Quasigroups and Related Systems **23** (2015), 5 − 30

Applications of complete mappings and orthomorphisms of finite groups

Anthony B. Evans

Abstract. For a finite group G a permutation of G is a *complete mapping* of G if the mapping $g \mapsto g\theta(g)$ is a permutation, and an *orthomorphism* of G if the mapping $g \mapsto g^{-1}\theta(g)$ is a permutation. Complete mappings of a finite group G correspond to transversals of the Cayley table M of G, and orthomorphisms of G correspond to permutations of the columns of M that yield latin squares orthogonal to M.

Complete mappings and orthomorphisms have been used in constructions of mutually orthogonal sets of latin squares and in constructions of latin squares with particular properties. They and related mappings have also been used in many other algebraic and combinatorial constructions. In this paper we will survey the applications of complete mappings, orthomorphisms, near complete mappings, and near orthomorphisms in the construction of orthogonal latin squares, group sequencings, and neofields.

1. Introduction

Let G be a finite group and let $\theta\colon G \to G$ be a permutation. We call θ a *complete mapping* of G if the mapping $\sigma\colon g \mapsto g\theta(g)$ is a permutation, an *orthomorphism* of G if the mapping $\delta\colon g \mapsto g^{-1}\theta(g)$ is a permutation, and a *strong complete mapping* of G if it is both a complete mapping and an orthomorphism of G. Complete mappings and orthomorphisms are very closely related as a permutation θ is a complete mapping of G if and only if the mapping $g \mapsto g\theta(g)$ is an orthomorphism of G and an orthomorphism of G if and only if the mapping $g \mapsto g^{-1}\theta(g)$ is a complete mapping of G. While either complete mappings or orthomorphisms can be used in applications, we will see that in some applications one is more natural than the other. For example, in describing transversals of latin squares complete mappings are more natural, whereas in constructing mutually orthogonal latin squares by permuting the columns of the Cayley table of a finite group orthomorphisms are more natural. In the special case in which G is the additive group of the finite field $GF(q)$, any permutation of G can be represented by a permutation polynomial of $GF(q)$. Those permutation polynomials that represent orthomorphisms are called *orthomorphism polynomials*, and those permutation polynomials that represent complete mappings are called *complete mapping polynomials* or *complete permu-*

2010 Mathematics Subject Classification: 05B15
Keywords: Complete mapping, orthomorphism, orthogonal latin square, group sequencing, neofield.

tation polynomials. A complete mapping or orthomorphism θ of G is said to be *normalized* or in *canonical form* if $\theta(1) = 1$. If θ is a complete mapping (orthomorphism) of G, then the mapping $\theta_0 \colon g \mapsto \theta(g)\theta(1)^{-1}$ is a normalized complete mapping (orthomorphism) of G: θ_0 is the *normalization* of θ.

Closely related to complete mappings and orthomorphisms are near complete mappings and near orthomorphisms, mappings that just fail to be complete mappings or orthomorphisms. By a *near complete mapping* of G we mean a bijection $\theta : G \setminus \{h\} \to G \setminus \{1\}$, $h \neq 1$, for which the mapping $\sigma : g \mapsto g\theta(g)$ is a bijection $\theta : G \setminus \{h\} \to G \setminus \{k\}$, for some $k \in G$, $k \neq h$. A *near orthomorphism* of G is a bijection $\theta : G \setminus \{h\} \to G \setminus \{1\}$, $h \neq 1$, for which the mapping $\delta \colon g \mapsto g^{-1}\theta(g)$ is a bijection $\theta : G \setminus \{h\} \to G \setminus \{k\}$, for some $k \in G$, $k \neq h^{-1}$. A near complete mapping (near orthomorphism) θ is *normalized* or in *canonical form* if $k = 1$, in which case h is the *exdomain element* of θ. Near complete mappings and near orthomorphisms are closely related as, if θ is a normalized near complete mapping with exdomain element h, then the mapping $g \mapsto g\theta(g)$ is a normalized near orthomorphism with exdomain element h; and, if θ is a normalized near orthomorphism with exdomain element h, then the mapping $g \mapsto g^{-1}\theta(g)$ is a normalized near complete mapping with exdomain element h.

In Section 2 we will discuss the relationship between complete mappings of groups and transversals of the Cayley tables of groups; and we will also discuss the use of orthomorphisms in constructing sets of mutually orthogonal latin squares. In Section 3 we will discuss group sequencings and its variations that can be constructed using (near) complete mappings or (near) orthomorphisms; and in Section 4 we wlll discuss the use of orthomorphisms and near orthomorphisms in the construction of neofields.

2. Latin squares and orthogonality

Complete mappings and orthomorphisms were first introduced in constructions of sets of mutually orthogonal latin squares (MOLS). Complete mappings were introduced by Mann [44] in 1944; and orthomorphisms were introduced by Johnson, Dulmage and Mendelsohn [36] in 1961, and under the name orthogonal mappings by Bose, Chakravarti, and Knuth [6] in 1960. A *latin square of order* n is an $n \times n$ matrix with entries chosen from a set of n *symbols*, such that each symbol appears exactly once in each row and exactly once in each column. Latin squares in general are covered in the books by Dénes and Keedwell ([12] and [13]) and the forthcoming book by Keedwell [42]. Two latin squares of the same order are *orthogonal* if each ordered pair of symbols appears exactly once when the squares are superimposed: each square is then an *orthogonal mate* of the other. A set of k *mutually orthogonal latin squares* (MOLS) of order n is a set of k latin squares of order n, each pair of which is orthogonal. We use $N(n)$ to denote the largest k for which a set of k MOLS of order n exists.

The following is well-known.

Theorem 1. *If $n > 1$, then the following hold.*

(1) $1 \leqslant N(n) \leqslant n-1$.

(2) $N(n) = 1$ *if and only if* $n = 2$ *or* $n = 6$.

(3) *If n is a prime power, then* $N(n) = n-1$.

Proof. See [12] for instance. □

For $n > 1$, a set of $n-1$ MOLS of order n is a *complete sets of MOLS* of order n. A set of k MOLS of order n is *maximal* if it cannot be extended to a larger set of MOLS of order n. A table of lower bounds for $N(n)$ up to $n = 10,000$ can be found in [11].

Cayley ([9] and [10]) pointed out that the multiplication/addition table of a group is a latin square. Let $G = \{g_1, \dots, g_n\}$ be a group of order n. The *Cayley table* M of G is the $n \times n$ matrix with ijth entry $g_i g_j$, and for θ a permutation of G, M_θ denotes the $n \times n$ matrix with ijth entry equal to $g_i\theta(g_j)$. It is easy to see that M is a latin square, and that M_θ is obtained from M by permuting columns.

