2007

Mutually orthogonal latin squares based on Z_3x Z_9

James Michael Carter
Wright State University

Mutually othogonal latin squares based on the group $\mathbb{Z}_3 \times \mathbb{Z}_9$

July 27, 2007

A thesis submitted for the partial fullfilment of the requirements for the degree of Master of Science

By

James Michael Carter

B.S., University of Pittsburgh, 2004

Wright State University

WRIGHT STATE UNIVERSITY

SCHOOL OF GRADUATE STUDIES

July 26, 2007

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY James Michael Carter ENTITLED Mutually orthogonal latins squares based on the group $\mathbb{Z}_3 \times \mathbb{Z}_9$ BE ACCEPTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Science

Anthony Evans, Ph.D.

Thesis Director

Joanne Dombrowski, Ph.D.

Department Chair

Comittee on Final Examination

Anthony Evans, Ph.D.

Qingbo Huang, Ph.D.

Joanne Dombrowski, Ph.D.

Lop-fat Ho, Ph.D.

Joseph F. Thomas, Jr., Ph.D.

Dean, School of Graduate Studies

Abstract

Carter, James Michael. M.S., Department of Mathematics and Statistics, Wright State University, 2007. Mutually Orthogonal Latin Squares Based On $\mathbb{Z}_3 \times \mathbb{Z}_9$.

This paper will investigate the number of mutually orthogonal latin squares, MOLS, that can be constructed using elements from the group $G = \mathbb{Z}_3 \times \mathbb{Z}_9$. In calculating this number, it is necessary to consider the group under the action of the homomorphism $f : G \to K$ defined by $f((g_1, g_2)) = (g_1 \bmod 3, g_2 \bmod 3)$ so that $K = Im(G) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, so that the action of f is to create the quotient group $K = G/\langle(0,3)\rangle$. Based on data from the group $\mathbb{Z}_2 \times \mathbb{Z}_4$, the elements of the image should be permuted and constants added before considering $G' = f^{-1}(K)$. The use of orthomorphisms will allow for the construction of orthogonal latin squares.

Contents

List of Tables

Table 1: $\mathcal{A}_1$ data

z	00	10	01	11	02	12	03	13
α_1	00	13	11	02	03	10	12	01
α_2	00	03	12	13	01	02	11	10
α_3	00	01	13	12	11	10	02	03
α_4	00	11	10	03	13	02	01	12

Table 2: $\mathcal{A}_1'$ data

	a	b	c	d	A	B	C	D
z	00	10	01	11	00	10	01	11
α_1	00	11	11	00	01	10	10	01
α_2	00	01	10	01	01	00	11	10

Table 3: reorganized $\mathcal{A}_1'$ data

00	10	01	11	00	10	01	11
00	11	10	01	01	10	11	00
00	01	11	10	01	00	10	01

Table 4: σ values from $\mathcal{A}_1$ data

z	0	1	σ	σ^2	0	1	σ
α_1	0	σ^2	1	σ	σ	1	σ^2
α_2	0	σ	σ^2	1	σ	0	1

Table 5: Condensed σ table

	z	z
α_1	$\sigma^2 z$	$\sigma^2 z + \sigma$
α_2	σz	$\sigma z + \sigma$

Table 6: Known values of ω

G	$\lvert G\rvert$	$\omega(G)$
$\mathbb{Z}_3$	3	1
$\mathbb{Z}_5$	5	3
$\mathbb{Z}_7$	7	5
$\mathbb{Z}_9$	9	1
$\mathbb{Z}_{11}$	11	9
$\mathbb{Z}_{13}$	13	11
$\mathbb{Z}_{15}$	15	3

G	$\lvert G\rvert$	$\omega(G)$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	4	2
$\mathbb{Z}_2 \times \mathbb{Z}_4$	8	2
D_4	8	1
Q_4	8	1
F_8^+	8	6
F_9^+	9	7
$\mathbb{Z}_2 \times \mathbb{Z}_6$	12	4
D_6	12	2
A_4	12	1

Table 7: multiplication of $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong GF(4)^+$

$*$	00	10	01	11
00	00	10	01	11
10		00	11	01
01			00	10
11				00

Table 8: multiplication of $\mathbb{Z}_3 \times \mathbb{Z}_3 \cong GF(9)^+$

$*$	00	10	01	11	20	02	12	21	22
00	00	10	01	11	20	02	12	21	22
10		20	11	21	00	12	22	01	02
01			02	12	21	00	10	22	20
11				22	01	10	20	01	00
20					10	22	02	11	12
02						01	11	20	21
12							21	00	01
21								12	10
22									11

Table 9: powers of σ for $GF(4)^+$

n	σ^n
1	σ
2	$1+\sigma$
3	1

Table 10: powers of σ for $GF(9)^+$

n	1	2	3	4	5	6	7	8
σ^n	σ	$1+2\sigma$	$2+2\sigma$	2	2σ	$2+\sigma$	$1+\sigma$	1
	$1+i$	$2i$	$1+2i$	2	$2+2i$	i	$2+i$	1

Table 11: Other data

z	00	10	01	11	02	12	03	13
β_2	00	02	12	10	11	13	01	03
β_4	00	02	10	12	01	03	13	11
γ_1	00	11	10	13	12	03	02	01
γ_3	00	13	02	03	12	01	10	11

