(t_r) + \left(\frac{1}{2^n - 2}\right) \vec{\mathbf{d}}(t_r). \end{aligned}$$

Solving for $\vec{\mathbf{d}}(t_r)$ yields

$$\vec{\mathbf{d}}(t_r) = (2^n - 2)\vec{\mathbf{d}}(t_r, i_s),$$

as desired. □

Finally, Lemma 17 will show that the orthomorphism sets from Cases 1 and 2 have the same distribution, and Lemma 18 will show that the orthomorphism sets from Cases 1 and 3 have the same distribution.

Lemma 17. For distinct $i, r, s, t \in \mathbb{Z}_2^n$ and $n > 1$,

$$\vec{\mathbf{d}}(t_t, i_s) = \vec{\mathbf{d}}(t_r, r_s)$$

Proof. If $t, r, s, i \in \mathbb{Z}_2^n$ are distinct, then

$$\begin{aligned} \vec{\mathbf{d}}(t_t, i_s) &= \left(\frac{1}{2^n - 2}\right) \vec{\mathbf{d}}(i_s) && \text{Lemma 10} \\ &= \left(\frac{1}{2^n - 2}\right) \vec{\mathbf{d}}(t_r) && \text{Theorem 11} \\ &= \vec{\mathbf{d}}(t_r, r_s) && \text{Corollary 14.} \end{aligned}$$

□

Lemma 18. For distinct $r, s, t \in \mathbb{Z}_2^n$ and $n > 1$,

$$\vec{\mathbf{d}}(t_t, r_s) = \vec{\mathbf{d}}(t_r, i_s)$$

for any $i \in \mathbb{Z}_2^n \setminus \{t, t + r + s\}$.

Proof. As in the previous lemma, we argue as follows

$$\begin{aligned}\vec{\mathbf{d}}(t_t, r_s) &= \left(\frac{1}{2^n - 2}\right) \vec{\mathbf{d}}(r_s) && \text{Lemma 10} \\ &= \left(\frac{1}{2^n - 2}\right) \vec{\mathbf{d}}(t_r) && \text{Theorem 11} \\ &= \vec{\mathbf{d}}(t_r, i_s),\end{aligned}$$

with the last equality holding: for $i = r$ by Corollary 14; for all $i \in \mathbb{Z}_2^n \setminus \{r, s, t, t + r + s\}$ by Corollary 16; and for $i = s$ by Lemma 10. Therefore, $\vec{\mathbf{d}}(t_t, r_s) = \vec{\mathbf{d}}(t_r, i_s)$ for all $i \in \mathbb{Z}_2^n \setminus \{t, t + r + s\}$. \square

To summarize, we have established the following.

Theorem 19. Suppose (t_r, i_s) and $(t'_{r'}, i'_{s'})$ are partial orthomorphisms of \mathbb{Z}_2^n and $n > 1$. Then

$$\vec{\mathbf{d}}(t_r, i_j) = \vec{\mathbf{d}}(t'_{r'}, i'_{j'}).$$

In other words, the distribution of cycle types of orthomorphisms of the group \mathbb{Z}_2^n that extend any given partial orthomorphism of size two is independent of the particular partial orthomorphism considered.

Cycle Type	Orthomorphism Count
1,4,4,7	23040
1,3,3,3,6	3840
1,4,5,6	57600
1,3,4,8	74880
1,3,12	109440
1,5,5,5	9984
1,4,11	80640
1,3,6,6	13440
1,15	332544
1,5,10	99072
1,7,8	92160
1,3,3,3,3,3	2048
1,6,9	46080
1,3,5,7	103680
1,3,3,9	42240
1,3,4,4,4	1920
total	1092608

Table 1: Cycle type distribution of $\mathcal{S}(t_r, i_j)$ in \mathbb{Z}_2^4 when (t_r, i_j) is a partial orthomorphism.

Cycle Type	π	σ	τ
1,4,4,7	1920	0	0
1,3,3,3,6	320	2304	0
1,4,5,6	4608	0	2304
1,3,4,8	5696	14976	6528
1,3,12	8768	21888	4224
1,5,5,5	768	0	768
1,4,11	6400	0	3840
1,3,6,6	1024	2688	1152
1,15	25600	0	25344
1,5,10	7488	0	9216
1,7,8	7104	0	6912
1,3,3,3,3,3	128	2048	512
1,6,9	3840	0	0
1,3,5,7	7360	20736	15360
1,3,3,9	3072	16896	5376
1,3,4,4,4	128	384	384
total	84224	81920	84224

Table 2: Cycle-type distributions for τ , π , and σ defined in Example 21.