2.1. Complete mappings and transversals. A set of cells in a latin square, exactly one in each row and exactly one in each column, whose entries are distinct is called a *transversal* of the latin square. The transversals of a latin square determine whether the square has an orthogonal mate or not. To see this, let L_1 and L_2 be an orthogonal pair of latin squares and let a be a symbol in L_2: the cells in L_1 corresponding to cells in L_2 with entry a form a transversal in L_1. The set of transversals of L_1 corresponding to the symbols of L_2 partitions the cells of L_1. We obtain the following.

Theorem 2. *A latin square possesses an orthogonal mate if and only if its cells can be partitioned by transversals.*

For the Cayley table M of a finite group G, a single transversal suffices.

Theorem 3. *The Cayley table M of a finite group G possesses an orthogonal mate if and only if it possesses a transversal.*

Proof. Let $G = \{g_1, \dots, g_n\}$ and let M be the Cayley table of G. If M does not possess a transversal, then it does not possess an orthogonal mate by Theorem 2.

Let us assume that M does possess a transversal. Let $\phi_k\colon \{1, \dots, n\} \to \{1, \dots, n\}$ be defined by $\phi_k(j) = t$ if $g_j g_k = g_t$, and let the ij_ith cells of M, $i = 1, \dots, n$ form a transversal T. For $k = 1, \dots, n$, let T_k consist of the $i\phi_k(j_i)$th cells of M, $i = 1, \dots, n$. Then $T_1, \dots, T_n$ are transversals of M that partition the cells of M. It follows that M possesses an orthogonal mate by Theorem 2. □

There is a natural correspondence between complete mappings of a group and transversals of its Cayley table.

Theorem 4. *There is a on-one correspondence between the complete mappings of a finite group G and the transversals of the Cayley table M of G.*

Proof. Let $G = \{g_1, \dots, g_n\}$ and let M be the Cayley table of G. Let T be a transversal of M consisting of the ij_ith cells of M, $i = 1, \dots, n$, n the order of G, and define $\theta\colon G \to G$ by $\theta(g_i) = g_{j_i}$. Then θ is a complete mapping of G and this correspondence establishes a bijection between the set of complete mappings of G and the set of transversals of M. □

To illustrate the proof of Theorem 4, Figure 1 shows a pair of orthogonal latin squares of order 7. The square M is the Cayley table of $\mathbb{Z}_7 = \{0, 1, 2, \dots, 6\}$, the operation being addition modulo 7. The entries of the cells in M corresponding to the cells in L with entry 3 are shown in italics: these cells clearly form a transversal of M. Let us define $\theta\colon \mathbb{Z}_7 \to \mathbb{Z}_7$ by $\theta(i) = j$ if the ijth entry of M is italicized: this mapping, depicted in Figure 2, is a complete mapping of $\mathbb{Z}_7$.

$$M = \begin{pmatrix} 0 & \textit{1} & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & \textit{0} \\ 2 & 3 & 4 & \textit{5} & 6 & 0 & 1 \\ \textit{3} & 4 & 5 & 6 & 0 & 1 & 2 \\ 4 & 5 & \textit{6} & 0 & 1 & 2 & 3 \\ 5 & 6 & 0 & 1 & \textit{2} & 3 & 4 \\ 6 & 0 & 1 & 2 & 3 & \textit{4} & 5 \end{pmatrix}, \quad L = \begin{pmatrix} 0 & 3 & 6 & 1 & 5 & 4 & 2 \\ 1 & 4 & 0 & 2 & 6 & 5 & 3 \\ 2 & 5 & 1 & 3 & 0 & 6 & 4 \\ 3 & 6 & 2 & 4 & 1 & 0 & 5 \\ 4 & 0 & 3 & 5 & 2 & 1 & 6 \\ 5 & 1 & 4 & 6 & 3 & 2 & 0 \\ 6 & 2 & 5 & 0 & 4 & 3 & 1 \end{pmatrix}$$

Figure 1: A pair of orthogonal latin squares of order 4.

i	0	1	2	3	4	5	6
$\theta(i)$	1	6	3	0	2	4	5
$i + \theta(i)$	1	0	5	3	6	2	4

Figure 2: A complete mapping of $\mathbb{Z}_7$.

Finite groups that admit complete mappings have been characterized.

Theorem 5. *The Cayley table of a finite group G possesses a transversal, equivalently a finite group G admits complete mappings, if and only if the Sylow 2-subgroup of G is either trivial or noncyclic.*

Proof. See [7], [20], [26], and [60]. □

As an immediate corollary to Theorems 3 and 5 we obtain the following.

Corollary 1. *The Cayley table of a finite group G possesses an orthogonal mate if and only if the Sylow 2-subgroup of G is either trivial or noncyclic.*

The literature contains many results on the number of complete mappings of small groups. Computer searches have confirmed and extended earlier results. In particular in 2004 Hsiang, Hsu, and Shieh [30] computed the number of complete mappings of $\mathbb{Z}_n$ for $n \leqslant 23$; and in 2006 McKay, McLeod, and Wanless [45] computed the number of complete mappings for all groups of order at most 23.

2.2. Orthomorphisms and MOLS. Let us reconsider the pair of orthogonal latin squares shown in Figure 1. We know that M is the Cayley table of $\mathbb{Z}_7$ and we observe that L can be obtained from M by permuting columns. This permutation ϕ, essentially the first row of L as a permutation of the first row of M, is shown in Figure 3: it is an orthomorphism of $\mathbb{Z}_7$.

i	0	1	2	3	4	5	6
$\phi(i)$	0	3	6	1	5	4	2
$\phi(i) - i$	0	2	4	5	1	6	3

Figure 3: An orthomorphism of $\mathbb{Z}_7$.

Theorem 6. *If M is the Cayley table of a finite group G and θ a permutation of G, then M_θ is orthogonal to M if and only if θ is an orthomorphism of G. If θ and ϕ are two permutations of G, then M_θ and M_ϕ are orthogonal if and only if the mapping $g \mapsto \phi(g)^{-1}\theta(g)$ is a permutation of G.*

Proof. Routine. □

We say that two mappings $\theta, \phi \colon G \to G$ are *orthogonal* if the mapping $g \mapsto \phi(g)^{-1}\theta(g)$ is a permutation. Thus a mapping $\theta \colon G \to G$ is a complete mapping of G if it is orthogonal to the mappings $g \mapsto 1$ and $g \mapsto g^{-1}$, and an orthomorphism if it is orthogonal to the mapping $g \mapsto 1$ and the identity mapping $g \mapsto g$. Orthogonality is a symmetric relationship. Note that, if θ and ϕ are orthomorphisms of G and θ_0 and ϕ_0 are their respective normalizations, then θ and ϕ are orthogonal if and only if θ_0 and ϕ_0 are orthogonal. By Theorem 6, pairwise orthogonal sets of orthomorphisms can be used to construct MOLS.

