

Orthomorphisms of Boolean Groups

by

Nichole Louise Schimanski

A dissertation submitted in partial fulfillment of the  
requirements for the degree of

Doctor of Philosophy  
in  
Mathematical Sciences

Dissertation Committee:  
John Caughman, Chair  
Thomas Shrimpton  
Derek Garton  
Joyce O'Halloran  
Bart Massey

Portland State University  
2016

## ABSTRACT

An *orthomorphism*,  $\pi$ , of a group,  $(G, +)$ , is a permutation of  $G$  with the property that the map  $x \mapsto -x + \pi(x)$  is also a permutation. In this paper, we consider orthomorphisms of the additive group of binary  $n$ -tuples,  $\mathbb{Z}_2^n$ . We use known orthomorphism preserving functions to prove a uniformity in the cycle types of orthomorphisms that extend certain partial orthomorphisms, and prove that extensions of particular sizes of partial orthomorphisms exist. Further, in studying the action of conjugating orthomorphisms by automorphisms, we find several symmetries within the orbits and stabilizers of this action, and other orthomorphism-preserving functions. In addition, we prove a lower bound on the number of orthomorphisms of  $\mathbb{Z}_2^n$  using the equivalence of orthomorphisms to transversals in Latin squares. Lastly, we present a Monte Carlo method for generating orthomorphisms and discuss the results of the implementation.

## **DEDICATION**

*This dissertation is dedicated to my mother, Tina Johnston, who constantly encourages me to do things that seem personally unachievable and provides support as I do them. And to my son, Grant, who helped me realize I needed to do something for myself; to my step-dad for inspiring me to look into cryptography; and the rest of my family for providing so much help when I needed it.*

## ACKNOWLEDGMENTS

First and foremost, I would like to thank my advisor, John Caughman, for his guidance and advice as well as his patience and kindness throughout my time as a student of his.

For independently discovering this fun type of permutation we call orthomorphism, and sharing the discovery, I thank Tom Shrimpton.

I would also like to thank my committee members for believing this work was worthy of pursuit.

I thank Bart Massey and David Johnston for writing the C code I used to generate and count orthomorphisms.

For teaching me how to use my computer, I thank Jarrod W. Brockman and Jeremy Shaw.

I am appreciative of the anonymous referees for helpful suggestions on the version of Chapter 3 to appear in *The Online Journal of Combinatorics*.

Lastly, I would like to thank my coworkers at iovation: Damon Buckwalter, Perry Hook, Kyle Joecken, Kris Kolve, Chan Pham, Curtis Ropp, and John Taylor. They are all incredibly encouraging and supportive of my goals.

## TABLE OF CONTENTS

<b>Abstract</b>	<b>i</b>
<b>Dedication</b>	<b>ii</b>
<b>Acknowledgments</b>	<b>iii</b>
<b>List of Tables</b>	<b>vi</b>
<b>List of Figures</b>	<b>vii</b>
<b>Chapter 1 Introduction</b>	<b>1</b>
1.1 Overview . . . . .	1
1.2 Organization . . . . .	3
<b>Chapter 2 Mathematical Preliminaries</b>	<b>5</b>
2.1 Orthomorphisms . . . . .	5
2.2 Latin Squares . . . . .	6
2.3 Notation for the Group $\mathbb{Z}_2^n$ . . . . .	7
<b>Chapter 3 Properties of Orthomorphisms: Cycle Structure</b>	<b>9</b>
3.1 Introduction . . . . .	10
3.2 Bijective, Cycle-Preserving Maps . . . . .	11
3.3 Notation . . . . .	15
3.4 Cycle Type Distributions and Partial Orthomorphisms of Size One . .	16
3.5 Cycle Type Distributions and Partial Orthomorphisms of Size Two .	19
3.6 Examples and the Case of Size Three . . . . .	26
3.7 Cycle-Type Distributions and Partial Orthomorphisms of Size Three .	27
<b>Chapter 4 Properties of Orthomorphisms: Group Actions</b>	<b>36</b>
4.1 Introduction . . . . .	36
4.2 Orthomorphism-Preserving Maps . . . . .	37

4.3	Notation . . . . .	39
4.4	The $G$ -Orbit of an Orthomorphism . . . . .	39
4.5	The $G$ -Stabilizer of an Orthomorphism . . . . .	46
4.6	Characterization of Commuting Permutations . . . . .	48
<b>Chapter 5</b>	<b>Getting a Count</b>	<b>54</b>
5.1	Introduction . . . . .	54
5.2	A Lower Bound . . . . .	56
5.3	An Orthomorphism Formula . . . . .	61
5.4	Remarks on Upper Bounds . . . . .	62
5.5	A Count for $n = 5$ . . . . .	63
<b>Chapter 6</b>	<b>Generating Orthomorphisms</b>	<b>65</b>
6.1	Introduction . . . . .	65
6.2	Metropolis-Hastings Algorithm . . . . .	67
6.3	Conclusions . . . . .	73
<b>Chapter 7</b>	<b>Conclusions and Future Directions</b>	<b>76</b>
	<b>References</b>	<b>79</b>
	<b>Appendix Cycle Types for <math>\mathbb{Z}_2^5</math></b>	<b>82</b>

## List of Tables

Table 2.1	An orthomorphism of $\mathbb{Z}_2^2$ . . . . .	6
Table 3.1	Cycle type distribution of $\mathcal{S}(t_r, i_j)$ in $\mathbb{Z}_2^4$ . . . . .	25
Table 3.2	Cycle-type distributions for $\tau$ , $\pi$ , and $\sigma$ defined in Example 3. . .	28
Table 3.3	Cycle type distribution for partial orthomorphisms of $\mathbb{Z}_2^4$ . . . . .	35
Table 5.1	Transversal counts for groups of order $\leq 23$ . . . . .	55

## List of Figures

Figure 1.1 Block cipher in Davies-Meyer mode . . . . .	1
Figure 2.1 A transversal in a Cayley table for $\mathbb{Z}_2^2$ . . . . .	7
Figure 3.1 Cycle type distributions of orthomorphisms and permutations of $\mathbb{Z}_2^4$	26
Figure 4.1 Cycle type distribution of $G$ -orbits . . . . .	40
Figure 4.2 Element $g$ maps $k$ th cycle of $\pi$ to $i$ th cycle of $\pi$ with shift $j$ . . . .	50
Figure 5.1 Cayley table, $C_3$ , for $\mathbb{Z}_2^3$ . . . . .	57
Figure 5.2 Association between column indices of $C_2$ and $C_3$ . . . . .	58
Figure 5.3 Association between row indices of $C_2$ and $C_3$ . . . . .	58
Figure 5.4 Cayley table, $C_3$ , partitioned into blocks . . . . .	59
Figure 5.5 Form description of every $2 \times 2$ block in Figure 5.4 . . . . .	59
Figure 6.1 Distribution for Trial 1, $n = 4$ . . . . .	71
Figure 6.2 Distribution for Trial 1, $n = 5$ . . . . .	72
Figure 6.3 Distribution for Trial 2, $n = 4$ . . . . .	74
Figure 6.4 Distribution for Trial 2, $n = 5$ . . . . .	75



## Chapter 1

### INTRODUCTION

#### 1.1 Overview

An *orthomorphism* of an additive group  $(G, +)$  is a permutation  $\pi : G \rightarrow G$  such that the map  $x \mapsto -x + \pi(x)$  is also a permutation. Motivated by applications of orthomorphisms to cryptography, we will be primarily concerned with the group  $\mathbb{Z}_2^n$  which has a natural association to fixed length bit strings and the operation of exclusive-or. The investigation of orthomorphisms of  $\mathbb{Z}_2^n$  contained in this dissertation was initially motivated by the study of a particular configuration of collision resistant hash functions which uses a block cipher as the compression function. In particular, when orthomorphisms are used as the block ciphers in Davies-Meyer mode (see Figure 1.1), the output is uniformly distributed--thus circumventing known attacks [16].

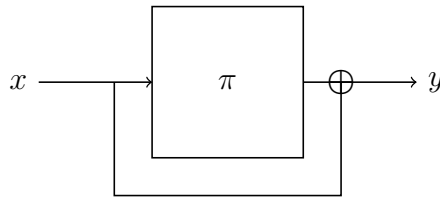


Figure 1.1: Block cipher in Davies-Meyer mode with an orthomorphism as the block cipher.

In the field of mathematics, the study of orthomorphisms grew out of the study of mutually orthogonal Latin squares, initiated by Euler in the 18th century [7]. The concept of an orthomorphism was further developed by Johnson, et al. in their 1961 paper [19], which was also motivated by the study of mutually orthogonal Latin squares. At the time, research in these topics was commonly applied to the study of the design of experiments [15].

Recent mathematical research regarding orthomorphisms has mainly been motivated by the study of transversals in Latin squares, which have been shown to be equivalent to orthomorphisms when the Latin square is a Cayley table [35]. Existence and extensions of partial orthomorphisms as well as bounds on the cardinality of orthomorphisms have also been studied extensively [2, 18, 33, 35]. Noticeably missing from this research, however, are investigations into the cycle structure of these and related objects, which we address in this dissertation. Further, we make use of the structure of Cayley tables of  $\mathbb{Z}_2^n$  to prove a lower bound on the cardinality of the set of orthomorphisms of  $\mathbb{Z}_2^n$ .

In the field of computer science, in contrast with mathematics, the study of orthomorphisms is just beginning. In this context, orthomorphisms of the group  $\mathbb{Z}_2^n$  (with its natural association to fixed-length bit strings--the building blocks of electronics) are of primary importance. In particular, orthomorphisms arise naturally in the field of symmetric-key cryptography--most famously in the FOX family of block ciphers [20] (now named IDEA NXT), but also in [36], where the authors use orthomorphisms in a so-called quasi-Feistel network. More recently, orthomorphisms have been used to strengthen the Even-Mansour block cipher against a cryptographic attack making use of the non-uniformity of  $p(x) - x$  when  $p$  is a random permutation [16]. Orthomorphisms

can play a useful role in the design of cryptographic primitives. In order to use them, however, we need a way to generate them efficiently. To quantitatively analyze their properties, we need to know, even just approximately, what proportion of permutations are orthomorphisms, and we need to know more about them in general, so that these properties can be exploited and statements about their security can be made.

As it pertains to cryptographic applications, interest in the algebraic structure of orthomorphisms of  $\mathbb{Z}_2^n$  can be found in [25] where Mittenhal shows that a permutation is an orthomorphism if and only if it maps every maximal subgroup half into itself and half into its complement. In this dissertation, we continue such investigations into the algebraic structures of orthomorphisms by thoroughly researching the mathematical properties related to various group actions on the set of orthomorphisms of  $\mathbb{Z}_2^n$ .

Further mathematical research on orthomorphisms of the group  $\mathbb{Z}_2^n$  can be found in [4] and [17] where the authors develop ways to generate and count particular subsets of orthomorphisms. In this dissertation, we also advance this direction of research by implementing a probabilistic method of generating orthomorphisms of  $\mathbb{Z}_2^n$ .

### 1.2 Organization

Chapter 2 provides a brief introduction to the main mathematical objects referenced throughout this dissertation, with examples to aid with understanding. The main results are separated into four chapters, each of which contains an in-depth review of the pertinent published literature. Chapter 3 delves into the cycle structure of orthomorphisms which extend partial orthomorphisms, and provides a proof that extensions of partial orthomorphisms of certain sizes exist. Chapter 4 contains research on the effects of

orthomorphism-preserving functions on the orbits and stabilizers of the automorphism group acting on the set of orthomorphisms of  $\mathbb{Z}_2^n$ . In Chapter 5, the relationship between the study of Latin squares and orthomorphisms is highlighted by proving a lower bound on the set of orthomorphisms of  $\mathbb{Z}_2^n$  using the structure of relevant Latin squares. In the final chapter, Chapter 6, we leverage the theory of Markov Chain Monte Carlo methods. Specifically, we use a Metropolis Hastings algorithm with various parameters to randomly generate sets of orthomorphisms of  $\mathbb{Z}_2^n$ . The appendix contains a table of cycle types of permutations of  $\mathbb{Z}_2^n$  and, in each case, lists an orthomorphism with the given cycle-type if one has been found.

## Chapter 2

### MATHEMATICAL PRELIMINARIES

Orthomorphisms are closely related to several other mathematical objects; and these relationships are leveraged throughout this document. In this chapter, we provide definitions for these objects and present some of the notation that will be used in later chapters.

#### 2.1 Orthomorphisms

**Definition 2.1.** *An orthomorphism,  $\pi$ , of a group,  $(G, +)$ , is a permutation of  $G$  with the property that the map  $x \mapsto -x + \pi(x)$  is also a permutation. An orthomorphism is canonical if  $\pi(0) = 0$ .*

**Definition 2.2.** *A complete map,  $\pi$ , of a group,  $(G, +)$ , is a permutation of  $G$  with the property that the map  $x \mapsto x + \pi(x)$  is a permutation.*

We will be primarily concerned with the group  $G = \mathbb{Z}_2^n$ . Since addition and subtraction are indistinguishable in  $\mathbb{Z}_2$ , the two definitions, orthomorphism and complete map, coincide. See [14] for a full characterization of all groups with this property.

$x$	$\pi(x)$	$\pi(x) + x$
(0, 0)	(0, 0)	(0, 0)
(0, 1)	(1, 0)	(1, 1)
(1, 0)	(1, 1)	(0, 1)
(1, 1)	(0, 1)	(1, 0)

Table 2.1: An orthomorphism of  $\mathbb{Z}_2^2$ 

**Example 1.** As an example of an orthomorphism of  $\mathbb{Z}_2^2$ , consider the permutation  $\pi : \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^2$  defined in the Table 2.1. We can see, in the rightmost column, that the map formed by adding the input of  $\pi$  to its output is indeed a permutation. Therefore  $\pi$  is an orthomorphism (and a complete map). The number of orthomorphisms of  $\mathbb{Z}_2^n$  for arbitrary  $n$  is unknown [35].

An alternate definition of orthomorphism can be stated in terms of a partial orthomorphism.

**Definition 2.3.** A partial orthomorphism of  $G$  is an injection  $\pi : S \rightarrow G$ , for some subset  $S \subseteq G$ , such that  $\pi(x) - x = \pi(y) - y$  implies  $x = y$  for all  $x, y \in S$ . The size of a partial orthomorphism is the cardinality of the domain  $S$ . If  $S = G$  then  $\pi$  is an orthomorphism.

Partial orthomorphisms are studied extensively in Chapter 3.

## 2.2 Latin Squares

**Definition 2.4.** A latin square of order  $N$  is an  $N \times N$  array of  $N$  symbols so that no symbol appears more than once in any row or column.

One family of latin squares is given by the Cayley tables of finite groups.

**Definition 2.5.** A transversal in a latin square of order  $N$  is a set of  $N$  distinct entries where no two entries appear in the same row or column.

**Example 2.** We use the Cayley table for  $\mathbb{Z}_2^2$  as an example in Figure 2.1. The bold entries constitute a transversal in this Latin square.

$\mathbb{Z}_2^2, +$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	<b>(0,0)</b>	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	<b>(1,1)</b>	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	<b>(0,1)</b>
(1,1)	(1,1)	<b>(1,0)</b>	(0,1)	(0,0)

Figure 2.1: A transversal in a Cayley table for  $\mathbb{Z}_2^2$

It is easily shown that an orthomorphism of a group corresponds directly to a transversal in a Cayley table for that group [10].

### 2.3 Notation for the Group $\mathbb{Z}_2^n$

The group  $(\mathbb{Z}_2^n, +)$  has a natural association with the set of bit strings of length  $n$  and the operation of bit-wise exclusive-or. More than that, there is a natural correspondence between bit strings of a fixed length  $n$  and the set of integers between 0 and  $2^n - 1$ . In this document, we will occasionally write elements of the group  $\mathbb{Z}_2^n$  with these associations in mind. For example, the element  $(1, 0, 0) \in \mathbb{Z}_2^3$  can be variously written as  $1||0^2$ ,  $1||\langle 0 \rangle_2$ ,  $100$ , or  $4$ .

Often, it is convenient to treat the group  $\mathbb{Z}_2^n$  as a vector space over  $\mathbb{Z}_2$  and use the theory developed in that setting. One case where this is especially useful is in the study

of the group  $\text{Aut}(\mathbb{Z}_2^n)$ . When  $\mathbb{Z}_2^n$  is treated as a vector space, the group  $\text{Aut}(\mathbb{Z}_2^n)$  is isomorphic to the general linear group  $\text{GL}_n(\mathbb{Z}_2)$ .



## Chapter 3

### PROPERTIES OF ORTHOMORPHISMS: CYCLE STRUCTURE

Despite receiving a fair amount of attention in the research literature, many basic questions remain concerning the number of orthomorphisms of a given group,  $G$ , 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 chapter, 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.

### 3.1 Introduction

Orthomorphisms have been studied extensively in the context of Latin squares. 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 [35] for an exposition of the current state of research in the context of Latin squares. In a series of articles, Evans has extended this work and has published on the existence of orthomorphisms and complete maps, including as a monograph on orthomorphism graphs (see [6, 8, 9, 10, 11, 12, 13, 14]). Further, the existence of extensions of partial orthomorphisms of various sizes for the group  $\mathbb{Z}_n$  has also been studied [2, 18, 33].

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.

### 3.2 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  $\pi$  is an orthomorphism. As conjugations, the functions  $C_h$  are bijective and cycle-type preserving [5, p. 125]. 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 3.1.** [19, p.361] *For any  $g \in \text{Aut}(\mathbb{Z}_2^n)$  and any orthomorphism  $\pi$  of  $\mathbb{Z}_2^n$ ,*

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

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

*Proof.* Since  $g, \pi$  are permutations of  $\mathbb{Z}_2^n$ , it suffices to show the map  $x \mapsto g\pi g^{-1}(x) - x$  is a permutation. Since  $\pi$  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 3.1 is generally true for any group  $G$ , not just  $\mathbb{Z}_2^n$ . Next we consider conjugating by translations.

**Lemma 3.2.** *For any  $k \in \mathbb{Z}_2^n$  and any orthomorphism  $\pi$  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  $T_k$  and  $\pi$  are permutations of  $\mathbb{Z}_2^n$ , it suffices to show that the map  $x \mapsto T_k \pi T_k^{-1}(x) - x$  is a permutation. Since  $\pi$  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. □

We note that, as the above proof shows, if  $G$  is an arbitrary group, then Lemma 3.2 holds.

**Corollary 3.3.** *If  $\pi$  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  $\pi$ .*

*Proof.* An immediate consequence of Lemmas 3.1 and 3.2. The cycle type of any permutation is preserved by conjugation [5, p. 125]. □

The final cycle-type preserving function on orthomorphism sets we describe in this paper is the inverse map, which will be used in Section 3.7. Once again, as the proof shows, the result is generally true for any group  $G$ .

**Lemma 3.4.** *For any orthomorphism  $\pi$  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  $\pi$ .*

*Proof.* Since  $\pi^{-1}$  is a permutation with the same cycle-type as  $\pi$ , it suffices to show  $x \mapsto \pi^{-1}(x) - x$  is injective. Let  $x, y \in \mathbb{Z}_2^n$ . Since  $\pi$  is bijective, there exist 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  $\pi$  is an orthomorphism,  $x' = y'$ . Further, since  $\pi$  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 3.4 and 3.5.

**Theorem 3.5.** *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  $g$  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  $g \in \text{Aut}(\mathbb{Z}_2^n)$ . 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 [5, Chapter 11] and [28]. □

### 3.3 Notation

**Definition 3.6.** If  $\pi$  is a partial orthomorphism of size one with a domain in  $\mathbb{Z}_2^n$  such that  $\pi(r) = i$ , then we write  $\pi$  as  $(i_r)$ . If  $\pi$  is a partial orthomorphism of size two such that  $\pi(r) = i$  and  $\pi(s) = j$  for distinct  $r, s$ , then we write  $\pi$  as  $(i_r, j_s)$ . Further, if  $\pi$  is a partial orthomorphism of size three such that  $\pi(r) = i$ ,  $\pi(s) = j$ , and  $\pi(t) = k$ , for distinct  $r, s, t$  then we write  $\pi$  as  $(i_r, j_s, k_t)$ .

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

**Definition 3.7.** *If  $\pi$  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  $\pi$  is denoted  $\mathcal{S}_n(i_r)$ , and  $\mathcal{S}(i_r)$  if the domain is clear from the context. Similarly, if  $(i_r, j_s)$  and  $(i_r, j_s, k_t)$  are partial orthomorphisms of size two and three, respectively, then the set of all orthomorphisms that extend is denoted  $\mathcal{S}(i_r, j_s)$  and  $\mathcal{S}(i_r, j_s, k_t)$ , respectively.*

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

**Definition 3.8.** *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.*

### 3.4 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 3.9.** *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.* First note that  $0, i, r$  must be distinct since  $(0_0, i_r)$  is a partial orthomorphism. 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 both linearly independent. So, by Theorem 3.5, there exists an automorphism  $g$  of  $\mathbb{Z}_2^n$  such that  $g(r) = r$  and  $g(i) = j$ . So 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 3.10.** *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  $\pi$  if and only if  $\pi(x) - x = 0$ . So, if  $r$  and  $s$  are fixed points of  $\pi$  then

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

but the map  $x \mapsto \pi(x) - x$  is a permutation when  $\pi$  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 3.5, 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. □

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

**Theorem 3.11.** *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.*

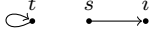
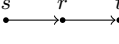

*Proof.* Let  $i, s, i', s' \in \mathbb{Z}_2^n$ . If  $i = s$  and  $i' = s'$  then  $C_h$  maps  $\mathcal{S}(i_s)$  onto  $\mathcal{S}(i'_{s'})$  bijectively when  $h = T_{s+s'}$ . If  $i \neq s$  and  $i' \neq s'$ , we can instead use the map  $h = T_{s'}gT_s$ , where  $g$  is any automorphism satisfying  $g(i + s) = i' + s'$ . We are left to show that  $\mathcal{S}(0_0)$  has the same cycle type distribution as  $\mathcal{S}(i_s)$  for some  $i \neq s$ . To this end, fix any  $0, i, s$  such that  $(0_0, i_s)$  is a partial orthomorphism. From Lemmas 3.9 and 3.10, we can write

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

and the statement is proved. □

### 3.5 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 possible cycle structures for any 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. In Case 3, however,  $(t_r, i_s)$  could be an orthomorphism without all of  $t, r, i, s$  being distinct. But if they are not distinct, any such orthomorphism would fall into Cases 1 or 2, so 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 3.12** (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 3.10 and Theorem 3.11, we have

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

□

**Lemma 3.13** (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 both linearly independent whenever  $(t_r, r_s)$  and  $(t'_{r'}, r'_{s'})$  are partial orthomorphisms. So, by Theorem 3.5, 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 3.14.** *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 3.13, 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,

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

$\square$

We now turn to Case 3.

**Lemma 3.15 (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 3.5, 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 3.16.** *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  $r, s, t \in \mathbb{Z}_2^n$  are distinct, we have

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

Using Lemma 3.15, Corollary 3.14, and Lemma 3.10, we see that, for any  $i \in \mathbb{Z}_2^n \setminus \{r, s, t, r + s + t\}$ ,

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

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

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

as desired. □

Finally, Lemma 3.17 will show that the orthomorphism sets from Cases 1 and 2 have the same distribution, and Lemma 3.18 will show that the orthomorphism sets from Cases 1 and 3 have the same distribution.

**Lemma 3.17.** *For distinct  $i, r, s, t \in \mathbb{Z}_2^n$  and  $n > 1$ ,*

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

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

$$\begin{aligned} \vec{d}(t_t, i_s) &= \left(\frac{1}{2^n - 2}\right) \vec{d}(i_s) && \text{Lemma 3.10} \\ &= \left(\frac{1}{2^n - 2}\right) \vec{d}(t_r) && \text{Theorem 3.11} \\ &= \vec{d}(t_r, r_s) && \text{Corollary 3.14.} \end{aligned}$$

□

**Lemma 3.18.** *For distinct  $r, s, t \in \mathbb{Z}_2^n$  and  $n > 1$ ,*

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

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

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

$$\begin{aligned} \vec{\mathbf{d}}(t_t, r_s) &= \left( \frac{1}{2^n - 2} \right) \vec{\mathbf{d}}(r_s) && \text{Lemma 3.10} \\ &= \left( \frac{1}{2^n - 2} \right) \vec{\mathbf{d}}(t_r) && \text{Theorem 3.11} \\ &= \vec{\mathbf{d}}(t_r, i_s), \end{aligned}$$

with the last equality holding: for  $i = r$  by Corollary 3.14; for all  $i \in \mathbb{Z}_2^n \setminus \{r, s, t, t + r + s\}$  by Corollary 3.16; and for  $i = s$  by Lemma 3.10. 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 3.19.** *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.*

As an illustration of Theorem 3.19, 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 3.1. All cycle types not listed have no orthomorphisms associated with them. In contrast to



the cycle-type distribution of orthomorphisms, we can see, in Figure 3.1, that the cycle-type distribution of permutations of  $\mathbb{Z}_2^4$  (for the cycle-types realized by orthomorphisms) is not proportional to that of orthomorphisms.

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

An important consequence of Theorem 3.19 is the following corollary.

