The Orthomorphism Graph $\mathcal{L}_3(q)$

Anthony B. Evans

Department of Mathematics and Statistics
Wright State University
Dayton, Ohio, U.S.A.

anthony.evans@wright.edu

Submitted: Mar 10, 2017; Accepted: Feb 3, 2018; Published: Mar 2, 2018
Mathematics Subject Classifications: 05B15

Abstract

Orthomorphisms of groups and pairwise orthogonal orthomorphisms have been used in several constructions of combinatorial designs, in particular in the construction of mutually orthogonal sets of latin squares based on groups. In this paper we will use difference equations to construct orthomorphisms in $\mathcal{L}_3(q)$, an orthomorphism graph of $GF(q)^+ \times GF(3)^+$, and to establish lower bounds for the number of pairwise orthogonal orthomorphisms in $\mathcal{L}_3(q)$.

Keywords: latin squares; orthomorphisms; MOLS

1 Introduction

For G a finite abelian group, a mapping $\theta\colon G \to G$ is an *orthomorphism* of G if the mappings $x \mapsto \theta(x)$ and $x \mapsto \theta(x) - x$ are both bijections. Two mappings $\theta, \phi\colon G \to G$ are said to be *orthogonal* if the mapping $x \mapsto \theta(x) - \phi(x)$ is a bijection. An orthomorphism θ of G is *normalized* if $\theta(0) = 0$. If θ is an orthomorphism of G, then the mapping $x \mapsto \theta(x) - \theta(0)$ is a normalized orthomorphism of G: normalization does not affect orthogonality. We will use $Orth(G)$ to denote the set of normalized orthomorphisms of G as well as the graph in which adjacency is orthogonality. Some automorphisms of $Orth(G)$, described in [7], are H_α, $\alpha \in Aut(G)$, defined by $H_\alpha[\theta] = \alpha\theta\alpha^{-1}$; T_g, $g \in G$, defined by $T_g[\theta](x) = \theta(x+g) - \theta(g)$; and R defined by $R[\theta](x) = x + \theta(-x)$. These automorphisms will prove useful in counting orthomorphisms in Section 4. An *orthomorphism graph* of G is a subgraph of $Orth(G)$. For an orthomorphism graph $\mathcal{H}$ of a group G one parameter is of particular interest: the *clique number* of $\mathcal{H}$, written $\omega(\mathcal{H})$, is the largest possible number of pairwise adjacent vertices of $\mathcal{H}$. The reason for interest in this parameter is that from r pairwise orthogonal orthomorphisms of G we can construct $r + 1$ mutually orthogonal latin squares (MOLS) of order $|G|$. Several constructions of large sets of $MOLS$ arise in this way: see [1] and [11] in the Handbook of Combinatorial Designs [4]. For more on orthomorphism graphs see [7], and for more on latin squares and MOLS see [5] and [15]. Closely related to orthomorphisms is the concept of a complete mapping. For G a finite abelian group, a mapping $\theta\colon G \to G$ is a *complete mapping* of G if the mappings $x \mapsto \theta(x)$ and $x \mapsto \theta(x) + x$ are both bijections. Note that a bijection $\theta\colon G \to G$ is a complete mapping of G if and only if the mapping $x \mapsto \theta(x) + x$ is an orthomorphism of G, and an orthomorphism of G if and only if the mapping $x \mapsto \theta(x) - x$ is a complete mapping of G. There is an extensive literature of constructions of complete mapping polynomials, i.e., polynomials that represent complete mappings of elementary abelian groups: see the survey [17]. Complete mappings and orthomorphisms have a number of applications: see the papers in [12] and [13] for instance.

In [16] a set of four MOLS of order 15 was constructed via a computer search. This construction implicitly used orthomorphisms of $\mathbb{Z}_{15}$, which turned out to have a very striking property: each orthomorphism had the following form.

$$\theta(x) = \begin{cases} ax \pmod 5 & \text{if } x \equiv 0 \pmod 3 \\ ax + 3 \pmod 5 & \text{if } x \equiv 1 \pmod 3 \\ ax - 3 \pmod 5 & \text{if } x \equiv 2 \pmod 3 \end{cases}$$

This suggests trying to construct large sets of MOLS of order $3p$, p a prime, $p \neq 2, 3$, using orthomorphisms of $\mathbb{Z}_{3p}$ that have a similar form.

$$\theta(x) = \begin{cases} ax \pmod p & \text{if } x \equiv 0 \pmod 3 \\ ax + b \pmod p & \text{if } x \equiv 1 \pmod 3 \\ ax - b \pmod p & \text{if } x \equiv 2 \pmod 3 \end{cases}$$

Here b is fixed. In [8] all orthomorphisms of this type were determined, and it was shown that no orthogonal pair of orthomorphisms can be constructed from this class of orthomorphisms if $b = 0$, and at most three if $b \neq 0$. In [9] this class of orthomorphisms was generalized to the group $\mathbb{Z}_{3n}$, where $n > 3$ is not divisible by either 2 or 3, constructing orthogonal pairs of orthomorphisms whenever $b \neq 0$: this was subsequently improved in [10] to three pairwise orthogonal orthomorphisms when $n \neq 7, 17$, n not divisible by 2 or 3. A number of special cases of this latter result had already been proved: see [2] for a summary of these special cases.

In this paper we will generalize these results by considering the orthomorphism graph $\mathcal{L}_3(q)$ of $GF(q)^+ \times GF(3)^+$. In Section 2 we will introduce the orthomorphism graph $\mathcal{L}_3(q)$ and show that orthomorphisms and orthogonalities in this graph can be obtained by solving systems of difference equations. In Section 3 we will use these difference equations to construct orthomorphisms in $\mathcal{L}_3(q)$, in Section 4 we will derive lower bounds for $|\mathcal{L}_3(q)|$, and in Section 5 we will give lower bounds for $\omega(\mathcal{L}_3(q))$.

2 The orthomorphism graph $\mathcal{L}_3(q)$

In this section we will define the orthomorphism graph $\mathcal{L}_3(q)$, $q > 3$ a prime power. We will see that the elements of $\mathcal{L}_3(q)$ and orthogonalities in $\mathcal{L}_3(q)$ can be determined by solving systems of difference equations.

First note that any mapping $GF(q) \times GF(3) \to GF(q) \times GF(3)$, and hence any orthomorphism of $GF(q)^+ \times GF(3)^+$, can be written as $\theta(x,y) = (\theta_{1,y}(x), \theta_{2,x}(y))$, where for each $y \in GF(3)$, $\theta_{1,y}$ is a mapping $GF(q) \to GF(q)$, and for each $x \in GF(q)$, $\theta_{2,x}$ is a mapping $GF(3) \to GF(3)$. We will call $\theta_{1,y}$, $y \in GF(3)$, the *first component mappings* of θ; and $\theta_{2,x}$, $x \in GF(q)$, the *second component mappings* of θ.

The orthomorphism graph $\mathcal{L}_3(q)$ is the induced subgraph of $Orth(GF(q)^+ \times GF(3)^+)$ whose orthomorphisms have first component mappings $\theta_{1,y}(x) = ax + b_y$, $a \neq 0, 1$ and $b_0 = 0$. From the first component mappings of a bijection $GF(q) \times GF(3) \to GF(q) \times GF(3)$ the form of the corresponding second component mappings can be determined.

Lemma 1. *Let the mapping $\theta\colon GF(q) \times GF(3) \to GF(q) \times GF(3)$ have first component mappings $\theta_{1,y}(x) = ax + b_y$, $a \neq 0$ and $b_0 = 0$. Then θ is a bijection if and only if each second component mapping can be written as*

$$\theta_{2,x}(y) = y\mathrm{def}_\theta(x + b_y/a) + \mathrm{sum}_\theta(x + b_y/a) \tag{1}$$

for some $\mathrm{def}_\theta, \mathrm{sum}_\theta\colon GF(q) \to GF(3)$*,* $\mathrm{def}_\theta(x) \neq 0$ *for all $x \in GF(q)$.*

Proof. Assume that θ is a bijection. For any given $z \in GF(q)$ the mapping $y \to \theta_{2,(z-b_y)/a}(y)$ is a bijection $GF(3) \to GF(3)$, as θ is a bijection and $\theta((z - b_y)/a, y) = (z, c) = \theta((z - b_w)/a, w)$ whenever $\theta_{2,(z-b_y)/a}(y) = \theta_{2,(z-b_w)/a}(w) = c$. Thus, using the fact that any permutation of the elements of $GF(3)$ can be represented as a nonconstant linear polynomial over $GF(3)$,

$$\theta_{2,(z-b_y)/a}(y) = yk(z) + h(z)$$

for some maps $k, h\colon GF(q) \to GF(3)$, $k(z) \neq 0$ for all $z \in GF(q)$. This equation holds for all $z \in GF(q)$ and $y \in GF(3)$. Setting $x = (z - b_y)/a$, $\mathrm{def}_\theta(x) = k(ax)$, and $\mathrm{sum}_\theta(x) = h(ax)$ yields Equation (1). The converse is routine. □

We will call the function def_θ in Lemma 1 the *defining sequence* for θ and the function sum_θ the *sum function* for θ. Any element $\theta \in \mathcal{L}_3(q)$ can be specified by stating its first component mappings, its sum function sum_θ, and its defining sequence def_θ. These functions must satisfy a system of difference equations.