Corollary 2. *From r pairwise orthogonal orthomorphisms of a group of order $n > 1$ we can construct a set of $r + 1$ MOLS of order n.*

Proof. Let M be the Cayley table of a group G of order $n > 1$, and let $\theta_1, \ldots, \theta_r$ be a pairwise orthogonal set of orthomorphisms of G.Then the squares $M, M_{\theta_1}, \ldots, M_{\theta_r}$ form a set of $r + 1$ MOLS of order n. □

2.3. Complete sets of MOLS. While complete sets of MOLS of prime power order were known long before the introduction of complete mappings and orthomorphisms, they are easily constructed from pairwise orthogonal sets of orthomorphisms.

Corollary 3. *If q is a prime power, then there exists a complete set of MOLS of order q.*

Proof. Let $G = GF(q)^+$, the additive group of the field of order q. Then the mappings $x \mapsto ax$, $a \neq 0, 1$, form a set of $q-2$ pairwise orthogonal orthomorphisms of G from which the result follows. □

The orthomorphisms used in the proof of Corollary 3 are called *linear orthomorphisms* and are represented by the orthomorphism polynomials ax, $a \neq 0, 1$, of $GF(q)$.

We define $\omega(G)$ to be the largest possible order of a set of pairwise orthogonal orthomorphisms of G. Theorems 1 and Corollary 2 yield bounds on $\omega(G)$ when $|G| > 1$.

Theorem 7. *If $|G| = n > 1$, then $0 \leqslant \omega(G) \leqslant n - 2$.*

By Theorem 5, the lower bound in Theorem 7 can be improved to 1 if the Sylow 2-subgroup of G is either trivial or noncyclic. By the proof of Corollary 3 the upper bound in Theorem 7 is achieved when G is elementary abelian.

For a group G of order $n > 2$ a set of $n-2$ pairwise orthogonal orthomorphisms of G is called a *complete set of orthomorphisms* of G. By Corollary 2, a complete set of orthomorphisms of a group G of order n yields a complete set of MOLS of order n.

It is well-known that a complete set of MOLS of order n corresponds to a projective plane of order n: see [11, 12, 13]. A *projective plane* is an incidence structure in which two distinct points are incident with exactly one line, two distinct lines meet in exactly one point, and there exist four points, no three of which are collinear. By removing one line of the projective plane and all the points on this line we obtain an *affine plane*. If π is a finite projective plane, then for some $n > 1$, each line of π is incident with $n + 1$ points, and each point of π is incident with $n+1$ lines: n is the *order* of π and also the *order* of the corresponding affine plane. Given a group G of order n and a complete set of orthomorphisms $\theta_1, \ldots, \theta_{n-2}$ of G we can construct an affine plane of order n as follows. Without loss of generality we may assume that $\theta_1, \ldots, \theta_{n-2}$ are normalized. Treat G as an additive group with identity 0 whether abelian or not. We next form an affine plane $\mathcal{A}$ of order n. The points of $\mathcal{A}$ are the ordered pairs (x, y), $x, y \in G$. The lines of $\mathcal{A}$ are described by the equations $y = b$, $b \in G$; $y = x + b$, $b \in G$; $y = \theta_i(x) + b$, $b \in G$, $i = 1, \ldots, n-2$; and $x = c$, $c \in G$. Each class of equations describes a *parallel class* of $\mathcal{A}$. A *collineation* of a affine plane is a permutation of the points of the plane that preserves lines, and a *translation* of an affine plane is a collineation that fixes all parallel classes and fixes all the lines of a given parallel class. For each $g \in G$ the mapping $\tau_g \colon (x, y) \mapsto (x, y + g)$ is a translation of $\mathcal{A}$, and the set $\{\tau_g \mid g \in G\}$ is a group of translations of $\mathcal{A}$ that is transitive on the points of any line $x = c$. This construction can be reversed.

Theorem 8. *An affine plane admits a group G of translations that fixes all lines of a given parallel class and is transitive on the points of a line of this parallel class if and only if G admits a complete set of orthomorphisms.*

If a projective plane is constructed from a complete set of orthomorphisms of a group G, then the corresponding projective plane is (P, l)-transitive for some line l and some point P on l, the corresponding collineation group being isomorphic to G: see [11, 12, 13] for the definition of (P, l)-transitivity. The only groups known to admit complete sets of orthomorphisms are the elementary abelian groups. An unsolved problem:

Problem 1. *Does there exist a group G, $|G| = n > 1$, which is not elementary abelian, that admits a complete set of orthomorphisms?*

In particular, as it has long been conjectured that all finite affine and projective planes are of prime power order, we might ask:

Problem 2. *Does there exist a group G, $|G| = n > 1$, n not a prime power, that admits a complete set of orthomorphisms?*

While many finite projective planes can be constructed from complete sets of orthomorphisms, this approach is rarely used in the study of finite projective planes. As an example, translation planes are the projective planes that can be constructed from complete sets of orthomorphisms, each of which is a fixed-point-free automorphism of an elementary abelian group. However, translation planes are usually constructed from other algebraic structures such as spreads and quasifields. There are, however, some instances in which orthomorphisms have been used to establish the nonexistence of certain affine and projective planes. In 1973 Baumert and Hall [4] showed that no projective plane of order 10 or 12, if such existed, could be (P, l)-transitive for any point P on any line l: for the plane of order 10, this result can be derived from Theorem 5. In 1972 Studnicka [58] showed that no projective plane of order $2p^m$, if such existed, could be (P, l)-transitive for any point P on any line l: this result can also be derived from Theorem 5. In 2004 Lazebnik and Thomason [43], using orthomorphisms and a computer, were able to construct 3 of the 4 known projective planes of order 9 and 16 of the 22 known projective planes of order 16: they found no new projective planes.

It has long been conjectured that, if p is a prime, then there is only one affine (projective) plane of order p. This plane can be constructed from the linear orthomorphisms used in the proof of Corollary 3. It was shown in 1984 by Evans and McFarland [23] that the existence of a complete set of normalized orthomorphisms of $\mathbb{Z}_p$, p a prime, that are not all linear, would imply the existence of at least two affine (projective) planes of order p.

Theorem 9 (Evans, McFarland, 1984)**.** *If, for a prime p, there exists more than one complete set of normalized orthomorphisms of $\mathbb{Z}_p$, then there exists more than one affine (projective) plane of order p.*

Problem 3. *Does there exist more than one complete set of normalized orthomorphisms of $\mathbb{Z}_p$ for any prime p?*

For primes 7 or less, Problem 3 is easily answered by hand: the answer is no. In 1961, via a computer search, Johnson, Dulmage, and Mendelsohn [36] showed that there was only one complete set of normalized orthomorphisms of $\mathbb{Z}_{11}$. Subsequent computer searches confirmed this; by Cates and Killgrove [8] in 1981; by Evans and McFarland [23] in 1984; and by Lazebnik and Thomason [43] in 2004. For $\mathbb{Z}_{13}$, in 1981 Cates and Killgrove [8] used a computer search to show that there was only one complete set of normalized orthomorphisms of this group. This was confirmed via computer searches by Mendelsohn and Wolk [46] in 1985, and by Lazebnik and Thomason [43] in 2004.