**Corollary 3.20.** *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 [27] or Proposition 5.5 below), there exists a partial orthomorphism of size two that the orthomorphism extends. So, by Theorem 3.19, every partial orthomorphism of size two can be extended to an

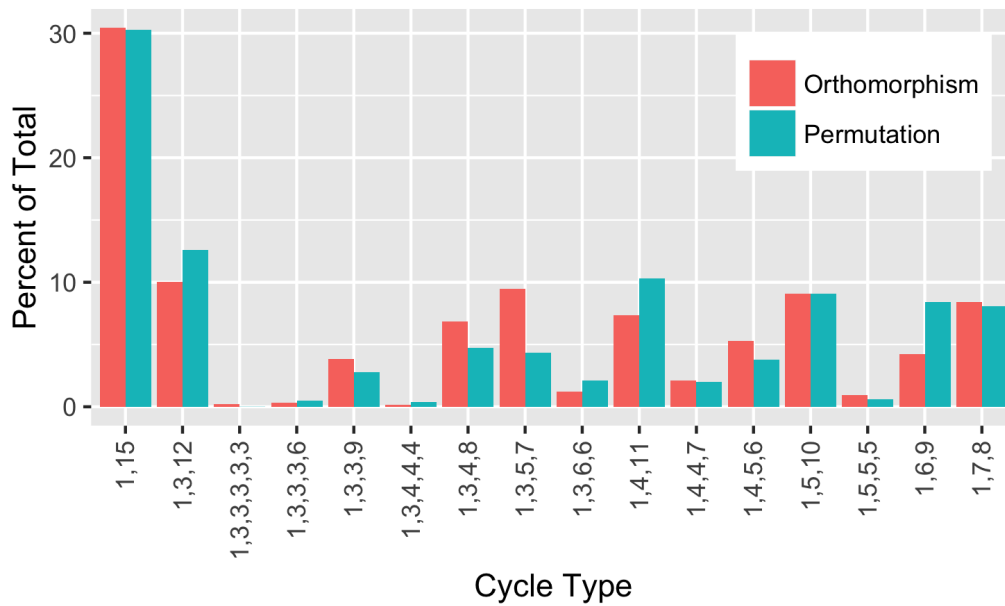


Figure 3.1: Cycle type distributions of orthomorphisms and permutations of  $\mathbb{Z}_2^4$  for cycle types realized by orthomorphisms of  $\mathbb{Z}_2^4$ .

orthomorphism. □

### 3.6 Examples and the Case of Size Three

**Example 3.** As shown in Theorem 3.19, 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  $\pi$ ,  $\sigma$ , and  $\tau$  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  $\pi$ , but there are 81,920 that extend  $\sigma$ . So the sets of orthomorphisms extending  $\pi$ ,  $\sigma$  do not share the same cardinality, much less the same distribution of cycle types.

On the other hand, the number of orthomorphisms extending  $\tau$  is also 84,224 which matches  $\pi$ , and yet these sets have different cycle-type distributions. See Table 3.2.

### 3.7 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.

Cycle Type	$\pi$	$\sigma$	$\tau$
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 3.2: Cycle-type distributions for  $\tau$ ,  $\pi$ , and  $\sigma$  defined in Example 3.

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 3.21.** *Suppose  $(i_r, j_s, k_t)$  and  $(i'_r, j'_s, k'_t)$  are partial orthomorphisms of  $\mathbb{Z}_2^n$ .*

Then

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

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 3.5, 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 3.21 is insignificant, as we see in Remark 3.22 below, since many symmetries exist among the parameters.

**Remark 3.22.** 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 3.4 of Section 3.2, 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 3.21, 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 3.22, we can reduce the upper bound on the number of cycle-type distributions further.

Note that there exist no partial orthomorphisms of  $\mathbb{Z}_2^n$  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 3.23** (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 3.21.  $\square$

**Lemma 3.24** (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 3.21, 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 3.22, 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 3.4, an orthomorphism set that satisfies equation (a) has the same cycle-type distribution as a set that satisfies equation (c). Thus, there are at most 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 3.25** (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 3.21.  $\square$

**Lemma 3.26** (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 3.21, 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 3.4, 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 3.27** (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 3.21, 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. One set of relations corresponds to the set  $\{i + r, j + r, s + r, k + r, t + r\}$  being linearly independent, and another corresponds to the single 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.

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

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



For the equations of Type 1a, we may relabel the elements in  $(i_r, j_s, k_t)$  and use Remark 3.22 to show  $\vec{d}(i_r, j_s, k_t)$  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 3.4.

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

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

**Theorem 3.28.** *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  $n$ , it happens that fewer than 12 cycle-type distributions are realized. For example, when  $n = 1$ , 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 3.3 for 9 representative partial orthomorphisms of size 3 and their cycle-type distribu-

tions, where we use the notation  $2^3i_3 + 2^2i_2 + 2i_1 + i_0 \in \mathbb{Z}$  for  $(i_3, i_2, i_1, i_0) \in \mathbb{Z}_2^4$ . 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  $n$ .

Chapter 3. Properties of Orthomorphisms: Cycle Structure

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

## Chapter 4

### PROPERTIES OF ORTHOMORPHISMS: GROUP ACTIONS

In Chapter 3, we proved statements about the structure of orthomorphism sets with the help of several cycle-type preserving group actions. In this chapter, we focus on a single group action: the group of automorphisms of  $\mathbb{Z}_2^n$  acting on the set of orthomorphisms of  $\mathbb{Z}_2^n$ , where  $n > 1$ , via conjugation. Specifically, we prove several statements about the orbits and stabilizers of orthomorphisms under this action.

#### 4.1 Introduction

As introduced in the previous chapter, there are several functions defined on the set of orthomorphisms that preserve cycle type. In this chapter, we consider a broader set of maps that preserve the orthomorphism property of a permutation; and we examine their effects on orbits and stabilizers. Specifically, we consider three functions, introduced in [19], defined on the set of orthomorphisms of  $\mathbb{Z}_2^n$ : the inverse map,  $R(\pi) = \pi^{-1}$ ; addition of the identity function,  $I(\pi) = \pi + \text{id}$ ; and translation,  $T_k(\pi) = \pi + k$ . Each of these functions map orthomorphisms to orthomorphisms, but only the inverse map preserves the cycle type of an orthomorphism.

Further, we find that functions  $I$  and  $R$  act on orbits as well as the orthomorphisms themselves, where the translation maps,  $T_k$ , do not. However, we prove the distribution of orthomorphisms among orbits, when  $T_k$  and  $T_{k'}$  is applied to an initial orbit, are the same. Further, though  $T_k$  does not preserve cycle-type, much less, orbit membership, we prove the distribution of translations  $T_k$ , for all  $k \in \mathbb{Z}_2^n$ , among orbits of any two orthomorphisms, in an initial orbit, are the same.

The final result of this chapter has applications to the stabilizer of an orthomorphism, and the set of orthomorphisms fixed when conjugated by automorphisms. Specifically, the biconditional statement presented describes a relationship between the cycles of commuting permutations.

## 4.2 Orthomorphism-Preserving Maps

In this section, we discuss in more detail two of the previously introduced functions defined on the set of orthomorphisms of  $\mathbb{Z}_2^n$ : addition of the identity function,  $I(\pi) = \pi + \text{id}$ ; and translation,  $T_k(\pi) = \pi + k$ . In Section 3.2, we showed that the inverse of an orthomorphism is an orthomorphism, and conjugating an orthomorphism by an automorphism produces an orthomorphism, for any group.

**Lemma 4.1.** *For any orthomorphism  $\pi$  of  $\mathbb{Z}_2^n$ , the map*

$$I(\pi) = \pi + \text{id}$$

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

*Proof.* Since  $I(\pi)$  is a permutation of  $\mathbb{Z}_2^n$ , it suffices to show that the map  $x \mapsto I\pi(x) - x$

is a permutation. Since  $I\pi(x) - x = \pi(x) + x - x = \pi(x)$ , the statement is proved.  $\square$

We note that orthomorphisms that satisfy this property for arbitrary groups are called *strong complete maps*. The group  $\mathbb{Z}_2^n$  is unusual in that all orthomorphisms are strong complete maps. For a full characterization of the groups that admit strong complete maps, see [14].

**Lemma 4.2.** *For any  $k \in \mathbb{Z}_2^n$  and any orthomorphism  $\pi$  of  $\mathbb{Z}_2^n$ , the map*

$$T_k(\pi) = \pi + k$$

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

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

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

is also a permutation.  $\square$

### 4.3 Notation

In the previous chapter, we defined an auxiliary function  $\vec{d}$  to describe the distribution of cycle types of orthomorphisms. In this chapter, we do something similar for the distribution of orbits.

**Definition 4.3.** For a fixed  $n$ , let  $\mathcal{O}_n$  be the set of all orbits of orthomorphisms of  $\mathbb{Z}_2^n$ . Then for any set of orthomorphisms  $A$ , we define

$$\vec{d}(A) = (n_t)_{t \in \mathcal{O}_n}$$

to be the  $|\mathcal{O}_n|$ -tuple of nonnegative integers, indexed by  $\mathcal{O}_n$ , whose entries  $n_t$  equal the number of elements of  $A$  in orbit  $t$ .

**Remark 4.4.** For the remaining sections, for ease of notation, we let  $G$  be the group of automorphisms of  $\mathbb{Z}_2^n$ . Further, we assume  $n > 1$  for all references to integer  $n$ .

### 4.4 The $G$ -Orbit of an Orthomorphism

In this section, we consider the  $G$ -orbit of an orthomorphism,  $\pi$ . That is, we consider the set  $\text{orb}_G(\pi) = \{g\pi g^{-1} : g \in G\}$ . It can be shown that all elements of  $\text{orb}_G(\pi)$  have the same cycle type. However, the set of all orthomorphisms with the same cycle type do not necessarily lie in the same orbit, as demonstrated below.

**Lemma 4.5.** If  $\sigma, \tau \in \text{orb}_G(\pi)$ , then  $\sigma$  and  $\tau$  have the same cycle type.

*Proof.* Since  $\sigma$  and  $\tau$  are conjugate permutations, the result follows from [5, p.126].  $\square$

The converse does not hold, as is illustrated in Figure 4.1, where we see that there are 804 orbits of the set of canonical orthomorphisms of  $\mathbb{Z}_2^4$  and only 16 possible cycle types.

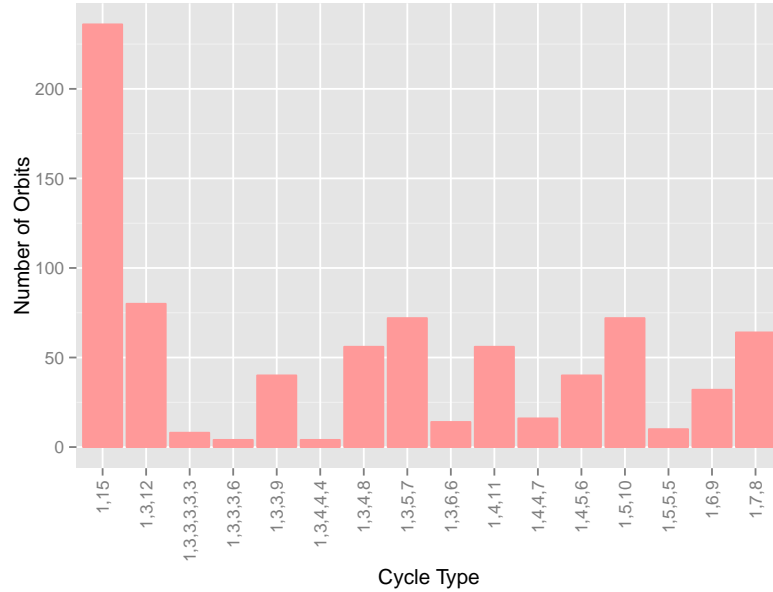


Figure 4.1: Cycle type distribution of the  $G$ -orbits of canonical  $\mathbb{Z}_2^4$  orthomorphisms.

#### 4.4.1 Effect of orthomorphism-preserving mappings

In this section, we examine the effects of orbit membership when applying each of the three orthomorphism-preserving functions. For functions  $F \in \{T_k\}_{k \neq 0} \cup \{R, I\}$ , it is typically not the case that  $\tau \in \text{orb}_G(\pi)$  implies  $F(\tau) \in \text{orb}_G(\pi)$ . However,  $R$  and  $I$  do satisfy a different statement:  $F(\tau) \in \text{orb}_G(F(\pi))$  when  $\tau \in \text{orb}_G(\pi)$ , while translation typically does not. Instead, we show there exists a prescribed pattern to the distribution of translated functions among orbits, and therefore, the cycle type distribution of those translated functions as well.



**Example 4.** In the next example, we write elements of  $\mathbb{Z}_2^4$  as integers (using the usual binary correspondence) and we use cyclic notation to describe the orthomorphisms. We show  $\tau \in \text{orb}_G(\pi)$  does not imply  $F(\tau) \in \text{orb}_G(\pi)$  for all orthomorphism-preserving functions  $F$ . Consider the orthomorphism  $\pi = (0)(1\ 2\ 6)(3\ 11\ 9\ 4\ 10\ 12\ 13\ 8\ 7\ 14\ 5\ 15)$  of  $\mathbb{Z}_2^4$ . There are 20160 elements in  $\text{orb}_G(\pi)$ , all of which have cycle type 1, 3, 12. The orthomorphisms

$$T_3(\pi) = (1)(0\ 3\ 8\ 4\ 9\ 7\ 13\ 11\ 10\ 15)(2\ 5\ 12\ 14\ 6) \text{ and}$$

$$I(\pi) = (0)(1\ 3\ 8\ 15\ 12)(2\ 4\ 14\ 11)(5\ 10\ 6\ 7\ 9\ 13)$$

have cycle types 1, 5, 10 and 1, 4, 5, 6, respectively, and therefore cannot be elements of  $\text{orb}_G(\pi)$  by Lemma 4.5. Applying the inverse map to  $\pi$  yields the orthomorphism

$$R(\pi) = (0)(1\ 6\ 2)(3\ 15\ 5\ 14\ 7\ 8\ 13\ 12\ 10\ 4\ 9\ 11)$$

which, as can be verified computationally, it is not a member of  $\text{orb}_G(\pi)$ .

As this example illustrates, there exist orbit elements that  $T_k$ ,  $R$ , and  $I$  map out of their orbits. However,  $R$  and  $I$  map all elements of a single orbit to a single common destination orbit, which is possibly different from the originating orbit. This is not the case for  $T_k$ , as we will see.

**Lemma 4.6.** *If  $\tau \in \text{orb}_G(\pi)$  then  $I(\tau) \in \text{orb}_G(I(\pi))$ .*

*Proof.* If  $\tau \in \text{orb}_G(\pi)$  then there exists  $g \in G$  such that  $\tau = g\pi g^{-1}$ . Hence

$$\begin{aligned} I(\tau) &= \tau + \text{id} \\ &= g\pi g^{-1} + \text{id} \\ &= g(\pi + \text{id})g^{-1} \\ &= gI(\pi)g^{-1}. \end{aligned}$$

Therefore,  $I(\tau) \in \text{orb}_G(I(\pi))$ . □

**Lemma 4.7.** *If  $\tau \in \text{orb}_G(\pi)$  then  $R(\tau) \in \text{orb}_G(R(\pi))$ .*

*Proof.* If  $\tau \in \text{orb}_G(\pi)$  then there exists  $g \in G$  such that  $\tau = g\pi g^{-1}$ . Hence

$$\begin{aligned} R(\tau) &= \tau^{-1} = (g\pi g^{-1})^{-1} \\ &= g(\pi^{-1})g^{-1} \\ &= (g)R(\pi)g^{-1}. \end{aligned}$$

Therefore,  $R(\tau) \in \text{orb}_G(R(\pi))$ . □

**Example 5.** We continue from Example 4 to show that translations do not map orbits to orbits. As before, let  $\pi = (0)(1\ 2\ 6)(3\ 11\ 9\ 4\ 10\ 12\ 13\ 8\ 7\ 14\ 5\ 15)$  and consider the orthomorphism  $\tau = (0)(1\ 13\ 14\ 6\ 4\ 3\ 10\ 5\ 8\ 9\ 15\ 11)(2\ 7\ 12)$  of  $\mathbb{Z}_2^4$  and automorphism  $g = (0)(1\ 11\ 3\ 13\ 9\ 5\ 7)(2\ 6\ 10\ 8\ 14\ 4\ 12)(15)$  of  $\mathbb{Z}_2^4$ . Since  $\tau = g^{-1}\pi g$ , we have  $\tau \in \text{orb}_G(\pi)$ . However,  $T_4(\tau)$  has cycle type  $(1, 3, 12)$  and  $T_4(\pi)$  has cycle type  $(1, 5, 10)$ , thus  $T_4(\tau) \notin \text{orb}_G(T_4(\pi))$ .

As Example 5 shows, translations do not act on orbits. However, there are many symmetries within translated orbits which we see in several of the following statements. To start, we describe a commuting condition on translation maps and conjugation by automorphisms. This lemma will be used in several of the following statements.

**Lemma 4.8.** *If  $\pi$  is an orthomorphism of  $\mathbb{Z}_2^n$  and  $g \in G$  then, for some nonzero  $k \in \mathbb{Z}_2^n$ ,*

$$T_k(g\pi g^{-1}) = gT_{g^{-1}(k)}(\pi)g^{-1}.$$

*Proof.* Let  $\pi$  be an orthomorphism of  $\mathbb{Z}_2^n$  and  $g$  be an automorphism of  $\mathbb{Z}_2^n$ . Then, for any nonzero  $k \in \mathbb{Z}_2^n$ , we have

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

as desired. □

The first theorem we discuss shows that, even though  $T_k(\sigma)$  and  $T_k(\tau)$  are not necessarily in the same orbit when  $\tau$  and  $\sigma$  are, if we take the collection of translations  $\{T_k\}_{k \in \mathbb{Z}_2^n}$  and apply those to  $\sigma$  and  $\tau$ , we end up with two collections of orthomorphisms distributed among orbits in the same way.

**Theorem 4.9.** *If  $\tau, \sigma \in \text{orb}_G(\pi)$  then*

$$\vec{\mathbf{d}}(\{T_k(\tau)\}_{k \in \mathbb{Z}_2^n}) = \vec{\mathbf{d}}(\{T_k(\sigma)\}_{k \in \mathbb{Z}_2^n}).$$

*Proof.* If  $\tau, \sigma \in \text{orb}_G(\pi)$ , then there exists  $g \in G$  such that  $\sigma = g\tau g^{-1}$ . Since conjugate permutations are in the same orbit, we have

$$\begin{aligned} \vec{\mathbf{d}}(\{T_k(\tau)\}_{k \in \mathbb{Z}_2^n}) &= \vec{\mathbf{d}}(\{\tau + k\}_{k \in \mathbb{Z}_2^n}) \\ &= \vec{\mathbf{d}}(\{g(\tau + k)g^{-1}\}_{k \in \mathbb{Z}_2^n}). \end{aligned}$$

Simplifying the right hand side by using Lemma 4.8, and using the fact that  $\{k\}_{k \in \mathbb{Z}_2^n} = \{g(k)\}_{k \in \mathbb{Z}_2^n}$  when  $g$  is a permutation, we get

$$\begin{aligned} \{g(T_k(\tau))g^{-1}\}_{k \in \mathbb{Z}_2^n} &= \{T_{g(k)}(g\tau g^{-1})\}_{k \in \mathbb{Z}_2^n} \\ &= \{T_k(\sigma)\}_{k \in \mathbb{Z}_2^n}. \end{aligned}$$

Thus

$$\vec{\mathbf{d}}(\{T_k(\tau)\}_{k \in \mathbb{Z}_2^n}) = \vec{\mathbf{d}}(\{T_k(\sigma)\}_{k \in \mathbb{Z}_2^n}).$$

□

**Corollary 4.10.** *For any orthomorphism  $\pi$  of  $\mathbb{Z}_2^n$ ,*

$$\vec{\mathbf{d}}(\{T_k(\text{orb}_G(\pi))\}_{k \in \mathbb{Z}_2^n}) = |(\text{orb}_G(\pi))| \cdot \vec{\mathbf{d}}(\{T_k(\pi)\}_{k \in \mathbb{Z}_2^n})$$

*Proof.* The statement follows directly from Theorem 4.9.  $\square$

In the next theorem, we show that for any two orbits, each non-identity translation maps the same number of elements from one orbit to the other.

**Theorem 4.11.** *For any two orbits  $t, t' \in \mathcal{O}_n$  and nonzero  $k_1, k_2 \in \mathbb{Z}_2^n$ , if  $N_1 = \{\tau \in t : \tau + k_1 \in t'\}$  and  $N_2 = \{\tau \in t : \tau + k_2 \in t'\}$  then*

$$|N_1| = |N_2|$$

*Proof.* Let  $g$  be any automorphisms such that  $g(k_1) = k_2$ . We will show  $gN_1g^{-1} = N_2$ . To begin, we show  $gN_1g^{-1} \subseteq N_2$ . To that end, let  $\pi \in gN_1g^{-1}$ , then there exists  $\tau \in N_1$  such that  $\pi = g\tau g^{-1}$ . Further,

$$\pi + k_2 = T_{k_2}(g\tau g^{-1}) = gT_{k_1}(\tau)g^{-1}$$

by Lemma 4.8. Since  $\pi + k_2$  is conjugate to  $T_{k_1}(\tau) \in t'$ , we have  $\pi + k_2 \in t'$  and therefore  $\pi \in N_2$ . Thus  $gN_1g^{-1} \subseteq N_2$ . Since the reverse containment  $N_2 \subseteq gN_1g^{-1}$  is equivalent to  $g^{-1}N_2g \subseteq N_1$ , we may simply swap the roles of  $g, k_1, N_1$  with  $g^{-1}, k_2, N_2$ , respectively, in the argument above to prove the desired result.  $\square$

As a corollary, we show that translating an orbit by any non-identity element of  $\mathbb{Z}_2^n$  distributes its members among the other orbits in the same way, regardless of the non-identity  $\mathbb{Z}_2^n$  element chosen. So, not only is the cycle-type distribution of  $T_k(\text{orb}(\pi))$  the same as  $T_{k'}(\text{orb}(\pi))$ , but the distribution of their elements among orbits is the same for both sets.

**Corollary 4.12.** *For all nonzero  $k, k' \in \mathbb{Z}_2^n$ , if  $\pi$  is an orthomorphism of  $\mathbb{Z}_2^n$ , then*

$$\vec{\mathbf{d}}(\{T_k(\tau)\}_{\tau \in \text{orb}_G(\pi)}) = \vec{\mathbf{d}}(\{T_{k'}(\tau)\}_{\tau \in \text{orb}_G(\pi)}).$$

*Proof.* Let  $t = \text{orb}_G(\pi)$ . Then for each subscript  $t' \in \mathcal{O}_n$  in the distribution vector  $\vec{\mathbf{d}}(\cdot)$  we have, by Theorem 4.11,

$$\vec{\mathbf{d}}_{t'}(\{T_k(\tau)\}_{\tau \in t}) = \vec{\mathbf{d}}_{t'}(\{T_{k'}(\tau)\}_{\tau \in t}).$$

As this holds for each  $t' \in \mathcal{O}_n$ , the corollary is proved. □

#### 4.5 The $G$ -Stabilizer of an Orthomorphism

In this section we briefly consider the stabilizer of an orthomorphism,  $\text{stab}_G(\pi) = \{g \in G : g\pi g^{-1} = \pi\}$ , and show that the orthomorphism preserving functions  $R$  and  $I$  preserve stabilizer membership where  $T_k$  does not in all cases.

**Lemma 4.13.** *For any orthomorphism  $\pi$  of  $\mathbb{Z}_2^n$ , we have  $g \in \text{stab}_G(\pi)$  if and only if  $g \in \text{stab}_G(I(\pi))$ .*

*Proof.* Suppose  $g \in \text{stab}_G(\pi)$  then

$$\begin{aligned}
 gI(\pi)g^{-1}(x) &= g(\pi + \text{id})g^{-1}(x) \\
 &= g(\pi(g^{-1}(x) + g^{-1}(x))) \\
 &= g\pi g^{-1}(x) + gg^{-1}(x) \\
 &= \pi(x) + x \\
 &= I(\pi).
 \end{aligned}$$

Now, if  $g \in \text{stab}_G(I(\pi))$  then  $\pi = I(I(\pi))$  and we apply the statement of the forward implication to conclude  $g \in \text{stab}_G(I(I(\pi))) = \text{stab}_G(\pi)$ .  $\square$

**Lemma 4.14.** *For any orthomorphism  $\pi$  of  $\mathbb{Z}_2^n$ , we have  $g \in \text{stab}_G(\pi)$  if and only if  $g \in \text{stab}_G(R(\pi))$ .*

*Proof.* We have  $\pi \in \text{stab}_G(\pi)$  if and only if

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

which holds if and only if  $g \in \text{stab}_G(R(\pi))$ .  $\square$

**Lemma 4.15.** *For any orthomorphism  $\pi$  of  $\mathbb{Z}_2^n$  and any  $k \in \mathbb{Z}_2^n$ , suppose  $g \in G$  satisfies  $g(k) = k$ . Then*

$$g \in \text{stab}_G(\pi) \iff g \in \text{stab}_G(T_k(\pi)).$$

*Proof.* Suppose  $g \in \text{stab}_G(\pi)$ . If  $g(k) = k$ , then by Lemma 4.8

$$\begin{aligned} gT_k(\pi)g^{-1} &= T_{g(k)}(g\pi g^{-1}) \\ &= T_{g(k)}(\pi) \\ &= T_k(\pi). \end{aligned}$$

So,  $g \in \text{stab}_G(T_k(\pi))$ . Now, if  $g \in \text{stab}_G(T_k(\pi))$  and  $g(k) = k$  then we note that  $T_k(T_k(\pi)) = \pi$  and we apply the statement of the forward implication to conclude  $g \in \text{stab}_G(T_k(T_k(\pi))) = \text{stab}_G(\pi)$ .  $\square$

#### 4.6 Characterization of Commuting Permutations

Analyzing the cycle structure of orthomorphisms in the context of group actions leads to an investigation of the relationship between the cycle structure of the automorphisms that act on the orthomorphisms, and the orthomorphisms themselves. A product of that investigation is the following biconditional statement which, in its most general form, characterizes permutations that commute with each other. As a consequence, we get statements about the stabilizers of orthomorphisms and the sets of orthomorphisms that fix automorphisms, as these are just particular collections of commuting permutations.