Theorem 2. *Let $\theta\colon GF(q) \times GF(3) \to GF(q) \times GF(3)$ be a bijection with first component mappings $\theta_{1,y}(x) = ax + b_y$, $a \neq 0, 1$ and $b_0 = 0$, defining sequence* def_θ*, and sum function* sum_θ*,* $\mathrm{sum}_\theta(0) = 0$*. Then $\theta \in \mathcal{L}_3(q)$ if and only if* def_θ *and* sum_θ *satisfy the following system of difference equations.*

$$\mathrm{sum}_\theta(x + C_{\theta,y}) - \mathrm{sum}_\theta(x) = y(\mathrm{discr}_\theta(x) - \mathrm{def}_\theta(x + C_{\theta,y}) + 1) \tag{2}$$

for all $y \in GF(3)$ and some $\mathrm{discr}_\theta\colon GF(q) \to GF(3)$*,* $\mathrm{discr}_\theta(x) \neq 0$ *for all $x \in GF(q)$, where*

$$C_{\theta,y} = \frac{-b_y}{a(a-1)}.$$

Proof. Assume that θ is an orthomorphism. For the mapping $(x, y) \mapsto \theta(x, y) - (x, y)$ the three images with first component $(a-1)x$ have second components $\mathrm{sum}_\theta(x + C_{\theta,y}) + y\mathrm{def}_\theta(x + C_{\theta,y}) - y$, and so, as these must all be different and any permutation of the elements of $GF(3)$ can be represented as a nonconstant linear polynomial over $GF(3)$,

$$\mathrm{sum}_\theta(x + C_{\theta,y}) + y\mathrm{def}_\theta(x + C_{\theta,y}) - y = y\mathrm{discr}_\theta(x) + c_\theta(x)$$

for some $\mathrm{discr}_\theta, c_\theta \colon GF(q) \to GF(3)$, $\mathrm{discr}_\theta(x) \neq 0$ for all $x \in GF(q)$. Setting $y = 0$ we see that $c_\theta(x) = \mathrm{sum}_\theta(x)$. This yields the system of equations (2). The converse is routine. □

We will call the function discr_θ in Theorem 2 the *discriminant function* for θ and we will call the system of equations (2) in Theorem 2 the *difference equations* for θ. Orthogonality in $\mathcal{L}_3(q)$ depends similarly on solutions to a system of equations.

Theorem 3. *Let $\theta, \phi \in \mathcal{L}_3(q)$ have first component mappings $\theta_{1,y}(x) = ax + b_y$, $a \neq 0, 1$ and $b_0 = 0$, and $\phi_{1,y}(x) = Ax + B_y$, $A \neq 0, 1, a$ and $B_0 = 0$, respectively, sum functions sum_θ and sum_ϕ, respectively, and defining sequences def_θ and def_ϕ, respectively. Then θ is orthogonal to ϕ if and only if*

$$(\mathrm{sum}_\theta(x + C_{\theta,\phi,y}) - \mathrm{sum}_\theta(x)) - (\mathrm{sum}_\phi(x + C_{\phi,\theta,y}) - \mathrm{sum}_\phi(x)) = \tag{3}$$

$$y(\mathrm{discr}_{\theta,\phi}(x) - \mathrm{def}_\theta(x + C_{\theta,\phi,y}) + \mathrm{def}_\phi(x + C_{\phi,\theta,y}))$$

for all $y \in GF(3)$, and some $\mathrm{discr}_{\theta,\phi} \colon GF(q) \to GF(3)$, $\mathrm{discr}_{\theta,\phi}(x) \neq 0$ for all $x \in GF(q)$, where

$$C_{\theta,\phi,y} = \frac{aB_y - Ab_y}{a(a-A)} \quad \text{and} \quad C_{\phi,\theta,y} = \frac{Ab_y - aB_y}{A(A-a)}.$$

Proof. Similar to the proof of Theorem 2. □

We will call the function $\mathrm{discr}_{\theta,\phi}$ in Theorem 3 the *discriminant function* for θ by ϕ and we will call the system of equations (3) in Theorem 3 the *adjacency difference equations* for θ and ϕ. Note that, in Theorem 3, a necessary condition for θ to be orthogonal to ϕ is $A \neq a$.

3 Constructions of orthomorphisms in $\mathcal{L}_3(q)$

In this section we will give some constructions of orthomorphisms in $\mathcal{L}_3(q)$. Throughout this paper, for a bijection $\theta \colon GF(q)^+ \times GF(3)^+ \to GF(q)^+ \times GF(3)^+$; def_θ will denote the defining sequence for θ, $\mathrm{def}_\theta(x) \neq 0$ for all $x \in GF(q)$; sum_θ will denote the sum function for θ; and, if the first component mappings for θ are $ax + b_y$, $y \in GF(3)$, then, as in Theorem 2, $C_{\theta,y} = -b_y/(a(a-1))$.

To construct orthomorphisms in $\mathcal{L}_3(q)$ we first specify first component mappings $ax + b_y$, $a \neq 0, 1$ and $b_0 = 0$, and then solve the difference equations (2) for def_θ and sum_θ. As the difference equation (2) with $y = 0$ is $0 = 0$, we need only solve the difference equations (2) for $y = 1, 2$. If we regard $GF(q)$ as a vector space over its prime subfield then $\{C_{\theta,y} \mid y = 1, 2\}$, equivalently $\{b_y \mid y = 1, 2\}$, spans a subspace of $GF(q)$ of dimension at most two: the dimension of this subspace will be called the *dimension* of θ. The simplest orthomorphisms in $\mathcal{L}_3(q)$ to construct are those of dimension 0.

Theorem 4. *If $\theta\colon GF(q) \times GF(3) \to GF(q) \times GF(3)$ is a bijection with first component mappings ax for all $y \in GF(3)$, $a \neq 0, 1$, then $\theta \in \mathcal{L}_3(q)$ if and only if $\mathrm{def}_\theta(x) = -1$ for all $x \in GF(q)$ and $\mathrm{sum}_\theta(0) = 0$.*

Proof. The difference equation (2) for θ with $y = 1$ and also $y = 2$ is

$$\mathrm{discr}_\theta(x) - \mathrm{def}_\theta(x) + 1 = 0.$$

As $\mathrm{discr}_\theta(x), \mathrm{def}_\theta(x) \neq 0$ for all $x \in GF(q)$, it follows that $\mathrm{discr}_\theta(x) = 1$ for all $x \in GF(q)$ and $\mathrm{def}_\theta(x) = -1$ for all $x \in GF(q)$. Hence

$$\theta(x, y) = (ax, -y + \mathrm{sum}_\theta(x)), \tag{4}$$

$a \neq 0, 1$, $\mathrm{sum}_\theta(0) = 0$.

It is routine to show that, if θ satisfies Equation (4), then θ satisfies the difference equations (2). □

In the following theorems we will describe more orthomorphisms in $\mathcal{L}_3(q)$ of dimension one.

Theorem 5. *If $\theta\colon GF(q) \times GF(3) \to GF(q) \times GF(3)$ is a bijection with first component mappings $ax+b_y$, $a \neq 0, 1$, $b_0 = b_1 = 0$, $b_2 \neq 0$, then $\theta \in \mathcal{L}_3(q)$ if and only if $\mathrm{def}_\theta(x) = -1$ for all $x \in GF(q)$, sum_θ is constant on orbits of $x \mapsto x + C_{\theta,2}$, and $\mathrm{sum}_\theta(0) = 0$.*

Proof. The difference equation (2) for θ with $y = 1$ is

$$\mathrm{discr}_\theta(x) - \mathrm{def}_\theta(x) + 1 = 0.$$

As $\mathrm{discr}_\theta(x), \mathrm{def}_\theta(x) \neq 0$ for all $x \in GF(q)$, it follows that $\mathrm{discr}_\theta(x) = 1$ for all $x \in GF(q)$ and $\mathrm{def}_\theta(x) = -1$ for all $x \in GF(q)$. It follows that the difference equation (2) for θ with $y = 2$ is

$$\mathrm{sum}_\theta(x + C_{\theta,2}) - \mathrm{sum}_\theta(x) = 0.$$

Hence, sum_θ is constant on orbits of $x \mapsto x + C_{\theta,2}$.

We leave it to the reader to verify that the defining sequence, sum function, and discriminant function we have constructed satisfy the conditions of Theorem 2. □

Theorem 6. *Let p be the characteristic of $GF(q)$, p odd. If $\theta\colon GF(q) \times GF(3) \to GF(q) \times GF(3)$ is a bijection with first component mappings $ax + b_y$, $a \neq 0, 1$, $b_0 = 0$, $b_2 = 2b_1 \neq 0$, then $\theta \in \mathcal{L}_3(q)$ if and only if $\mathrm{sum}_\theta(0) = 0$ and, for each orbit O of $x \mapsto x + C_{\theta,1}$, one of the following holds.*

(i) $\sum_{x \in O} \mathrm{def}_\theta(x) = -p$ *and*

$$\mathrm{sum}_\theta(w + nC_{\theta,1}) = \mathrm{sum}_\theta(w) + n + \sum_{i=1}^{n} \mathrm{def}_\theta(w + iC_{\theta,1}),$$

where w is a given element of O.

(ii) $p = 3$, $\mathrm{def}_\theta(x) = 1$ *for all $x \in O$, and*

$$\mathrm{sum}_\theta(w + nC_{\theta,1}) = \mathrm{sum}_\theta(w) + n,$$

where w is a given element of O.

(iii) $p = 3$, $\mathrm{def}_\theta(x) = -1$ *for all $x \in O$, and*

$$\mathrm{sum}_\theta(w + nC_{\theta,1}) = \mathrm{sum}_\theta(w) + n,$$

where w is a given element of O.