An alternative approach to searching for other complete sets of normalized orthomorphisms of $\mathbb{Z}_p$, p prime, was tried by Mendelsohn and Wolk [46] in 1985. They restricted themselves to quadratic orthomorphisms. For q an odd prime power, the *quadratic orthomorphism* $[A, B]$ of $GF(q)^+$ is defined by

$$[A,B](g) = \begin{cases} 0 & \text{if } g = 0, \\ Ag & \text{if } g \text{ is a nonzero square}, \\ Bg & \text{if } g \text{ is a nonsquare}, \end{cases}$$

where AB and $(A-1)(B-1)$ are both nonzero squares. Note that the quadratic orthomorphism $[A, B]$ of $GF(q)^+$ is represented by the orthomorphism polynomial $ax^{(q+1)/2} + bx$, where $a = (A - B)/2$ and $b = (A + B)/2$. The orthomorphism of $\mathbb{Z}_7$, depicted in Figure 3, is the quadratic orthomorphism $[3, 5]$. Mendelsohn and Wolk showed by a computer search that there is only one complete set of quadratic orthomorphisms of $GF(13)^+$ and of $GF(17)^+$, that is the known complete set of linear orthomorphisms. In 1987 Evans [14] extended this result to all primes $p \leqslant 47$ using simple hand calculations, and in 1989 Evans [15] extended this result to all primes.

2.4. Lower bounds for $N(n)$. A number of the best lower bounds for $N(n)$ have been obtained using difference matrices. For G a group of order n an $(n, r; \lambda)$-*difference matrix* over G is an $r \times \lambda n$ matrix $D = (d_{ij})$ with entries from G such that for any $i, k \in \{1, \ldots, r\}$, $i \neq k$, each element of G appears λ times in the form $d_{ij}^{-1} d_{kj}$. We call λ the *index* of D. An $(n, r; \lambda)$-*difference matrix* can be transformed into another $(n, r; \lambda)$-*difference matrix* by permuting columns, permuting rows, multiplying all the elements of a row on the right by an element of G, and multiplying all the elements of a column on the left by an element of G. Employing these operations we may transform any difference matrix into a *normalized* difference matrix, that is, one in which every entry in the first row and first column is the identity. Given a normalized $(n, r; 1)$-*difference matrix* over a group G, the second row is a listing of the elements of G and the third through rth rows, regarded as permutations of the second row, form a set of $r - 2$ pairwise orthogonal normalized orthomorphisms of G: this construction can be reversed.

Table 1 shows some of the lower bounds for $N(n)$ that have been obtained from difference matrices with the corresponding groups: this data is from [11].

n	$N(n) \geqslant$	The group
12	5	$GF(3)^+ \times GF(4)^+$
15	4	$GF(3)^+ \times GF(5)^+$
21	5	$GF(3)^+ \times GF(7)^+$
24	7	$GF(3)^+ \times GF(8)^+$
28	5	$GF(4)^+ \times GF(7)^+$
33	5	$GF(3)^+ \times GF(11)^+$
35	5	$GF(5)^+ \times GF(7)^+$
36	8	$GF(4)^+ \times GF(9)^+$
39	5	$GF(3)^+ \times GF(13)^+$
40	7	$GF(5)^+ \times GF(8)^+$
44	5	$GF(4)^+ \times GF(11)^+$
45	6	$GF(5)^+ \times GF(9)^+$
48	8	$GF(3)^+ \times GF(16)^+$

Table 1: MOLS from groups.

Problem 4. *For a finite group G determine $\omega(G)$ or improve bounds on $\omega(G)$.*

Problem 4 has only been completely answered for small groups, elementary abelian groups (see Corollary 3), and for groups with nontrivial, cyclic Sylow 2-subgroups (See Theorem 5).

2.5. Maximal sets of MOLS. Given a maximal set of pairwise orthogonal orthomorphisms of a group finite G, is the corresponding set of MOLS also maximal? The answer to this question is yes. This was implicitly proved by Ostrom [50] in 1966 in the language of nets.

Theorem 10 (Ostrom, 1966)**.** *Let G be a finite group of order n and let M be its Cayley table. If $\theta_1, \ldots, \theta_r$ is a maximal set of pairwise orthogonal orthomorphisms of G, then M, M_{θ_1}, …, M_{θ_r} is a maximal set of MOLS of order n.*

As an example, the orthomorphism of $\mathbb{Z}_7$, depicted in Figure 3, is not orthogonal to any other orthomorphism of $\mathbb{Z}_7$. Hence, by Theorem 10, the latin squares in Figure 1 form a maximal set of 2 MOLS of order 7. A difference matrix over a group G is *maximal* if it cannot be extended to a larger difference matrix over G by adding rows. As a corollary to Theorem 10 we obtain the following.

Corollary 4. *If there exists a maximal $(n, r; 1, G)$-difference matrix, then there exists a maximal set of $r - 1$ MOLS of order n.*

All maximal $(n, r; 1, G)$-difference matrices over groups of order at most 10 were determined by Jungnickel and Grams [37] in 1986. In 1991 Evans [17] generalized Corollary 4.

Theorem 11 (Evans, 1991). *If there exists an $(n, r; 1, G)$-difference matrix D for which $mD = (D \ldots D)$, i.e., m consecutive copies of D, is maximal and if either $m = 1$ or there exist a set of $r - 1$ MOLS of order m, then there exists a maximal set of $r - 1$ MOLS of order nm.*

Theorem 11 was used to prove the following.

Theorem 12 (Evans, 1991). *If $n = mp^r$, p a prime,* $\gcd(m, p) = 1$, *and either $m = 1$ or there exist a set of $p - 1$ MOLS of order m then there exists a maximal set of $p - 1$ MOLS of order n.*

The proof of Theorem 12 was obtained by generalizing the construction of a maximal set of $p - 2$ pairwise orthogonal orthomorphisms of $\mathbb{Z}_{p^r}$, p a prime. In 1992 Evans [18] used quadratic orthomorphisms to construct two infinite classes of maximal sets of MOLS.