For ease of notation, we use cyclic notation to describe an arbitrary permutation  $\pi$  as follows

$$\pi = (x_{11}x_{12} \cdots x_{1s_1}) \cdots (x_{r1}x_{r2} \cdots x_{rs_r}). \quad (4.16)$$



Second subscripts are taken modulo their respective cycle length, that is to say,  $x_{k,\beta} = x_{k,\beta \bmod s_k}$ . Additionally, we can refer to a cycle in a permutation using orbit notation. For example, we can write the first cycle in the permutation  $\pi$  above as  $\text{orb}_\pi(x_{11}) = \{x_{11}, x_{12}, \dots, x_{1s_1}\}$ .

**Example 6.** To illustrate the notation, consider the orthomorphism  $\pi = (0)(1\ 2\ 5\ 3\ 7\ 6\ 4)$  of  $\mathbb{Z}_2^3$ . Since this permutation has two cycles, we have  $r = 2$ . The first cycle has one element so  $s_1 = 1$  and the second has 7 elements so  $s_2 = 7$ . Further, we can write  $\text{orb}_\pi(1) = \{1, 2, 3, 4, 5, 6, 7\}$ .

**Theorem 4.17.** *Let  $\pi$  and  $g$  be permutations of a set  $X$  where  $\pi$  is as in (4.16). Then  $\pi$  and  $g$  commute with each other if and only if for all positive integers  $k \leq r$  there exist subscripts  $j \leq s_k$  and  $i \leq r$  such that  $g(x_{k,\beta}) = x_{i,j+\beta}$  for all positive integers  $\beta \leq s_k$ .*

*Proof.* For the forward implication, suppose  $g\pi = \pi g$  and  $k$  is some positive integer less than or equal to  $r$ . Then, since  $g$  is a function of  $X$ , there exist positive integers  $i \leq r, j \leq s_i$  such that  $g(x_{k,1}) = x_{i,j+1}$ . So, for any  $\beta \leq s_k$ , we have

$$\begin{aligned} g(x_{k,\beta}) &= g(\pi^{\beta-1}(x_{k,1})) \\ &= \pi^{\beta-1}(g(x_{k,1})) \\ &= \pi^{\beta-1}(x_{i,j+1}) \\ &= x_{i,j+\beta}, \end{aligned}$$

as desired.

Conversely, we will show  $\pi$  and  $g$  commute with each other. To that end, let  $x_{k,\beta} \in$

$\mathbb{Z}_2^n$ . Then by the hypothesis

$$\pi(g(x_{k,\beta})) = \pi(x_{i,j+\beta}) = x_{i,j+\beta+1}.$$

Similarly, we get

$$g(\pi(x_{k,\beta})) = g(x_{k,\beta+1}) = x_{i,j+\beta+1},$$

and the result is proved. □

**Example 7.** To illustrate Theorem 4.17, consider the orthomorphism introduced in Example 6,  $\pi = (0)(1\ 2\ 5\ 3\ 7\ 6\ 4)$ , and the automorphism  $g = (0)(1\ 5\ 7\ 4\ 2\ 3\ 6)$ . Since  $g \in \text{stab}_G(\pi)$ , the two permutations  $g$  and  $\pi$  commute. The theorem states that, for any  $\pi$ -cycle (or  $\pi$ -orbit) with index  $k \leq r$ ,  $g$  maps all of its elements to  $\pi$ -cycle with index  $i$ . In the case of this example,  $g$  maps the  $k = 2$  cycle of  $\pi$  to the  $i = 2$  cycle. Further, the theorem states,  $g$  maps the first element of that cycle to the element in position  $j + 1$ , which in this case, is the element in position  $2 + 1 = 3$ . The remaining elements mapped follow the same shift pattern as is illustrated in Figure 4.2.

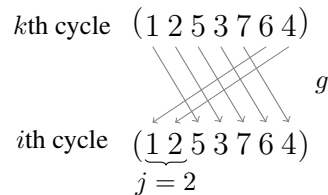


Figure 4.2: Element  $g$  maps  $k$ th cycle of  $\pi$  to  $i$ th cycle of  $\pi$  with shift  $j$

With this theorem we can begin to investigate the structure of the cycles of  $g$  relative to  $\pi$ , specifically, this theorem considers where elements of  $\pi$ -cycles are mapped to by

$g$ ; and the patterns of those mappings determine their commutative property. In the following corollaries, we assume  $g$  and  $\pi$  commute. In the next corollary we find the size of  $g$ -orbits of elements of the same  $\pi$ -orbit are the same.

**Corollary 4.18.** *Suppose  $g$  commutes with  $\pi$ . Then, for any  $1 \leq k \leq r$ ,  $|\text{orb}_g(x_{k1})| = |\text{orb}_g(x_{k\beta})|$  for all  $1 \leq \beta \leq s_k$ .*

*Proof.* Suppose  $g$  commutes with  $\pi$ . By definition of orbit,

$$\text{orb}_g(x_{k,1}) = \{g^i(x_{k1}) : i \leq m\}$$

where  $m$  is the least positive integer such that  $g^{m+1}(x_{k1}) = x_{k1}$ . Note that the integer  $m$  exists since the domain of the permutation  $g$  is finite. Further,  $m$  is the least positive integer such that  $g^{m+1}(x_{k0\beta}) = x_{k0\beta}$ , for all  $\beta$ , by Theorem 4.17. Thus,

$$|\text{orb}_g(x_{k1})| = |\text{orb}_g(x_{k\beta})|$$

for all  $1 \leq \beta \leq s_k$ . □

In the next corollary, when we consider the case where  $g$  maps an element  $x$  of a  $\pi$ -orbit back into its  $\pi$  orbit, we are able to state the size of  $\text{orb}_g(x)$  explicitly.

**Corollary 4.19.** *If  $g$  commutes with  $\pi$  and  $g(x_{k1}) \in \text{orb}_\pi(x_{k1})$ , then for all  $1 \leq \beta \leq s_k$ ,*

$$|\text{orb}_g(x_{k\beta})| = \frac{s_k}{\text{gcd}(s_k, j)}$$

where  $j$  satisfies  $g(x_{k1}) = x_{k,1,j}$ .

*Proof.* If  $g$  commutes with  $\pi$  and  $g(x_{k1}) = x_{k,1+j}$  for some  $1 \leq j \leq s_k$ , then by Theorem 4.17, for all  $1 \leq \beta \leq s_k$ ,

$$\begin{aligned} g(x_{k,\beta}) &= x_{k,\beta+j} \\ &= \pi^j(x_{k,\beta}). \end{aligned}$$

Applying  $g$  repeatedly, we get  $g^t(x_{k,\beta+tj}) = \pi^{tj}(x_{k,\beta})$  for all  $t$ . Thus  $\text{orb}_g(x_{k,\beta}) = \text{orb}_{\pi^j}(x_{k,\beta})$  for all  $1 \leq \beta \leq s_k$ . Since the second subscript is taken modulo  $s_k$ , we have  $|\{\beta + tj \bmod s_k\}_{t \in \mathbb{Z}}| = s_k / \gcd(s_k, j)$  elements in  $\text{orb}_{\pi^j}(x_{k,\beta})$ . Therefore,  $|\text{orb}_g(x_{k,\beta})| = s_k / \gcd(s_k, j)$ .  $\square$

And, as our final corollary of Theorem 4.17, we show that if a  $g$ -orbit and a  $\pi$ -orbit share any elements, then the sizes of several related orbits are the same.

**Proposition 4.20.** *If  $g$  and  $\pi$  commute then*

$$\text{orb}_g(x_{k1}) \cap \text{orb}_\pi(x_{k'1}) \neq \emptyset$$

*implies*

$$\text{orb}_g(x_{k\beta}) \cap \text{orb}_\pi(x_{k'\beta}) \neq \emptyset$$

*for all  $1 \leq \beta \leq s_k$ . In particular,  $s_k = s_{k'}$ .*

*Proof.* Suppose  $g$  and  $\pi$  commute and  $\text{orb}_g(x_{k1}) \cap \text{orb}_\pi(x_{k'1}) \neq \emptyset$ . Then there exists  $t$  and  $j$  such that  $g^t(x_{k1}) = x_{k'1+j}$ . Further, by Theorem 4.17,  $g^t(x_{k\beta}) = x_{k'\beta+j}$  for all

$1 \leq \beta \leq s_k$ . Hence,

$$\text{orb}_g(x_{k\beta}) \cap \text{orb}_\pi(x_{k'1}) \neq \emptyset.$$

Finally, we show  $g^t$  defines a bijective mapping from  $\text{orb}_\pi(x_{k1})$  to  $\text{orb}_\pi(x_{k'1})$ , proving  $s_k = s_{k'}$ . Let  $x_{k'q} \in \text{orb}_\pi(x_{k'1})$ . Then

$$\begin{aligned} x_{k'q} &= \pi^{q-j-1}(x_{k'1+j}) \\ &= \pi^{q-j-1}(g^t(x_{k1})) \\ &= g^t(\pi^{q-j-1}(x_{k1})) \\ &= g^t(x_{kq-j}) \end{aligned}$$

which proves  $g^t$  is surjective. Injectivity follows from the fact that  $g^t$  is a permutation. □

**Remark 4.21.** Theorem 4.17 and its corollaries describe the cycle structure of permutations that commute with each other. These statements can be applied to the collection of automorphisms that commute with  $\pi$  (i.e.,  $\text{stab}_G(\pi)$ ) to possibly determine the set of valid cycle-types of orthomorphisms among other things. In future work, we hope to apply these results to the sets of orthomorphisms that leave automorphisms fixed and use Burnside's Lemma to determine, or bound, the number of orthomorphisms that exist.

## Chapter 5

### GETTING A COUNT

A *transversal* in a latin square of order  $N$  is a set of  $N$  entries such that no two entries are in the same row or column. It is known that transversals in the Cayley table (a Latin square) of a group correspond to orthomorphisms of that group. In this chapter, we use this association to prove a lower bound on the number of orthomorphisms of the group  $\mathbb{Z}_2^n$ , and to derive an explicit formula that gives an orthomorphism of  $\mathbb{Z}_2^n$ , for  $n > 2$ . Further, we show that a proposed upper bound on the number of orthomorphisms of  $\mathbb{Z}_2^n$  is no tighter than the known best upper bound for transversals in Latin squares. Lastly, we present the current results of the ongoing endeavor to determine the number of orthomorphisms of  $\mathbb{Z}_2^5$ .

#### 5.1 Introduction

There has been significant research on the number of transversals in Cayley tables for  $\mathbb{Z}_N$  when  $N$  is odd and, more generally, on the number of transversals in arbitrary latin squares of order  $N$ . Current known counts are given in Figure 5.1. The bold entries correspond to the group  $\mathbb{Z}_2^n$  with  $N = 2^n$ .

N	Number of transversals in groups of order $N$
3	3
4	0, <b>8</b>
5	15
7	133
8	0, <b>384</b> , 384, 384, 384
9	2025, 2241
11	37851
12	0, 198144, 76032, 46080, 0
13	1030367
15	36362925
16	0, 235765760, 237010944, 238190592, <b>244744192</b> , 125599744, 121143296, 123371520, 123895808, 122191872, 121733120, 62881792, 62619648, 62357504
17	1606008513
19	87656896891
20	0, 697292390400, 140866560000, 0, 0
21	5778121715415, 826814671200
23	452794797220965

Table 5.1: Transversal counts for groups of order  $\leq 23$ . Table adapted from [35].

A thorough discussion of the current state of research in this area is given in [35]. If  $N \geq 5$  and we denote by  $T(N)$  the maximum number of transversals of any latin square of order  $N$ , then this quantity is known [24] to be bounded by the following inequality:

$$15^{N/5} \leq T(N) \leq c^N \sqrt{N} N! \quad (5.1)$$

where  $c = \sqrt{\frac{3 - \sqrt{3}}{6}} e^{\sqrt{3}/6} \approx 0.61354$ .

By contrast, the literature concerning the number of orthomorphisms of the group  $\mathbb{Z}_2^n$  is much more limited. If  $\mathcal{S}_n$  is the number of orthomorphisms of  $\mathbb{Z}_2^n$  then [29] provides

a lower bound on the number of orthomorphisms of  $\mathbb{Z}_2^n$ . (Unfortunately, as of the time of this writing, some translation issues prevented our complete understanding of their proof.) In any case, their purported bound is:

$$\mathcal{S}_n \geq \mathcal{S}_{n-3}^2 \times 2^{n!!}$$

for  $n > 4$ , which would represent the strongest bound known.

In this chapter, we present a different lower bound on the number of orthomorphisms of  $\mathbb{Z}_2^n$  by using features of a Cayley table of  $(\mathbb{Z}_2^n, +)$ . We walk through the proof of the lower bound, Theorem 5.2, with the help of an example. In addition, we discuss an upper bound on the number of orthomorphisms of  $\mathbb{Z}_2^n$ . Lastly, we present a formula for an orthomorphism of  $\mathbb{Z}_2^n$  with a proof that the stated function is actually an orthomorphism.

## 5.2 A Lower Bound

**Theorem 5.2.** *If  $\mathcal{S}_n$  is the number of orthomorphisms of the group  $\mathbb{Z}_2^n$  for  $n \geq 3$ , then*

$$\mathcal{S}_n \geq \mathcal{S}_{n-1} 2^{2^{n-2}} (2^{n-1} - 1).$$

### Proving the Lower Bound

The proof is broken up into a number of pieces. First, we describe a non-standard way of writing the Cayley table,  $C_n$ , for the group  $(\mathbb{Z}_2^n, +)$ . Then we present a natural correspondence between entries in  $C_{n-1}$  and  $C_n$ ; and briefly analyze properties of this correspondence. Finally, we show that a transversal in  $C_{n-1}$  corresponds to several



transversals in  $C_n$ . We will use the notation  $\langle k \rangle_n$ , introduced in Chapter 2, to denote the  $n$ -bit representation of the integer  $k$ ; and we will drop the subscript when the length of the representation is obvious given the context.

### The Cayley Table $C_n$

We will write the Cayley table,  $C_n$ , for  $\mathbb{Z}_2^n$  in the following order. The rows of  $C_n$  are indexed by  $\mathbb{Z}_2^n$  in lexicographic order. We index the columns of  $C_n$  two at a time by the pairs  $0\langle k \rangle_{n-1}$  and  $1\langle k \rangle_{n-1}$  where  $k$  starts at 0 and ends at  $2^{n-1} - 1$ . In Figure 5.1, the Cayley table  $C_3$  is given which follows this construction.

$(\mathbb{Z}_2^3, +)$	000	100	001	101	010	110	011	111
000	000	100	001	101	010	110	011	111
001	001	101	000	100	011	111	010	110
010	010	110	011	111	000	100	001	101
011	011	111	010	110	001	101	000	100
100	100	000	101	001	110	010	111	011
101	101	001	100	000	111	011	110	010
110	110	010	111	011	100	000	101	001
111	111	011	110	010	101	001	100	000

Figure 5.1: Cayley table,  $C_3$ , for  $\mathbb{Z}_2^3$ .

### Correspondence between $C_{n-1}$ and $C_n$

The Cayley table  $C_n$  has twice as many columns and rows as  $C_{n-1}$ . We associate column (row)  $i$  of  $C_{n-1}$  with columns (rows)  $2i$  and  $(2i + 1)$  of  $C_n$ . So, the column of  $C_{n-1}$  with index  $0\langle k \rangle_{n-2}$  maps to the pair of columns  $(0\langle 2k \rangle_{n-1}, 1\langle 2k \rangle_{n-1})$  in  $C_n$ , and the column with index  $1\langle k \rangle_{n-2}$  maps to the pair  $(0\langle 2k + 1 \rangle_{n-1}, 1\langle 2k + 1 \rangle_{n-1})$ . Further, the row with index  $\langle k \rangle_{n-1}$  maps to the pair of rows  $(\langle 2k \rangle_n, \langle 2k + 1 \rangle_n)$ .

For the case when  $n = 3$ , the column indices of  $C_{n-1}$  are associated with the column indices of  $C_n$  as shown in Figure 5.2. The association of rows is shown in Figure 5.3.

Column index of $C_2$	00	10	01	11
Column index of $C_3$	000 100	001 101	010 110	011 111

Figure 5.2: Association between column indices of  $C_2$  and  $C_3$

Row index of $C_2$	Row index of $C_3$
00	000 001
01	010 011
10	100 101
11	110 111

Figure 5.3: Association between row indices of  $C_2$  and  $C_3$

This index association between  $C_{n-1}$  and  $C_n$  naturally associates entries of  $C_{n-1}$  with  $2 \times 2$  blocks in  $C_n$ . For example, the association between  $C_2$  and  $C_3$  divides  $C_3$  into 16 blocks as shown in Figure 5.4. Each block corresponds to one entry in the Cayley table  $C_2$ .

In general, we denote the  $2 \times 2$  block in  $C_n$  that corresponds to the entry  $0\langle k \rangle$  ( $1\langle k \rangle$ ) in  $C_{n-1}$  by  $[0\langle k \rangle]_u$  ( $[1\langle k \rangle]_u$ ) for  $k \in \{0, 1, \dots, 2^{n-2} - 1\}$  when the entries are in the upper half of the table; we use the subscript  $l$  on the blocks in the lower half of the table. For instance, if  $0\langle i \rangle$  is a row in  $C_{n-1}$  and  $0\langle j \rangle$  is a column, then the entry of  $C_{n-1}$  in that row and column is  $0\langle k \rangle = 0\langle i \rangle + 0\langle j \rangle$ . The corresponding  $2 \times 2$  block in  $C_n$  is denoted  $[0\langle k \rangle]_u$  has entries  $0\langle 2k \rangle, 1\langle 2k \rangle, 0\langle 2k + 1 \rangle, 1\langle 2k + 1 \rangle$ . In Figure 5.5, the structure of  $[0\langle k \rangle]_u, [0\langle k \rangle]_l, [1\langle k \rangle]_u,$  and  $[1\langle k \rangle]_l$  for  $k \in \{0, 1, \dots, 2^{n-2} - 1\}$  is shown.

		00		10		01		11	
00	000	000	100	001	101	010	110	011	111
	001	001	101	000	100	011	111	010	110
01	010	010	110	011	111	000	100	001	101
	011	011	111	010	110	001	101	000	100
10	100	100	000	101	001	110	010	111	011
	101	101	001	100	000	111	011	110	010
11	110	110	010	111	011	100	000	101	001
	111	111	011	110	010	101	001	100	000

Figure 5.4: Cayley table,  $C_3$ , partitioned into blocks associated with entries in  $C_2$ .

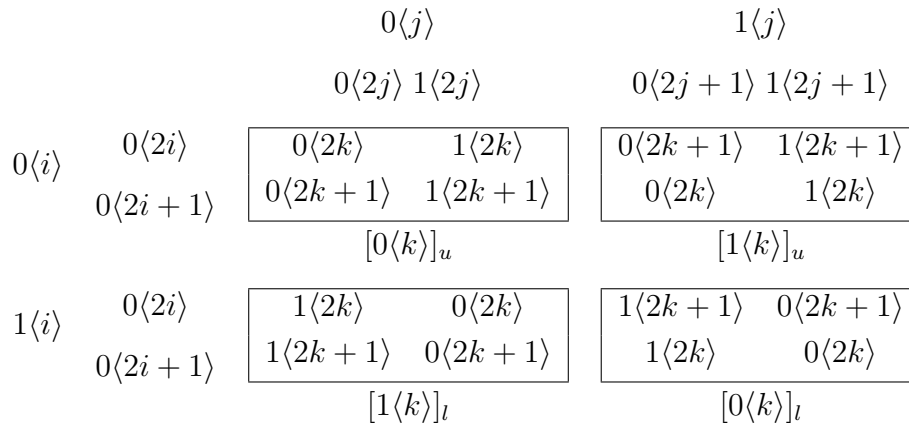


Figure 5.5: Diagram describes the form of every  $2 \times 2$  block in Figure 5.4 blocks  $[0\langle k \rangle]_*$  and  $[1\langle k \rangle]_*$  for  $\langle k \rangle = \langle i \rangle + \langle j \rangle$  in  $C_n$  for  $i, j \in \{0, 1, \dots, 2^{n-2} - 1\}$

**Remark 5.3.** Note that all four blocks  $[0\langle k \rangle]_u$ ,  $[0\langle k \rangle]_l$ ,  $[1\langle k \rangle]_u$ , and  $[1\langle k \rangle]_l$  contain the same elements. Additionally, diagonal elements are shared among all four blocks. The difference between the blocks in the upper half of the table and the lower half is unimportant for the transversal argument used to prove the lower bound, as such we sometimes use  $*$  to denote the value  $u$  or  $l$  in the subscript of the blocks.

Transversals in  $C_{n-1}$  and  $C_n$

Recall that a transversal in a Cayley table (or Latin square) of order  $2^n$  is a set of  $2^n$  distinct entries such that no two entries are in the same row or column.

Each transversal in  $C_{n-1}$  is a set of  $2^{n-1}$  entries with values

$$\{0\langle 0 \rangle, 1\langle 0 \rangle, 0\langle 1 \rangle, 1\langle 1 \rangle, \dots, 0\langle 2^{n-2} - 1 \rangle, 1\langle 2^{n-2} - 1 \rangle\}.$$

Each of these  $2^{n-1}$  entries corresponds to one of  $2^{n-1}$  blocks in  $C_n$  such that no two blocks have a row or column in common. These blocks are

$$\{[0\langle 0 \rangle]_*, [1\langle 0 \rangle]_*, \dots, [0\langle 2^{n-2} - 1 \rangle]_*, [1\langle 2^{n-2} - 1 \rangle]_*\}$$

where  $* \in \{u, l\}$ . Note that exactly half of the blocks are in the upper half of the Cayley table and have subscript  $u$  and the other half have subscript  $l$ ; however, knowledge of the particular subscript for each block is unnecessary for the argument that follows.

We construct a set of transversals in  $C_n$  by choosing diagonal elements from the blocks. For each  $k \in \{0, 1, \dots, 2^{n-2} - 1\}$ , there are two diagonals in  $[0\langle k \rangle]_*$  from which to choose. Note that a choice of diagonals in  $[0\langle k \rangle]_*$  forces our choice in  $[1\langle k \rangle]_*$  by Remark 5.3. Thus, the number of transversals in  $C_n$  is at least  $2^{2^{n-2}}$  times the number of transversals in  $C_{n-1}$ . Equivalently, the number of orthomorphisms of  $\mathbb{Z}_2^n$  is at least  $2^{2^{n-2}}$  times the number of orthomorphisms of  $\mathbb{Z}_2^{n-1}$ .

We can improve this bound by fixing the entry of  $C_{n-1}$  in the first row and first column. Using the notation for sets of orthomorphisms extending partial orthomorphisms

given in Section 3.3, we have  $\mathcal{S}_n(0_0, (2^n - 1)_1) \geq \mathcal{S}_{n-1}(0_0)2^{2^{n-2}-2}$ , but  $\mathcal{S}_n(0_0, (2^n - 1)_1) = \mathcal{S}_n/(2^n(2^n - 2))$  and  $\mathcal{S}_{n-1}(0_0) = \mathcal{S}_{n-1}/2^{n-1}$ . Therefore,

$$\mathcal{S}_n \geq \mathcal{S}_{n-1}2^{2^{n-2}}(2^{n-1} - 1),$$

for all  $n > 2$ .

For a non-recursive lower bound, we have the following corollary.

**Corollary 5.4.** *For  $n > 5$ ,*

$$\mathcal{S}_n \geq 244744192 \prod_{k=4}^{n-1} 2^{2^{k-1}}(2^k - 1).$$

### 5.3 An Orthomorphism Formula

Several formulas for orthomorphisms of  $\mathbb{Z}_2^n$  for arbitrary  $n > 1$  can be derived by analyzing the structure of transversals of the Cayley table  $C_n$ . Using the notation  $(x_1, x_2, \dots, x_n) \in \mathbb{Z}_2^n$ , we provide one such formula.

**Proposition 5.5.** *If  $\pi : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$  such that  $n > 1$  and*

$$\pi(x_1, x_2, \dots, x_n) = (x_1 + x_n, x_1, x_2, \dots, x_{n-1}),$$

*then  $\pi$  is an orthomorphism.*

*Proof.* To prove  $\pi$  is an orthomorphism, we first show  $\pi$  is a permutation of the finite

group  $\mathbb{Z}_2^n$  by showing the function is surjective. Then we show the function

$$\pi + \text{id} : (x_1, x_2, \dots, x_n) \mapsto (x_n, x_1 + x_2, \dots, x_{n-1} + x_n)$$

is a permutation of  $\mathbb{Z}_2^n$  by showing  $\pi + \text{id}$  is surjective.

To begin, let  $(y_1, y_2, \dots, y_n) \in \mathbb{Z}_2^n$  and note that

$$\pi(y_2, y_3, \dots, y_n, y_1 + y_2) = (y_1, y_2, \dots, y_n).$$

Thus,  $\pi$  is surjective. Further, since  $\pi + \text{id}$  maps the element

$$\left( y_1 + \sum_{i=2}^n y_i, y_1 + \sum_{i=3}^n y_i, \dots, y_1 + y_n, y_1 \right) \in \mathbb{Z}_2^n$$

to  $(y_1, y_2, \dots, y_n)$  we may conclude  $\pi + \text{id}$  is surjective. □

#### 5.4 Remarks on Upper Bounds

The only upper bound in the literature for the number of orthomorphisms of  $\mathbb{Z}_2^n$  is the upper bound for the number of transversals in a latin square of order  $N = 2^n$  given in (5.1) above. Another upper bound for the cardinality of the set orthomorphisms of  $\mathbb{Z}_2^n$  is the number of permutations with precisely one fixed point and no transpositions (see [22]). However, this bound is not as tight as the current published bound.