Proof. Adding the difference equation (2) for θ with $y = 1$ to the difference equation (2) for θ with $y = 1$ and x replaced by $x + C_{\theta,1}$ yields

$$\begin{aligned}\mathrm{sum}_\theta(x + 2C_{\theta,1}) - \mathrm{sum}_\theta(x) = {} & \mathrm{discr}_\theta(x + C_{\theta,1}) + \mathrm{discr}_\theta(x) \\ & - \mathrm{def}_\theta(x + C_{\theta,1}) - \mathrm{def}_\theta(x + 2C_{\theta,1}) - 1.\end{aligned}$$

Comparing this with the difference equation (2) for θ with $y = 2$ yields

$$\mathrm{discr}_\theta(x + C_{\theta,1}) + \mathrm{def}_\theta(x + 2C_{\theta,1}) = \mathrm{discr}_\theta(x) + \mathrm{def}_\theta(x + C_{\theta,1}).$$

Thus $\mathrm{discr}_\theta(x) + \mathrm{def}_\theta(x + C_{\theta,1})$ is constant on orbits of $x \mapsto x + C_{\theta,1}$.

Let O be an orbit of $x \mapsto x + C_{\theta,1}$.

If $\mathrm{discr}_\theta(x) + \mathrm{def}_\theta(x + C_{\theta,1}) = 0$ for all $x \in O$, then

$$\mathrm{sum}_\theta(x + C_\theta) - \mathrm{sum}_\theta(x) = \mathrm{def}_\theta(x + C_{\theta,1}) + 1,$$

from which (**i**) follows.

If $\mathrm{discr}_\theta(x) + \mathrm{def}_\theta(x + C_{\theta,1}) = 1$ for all $x \in O$, then $\mathrm{discr}_\theta(x) = \mathrm{def}_\theta(x + C_{\theta,1}) = -1$ for all $x \in O$. If $\mathrm{discr}_\theta(x) + \mathrm{def}_\theta(x + C_{\theta,1}) = -1$ for all $x \in O$, then $\mathrm{discr}_\theta(x) = \mathrm{def}_\theta(x + C_{\theta,1}) = 1$ for all $x \in O$. In either case $\mathrm{sum}_\theta(x + C_{\theta,1}) - \mathrm{sum}_\theta(x) = 1$, which can only occur if $p = 3$. (**ii**) and (**iii**) follow.

We leave it to the reader to verify that the defining sequence, sum function, and discriminant function we have constructed satisfy the conditions of Theorem 2. □

Let us consider more generally, for $GF(q)$ of odd characteristic, the case of orthomorphisms in $\mathcal{L}_3(q)$ of dimension 1 that have first component mappings of the form $ax + b_y$, where $b_1, b_2 \neq 0$. For such an orthomorphism $b_2 = m.b_1 \neq 0 = b_0$ for some positive integer m, $1 \leqslant m < p - 1$, p the characteristic of $GF(q)$.

Theorem 7. *Let p be the characteristic of $GF(q)$, p odd. If $\theta\colon GF(q) \times GF(3) \to GF(q) \times GF(3)$ is a bijection with first component mappings $ax + b_y$, $y \in GF(3)$, $a \neq 0, 1$, $b_2 = m.b_1 \neq 0 = b_0$, $1 \leqslant m < p$, then $\theta \in \mathcal{L}_3(q)$ if and only if* $\mathrm{sum}_\theta(0) = 0$*, and, for all $x \in GF(q)$,*

$$\sum_{i=0}^{p-1} \mathrm{discr}_\theta(x + iC_{\theta,1}) - \sum_{i=0}^{p-1} \mathrm{def}_\theta(x + iC_{\theta,1}) + p = 0, \tag{5}$$

$$\begin{gathered} \mathrm{discr}_\theta(x) - \mathrm{def}_\theta(x + mC_{\theta,1}) + \sum_{i=0}^{m-1} \mathrm{discr}_\theta(x + iC_{\theta,1}) \\ - \sum_{i=1}^{m} \mathrm{def}_\theta(x + iC_{\theta,1}) + m + 1 = 0, \end{gathered} \tag{6}$$

and for any orbit O of $x \mapsto x + C_{\theta,1}$

$$\mathrm{sum}_\theta(w + nC_{\theta,1}) = \mathrm{sum}_\theta(w) + \sum_{i=0}^{n-1} \mathrm{discr}_\theta(w + iC_{\theta,1}) - \sum_{i=1}^{n} \mathrm{def}_\theta(w + iC_{\theta,1}) + n, \tag{7}$$

where w is a given element of O.

Proof. Summing the difference equation (2) with $y = 1$ over an orbit of $x \mapsto x + C_{\theta,1}$ yields Equation (5), and summing the difference equation (2) with $y = 1$ with $x = w$ through $x = w + (n-1)C_{\theta,1}$ yields Equation (7). Comparing Equation (7), with $w = x$ and $n = m$, with the difference equation (2) with $y = 2$ yields Equation (6).

It is routine to show that, if equations (5), (6), and (7) hold, then the difference equations for θ are satisfied. □

We will apply Theorem 7 in the special case $m = 3$ and the characteristic of $GF(q)$ is 7.

Theorem 8. *Let the characteristic of $GF(q)$ be 7. If $\theta\colon GF(q) \times GF(3) \to GF(q) \times GF(3)$ is a bijection with first component mappings $ax + b_y$, $y \in GF(3)$, $a \neq 0, 1$, $b_2 = 3.b_1 \neq 0 = b_0$, then $\theta \in \mathcal{L}_3(q)$ if and only if* $\mathrm{sum}_\theta(0) = 0$*; for all $x \in GF(q)$,*

$$\begin{gathered} \mathrm{discr}_\theta(x) = \mathrm{def}_\theta(x + 6C_{\theta,1}) - \mathrm{def}_\theta(x + 5C_{\theta,1}) \\ - \mathrm{def}_\theta(x + 4C_{\theta,1}) - \mathrm{def}_\theta(x + 2C_{\theta,1}) - 1; \end{gathered} \tag{8}$$

for O an orbit of $x \mapsto x + C_{\theta,1}$, either $\mathrm{def}_\theta(x) = -1$ *for all $x \in O$ and* sum_θ *is constant on O, or* $(\mathrm{def}_\theta(x), \mathrm{def}_\theta(x + C_{\theta,1}), \ldots, \mathrm{def}_\theta(x + 6C_{\theta,1}))$ *is a cyclic permutation of* $(1, 1, -1, -1, -1, 1, -1)$*; and* sum_θ *is given by*

$$\begin{gathered} \mathrm{sum}_\theta(x + mC_{\theta,1}) = \sum_{i=1}^{m} (\mathrm{def}_\theta(x + 6iC_{\theta,1}) - \mathrm{def}_\theta(x + 5iC_{\theta,1}) \\ - \mathrm{def}_\theta(x + 4iC_{\theta,1}) - \mathrm{def}_\theta(x + 2iC_{\theta,1}) - \mathrm{def}_\theta(x + iC_{\theta,1})) + c, \end{gathered} \tag{9}$$

where c is constant on O.

Proof. Assume that $\theta \in \mathcal{L}_3(q)$. By Equation (6) of Theorem 7, the difference equations for θ have a solution only if

$$\begin{aligned} -\mathrm{discr}_\theta(x) + \mathrm{discr}_\theta(x+C_{\theta,1}) + \mathrm{discr}_\theta(x+2C_{\theta,1}) \\ = \mathrm{def}_\theta(x+C_{\theta,1}) + \mathrm{def}_\theta(x+2C_{\theta,1}) - \mathrm{def}_\theta(x+3C_{\theta,1}) - 1, \end{aligned} \tag{10}$$

for all $x \in GF(q)$. A solution to Equation (10) for discr_θ is

$$\begin{aligned} \mathrm{discr}_\theta(x) = \mathrm{def}_\theta(x+6C_{\theta,1}) - \mathrm{def}_\theta(x+5C_{\theta,1}) \\ -\mathrm{def}_\theta(x+4C_{\theta,1}) - \mathrm{def}_\theta(x+2C_{\theta,1}) - 1, \end{aligned}$$

which is Equation (8). To see that this is the only solution suppose that discr'_θ is another potential discriminant function for θ that satisfies Equation (10) and set $d(x) = \mathrm{discr}_\theta(x) - \mathrm{discr}'_\theta(x)$. Then $d(x) = d(x+C_{\theta,1}) + d(x+2C_{\theta,1})$: we leave it to the reader to verify that, for O any orbit of $x \mapsto x + C_{\theta,1}$, $d(x) = 0$ is the only solution to this recurrence relation on O. From this and Equation (7) we can derive Equation (9). The solution to Equation (10) satisfies Equation (6) of Theorem 7. As $\mathrm{discr}_\theta(x) \neq 0$ for all $x \in GF(q)$ we obtain the inequality

$$\mathrm{def}_\theta(x+6C_{\theta,1}) - \mathrm{def}_\theta(x+5C_{\theta,1}) - \mathrm{def}_\theta(x+4C_{\theta,1}) - \mathrm{def}_\theta(x+2C_{\theta,1}) \neq 1, \tag{11}$$

for all $x \in GF(q)$.

Let O be an orbit of $x \to x + C_{\theta,1}$ and set $N = |\{x \in O \mid \mathrm{def}_\theta(x) = 1\}|$. We will show that $N \in \{0,3\}$. It is easy to rule out the possibilities $N = 1$, 6, or 7.

If $N = 2$ then $\mathrm{def}_\theta(z) = \mathrm{def}_\theta(z + jC_{\theta,1}) = 1$ for some $z \in O$ and some $j \in \{1,2,3\}$. If $j = 1$ then setting $x = z - 4C_{\theta,1}$ in Inequality (11) leads to a contradiction: if $j = 2$ then setting $x = z - 2C_{\theta,1}$ in Inequality (11) leads to a contradiction; and if $j = 3$ then setting $x = z - 2C_{\theta,1}$ in Inequality (11) leads to a contradiction. Thus $N \neq 2$.