Theorem 13 (Evans, 1992). *Let $p \geqslant 7$ be a prime.*

(1) *If $p \equiv 3 \pmod 4$, then there exists a maximal set of $(p - 3)/2$ MOLS of order p.*

(2) *If $p \equiv 1 \pmod 4$, then there exists a maximal set of $(p - 1)/2$ MOLS of order p.*

The maximal sets of MOLS, constructed in Theorem 13, are obtained from maximal sets of pairwise orthogonal orthomorphisms of $GF(p)^+$ that are constructed in the following way. If p is a prime and $[A, B]$ is a nonlinear, quadratic orthomorphism of $GF(p)^+$, then $[A, B]$ is orthogonal to precisely $(p-7)/2$ linear orthomorphisms of $GF(p)^+$, forming a set of $(p-5)/2$ pairwise orthogonal orthomorphisms of $GF(p)^+$. If $p \equiv 3 \pmod 4$, then this set is maximal. If $p \equiv 1 \pmod 4$, then $[B, A]$ must be included yielding a maximal set of $(p-3)/2$ pairwise orthogonal orthomorphisms of $GF(p)^+$. As examples, $[7, 7], [8, 8], [2, 6]$ is a maximal set of 3 pairwise orthogonal orthomorphisms of $GF(11)^+$, and $[6, 6], [7, 7], [10, 10], [2, 5]$, $[5, 2]$ is a maximal set of 5 pairwise orthogonal orthomorphisms of $GF(13)^+$.

In 1993 Pott [54] gave a simpler proof of Theorem 13 using a result of Rédei. Using a computer and cyclotomic orthomorphisms, a generalization of quadratic orthomorphisms, Pott found a maximal set of 2 MOLS of order 13, a maximal set of 4 MOLS of order 13, a maximal set of 3 MOLS of order 17, a maximal set of 4 MOLS of order 17, a maximal set of 3 MOLS of order 19, and a maximal set of 6 MOLS of order 19.

2.6. Strong complete mappings and Knut Vic designs. Let $G = \{g_1, \ldots, g_n\}$ be a group of order n. The *normal multiplication table* of G is the $n \times n$ array with ijth entry $g_i g_j^{-1}$. Strong complete mappings are important in determining the existence of latin squares orthogonal to both N and the Cayley table M of G.

Theorem 14. *Let G be a finite group with Cayley table M and normal multiplication table N. There exists a latin square orthogonal to both M and N if and only if G admits a strong complete mapping.*

Proof. See [22]. □

In fact, if θ is a strong complete mapping of G, then M_θ is orthogonal to both M and N. In the special case $G = \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, any latin square L orthogonal to both the Cayley table of G and the normal multiplication table of G is a *Knut Vic design*: these are characterized by each broken left and right diagonal being a transversal.

Problem 5. *Which finite groups admit strong complete mappings?*

Problem 5 was implicitly solved for cyclic groups in papers by Hedayat and Federer [28] in 1975 and Hedayat [27] in 1977.

Theorem 15 (Hedayat, Federer, 1975 & 1977)**.** *$\mathbb{Z}_n$ admits strong complete mappings if and only if* $\gcd(n, 6) = 1$.

As a consequence of Theorem 5, if the Sylow 2 subgroup of a finite group G is nontrivial and cyclic, then G cannot admit strong complete mappings. In 1990 Evans [16] and Horton [29] showed that the structure of the Sylow 3-subgroup also plays a role in determining the existence of strong complete mappings.

Theorem 16. *If a finite group G has a nontrivial, cyclic Sylow 3-subgroup that is a homomorphic image of G, then G does not admit strong complete mappings.*

The special case of Theorem 16, G abelian, was proved by Horton and the general case by Evans. For finite abelian groups the existence of strong complete mappings is completely determined by the structure of the Sylow 2-subgroups and the Sylow 3-subgroups: this was proved by Evans [21] in 2012.

Theorem 17 (Evans, 2012)**.** *A finite abelian group with a trivial or noncyclic Sylow 2-subgroup and a trivial or noncyclic Sylow 3-subgroup admits strong complete mappings.*

In light of Theorem 5, it is natural to ask whether it is true that a finite group with a nontrivial, cyclic Sylow 3-subgroup does not admit strong complete mappings. The answer to this question was shown to be no by Shieh, Hsiang, and Hsu [57], who described a strong complete mapping of D_{12}, the dihedral group of order 12. Since then, Evans [22] has shown a number of classes of dihedral groups and quaternion groups to admit strong complete mappings, as well as most groups of order at most 31. Let $D_{4k} = \langle a, b \mid a^{2k} = b^2 = 1, ab = ba^{-1} \rangle$ denote the dihedral group of order $4k$, and $Q_{4k} = \langle a, b \mid a^{2k} = 1, b^2 = a^k, bab^{-1} = a^{-1} \rangle$ the quaternion group of order $4k$. Evans' results are given in Theorems 18, 19, and 20.

Theorem 18. *D_8 does not admit strong complete mappings. If* $\gcd(m, 6) = 1$, *then D_{4m}, D_{12m}, D_{16m}, and D_{24m} admit strong complete mappings.*

Similar results hold for the quaternion groups.

Theorem 19. *Q_8 does not admit strong complete mappings. If $\gcd(m,6)=1$, then Q_{16m} and Q_{24m} admit strong complete mappings.*

The following is the result of a computer search for strong complete mappings.

Theorem 20. *All groups of order at most 31 admit strong complete mappings with the following exceptions:*

(1) *any group with nontrivial, cyclic Sylow 2-subgroups,*
(2) *any group G with a nontrivial, cyclic Sylow 3-subgroup that is a homomorphic image of G,*
(3) *D_8, and*
(4) *Q_8.*

3. Group labeling problems

In this section we will discuss group sequencings, which can be constructed from a class of near complete mappings: these arose in the construction of complete latin squares. We will also discuss two variants of group sequencings, R-sequencings and harmonious orderings, both of which can be constructed from classes of orthomorphisms.

3.1. Group sequencings. A *sequencing* of a group G of order n is an ordering $a_0=1, a_1, a_2, \ldots, a_{n-1}$ of the elements of G such that the *partial products* $b_0=a_0=1$, $b_1=a_0a_1$, $b_2=a_0a_1a_2$ $, \ldots, b_{n-1}=a_0a_1a_2\cdots a_{n-1}$ are distinct. We say that a group is *sequenceable* if it possesses a sequencing.

Group sequencings were introduced by Gordon [25] in 1961 in the construction of complete latin squares. A latin square $L=\{l_{ij}\}$ of order n is *row complete* if the $n(n-1)$ ordered pairs $(l_{ij}, l_{i,j+1})$, $i=1,\ldots,n$ and $j=1,\ldots,n-1$, are distinct, *column complete* if the $n(n-1)$ ordered pairs $(l_{ij}, l_{i+1,j})$, $i=1,\ldots,n-1$ and $j=1,\ldots,n$, are distinct, and *complete* if it is both row complete and column complete.