**Theorem 5.6.** For any  $n > 1$ ,

$$\begin{aligned}
 \mathcal{S}_n &\leq 2^n! \sum_{m=1}^{2^n-1} \frac{1}{m!} \sum_{k=0}^m k! (-1)^{m-k} \binom{m}{k} \\
 &\quad \cdot \sum_{i=0}^{2^n-1-m} \frac{2^{-2^n-1+m+i}}{(i+k)!} |s(i+k, k)| \binom{m-k}{2^n-1-m-i} \\
 &\sim 2^n! e^{-3/2}
 \end{aligned} \tag{5.7}$$

*Proof.* Note that  $s(\cdot, \cdot)$  represents the Stirling number of the first kind. Since an orthomorphism of  $\mathbb{Z}_2^n$  has precisely one fixed point and no transpositions, the number of permutations of  $\mathbb{Z}_2^n$  with this property provides an upper bound. The stated result follows from [22].  $\square$

Note that Equation (5.7) is significantly greater than the upper bound given in Equation (5.1), for small  $n$  and in the limit.

### 5.5 A Count for $n = 5$

Determining the number of orthomorphisms of  $\mathbb{Z}_2^5$  computationally is a difficult problem. Implementing a naive breadth-first search of the set of permutations of  $\mathbb{Z}_2^n$  for  $n = 2, 3, 4$  (see Algorithm 1) in the Python programming language, on currently available commodity hardware, yields results in a reasonable amount of time. However, this approach is too computationally difficult to address the  $n = 5$  case. With the help of Bart Massey and David Johnston, a naive depth-first search algorithm was implemented in the C programming language which takes partial orthomorphisms as parameters, and optionally returns orthomorphisms or a count, was developed [31]. At the date of this

writing, a process using this implementation is running on the Portland State University research computers, and is currently at a count of 76,596,911,431,680 orthomorphisms of  $\mathbb{Z}_2^5$ .

For all computer implementations we have described, we use integers to represent elements in  $\mathbb{Z}_2^n$  in the natural way, and use the ordering inherent to integers. Further, in the implementations we have described, an injective function  $\pi : \{1, 2, \dots, m\} \rightarrow \mathbb{Z}_2^n$ , where  $m < 2^n$ , is represented as a tuple. That is, we represent  $\pi$  as  $(\pi(0), \pi(1), \dots, \pi(m))$  so that element  $i$  of the tuple is the image of  $i$  under  $\pi$ . A presentation of the pseudocode of the algorithm used in the Python implementation is given below.

---

**Algorithm 1** Naive breadth-first search algorithm generates orthomorphisms of  $\mathbb{Z}_2^n$

---

```
function ORTHOMORPHISMS(partials,n)
  while the length of the elements of partials are not equal to  $2^n$  do
    Let newpartials be an empty list
    for  $\pi$  in partials do
       $\tau = \pi \oplus [0, 1, \dots, |\pi| - 1]$ 
      Let valid be an empty list
      for  $i = 0..(2^n - 1)$  do
        if  $i$  not in  $\pi$  and  $i \oplus |\pi|$  not in  $\tau$  then
          append  $i$  to valid
      for  $i$  in valid do
        extend  $\pi$  so that  $\pi(|\pi|) = i$  and add to newpartials
    partials = newpartials
  return partials
```

---



## Chapter 6

### GENERATING ORTHOMORPHISMS

Applications of orthomorphisms to cryptography require an efficient way to sample from the set of orthomorphisms of  $\mathbb{Z}_2^n$ , and knowledge of the cardinality of the set of orthomorphisms for any given  $n$ . We use a Metropolis-Hastings Markov Chain Monte Carlo algorithm to sample from a particular distribution on the set of permutations that weighs orthomorphisms highest. Additionally, we present an algorithm for sampling orthomorphisms uniformly using the algebraic objects introduced in Chapter 4. Lastly, we discuss applications of importance sampling to getting a count of the number of orthomorphisms of  $\mathbb{Z}_2^n$ .

#### 6.1 Introduction

In order to use orthomorphisms in any cryptographic primitive, we need a way to generate them. Failing that, we would at least like a way to generate a large subset of them. Randomly generating orthomorphisms is not only valuable for cryptographic applications but is valuable to the field of mathematics itself [1].

For the group  $\mathbb{Z}_2^n$ , some work in this direction has been done (see [4], [17], and [34]).

In [34], the authors develop an evolutionary algorithm that generates orthomorphisms of  $\mathbb{Z}_2^8$  based on an initial population of orthomorphisms of  $\mathbb{Z}_2^2$ ,  $\mathbb{Z}_2^3$  and  $\mathbb{Z}_2^4$ . An algorithm that generates all *linear* orthomorphisms is given in [4]. In this paper they find the number of linear orthomorphisms for  $n \in \{1, \dots, 10\}$ . Based on this data, we can see the proportion of automorphisms that are linear orthomorphisms approaches 0.288 quickly. The proportion of orthomorphisms that are linear is 1, 1, and  $\approx 0.0003$  for  $n = 2, 3$ , and 4, respectively. In [17], the authors develop a method of generating non-linear orthomorphisms based on linear ones via a *bar-sinister* latin square. The non-linear orthomorphisms are especially useful in the construction of block substitutions [20, 34].

It is already known that orthomorphisms are precisely those permutations that have the so-called “balanced-map property” [25]. That is, a permutation is an orthomorphism if and only if it maps all maximal subgroups of the group half-in and half-out of themselves. We use the balanced-map property to improve the results of our implementation of the Metropolis-Hastings algorithm.

In this chapter, we describe implementations of the Metropolis-Hastings algorithm that generate sets of orthomorphisms. Ideally, we would be able to develop a method to sample from the set of orthomorphisms of  $\mathbb{Z}_2^n$  for a given  $n$  uniformly. In the context of the Metropolis Hastings algorithm, that would require a set of functions that act transitively on the set of orthomorphisms. Candidates for this set include the known functions described in previous chapters that preserve the orthomorphism property of a permutation. However, these functions, in their action on the set of orthomorphisms, do not generate a single orbit. We are left to work in a set of permutations that contains the orthomorphisms and use functions that prioritize the orthomorphism property of a

permutation.

## 6.2 Metropolis-Hastings Algorithm

A Markov Chain Monte Carlo (MCMC) method for the simulation of a distribution  $f$  is any method producing an ergodic Markov chain  $(X^{(t)})$  whose stationary distribution is  $f$  [3]. The Metropolis-Hastings algorithm is an algorithm that produces such a Markov chain. In essence, the Metropolis-Hastings algorithm provides a way to generate a sequence of samples that approximates a target distribution,  $f$ , even if the distribution's normalizing factor is unknown. The samples returned by the algorithm have the property that a given sample is only dependent on the previous sample, thus making it a Markov chain. In particular, for any given step, a candidate sample is drawn from a proposal distribution,  $q$ , and is accepted as the next sample (or rejected) with some probability dependent on the target and proposal distributions. Further, as the number of iterations increases, the distribution of the samples more closely approximates the target distribution.

**Remark.** *Note that the ratio in the definition of  $\alpha$  eliminates the necessity of knowing the normalizing constant associated with  $f$ . This is of particular interest in the application of this algorithm to generating samples from the set of orthomorphisms of  $\mathbb{Z}_2^n$  since so little is known about the cardinality of the set.*

The parameters of the Metropolis-Hastings algorithm over which we have control are the sample (state) space  $S$  which contains  $(X^{(t)})_t$ , the target distribution  $f$ , and the proposal distribution  $q$ .

---

**Algorithm 2** Metropolis-Hastings Algorithm

---

Given  $x^{(t)}$   
 Sample  $y_t$  from  $Y_t \sim q(y|x^{(t)})$   
 Take  $x^{(t+1)}$  from

$$X^{(t+1)} = \begin{cases} y_t & \text{with probability } \alpha(x^{(t)}, y_t), \\ x^{(t)} & \text{with probability } 1 - \alpha(x^{(t)}, y_t), \end{cases}$$

where

$$\alpha(x, y) = \begin{cases} \min \left\{ \frac{f(y)q(x|y)}{f(x)q(y|x)}, 1 \right\} & \text{if } f(x)q(y|x) > 0 \\ 1 & \text{otherwise.} \end{cases}$$


---

In order for the algorithm to produce samples from a target distribution, several conditions related to the proposal distribution  $q(y|x)$  must be satisfied.

**Theorem 6.1.** [3] *Let  $(X^{(t)})$  be the Markov chain produced by Algorithm 2. For every proposal distribution  $q$ , if the support of  $q$  includes that of the target distribution  $f$ , then  $f$  is a stationary distribution of  $(X^{(t)})$ .*

As stated previously, in order for the Metropolis-Hasting algorithm to be an MCMC method, the resulting Markov chain must be ergodic. A Markov chain,  $(X^{(t)})$ , with a finite state space is *ergodic* if it is irreducible (it is possible to get to any state from any state) and at least one state,  $i$ , is *aperiodic* (there exists  $n$  such that for all  $n' > n$ ,  $P(X^{(n')} = i | X^{(0)} = i) > 0$ ) [32]. The ergodicity of the Markov chain is necessary to consider when choosing parameters of the Metropolis-Hastings algorithm. Further, it ensures that the Markov chain converges uniquely to the target distribution, as the following theorem shows.

**Theorem 6.2.** [30] *If the Markov chain,  $(X^{(t)})$ , drawn from a finite state space is ergodic (aperiodic and irreducible) then the Markov chain converges to its stationary distribution  $f$ .*

**Remark.** *A common practice among users of MCMC methods is to disregard several initial samples from a single run; disregarding these initial samples is referred to as a “burn-in” period. Though there is little mathematical basis for the practice, it can address the problem of starting in a part of the state space that is unrepresentative of the stationary distribution. To address this problem, in each of our trials and in the first iteration of the algorithm, a permutation is continually sampled until it maps the subgroup  $\{0, 1, \dots, 2^{n-1} - 1\}$  exactly half in to itself, thus making use of the balanced-map property of orthomorphisms.*

**Remark.** *Note that the set of samples produced by the Metropolis-Hastings algorithm are not independent samples, as  $x^{(t+1)}$  is dependent on  $x^{(t)}$ . Theoretically, to obtain i.i.d. samples from the distribution  $f$ , one can take the terminus of several runs of the Metropolis-Hastings algorithm. Some researchers approximate i.i.d. samples by taking every  $N$ th sample from a single run of the algorithm [21]. Note that, in practice, one cannot obtain i.i.d. samples if the random inputs to the algorithm are not i.i.d. as well [23].*

### 6.2.1 Implementation

For the implementations of the Metropolis-Hastings algorithm we present in this chapter, we consider sample spaces  $S$  that are contained in the set of permutations of  $\mathbb{Z}_2^n$ ;

and a target distribution,  $f$ , defined on those spaces that weigh orthomorphisms highest. Further, we consider several proposal distributions,  $q$ , one of which is symmetric (i.e.,  $q(x|y) = q(y|x)$ ) and one that is more likely to return permutations that are “closer”, in some sense, to orthomorphisms.

Since it is currently infeasible to use the uniform distribution on the set of orthomorphisms as the target distribution, we use a target distribution that weighs orthomorphisms higher than other permutations:

$$f(\pi) = \frac{10^{|\text{im}(\pi+\text{id})|}}{Z}, \quad Z = \sum_{\pi} 10^{|\text{im}(\pi+\text{id})|}.$$

Note that, if  $\pi$  is an orthomorphism of  $\mathbb{Z}_2^n$ , then  $|\text{im}(\pi + \text{id})| = 2^n$ .

### **Trial 1**

For our initial implementation of the Metropolis-Hastings algorithm, we use the entire set of permutations on  $\mathbb{Z}_2^n$  for  $n = 4$  and  $n = 5$ . For the proposal distribution we use

$$q(x|y) = q(x) = \frac{1}{(2^n)!},$$

i.e., our candidate samples are drawn from the set of permutations on  $\mathbb{Z}_2^n$ , all with equal probability.

In Figure 6.1 we see results of this implementation for  $n = 4$  with  $2^{22}$  iterations. To get a sample that is closer to independent, we follow a heuristic often used with these methods by taking every  $2^{10}$  samples. Further, we use a burn-in method that relies on the balanced map property of orthomorphisms; that is, we start collecting samples after

we find the first permutation that maps the maximal subgroup  $\{0, 1, 2, \dots, 2^{n-1} - 1\}$  half into itself and half outside of itself.

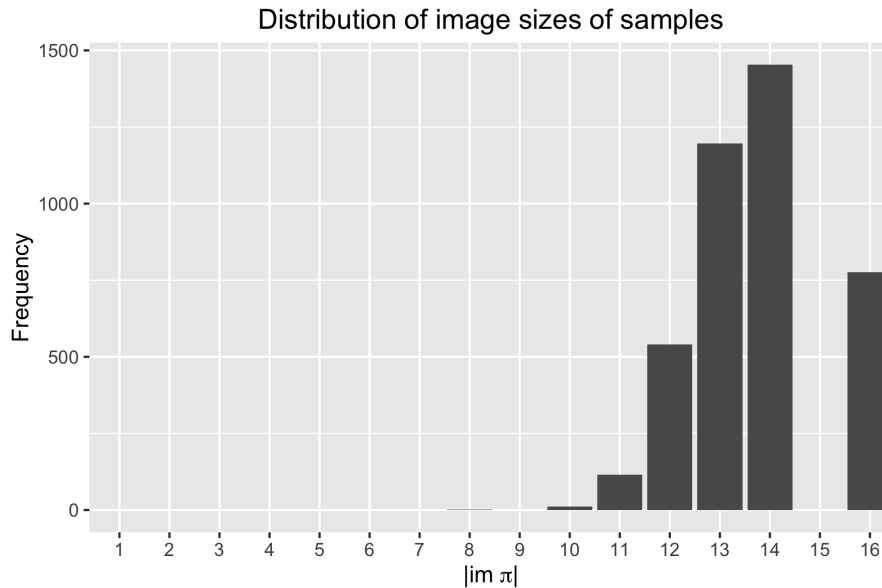


Figure 6.1: Distribution for Trial 1,  $n = 4$ ,  $2^{22}$  iterations, acceptance rate 5.12%

The rate of convergence of the algorithm to the desired target distribution can be affected by the proposal distribution. Determining the rate of convergence of the Metropolis Hastings algorithm is an active area of research, and in many cases the acceptance rate of a run is used as an indicator of convergence. The acceptance rate is the proportion of times the proposed sample is accepted. Work has yet to be done in studying convergence rates of the Metropolis-Hastings algorithm in the context we are concerned with, so we have inadequate information to determine if our chain has converged.

Executing this algorithm for  $n = 5$  results in a sample with no orthomorphisms, as shown in Figure 6.2. Assuming this indicates our chain is not quickly converging, we consider reducing the size of our state space and changing the proposal distribution used

in the algorithm. We describe these changes in detail in the next section.

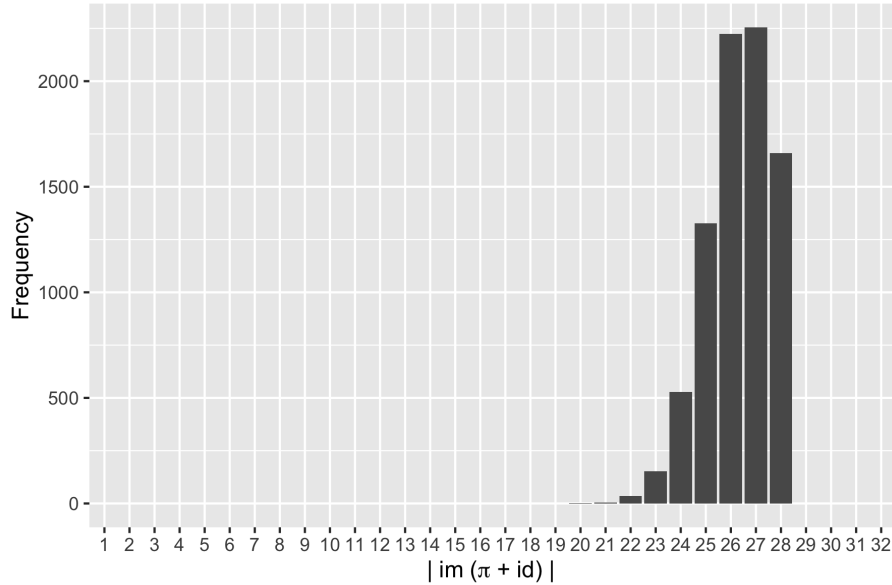


Figure 6.2: Distribution for Trial 1,  $n = 5$ ,  $2^{22}$  iterations, acceptance rate 0.17%

### Trial 2

The implementation of the Metropolis-Hastings algorithm that generates the most orthomorphisms has as its sample space a subset of permutations of  $\mathbb{Z}_2^n$ . Specifically, for a given tuple  $p = (p_1, p_2, \dots, p_m)$ ,  $m < 2^n$ , we define our sample space  $S_p = \{\pi : \pi(i) = p_i \text{ for } 1 \leq i \leq m\}$ . Essentially, our sample space is the set of permutations whose first  $m$  elements all share the same image.

For this implementation, we use a more complex proposal distribution which we describe here. Given a permutation  $x$  and some number  $\beta \in [0, 1]$ , we permute 4 randomly selected elements of  $(x(m + 1), \dots, x(2^n - 1))$  with probability  $\beta$ , and with probability  $1 - \beta$  we transpose the image of the element  $k = \min\{i \in \mathbb{Z}_2^n : x(i) + i =$



$x(j) + j, j \in \mathbb{Z}_2^n$  with the image of a randomly selected element  $l > k$ , unless  $x$  is an orthomorphism. If  $x$  is an orthomorphism, we permute 4 randomly selected elements of  $(x(m+1), \dots, x(2^n - 1))$ .

So, if  $x$  is a permutation of  $\mathbb{Z}_2^n$  and we sample  $y$  by the method previously described, then the proposal density can be written as

$$q(y|x) = \begin{cases} \beta \left( \frac{(2^n - m - 4)!}{(2^n - m)!} \right) + (1 - \beta) \left( \frac{1}{2^n - m - k + 1} \right) & \text{if } x \text{ is not an orthomorphism} \\ \frac{(2^n - m - 4)!}{(2^n - m)!} & \text{if } x \text{ is an orthomorphism.} \end{cases}$$

Implementing these changes to the proposal distribution and sample space produces a significantly larger number of orthomorphisms for both the  $n = 4$  case, as can be seen in Figure 6.3, and the  $n = 5$  case, as seen in Figure 6.4. However, the run time of the algorithm increases by a factor of five. For this implementation, we use a sample space  $S_p$  where  $p = (0, 2)$ .

### 6.3 Conclusions

The change in proposal distribution led to a significant increase in orthomorphisms sampled. For the  $n = 5$  case, we are able to use the resulting sample of orthomorphisms to add to the list of cycle types realized, which is displayed in Appendix 7. However, the sampling is not uniform across the set of orthomorphisms and our choice of target distribution limits our ability to determine the size of the set of orthomorphisms. The approach of using the Metropolis-Hastings algorithm could, in principle, be improved by finding a set of functions that act transitively on the set of all orthomorphisms for a given

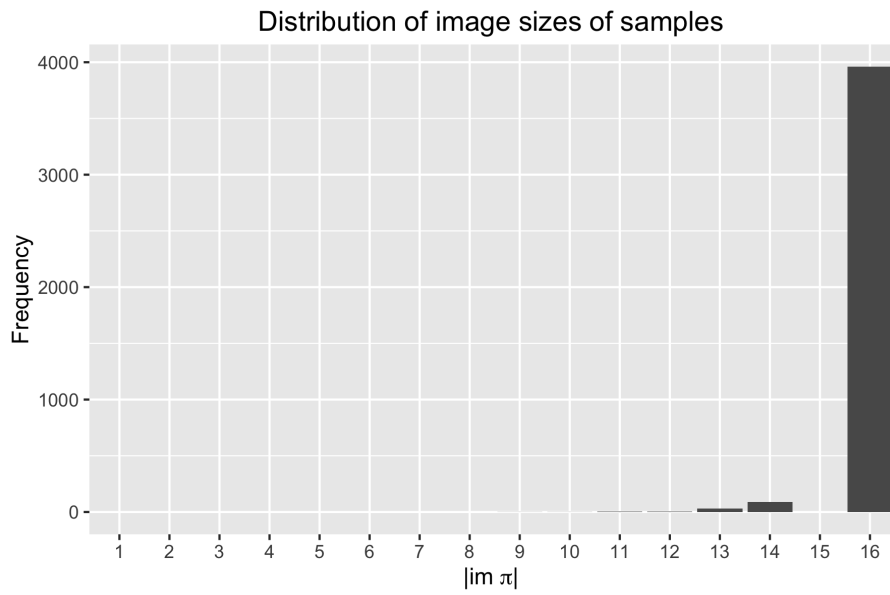


Figure 6.3: Distribution for Trial 2,  $n = 4$ ,  $2^{20}$  iterations, acceptance rate 5.00%

$n$ . With such a set of functions, the algorithm could then be used to sample from the set of orthomorphisms uniformly and estimate the cardinality of the set of orthomorphisms.

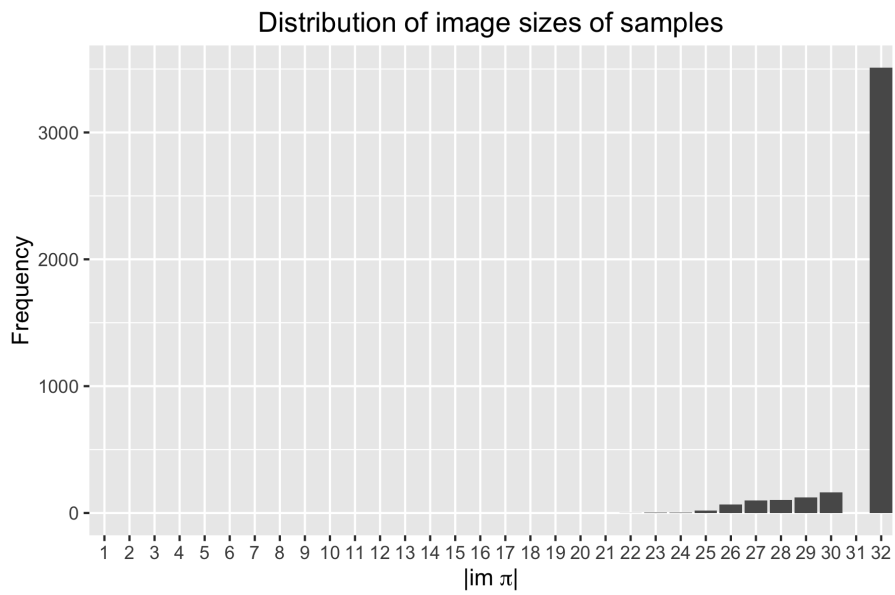


Figure 6.4: Distribution for Trial 2,  $n = 5$ ,  $2^{20}$  iterations, acceptance rate 6.22%

## Chapter 7

### CONCLUSIONS AND FUTURE DIRECTIONS

The research contained in this document extends human knowledge of orthomorphisms of the group  $\mathbb{Z}_2^n$  in terms of both theoretical understanding and applications to cryptography. There are many further avenues of research concerning orthomorphisms of  $\mathbb{Z}_2^n$ . We outline some specific directions based on each chapter's content.

The work on the cycle-type distribution of partial orthomorphisms can be extended to consider partial orthomorphisms of larger sizes and assist in determining valid cycle types of orthomorphisms of  $\mathbb{Z}_2^n$ . Additionally, these methods can be pursued to determine conditions in which extensions of partial orthomorphisms of  $\mathbb{Z}_2^n$ , with size greater than 2, exist. Beyond extensions and cycle type distributions, the techniques described in Chapter 3 can be used to determine statements about the divisibility of the cardinality of the set of orthomorphisms of  $\mathbb{Z}_2^n$ .

The theory developed in Chapter 4 concerning the group of automorphisms of  $\mathbb{Z}_2^n$  acting on the set of orthomorphisms can be extended in many ways. Extending the theory concerning orbits of the group action can be generalized to statements about the cycle types of orthomorphisms of  $\mathbb{Z}_2^n$ . Further, such theoretical extensions can be used

in conjunction with Burnside's lemma to determine, or bound, the number of orthomorphisms that exist.

The new lower bound and upper bound on the cardinality of orthomorphisms, specific to the group  $\mathbb{Z}_2^n$ , described in Chapter 5 have potential for improvement. Experimenting with varying the column structure of the Cayley table for  $\mathbb{Z}_2^n$  and applying the same block argument could lead to a tighter lower bound; and, investigating and applying new theory concerning the valid cycle types of orthomorphisms of  $\mathbb{Z}_2^n$  can be used to tighten the upper bound.

Another direction for further research, as it pertains to generating orthomorphisms, concerns uniform and importance sampling. The Metropolis-Hastings algorithm can be used to generate a uniform sampling of orthomorphisms of  $\mathbb{Z}_2^n$  if we can get a set of representatives from each orbit under any known group action on the set of orthomorphisms. For example, given the action of conjugation by automorphisms and a set  $\{\pi_i\}$  of orbit representatives, we can define a proposal distribution

$$q(x, y) = \frac{1}{|\{\pi_i\}|} \frac{\text{stab}_G(\pi_j)}{|\text{Aut}(\mathbb{Z}_2^n)|}, x \in \text{orb}(\pi_j)$$

from which we sample by uniformly selecting an orbit representative and automorphism independent of the orthomorphism  $y$ . Implementing and executing a Metropolis-Hastings algorithm with this proposal distribution and a uniform target distribution will result in set of uniformly sampled orthomorphisms. Ideally, we could avoid all this if we could discover a set of orthomorphism-preserving transformations that, collectively, act transitively on the set of orthomorphisms.