As an illustration of Theorem 19, consider the set of orthomorphisms of \mathbb{Z}_2^4 . For any given partial orthomorphism of size two, there are 1,092,608 orthomorphisms that extend it. The cycle-type distribution of this set of orthomorphisms is given in Table 1.

An important consequence of Theorem 19 is the following corollary.

Corollary 20. *Every partial orthomorphism of size two of \mathbb{Z}_2^n for $n > 1$ can be extended to an orthomorphism.*

Proof. Since an orthomorphism exists for each $n > 1$ in \mathbb{Z}_2^n (see [11]), there exists a partial orthomorphism of size two that the orthomorphism extends. So, by Theorem 19, every partial orthomorphism of size two can be extended to an orthomorphism. \square

6 Examples and the case of size three

Example 21. As shown in Theorem 19, the cycle-type distribution of orthomorphisms that extend partial orthomorphisms of size two is independent of the particular partial orthomorphism of size two chosen. However, as mentioned earlier, a similar statement for partial orthomorphisms of size three does not hold. For example, consider the group \mathbb{Z}_2^4 and let π , σ , and τ denote the partial orthomorphisms of size three defined below.

x	$\pi(x)$	$\sigma(x)$	$\tau(x)$
0000	0000	0001	0000
0001	0010	0010	0010
0010	0100	0000	0011

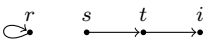
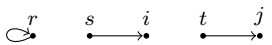
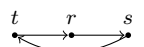
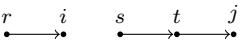

There are 84,224 orthomorphisms that extend π , but there are 81,920 that extend σ . So the sets of orthomorphisms extending π , σ do not share the same cardinality, much less the same distribution of cycle types.

On the other hand, the number of orthomorphisms extending τ is also 84,224 which matches π , and yet these sets have different cycle-type distributions. See Table 2.

7 Cycle-type distributions and partial orthomorphisms of size three

As illustrated in the previous section, the cycle-type distributions of orthomorphisms that extend partial orthomorphisms of size three are not all the same. In this section, we show that, for any $n > 2$, there are at most 12 cycle-type distributions for these orthomorphisms.

Similar to orthomorphism sets that extend partial orthomorphisms of size two, a set of 5 basic types of cycle structures arise. We consider each case separately. In each of the cases displayed in the following table, we assume the elements in each of the partial orthomorphisms are distinct.

Case	Orthomorphism Set	Digraph Representation
1	$\mathcal{S}(r_r, t_s, i_t)$	
2	$\mathcal{S}(r_r, i_s, j_t)$	
3	$\mathcal{S}(r_t, s_r, t_s)$	
4	$\mathcal{S}(i_r, t_s, j_t)$	
5	$\mathcal{S}(i_r, j_s, k_t)$	

(*)

We begin with the following lemma which is the basis for each of the case arguments in this section.

Lemma 22. Suppose (i_r, j_s, k_t) and $(i'_r, j'_{s'}, k'_{t'})$ are partial orthomorphisms of \mathbb{Z}_2^n . Then

$$\vec{d}(i_r, j_s, k_t) = \vec{d}(i'_r, j'_{s'}, k'_{t'})$$

whenever $(i + r, j + r, s + r, k + r, t + r)$ and $(i' + r', j' + r', s' + r', k' + r', t' + r')$ satisfy the same set of dependence relations.

Proof. By Theorem 5, let g be an automorphism that satisfies $g(i + r) = i' + r'$, $g(j + r) = j' + r'$, $g(s + r) = s' + r'$, $g(k + r) = k' + r'$, and $g(t + r) = t' + r'$, then apply C_h where $h = T_{r'}gT_r$ to $\mathcal{S}(i_r, j_s, k_t)$. \square

The apparent distinction of r (and r') relative to the other parameters in Lemma 22 is insignificant, as we see in Remark 23 below, since many symmetries exist among the parameters.