If $N = 5$ then $\mathrm{def}_\theta(z) = \mathrm{def}_\theta(z + jC_{\theta,1}) = -1$ for some $z \in O$ and some $j \in \{1,2,3\}$. If $j = 1$ then setting $x = z$ in Inequality (11) leads to a contradiction: if $j = 2$ then setting $x = z - C_{\theta,1}$ in Inequality (11) leads to a contradiction; and if $j = 3$ then setting $x = z$ in Inequality (11) leads to a contradiction. Thus $N \neq 5$.

If $N = 4$ then there are two possibilities. It could be that $\mathrm{def}_\theta(z) = \mathrm{def}_\theta(z + C_{\theta,1}) = \mathrm{def}_\theta(z + jC_{\theta,1}) = -1$ for some $z \in O$ and some $j \in \{2,3,4,5\}$: in this case if $j = 2$ then setting $x = z - 5C_{\theta,1}$ in Inequality (11) yields a contradiction; if $j = 3$ then setting $x = z - 5C_{\theta,1}$ in Inequality (11) yields a contradiction; if $j = 4$ then setting $x = z - 2C_{\theta,1}$ in Inequality (11) yields a contradiction; and if $j = 5$ then setting $x = y - C_{\theta,1}$ in Inequality (11) yields a contradiction. The other possibility is that $(\mathrm{def}_\theta(z), \ldots, \mathrm{def}_\theta(z + 6C_{\theta,1})) = (-1,1,-1,1,-1,1,1)$ for some $z \in O$. In this case setting $x = z + 3C_{\theta,1}$ in Inequality (11) yields a contradiction. Thus $N \neq 4$ and so $N \in \{0,3\}$.

If $N = 0$ then $\mathrm{def}_\theta(x) = -1$ for all $x \in O$, Inequality (11) is satisfied, $\mathrm{discr}_\theta(x) = 1$ for all $x \in O$, and the sum function is constant on O.

If $N = 3$ then there are two possibilities. It could be that $(\mathrm{def}_\theta(z), \ldots, \mathrm{def}_\theta(z + 6C_{\theta,1})) = (1,-1,1,-1,1,-1,-1)$ for some $z \in O$, in which case setting $x = z$ in Inequality (11) yields a contradiction, or it could be that $\mathrm{def}_\theta(z) = \mathrm{def}_\theta(z+B) = \mathrm{def}_\theta(z+jC_{\theta,1}) =$

1 for some $z \in O$ and some $j \in \{2, 3, 4, 5\}$: in this case if $j = 2$ then setting $x = z - 2C_{\theta,1}$ in Inequality (11) yields a contradiction; if $j = 3$ then setting $x = z - C_{\theta,1}$ in Inequality (11) yields a contradiction; if $j = 4$ then setting $x = z - C_{\theta,1}$ in Inequality (11) yields a contradiction; and if $j = 5$ then Inequality (11) is satisfied.

We leave it to the reader to verify that, if θ satisfies the conditions of the theorem, then θ satisfies the conditions of Theorem 7 and hence that $\theta \in \mathcal{L}_3(q)$. □

In principle the techniques used in the proof of Theorem 8 can be employed to compute all orthomorphisms in $\mathcal{L}_3(q)$ of dimension one for any given characteristic of $GF(q)$. It is clear though that the length of the proof must increase as the characteristic of $GF(q)$ increases, making this approach impractical in general. This problem gets worse in the dimension two case. We will describe all orthomorphisms in $\mathcal{L}_3(q)$ when the characteristic of $GF(q)$ is 2 only. First we need a dimension two analogue of Theorem 7.

Theorem 9. *If $\theta\colon GF(q) \times GF(3) \to GF(q) \times GF(3)$ is a bijection with first component mappings $ax + b_y$, $y \in GF(3)$, $a \neq 0, 1$, $b_0 = 0$, for which $\{b_1, b_2\}$ spans a 2-dimensional subspace of $GF(q)$, viewed as a vector space over its prime subfield, then $\theta \in \mathcal{L}_3(q)$ if and only if, for all $x \in GF(q)$,*

$$\sum_{i=0}^{p-1} \mathrm{discr}_\theta(x + iC_{\theta,y}) - \sum_{i=0}^{p-1} \mathrm{def}_\theta(x + iC_{\theta,y}) + p = 0 \tag{12}$$

for $y = 1, 2$, where p is the characteristic of $GF(q)$; and

$$\begin{aligned} \mathrm{discr}_\theta(x) + \mathrm{discr}_\theta(x + C_{\theta,1}) + \mathrm{discr}_\theta(x + C_{\theta,2}) + \mathrm{def}_\theta(x + C_{\theta,1}) \\ + \mathrm{def}_\theta(x + C_{\theta,1} + C_{\theta,2}) + \mathrm{def}_\theta(x + C_{\theta,2}) = 0. \end{aligned} \tag{13}$$

Proof. Let $\theta \in \mathcal{L}_3(q)$. Summing the difference equation (2) for θ with $y = 1$ over an orbit of $x \mapsto x + C_{\theta,1}$ yields Equation (12) for $y = 1$, and summing the difference equation (2) for θ with $y = 2$ over an orbit of $x \mapsto x + C_{\theta,2}$ yields Equation (12) for $y = 2$.

Equation (13) can be derived by using the difference equations (2) to evaluate

$$\begin{aligned} (\mathrm{sum}_\theta(x + C_{\theta,2}) - \mathrm{sum}_\theta(x)) + (\mathrm{sum}_\theta(x + C_{\theta,1} + C_{\theta,2}) - \mathrm{sum}_\theta(x + C_{\theta,2})) \\ -(\mathrm{sum}_\theta(x + C_{\theta,1} + C_{\theta,2}) - \mathrm{sum}_\theta(x + C_{\theta,1})) - (\mathrm{sum}_\theta(x + C_{\theta,1}) - \mathrm{sum}_\theta(x)). \end{aligned}$$

We leave it to the reader to verify that, if θ satisfies the conditions of the theorem, then θ satisfies the conditions of Theorem 2 and hence that $\theta \in \mathcal{L}_3(q)$. □

Using Theorem 9 we can now describe all orthomorphisms of dimension two in $\mathcal{L}_3(q)$ when the characteristic of $GF(q)$ is 2.

Theorem 10. *Let the characteristic of $GF(q)$ be 2. If $\theta\colon GF(q) \times GF(3) \to GF(q) \times GF(3)$ is a bijection with first component mappings $ax + b_y$, $y \in GF(3)$, $a \neq 0, 1$, $b_0 = 0$, for which $\{b_1, b_2\}$ spans a 2-dimensional subspace of $GF(q)$, viewed as a vector space over its prime subfield, then $\theta \in \mathcal{L}_3(q)$ if and only if* $\mathrm{sum}_\theta(0) = 0$, *and, for each orbit O of $\langle x \to x + C_{\theta,1}, x \to x + C_{\theta,2} \rangle$, either*

(i) *for all* $x \in O$, $\operatorname{def}_\theta(x) = -1$, $\operatorname{discr}_\theta(x) = 1$, *and* $\operatorname{sum}_\theta$ *is constant on* O*, or,*

(ii) *for some* $w \in O$, $\operatorname{def}_\theta(w) = -1$, $\operatorname{def}_\theta(x) = 1$ *for all* $x \in O \setminus \{w\}$, $\operatorname{discr}_\theta(w + C_{\theta,1} + C_{\theta,2}) = 1$, $\operatorname{discr}_\theta(x) = -1$ *for all* $x \in O \setminus \{w + C_{\theta,1} + C_{\theta,2}\}$*, and*

$$\begin{aligned}(\operatorname{sum}_\theta(w), \operatorname{sum}_\theta(w + C_{\theta,1}), \operatorname{sum}_\theta(w + C_{\theta,2}), \operatorname{sum}_\theta(w + C_{\theta,1} + C_{\theta,2}))& \\ = (c, -1 + c, 1 + c, c),&\end{aligned} \tag{14}$$

where c is a constant.

Proof. Let $\theta \in \mathcal{L}_3(q)$. Equation (12) reduces to

$$\operatorname{discr}_\theta(x) + \operatorname{discr}_\theta(x + C_{\theta,y}) = \operatorname{def}_\theta(x) + \operatorname{def}_\theta(x + C_{\theta,y}) + 1.$$

It follows that

$$\begin{aligned}\operatorname{discr}_\theta(x) = \operatorname{def}_\theta(x + C_{\theta,1} + C_{\theta,2}) - \operatorname{def}_\theta(x)& \\ -\operatorname{def}_\theta(x + C_{\theta,1}) - \operatorname{def}_\theta(x + C_{\theta,2}) - 1.&\end{aligned}$$

Plugging this into Equation (13) yields

$$\operatorname{def}_\theta(x + C_{\theta,1} + C_{\theta,2}) - \operatorname{def}_\theta(x) - \operatorname{def}_\theta(x + C_{\theta,1}) - \operatorname{def}_\theta(x + C_{\theta,2}) \neq 1,$$

for all $x \in GF(q)$.