Alternative Monte Carlo methods can be used to generate an independent sample of permutations of  $\mathbb{Z}_2^n$  that over-weight orthomorphisms, and the theory surrounding importance sampling can be used to estimate the number of orthomorphisms of  $\mathbb{Z}_2^n$ . An excellent presentation of this approach can be found in [26].

In conclusion, the study of orthomorphisms of  $\mathbb{Z}_2^n$  is relatively new in both the mathematics community as well as with cryptography researchers. Our work extending this theory has led to many new problems and areas of potential research.

## REFERENCES

- [1] Masood Aryapoor and ES Mahmoodian. On uniformly generating Latin squares. *arXiv preprint arXiv:1005.0121*, 2010. [65](#)
- [2] 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](#), [10](#)
- [3] George Casella Christian Robert. *Monte Carlo Statistical Methods*. Springer Texts in Statistics. Springer, 2nd edition, 2004. [67](#), [68](#)
- [4] Zong Duo Dai, Solomon W. Golomb, and Guang Gong. Generating all linear orthomorphisms without repetition. *Discrete Mathematics*, 205(1):47–55, 1999. [3](#), [65](#), [66](#)
- [5] David Steven Dummit and Richard M. Foote. *Abstract algebra*. Prentice Hall Englewood Cliffs, 3rd edition, 2004. [12](#), [13](#), [15](#), [39](#)
- [6] Paul Erdős and Anthony B. Evans. Representations of graphs and orthogonal Latin square graphs. *Journal of Graph Theory*, 13(5):593–595, November 1989. [10](#)
- [7] Leonhard Euler. *Recherches sur une nouvelle espece de quarrés magiques*. Zeeuwsch Genootschao, 1782. [2](#)
- [8] Anthony B. Evans. Generating Orthomorphisms of  $GF(q)^+$ . *Discrete Mathematics*, 63(1):21–26, January 1987. [10](#)
- [9] Anthony B Evans. Orthomorphisms of  $Z_p$ . *Discrete Mathematics*, 64:147–156, 1987. [10](#)
- [10] Anthony B. Evans. Orthomorphism graphs of groups. *Journal of Geometry*, 35(1-2):66–74, July 1989. [7](#), [10](#)
- [11] Anthony B. Evans. Orthomorphisms of groups. *Annals of the New York Academy of Sciences*, 555(1 Combinatorial):187–191, May 1989. [10](#)

## References

---

- [12] Anthony B. Evans. Maximal sets of mutually orthogonal Latin squares. *European Journal of Combinatorics*, 13(5):345–350, September 1992. [10](#)
- [13] Anthony B. Evans. On orthogonal orthomorphisms of cyclic and non-abelian groups. *Journal of Combinatorial Designs*, 15(3):195–209, May 2007. [10](#)
- [14] Anthony B. Evans. The existence of strong complete mappings. *The Electronic Journal of Combinatorics*, 19(1):P34, 2012. [5](#), [10](#), [38](#)
- [15] Sir Ronald Aylmer Fisher. *The Design of Experiments*. Macmillan, 9th edition, 1935/1971. [2](#)
- [16] Shoni Gilboa and Shay Gueron. Balanced permutations Even-Mansour ciphers. Cryptology ePrint Archive, Report 2014/642, 2014. [1](#), [2](#)
- [17] Solomon W Golomb, Guang Gong, and Lothrop Mittenthal. Constructions of orthomorphisms of. In *Finite Fields and Applications: Proceedings of The Fifth International Conference on Finite Fields and Applications*, page 178. Springer Science & Business Media, 2001. [3](#), [65](#), [66](#)
- [18] Martin Grüttmüller. Completing partial Latin squares with two cyclically generated prescribed diagonals. *Journal of Combinatorial Theory, Series A*, 103(2):349–362, 2003. [2](#), [10](#)
- [19] Diane M. Johnson, A.L. Dulmage, and N.S. Mendelsohn. Orthomorphisms of groups and orthogonal Latin squares. *Canad. J. Math*, 13:356–372, 1961. [2](#), [12](#), [36](#)
- [20] Pascal Junod and Serge Vaudenay. Fox: a new family of block ciphers. In *The 11th International Workshop on Selected Areas in Cryptography, SAC 2004*, volume 3357, pages 114–129, 2004. [2](#), [66](#)
- [21] Tjonnie GF Li. *Extracting Physics from Gravitational Waves: Testing the Strong-field Dynamics of General Relativity and Inferring the Large-scale Structure of the Universe*. Springer, 2015. [69](#)
- [22] James Mahoney. Sequence A221145 in The Online Encyclopedia of Integer Sequences, 2012. [62](#), [63](#)
- [23] James L McInnes and Benny Pinkas. On the impossibility of private key cryptography with weakly random keys. In *Advances in Cryptology-CRYPT090*, pages 421–435. Springer, 1990. [69](#)



- [24] Brendan D McKay, Jeanette C McLeod, and Ian M Wanless. The number of transversals in a Latin square. *Designs, Codes and Cryptography*, 40(3):269–284, 2006. 55
- [25] Lothrop Mittenthal. Block substitutions using orthomorphic mappings. *Advances in Applied Mathematics*, 16(1):59–71, 1995. 3, 66
- [26] Art B. Owen. Monte Carlo theory, methods and examples. See <http://statweb.stanford.edu/owen/mc/> for current draft., 2013. 78
- [27] L.J. Paige. A note on finite abelian groups. *Bulletin of the American Mathematical Society*, 53(6):590–593, 1947. 25
- [28] David Poole. *Linear Algebra: A Modern Introduction*. Cengage Learning, 3rd edition, 2014. 15
- [29] Liu Qi, Zhang Yin, Chen Cheng, and Lv Shuwang. Construction and Counting Orthomorphism Based on Transversal. *2008 International Conference on Computational Intelligence and Security*, 2:369–373, December 2008. 55
- [30] Gareth O Roberts, Jeffrey S Rosenthal, et al. General state space markov chains and MCMC algorithms. *Probability Surveys*, 1:20–71, 2004. 69
- [31] Nichole L Schimanski. Orthomorphism counter. <https://github.com/nlschimanski/orthomorphism-counter>, 2016. 63
- [32] Daniel Sorensen and Daniel Gianola. *Likelihood, Bayesian, and MCMC methods in quantitative genetics*. Springer Science & Business Media, 2007. 68
- [33] Douglas S. Stones and Ian M. Wanless. Compound orthomorphisms of the cyclic group. *Finite Fields and Their Applications*, 16(4):277–289, 2010. 2, 10
- [34] Yan Tong, Huanguo Zhang, and Haiqing Han. Using Evolutionary Computation in Construction of Orthomorphism. *2009 International Conference on Multimedia Information Networking and Security*, pages 478–481, 2009. 65, 66
- [35] Ian Wanless. Transversals in latin squares. *Quasigroups and Related Systems*, 15(1):169–190, 2007. 2, 6, 10, 55
- [36] Aaram Yun, Je Hong Park, and Jooyoung Lee. Lai-Massey scheme and quasi-Feistel networks. Cryptology ePrint Archive, Report 2007/347, 2007. 2

## APPENDIX CYCLE TYPES FOR $\mathbb{Z}_2^5$

The number of valid cycle types of orthomorphisms of  $\mathbb{Z}_2^n$  is known for  $n < 5$ . For the  $n = 5$  case, we have found examples of orthomorphisms with 347 different cycle-types out of the 391 possible cycle types of permutations that have no transpositions and precisely one fixed point.

Cycle Types	Orthomorphism
(1, 3, 5, 5, 7, 11)	(1, 2, 3)(4, 8, 16, 23, 30)(5, 10, 22, 28, 26, 17, 21)(6, 11, 20, 7, 9, 18, 15, 29, 24, 14, 31)(12, 25, 13, 19, 27)
(1, 3, 6, 10, 12)	(0, 9, 28, 31, 15, 21, 4, 10, 12, 23)(1, 11, 24, 7, 25, 5)(2, 13, 20)(3, 8, 26, 29, 17, 16, 18, 6, 14, 22, 19, 30)
(1, 3, 6, 9, 13)	(0, 19, 30, 9, 6, 20, 24, 7, 3, 18, 4, 16, 8)(1, 17, 11, 2, 23, 10, 22, 29, 26)(5, 27, 21, 31, 25, 28)(12, 13, 14)
(1, 4, 6, 8, 13)	(1, 2, 4, 3)(5, 8, 19, 6, 7, 16, 13, 20, 28, 24, 9, 21, 10)(11, 17, 31, 22, 26, 12, 18, 25)(14, 29, 23, 15, 27, 30)
(1, 6, 6, 8, 11)	(1, 2, 15, 3, 21, 19, 18, 9, 29, 8, 24)(4, 23, 25, 30, 6, 26, 5, 13)(7, 12, 14, 28, 11, 22)(10, 16, 31, 27, 17, 20)
(1, 7, 8, 8, 8)	unknown
(1, 3, 7, 10, 11)	(0, 1, 3)(2, 5, 9, 20, 27, 15, 29, 24, 21, 10, 4)(7, 17, 25, 12, 31, 8, 18, 22, 14, 30)(11, 16, 26, 19, 13, 28, 23)
(1, 3, 3, 4, 7, 14)	(1, 2, 4, 3)(5, 8, 19, 25, 12, 18, 10)(6, 7, 16, 13, 20, 11, 17, 31, 15, 27, 9, 21, 28, 23)(14, 29, 24)(22, 30, 26)
(1, 3, 6, 6, 7, 9)	(0, 10, 5, 7, 29, 14, 27, 31, 30)(1, 9, 22, 6, 11, 16)(2, 12, 24, 4, 13, 26)(3, 8, 17)(15, 25, 21, 19, 20, 23, 18)
(1, 3, 13, 15)	(0, 21, 30, 1, 23, 27, 7, 5, 29, 28, 31, 15, 9)(2, 17, 12, 11, 4, 22, 13, 8, 6, 18, 26, 3, 20, 25, 19)(10, 16, 14)
(1, 4, 6, 9, 12)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16, 13, 20, 24, 28, 25, 23)(9, 21, 31, 22, 30, 14, 29, 11, 17, 26, 15, 27)
(1, 3, 4, 6, 7, 11)	(1, 2, 4, 3)(5, 8, 19, 23, 28, 12, 18, 26, 15, 27, 10)(6, 7, 16, 13, 20, 30)(9, 21, 25, 11, 17, 31, 22)(14, 29, 24)
(1, 3, 3, 3, 3, 3, 6, 10)	(1, 2, 3)(4, 8, 16)(5, 10, 22, 28, 18, 27)(6, 11, 25)(7, 12, 23, 13, 20, 19, 14, 29, 21, 17)(9, 24, 30)(15, 31, 26)
(1, 4, 8, 19)	(1, 2, 4, 3)(5, 8, 19, 25, 15, 27, 9, 21, 30, 23, 6, 7, 16, 13, 20, 11, 17, 31, 10)(12, 18, 26, 22, 14, 29, 24, 28)
(1, 3, 3, 3, 7, 15)	(0, 27, 9, 14, 4, 24, 29, 3, 26, 15, 7, 11, 10, 30, 16)(1, 25, 22)(2, 31, 18, 20, 23, 21, 17)(5, 19, 12)(6, 28, 13)
(1, 4, 6, 7, 14)	(1, 2, 4, 3)(5, 8, 19, 23, 15, 27, 14, 29, 11, 17, 31, 22, 26, 10)(6, 7, 16, 13, 20, 28, 25)(9, 21, 30, 12, 18, 24)
(1, 3, 4, 4, 4, 4, 6, 6)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16, 24, 28, 23)(9, 21, 25)(11, 17, 31, 22)(13, 20, 30, 27)(14, 29, 15, 26)
(1, 3, 3, 5, 5, 6, 9)	(1, 2, 3)(4, 8, 16, 23, 28, 26, 7, 9, 18)(5, 10, 22)(6, 11, 20, 30, 14, 31)(12, 25, 13, 19, 27)(15, 29, 24, 17, 21)
(1, 3, 3, 4, 8, 13)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 25, 11, 17, 31, 23, 15, 27, 10)(6, 7, 16, 13, 20, 30, 26, 22)(9, 21, 28)(14, 29, 24)
(1, 3, 3, 3, 4, 4, 4, 10)	(1, 2, 4, 3)(5, 8, 19, 14, 29, 23, 30, 22, 24, 10)(6, 7, 16)(9, 21, 25, 28)(11, 17, 26)(12, 18, 13, 20)(15, 27, 31)
(1, 8, 23)	(0, 8, 19, 12, 26, 6, 9, 20, 23, 22, 4, 15, 27, 1, 11, 18, 21, 16, 3, 10, 7, 31, 17)(2, 14, 25, 29, 13, 24, 30, 28)
(1, 3, 3, 5, 9, 11)	(0, 30, 10, 17, 23)(1, 29, 26, 18, 27, 11, 4, 25, 8, 5, 19)(2, 24, 20, 16, 21, 6, 31, 7, 9)(3, 28, 22)(13, 14, 15)
(1, 6, 6, 6, 6, 7)	unknown
(1, 4, 5, 5, 6, 11)	(1, 2, 4, 3)(5, 8, 19, 26, 10)(6, 7, 16, 15, 27)(9, 21, 25, 28, 23, 31, 13, 20, 30, 11, 17)(12, 18, 22, 24, 14, 29)
(1, 3, 3, 3, 11, 11)	(1, 2, 3)(4, 8, 16, 23, 17, 12, 25, 28, 6, 11, 20)(5, 10, 22)(7, 9, 18, 24, 14, 31, 27, 15, 29, 21, 30)(13, 19, 26)

Continued on next page

Cycle Types	Orthomorphism
(1, 5, 5, 5, 6, 10)	unknown
(1, 5, 9, 17)	(0, 15, 28, 7, 24, 5, 2, 9, 19, 17, 6, 14, 30, 23, 22, 18, 10)(1, 12, 29, 11, 21, 16, 4, 8, 20)(3, 13, 31, 25, 26)
(1, 10, 21)	(0, 14, 31, 23, 16, 5, 3, 12, 28, 4, 9, 18, 19, 10, 1, 13, 30, 27, 7, 25, 26)(2, 8, 21, 17, 6, 15, 29, 11, 20, 22)
(1, 3, 3, 3, 3, 4, 15)	(1, 2, 4, 3)(5, 8, 19, 14, 29, 22, 9, 21, 31, 26, 30, 23, 15, 27, 10)(6, 7, 16)(11, 17, 25)(12, 18, 28)(13, 20, 24)
(1, 3, 5, 11, 12)	(0, 5, 13, 24, 23, 11, 20, 31, 12, 27, 10)(1, 7, 21, 15, 25, 9, 16, 30, 3, 4, 6, 2)(8, 22, 14, 26, 19)(17, 29, 28)
(1, 4, 5, 7, 7, 8)	(1, 2, 4, 3)(5, 8, 19, 24, 9, 21, 10)(6, 7, 16, 13, 20)(11, 17, 25, 23, 15, 27, 14, 29)(12, 18, 30, 26, 31, 22, 28)
(1, 5, 7, 7, 12)	unknown
(1, 3, 3, 3, 4, 18)	(1, 2, 4, 3)(5, 8, 19, 6, 7, 16, 13, 20, 11, 17, 31, 22, 14, 29, 23, 28, 24, 10)(9, 21, 25)(12, 18, 26)(15, 27, 30)
(1, 6, 6, 7, 12)	unknown
(1, 3, 3, 3, 3, 19)	(0, 27, 9, 14, 4, 24, 21, 17, 2, 31, 29, 3, 26, 15, 7, 11, 10, 30, 16)(1, 25, 22)(5, 19, 12)(6, 28, 13)(18, 20, 23)
(1, 4, 4, 10, 13)	(1, 2, 4, 3)(5, 8, 19, 25, 12, 18, 30, 23, 15, 27, 9, 21, 10)(6, 7, 16, 13, 20, 28, 24, 14, 29, 22)(11, 17, 31, 26)
(1, 4, 4, 4, 6, 13)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16, 13, 20, 28, 14, 29, 24, 9, 21, 31, 22)(11, 17, 26, 30)(15, 27, 23, 25)
(1, 3, 3, 4, 6, 6, 9)	(1, 2, 4, 3)(5, 8, 19, 24, 13, 20, 9, 21, 10)(6, 7, 16)(11, 17, 31, 22, 28, 25)(12, 18, 26, 30, 14, 29)(15, 27, 23)
(1, 6, 9, 16)	(0, 24, 30, 19, 15, 4, 27, 10, 29)(1, 26, 12, 6, 31, 17)(2, 28, 14, 7, 8, 11, 9, 13, 5, 16, 3, 25, 21, 18, 23, 22)
(1, 3, 3, 3, 4, 5, 13)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 28, 22, 30, 23, 15, 27, 31, 10)(6, 7, 16, 13, 20)(9, 21, 25)(11, 17, 26)(14, 29, 24)
(1, 3, 3, 3, 3, 3, 3, 10)	unknown
(1, 13, 18)	(0, 13, 29, 8, 22, 1, 14, 28, 7, 26, 3, 15, 30, 24, 19, 9, 17, 5)(2, 11, 23, 20, 21, 18, 16, 6, 12, 31, 27, 4, 10)
(1, 5, 5, 6, 15)	unknown
(1, 4, 4, 5, 6, 12)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 24, 22, 31, 23, 15, 27, 10)(6, 7, 16, 13, 20)(9, 21, 25, 28)(11, 17, 26, 30, 14, 29)
(1, 5, 5, 5, 16)	unknown
(1, 3, 3, 3, 6, 7, 9)	(0, 29, 11, 7, 10, 18, 24, 17, 20)(1, 30, 25, 2, 27, 9)(3, 31, 8, 6, 28, 23, 19)(4, 26, 21)(5, 16, 22)(12, 15, 14)
(1, 3, 4, 4, 5, 5, 5, 5)	(1, 2, 4, 3)(5, 8, 19, 26, 10)(6, 7, 16, 13, 20)(9, 21, 30, 22)(11, 17, 31, 14, 29)(12, 18, 24, 28, 25)(15, 27, 23)
(1, 3, 3, 3, 3, 3, 13)	unknown
(1, 3, 14, 14)	(0, 10, 28, 6, 13, 31, 16, 12, 15, 27, 21, 2, 14, 29)(1, 8, 24, 3, 11, 26, 5, 4, 9, 17, 19, 22, 18, 20)(7, 30, 25)
(1, 3, 4, 5, 6, 6, 7)	(1, 2, 4, 3)(5, 8, 19, 25, 9, 21, 10)(6, 7, 16, 13, 20)(11, 17, 26, 31, 22, 30)(12, 18, 28, 24, 14, 29)(15, 27, 23)
(1, 3, 4, 10, 14)	(1, 2, 4, 3)(5, 8, 19, 25, 11, 17, 31, 9, 21, 10)(6, 7, 16, 13, 20, 24, 28, 12, 18, 26, 15, 27, 30, 23)(14, 29, 22)
(1, 3, 3, 3, 3, 4, 7, 8)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 15, 26, 10)(6, 7, 16)(9, 21, 13, 20, 31, 14, 29)(11, 17, 25)(22, 28, 24)(23, 30, 27)
(1, 3, 3, 3, 4, 5, 6, 7)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16, 13, 20)(9, 21, 25, 23, 30, 22, 28)(11, 17, 26)(14, 29, 24)(15, 27, 31)
(1, 3, 3, 12, 13)	(0, 31, 6, 30, 11, 5, 18, 2, 25, 10, 16, 20)(1, 28, 21, 7, 8, 4, 24, 9, 3, 29, 26, 17, 23)(12, 13, 15)(19, 27, 22)
(1, 3, 3, 3, 5, 6, 11)	(0, 1, 3)(2, 5, 9, 20, 8, 18, 22, 15, 29, 10, 4)(7, 17, 25)(11, 16, 26, 19, 12, 31)(13, 28, 23, 24, 21)(14, 30, 27)
(1, 3, 3, 3, 4, 4, 7, 7)	(1, 2, 4, 3)(5, 8, 19, 14, 29, 24, 10)(6, 7, 16)(9, 21, 25, 23, 30, 22, 28)(11, 17, 26)(12, 18, 13, 20)(15, 27, 31)
(1, 4, 5, 10, 12)	(1, 2, 4, 3)(5, 8, 19, 24, 11, 17, 14, 22, 31, 10)(6, 7, 16, 13, 20, 26, 30, 15, 25, 28, 12, 18)(9, 21, 29, 23, 27)
(1, 3, 3, 4, 9, 12)	(1, 2, 4, 3)(5, 8, 19, 26, 15, 27, 30, 12, 18, 24, 28, 10)(6, 7, 16, 13, 20, 11, 17, 31, 23)(9, 21, 25)(14, 29, 22)
(1, 3, 7, 7, 14)	(1, 2, 3)(4, 8, 16, 23, 7, 9, 18)(5, 10, 22, 30, 26, 14, 31)(6, 11, 20, 13, 19, 24, 15, 29, 27, 17, 12, 25, 28, 21)
(1, 4, 4, 4, 4, 5, 10)	(1, 2, 4, 3)(5, 8, 19, 24, 10)(6, 7, 16, 25)(9, 21, 13, 20)(11, 17, 31, 23, 27, 30, 15, 26, 14, 29)(12, 18, 22, 28)
(1, 7, 7, 17)	(0, 7, 23, 9, 18, 8, 20, 11, 22, 31, 29, 14, 24, 10, 2, 3, 6)(1, 5, 15, 27, 21, 12, 25)(13, 26, 17, 30, 19, 16, 28)
(1, 3, 4, 6, 6, 6, 6)	(1, 2, 4, 3)(5, 8, 19, 22, 31, 10)(6, 7, 16, 13, 20, 30)(9, 21, 25, 23, 28, 24)(11, 17, 14, 29, 15, 27)(12, 18, 26)
(1, 7, 12, 12)	(0, 22, 11, 12, 4, 17, 31)(1, 21, 9, 10, 25, 3, 20, 24, 26, 30, 14, 7)(2, 16, 29, 18, 19, 8, 13, 6, 23, 15, 5, 27)
(1, 3, 3, 8, 17)	(0, 16, 27, 4, 23, 30, 20, 13)(1, 19, 14)(2, 22, 8, 11, 10, 31, 5, 29, 6, 17, 25, 15, 3, 18, 21, 9, 12)(24, 28, 26)
(1, 3, 3, 3, 3, 3, 6, 7)	unknown
(1, 3, 4, 5, 5, 7, 7)	(1, 2, 4, 3)(5, 8, 19, 24, 9, 21, 10)(6, 7, 16, 13, 20)(11, 17, 31, 15, 27, 23, 30)(12, 18, 26)(14, 29, 25, 28, 22)
(1, 9, 11, 11)	(1, 2, 24, 16, 23, 12, 9, 13, 4, 15, 17)(3, 27, 29, 10, 25, 6, 8, 30, 11, 18, 31)(5, 20, 21, 26, 22, 28, 14, 19, 7)
(1, 3, 7, 7, 7, 7)	(1, 2, 3)(4, 8, 16, 12, 24, 28, 20)(5, 10, 19, 13, 26, 29, 23)(6, 11, 17, 14, 27, 30, 21)(7, 9, 18, 15, 25, 31, 22)
(1, 4, 4, 4, 4, 4, 5, 6)	(1, 2, 4, 3)(5, 8, 19, 22, 30, 10)(6, 7, 16, 25)(9, 21, 13, 20, 24)(11, 17, 31, 27)(12, 18, 15, 26)(14, 29, 23, 28)
(1, 3, 4, 5, 9, 10)	(1, 2, 4, 3)(5, 8, 19, 24, 10)(6, 7, 16, 13, 20, 26, 31, 12, 18)(9, 21, 28)(11, 17, 14, 22, 30, 15, 25, 29, 23, 27)