Remark 23. Notice that, by construction, the order in which the coordinates are written in the expression (i_r, j_s, k_t) has no effect on the cycle-type distribution of $\mathcal{S}(i_r, j_s, k_t)$. That is,

$$\begin{aligned}\vec{\mathbf{d}}(i_r, j_s, k_t) &= \vec{\mathbf{d}}(i_r, k_t, j_s) = \vec{\mathbf{d}}(j_s, k_t, i_r) \\ &= \vec{\mathbf{d}}(j_s, i_r, k_t) = \vec{\mathbf{d}}(k_t, j_s, i_r) = \vec{\mathbf{d}}(k_t, i_r, j_s).\end{aligned}$$

Additionally, using the inverse map, R , presented in Lemma 4 of Section 2, we find

$$\vec{\mathbf{d}}(i_r, j_s, k_t) = \vec{\mathbf{d}}(r_i, s_j, t_k).$$

Each of the case arguments in this section have the following form. With Lemma 22, it is sufficient to examine the collection of the possible sets of dependence relations on $\{i + r, j + r, s + r, k + r, t + r\}$ to determine the possible cycle-type distributions of $\mathcal{S}(i_r, j_s, k_t)$. So, the number of cycle-type distributions is at most the number of sets of dependence relations. With the help of the content of Remark 23, we can reduce the upper bound on the number of cycle-type distributions further.

Note that there exist no partial orthomorphisms of \mathbb{Z}_2^2 that fall into Cases 2, 4, or 5, as there are only 4 elements in \mathbb{Z}_2^2 and each of these cases requires more than 4 distinct elements. We now proceed with each of the five cases given in (*).

Lemma 24 (Case 1). *Suppose (r_r, t_s, i_t) is a partial orthomorphism for distinct $i, r, s, t \in \mathbb{Z}_2^n$ and $n > 1$. Then $\mathcal{S}(r_r, t_s, i_t)$ has one of at most 2 different cycle-type distributions.*

Proof. Note that $\{t + r, s + r, i + r\}$ is linearly dependent if and only if $t + r + s + i = 0$, since all other possible dependence relations contradict the assumption that (r_r, t_s, i_t) is a partial orthomorphism and i, r, s, t are distinct. The statement then follows from Lemma 22. \square

Lemma 25 (Case 2). *Suppose (r_r, i_s, j_t) is a partial orthomorphism for distinct $i, j, r, s, t \in \mathbb{Z}_2^n$ and $n > 2$. Then $\mathcal{S}(r_r, i_s, j_t)$ has one of at most 2 different cycle-type distributions.*

Proof. By Lemma 22, it is sufficient to examine the possible sets of dependence relations on the set $\{i + r, s + r, j + r, t + r\}$ to determine the possible cycle-type distributions of $\mathcal{S}(r_r, i_s, j_t)$. If $\{i + r, s + r, j + r, t + r\}$ is linearly dependent and (r_r, i_s, j_t) is a partial orthomorphism for distinct i, j, r, s, t , then one of the following is true: (a) $r + s + t + i = 0$, (b) $r + s + t + j = 0$, (c) $r + s + i + j = 0$, (d) $r + t + i + j = 0$. By Remark 23, an orthomorphism set in Case 2 that satisfies equation (a) has the same cycle-type distribution as a set that satisfies equation (b). Similarly for sets that satisfy (c) and (d). By Lemma 4, an orthomorphism set that satisfies equation (a) has the same cycle-type distribution as a set that satisfies equation (c). Thus, there are two possible cycle-type distributions for orthomorphism sets in Case 2 distinguished by whether the set $\{i + r, s + r, j + r, t + r\}$ is linearly dependent or not. \square

Lemma 26 (Case 3). *Suppose (r_t, s_r, t_s) is a partial orthomorphism for distinct $r, s, t \in \mathbb{Z}_2^n$ and $n > 1$. Then $\mathcal{S}(r_t, s_r, t_s)$ shares one common cycle-type distribution.*

Proof. Since (r_t, s_r, t_s) is a partial orthomorphism for distinct r, s, t , the set $\{s + r, t + r\}$ is linearly independent. The stated lemma follows from Lemma 22. \square

Lemma 27 (Case 4). *Suppose (i_r, t_s, j_t) is a partial orthomorphism for distinct $i, j, r, s, t \in \mathbb{Z}_2^n$ and $n > 2$. Then $\mathcal{S}(i_r, t_s, j_t)$ has one of at most 3 different cycle-type distributions.*

Proof. By Lemma 22, it is sufficient to examine the possible sets of dependence relations on the set $\{i + r, s + r, t + r, j + r\}$ to determine the possible cycle-type distributions of $\mathcal{S}(i_r, t_s, j_t)$. If $\{i + r, s + r, t + r, j + r\}$ is linearly dependent and (i_r, t_s, j_t) is a partial orthomorphism for distinct i, j, r, s, t , then one of the following is true: (a) $s + t + i + j = 0$, (b) $r + s + t + j = 0$, (c) $r + s + i + j = 0$. By Lemma 4, an orthomorphism set in Case 4 that satisfies equation (a) has the same cycle-type distribution as a set that satisfies equation (b). Thus, there are at most three possible cycle-type distributions for orthomorphism sets in Case 4: two when $\{i + r, s + r, j + r, t + r\}$ is linearly dependent and one when $\{i + r, s + r, j + r, t + r\}$ is linearly independent. \square