1 Introduction

An *orthomorphism* is a permutation, θ, operating on a group, G, such that the mapping $f_1 : x \mapsto x^{-1}\theta(x)$ is also a permutation. Two orthomorphisms θ, ϕ are *orthogonal* if the mapping $f_2 : x \mapsto \theta^{-1}(x)\phi(x)$ is a permutation of G. Orthogonality is a symmetric property as shown by the calculations:

Let

$$f_3(x) = x^{-1}$$

so since the composition of two permutations is again a permutation and both f_2 and f_3 are permutations, then

$$(f_3 \circ f_2)(x) = (\theta^{-1}(x)\phi(x))^{-1} = \phi^{-1}(x)\theta(x)$$

is also a permutation and therefore orthogonality is a symmetric property as claimed. Denote by $Orth(G) = \{\theta : \theta \text{ is an orthomorphism of } G\}$ the set of orthomorphisms of a group G as well as the graph whose vertices are the orthomorphisms of G such that there is an edge between two vertices if and only if they are orthogonal. Note that orthogonality and adjacency are equivalent in this graph. An *r-clique* will be a set of r mutually adjacent orthomorphsims in $Orth(G)$. So that the *clique number* of $Orth(G), \omega(Orth(G))$, is the largest value of r for which the graph has an r-clique. The value of the clique number is known for only very few classes of groups. Some known results will be presented and a theoretic procedure for improving the lower bound for clique number for $G_0 = \mathbb{Z}_3 \times \mathbb{Z}_9$ will be discussed. A *latin square of order n* with elements from G is defined to be an $n \times n$ matrix in which each of the elements of the group $G = \{g_1, \ldots, g_n\}$ appears exactly once in each row and exactly once in each column. This obviously implies that each row and each column is a permutation of the elements $\{g_1, \ldots, g_n\}$.

It has been shown that the addition or multiplication table of a group is a latin square since it is defined such that the ij entry of the square is $g_i g_j$, the product of the i^{th} and j^{th} elements of the group. The fact that this is a latin square follows from the cancellation properties groups. Two latin squares, $L = \{l_{ij}\}$ and $L' = \{l'_{ij}\}$, are said to be *orthogonal* if for each symbol a in the symbol set of L and each b in the symbol set of L' there exists a unique pair ij for which $l_{ij} = a$ and $l'_{ij} = b$. Thus if the two squares are superimposed on each other, the ordered pair (a, b) appears exactly one time.

Theorem 1.1 *If $G = \{g_1, g_2, \ldots, g_n\}$ is a group, then the matrix $L = \{l_{ij}\} = \{g_i \cdot g_j\}$ is a latin square called the Cayley table of G and denoted $\mathcal{C}_G$*

Mutually orthogonal orthomorphisms can be used to construct mutually orthogonal latin squares (MOLS) from the Cayley table of a given group. Let $\mathcal{C}_G$ be the Cayley table of the group G. Then a set of $\omega(Orth(G))+1$ MOLS can be constructed. Let θ_k, $1 \leq k \leq \omega$ be an ω-clique of $Orth(G)$. If $M_k, 1 \leq k \leq \omega$ are all latin squares in which M_k is constructed by letting θ_k permute the columns of $\mathcal{C}_G$. By defining $M_0 = \mathcal{C}_G$, this gives a set of $\omega + 1$ MOLS of order $|G|$. The functions θ_k are mutually orthogonal, so the ω-clique is a complete induced subgraph of $Orth(G)$. To prove this, consider θ_1, θ_2 and let $a = x^{-1}\theta_1(y)$ and $b = x^{-1}\theta_2(y)$ and compute $a^{-1}b = (\theta_1(y))^{-1}(x^{-1})^{-1}x^{-1}\theta_2(y) = (\theta_1(y))^{-1}\theta_2(y)$ which uniquely determines y from a and b and thus x from y is also unique. Similarly, each of the θ_k is orthogonal to every other function in the set.

A square L_f with entries given by $g_i \cdot f(g_j)$ is related to $\mathcal{C}_G$ and is a latin square if and only if f is a permutation and it is orthogonal to $\mathcal{C}_G$ if and only if f is an orthomorphsim. Also two orthomorphisms are orthogonal if and only if their corresponding latin squares are orthogonal. This construction is exemplified below using the Cayley table, $\mathcal{C}_G$, and using α_1 and α_2 from Table 1.

00	10	01	11	02	12	03	13
10	00	11	01	12	02	13	03
01	11	02	12	03	03	00	10
11	01	12	02	13	03	10	00
02	12	03	13	00	10	01	11
12	02	13	03	10	00	11	01
03	13	00	10	01	11	02	12
13	03	10	00	11	01	12	02

00	13	11	02	03	10	12	01
10	03	01	12	13	00	02	11
01	10	12	03	00	11	03	02
11	00	02	13	10	01	03	12
02	11	13	00	01	12	10	03
12	01	03	10	11	02	00	13
03	12	10	01	02	13	11	00
13	02	00	11	12	03	01	10

00	03	12	13	01	02	11	10
10	13	02	03	11	12	01	00
01	00	03	10	02	03	12	11
11	10	03	00	12	13	02	01
02	01	10	11	03	00	13	12
12	11	00	01	13	10	03	02
03	02	11	12	00	01	10	13
13	12	01	02	10	11	00	03

Each column of the Cayley table appears in each of these two new squares, but the order in which they appear is altered according to the action of α_i on the elements in the first row of the Cayley table. These two squares are orthogonal latin squares by construction or by tedious inspection. Also, both of them are orthogonal to the Cayley table upon which they are based, so taken as a triplet these form a set of MOLS for the group $\mathbb{Z}_2 \times \mathbb{Z}_4$.