For O an orbit of $\langle x \to x + C_{\theta,1}, x \to x + C_{\theta,2}\rangle$ let $N = |\{x \in O \mid \operatorname{def}_\theta(x) = 1\}|$. It is easy to prove that $N \in \{0, 3\}$. If $N = 0$ then $\operatorname{def}_\theta(x) = -1$ and $\operatorname{discr}_\theta(x) = 1$ for all $x \in O$, and $\operatorname{sum}_\theta$ is constant on O. If $N = 3$ then let w be the unique element in O for which $\operatorname{def}_\theta(w) = -1$. Then $\operatorname{def}_\theta(x) = 1$ for all $x \in O$, $x \neq w$, and simple computation shows that $\operatorname{discr}_\theta(w + C_{\theta,1} + C_{\theta,2}) = 1$ and $\operatorname{discr}_\theta(x) = -1$ for all $x \in O$, $x \neq w + C_{\theta,1} + C_{\theta,2}$. The sum function $\operatorname{sum}_\theta$ can then be computed using the difference equations (2).

We leave it to the reader to verify that, if θ satisfies the conditions of the theorem, then θ satisfies the conditions of Theorem 9 and hence that $\theta \in \mathcal{L}_3(q)$. □

As in the dimension one case the amount of computation needed to describe all orthomorphisms in $\mathcal{L}_3(q)$ of dimension 2 for any given characteristic increases as the characteristic increases. For any $\theta \in \mathcal{L}_3(q)$, as $\operatorname{discr}_\theta(x), \operatorname{def}_\theta(x) \neq 0$ for all $x \in G(q)$, $\operatorname{discr}_\theta(x) = \pm\operatorname{def}_\theta(x)$ for any $x \in GF(q)$. In Theorem 11 we will characterize $\theta \in \mathcal{L}_3(q)$ of dimension two for which $\operatorname{discr}_\theta(x) = -\operatorname{def}_\theta(x)$ for all $x \in GF(q)$, and in Theorem 12 we will characterize $\theta \in \mathcal{L}_3(q)$ of dimension two for which $\operatorname{discr}_\theta(x) = \operatorname{def}_\theta(x)$ for all $x \in GF(q)$.

Theorem 11. *Let the characteristic of* $GF(q)$ *be* p*,* p *odd. Let* $\theta\colon GF(q) \times GF(3) \to GF(q) \times GF(3)$ *be a bijection with first component mappings* $ax + b_y$*,* $y \in GF(3)$*,* $a \neq 0, 1$*,* $b_0 = 0$*, for which* $\{b_1, b_2\}$ *spans a 2-dimensional subspace of* $GF(q)$*, viewed as a vector space over its prime subfield, and* $\operatorname{discr}_\theta(x) = -\operatorname{def}_\theta(x)$ *for all* $x \in GF(q)$*. For an orbit* O *of* $\langle x \to x + C_{\theta,1}, x \to x + C_{\theta,2}\rangle$*, let* G_O *be the* $p \times p$ *matrix with* ij*th entry*

$\mathrm{def}_\theta(w + (i-1)C_{\theta,1} + (j-1)C_{\theta,2})$*, where* $w \in O$ *is fixed. Then* $\theta \in \mathcal{L}_3(q)$ *if and only if for all orbits* O *of* $\langle x \to x + C_{\theta,1}, x \to x + C_{\theta,2}\rangle$ *the matrix* G_O *is a circulant matrix with first row summing to* $-p$*, and*

$$\begin{aligned}\mathrm{sum}_\theta(a + iC_{\theta,1} + jC_{\theta,2}) &= \sum_{k=0}^{j-1} \mathrm{def}_\theta(w + (i-k)C_{\theta,1}) \\ &+ \sum_{k=1}^{j} \mathrm{def}_\theta(w + (i-k)C_{\theta,1}) - \sum_{k=0}^{i-1} \mathrm{def}_\theta(w + kC_{\theta,1}) \\ &- \sum_{k=1}^{i} \mathrm{def}_\theta(w + kC_{\theta,1}) + i - j + c,\end{aligned} \tag{15}$$

where $w \in O$ *is fixed and* c *is a constant.*

Proof. Let $\theta \in \mathcal{L}_3(q)$. If $\mathrm{discr}_\theta(x) = -\mathrm{def}_\theta(x)$ then the equations of Theorem 9 become

$$\sum_{i=0}^{p-1} \mathrm{def}_\theta(x + iC_{\theta,y}) = -p, \tag{16}$$

for $y = 1, 2$ and all $x \in GF(q)$, and

$$\mathrm{def}_\theta(x + C_{\theta,1} + C_{\theta,2}) = \mathrm{def}_\theta(x), \tag{17}$$

for all $x \in GF(q)$.

Equation (17) implies that, for each orbit O of $\langle x \to x + C_{\theta,1}, x \to x + C_{\theta,2}\rangle$, G_O must be a circulant matrix, and so each row sum and each column sum must be the same, $-p$ by Equation (16). Any circulant $p \times p$ matrix with row sum $-p$ satisfies Equation (16) and Equation (17).

By induction on Equation (17) we see that

$$\mathrm{def}_\theta(x + iC_{\theta,1} + jC_{\theta,2}) = \mathrm{def}_\theta(x + (i-j)C_{\theta,1}) = \mathrm{def}_\theta(x + (j-i)C_{\theta,2}).$$

Then sum_θ can then computed using the difference equations (2).

We leave it to the reader to verify that, if θ satisfies the conditions of the theorem, then θ satisfies the conditions of Theorem 9 and hence that $\theta \in \mathcal{L}_3(q)$. □

Theorem 12. *Let the characteristic of* $GF(q)$ *be* p*,* p *odd. Let* $\theta\colon GF(q) \times GF(3) \to GF(q) \times GF(3)$ *be a bijection with first component mappings* $ax + b_y$*,* $y \in GF(3)$*,* $a \neq 0, 1$*,* $b_0 = 0$*, for which* $\{b_1, b_2\}$ *spans a 2-dimensional subspace of* $GF(q)$*, viewed as a vector space over its prime subfield, and* $\mathrm{discr}_\theta(x) = \mathrm{def}_\theta(x)$ *for all* $x \in GF(q)$*. For an orbit* O *of* $\langle x \to x + C_{\theta,1}, x \to x + C_{\theta,2}\rangle$*, let* G_O *be the* $p \times p$ *matrix with* ij*th entry* $\mathrm{def}_\theta(w + (i-1)C_{\theta,1} + (j-1)C_{\theta,2})$*, where* $w \in O$ *is fixed. Then* $\theta \in \mathcal{L}_3(q)$ *if and only if*

$p = 3$, for each orbit O of $\langle x \to x + C_{\theta,1}, x \to x + C_{\theta,2}\rangle$, each row of G_O is either $(1,1,1)$ *or* $(-1,-1,-1)$*, or each column of G_O is either* $(1,1,1)^T$ *or* $(-1,-1,-1)^T$*, and*

$$\begin{aligned}\mathrm{sum}_\theta(w + iC_{\theta,1} + jC_{\theta,2}) = \sum_{k=0}^{i-1} \mathrm{def}_\theta(w + kC_{\theta,1}) \\ - \sum_{k=1}^{i} \mathrm{def}_\theta(w + kC_{\theta,1}) + i - j + c,\end{aligned} \tag{18}$$

if each row of G_O is either $(1,1,1)$ *or* $(-1,-1,-1)$*, or*

$$\begin{aligned}\mathrm{sum}_\theta(w + iC_{\theta,1} + jC_{\theta,2}) = \sum_{k=1}^{j} \mathrm{def}_\theta(w + kC_{\theta,2}) - \\ \sum_{k=0}^{j-1} \mathrm{def}_\theta(w + kC_{\theta,2}) + i - j + c,\end{aligned} \tag{19}$$

if each column of G_O is either $(1,1,1)^T$ *or* $(-1,-1,-1)^T$*, where $w \in O$ is fixed and c is a constant.*

Proof. Let $\theta \in \mathcal{L}_3(q)$. If $\mathrm{discr}_\theta(x) = \mathrm{def}_\theta(x)$ then the equations of Theorem 9 become $p = 0$, i.e., $p = 3$, and

$$\mathrm{def}_\theta(x + C_{\theta,1} + C_{\theta,2}) + \mathrm{def}_\theta(x) = \mathrm{def}_\theta(x + C_{\theta,1}) + \mathrm{def}_\theta(x + C_{\theta,2}).$$

It is an exercise to show that this is equivalent to either each row of G_O being either $(1,1,1)$ or $(-1,-1,-1)$, or each column of G_O being either $(1,1,1)^T$ or $(-1,-1,-1)^T$, for each orbit O of $\langle x \to x + C_{\theta,1}, x \to x + C_{\theta,2}\rangle$. Then sum_θ can computed using the difference equations (2).

We leave it to the reader to verify that, if θ satisfies the conditions of the theorem, then θ satisfies the conditions of Theorem 9 and hence that $\theta \in \mathcal{L}_3(q)$. □

4 The number of orthomorphisms in $\mathcal{L}_3(q)$

In this section we will count the number of orthomorphisms in $\mathcal{L}_3(q)$. We will pay particular attention to the smallest cases of interest, in which the characteristic of $GF(q)$ is 2, 3, 5, or 7. In Section 1 we described the following automorphisms of $Orth(G)$: H_α, $\alpha \in Aut(G)$, defined by $H_\alpha[\theta] = \alpha\theta\alpha^{-1}$; T_g, $g \in G$, defined by $T_g[\theta](x) = \theta(x + g) - \theta(g)$; and R defined by $R[\theta](x) = x + \theta(-x)$. For $G = GF(q)^+ \times GF(3)^+$ we will restrict automorphisms of G to automorphisms of the form $(x, y) \mapsto (dx, ey)$, $d, e \neq 0$. These automorphisms of $Orth(G)$ turn out to be automorphisms of $\mathcal{L}_3(q)$.