Lemma 28 (Case 5). *Suppose (i_r, j_s, k_t) is a partial orthomorphism for distinct $i, j, k, r, s, t \in \mathbb{Z}_2^n$ and $n > 2$. Then $\mathcal{S}(i_r, j_s, k_t)$ has one of at most 4 different cycle-type distributions.*

Proof. By Lemma 22, it is sufficient to examine the possible sets of dependence relations on the set $\{i + r, j + r, s + r, k + r, t + r\}$ to determine the possible cycle-type distributions of $\mathcal{S}(i_r, j_s, k_t)$. There are 14 possible sets of linear relations on $\{i + r, j + r, s + r, k + r, t + r\}$ when (i_r, j_s, k_t) is a partial orthomorphism and $i, j, r, s, t \in \mathbb{Z}_2^n$ are distinct. Two of the sets of relations correspond to the set $\{i + r, j + r, s + r, k + r, t + r\}$ being linearly independent, and the dependence relation $r + s + t + i + j + k = 0$. We show the remaining 12 sets of relations reduce to orthomorphism sets with just two different cycle-type distributions by first grouping the single-element relation sets in the following way.

$$\left. \begin{array}{l} i + s + j + k = 0 \\ i + t + j + k = 0 \\ i + j + k + r = 0 \end{array} \right\} \text{Type 1a} \quad \left. \begin{array}{l} r + i + s + t = 0 \\ r + j + s + t = 0 \\ r + s + k + t = 0 \end{array} \right\} \text{Type 1b} \quad \left. \begin{array}{l} i + j + s + t = 0 \\ i + s + t + k = 0 \\ r + i + t + j = 0 \\ r + i + s + k = 0 \\ r + j + s + k = 0 \\ r + j + k + t = 0 \end{array} \right\} \text{Type 2}$$

For the equations of Type 1a, we may relabel the elements in (i_r, j_s, k_t) and use Remark 23 to show $\vec{\mathbf{d}}(i_r, j_s, k_t)$ is the same for each line. A similar argument holds for the equations of Type 1b and equations of Type 2. To show orthomorphism sets with relations of Type 1a and Type 1b have the same cycle-type distribution, we may relabel the elements in (i_r, j_s, k_t) and use Lemma 4.

Thus, there are at most four possible cycle-type distributions for orthomorphism sets in Case 5. \square

With the lemmas above, we are now ready to prove our result concerning partial orthomorphisms of size 3.

Cycle Type	$(0_0, 2_1, 3_2)$	$(0_0, 2_1, 8_4)$	$(1_0, 2_1, 0_2)$	$(1_0, 4_2, 3_4)$	$(1_0, 4_2, 6_4)$
1,4,4,7	0	1920	0	1920	1920
1,3,3,3,6	0	320	2304	128	320
1,4,5,6	2304	4896	0	4800	4608
1,3,4,8	6528	6512	14976	4992	5696
1,3,12	4224	9296	21888	7296	8768
1,5,5,5	768	864	0	832	768
1,4,11	3840	6880	0	6720	6400
1,3,6,6	1152	1168	2688	896	1024
1,15	25344	28768	0	27712	25600
1,5,10	9216	8640	0	8256	7488
1,7,8	6912	7968	0	7680	7104
1,3,3,3,3,3	512	192	2048	0	128
1,6,9	0	3840	0	3840	3840
1,3,5,7	15360	9280	20736	6912	7360
1,3,3,9	5376	3744	16896	2112	3072
1,3,4,4,4	384	176	384	128	128
total	81920	94464	81920	84224	84224

Cycle Type	$(1_0, 4_2, 8_4)$	$(1_0, 8_2, 4_3)$	$(1_0, 8_2, 3_4)$	$(1_0, 8_2, 12_7)$
1,4,4,7	1920	2072	1768	1920
1,3,3,3,6	368	288	304	416
1,4,5,6	4848	5088	4464	4800
1,3,4,8	6688	6392	5640	6864
1,3,12	9664	9184	8512	10032
1,5,5,5	848	872	776	832
1,4,11	6800	7016	6344	6720
1,3,6,6	1200	1160	1000	1232
1,15	28240	29216	25680	27712
1,5,10	8448	8520	7800	8256
1,7,8	7824	7920	7296	7680
1,3,3,3,3,3	224	144	144	256
1,6,9	3840	4032	3648	3840
1,3,5,7	9392	8816	7712	9504
1,3,3,9	3984	3584	2992	4224
1,3,4,4,4	176	160	144	176
total	94464	94464	84224	94464

Table 3: Cycle type distributions realized for 9 representative partial orthomorphisms of size three of \mathbb{Z}_2^4 .