Theorem 21 (Gordon, 1961). *Let $a_0, a_1, a_2, \ldots, a_{n-1}$ be a sequencing of a group G of order n and let $b_0, b_1, b_2, \ldots, b_{n-1}$ be the corresponding sequence of partial products. Then the $n\times n$ matrix with ijth entry $\{b_i^{-1}b_j\}$ is a complete latin square of order n.*

Proof. See Theorem 2 in [25]. □

Example 1. *Let $0,1,8,3,6,5,4,7,2,9$ be an ordering of the elements of $\mathbb{Z}_{10}$. As the partial sums $0,1,9,2,8,3,7,4,6,5$ are distinct this is a sequencing of $\mathbb{Z}_{10}$. The associated complete latin square is shown in Figure 4.*

The sequencing of Example 1 can be generalized: the ordering

$$0,1,-2,3,-4,\ldots,2n-3,-(2n-2),2n-1$$

is a sequencing of $\mathbb{Z}_{2n}$ as the partial sums are

$$0, 1, -1, 2, -2, \ldots, n-1, -(n-1), n.$$

$$\begin{pmatrix}
0 & 1 & 9 & 2 & 8 & 3 & 7 & 4 & 6 & 5 \\
9 & 0 & 8 & 1 & 7 & 2 & 6 & 3 & 5 & 4 \\
1 & 2 & 0 & 3 & 9 & 4 & 8 & 5 & 7 & 6 \\
8 & 9 & 7 & 0 & 6 & 1 & 5 & 2 & 4 & 3 \\
2 & 3 & 1 & 4 & 0 & 5 & 9 & 6 & 8 & 7 \\
7 & 8 & 6 & 9 & 5 & 0 & 4 & 1 & 3 & 2 \\
3 & 4 & 2 & 5 & 1 & 6 & 0 & 7 & 9 & 8 \\
6 & 7 & 5 & 8 & 4 & 9 & 3 & 0 & 2 & 1 \\
4 & 5 & 3 & 6 & 2 & 7 & 1 & 8 & 0 & 9 \\
5 & 6 & 4 & 7 & 3 & 8 & 2 & 9 & 1 & 0
\end{pmatrix}$$

Figure 4: A complete latin square of order 10.

It should be noted that the complete latin square in Figure 4 can be obtained from the Cayley table of $\mathbb{Z}_{10}$ by permuting rows and columns. This was observed by Keedwell [38] in 1976.

Theorem 22. *A complete latin square can be obtained from the Cayley table of a finite group G, by permuting rows and columns, if and only if G is sequenceable.*

From a sequencing of a group we can construct a near complete mapping of the group.

Theorem 23. *Let $a_0, a_1, a_2, \ldots, a_{n-1}$ be a sequencing of a group G of order n and let $b_0, b_1, b_2, \ldots, b_{n-1}$ be the partial products. Define $\theta\colon G \setminus \{b_{n-1}\} \to G \setminus \{1\}$ by*

$$\theta(b_i) = a_{i+1}, i = 0, \ldots, n-2.$$

Then θ is a near complete mapping of G with exdomain element b_{n-1}.

Proof. First note that $\{b_0, \ldots, b_{n-2}\} = G \setminus \{b_{n-1}\}$.

Now

$$\{\theta(b_0), \ldots, \theta(b_{n-2})\} = \{a_1, \ldots, a_{n-1}\} = G \setminus \{1\}$$

and

$$\{b_0\theta(b_0), \ldots, b_{n-2}\theta(b_{n-2})\} = \{b_1, \ldots, b_{n-1}\} = G \setminus \{1\},$$

from which the result follows. □

As an example, the near complete mapping derived from the sequencing of $\mathbb{Z}_{10}$, described in Example 1, is shown in Figure 5. The exdomain element of this near complete mapping is 5.

g	0	1	2	3	4	5	6	7	8	9
$\theta(g)$	1	8	6	4	2	.	9	7	5	3
$g+\theta(g)$	1	9	8	7	6	.	5	4	3	2

Figure 5: A near complete mapping from a sequencing of $\mathbb{Z}_{10}$.

Just as the cycle $(c_0\ c_1\ \cdots\ c_{k-1})$ is used to represent the mapping $c_i \mapsto c_{i+1}$, $i = 0, \ldots, k-1$, the subscripts being added modulo k, the sequence $[c_0\ c_1\ \cdots\ c_{k-1}]$ is used to denote the mapping is used to represent the mapping $c_i \mapsto c_{i+1}$, $i = 0, \ldots, k-2$. Any complete mapping, orthomorphism, near complete mapping, or near orthomorphism can be written as a product of disjoint cycles and sequences. The near orthomorphism, $g \mapsto g+\theta(g)$, associated with the near complete mapping in Figure 5 can be written as the sequence [0 1 9 2 8 3 7 4 6 5].

In 1984 Hsu and Keedwell [34] characterized the normalized near orthomorphisms from which group sequencings can be constructed.

Theorem 24 (Hsu, Keedwell, 1984). *A group G of order n is sequenceable if and only if it admits a normalized near orthomorphism that consists of one sequence of length n.*

Proof. Let $a_0, a_1, a_2, \ldots, a_{n-1}$ be a sequencing of a group G of order n and let $b_0, b_1, b_2, \ldots, b_{n-1}$ be the partial products. Then $[b_0\ b_1\ \cdots\ b_{n-1}]$ is a normalized near orthomorphism of G.

If $[b_0\ b_1\ \cdots\ b_{n-1}]$ is a normalized near orthomorphism of G, then setting

$$a_i = \begin{cases} 1 & \text{if } i = 0, \\ b_{i-1}^{-1} b_i & \text{if } i = 1, \ldots, n-1, \end{cases}$$

yields a sequencing $a_0, \ldots, a_{n-1}$ of G. □

Problem 6. *Which groups are sequenceable?*

Problem 6 was answered for abelian groups by Gordon [25] in 1961.

Theorem 25 (Gordon, 1961). *An abelian group is sequenceable if and only if it has a unique element of order* 2.

Proof. See Theorem 1 in [25]. □

The situation is different for nonabelian groups. Order 10 appears to be a dividing line.

Theorem 26. *No nonabelian group of order less than* 10 *is sequenceable.*

Proof. See Gordon [25]. □

However, the nonabelian group of order 10, the dihedral group $D_{10} = \langle a, b \mid a^5 = b^2 = 1, ab = ba^{-1}\rangle$ is sequenceable. $1, ba, a^4, ba^2, b, ba^4, a^2, a, ba^3, a^3$ is a sequencing for this group. In 1983 Keedwell [40] conjectured that nonabelian groups of order less that 10 were the only nonsequenceable nonabelian groups.

Conjecture 1 (Keedwell). *All nonabelian groups of order at least* 10 *are sequenceable.*

Keedwell's conjecture has been proved true for many classes of groups.