2 Known Results

In [2], many results are presented. Some of the more useful include

Theorem 2.1 *If G is non-trivial, then $\omega(Orth(G)) \leq |G| - 2$*

When there is equality above, the set of vertices in the ω-clique is called a *complete set* of orthomorphisms of G. This gives an upper bound, but it is not particularly practical. Another useful result is

Theorem 2.2 $\omega(Orth(G \times G')) \geq min\{\omega(Orth(G), \omega(Orth(G')\}$

This will give a lower bound for $\omega(Orth(G_0))$.

Using these two results, it can be shown that a bounded range for the value of $\omega(G_0)$ is $1 \leq \omega \leq 25$ since according to [4], $\omega(\mathbb{Z}_3) = \omega(\mathbb{Z}_9) = 1$ and $|\mathbb{Z}_3 \times \mathbb{Z}_9| = 27$.

Two open conjectures about the bounds for ω are:

1. The bound in Theorem 2.1 cannot be attained if $|G|$ is not a power of a prime.

2. The bound in Theorem 2.1 cannot be attained if G is not elementary abelian.

Andrew Bowler proved in [3] that for $n \equiv 1, 5 \pmod 6$ the dihedral group, D_{4n}, of order $4n$ admits a pair of orthogonal orthomorphisms. That is $\omega(D_{4n}) \geq 2$. Other conclusions include that $\omega(D_{2n}) = 0$ if n is odd, $\omega(D_4) = 2, \omega(D_8) = 1$,and $\omega(D_{12}) = 2$. In general, if $m = 2n$ is even, then $\omega(D_{2m}) \geq 1$.

In [1], some results for linear groups are improved as well as results for $\mathbb{Z}_m$ where $m > 3$ and not divisible by 9. This paper indicates that $\omega(D_{8m}) \geq 3$. If m is not divisible by 9. Another result is that if $q > 8$ is even and neither $q \pm 1$ are dvisible by 9, then $\omega(GL(2, q)) \geq 3$ and $\omega(SL(2, q)) \geq 3$. In the paper [5] the lower bound for the group $\mathbb{Z}_3 \times \mathbb{Z}_9$ of order 27 can be established as 1.

2.1 Classes of orthomorphisms

Some examples of classes of functions that may be orthomorphisms include the mappings of the form $f_a := z \mapsto az$ for some fixed $a \in G$ where G is the additive group of a finite field. For example, if $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \cong GF(4)^+ = \{x + \sigma y : x, y \in \mathbb{Z}_2, \sigma^2 + \sigma + 1 = 0\}$ then $f_\sigma(z) = \sigma \cdot z$. The isomorphism is chosen based on the

polynomial $x^2 + x + 1$ which is irreducible over the field $GF(2)$. In this case, the formula $\sigma^2 = 1 + \sigma$ will be used as a reduction formula to condense entries in Table 3 to the single elements found in Table 4. By examining the Table 4, an explicit function $f(z)$ can be found that can be used to further simplify the table into 5.

As another example, if $G = \mathbb{Z}_3 \times \mathbb{Z}_3 \cong GF(9)^+ = \{x+iy : x, y \in \mathbb{Z}_3, i^2 = 2\}$. The function $f_\sigma(z) = \sigma \cdot z$ becomes multiplication of the group elements by $\sigma = 1 + i$. Here the isomorphism can also be written as $GF(9)^+ \cong \{x + \sigma y : \sigma^2 + \sigma + 2 = 0, x, y \in \mathbb{Z}_3\}$ where the irreducible polynomial used is $x^2 + x + 2$. In this case, it can be seen that $\sigma^2 = 1 + 2\sigma$ will be used as a reduction formula to generate the powers of σ found in Table 10. In this table, the third row is derived from noting the action of σ^6, so that $\sigma = 1 + i$ and $\langle\sigma\rangle = \langle 1 + i\rangle = GF(9)^\times$ is clearly an appropriate generator. In both cases, the field is generated by the element σ, a root of the appropriate irreducible polynomial

The functions f_a contains a complete set of orthomorphsims for an elementary abelian group when considered as the set $\{f_a : a \in G, a \neq 0, 1\}$ since this is a set of $|G| - 2$ mutually orthogonal orthomorphisms. The group G is finite so that the order of the group is well defined. These functions are clearly permutations since they are easily shown to be injective and in the finite setting this implies they are also surjective and therefore bijective. Two of these functions f_a, f_b are seen to be either orthogonal if $a \neq b$ or else identical. Those functions where $a \neq 0, 1$ are called linear orthomorphisms.

This particular class of functions is especially useful when dealing with elementary abelian groups where the group operation is addition. Both of these examples can be generalized to functions of the form $f_{a,b} := x \mapsto ax + b$.