Continued on next page

Cycle Types	Orthomorphism
(1, 4, 4, 4, 4, 5, 5, 5)	(1, 2, 4, 3)(5, 8, 19, 24, 10)(6, 7, 16, 25, 23)(9, 21, 13, 20)(11, 17, 14, 29)(12, 18, 30, 22, 28)(15, 26, 31, 27)
(1, 3, 3, 3, 3, 3, 4, 6, 6)	(1, 2, 3)(4, 8, 16)(5, 10, 19, 21)(6, 11, 23, 13, 31, 24)(7, 12, 17)(9, 28, 22)(14, 29, 25)(15, 20, 26, 18, 27, 30)
(1, 5, 10, 16)	(0, 26, 14, 5, 18, 21, 16, 1, 24, 28, 12, 4, 25, 23, 20, 22)(2, 30, 17, 3, 27, 8, 9, 15, 6, 29)(7, 10, 31, 19, 13)
(1, 3, 3, 5, 5, 7, 8)	(1, 2, 3)(4, 8, 16, 12, 22)(5, 10, 29, 26, 31, 20, 28)(6, 11, 24)(7, 9, 18, 13, 25, 15, 30, 23)(14, 27, 17, 21, 19)
(1, 3, 3, 3, 22)	(0, 31, 25, 19, 8, 12, 1, 29, 7, 15, 3, 30, 21, 18, 16, 4, 28, 9, 10, 26, 11, 14)(2, 27, 13)(5, 23, 22)(6, 24, 17)
(1, 5, 6, 6, 7, 7)	unknown
(1, 4, 4, 4, 6, 6, 7)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16, 13, 20, 24, 22)(9, 21, 28, 25, 15, 27)(11, 17, 26, 30)(14, 29, 23, 31)
(1, 4, 4, 5, 5, 5, 8)	(1, 2, 4, 3)(5, 8, 19, 27, 10)(6, 7, 16, 30, 23, 15, 26, 22)(9, 21, 31, 13, 20)(11, 17, 14, 29)(12, 18, 25, 28, 24)
(1, 3, 3, 3, 3, 3, 3, 5, 8)	unknown
(1, 3, 4, 4, 6, 14)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 22, 24, 14, 29, 15, 27, 23, 31, 10)(6, 7, 16, 13, 20, 30)(9, 21, 28, 25)(11, 17, 26)
(1, 4, 4, 4, 4, 4, 11)	(1, 2, 4, 3)(5, 8, 19, 25, 23, 31, 11, 17, 9, 21, 10)(6, 7, 16, 27)(12, 18, 22, 26)(13, 20, 29, 24)(14, 28, 15, 30)
(1, 3, 3, 3, 3, 3, 3, 4, 4, 5)	unknown
(1, 3, 3, 5, 6, 6, 8)	(0, 1, 3)(2, 5, 9, 20, 10, 4)(7, 17, 25, 14, 30, 27)(8, 18, 22, 15, 29)(11, 16, 26, 23, 24, 19, 12, 31)(13, 28, 21)
(1, 3, 4, 4, 4, 4, 4, 8)	(1, 2, 4, 3)(5, 8, 19, 23, 28, 22, 24, 10)(6, 7, 16, 25)(9, 21, 13, 20)(11, 17, 29)(12, 18, 26, 31)(14, 27, 15, 30)
(1, 3, 3, 4, 5, 6, 10)	(1, 2, 4, 3)(5, 8, 19, 26, 11, 17, 31, 9, 21, 10)(6, 7, 16, 13, 20)(12, 18, 25)(14, 29, 24, 28, 22, 30)(15, 27, 23)
(1, 3, 4, 12, 12)	(1, 2, 4, 3)(5, 8, 19, 22, 14, 29, 15, 27, 11, 17, 31, 10)(6, 7, 16, 13, 20, 30, 23, 28, 24, 9, 21, 25)(12, 18, 26)
(1, 3, 3, 3, 3, 5, 5, 9)	(1, 2, 3)(4, 8, 16, 22, 15, 19, 6, 11, 31)(5, 10, 24)(7, 12, 29, 25, 17)(9, 26, 13, 18, 23)(14, 30, 20)(21, 27, 28)
(1, 3, 5, 5, 6, 12)	(0, 4, 7, 16, 2)(1, 6, 3, 5, 10, 18, 26, 11, 20, 15, 21, 12)(8, 22, 28)(9, 31, 30, 23, 25)(13, 17, 29, 14, 19, 24)
(1, 4, 4, 4, 5, 7, 7)	(1, 2, 4, 3)(5, 8, 19, 24, 9, 21, 10)(6, 7, 16, 28, 25, 13, 20)(11, 17, 31, 27)(12, 18, 15, 26)(14, 29, 23, 30, 22)
(1, 3, 3, 3, 4, 4, 6, 8)	(1, 2, 4, 3)(5, 8, 19, 14, 29, 15, 27, 10)(6, 7, 16)(9, 21, 25)(11, 17, 26, 31, 23, 30)(12, 18, 13, 20)(22, 28, 24)
(1, 5, 5, 5, 8, 8)	unknown
(1, 3, 3, 3, 4, 5, 5, 8)	(1, 2, 4, 3)(5, 8, 19, 14, 29, 12, 18, 10)(6, 7, 16)(9, 21, 31, 15, 27)(11, 17, 24, 13, 20)(22, 30, 26)(23, 28, 25)
(1, 4, 5, 5, 7, 10)	(1, 2, 4, 3)(5, 8, 19, 26, 10)(6, 7, 16, 15, 27)(9, 21, 25, 28, 23, 31, 14, 29, 11, 17)(12, 18, 22, 24, 13, 20, 30)
(1, 3, 4, 4, 5, 5, 10)	(1, 2, 4, 3)(5, 8, 19, 24, 10)(6, 7, 16, 15, 27)(9, 21, 31, 22, 26, 30, 14, 29, 11, 17)(12, 18, 23, 25)(13, 20, 28)
(1, 3, 3, 4, 4, 5, 12)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 28, 22, 31, 23, 15, 27, 10)(6, 7, 16, 13, 20)(9, 21, 25)(11, 17, 26, 30)(14, 29, 24)
(1, 5, 5, 8, 13)	unknown
(1, 3, 5, 7, 7, 9)	(1, 2, 3)(4, 8, 16, 12, 24, 30, 21)(5, 10, 19, 23, 29, 13, 26, 31, 22)(6, 11, 17, 14, 27, 28, 20)(7, 9, 18, 15, 25)
(1, 3, 3, 3, 3, 5, 6, 8)	(1, 2, 3)(4, 8, 16, 13, 20, 17)(5, 10, 21, 6, 11, 23, 9, 30)(7, 12, 29)(14, 28, 27, 19, 26)(15, 31, 25)(18, 24, 22)
(1, 5, 5, 5, 7, 9)	unknown
(1, 3, 3, 4, 6, 15)	(1, 2, 4, 3)(5, 8, 19, 22, 24, 10)(6, 7, 16, 13, 20, 28, 12, 18, 30, 23, 15, 27, 14, 29, 25)(9, 21, 31)(11, 17, 26)
(1, 3, 3, 4, 6, 7, 8)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16, 13, 20, 26, 22)(9, 21, 31)(11, 17, 25)(14, 29, 24, 28, 23, 30, 15, 27)
(1, 3, 5, 5, 18)	(31)(0, 20, 14, 11, 5, 28, 2, 16, 15, 8, 7, 4, 23, 30, 18, 3, 21, 24)(1, 22, 29, 13, 9)(6, 19, 25, 27, 26)(10, 17, 12)
(1, 4, 4, 4, 4, 4, 4, 7)	(1, 2, 4, 3)(5, 8, 19, 29, 14, 24, 10)(6, 7, 16, 25)(9, 21, 13, 20)(11, 17, 27, 31)(12, 18, 23, 28)(15, 30, 22, 26)
(1, 3, 3, 3, 3, 4, 4, 5, 6)	(1, 2, 4, 3)(5, 8, 19, 27, 23, 10)(6, 7, 16)(9, 21, 28, 25)(11, 17, 31, 13, 20)(12, 18, 24)(14, 29, 22)(15, 26, 30)
(1, 3, 3, 4, 4, 4, 4, 9)	(1, 2, 4, 3)(5, 8, 19, 24, 28, 22, 30, 23, 10)(6, 7, 16)(9, 21, 25)(11, 17, 31, 26)(12, 18, 13, 20)(14, 29, 15, 27)
(1, 3, 3, 6, 7, 12)	(0, 10, 5, 7, 29, 14, 27, 31, 30, 2, 12, 24)(1, 9, 22, 6, 11, 16)(3, 8, 17)(4, 13, 26)(15, 25, 21, 19, 20, 23, 18)
(1, 9, 22)	(0, 24, 22, 2, 28, 14, 7, 8, 11, 9, 13, 5, 16, 3, 25, 20, 19, 15, 4, 27, 10, 29)(1, 26, 12, 6, 31, 30, 18, 23, 17)
(1, 6, 8, 8, 9)	(1, 2, 22, 30, 6, 3, 12, 11, 23)(4, 9, 16, 10, 20, 24, 28, 13)(5, 7, 21, 27, 17, 26)(8, 19, 18, 15, 31, 25, 14, 29)
(1, 3, 4, 7, 17)	(1, 2, 4, 3)(5, 8, 19, 24, 29, 23, 27, 31, 12, 18, 6, 7, 16, 13, 20, 26, 10)(9, 21, 28)(11, 17, 14, 22, 30, 15, 25)
(1, 4, 5, 6, 16)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 25, 9, 21, 28, 24, 14, 29, 23, 15, 27, 10)(6, 7, 16, 13, 20)(11, 17, 31, 26, 22, 30)
(1, 7, 24)	(0, 13, 29, 8, 22, 1, 14, 28, 7, 26, 3, 15, 30, 24, 27, 4, 10, 2, 11, 23, 19, 9, 17, 5)(6, 12, 31, 20, 21, 18, 16)
(1, 3, 3, 3, 4, 9, 9)	(1, 2, 4, 3)(5, 8, 19, 25, 12, 18, 30, 23, 10)(6, 7, 16)(9, 21, 13, 20, 28, 14, 29, 24, 22)(11, 17, 26)(15, 27, 31)
(1, 3, 6, 6, 6, 10)	(1, 2, 3)(4, 8, 16, 7, 12, 31)(5, 10, 28, 14, 27, 21, 19, 15, 17, 24)(6, 11, 26, 29, 9, 25)(13, 20, 30, 22, 18, 23)
(1, 4, 4, 4, 4, 6, 9)	(1, 2, 4, 3)(5, 8, 19, 23, 27, 11, 17, 24, 10)(6, 7, 16, 30)(9, 21, 31, 14, 29, 22)(12, 18, 15, 26)(13, 20, 28, 25)
(1, 4, 11, 16)	(1, 2, 4, 3)(5, 8, 19, 25, 28, 23, 15, 27, 9, 21, 10)(6, 7, 16, 13, 20, 24, 14, 29, 12, 18, 26, 30, 11, 17, 31, 22)

Continued on next page

Cycle Types	Orthomorphism
(1, 3, 5, 9, 14)	(0, 20, 11, 14, 5, 25, 1, 23, 10, 27, 29, 17, 28, 30)(2, 18, 9, 8, 15, 7, 3, 22, 24)(4, 19, 16, 31, 13)(6, 21, 12)
(1, 3, 3, 4, 4, 5, 5, 7)	(1, 2, 4, 3)(5, 8, 19, 26, 10)(6, 7, 16, 15, 27)(9, 21, 31, 14, 29, 11, 17)(12, 18, 22, 30)(13, 20, 24)(23, 28, 25)
(1, 7, 7, 7, 10)	unknown
(1, 4, 4, 7, 7, 9)	(1, 2, 4, 3)(5, 8, 19, 31, 9, 21, 10)(6, 7, 16, 13, 20, 12, 18, 24, 22)(11, 17, 25, 28, 23, 30, 26)(14, 29, 15, 27)
(1, 3, 7, 9, 12)	(0, 22, 14, 7, 1, 21, 15, 5, 27, 2, 16, 29)(3, 20, 11, 12, 4, 17, 31)(6, 23, 24, 26, 30, 18, 19, 8, 13)(9, 10, 25)
(1, 3, 5, 6, 7, 10)	(0, 28, 10, 19, 24, 9)(1, 31, 25, 3, 30, 22, 18)(2, 26, 16, 23, 5, 17, 20, 4, 27, 21)(6, 29, 8, 7, 11)(12, 14, 13)
(1, 4, 4, 4, 19)	(1, 2, 4, 3)(5, 8, 19, 11, 17, 25, 23, 6, 7, 16, 13, 20, 31, 15, 27, 14, 29, 24, 10)(9, 21, 28, 22)(12, 18, 30, 26)
(1, 3, 4, 8, 16)	(1, 2, 4, 3)(5, 8, 19, 11, 17, 31, 26, 10)(6, 7, 16, 13, 20, 30, 22, 9, 21, 28, 24, 14, 29, 15, 27, 23)(12, 18, 25)
(1, 3, 3, 3, 3, 3, 4, 4, 8)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 15, 31, 10)(6, 7, 16)(9, 21, 30, 27)(11, 17, 24)(13, 20, 28)(14, 26, 22)(23, 29, 25)
(1, 4, 4, 6, 8, 9)	(1, 2, 4, 3)(5, 8, 19, 22, 26, 10)(6, 7, 16, 13, 20, 30, 12, 18, 25)(9, 21, 28, 24)(11, 17, 31, 23, 15, 27, 14, 29)
(1, 5, 6, 6, 6, 8)	unknown
(1, 3, 4, 6, 8, 10)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 23, 31, 15, 27, 10)(6, 7, 16, 13, 20, 30)(9, 21, 28)(11, 17, 26, 22, 24, 14, 29, 25)
(1, 3, 4, 4, 8, 12)	(1, 2, 4, 3)(5, 8, 19, 25, 9, 21, 28, 10)(6, 7, 16, 13, 20, 11, 17, 26, 15, 27, 31, 23)(12, 18, 30)(14, 29, 24, 22)
(1, 3, 3, 5, 7, 13)	(0, 3, 1)(2, 5, 14, 18, 6)(7, 20, 13, 19, 28, 11, 25, 21, 27, 22, 30, 23, 29)(8, 24, 9, 31, 26, 15, 16)(10, 12, 17)
(1, 5, 5, 7, 7, 7)	unknown
(1, 3, 3, 3, 5, 7, 10)	(0, 29, 24, 11, 7, 10, 18)(1, 30, 9)(2, 27, 20)(3, 31, 4, 26, 19, 25, 8, 6, 28, 23)(5, 16, 22, 17, 21)(12, 15, 14)
(1, 3, 3, 6, 6, 6, 7)	(1, 2, 3)(4, 8, 16, 24, 15, 31)(5, 10, 23, 17, 21, 28)(6, 11, 29, 9, 26, 20)(7, 12, 22)(13, 18, 14, 27, 30, 25, 19)
(1, 6, 6, 6, 13)	unknown
(1, 4, 5, 5, 5, 5, 7)	(1, 2, 4, 3)(5, 8, 19, 24, 12, 18, 10)(6, 7, 16, 28, 22)(9, 21, 27, 13, 20)(11, 17, 14, 29, 25)(15, 26, 31, 23, 30)
(1, 6, 7, 8, 10)	(0, 23, 9, 11, 13, 7)(1, 20, 15, 4, 16, 28, 29, 18, 10, 24)(2, 17, 31, 14, 6, 22, 27, 30)(3, 21, 8, 12, 5, 26, 25)
(1, 3, 3, 3, 3, 3, 4, 4, 4, 4)	unknown
(1, 3, 3, 3, 5, 5, 5, 7)	unknown
(1, 5, 6, 8, 12)	unknown
(1, 5, 7, 8, 11)	(0, 4, 7, 20, 13, 25, 2)(1, 6, 3, 5, 12, 26, 22, 10)(8, 23, 29, 15, 24, 16, 31, 14, 27, 11, 21)(9, 17, 28, 18, 19)
(1, 4, 5, 5, 5, 12)	(1, 2, 4, 3)(5, 8, 19, 24, 10)(6, 7, 16, 13, 20, 26, 31, 27, 23, 29, 12, 18)(9, 21, 28, 15, 25)(11, 17, 14, 22, 30)
(1, 3, 5, 10, 13)	(0, 5, 13, 24, 11, 20, 14, 26, 17, 28, 19, 18, 10)(1, 7, 21, 8, 22, 31, 3, 4, 6, 2)(9, 16, 30, 15, 25)(12, 27, 23)
(1, 3, 3, 3, 4, 4, 14)	(1, 2, 4, 3)(5, 8, 19, 14, 29, 13, 20, 30, 22, 9, 21, 28, 24, 10)(6, 7, 16)(11, 17, 31, 26)(12, 18, 25)(15, 27, 23)
(1, 4, 5, 8, 14)	(1, 2, 4, 3)(5, 8, 19, 24, 13, 20, 28, 10)(6, 7, 16, 15, 27)(9, 21, 31, 22, 26, 30, 14, 29, 12, 18, 23, 25, 11, 17)
(1, 4, 5, 11, 11)	(1, 2, 4, 3)(5, 8, 19, 24, 22, 26, 12, 18, 23, 31, 10)(6, 7, 16, 15, 27)(9, 21, 28, 13, 20, 30, 14, 29, 25, 11, 17)
(1, 3, 6, 11, 11)	(0, 21, 31, 19, 24, 7, 5, 29, 30, 15, 9)(1, 23, 12, 11, 4, 22, 27, 26, 3, 20, 28)(2, 17, 13, 8, 6, 18)(10, 16, 14)
(1, 3, 3, 25)	(0, 6, 7, 17, 14, 23, 31, 3, 4, 1, 5, 11, 28, 16, 13, 22, 8, 29, 18, 27, 15, 21, 24, 19, 2)(9, 26, 10)(12, 20, 30)
(1, 3, 3, 3, 10, 12)	(0, 31, 25, 18, 16, 4, 28, 9, 10, 26, 11, 14)(1, 29, 7, 15, 3, 30, 20, 19, 8, 12)(2, 27, 13)(5, 23, 22)(6, 24, 17)
(1, 3, 4, 4, 5, 6, 9)	(1, 2, 4, 3)(5, 8, 19, 31, 23, 25, 12, 18, 10)(6, 7, 16, 13, 20)(9, 21, 28, 22)(11, 17, 26, 30, 15, 27)(14, 29, 24)
(1, 4, 7, 8, 12)	(1, 2, 4, 3)(5, 8, 19, 24, 9, 21, 10)(6, 7, 16, 13, 20, 28, 22, 26, 12, 18, 23, 30)(11, 17, 31, 15, 27, 14, 29, 25)
(1, 3, 4, 4, 4, 4, 12)	(1, 2, 4, 3)(5, 8, 19, 25, 11, 17, 31, 26, 15, 27, 23, 10)(6, 7, 16)(9, 21, 28, 24)(12, 18, 13, 20)(14, 29, 22, 30)
(1, 3, 3, 5, 10, 10)	(1, 2, 3)(4, 8, 16, 23, 28, 26, 14, 31, 12, 25)(5, 10, 22, 6, 11, 20, 30, 7, 9, 18)(13, 19, 27)(15, 29, 24, 17, 21)
(1, 3, 3, 3, 6, 6, 10)	(1, 2, 3)(4, 8, 16, 22, 17, 24, 15, 19, 23, 25)(5, 10, 26)(6, 11, 29, 7, 12, 18)(9, 27, 30, 13, 20, 28)(14, 21, 31)
(1, 4, 6, 6, 7, 8)	(1, 2, 4, 3)(5, 8, 19, 25, 9, 21, 10)(6, 7, 16, 13, 20, 24, 28, 23)(11, 17, 31, 22, 14, 29)(12, 18, 26, 15, 27, 30)
(1, 3, 4, 4, 6, 7, 7)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 24, 10)(6, 7, 16, 13, 20, 28, 23)(9, 21, 25)(11, 17, 31, 22, 14, 29)(15, 27, 30, 26)
(1, 4, 27)	(1, 2, 4, 3)(5, 8, 19, 24, 28, 9, 21, 29, 23, 27, 30, 15, 25, 11, 17, 14, 22, 31, 12, 18, 6, 7, 16, 13, 20, 26, 10)
(1, 3, 3, 3, 3, 3, 7, 9)	(1, 2, 3)(4, 8, 16, 7, 12, 18, 27, 15, 22)(5, 10, 26)(6, 11, 30, 13, 28, 24, 29)(9, 21, 31)(14, 19, 20)(17, 23, 25)
(1, 3, 4, 5, 19)	(1, 2, 4, 3)(5, 8, 19, 24, 22, 26, 12, 18, 23, 30, 14, 29, 25, 11, 17, 9, 21, 31, 10)(6, 7, 16, 15, 27)(13, 20, 28)
(1, 3, 3, 3, 6, 8, 8)	(0, 16, 11, 1, 18, 7)(2, 20, 10, 21, 29, 9, 5, 24)(3, 17, 8)(4, 19, 28)(6, 23, 25, 31, 22, 27, 30, 26)(12, 14, 15)
(1, 3, 3, 3, 3, 3, 3, 4, 6)	unknown
(1, 3, 3, 6, 6, 13)	(1, 2, 3)(4, 8, 16, 12, 22, 19, 5, 10, 29, 26, 28, 14, 27)(6, 11, 24)(7, 9, 18, 15, 30, 23)(13, 25, 17, 21, 31, 20)

Continued on next page

Cycle Types	Orthomorphism
(1, 3, 3, 6, 9, 10)	(0, 16, 11, 1, 18, 7)(2, 20, 28, 25, 31, 27, 22, 10, 21, 26)(3, 17, 8)(4, 19, 29, 9, 5, 24, 6, 23, 30)(12, 14, 15)
(1, 3, 3, 4, 4, 4, 5, 8)	(1, 2, 4, 3)(5, 8, 19, 25, 28, 9, 21, 10)(6, 7, 16)(11, 17, 24, 22)(12, 18, 26, 30)(13, 20, 31, 14, 29)(15, 27, 23)
(1, 3, 4, 5, 7, 12)	(1, 2, 4, 3)(5, 8, 19, 25, 28, 24, 14, 29, 12, 18, 26, 10)(6, 7, 16, 13, 20)(9, 21, 30, 11, 17, 31, 22)(15, 27, 23)
(1, 3, 3, 3, 4, 6, 6, 6)	(1, 2, 4, 3)(5, 8, 19, 26, 30, 10)(6, 7, 16)(9, 21, 31, 15, 23, 27)(11, 17, 14, 29, 24, 22)(12, 18, 25)(13, 20, 28)
(1, 3, 4, 5, 8, 11)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 24, 9, 21, 25, 28, 10)(6, 7, 16, 13, 20)(11, 17, 31, 23, 30, 26, 15, 27)(14, 29, 22)
(1, 3, 3, 5, 6, 7, 7)	(1, 2, 3)(4, 8, 16, 23, 28, 12, 25)(5, 10, 22, 30, 26, 14, 31)(6, 11, 20, 13, 19, 21)(7, 9, 18, 27, 17)(15, 29, 24)
(1, 4, 4, 4, 5, 14)	(1, 2, 4, 3)(5, 8, 19, 26, 11, 17, 9, 21, 31, 13, 20, 24, 28, 10)(6, 7, 16, 15, 27)(12, 18, 23, 25)(14, 29, 22, 30)
(1, 3, 4, 6, 9, 9)	(1, 2, 4, 3)(5, 8, 19, 26, 22, 24, 9, 21, 10)(6, 7, 16, 13, 20, 30)(11, 17, 25, 12, 18, 23, 28, 14, 29)(15, 27, 31)
(1, 4, 4, 6, 6, 11)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16, 13, 20, 30, 26, 11, 17, 24, 22)(9, 21, 25, 28, 23, 31)(14, 29, 15, 27)
(1, 3, 4, 6, 6, 12)	(1, 2, 4, 3)(5, 8, 19, 24, 28, 10)(6, 7, 16, 13, 20, 11, 17, 31, 22, 14, 29, 23)(9, 21, 25)(12, 18, 26, 15, 27, 30)
(1, 3, 3, 4, 4, 4, 13)	(1, 2, 4, 3)(5, 8, 19, 6, 7, 16, 13, 20, 26, 31, 9, 21, 10)(11, 17, 25)(12, 18, 24, 28)(14, 29, 22)(15, 27, 23, 30)
(1, 3, 3, 5, 20)	(0, 31, 6, 30, 10, 16, 20, 7, 8, 4, 24, 9, 3, 29, 26, 17, 23, 1, 28, 21)(2, 25, 11, 5, 18)(12, 13, 15)(19, 27, 22)
(1, 3, 5, 7, 16)	(1, 2, 3)(4, 8, 16, 23, 30)(5, 10, 22, 6, 11, 20, 28, 15, 29, 27, 13, 19, 7, 9, 18, 24)(12, 25, 14, 31, 26, 17, 21)
(1, 7, 9, 15)	(0, 28, 10, 25, 17, 5, 20, 16, 7, 12, 2, 24, 26, 8, 15)(1, 30, 23, 18, 19, 11, 13)(3, 29, 4, 31, 21, 22, 6, 27, 14)
(1, 6, 7, 9, 9)	(1, 2, 4, 14, 18, 29, 16, 27, 26)(3, 19, 12, 9, 28, 20)(5, 24, 6, 10, 25, 23, 13, 21, 7)(8, 17, 22, 31, 11, 15, 30)
(1, 6, 10, 15)	(0, 9, 28, 3, 8, 26, 31, 19, 30, 29)(1, 11, 24, 4, 10, 12, 23, 7, 25, 15, 21, 2, 13, 20, 5)(6, 14, 22, 17, 16, 18)
(1, 4, 4, 8, 15)	(1, 2, 4, 3)(5, 8, 19, 23, 30, 6, 7, 16, 13, 20, 28, 12, 18, 24, 10)(9, 21, 25, 15, 27, 14, 29, 22)(11, 17, 31, 26)
(1, 5, 8, 18)	(0, 17, 24, 27, 4, 22, 12, 3, 19, 15, 2, 23, 31, 8, 10, 30, 21, 14)(1, 18, 20, 9, 13)(5, 28, 25, 7, 6, 16, 26, 29)
(1, 3, 3, 3, 6, 16)	(0, 16, 11, 1, 18, 7)(2, 20, 28, 25, 31, 27, 22, 10, 21, 26, 4, 19, 29, 9, 5, 24)(3, 17, 8)(6, 23, 30)(12, 14, 15)
(1, 5, 5, 6, 7, 8)	unknown
(1, 3, 5, 6, 17)	(0, 25, 22, 16, 2, 29)(1, 27, 23, 19, 20, 3, 24, 11, 8, 10, 28, 13, 4, 26, 15, 5, 17)(6, 30, 31, 18, 14)(7, 9, 12)
(1, 4, 4, 4, 4, 7, 8)	(1, 2, 4, 3)(5, 8, 19, 23, 30, 12, 18, 10)(6, 7, 16, 27)(9, 21, 31, 15, 26, 22, 24)(11, 17, 14, 29)(13, 20, 28, 25)
(1, 3, 9, 9, 10)	(1, 2, 3)(4, 8, 16, 12, 24, 29, 15, 25, 31, 20)(5, 10, 19, 23, 6, 11, 17, 14, 27)(7, 9, 18, 21, 28, 22, 30, 13, 26)
(1, 5, 8, 8, 10)	unknown
(1, 6, 25)	(0, 9, 21, 17, 1, 10, 6, 8, 18, 20, 22, 5, 4, 14, 24, 31, 16, 2, 15, 26, 7, 30, 29, 12, 27)(3, 11, 19, 13, 25, 28)
(1, 3, 4, 4, 4, 16)	(1, 2, 4, 3)(5, 8, 19, 24, 22, 6, 7, 16, 13, 20, 11, 17, 9, 21, 31, 10)(12, 18, 26)(14, 29, 25, 28)(15, 27, 23, 30)
(1, 3, 3, 3, 3, 3, 4, 5, 7)	unknown
(1, 3, 3, 3, 3, 5, 14)	(0, 3, 1)(2, 5, 14, 18, 6)(7, 20, 30)(8, 24, 9, 31, 22, 27, 23, 13, 19, 29, 21, 26, 15, 16)(10, 12, 17)(11, 25, 28)
(1, 4, 4, 23)	(1, 2, 4, 3)(5, 8, 19, 25, 11, 17, 31, 22, 6, 7, 16, 13, 20, 28, 23, 15, 27, 14, 29, 24, 9, 21, 10)(12, 18, 30, 26)
(1, 4, 4, 6, 7, 10)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16, 13, 20, 24, 9, 21, 31, 22)(11, 17, 25, 23, 28, 14, 29)(15, 27, 30, 26)
(1, 3, 4, 4, 4, 5, 5, 6)	(1, 2, 4, 3)(5, 8, 19, 24, 10)(6, 7, 16, 30)(9, 21, 31, 22)(11, 17, 12, 18, 23, 27)(13, 20, 28)(14, 29, 25, 15, 26)
(1, 3, 3, 3, 5, 17)	(0, 27, 14, 10, 20, 21, 3, 25, 13, 11, 1, 24, 17, 18, 30, 15, 8)(2, 29, 31)(4, 28, 19)(5, 22, 6, 26, 23)(7, 12, 9)
(1, 3, 4, 5, 5, 6, 8)	(1, 2, 4, 3)(5, 8, 19, 24, 10)(6, 7, 16)(9, 21, 25, 28, 22)(11, 17, 31, 23, 30, 26)(12, 18, 15, 27, 14, 29, 13, 20)
(1, 3, 5, 5, 5, 5, 8)	unknown
(1, 5, 8, 9, 9)	(0, 20, 12, 6, 21, 11, 14, 5, 25)(1, 23, 10, 27, 29, 17, 28, 30)(2, 18, 9, 8, 15, 7, 3, 22, 24)(4, 19, 16, 31, 13)
(1, 4, 4, 4, 7, 12)	(1, 2, 4, 3)(5, 8, 19, 11, 17, 24, 22, 28, 25, 9, 21, 10)(6, 7, 16, 13, 20, 31, 23)(12, 18, 30, 26)(14, 29, 15, 27)
(1, 3, 28)	(0, 8, 27, 26, 28, 30, 2, 12, 22, 18, 7, 24, 6, 15, 20, 3, 9, 29, 16, 19, 31, 14, 23, 1, 10, 13, 21, 5)(4, 11, 25)
(1, 3, 5, 5, 5, 13)	(1, 2, 3)(4, 8, 16, 12, 22)(5, 10, 29, 23, 31, 15, 30, 21, 17, 20, 19, 26, 28)(6, 11, 24, 14, 27)(7, 9, 18, 13, 25)
(1, 4, 4, 6, 17)	(1, 2, 4, 3)(5, 8, 19, 6, 7, 16, 13, 20, 24, 14, 29, 23, 15, 27, 9, 21, 10)(11, 17, 31, 22, 30, 26)(12, 18, 25, 28)
(1, 8, 8, 15)	(0, 23, 30, 28, 1, 21, 29, 15, 11, 6, 16, 12, 9, 2, 19)(3, 22, 13, 10, 18, 24, 25, 26)(4, 20, 27, 5, 31, 17, 14, 8)
(1, 5, 6, 6, 14)	unknown
(1, 5, 5, 5, 5, 5, 6)	unknown
(1, 4, 4, 4, 9, 10)	(1, 2, 4, 3)(5, 8, 19, 24, 14, 29, 23, 15, 27, 10)(6, 7, 16, 13, 20, 11, 17, 31, 22)(9, 21, 25, 28)(12, 18, 26, 30)
(1, 3, 3, 11, 14)	(0, 27, 9, 14, 4, 24, 21, 22, 1, 25, 23, 18, 20, 16)(2, 31, 29, 3, 26, 15, 7, 11, 10, 30, 17)(5, 19, 12)(6, 28, 13)
(1, 3, 3, 7, 7, 11)	(0, 30, 26, 18, 27, 11, 4, 25, 8, 5, 19)(1, 29, 10, 17, 23, 16, 21)(2, 24, 20, 6, 31, 7, 9)(3, 28, 22)(13, 14, 15)