Theorem 27 (Anderson, 1987). *All nonabelian groups of order n, $10 \leqslant n \leqslant 32$ are sequenceable.*

Proof. See [1] and [2]. □

Theorem 28 (Anderson, 1987). *A_5 and S_5 are sequenceable.*

Proof. See [1]. □

The proof that the dihedral groups satisfy Keedwell's conjecture is the result of work by several mathematicians, whose work is described in the dynamic survey [49] by Ollis.

Theorem 29. *The dihedral group of order $2n$, D_{2n}, $n \geqslant 5$, is sequenceable.*

There are a number of results for binary groups: a group is *binary* if it has exactly one involution. Theorem 25 can be restated as, a finite abelian group is sequenceable if and only if it is a binary group. Keedwell's conjecture has been proved for binary solvable groups.

Theorem 30 (Anderson and Ihrig, 1993). *All binary solvable groups, except the quaternion group of order* 8*, are sequenceable.*

Proof. See [3]. □

Anderson and Ihrig actually proved the stronger result that solvable groups with a unique element of order 2 are symmetrically sequenceable. A *symmetric sequencing* of a group G of order $2n$, with a unique element u of order 2, is a sequencing $a_0 = 1, a_1, a_2, \dots, a_{2n-1}$ of G for which $a_n = u$ and $a_{n-i} = a_{n+i}^{-1}$, $i = 1, 2, \dots, n-1$. A group is *symmetrically sequenceable* if it possesses a symmetric sequencing. A number of other groups have been shown to be sequenceable including many binary groups and groups of odd order: see [49] for details.

3.2. R-sequencings. An *R-sequencing* of a group G of order n is an ordering $a_0 = 1, a_1, a_2, \dots, a_{n-1}$ of the elements of G such that the *partial products* $b_0 = a_0 = 1$, $b_1 = a_0a_1$, $b_2 = a_0a_1a_2$ $, \dots, b_{n-2} = a_0a_1a_2\cdots a_{n-2}$ are distinct and $a_0a_1a_2\cdots a_{n-1} = 1$. A group is *R-sequenceable* if it possesses an R-sequencing. R-sequencings were introduced by Paige [53] in 1951 as a sufficient condition for a group to admit complete mappings, equivalently orthomorphisms. they were also used by Ringel [55] in 1974 in his solution of the map coloring problem for all compact 2-dimensional manifolds except the sphere. Note that in and R-sequencing of a finite group G exactly one element of G does not appear as a partial product.

Theorem 31. *Let $a_0, a_1, a_2, \ldots, a_{n-1}$ be an R-sequencing of a group G of order n, let $b_0, b_1, b_2, \ldots, b_{n-2}$ be the corresponding sequence of partial products, and let c be the element of G that is not in the list of partial products. Then, the mapping $\theta\colon G \to G$ defined by*

$$\theta(g) = \begin{cases} b_{i+1} & \textit{if } g = b_i, i = 0, 1, \ldots, n-3, \\ b_0 & \textit{if } g = b_{n-2}, \\ c & \textit{if } g = c, \end{cases}$$

is an orthomorphism of G.

Proof. Routine. □

An immediate consequence of Theorems 5 and 31.

Corollary 5. *If G is a finite R-sequenceable group, then its Sylow 2 subgroup is either trivial or non-cyclic.*

As an example $0, 12, 2, 10, 4, 8, 6, 5, 9, 3, 11, 1, 7$ is an R-sequencing of $\mathbb{Z}_{13}$. The partial sums are $0, 12, 1, 11, 2, 10, 3, 8, 4, 7, 5, 6$, missing 9. The associated orthomorphism is shown in Figure 6.

g	0	1	2	3	4	5	6	7	8	9	10	11	12
$\theta(g)$	12	11	10	8	7	6	0	5	4	9	3	2	1
$\theta(g) - g$	12	10	8	5	3	1	7	11	9	0	6	4	2

Figure 6: An orthomorphism of $\mathbb{Z}_{13}$.

The orthomorphism in Figure 6 is the cycle (0 12 1 11 2 10 3 8 4 7 5 6). In 1984 Hsu and Keedwell [34] characterized the normalized orthomorphisms from which R-sequencings can be constructed.

Theorem 32 (Hsu, Keedwell, 1984)**.** *A group G of order n is R-sequenceable if and only if it admits a normalized orthomorphism that consists of one cycle of length $n-1$.*

Proof. Similar to the proof of Theorem 24. □

Problem 7. *Which finite groups are R-sequenceable?*

Cyclic groups of odd order were shown to be R-sequenceable groups by Friedlander, Gordon, and Miller [24] in 1978.

Theorem 33 (Friedlander, Gordon and Miller, 1978)**.** *If n is odd, then $\mathbb{Z}_n$ is R-sequenceable.*

Proof.

$$\begin{gathered}0, -1, 2, -3, 4, \ldots, -(2n-1), 2n, 2n-1, -(2n-2),\\ 2n-3, -(2n-4), \ldots, 3, -2, 1, -2n\end{gathered}$$

is an R-sequencing of $\mathbb{Z}_{4n+1}$, and

$$\begin{gathered}0, -1, 2, -3, 4, \ldots, -(2n-1), 2n, -(2n+2), 2n+3,\\ -(2n+4), \ldots, -4n, 4n+1, -(4n+2), 2n+2\end{gathered}$$

is an R-sequencing of $\mathbb{Z}_{4n+3}$. □

There are many other classes of R-sequenceable groups known: see Ollis [49].

3.3. Harmonious groups. A *harmonious ordering* of a group G of order n is an ordering $a_0 = 1, a_1, a_2, \ldots, a_{n-1}$ of the elements of G such that the products a_0a_1, a_1a_2, $a_2a_3, \ldots,$ $a_{n-1}a_0$ are distinct. G is a *harmonious* group if it possesses a harmonious ordering. Harmonious groups were introduced by Beals, Gallian, Headley, and Jungreis [5] in 1991.

Theorem 34. *If $a_0 = 1, a_1, a_2, \ldots, a_{n-1}$ is a harmonious ordering of a group G, of order n, then the mapping $a_i \mapsto a_ia_{i+1}$, indices added modulo n, is an orthomorphism of G.*

Proof. Routine. □

As an example, $0, 1, 2, \ldots, n-1$ is a harmonious ordering of $\mathbb{Z}_n$ if n is odd. The associated orthomorphism is $i \mapsto 2i + 1$. Note that this orthomorphism is not normalized, and that its associated complete mapping $i \mapsto i + 1$ is a cycle of length n. Beals, Gallian, Headley, and Jungreis characterized complete mappings from which harmonious orderings can be constructed.

Theorem 35. *A group G of order n is harmonious if and only if it admits a complete mapping that consists of one cycle of length n.*

Proof. Routine. □

An immediate corollary of Theorems 5 and 34.

Corollary 6. *Finite groups with nontrivial cyclic 2-groups are not harmonious.*

Beals, Gallian, Headley, and Jungreis [5] discovered an additional class of non-harmonious groups.