Another class of functions is given by $f_r := x \mapsto x^r$. With some restrictions on the value of r, namely that $(r, n) = (r - 1, n) = 1$, it is possible to form sets

of orthomorphisms $\{f_r : (r,n) = (r-1,n) = 1\}$ and $n = |G|$. If the restrictions are relaxed to only include $(r,n) = 1$, then the set of functions $\{f_r\}$ form a set of permutations of G. If the restriction imposed on two functions, f_r, f_s, is $(s-r,n) = 1$, then the functions are orthogonal. Those functions which satisfy both of the conditions above form the class of power orthomorphisms. By a theorem in [2], it can be shown that if $\mathcal{P}(G) = \{f_r : f_r \in Orth(G)\}$ then $\omega(\mathcal{P}(\mathbb{Z}_3 \times \mathbb{Z}_9)) = 3 - 2 = 1$ since the group has order 27 and 3 is the smallest prime dividing the order .

3 Groups of order 8

Theorem 3.1 *Hall and Paige(1955). A finite group admits no orthomorphisms if its Sylow 2-subgroup is non-trivial and cyclic.*

There are 5 non-isomorphic groups of order 8: $\mathbb{Z}_8, Q_8, D_8, \mathbb{Z}_2 \times \mathbb{Z}_4$, and $GF(8)^+$. By Theorem 3.1, $\mathbb{Z}_8$ has no orthomorphisms and in [6] Chang and Tai showed that both Q_8 and D_8 have 48 orthomorphisms though no two are adjacent. However, it is interesting to note that $\mathbb{Z}_2 \times \mathbb{Z}_4$ and $GF(8)^+$ both have 48 orthomorphisms but each has different adjacency relations and different values of ω. In [4], values of ω are presented for groups up to order 23 and it can be seen that $\omega(\mathbb{Z}_2 \times \mathbb{Z}_4) = 2$ and $\omega(GF(8)^+) = 6$.

The 48 orthomorphisms of the group $\mathbb{Z}_2 \times \mathbb{Z}_4$ can be partitioned into 12 4-cycles [2]. Twenty-four of these are presented in [2], in 6 groups, denoted $\mathcal{A}_k$, of 4 orthomorphisms each. Those not listed can be found using automorphisms of $Orth(G)$. In each $\mathcal{A}_k$ the orthomorphisms are labeled with a greek letter and subscripts between 1 and 4, thus $\mathcal{A}_1 = \{\alpha_i : 1 \leq i \leq 4\}, \mathcal{A}_2 = \{\beta_i : 1 \leq i \leq 4\}$, etc. It should be noted that $\alpha_i \perp \alpha_j \Leftrightarrow i - j \equiv \pm 1 \bmod 4$ and that since orthogonality is the property of interest, the pairs (α_i, α_j) such that $i - j \equiv$

$\pm 1 \bmod 4$ should be considered. For simplicity, choose $k = 1, i = 1, j = 2$. Note that the enty $xy = (x, y)$ where $x \in \mathbb{Z}_2, y \in \mathbb{Z}_4$.

There are also 48 orthomorphisms of $GF(8)^+$ which can be determined using the following from [2]

Theorem 3.2 *The degree of an orthomorphism or complete mapping polynomial, reduced modulo $x^q - x$ is at most $q - 3, q > 2$.*

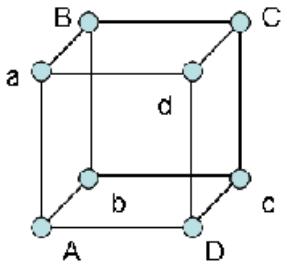
These are found by listing all orthomorphism polynomials of degree at most 5 since here $q = 8$ and $q - 3 = 8 - 3 = 5$. The maximal cliques of this group have been found to have sized 2 and 6 by Jungnickel and Grams in 1986. This can also be realized by noting that all of the 48 orthomorphisms are elements of the set of automorphisms of the group $GF(8)^+$ and that they are precisely the elements in this group of order 7 with the 6-cliques formed from the set of non-identity elements of each of the 8 Sylow 7-subgroups. Since ω is defined to be the largest value of clique size for all possible subgraphs, it is defined to be 6 for this group rather than 2.

4 $G_0 = \mathbb{Z}_3 \times \mathbb{Z}_9$

In order to study $\mathbb{Z}_3 \times \mathbb{Z}_9$, the data for $\mathbb{Z}_2 \times \mathbb{Z}_4$ should be considered. It is presented in [2] and reproduced in part in Table 1. It is simpler to consider the homomorphic image under a specific function, since this will be a group of smaller order. In general, the function is $\Pi : \mathbb{Z}_p \times \mathbb{Z}_{p^n} \to \mathbb{Z}_p \times \mathbb{Z}_p$ given by $\Pi(x, y) = (x, y \bmod p)$ with kernel $K = \langle (0, p) \rangle$. First consider the data for a subset $\mathcal{A}_1' \subset \mathcal{A}_1 \subset Orth(\mathbb{Z}_2 \times \mathbb{Z}_4)$ under the function Π as presented in Table 2. By using Table 2, a conflict graph can be constructed by connecting two vertices, z values from Table 2, if in a given row the same point from

$Im(G)$ appears in both columns. For example, the column $d = 11$ is adjacent to columns $D = 11, a = 00$, and $A = 01$ since in the first row the value 11 appears in columns d and D, and in the second row the value 00 appears in columns a and d, and in the third row the value 01 appears in columns d and A.