Lemma 13. *If $\theta \in \mathcal{L}_3(q)$ has first component mappings $\theta_{1,y}(x) = ax + b_y$, $a \neq 0, 1$, $b_0 = 0$, then the following hold.*

1. *$R[\theta] \in \mathcal{L}_3(q)$ and has first component mappings*

$$R[\theta]_{1,y}(x) = (1-a)x + b_{-y}.$$

2. *For all $(b,c) \in GF(q)^+ \times GF(3)^+$, $T_{(b,c)}[\theta] \in \mathcal{L}_3(q)$ and has first component mappings*

$$T_{(b,c)}[\theta]_{1,0}(x), = ax;$$

$$T_{(b,c)}[\theta]_{1,1}(x) = \begin{cases} ax + b_1 & \textit{if } c = 0, \\ ax + (b_2 - b_1) & \textit{if } c = 1, \\ ax - b_2 & \textit{if } c = 2; \end{cases}$$

$$T_{(b,c)}[\theta]_{1,2}(x) = \begin{cases} ax + b_2 & \textit{if } c = 0, \\ ax - b_1 & \textit{if } c = 1, \\ ax + (b_1 - b_2) & \textit{if } c = 2; \end{cases}$$

3. *For all $\alpha \in Aut(GF(q)^+ \times GF(3)^+)$ of the form $(x,y) \mapsto (dx, ey)$,$H_\alpha[\theta] \in \mathcal{L}_3(q)$ and has first component mappings*

$$H_\alpha[\theta]_{1,y}(x) = \begin{cases} ax + db_y & \textit{if } \alpha(x,y) = (dx, y); \\ ax + db_{-y} & \textit{if } \alpha(x,y) = (dx, -y). \end{cases}$$

Proof. Routine computation. □

We will use $M_{(b_1,b_2)}$ to denote the number of orthomorphisms in $\mathcal{L}_3(q)$ with first component mappings $\theta_{1,y}(x) = ax + b_y$, $a \neq 0, 1$ and $b_0 = 0$. From the constructions in Section 3 and the actions of automorphisms of $\mathcal{L}_3(q)$ in Lemma 13 we can compute $M_{(b_1,b_2)}$ in a number of cases.

Lemma 14. *Let p be the characteristic of $GF(q)$ and let $b \in GF(q)$, $b \neq 0$. Then the following hold.*

$$M_{(0,0)} = (q-2)3^{q-1};$$

$$M_{(0,b)} = M_{(b,0)} = M_{(b,b)} = (q-2)3^{(q/p)-1};$$

$$M_{(b,2b)} = (q-2)3^{(q/p)-1}4^{q/3}, \ \textit{if } p = 3;$$

$$M_{(b,2b)} = M_{(b,((p-1)/2)b)} = M_{(b,(p-1)b)} = (q-2)3^{(q/p)-1}\left(\sum_{i \geqslant 0} \binom{p}{3i}\right)^{q/p}, \ \textit{if } p > 3;$$

and

$$M_{(b,3b)} = M_{(b,5b)} = (q-2)3^{(q/p)-1}8^{q/7}, \ \textit{if } p = 7;$$

If q is not prime, let $b, c \in GF(q)$ span a 2-dimensional subspace of $GF(q)$, viewed as a vector space over its prime subfield. Then the following hold.

$$M_{(b,c)} = (q-2)3^{(q/4)-1}5^{q/4}, \ \textit{if } p = 2;$$

$$M_{(b,c)} \geqslant (q-2)3^{(q/9)-1}4^{q/9}, \text{ if } p=3;$$

and

$$M_{(b,c)} \geqslant (q-2)3^{(q/p^2)-1}\left(\sum_{i\geqslant 0}\binom{p}{3i}\right)^{q/p^2}, \text{ if } p>3.$$

Proof. The calculation of $M_{(0,0)}$; $M_{(0,b)}$; $M_{(b,2b)}$; $M_{(b,3b)}$ for $p=7$; and $M_{(b,c)}$ is straightforward from the characterizations of orthomorphisms given in Theorems 4, 5, 6, 8, 10, 11, and 12. From the actions of automorphisms, described in Lemma 14, we see that $M_{(0,b)} = M_{(b,0)} = M_{(b,b)}$, $M_{(b,2b)} = M_{(b,((p-1)/2)b)} = M_{(b,(p-1)b)}$ if $p \neq 2,3$, and $M_{(b,3b)} = M_{(b,5b)}$ if $p=7$. □

Theorem 15. *Let p be the characteristic of $GF(q)$. The following hold.*

(i) *If $p=2$, then*

$$|\mathcal{L}_3(q)| = (q-2)3^{q-1} + (q-1)(q-2)3^{q/2} + (q-2)^2(q-1)3^{(q/4)-1}5^{q/4}.$$

(ii) *If $p=3$, then*

$$\begin{aligned}|\mathcal{L}_3(q)| \geqslant (q-2)3^{q-1} + (q-1)(q-2)3^{q/3} + (q-1)(q-2)3^{(q/3)-1}4^{q/3}\\ +(q-1)(q-2)(q-3)3^{(q/9)-1}4^{q/9}.\end{aligned}$$

(iii) *If $p=5$, then*

$$\begin{aligned}|\mathcal{L}_3(q)| \geqslant (q-2)3^{q-1} + (q-1)(q-2)3^{q/5} + (q-1)(q-2)3^{q/5}11^{q/5}\\ +(q-1)(q-2)(q-5)3^{(q/25)-1}11^{(q/25)}.\end{aligned}$$

(iv) *If $p=7$, then*

$$\begin{aligned}|\mathcal{L}_3(q)| \geqslant (q-2)3^{q-1} + (q-1)(q-2)3^{q/7} + (q-1)(q-2)3^{q/7}43^{q/7}\\ +2(q-1)(q-2)8^{q/7}3^{(q/7)-1} + (q-1)(q-2)(q-7)3^{(q/49)-1}43^{q/49}.\end{aligned}$$

(v) *If $p>7$, then*

$$\begin{aligned}|\mathcal{L}_3(q)| \geqslant (q-2)3^{q-1} + (q-1)(q-2)3^{q/p} + (q-1)(q-2)3^{(q/p)-1}\left(\sum_{i\geqslant 0}\binom{p}{3i}\right)^{q/p}\\ +(q-1)(q-2)(q-p)3^{(q/p^2)-1}\left(\sum_{i\geqslant 0}\binom{p}{3i}\right)^{q/p^2},\end{aligned}$$

Proof. If q is not prime, let $b, c \in GF(q)$ span a 2-dimensional subspace of $GF(q)$, viewed as a vector space over its prime subfield. If q is prime, let $b \in GF(q) \setminus \{0\}$ and set $M_{(b,c)} = 0$.

If $p = 2$, then

$$|\mathcal{L}_3(q)| = M_{(0,0)} + (q-1)(M_{(0,b)} + M_{(b,0)} + M_{(b,b)}) + (q-1)(q-2)M_{(b,c)}.$$

If $p = 3$, then

$$\begin{aligned}|\mathcal{L}_3(q)| = M_{(0,0)} + (q-1)(M_{(0,b)} + M_{(b,0)} + M_{(b,b)}) + (q-1)M_{(b,2b)} \\ +(q-1)(q-2)M_{(b,c)}.\end{aligned}$$

If $p = 5$, then

$$\begin{aligned}|\mathcal{L}_3(q)| = M_{(0,0)} + (q-1)(M_{(0,b)} + M_{(b,0)} + M_{(b,b)}) \\ +(q-1)(M_{(b,2b)} + M_{(b,3b)} + M_{(b,4b)}) + (q-1)(q-2)M_{(b,c)}.\end{aligned}$$

If $p = 7$, then

$$\begin{aligned}|\mathcal{L}_3(q)| = M_{(0,0)} + (q-1)(M_{(0,b)} + M_{(b,0)} + M_{(b,b)}) \\ +(q-1)(M_{(b,2b)} + M_{(b,4b)} + M_{(b,6b)}) + (q-1)(M_{(b,3b)} + M_{(b,5b)}) \\ +(q-1)(q-2)M_{(b,c)}.\end{aligned}$$

If $p > 7$, then

$$\begin{aligned}|\mathcal{L}_3(q)| \geqslant M_{(0,0)} + (q-1)(M_{(0,b)} + M_{(b,0)} + M_{(b,b)}) \\ +(q-1)(M_{(b,2b)} + M_{(b,((p-1)/2)b)} + M_{(b,(p-1)b)}) + (q-1)(q-2)M_{(b,c)}.\end{aligned}$$

The result then follows from Lemma 14. □

5 Bounds on $\omega(\mathcal{L}_3(q))$

In this section we will establish lower bounds on $\omega(\mathcal{L}_3(q))$ when q is not a power of 3. Throughout this section, for $\theta, \phi \in \mathcal{L}_3(q)$, $\mathrm{discr}_{\theta,\phi}$ will denote the discriminant function for θ by ϕ, $\mathrm{discr}_{\phi,\theta}$ will denote the discriminant function for ϕ by θ, and, if the first component mappings for θ are $ax + b_y$, $y \in GF(3)$, and the first component mappings for ϕ are $Ax + B_y$, $y \in GF(3)$, then, as in Theorem 3, $C_{\theta,\phi,y} = (aB_y - Ab_y)/(a(a-A))$, and $C_{\phi,\theta,y} = (Ab_y - aB_y)/(A(A-a))$. First let us note an easily established upper bound.