Continued on next page

Cycle Types	Orthomorphism
(1, 3, 3, 4, 10, 11)	(1, 2, 4, 3)(5, 8, 19, 11, 17, 31, 15, 27, 9, 21, 10)(6, 7, 16, 13, 20, 28, 22, 26, 30, 23)(12, 18, 25)(14, 29, 24)
(1, 3, 3, 4, 5, 8, 8)	(1, 2, 4, 3)(5, 8, 19, 24, 10)(6, 7, 16)(9, 21, 28, 25, 12, 18, 13, 20)(11, 17, 31, 14, 29, 23, 15, 27)(22, 30, 26)
(1, 3, 12, 16)	(0, 21, 31, 19, 2, 17, 12, 11, 4, 22, 15, 9)(1, 23, 28, 3, 20, 25, 24, 27, 7, 5, 29, 13, 8, 6, 18, 26)(10, 16, 14)
(1, 3, 3, 3, 3, 3, 4, 12)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 15, 31, 27, 30, 23, 25, 10)(6, 7, 16)(9, 21, 29)(11, 17, 26)(13, 20, 24)(14, 28, 22)
(1, 6, 8, 17)	(0, 18, 12, 23, 15, 3, 19, 14, 5, 28, 30, 1, 16, 20, 25, 31, 8)(2, 22, 10, 4, 17, 11)(6, 21, 26, 29, 24, 27, 13, 7)
(1, 3, 5, 5, 9, 9)	(1, 2, 3)(4, 8, 16, 23, 30, 27, 6, 11, 20)(5, 10, 22, 28, 24, 15, 29, 14, 31)(7, 9, 18, 26, 17)(12, 25, 13, 19, 21)
(1, 3, 8, 10, 10)	(0, 5, 13, 24, 23, 15, 25, 10)(1, 7, 21, 9, 16, 30, 3, 4, 6, 2)(8, 22, 12, 27, 11, 20, 31, 14, 26, 19)(17, 29, 28)
(1, 3, 3, 3, 4, 6, 12)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16, 13, 20, 26, 22, 28, 9, 21, 30, 23)(11, 17, 25)(14, 29, 24)(15, 27, 31)
(1, 5, 13, 13)	(0, 4, 3, 6, 5, 9, 24, 10, 11, 30, 14, 21, 29)(1, 7, 19, 26, 12, 22, 8, 31, 16, 15, 23, 28, 18)(13, 20, 25, 27, 17)
(1, 4, 4, 9, 14)	(1, 2, 4, 3)(5, 8, 19, 11, 17, 31, 22, 30, 26, 15, 27, 9, 21, 10)(6, 7, 16, 13, 20, 24, 14, 29, 23)(12, 18, 25, 28)
(1, 3, 3, 5, 5, 5, 10)	(1, 2, 3)(4, 8, 16, 12, 22)(5, 10, 29, 20, 19, 23, 28, 26, 31, 21)(6, 11, 24)(7, 9, 18, 15, 30)(13, 25, 17, 14, 27)
(1, 3, 3, 3, 5, 8, 9)	(1, 2, 3)(4, 8, 16, 23, 30)(5, 10, 22)(6, 11, 20, 13, 19, 24, 15, 29, 27)(7, 9, 18, 26, 14, 31, 21, 17)(12, 25, 28)
(1, 3, 4, 5, 5, 5, 9)	(1, 2, 4, 3)(5, 8, 19, 26, 10)(6, 7, 16)(9, 21, 25, 28, 24)(11, 17, 31, 23, 15, 27, 14, 29, 22)(12, 18, 13, 20, 30)
(1, 3, 4, 7, 8, 9)	(1, 2, 4, 3)(5, 8, 19, 25, 9, 21, 10)(6, 7, 16, 13, 20, 24, 28, 23)(11, 17, 31, 22, 14, 29, 15, 27, 30)(12, 18, 26)
(1, 7, 10, 14)	(0, 24, 13, 8, 3, 26, 20)(1, 27, 17, 16, 19, 28, 14, 9, 4, 31, 29, 12, 10, 23)(2, 30, 18, 5, 21, 6, 25, 7, 15, 11)
(1, 3, 3, 4, 21)	(1, 2, 4, 3)(5, 8, 19, 25, 11, 17, 31, 15, 27, 30, 23, 6, 7, 16, 13, 20, 24, 28, 9, 21, 10)(12, 18, 26)(14, 29, 22)
(1, 3, 3, 3, 3, 3, 5, 11)	unknown
(1, 3, 4, 4, 20)	(1, 2, 4, 3)(5, 8, 19, 25, 11, 17, 31, 14, 29, 22, 6, 7, 16, 13, 20, 24, 28, 9, 21, 10)(12, 18, 26)(15, 27, 30, 23)
(1, 3, 5, 6, 6, 11)	(1, 2, 3)(4, 8, 16, 23, 30)(5, 10, 22, 15, 29, 21)(6, 11, 20, 7, 9, 18)(12, 25, 28, 26, 13, 19, 24, 14, 31, 27, 17)
(1, 4, 6, 10, 11)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 26, 11, 17, 31, 10)(6, 7, 16, 13, 20, 24, 14, 29, 25, 28, 22)(9, 21, 30, 23, 15, 27)
(1, 3, 4, 4, 5, 7, 8)	(1, 2, 4, 3)(5, 8, 19, 26, 11, 17, 31, 10)(6, 7, 16, 13, 20)(9, 21, 30, 22)(12, 18, 24, 14, 29, 25, 28)(15, 27, 23)
(1, 4, 9, 18)	(1, 2, 4, 3)(5, 8, 19, 24, 11, 17, 14, 22, 31, 15, 25, 28, 9, 21, 29, 23, 27, 10)(6, 7, 16, 13, 20, 26, 30, 12, 18)
(1, 3, 3, 4, 5, 5, 5, 6)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16)(9, 21, 25, 13, 20)(11, 17, 27)(14, 29, 15, 26, 31)(22, 30, 23, 28, 24)
(1, 4, 10, 17)	(1, 2, 4, 3)(5, 8, 19, 24, 9, 21, 29, 15, 25, 10)(6, 7, 16, 13, 20, 26, 31, 27, 23, 30, 11, 17, 14, 22, 28, 12, 18)
(1, 3, 3, 3, 5, 5, 12)	(0, 27, 21, 22, 16)(1, 25, 20)(2, 31, 29)(3, 26, 9, 14, 4, 24, 15, 7, 11, 10, 30, 17)(5, 19, 23, 18, 12)(6, 28, 13)
(1, 4, 5, 6, 7, 9)	(1, 2, 4, 3)(5, 8, 19, 25, 9, 21, 10)(6, 7, 16, 13, 20)(11, 17, 26, 22, 31, 23, 15, 27, 30)(12, 18, 28, 24, 14, 29)
(1, 4, 4, 5, 9, 9)	(1, 2, 4, 3)(5, 8, 19, 24, 9, 21, 25, 28, 10)(6, 7, 16, 13, 20, 11, 17, 31, 22)(12, 18, 26, 30)(14, 29, 23, 15, 27)
(1, 3, 3, 9, 16)	(0, 29, 11, 7, 10, 18, 24, 17, 20)(1, 30, 25, 8, 6, 28, 23, 19, 3, 31, 4, 26, 21, 2, 27, 9)(5, 16, 22)(12, 15, 14)
(1, 4, 7, 7, 13)	(1, 2, 4, 3)(5, 8, 19, 24, 9, 21, 10)(6, 7, 16, 13, 20, 28, 22)(11, 17, 31, 26, 12, 18, 30, 23, 15, 27, 14, 29, 25)
(1, 3, 3, 3, 4, 8, 10)	(1, 2, 4, 3)(5, 8, 19, 22, 30, 12, 18, 10)(6, 7, 16, 13, 20, 24, 14, 29, 23, 25)(9, 21, 28)(11, 17, 26)(15, 27, 31)
(1, 3, 4, 4, 4, 4, 4, 4, 4)	unknown
(1, 4, 6, 6, 6, 9)	(1, 2, 4, 3)(5, 8, 19, 31, 26, 10)(6, 7, 16, 13, 20, 30, 11, 17, 25)(9, 21, 28, 23, 15, 27)(12, 18, 22, 24, 14, 29)
(1, 3, 6, 7, 7, 8)	(0, 18, 5, 26, 6, 21, 24)(1, 16, 9, 7, 2, 22, 8)(3, 19, 31, 25, 29, 11)(4, 17, 10, 23, 28, 27, 20, 30)(13, 15, 14)
(1, 3, 5, 8, 15)	(0, 9, 28, 31, 3, 8, 26, 27, 15, 21, 5, 1, 11, 24, 29)(2, 13, 20)(4, 10, 12, 23, 16, 18, 30, 19)(6, 14, 22, 7, 25)
(1, 3, 3, 3, 3, 3, 3, 3, 3, 4)	unknown
(1, 5, 12, 14)	(0, 22, 9, 10, 25)(1, 21, 15, 5, 27, 3, 20, 24, 28, 30, 14, 7)(2, 16, 29, 18, 19, 8, 13, 6, 23, 11, 12, 4, 17, 31)
(1, 5, 5, 10, 11)	(0, 17, 24, 31, 5, 28, 4, 22, 29, 21, 14)(1, 18, 20, 9, 13)(2, 23, 8, 10, 30, 27, 12, 3, 19, 15)(6, 16, 26, 25, 7)
(1, 3, 7, 8, 13)	(0, 29, 24, 11, 7, 10, 18)(1, 30, 8, 6, 28, 23, 3, 31, 4, 26, 19, 25, 9)(2, 27, 20, 5, 16, 22, 17, 21)(12, 15, 14)
(1, 4, 7, 9, 11)	(1, 2, 4, 3)(5, 8, 19, 24, 29, 23, 27, 31, 10)(6, 7, 16, 13, 20, 26, 9, 21, 28, 12, 18)(11, 17, 14, 22, 30, 15, 25)
(1, 4, 4, 5, 6, 6, 6)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16, 13, 20)(9, 21, 25, 28)(11, 17, 26, 30, 15, 27)(14, 29, 23, 31, 22, 24)
(1, 4, 6, 7, 7, 7)	(1, 2, 4, 3)(5, 8, 19, 25, 9, 21, 10)(6, 7, 16, 30, 27, 13, 20)(11, 17, 24, 28, 23, 31)(12, 18, 15, 26, 22, 14, 29)
(1, 4, 4, 4, 4, 15)	(1, 2, 4, 3)(5, 8, 19, 23, 31, 22, 11, 17, 27, 13, 20, 24, 9, 21, 10)(6, 7, 16, 30)(12, 18, 25, 28)(14, 29, 15, 26)
(1, 3, 3, 3, 3, 7, 12)	(1, 2, 3)(4, 8, 16, 20, 17, 27, 19, 26, 14, 28, 15, 18)(5, 10, 21)(6, 11, 23, 9, 30, 25, 31)(7, 12, 29)(13, 24, 22)
(1, 3, 3, 4, 4, 7, 10)	(1, 2, 4, 3)(5, 8, 19, 24, 9, 21, 10)(6, 7, 16, 13, 20, 30, 11, 17, 31, 22)(12, 18, 26)(14, 29, 25, 28)(15, 27, 23)
(1, 3, 3, 4, 4, 4, 4, 5)	(1, 2, 4, 3)(5, 8, 19, 25, 10)(6, 7, 16)(9, 21, 29)(11, 17, 24, 22)(12, 18, 13, 20)(14, 28, 23, 27)(15, 31, 26, 30)

Continued on next page

Cycle Types	Orthomorphism
(1, 5, 5, 6, 6, 9)	unknown
(1, 3, 3, 3, 4, 4, 5, 9)	(1, 2, 4, 3)(5, 8, 19, 11, 17, 12, 18, 26, 10)(6, 7, 16)(9, 21, 31, 22)(13, 20, 24)(14, 29, 25, 23, 28)(15, 27, 30)
(1, 15, 16)	(0, 24, 14, 9, 4, 31, 1, 27, 17, 16, 19, 28, 18, 5, 21)(2, 30, 12, 10, 23, 6, 25, 13, 8, 3, 26, 22, 20, 7, 15, 11)
(1, 4, 4, 4, 8, 11)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 25, 11, 17, 24, 28, 10)(6, 7, 16, 30, 27, 15, 26, 22)(9, 21, 13, 20)(14, 29, 23, 31)
(1, 3, 3, 4, 5, 16)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 26, 30, 11, 17, 31, 22, 28, 23, 15, 27, 10)(6, 7, 16, 13, 20)(9, 21, 25)(14, 29, 24)
(1, 3, 3, 3, 9, 13)	(0, 12, 18, 27, 2, 8, 31, 7, 28, 6, 11, 29, 21)(1, 14, 19)(3, 13, 17, 20, 5, 4, 15, 16, 23)(9, 25, 10)(24, 26, 30)
(1, 3, 3, 4, 4, 4, 6, 7)	(1, 2, 4, 3)(5, 8, 19, 25, 9, 21, 10)(6, 7, 16)(11, 17, 31, 26)(12, 18, 15, 27, 23, 30)(13, 20, 28, 24)(14, 29, 22)
(1, 7, 11, 13)	(0, 6, 1, 4, 5, 14, 25, 11, 23, 8, 21, 12, 24)(3, 7, 22, 28, 16, 29, 30, 13, 27, 20, 10)(9, 19, 17, 31, 15, 26, 18)
(1, 3, 4, 4, 4, 4, 5, 7)	(1, 2, 4, 3)(5, 8, 19, 25, 23, 31, 10)(6, 7, 16)(9, 21, 28, 24)(11, 17, 26, 22)(12, 18, 13, 20)(14, 29, 15, 27, 30)
(1, 3, 3, 7, 18)	(0, 4, 3, 6, 5, 9, 24, 18, 25, 17, 12, 22, 8, 31, 29, 1, 7, 19)(10, 11, 30, 16, 15, 23, 26)(13, 20, 27)(14, 21, 28)
(1, 3, 3, 4, 4, 6, 11)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16)(9, 21, 31, 15, 27, 23, 30, 22, 24, 13, 20)(11, 17, 26)(14, 29, 25, 28)
(1, 3, 5, 5, 5, 6, 7)	(1, 2, 3)(4, 8, 16, 12, 22)(5, 10, 29, 26, 17, 20, 28)(6, 11, 24, 14, 27)(7, 9, 18, 13, 25)(15, 30, 23, 19, 21, 31)
(1, 5, 5, 7, 14)	(0, 15, 19, 2, 11, 30, 9, 26, 29, 22, 6, 8, 28, 25)(1, 13, 18, 24, 27)(3, 14, 16, 20, 21)(4, 12, 17, 23, 5, 7, 31)
(1, 3, 3, 6, 19)	(0, 28, 22, 16, 23, 2, 26, 18, 1, 31, 5, 17, 20, 4, 27, 21, 3, 30, 9)(6, 29, 25, 8, 7, 11)(10, 19, 24)(12, 14, 13)
(1, 3, 3, 4, 4, 8, 9)	(1, 2, 4, 3)(5, 8, 19, 14, 29, 13, 20, 24, 10)(6, 7, 16)(9, 21, 28, 22)(11, 17, 31, 23, 15, 27, 30, 26)(12, 18, 25)
(1, 3, 3, 3, 4, 7, 11)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 24, 10)(6, 7, 16)(9, 21, 25)(11, 17, 31, 26, 30, 23, 15, 27, 14, 29, 22)(13, 20, 28)
(1, 5, 6, 20)	(0, 3, 2, 7, 19, 20, 15, 31, 5, 11, 18, 12, 29, 27, 17, 26, 23, 10, 6, 4)(8, 16, 24, 13, 30)(9, 22, 25, 14, 28, 21)
(1, 5, 5, 21)	(0, 17, 24, 29, 5, 28, 27, 4, 22, 12, 3, 19, 15, 2, 23, 31, 8, 10, 30, 21, 14)(1, 18, 20, 9, 13)(6, 16, 26, 25, 7)
(1, 5, 26)	(0, 24, 14, 9, 4, 31, 1, 27, 17, 16, 19, 28, 18, 5, 21, 7, 15, 11, 2, 30, 13, 8, 3, 26, 22, 20)(6, 25, 12, 10, 23)
(1, 4, 5, 5, 8, 9)	(1, 2, 4, 3)(5, 8, 19, 26, 12, 18, 23, 31, 10)(6, 7, 16, 15, 27)(9, 21, 25, 11, 17)(13, 20, 30, 14, 29, 22, 24, 28)
(1, 3, 4, 5, 6, 13)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 28, 24, 14, 29, 23, 15, 27, 10)(6, 7, 16, 13, 20)(9, 21, 25)(11, 17, 26, 31, 22, 30)
(1, 6, 12, 13)	(0, 10, 15, 22, 16, 17, 19, 29, 18, 5, 2, 14, 21)(1, 8, 25, 7, 26, 30)(3, 11, 27, 24, 12, 20, 6, 13, 23, 4, 9, 31)
(1, 11, 20)	(0, 16, 27, 25, 4, 23, 9, 12, 2, 22, 28, 26, 30, 5, 29, 21, 15, 3, 18, 13)(1, 19, 20, 8, 11, 10, 31, 6, 17, 24, 14)
(1, 3, 4, 7, 7, 10)	(1, 2, 4, 3)(5, 8, 19, 11, 17, 24, 10)(6, 7, 16, 13, 20, 28, 12, 18, 23, 25)(9, 21, 31)(14, 29, 22, 26, 30, 15, 27)
(1, 4, 4, 5, 18)	(1, 2, 4, 3)(5, 8, 19, 6, 7, 16, 13, 20, 24, 28, 12, 18, 25, 15, 27, 9, 21, 10)(11, 17, 31, 26)(14, 29, 23, 30, 22)
(1, 3, 3, 3, 3, 6, 6, 7)	(1, 2, 3)(4, 8, 16, 30, 15, 22, 17)(5, 10, 24, 28, 26, 31)(6, 11, 21)(7, 12, 23)(9, 20, 29)(13, 27, 19, 25, 14, 18)
(1, 4, 5, 22)	(1, 2, 4, 3)(5, 8, 19, 24, 10)(6, 7, 16, 13, 20, 26, 30, 15, 25, 28, 9, 21, 29, 23, 27, 11, 17, 14, 22, 31, 12, 18)
(1, 3, 6, 6, 8, 8)	(1, 2, 3)(4, 8, 16, 5, 10, 28, 14, 31)(6, 11, 23, 25, 30, 22)(7, 12, 21, 17, 27, 15, 24, 29)(9, 20, 18, 13, 19, 26)
(1, 4, 4, 7, 8, 8)	(1, 2, 4, 3)(5, 8, 19, 25, 28, 9, 21, 10)(6, 7, 16, 13, 20, 31, 23)(11, 17, 24, 22, 14, 29, 15, 27)(12, 18, 30, 26)
(1, 9, 9, 13)	(0, 18, 23, 15, 1, 17, 27, 7, 5, 31, 6, 19, 12)(2, 20, 28, 26, 30, 10, 29, 22, 13)(3, 16, 25, 4, 21, 11, 8, 9, 14)
(1, 3, 3, 3, 3, 4, 5, 5, 5)	(1, 2, 3)(4, 8, 16)(5, 10, 17, 15, 21)(6, 11, 23)(7, 12, 19, 26, 18)(9, 20, 13, 31)(14, 25, 29)(22, 28, 27, 30, 24)
(1, 3, 3, 3, 3, 3, 4, 9)	unknown
(1, 5, 6, 9, 11)	(1, 2, 27, 18, 10)(3, 11, 28, 13, 7, 23, 16, 21, 19, 30, 12)(4, 8, 9, 31, 29, 25)(5, 22, 24, 6, 26, 15, 20, 14, 17)
(1, 3, 4, 11, 13)	(1, 2, 4, 3)(5, 8, 19, 24, 29, 23, 27, 31, 15, 25, 10)(6, 7, 16, 13, 20, 26, 11, 17, 14, 22, 30, 12, 18)(9, 21, 28)
(1, 3, 6, 8, 14)	(0, 25, 13, 9, 5, 20, 1, 26, 23, 7, 14, 8, 2, 31)(3, 27, 16, 18, 4, 30, 12, 11)(6, 24, 15, 10, 22, 21)(19, 29, 28)
(1, 3, 4, 4, 9, 11)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 25, 28, 24, 10)(6, 7, 16)(9, 21, 13, 20)(11, 17, 31, 14, 29, 23, 30, 22, 26, 15, 27)
(1, 3, 6, 7, 15)	(0, 18, 29, 10, 23, 27)(1, 16, 9, 7, 2, 22, 8)(3, 19, 5, 26, 6, 21, 31, 20, 25, 30, 24, 28, 4, 17, 11)(13, 15, 14)
(1, 3, 6, 6, 16)	(0, 21, 25, 26, 7, 5, 29, 12, 11, 4, 22, 28, 3, 20, 15, 9)(1, 23, 31, 30, 19, 24)(2, 17, 13, 8, 6, 18)(10, 16, 14)
(1, 4, 4, 11, 12)	(1, 2, 4, 3)(5, 8, 19, 6, 7, 16, 13, 20, 24, 9, 21, 10)(11, 17, 31, 22, 14, 29, 23, 28, 25, 15, 27)(12, 18, 26, 30)
(1, 3, 4, 4, 4, 7, 9)	(1, 2, 4, 3)(5, 8, 19, 25, 11, 17, 31, 23, 10)(6, 7, 16)(9, 21, 28, 24)(12, 18, 13, 20)(14, 29, 22, 26, 15, 27, 30)
(1, 4, 7, 10, 10)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 24, 10)(6, 7, 16, 13, 20, 28, 9, 21, 30, 23)(11, 17, 31, 26, 22, 14, 29, 25, 15, 27)
(1, 3, 8, 8, 12)	(0, 17, 25, 4, 22, 29, 20, 14)(1, 18, 12, 3, 19, 21, 9, 13)(2, 23, 15)(5, 28, 27, 24, 7, 6, 16, 26, 31, 8, 10, 30)
(1, 3, 3, 3, 3, 8, 11)	(0, 1, 3)(2, 5, 9, 20, 8, 18, 22, 15, 29, 10, 4)(7, 17, 25)(11, 16, 26, 23, 24, 19, 12, 31)(13, 28, 21)(14, 30, 27)
(1, 5, 7, 9, 10)	(0, 15, 19, 2, 11, 30, 9, 26, 25)(1, 13, 18, 24, 29, 22, 6, 8, 28, 27)(3, 14, 16, 20, 21)(4, 12, 17, 23, 5, 7, 31)
(1, 6, 6, 9, 10)	unknown