Figure 1: conflict graph



Since this graph can be drawn as a cube, the vertices can be partitioned into two sets of non-conflicting vertices $\{a, b, C, D\}, \{A, B, c, d\}$. Since $Im(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong GF(4)^+$, the additive group of a field of order 4, if $GF(4)^+ = \{i+\sigma j : \sigma^2+\sigma+1 = 0\}$ then each element of $Im(G)$ can be assigned a value $ij = (i, j)$. Now Table 2 becomes Table 4 which can further be simplified to Table 5 where z represents all of the group elements.

Any graph drawn in this manner based on the data in [2] will be such that all vertices have degree 3, though not all graphs can be partitioned in a convenient way. The following figures illustrate the other two types of conflict graphs that can arise from this data. The first is the union of two K_4-graphs while the second is the union of two disjoint non-complete graphs. Both of these are the conflict graphs for non-adjacent orthomorphisms, such as γ_1 and γ_3 or β_2 and β_4 in Table 11, though not all pairs of non-ajdacent orthomorphisms produce graphs such as these, in fact the conflict graph for α_1 and α_3 is also a cube.

Figure 2: K4-conflict

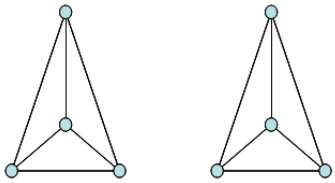
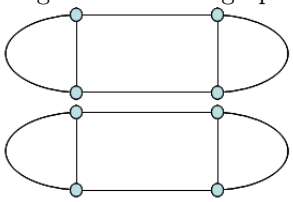


Figure 3: conflict graph



The desired procedure is to find a multiple n, equivalently power, since σ is a function and multiples become composites, of the generator σ and a constant $c \in Im(G_0)$ such that $\sigma^n z + c$ is an orthomorphism. To apply this procedure to the larger group G_0, consider $R = Im(G_0) = \mathbb{Z}_3 \times \mathbb{Z}_3$ under the action of Π. In this case, there are 3 blocks in the first row of the equivalent of Table 3 and in general there are p blocks. Since the funciton Π is surjective but not injective, it is necessary to say that $G_0 = H_1 \cup H_2 \cup H_3$ and that if $\Pi(x_1, y_1) = \Pi(x_2, y_2) = \Pi(x_3, y_3)$ then $(x_i, y_i) \in H_i$ for $i = 1, 2, 3$. For the general case, let $\Pi(x_i, y_i) = \Pi(x_j, y_j) \Rightarrow (x_i, y_i) \in H_i$ and $(x_j, y_j) \in H_j$ for all $i, j = 1, \ldots, n = |G|$. Using this, a semi-exhaustive search method will be used and called semi-exhaustive since it will consider all possible powers of sigma and all possible constants in all possible combinations, but cannot produce a complete set of orthomorphisms. The construction begins by listing the elements of $\Pi(H_i) = R$ in a matrix D such that the entries in the first row are all of the group elements partitioned into 3 blocks of 9 elements each. These blocks will be denoted $D_{1,1}, D_{1,2}, D_{1,3}$ where $D_{a,b}$ is the b^{th} block of the a^{th}

row. To construct the second row, the first element $(x_{2,1}, y_{2,1})$ in $D_{2,1}$ is formed from the first element $(x_{1,1}, y_{1,1})$ of $D_{1,1}$ by the coordinatewise operations:

$$\begin{aligned} D_{2,1}(x) &= (D_{1,1}(x) + D_{1,1}(y)) \bmod 3 \\ D_{2,1}(y) &= (D_{1,1}(x) - D_{1,1}(y)) \bmod 3 \end{aligned}$$

Each subsequent coordinate can be found from the previous row by the generalized coordinatewise operations:

$$\begin{aligned} D_{i,j}(x) &= (D_{i-1,j}(x) + D_{i-1,j}(y)) \bmod 3 \\ D_{i,j}(y) &= (D_{i-1,j}(x) - D_{i-1,j}(y)) \bmod 3 \end{aligned}$$

This coordinatewise definition is derived from the value of σ, which is a generator for the additive group of a field of order 9, which is necessary since the image of G_0 under Π has order 9. Here $\sigma = 11 = (1,1) = 1 + i$ and $D_{i,j} = \sigma D_{i-1,j}$ for $2 \leq i \leq 8$ so that row i is multiplication of the list of group elements by σ^i. Then constants, which are elements of the set $C = \{x \in \mathbb{Z}_3 \times \mathbb{Z}_3\}$ and will be denoted c_i, are added blockwise in triples (c_0, c_1, c_2) such that a unique constant c_j is added to each block $D_{i,j}$ for $j = 1, 2, 3$ in a given row i. This process can be normalized by taking $c_0 = (0,0)$, so that each row D_i could have one of $\binom{8}{2} = 28$ pairs of constants (c_1, c_2) added to it in one of $2! = 2$ ways giving 56 total possible combinations. Since this addition is performed in the image, there are still the sets H_1, H_2, H_3 in some order; in particular each pair $(a, b) \in \mathbb{Z}_3 \times \mathbb{Z}_3$ occurs 3 times. In order to transform this particular row of D, row i, to the preimage, it is possible to consider the each of the 9 triples individually. To each of these triples, one of the following must be added: $p_1 = (0,0), p_2 = (0,3), p_3 = (0,6)$. This can be done in one of $3! = 6$

ways. Therefore for each row of D, there are $56 * 6^9 = 564,350,976$ possible preimages.