Theorem 16. *$\omega(\mathcal{L}_3(q)) \leqslant q - 2$.*

Proof. Let $\theta_1, \ldots, \theta_n$ be a pairwise orthogonal set of orthomorphisms in $\mathcal{L}_3(q)$, and let the first component mappings of θ_i be $a_i x + b_{i,y}$ for $i = 1, \ldots, n$. Then $0, 1, a_1, \ldots, a_n$ are distinct elements of $GF(q)$. The result follows. □

In [9] it was shown that $\omega(\mathbb{Z}_{3n}) \geqslant 2$ for all $n \geqslant 5$, n not divisible by 2 or 3. We will show that this result also holds for $\omega(\mathcal{L}_3(q))$ when the characteristic of $GF(q)$ is not 2 or 3. In the process we will show how the orthogonal pair of orthomorphisms, constructed in [9], can be obtained by solving the difference equations (2) and adjacency difference equations (3): this should shed light on the construction used in [9].

Theorem 17. *If $q > 2$ is a power of a prime greater than 3 then $\omega(\mathcal{L}_3(q)) \geqslant 2$.*

Proof. Let p be the characteristic of $GF(q)$. Let $\theta, \phi \colon GF(q) \times GF(3)$ be bijections; let θ have first component mappings $\theta_{1,0}(x) = 2x$, $\theta_{1,1}(x) = 2x - 2$, and $\theta_{1,2}(x) = 2x + 2$; and let ϕ have first component mappings $\phi_{1,0}(x) = -x$, $\phi_{1,1}(x) = -x - 2$, and $\phi_{1,2}(x) = -x + 2$. These are the first component mappings used in [9] for $\mathbb{Z}_{3n}$, as opposed to $GF(q)^+ \times GF(3)^+$. Simple calculations show that $C_{\theta,1} = 1 = C_{\phi,1}$ and $C_{\theta,2} = -1 = C_{\phi,2}$. Thus the difference equations (2) for θ are identical to the difference equations (2) for ϕ. Hence, we may impose the conditions $\text{sum}_\theta = \text{sum}_\phi = \text{sum}$, $\text{def}_\theta = \text{def}_\phi = \text{def}$, and $\text{discr}_\theta = \text{discr}_\phi = \text{discr}$. We will also impose the condition $\text{discr} = -\text{def}$: we leave it to the reader to show that this condition can be derived from the difference equations (2). Then the difference equations (2) for both θ and ϕ reduce to

$$\text{sum}(x+1) - \text{sum}(x) = -\text{def}(x) - \text{def}(x+1) + 1. \tag{20}$$

Equation (20) has a solution if and only if, for each orbit O of $x \mapsto x + 1$,

$$\sum_{x \in O} \text{def}(x) = -p.$$

Now $C_{\theta,\phi,1} = -1$, $C_{\theta,\phi,2} = 1$, $C_{\phi,\theta,1} = 2$ and $C_{\phi,\theta,2} = -2$, and the adjacency difference equations for θ and ϕ reduce to

$$\begin{aligned} &\text{sum}(x-1) - \text{sum}(x+2) \\ &= \text{discr}_{\theta,\phi}(x) - \text{def}(x-1) + \text{def}(x+2) \\ &= \text{discr}_{\theta,\phi}(x+1) - \text{def}(x+2) + \text{def}(x-1). \end{aligned} \tag{21}$$

Equation (20) can be used repeatedly to compute $\text{sum}(x+m) - \text{sum}(x+n)$ for all integers m and n. Doing so yields

$$\begin{aligned} \text{sum}(x+2) - \text{sum}(x-1) &= -\text{discr}_{\theta,\phi}(x) + \text{def}(x-1) - \text{def}(x+2) \\ &= -\text{discr}_{\theta,\phi}(x+1) + \text{def}(x+2) - \text{def}(x-1) \\ &= -\text{def}(x+2) + \text{def}(x+1) + \text{def}(x) - \text{def}(x-1). \end{aligned} \tag{22}$$

Thus

$$\text{discr}_{\theta,\phi}(x) = -\text{def}(x+1) - \text{def}(x) - \text{def}(x-1).$$

Hence θ can be orthogonal to ϕ if and only if $\sum_{x \in O} \text{def}(x) = -p$, for each orbit O of $x \mapsto x + 1$, i.e., $\theta, \phi \in \mathcal{L}_3(q)$; and

$$\text{def}(x) + \text{def}(x+1) + \text{def}(x+2) \neq 0$$

for all $x \in GF(q)$. Such a def exists. For example set $\mathrm{def}(w), \mathrm{def}(w+1), \ldots, \mathrm{def}(w+p-1) = 1, -1, 1, -1, \ldots, 1, -1, \epsilon$, where $\epsilon \equiv -p \pmod 3$ and w is a given element of an orbit O of $x \mapsto x+1$: this is the solution that was used in [9]. □

In [10] the result that $\omega(\mathbb{Z}_{3n}) \geqslant 2$ for all $n \geqslant 5$, n not divisible by 2 or 3, was improved to $\omega(\mathbb{Z}_{3n}) \geqslant 3$ for all $n \geqslant 5$, n not divisible by 2 or 3, $n \neq 7, 17$. This yields a better lower bound for $\omega(\mathcal{L}_3(q))$ when the characteristic of $GF(q)$ is not 2, 3, 7, or 17.

Theorem 18. *If the characteristic of $GF(q)$ is not 2, 3, 7, or 17, then*

$$\omega(\mathcal{L}_3(q)) \geqslant 3.$$

Proof. Let p be the characteristic of $GF(q)$. Let $\theta, \phi, \gamma \colon GF(q) \times GF(3)$ be bijections; let θ have first component mappings $\theta_{1,0}(x) = 2x$, $\theta_{1,1}(x) = 2x+2$, and $\theta_{1,2}(x) = 2x-2$; let ϕ have first component mappings $\phi_{1,0}(x) = -x$, $\phi_{1,1}(x) = -x+2$, and $\phi_{1,2}(x) = -x-2$; let γ have first component mappings $\gamma_{1,0}(x) = ((p+1)/2)x$, $\gamma_{1,1}(x) = ((p+1)/2)x+2$, and $\gamma_{1,2}(x) = ((p+1)/2)x-2$. These are the first component mappings used in [10] for $\mathbb{Z}_{3n}$, as opposed to $GF(q)^+ \times GF(3)^+$. Simple calculations show that $C_{\theta,1} = -1 = C_{\phi,1}$, $C_{\theta,2} = 1 = C_{\phi,2}$, $C_{\gamma,1} = -8$, $C_{\gamma,2} = -8$, $C_{\theta,\phi,1} = 1$, $C_{\theta,\phi,2} = -1$, $C_{\phi,\theta,1} = -2$, $C_{\phi,\theta,2} = 2$, $C_{\theta,\gamma,1} = 1$, $C_{\theta,\gamma,2} = -1$, $C_{\gamma,\theta,1} = 4$ and $C_{\gamma,\theta,2} = -4$, $C_{\gamma,\phi,1} = 4$, $C_{\gamma,\phi,2} = -4$, $C_{\phi,\gamma,1} = -2$, and $C_{\phi,\gamma,2} = 2$. We will impose the conditions $\mathrm{sum}_\theta = \mathrm{sum}_\phi = \mathrm{sum}$, $\mathrm{def}_\theta = \mathrm{def}_\phi = \mathrm{def}$, $\mathrm{discr}_\theta = \mathrm{discr}_\phi = -\mathrm{def}$, and $\mathrm{discr}_\gamma = -\mathrm{def}_\gamma$.

Let sum, def, sum_γ, and def_γ, restricted to $\{0, 1, \ldots, p-1\}$, be as defined in [10]. Note that in [10] sum was denoted f, def was denoted g, sum_γ was denoted f', and def_γ was denoted g'. Let $0, w_1, \ldots, w_{(q/p)-1}$ be representatives of the orbits of $x \mapsto x+1$ in $GF(q)$, and let us extend the definitions of sum, def, sum_γ, and def_γ, by setting $\mathrm{sum}(w_i + j) = \mathrm{sum}(j)$, $\mathrm{def}(w_i + j) = \mathrm{def}(j)$, $\mathrm{sum}_\gamma(w_i + j) = \mathrm{sum}_\gamma(j)$, and $\mathrm{def}_\gamma(w_i + j) = \mathrm{def}_\gamma(j)$ for $i = 1, \ldots, (q/p)-1$ and $j = 0, 1, \ldots, p-1$. These functions solve the difference equations (2) for θ, ϕ, and γ. As in the proof of Theorem 17, $\mathrm{discr}_{\theta,\phi}$, $\mathrm{discr}_{\theta,\gamma}$, and $\mathrm{discr}_{\gamma,\phi}$ can be determined from the adjacency difference equations (3). These functions satisfy the adjacency difference equations (3) for θ and ϕ, for θ and γ, and for γ and ϕ. Hence, θ, ϕ, and γ are pairwise orthogonal orthomorphisms in $\mathcal{L}_3(q)$. □

Similarly, when the characteristic of $GF(q)$ is 2, we can find solutions to the difference equations (2) and the adjacency difference equations (3) that yield orthogonal pairs of orthomorphisms in $\mathcal{L}_3(q)$.

Theorem 19. *If $q > 2$ is even, then $\omega(\mathcal{L}_3(q)) \geqslant 2$.*

Proof. There are two cases to consider, q an even power of 2, and q an odd power of 2.

Case 1. Let q an even power of 2, let a be a solution to $x^2 + x + 1 = 0$ in $GF(q)$, and let $A = a + 1$. Let $\theta, \phi \colon GF(q) \times GF(3)$ be bijections; let θ have first component mappings $\theta_{1,0}(x) = ax$, $\theta_{1,1}(x) = ax + 1$, and $\theta_{1,2}(x) = ax$;and let ϕ have first component mappings $\phi_{1,0}(x) = Ax$, $\phi_{1,1}(x) = Ax$, and $\phi_{1,2}(x) = Ax + 1$. Simple calculations show that $C_{\theta,1} = 1 = C_{\phi,2}$, $C_{\theta,2} = 0 = C_{\phi,1}$, $C_{\theta,\phi,1} = a^2 + 1$, $C_{\theta,\phi,2} = 1$, $C_{\phi,\theta,1} = 1$, and $C_{\phi,\theta,2} = a^2$.