Continued on next page



Cycle Types	Orthomorphism
(1, 12, 19)	(0, 23, 30, 29, 15, 11, 6, 16, 12, 9, 2, 19)(1, 21, 26, 3, 22, 13, 10, 18, 24, 25, 27, 5, 31, 17, 14, 8, 4, 20, 28)
(1, 3, 4, 4, 4, 8, 8)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 15, 27, 10)(6, 7, 16)(9, 21, 28, 25)(11, 17, 26, 30)(13, 20, 24, 22, 14, 29, 23, 31)
(1, 4, 5, 5, 17)	(1, 2, 4, 3)(5, 8, 19, 24, 13, 20, 26, 30, 14, 29, 12, 18, 23, 31, 22, 28, 10)(6, 7, 16, 15, 27)(9, 21, 25, 11, 17)
(1, 3, 5, 6, 8, 9)	(0, 28, 20, 4, 27, 9)(1, 31, 5, 17, 21, 3, 30, 24, 22)(2, 26, 16, 23, 18, 25, 10, 19)(6, 29, 8, 7, 11)(12, 14, 13)
(1, 3, 4, 4, 4, 6, 10)	(1, 2, 4, 3)(5, 8, 19, 14, 29, 23, 31, 22, 24, 10)(6, 7, 16)(9, 21, 25, 28)(11, 17, 26, 30, 15, 27)(12, 18, 13, 20)
(1, 3, 4, 4, 6, 6, 8)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16)(9, 21, 31, 26, 15, 27)(11, 17, 25, 23, 30, 14, 29, 22)(13, 20, 24, 28)
(1, 3, 4, 8, 8, 8)	(1, 2, 4, 3)(5, 8, 19, 14, 29, 12, 18, 10)(6, 7, 16)(9, 21, 28, 24, 13, 20, 30, 22)(11, 17, 26, 31, 15, 27, 23, 25)
(1, 3, 3, 4, 4, 5, 6, 6)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16, 13, 20)(9, 21, 25, 28)(11, 17, 26)(14, 29, 23, 30, 22, 24)(15, 27, 31)
(1, 4, 5, 6, 8, 8)	(1, 2, 4, 3)(5, 8, 19, 31, 23, 15, 27, 10)(6, 7, 16, 13, 20)(9, 21, 28, 25, 12, 18, 24, 22)(11, 17, 26, 30, 14, 29)
(1, 3, 3, 3, 3, 4, 4, 4, 7)	(1, 2, 4, 3)(5, 8, 19, 26, 9, 21, 10)(6, 7, 16)(11, 17, 27, 31)(12, 18, 15, 29)(13, 20, 24)(14, 22, 30)(23, 28, 25)
(1, 4, 4, 5, 7, 11)	(1, 2, 4, 3)(5, 8, 19, 24, 9, 21, 10)(6, 7, 16, 13, 20, 28, 25, 11, 17, 31, 22)(12, 18, 30, 26)(14, 29, 23, 15, 27)
(1, 4, 7, 20)	(1, 2, 4, 3)(5, 8, 19, 25, 28, 24, 14, 29, 15, 27, 23, 6, 7, 16, 13, 20, 12, 18, 26, 10)(9, 21, 30, 11, 17, 31, 22)
(1, 3, 3, 3, 3, 4, 4, 11)	(1, 2, 4, 3)(5, 8, 19, 14, 29, 15, 27, 30, 23, 31, 10)(6, 7, 16)(9, 21, 25)(11, 17, 26)(12, 18, 13, 20)(22, 28, 24)
(1, 4, 4, 4, 5, 6, 8)	(1, 2, 4, 3)(5, 8, 19, 23, 31, 9, 21, 10)(6, 7, 16, 13, 20, 30)(11, 17, 24, 22, 26)(12, 18, 25, 28)(14, 29, 15, 27)
(1, 3, 3, 6, 8, 11)	(0, 1, 2, 7, 22, 25, 23, 15, 18, 4, 6)(5, 12, 19, 31, 20, 30)(8, 26, 9, 29, 21, 24, 13, 17)(10, 14, 16)(11, 27, 28)
(1, 3, 3, 3, 3, 3, 3, 3, 7)	unknown
(1, 5, 7, 19)	(0, 28, 16, 26, 19)(1, 30, 15, 13, 9, 7, 8, 14, 11, 12, 25, 17, 5, 18, 2, 24, 21, 20, 23)(3, 29, 22, 4, 31, 6, 27)
(1, 3, 3, 5, 8, 12)	(0, 17, 9, 4, 18, 6, 22, 11)(1, 19, 28, 24, 7)(2, 21, 27, 23, 31, 26, 3, 16, 10, 20, 29, 8)(5, 25, 30)(12, 15, 13)
(1, 3, 3, 7, 9, 9)	(0, 30, 6, 31, 8, 5, 19)(1, 29, 26, 22, 3, 28, 20, 16, 21)(2, 24, 18, 27, 10, 17, 23, 7, 9)(4, 25, 11)(13, 14, 15)
(1, 6, 7, 18)	(0, 17, 24, 27, 4, 22, 14)(1, 18, 20, 31, 5, 28, 25, 7, 6, 16, 26, 29, 21, 8, 10, 30, 9, 13)(2, 23, 12, 3, 19, 15)
(1, 3, 3, 7, 8, 10)	(0, 28, 22, 3, 30, 4, 27, 9)(1, 31, 8, 7, 11, 6, 29, 24, 16, 23)(2, 26, 20, 18, 25, 10, 19)(5, 17, 21)(12, 14, 13)
(1, 3, 3, 4, 5, 5, 11)	(1, 2, 4, 3)(5, 8, 19, 26, 22, 30, 11, 17, 9, 21, 10)(6, 7, 16, 13, 20)(12, 18, 24, 14, 29)(15, 27, 31)(23, 28, 25)
(1, 3, 4, 4, 4, 5, 11)	(1, 2, 4, 3)(5, 8, 19, 24, 10)(6, 7, 16)(9, 21, 13, 20)(11, 17, 14, 29, 23, 31, 22, 26, 30, 15, 27)(12, 18, 28, 25)
(1, 4, 5, 6, 6, 10)	(1, 2, 4, 3)(5, 8, 19, 24, 28, 10)(6, 7, 16, 13, 20)(9, 21, 25, 12, 18, 26, 11, 17, 31, 22)(14, 29, 23, 15, 27, 30)
(1, 4, 4, 5, 8, 10)	(1, 2, 4, 3)(5, 8, 19, 24, 28, 12, 18, 10)(6, 7, 16, 13, 20)(9, 21, 25, 15, 27, 14, 29, 23, 30, 22)(11, 17, 31, 26)
(1, 3, 3, 3, 5, 5, 6, 6)	unknown
(1, 3, 3, 5, 5, 5, 5, 5)	unknown
(1, 3, 3, 4, 4, 17)	(1, 2, 4, 3)(5, 8, 19, 6, 7, 16, 13, 20, 11, 17, 31, 22, 28, 23, 15, 27, 10)(9, 21, 25)(12, 18, 26, 30)(14, 29, 24)
(1, 3, 3, 3, 3, 3, 16)	(0, 11, 26, 31, 13, 22, 17, 18, 4, 8, 24, 5, 3, 10, 14, 20)(1, 9, 30)(2, 15, 23)(6, 12, 21)(7, 27, 25)(19, 28, 29)
(1, 3, 5, 5, 8, 10)	(1, 2, 3)(4, 8, 16, 23, 28, 15, 29, 24, 12, 25)(5, 10, 22, 30, 26, 13, 19, 21)(6, 11, 20, 14, 31)(7, 9, 18, 27, 17)
(1, 4, 4, 5, 5, 13)	(1, 2, 4, 3)(5, 8, 19, 24, 10)(6, 7, 16, 15, 27)(9, 21, 28, 25, 23, 31, 14, 29, 13, 20, 30, 11, 17)(12, 18, 22, 26)
(1, 3, 8, 9, 11)	(0, 25, 13, 9, 5, 20, 1, 26, 23)(2, 31, 15, 10, 22, 21, 6, 24, 7, 14, 8)(3, 27, 16, 18, 4, 30, 12, 11)(19, 29, 28)
(1, 3, 3, 3, 3, 9, 10)	(0, 11, 26, 25, 4, 8, 24, 31, 13, 22)(1, 9, 30)(2, 15, 23)(3, 10, 14, 20, 17, 19, 7, 27, 5)(6, 12, 21)(18, 28, 29)
(1, 14, 17)	(0, 18, 15, 1, 17, 26, 28, 24, 4, 21, 13, 2, 20, 10, 29, 23, 12)(3, 16, 25, 6, 19, 22, 30, 7, 5, 31, 11, 8, 9, 14)
(1, 3, 3, 3, 3, 3, 3, 3, 5, 5)	unknown
(1, 4, 4, 4, 5, 5, 9)	(1, 2, 4, 3)(5, 8, 19, 23, 15, 26, 22, 30, 10)(6, 7, 16, 27)(9, 21, 28, 25)(11, 17, 31, 13, 20)(12, 18, 24, 14, 29)
(1, 4, 4, 5, 5, 6, 7)	(1, 2, 4, 3)(5, 8, 19, 31, 9, 21, 10)(6, 7, 16, 13, 20)(11, 17, 24, 22, 30, 26)(12, 18, 25, 28)(14, 29, 23, 15, 27)
(1, 5, 6, 7, 13)	(0, 4, 7, 20, 30, 2)(1, 6, 3, 5, 12, 26, 18, 19, 8, 23, 14, 27, 10)(9, 17, 28, 16, 31, 13, 25)(11, 21, 15, 24, 22)
(1, 3, 4, 6, 18)	(1, 2, 4, 3)(5, 8, 19, 26, 12, 18, 24, 28, 23, 6, 7, 16, 13, 20, 11, 17, 31, 10)(9, 21, 25)(14, 29, 15, 27, 30, 22)
(1, 3, 3, 3, 4, 4, 4, 4, 6)	(1, 2, 4, 3)(5, 8, 19, 31, 23, 10)(6, 7, 16)(9, 21, 27)(11, 17, 24)(12, 18, 13, 20)(14, 26, 15, 30)(22, 29, 25, 28)
(1, 4, 6, 6, 15)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16, 13, 20, 26, 31, 22, 28, 24, 14, 29, 15, 27, 23)(9, 21, 30, 11, 17, 25)
(1, 4, 5, 9, 13)	(1, 2, 4, 3)(5, 8, 19, 24, 29, 23, 27, 31, 10)(6, 7, 16, 13, 20, 26, 11, 17, 14, 22, 30, 12, 18)(9, 21, 28, 15, 25)
(1, 3, 3, 3, 8, 14)	(0, 16, 27, 5, 29, 20, 30, 8, 11, 10, 31, 4, 23, 13)(1, 19, 14)(2, 22, 15, 3, 18, 21, 9, 12)(6, 17, 25)(24, 28, 26)
(1, 7, 7, 8, 9)	unknown
(1, 3, 4, 5, 5, 14)	(1, 2, 4, 3)(5, 8, 19, 26, 10)(6, 7, 16, 15, 27)(9, 21, 31, 13, 20, 24, 14, 29, 12, 18, 22, 30, 11, 17)(23, 28, 25)

Continued on next page

Cycle Types	Orthomorphism
(1, 4, 4, 7, 16)	(1, 2, 4, 3)(5, 8, 19, 24, 14, 29, 25, 12, 18, 30, 23, 15, 27, 9, 21, 10)(6, 7, 16, 13, 20, 28, 22)(11, 17, 31, 26)
(1, 3, 3, 3, 7, 7, 8)	(1, 2, 3)(4, 8, 16, 23, 28, 12, 25)(5, 10, 22, 15, 29, 7, 9, 18)(6, 11, 20, 30, 24, 17, 21)(13, 19, 27)(14, 31, 26)
(1, 4, 5, 5, 5, 6, 6)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 10)(6, 7, 16, 13, 20)(9, 21, 31, 23, 28)(11, 17, 24, 22, 26)(14, 29, 25, 15, 27, 30)
(1, 3, 4, 4, 7, 13)	(1, 2, 4, 3)(5, 8, 19, 31, 9, 21, 10)(6, 7, 16, 13, 20, 28, 14, 29, 25, 12, 18, 24, 22)(11, 17, 26)(15, 27, 30, 23)
(1, 3, 3, 4, 5, 7, 9)	(1, 2, 4, 3)(5, 8, 19, 25, 28, 24, 9, 21, 10)(6, 7, 16, 13, 20)(11, 17, 31, 15, 27, 23, 30)(12, 18, 26)(14, 29, 22)
(1, 3, 3, 5, 5, 15)	(0, 3, 1)(2, 5, 14, 18, 6)(7, 20, 13, 19, 29)(8, 24, 9, 31, 21, 28, 11, 25, 22, 30, 27, 23, 26, 15, 16)(10, 12, 17)
(1, 3, 3, 3, 3, 5, 7, 7)	(1, 2, 3)(4, 8, 16)(5, 10, 24, 18, 13, 26, 30)(6, 11, 22, 17, 20, 14, 23)(7, 12, 31, 15, 25)(9, 28, 21)(19, 27, 29)
(1, 5, 5, 9, 12)	unknown
(1, 4, 6, 21)	(1, 2, 4, 3)(5, 8, 19, 25, 12, 18, 26, 22, 6, 7, 16, 13, 20, 11, 17, 31, 14, 29, 24, 28, 10)(9, 21, 30, 23, 15, 27)
(1, 6, 6, 19)	(0, 23, 14, 6, 22, 25, 8, 12, 5, 26, 27, 30, 29, 3, 21, 9, 11, 13, 7)(1, 20, 15, 4, 16, 28)(2, 17, 31, 18, 10, 24)
(1, 4, 8, 9, 10)	(1, 2, 4, 3)(5, 8, 19, 25, 11, 17, 31, 9, 21, 10)(6, 7, 16, 13, 20, 12, 18, 26, 22)(14, 29, 24, 28, 23, 30, 15, 27)
(1, 3, 4, 4, 10, 10)	(1, 2, 4, 3)(5, 8, 19, 11, 17, 26, 31, 15, 27, 10)(6, 7, 16, 13, 20, 24, 14, 29, 23, 25)(9, 21, 28)(12, 18, 22, 30)
(1, 3, 3, 3, 3, 3, 8, 8)	(1, 2, 3)(4, 8, 16)(5, 10, 25, 29, 26, 19, 9, 28)(6, 11, 20)(7, 12, 27, 13, 17, 15, 18, 23)(14, 21, 31)(22, 30, 24)
(1, 3, 3, 3, 3, 3, 5, 5, 6)	unknown
(1, 4, 5, 7, 15)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 26, 10)(6, 7, 16, 13, 20, 30, 11, 17, 31, 22, 14, 29, 24, 28, 23)(9, 21, 25, 15, 27)
(1, 3, 3, 5, 6, 14)	(0, 16, 11, 1, 18, 7)(2, 20, 25, 22, 10, 21, 28, 26, 4, 19, 29, 9, 5, 24)(3, 17, 8)(6, 23, 31, 27, 30)(12, 14, 15)
(1, 3, 4, 4, 5, 15)	(1, 2, 4, 3)(5, 8, 19, 12, 18, 24, 14, 29, 22, 30, 26, 11, 17, 31, 10)(6, 7, 16, 13, 20)(9, 21, 28, 25)(15, 27, 23)
(1, 3, 3, 8, 8, 9)	(1, 2, 3)(4, 8, 16, 13, 23, 18, 24, 31)(5, 10, 25, 17, 15, 22, 7, 12, 19)(6, 11, 28, 9, 21, 27, 29, 20)(14, 26, 30)
(1, 3, 3, 3, 3, 4, 6, 9)	(1, 2, 4, 3)(5, 8, 19, 14, 29, 23, 15, 27, 10)(6, 7, 16)(9, 21, 30, 26, 31, 22)(11, 17, 25)(12, 18, 28)(13, 20, 24)
(1, 4, 8, 8, 11)	(1, 2, 4, 3)(5, 8, 19, 26, 12, 18, 24, 10)(6, 7, 16, 13, 20, 11, 17, 31, 15, 27, 23)(9, 21, 30, 22, 14, 29, 25, 28)
(1, 7, 8, 16)	(0, 20, 24, 25, 18, 27, 6, 19, 3, 21, 31, 14, 11, 5, 28, 30)(1, 22, 12, 10, 17, 13, 9)(2, 16, 15, 8, 7, 4, 23, 26)
(1, 5, 5, 5, 5, 11)	unknown
(1, 6, 7, 7, 11)	(1, 2, 30, 26, 15, 31)(3, 18, 24, 20, 12, 13, 10)(4, 16, 9, 11, 28, 19, 22)(5, 14, 21, 6, 27, 29, 7, 17, 25, 23, 8)
(1, 3, 3, 3, 3, 4, 5, 10)	(1, 2, 4, 3)(5, 8, 19, 14, 29, 25, 28, 9, 21, 10)(6, 7, 16)(11, 17, 27)(12, 18, 26, 22, 24)(13, 20, 31)(15, 23, 30)
(1, 3, 3, 10, 15)	(0, 23, 29, 14, 8, 4, 20, 13, 10, 18)(1, 21, 28)(2, 19, 27, 25, 26, 5, 31, 30, 17, 15, 11, 6, 16, 12, 9)(3, 22, 24)
(1, 4, 9, 9, 9)	(1, 2, 4, 3)(5, 8, 19, 6, 7, 16, 15, 27, 10)(9, 21, 25, 28, 23, 31, 22, 11, 17)(12, 18, 24, 14, 29, 13, 20, 26, 30)
(1, 3, 3, 4, 7, 7, 7)	(1, 2, 4, 3)(5, 8, 19, 26, 12, 18, 10)(6, 7, 16, 13, 20, 31, 23)(9, 21, 25)(11, 17, 14, 29, 15, 27, 30)(22, 28, 24)
(1, 3, 3, 3, 3, 6, 13)	(0, 16, 11, 1, 18, 7)(2, 20, 10, 21, 27, 30, 22, 31, 25, 29, 9, 5, 24)(3, 17, 8)(4, 19, 28)(6, 23, 26)(12, 14, 15)
(1, 3, 5, 5, 6, 6, 6)	(0, 1, 3)(2, 5, 9, 20, 10, 4)(7, 17, 25, 14, 30, 27)(8, 18, 22, 15, 29)(11, 16, 26, 19, 12, 31)(13, 28, 23, 24, 21)
(1, 5, 6, 10, 10)	(1, 2, 10, 27, 29, 7, 17, 26, 15, 5)(3, 30, 14, 21, 6)(4, 13, 25, 23, 8, 22)(9, 11, 28, 19, 18, 31, 24, 20, 12, 16)
(1, 3, 5, 7, 8, 8)	(1, 2, 3)(4, 8, 16, 7, 12, 21, 31, 17)(5, 10, 22, 13, 25, 6, 11, 27)(9, 20, 29, 26, 18, 23, 19)(14, 28, 15, 30, 24)
(1, 3, 4, 9, 15)	(1, 2, 4, 3)(5, 8, 19, 24, 9, 21, 29, 23, 27, 11, 17, 14, 22, 31, 10)(6, 7, 16, 13, 20, 26, 30, 12, 18)(15, 25, 28)
(1, 3, 3, 3, 4, 4, 4, 5, 5)	(1, 2, 4, 3)(5, 8, 19, 23, 10)(6, 7, 16, 25)(9, 21, 13, 20, 24)(11, 17, 31)(12, 18, 26)(14, 27, 30)(15, 29, 22, 28)
(1, 3, 6, 22)	(31)(0, 16, 8, 4, 2, 1)(3, 17, 24, 12, 6, 19, 9, 20, 10, 21, 26, 29, 14, 23, 11, 5, 18, 25, 28, 30, 15, 7)(13, 22, 27)
(1, 4, 12, 15)	(31)(0, 16, 24, 12, 22, 27, 13, 6, 19, 25, 28, 14, 7, 3, 1)(2, 17, 8, 4)(5, 18, 9, 20, 26, 29, 30, 15, 23, 11, 21, 10)
(1, 3, 4, 24)	(1, 16, 24, 12, 6, 19, 9, 20, 26, 29, 30, 31, 15, 23, 11, 21, 10, 5, 18, 25, 28, 14, 7, 3)(2, 17, 8, 4)(13, 22, 27)
(1, 3, 7, 21)	(1, 16, 24, 28, 30, 31, 15, 23, 11, 21, 10, 5, 18, 25, 12, 6, 3, 17, 8, 4, 2)(7, 19, 9, 20, 26, 29, 14)(13, 22, 27)
(1, 4, 13, 14)	(1, 16, 24, 28, 30, 31, 15, 20, 26, 29, 14, 4, 2)(3, 17, 8, 7, 19, 9, 23, 11, 22, 27, 13, 21, 10, 6)(5, 18, 25, 12)
(1, 3, 5, 23)	(1, 16, 8, 4, 2)(3, 17, 24, 12, 6, 19, 9, 20, 10, 21, 26, 29, 14, 23, 11, 5, 18, 25, 28, 30, 31, 15, 7)(13, 22, 27)
(1, 3, 8, 20)	(31)(0, 16, 8, 4, 2, 17, 24, 28, 14, 23, 11, 21, 10, 5, 18, 25, 12, 6, 3, 1)(7, 19, 9, 20, 26, 29, 30, 15)(13, 22, 27)
(1, 3, 11, 17)	(31)(0, 16, 8, 20, 10, 21, 26, 13, 6, 3, 1)(2, 17, 24, 28, 14, 23, 27, 29, 30, 15, 7, 19, 25, 12, 22, 11, 5)(4, 18, 9)
(1, 5, 11, 15)	(1, 16, 8, 4, 2)(3, 17, 24, 12, 22, 27, 13, 6, 19, 25, 28, 30, 31, 15, 7)(5, 18, 9, 20, 26, 29, 14, 23, 11, 21, 10)
(1, 3, 9, 19)	(1, 16, 24, 28, 30, 31, 15, 23, 11, 5, 18, 25, 12, 6, 3, 17, 8, 4, 2)(7, 19, 9, 20, 10, 21, 26, 29, 14)(13, 22, 27)
(1, 9, 10, 12)	(1, 16, 24, 12, 6, 19, 9, 4, 2)(3, 17, 8, 20, 10, 21, 26, 29, 14, 7)(5, 18, 25, 28, 30, 31, 15, 23, 27, 13, 22, 11)
(1, 8, 10, 13)	(1, 16, 24, 28, 30, 31, 15, 23, 11, 21, 10, 5, 2)(3, 17, 8, 4, 18, 25, 12, 6)(7, 19, 9, 20, 26, 13, 22, 27, 29, 14)

Continued on next page

Cycle Types	Orthomorphism
(1, 10, 10, 11)	(1, 16, 8, 4, 18, 9, 20, 26, 13, 6, 3)(2, 17, 24, 28, 14, 23, 11, 21, 10, 5)(7, 19, 25, 12, 22, 27, 29, 30, 31, 15)
(1, 8, 11, 12)	(1, 16, 24, 31, 12, 6, 3, 17, 8, 4, 2)(5, 18, 25, 15, 23, 11, 21, 10)(7, 19, 9, 20, 26, 30, 28, 29, 13, 22, 27, 14)
(1, 6, 11, 14)	(31)(0, 16, 8, 4, 2, 1)(3, 17, 24, 28, 30, 15, 7, 19, 25, 12, 22, 27, 13, 6)(5, 18, 9, 20, 26, 29, 14, 23, 11, 21, 10)
(1, 8, 9, 14)	(1, 16, 24, 12, 6, 19, 9, 4, 2)(3, 17, 8, 20, 26, 29, 14, 7)(5, 18, 25, 28, 30, 31, 15, 23, 27, 13, 22, 11, 21, 10)
(1, 3, 10, 18)	(31)(0, 16, 24, 12, 6, 19, 9, 20, 26, 29, 14, 7, 3, 17, 8, 4, 2, 1)(5, 18, 25, 28, 30, 15, 23, 11, 21, 10)(13, 22, 27)
(1, 31)	(1, 16, 8, 4, 18, 9, 20, 26, 13, 6, 19, 25, 28, 30, 31, 15, 7, 3, 17, 24, 12, 22, 27, 29, 14, 23, 11, 21, 10, 5, 2)

Cycle-types and examples of orthomorphisms of  $\mathbb{Z}_2^5$ .