For example, since

$$D_2 = \{00, 21, 12, 11, 02, 20, 22, 10, 01\}, \{00, 21, 12, 11, 02, 20, 22, 10, 01\},$$
$$\{00, 21, 12, 11, 02, 20, 22, 10, 01\}$$

where set notation is used to denote blocks, and say $c_1 = 10, c_2 = 02$, then

$$D_2^* = \{00, 21, 12, 11, 02, 20, 22, 10, 01\}, \{10, 01, 22, 21, 12, 00, 02, 20, 11\},$$
$$\{02, 20, 11, 10, 01, 22, 21, 12, 00\}$$

and since column indices that are the 9 triples are completley decided by the first block, that is the pair 00 in the first block determines the same triple as the pair 00 in the second block, it is possible that the first 8 triples are not permuted. At this time, it is necessary to consider each triple individually and to each element of each triple one of the following must be added: $00, 03, 06$. This will determine a preimage once completed on all triples. This final step should be done by considering permutations to occur on these three constants, which gives 6 possibilites for each triple. Since 00 has triple $(1, 15, 27)$, and it is one of the first 8 triples which for this example are not permuted, D_2^* becomes

$$D_2^{**} = \{\underline{00}, 21, 12, 11, 02, 20, 22, 10, 01\}, \{10, 01, 22, 21, 12, \underline{03}, 02, 20, 11\},$$
$$\{02, 20, 11, 10, 01, 22, 21, 12, \underline{06}\}$$

continuing in this manner,

$$D_2' = \{00, 21, 12, 11, 02, 20, 22, 10, 01\}, \{13, 01, 25, 24, 15, 03, 05, 23, 14\},$$
$$\{08, 26, 17, 16, 01, 28, 27, 18, 06\}$$

where the last triple 01 is still to be altered. This procedure basically results in adding 00 to the first block, 03 to the second, and 06 to the third, execpt for the last triple. If the addition of the final constants to the final triple is to be done in the order $00, 06, 03$, then the preimage to consider is

$$D_2'' = \{00, 21, 12, 11, 02, 20, 22, 10, 01\}, \{13, 07, 25, 24, 15, 03, 05, 23, 14\},$$
$$\{08, 26, 17, 16, 04, 28, 27, 18, 06\}$$

although a different choice for the last triple can result in another distinct valid preimage, say

$$D_2^0 = \{00, 21, 12, 11, 02, 20, 22, 10, 07\}, \{13, 04, 25, 24, 15, 03, 05, 23, 14\},$$
$$\{08, 26, 17, 16, 01, 28, 27, 18, 06\}$$

Since both D_2'' and D_2^0 are valid possibilities, this procedure is very computationally expensive.

Proposition:

Given $G = \mathbb{Z}_p \times \mathbb{Z}_{p^2}$ and f defined by $f((g_1, g_2)) = (g_1, g_2 \bmod p)$, then $f : G \to K \cong \mathbb{Z}_p \times \mathbb{Z}_p$ and by letting $x_i \in H_i$ and $x_j \in H_j$ if $f(x_i) = f(x_j)$ for

$1 \leq i \neq j \leq p$. Then $G = \bigcup_{i=1}^{p} H_i, |H_i| = p^2$ and there are

$$T(p) = \left((p-1)!\binom{p^2-1}{p-1}(p!)^{p^2}\right)^{p^2-2}$$

possible preimages $G' = f^{-1}(K)$.

Proof:

Create a matrix D by rows as follows: the first row is to be a listing of the group elements in some order. Each subsequent row is created from the previous row by multiplying by σ which is chosen as a root of an irreducible polynomial over the field $\mathbb{Z}_p$. Choose $p-1$ constants $c_i, 1 \leq i \leq p-1$ from the set $C = \mathbb{Z}_p \times \mathbb{Z}_p$ and $c_0 = 0 \in C$ to add to the p blocks of G, always choosing to add c_0 to the first block. This gives $\binom{p^2-1}{p-1}$ choices for constants. For each set of $p-1$ constants, an order must be chosen in one of $(p-1)!$ ways. To obtain a possible preimage, need to choose numbers $c'_j \in C' = \{(0, kp) : 0 \leq k \leq p-1\}$ for $1 \leq j \leq p^2$ to add to the j^{th} place in the p-tuple in each block. There are $|C'| = p$ choices for each j giving $p!$ choices to be made p^2 times. Using the multiplicaiton principle, this gives a total number of $(p-1)!\binom{p^2-1}{p-1}(p!)^{p^2}$ possibilities per row of D. There are p^2-2 rows in D to be considered since the first row is unaltered and the degree of the irreducible polynomial is at most p^2 so any power of σ can be written using exponents at most p^2-1. $\square$

Therefore there are $T(3)^{j-1}$ possibile preimages of orthomorphisms to consider in the group G_0 since $\sigma^8 = 1$ and the desired orthomorphisms will be orthogonal to this, it is only necessary to consider the non-identity elements. Thus, since the array D above has $j = 8$ rows and the proposition applies to each row, the first row is subtracted off in this calculation, and the use of the multiplication rule results in $T(3)^7 \approx 1.8 * 10^{61}$ total possible preimages. Assuming that a given processor can perform 1 million matrix comparisons per

second, this would take approximately $5.78 * 10^{47}$ years of computing time to make every possible comparison.