Theorem 29. *For any integer $n > 2$, the set of orthomorphisms of the group \mathbb{Z}_2^n that extend any given partial orthomorphism of size three has one of at most 12 different cycle-type distributions.*

For small values of n , not all cycle-type distributions are realized. For $n = 1$, there exist no orthomorphisms. For $n = 2$, there is only one possible cycle-type distribution for the set of all orthomorphisms that extend a particular partial orthomorphism of size three, since there is only one orthomorphism that extends any partial orthomorphism of size three, and all orthomorphisms of \mathbb{Z}_2^2 have cycle-type 1,3.

As in the case when $n = 2$, it turns out for $n = 3$ there is only one cycle-type distribution for the set of all orthomorphisms that extend any particular partial orthomorphism of size three. For $n = 4$, there are 9 different cycle-type distributions realized. See Table 3 for 9 representative partial orthomorphisms of size 3 and their cycle-type distributions, where we use the notation $2^3i_3 + 2^2i_2 + 2i_1 + i_0 \in \mathbb{Z}$ for $(i_3, i_2, i_1, i_0) \in \mathbb{Z}_2^n$. Values of n greater than 4 have yet to be studied computationally in this context, as working with orthomorphisms of this group is infeasible with current knowledge and technologies. Hopefully, future research will better illuminate the structure of orthomorphisms for larger values of n .

Acknowledgements

The authors would like to thank the anonymous referees for a number of helpful suggestions.

References

- [1] Nicholas J. Cavenagh, Carlo Hämäläinen, and Adrian M. Nelson. On completing three cyclically generated transversals to a Latin square. *Finite Fields and Their Applications*, 15(3):294–303, 2009.
- [2] Zong Duo Dai, Solomon W. Golomb, and Guang Gong. Generating all linear orthomorphisms without repetition. *Discrete Mathematics*, 205(1):47–55, 1999.
- [3] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Prentice Hall Englewood Cliffs, 3rd edition, 2004.
- [4] Leonhard Euler. *Recherches sur une nouvelle espece de quarrés magiques*. Zeeuwsch Genootschao, 1782.
- [5] Shoni Gilboa and Shay Gueron. Balanced permutations Even-Mansour ciphers. Cryptology ePrint Archive, Report 2014/642, 2014.
- [6] Solomon W. Golomb, Guang Gong, and Lothrop Mittenenthal. Constructions of orthomorphisms of \mathbb{Z}_2^n . In *Finite Fields and Applications: Proceedings of The Fifth International Conference on Finite Fields and Applications*, page 178. Springer Science & Business Media, 2001.

- [7] Martin Grüttmüller. Completing partial Latin squares with two cyclically generated prescribed diagonals. *Journal of Combinatorial Theory, Series A*, 103(2):349–362, 2003.
- [8] Diane M. Johnson, A. Lloyd Dulmage, and Nathan S. Mendelsohn. Orthomorphisms of groups and orthogonal Latin squares. *Canadian Journal of Mathematics*, 13:356–372, 1961.
- [9] Pascal Junod and Serge Vaudenay. Fox: a new family of block ciphers. In *The 11th International Workshop on Selected Areas in Cryptography*, volume 3357, pages 114–129, 2004.
- [10] Lothrop Mittenenthal. Block substitutions using orthomorphic mappings. *Advances in Applied Mathematics*, 16(1):59–71, 1995.
- [11] Lowell J. Paige. A note on finite abelian groups. *Bulletin of the American Mathematical Society*, 53(6):590–593, 1947.
- [12] David Poole. *Linear Algebra: A Modern Introduction*. Cengage Learning, 3rd edition, 2014.
- [13] Douglas S. Stones and Ian M. Wanless. Compound orthomorphisms of the cyclic group. *Finite Fields and Their Applications*, 16(4):277–289, 2010.
- [14] Ian M. Wanless. Transversals in Latin squares: a survey. In Robin Chapman, editor, *Surveys in Combinatorics 2011*, pages 403 – 437. Cambridge University Press, 2011.
- [15] Aaram Yun, Je Hong Park, and Jooyoung Lee. Lai-Massey scheme and quasi-Feistel networks. Cryptology ePrint Archive, Report 2007/347, 2007.