By Theorem 5, $\mathrm{def}_\phi(x) = -1$ for all $x \in GF(q)$, $\mathrm{discr}_\phi(x) = 1$ for all $x \in GF(q)$, and sum_ϕ is constant on orbits of $x \mapsto x + 1$. A similarly proof to that of Theorem 5 shows that $\mathrm{def}_\theta(x) = -1$ for all $x \in GF(q)$, $\mathrm{discr}_\theta(x) = 1$ for all $x \in GF(q)$, and sum_θ is constant on orbits of $x \mapsto x + 1$.

Let us impose the condition $\mathrm{sum}_\theta = \mathrm{sum}_\phi = \mathrm{sum}$. It is clear that $\theta, \phi \in \mathcal{L}_3(q)$ if and only if $\mathrm{sum}(0) = 0$, sum is constant on orbits of $x \mapsto x + 1$, and $\mathrm{def}_\theta(x) = \mathrm{def}_\phi(x) = -1$ for all $x \in GF(q)$.

With these conditions on θ and ϕ, the adjacency difference equations (3) are

$$\mathrm{sum}(x + a^2 + 1) - \mathrm{sum}(x + 1) = \mathrm{discr}_{\theta,\phi}(x),$$

and

$$\mathrm{sum}(x + 1) - \mathrm{sum}(x + a^2) = -\mathrm{discr}_{\theta,\phi}(x).$$

These two equations are equivalent as sum is constant on orbits of $x \mapsto x + 1$. It follows from these equations that θ and ϕ are orthogonal if $\mathrm{sum}(x + a^2) \neq \mathrm{sum}(x)$ for all $x \in GF(q)$. Set $H = \{0, 1, a^2, 1+a^2\}$. H is a subgroup of $GF(q)^+$. let $0 = w_0, w_1, \ldots, w_{(q/4)-1}$ be a system of coset representatives for H in $GF(q)^+$, and set $\mathrm{sum}(w_i) = \mathrm{sum}(w_i+1) = 0$ and $\mathrm{sum}(w_i + a^2) = \mathrm{sum}(w_i + a^2 + 1) = 1$ for $i = 0, \ldots, (q/4) - 1$. With this choice of sum, θ and ϕ are orthogonal orthomorphisms in $\mathcal{L}_3(q)$.

Case 2. Let q be an odd power of 2, let $a^2 + a + 1 \neq 0$ and let $A = a + 1$. Let $\theta, \phi, \gamma \colon GF(q) \times GF(3)$ be bijections; let θ have first component mappings $\theta_{1,0}(x) = ax$, $\theta_{1,1}(x) = ax + a^2 + a$, $\theta_{1,2}(x) = ax$; and let ϕ have first component mappings $\phi_{1,0}(x) = Ax$, $\phi_{1,1}(x) = Ax$, $\phi_{1,2}(x) = Ax + a^2 + a$. Simple calculations show that $C_{\theta,1} = 1 = C_{\phi,2}$, $C_{\theta,2} = 0 = C_{\phi,1}$, $C_{\theta,\phi,1} = a^2 + 1$, $C_{\theta,\phi,2} = a^2 + a$, $C_{\phi,\theta,1} = a^2 + a$, and $C_{\phi,\theta,2} = a^2$. As in the case q an even power of 2, we can show that $\mathrm{def}_\theta(x) = -1$ for all $x \in GF(q)$, $\mathrm{discr}_\theta(x) = 1$ for all $x \in GF(q)$, $\mathrm{def}_\phi(x) = -1$ for all $x \in GF(q)$, $\mathrm{discr}_\phi(x) = 1$ for all $x \in GF(q)$, sum_θ is constant on orbits of $x \mapsto x + 1$, and sum_ϕ is constant on orbits of $x \mapsto x + 1$. As in the case q an even power of 2, we will impose the condition $\mathrm{sum}_\theta = \mathrm{sum}_\phi = \mathrm{sum}$. It is clear that $\theta, \phi \in \mathcal{L}_3(q)$ if and only if $\mathrm{sum}(0) = 0$, sum is constant on orbits of $x \mapsto x + 1$, and $\mathrm{def}_\theta(x) = \mathrm{def}_\phi(x) = -1$ for all $x \in GF(q)$.

With these conditions on θ and ϕ, the adjacency difference equations (3) are

$$\mathrm{sum}(x + a^2 + 1) - \mathrm{sum}(x + a^2 + a) = \mathrm{discr}_{\theta,\phi}(x),$$

and

$$\mathrm{sum}(x + a^2 + a) - \mathrm{sum}(x + a^2) = -\mathrm{discr}_{\theta,\phi}(x).$$

These two equations are equivalent as sum is constant on orbits of $x \mapsto x + 1$. It follows from these equations that θ and ϕ are orthogonal if $\mathrm{sum}(x+a) \neq \mathrm{sum}(x)$ for all $x \in GF(q)$. Set $H = \{0, 1, a, 1 + a\}$. H is a subgroup of $GF(q)^+$. let $0 = w_0, w_1, \ldots, w_{(q/4)-1}$ be a system of coset representatives for H in $GF(q)^+$, and set $\mathrm{sum}(w_i) = \mathrm{sum}(w_i+1) = 0$ and $\mathrm{sum}(w_i + a) = \mathrm{sum}(w_i + a + 1) = 1$ for $i = 0, \ldots, (q/4) - 1$. With this choice of sum, θ and ϕ are orthogonal orthomorphisms in $\mathcal{L}_3(q)$. □

The smallest example, where $q = 4$, is given in Figure 1, where an element of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ is denoted ijk, $i, j = 0, 1$, and $k = 0, 1, 2$. A pair of orthogonal orthomorphisms of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ was first found via a computer search (see [6]): subsequent computer searches (see [3] or [14]) improved this to four pairwise orthogonal orthomorphisms.

x	000	010	100	110	001	011	101	111	002	012	102	112
$\theta(x)$	000	111	010	101	100	012	110	002	001	112	011	102
$\phi(x)$	000	101	110	011	002	100	112	010	102	001	012	111

Figure 1: Orthogonal orthomorphisms in $\mathcal{L}_3(4)$.

References

[1] R. J. R. Abel, C. J. Colbourn, and J. H.Dinitz. Mutually orthogonal latin squares (MOLS). In: Colbourn, C.J., Dinitz, J.H. (eds) *Handbook of Combinatorial Designs*, 2nd. edition, 160–193. Chapman & Hall/CRC, Florida, 2007.

[2] R. J. R. Abel, N. J. Finizio, G. Ge, and M. Greig. New $\mathbb{Z}$-cyclic triplewhist frames and triplewhist tournament designs. *Discrete Appl. Math.* 154: 1649–1673, 2006.

[3] R. C. Bose, I. M. Chakravarti, and D. E. Knuth, D.E. On methods of constructing sets of mutually orthogonal latin squares using a computer. I. *Technometrics* 2: 507–516, 1960.

[4] C. J. Colbourn and J. H. Dinitz (eds). Handbook of combinatorial designs, 2nd edition, Chapman and Hall, CRC, Florida, 2007.

[5] J. Dénes and A. D. Keedwell. Latin squares and their applications, 2nd. edition, North Holland, Amsterdam, 2015.

[6] A. L. Dulmage, D. Johnson, and N. S. Mendelsohn. Orthogonal latin squares: preliminary report. *Can. Math. Bull.* 2: 211–216, 1959.

[7] A. B. Evans. Orthomorphism graphs of groups, Lecture Notes in Mathematics *1535*, Springer-Verlag, New York, 1992.

[8] A. B. Evans. Latin squares based on the cyclic group of order $3p$. In *Proc. Eighth Internat. Conf. on Graph Theory, Combinatorics, Algorithms and Applications* (Kalamazoo, Michigan, 1996), 379–386, New Issues Press, Michigan, 1999.

[9] A. B. Evans. On orthogonal orthomorphisms of cyclic and non-abelian groups. *Discrete Math.* 243: 229–233, 2002.

[10] A. B. Evans. On orthogonal orthomorphisms of cyclic and non-abelian groups. II. *Journal of Combin. Designs* 15: 195–209, 2007.

[11] A. B. Evans. Complete mappings and sequencings of finite groups. In: Colbourn, C.J., Dinitz, J.H. (eds) *Handbook of Combinatorial Designs*, 2nd. edition, 345–352. Chapman & Hall/CRC, Florida, 2007.

[12] D. F. Hsu (ed.). Advances in Discrete Mathematics and Computer Science, Volume **I**, Neofields and Combinatorial Designs, Hadronic Press, Nonantum, Mass., 1985.

[13] D. F. Hsu (ed.). Advances in Discrete Mathematics and Computer Science, Volume **II**, Generalized Complete Mappings, Hadronic Press, Nonantum, Mass., 1987.

[14] D. M. Johnson, A. L. Dulmage, and N. S. Mendelsohn. Orthomorphisms of groups and orthogonal latin squares.I. *Canad. J. Math.* 13: 356–372, 1961.

[15] C. F. Laywine and G. L. Mullen. Discrete Mathematics using latin squares, Wiley, New York, 1998.

[16] P. J. Schellenberg, G. H. J. Van Rees, and S. A. Vanstone. Four pairwise orthogonal latin squares of order 15. *Ars Combinatoria* 6: 141–150, 1978.

[17] A. Winterhof. Generalizations of complete mappings of finite fields and some applications. *J. Symbolic Comput.* 64: 42–52, 2014.