The MATLAB files included in the appendix implement this method, though the amount of computational overhead for the files to run is extremely large. The first file is the main program to be run with the necessary function files following on subsequent pages. Only those function files that are not built in MATLAB commands are included in the appendix.

5 Appendix

```
%%
B=initmat(3); % intialize B - matrix of zeros
%%
% create images of rows and preimage of row 1
for i=1:3
    for j=1:9
        for k=1:7
            B{1,9*(i-1)+j}(1,1)=fix((j-1)/3);
            B{1,9*(i-1)+j}(1,2)=mod(j-1,3);
            B{k+1,9*(i-1)+j}(1,1)=mod(B{k,9*(i-1)+j}(1,1)-B{k,9*(i-1)+j}(1,2),3);
            B{k+1,9*(i-1)+j}(1,2)=mod(B{k,9*(i-1)+j}(1,1)+B{k,9*(i-1)+j}(1,2),3);
            B{1,9*(i-1)+j}(1,2)=B{1,9*(i-1)+j}(1,2)+3*(i-1);
        end
    end
end
%%
% preparatory calculations to create subsequent rows
h=cell(1,9);
for i=1:9
    h{1,i}=B{1,i};
end
F=perms(1:3);
s=nchoosek(8,2);
N=nchoosek(2:9,2);
M1=cell(7*s,27,2);
%%
% M1 is a 3-D (196x27x2) array of images plus constants
for i=1:7
    for j=1:s
        M1(28*(i-1)+j,:,:)=addconst3(B(i+1,:),h{N(j,1)},h{N(j,2)});
    end
end
%%
% M is a 2-D (392x27) array of images plus constants
% M is arranged in blocks: the frist 56 rows are based on row 2 of B and
% represent the 56 ways to add the 28 pairs of 2 constants each. The second
% 56 rows are based on row 3 of B...etc.
M=cell(392,27);
d=zeros(392,2);
for i=1:7
    for k=1:2*s
        d(2*s*(i-1)+k,1)=floor((k+1)/2+(s*(i-1)));
        d(2*s*(i-1)+k,2)=mod(k-1+s*(i-1),2)+1;
```

```
        M(2*s*(i-1)+k,:)=M1(d(2*s*(i-1)+k,1),:,d(2*s*(i-1)+k,2));
    end
end
s_1=size(M(:,1));
clear M1 N d i k j;
%%
% create cell array G such that row i contains a character string of
% numbers, treated as base 6, that encodes the permutation of the indices
% used on the jth row of Y2=findtrips(M(:,:)) in the jth digit.
G=permcodes(6^9,0);
%%
MOLS=cell(392,27);
MOLS(1,:)=B(1,:);
IMAGES={};
CODES={};
ROWS={};
COLUMNS={};
for i=1:7
    for j=1:56
        [col,S]=findperm(M(56*(i-1)+j,:),MOLS,G,F);
        if S==1
            MOLS=[MOLS;experm(M(56*(i-1)+j,:),G{col},F)];
            CODES=[CODES;G{col}];
            IMAGES=[IMAGES;M(56*(i-1)+j,:)];
            ROWS=[ROWS;56*(i-1)+j];
            COLUMNS=[COLUMNS;col];
            continue
        else
            MOLS=MOLS;
            CODES=CODES;
            IMAGES=IMAGES;
            ROWS=ROWS;
            COLUMNS=COLUMNS;
        end
    end
end
%%
[z0_r,z0_c]=size(MOLS);
z=z0_r
```

```
function [B]=initmat(m)
% this function preallocates a cell array of zeros for Z_m x Z_m^2
b=zeros(1,2);
B=cell(m^2-1,m^3);
for i=1:m^3
    for j=1:m^2-1
        B{j,i}=b;
    end
end
```

```
function [Y]=addconst3(X,h1,h2)
% this function adds the constants h1,h2 blockwise to X in the 2!=2 ways
% possible. each possibility is stored on a separate page of the output
% array Y.
% h_i are constants
% X is the array to be modified, a row from B in research2.m
for j=1:9
    for i=1:2
        Y{1,j,1}(1,i)=mod(X{1,j}(1,i),3);
    end
end
for j=1:9
    for i=1:2
        Y{1,9+j,1}(1,i)=mod(X{1,9+j}(1,i)+h1(1,i),3);
    end
end
for j=1:9
    for i=1:2
        Y{1,18+j,1}(1,i)=mod(X{1,18+j}(1,i)+h2(1,i),3);
    end
end
for j=1:9
    for i=1:2
        Y{1,j,2}(1,i)=mod(X{1,j}(1,i),3);
    end
end
for j=1:9
    for i=1:2
        Y{1,9+j,2}(1,i)=mod(X{1,9+j}(1,i)+h2(1,i),3);
    end
end
for j=1:9
    for i=1:2
        Y{1,18+j,2}(1,i)=mod(X{1,18+j}(1,i)+h1(1,i),3);
    end
end
```

```
function G=permcodes(b_size,init_val)
G={};
G_1=cell(b_size,1);
    for j=1:b_size
        G_1{j}=dec2base(j+init_val-1,6);
    end
G=[G;G_1];
end
```

```
function [col,S]=findperm(A,MOLS,G,F,B)
% findperm(.) determines if any permutation of A coded in G is acceptable
% to be added to MOLS. If so, S=1; if not S=0.
Y=zeros(1,length(G));
Y=compperm(A,MOLS,G,F,B);
if isempty(find(Y,1))
    S=0;
    col=[];
else
    S=1;
    col=find(Y,1);
end
```

```
function y=compperm(X,MOLS,G,F,B)
% compperm will compare the array X to all rows already in MOLS. The
output
% is logical 1 if row i of X under G(i) is an acceptable addition to MOLS,
% it is 0 if no permutation of X is acceptable in MOLS.
z=size(MOLS);
len_MOLS=zeros(1,z(1));
for i=1:z(1)
    len_MOLS(i)=~isempty(MOLS{i,1});
end
L_MOLS=sum(len_MOLS);
M_1=reshape(cell2mat(B(1,:)),2,27)';
M1=experm2(X,G,F);
s=size(M1);
r=zeros(L_MOLS,s(1));
y=zeros(1,s(1));
for i=1:s(1)
    M2=reshape(cell2mat(M1(i,:)),2,27)';
    DM=zeros(27,2);
        for j=1:L_MOLS
            M_2=reshape(cell2mat(MOLS(j,:)),2,27)';
            DM(:,1)=mod(M_2(:,1)-M2(:,1),3);
            DM(:,2)=mod(M_2(:,2)-M2(:,2),9);
            r(j,i)=iseqmat(DM,M_1);
        end
    y(i)=sum(r(:,i)==L_MOLS);
end
```

```
function A=experm2(X,G,F)
% this function will exectue all permutations in cell array (of characters)
% G on X, taking X to the pre-image in all (length(G)) possible ways. The
% necessary permutations of 1,2,3 are given in the input F.
size_G=length(G);
Y1=findtrips2(X);
Y2=Y1(1:9,:);
A=cell(size_G,length(X(1,:)));
for i=1:size_G
    A(i,:)=X;
    g=char(G{i});
    if length(g)<9
        g=sprintf('%09s',g);
    end
    x=zeros(1,9);
    for j=1:9
        x(j)=mod(str2num(g(j)),6)+1;
    end
    for k=1:9
        v=Y2(k,:);
        u=F(x(k),:);
        Y2(k,:)=v(u);
    end
    for m=1:9
        A(i,:)=addconst2(A(i,:),Y2(m,:));
    end
end
```

```
function Y=findtrips(X)
% this function will search the array X for the column indices of the triples
of ordered pairs
Y=zeros(27,3);
if iscell(X)
    X1=reshape(cell2mat(X),2,27)';
else
X1=X;
end
for i=1:27
    G=repmat(X1(i,:),27,1);
    H=G==X1;
    for j=1:27
        H(j,3)=H(j,1)*H(j,2);
    end
    x=find(H(:,3)==1);
    for k=1:3
        Y(i,k)=x(k);
    end
end
```

```
function [Y]=addconst2(X,v)
% this function maps X to the preimage (Z_3 x Z_9) by adding 3 vectors
to
% the entries specified by by vector v.
% v is a vector of indices in X to be modified
% X is the row to be modified from the matrix M in research2.m
Y=X;
for i=1:3
    Y{v(i)}=X{v(i)}+(i-1)*[0 3];
end
```

```
function [p] = iseqmat(X,Y)
[n_x,m_x] = size(X);
[n_y,m_y] = size(Y);
[Xs,Ix] = sort(X,1);
[Ys,Iy] = sort(Y,1);
p = 1;
if n_x ~= n_y || m_x ~= m_y
    p = 0;
else
    if sum(sum(X(Ix(:,1),:)==Y(Iy(:,1),:))) ~= n_x*m_x
        p = 0;
    end
end
```

```
function A=experm(X,g,F)
% this function executes the single permutation of the numbers 1,2,3 coded
in g,
% on array X, taking X to the preimage. The permutations of 1,2,3 are given
% in the input F.
g=char(g);
Y1=findtrips(X); Y2=Y1(1:9,:); x=zeros(1,9); A=X;
for i=1:9
    x(i)=mod(g(10-i),6)+1;
end
for k=1:9
    v=Y2(k,:);
    u=F(x(k),:);
    Y2(k,:)=v(u);
end
for j=1:9
    A=addconst2(A,Y2(j,:));
end
```

6 References

[1] A.B. Evans, On orthogonal orthomorphisms of cyclic and non-abelian groups II, Cominatorial Designs 15 (2007) 195-209.

[2] A.B. Evans, Orthomorphism Graphs of Groups, Lecture Notes in Mathematics, Vol 1535, Springer, Berlin, 1992.

[3] Andrew Bowler, Orthomorphisms of dihedral groups, Discrete Mathematics 167/168 (1997) 141-144.

[4] C.J. Colbourn, J.H. Dinitz (Eds.) The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 5005.

[5] A.B. Evans, On orthogonal orthomorphisms of cyclic and non-abelian groups, Discrete Mathematics 243 (2002) 229-233.

[6] L.Q. Chang, K. Hsiang, and S. Tai, Congruent mappings and congruence classes of orthomorphisms of groups. Acta Math. Sinica 14, (1964) 747-756.