Theorem 36 (Beals, Gallian, Headley, and Jungreis, 1991)**.** *The additive group of the finite field $GF(2^n)$ is not harmonious.*

Problem 8. *Which finite groups are harmonious?*

Beals, Gallian, Headley, and Jungreis [5] completely characterized finite abelian harmonious groups and showed all groups of odd order to be harmonious.

Theorem 37 (Beals, Gallian, Headley, and Jungreis, 1991)**.** *Groups of odd order are harmonious.*

Theorem 38 (Beals, Gallian, Headley, and Jungreis, 1991)**.** *Abelian groups, except $GF(2^n)^+$, with trivial or noncyclic 2-groups, are harmonious.*

In addition, several dihedral and quaternion groups have been shown to be harmonious: See Ollis [49]

4. Neofields

Neofields were first introduced in 1949 by Paige [52]: they were also the subject of his 1947 Ph.D thesis [51]. A *left neofield* is a set N with two binary operations, addition and multiplication, satisfying the following:

1. The elements of N form a loop under addition, with identity 0.
2. The nonzero elements of N form a group under multiplication, with identity 1.
3. The left distributive law holds: $a(b+c) = ab + ac$ for all $a, b, c \in N$.

A left neofield is called a *neofield* if the right distributive law is also satisfied. For a neofield or left neofield we will use N^+ to denote the additive loop and N^* to denote the multiplicative group of nonzero elements.

Loops that can be the additive loop of a left neofield can be characterized by their automorphism groups.

Theorem 39. *A loop can be the additive loop of a left neofield if and only if it admits an automorphism group that acts sharply transitively on its nonidentity elements.*

Proof. Let N be a left neofield and, for each $g \in N^*$, define $\tau_g \colon N \to N$ by $\tau_g(a) = ga$. Then $\{\tau_g \mid g \in N^*\}$ is an automorphism group of N^+ that acts sharply transitively on the nonzero elements of N.

Conversely, let L be a loop written additively with identity 0. Let us assume that G is an automorphism group of L that acts sharply transitively on the nonzero elements of L. We will use G to define multiplication on L. Pick a nonzero element of L and denote it 1 and for each nonzero element $a \in L$, let τ_a denote the unique element of G satisfying $\tau_a(1) = a$. Define multiplication on L by:

$$ab = \begin{cases} 0 & \text{if } \ a = 0 \text{ or } b = 0, \\ \tau_a(b) & \text{if } \ a, b \neq 0. \end{cases}$$

With this multiplication L is a left neofield. □

An *automorphism* of a left neofield N is a bijection $\alpha : N \to N$ for which $\alpha(a+b) = \alpha(a)+\alpha(b)$, and $\alpha(ab) = \alpha(a)\alpha(b)$, for all $a, b \in N$. Clearly the automorphism group $Aut(N)$ of a left neofield N is a subgroup of the automorphism group of N^*, as well as a subgroup of the automorphism group of N^+.

4.1. Orthomorphisms and near orthomorphisms. The *presentation function* of a left neofield N is the mapping $\theta\colon N \to N$ defined by $\theta(x) = 1 + x$. A left neofield N is complete determined by its multiplicative group N^* and its presentation function θ as, if $a, b \neq 0$, then

$$a + b = a(1 + a^{-1}b) = a\theta(a^{-1}b).$$

The presentation function of a left neofield N is essentially an orthomorphism or near orthomorphism of N^* depending on whether $1 + 1 = 0$ in N or not. Bruck (see [52], Theorem I.1) implicitly established the connection between neofields with multiplicative group G and orthomorphisms and near orthomorphisms of G. Later in 1984 Hsu and Keedwell [34] generalized this result to establish a correspondence between left neofields with multiplicative group G and orthomorphisms and near orthomorphisms of G. Neofields in which $1 + 1 = 0$ can be constructed from orthomorphisms.

Theorem 40 (Hsu, Keedwell, 1984). *Let G be a group, written multiplicatively with identity* 1, *let θ be a normalized orthomorphism of G, and define $\theta'\colon G\cup\{0\} \to G \cup \{0\}$ by*

$$\theta'(g) = \begin{cases} 0 & \textit{if } \ g = 1, \\ 1 & \textit{if } \ g = 0, \\ \theta(g) & \textit{if } \ g \neq 0, 1. \end{cases}$$

Then θ' is the presentation function of a left neofield in which $1 + 1 = 0$.

Proof. Let $N = G \cup \{0\}$ and define addition and multiplication in N as follows. Multiplication is as in G except that $0a = a0 = 0$ for all $a \in N$. To define addition,

$$x + y = \begin{cases} y & \text{if } \ x = 0, \\ x\theta'(x^{-1}y) & \text{if } \ x \neq 0. \end{cases}$$

N is then a left neofield, with presentation function θ', in which $1 + 1 = 0$. □

This construction can be reversed.

Theorem 41 (Hsu, Keedwell, 1984). *Let θ be the presentation function of a left neofield, in which $1 + 1 = 0$, with multiplicative group G. Define $\theta'\colon G \to G$ by*

$$\theta'(g) = \begin{cases} 1 & \textit{if } \ g = 1, \\ \theta(g) & \textit{if } \ g \neq 1. \end{cases}$$

Then θ' is a normalized orthomorphism of G.

Proof. Routine. □

The constructions of Theorems 40 and 41 establish a one-one correspondence.

Corollary 7. *There is a one to one correspondence between the set of normalized orthomorphisms of a group G and the set of left neofields, in which $1+1=0$, with multiplicative group G.*

Neofields in which $1+1\neq 0$ can be constructed from near orthomorphisms.

Theorem 42 (Hsu, Keedwell, 1984)**.** *Let G be a group, written multiplicatively with identity 1, let θ be a normalized near orthomorphism of G, with exdomain element t, and define $\theta'\colon G\cup\{0\}\to G\cup\{0\}$ by*

$$\theta'(g)=\begin{cases}0 & \textit{if } \ g=t,\\ 1 & \textit{if } \ g=0,\\ \theta(g) & \textit{if } \ g\neq 0,t.\end{cases}$$

Then θ' is the presentation function of a left neofield in which $1+t=0$.

Proof. Similar to the proof of Theorem 40. □

This construction can be reversed.

Theorem 43 (Hsu, Keedwell, 1984)**.** *If θ is the presentation function of a left neofield, in which $1+t=0$, $t\neq 1$, with multiplicative group G, then θ, restricted to $G\setminus\{t\}$, is a normalized near orthomorphism of G with exdomain element t.*

Proof. Similar to the proof of Theorem 41. □

The constructions of Theorems 42 and 43 establish a one-one correspondence.

Corollary 8. *There is a one to one correspondence between normalized near orthomorphisms of a group G and left neofields, in which $1+1\neq 0$, with multiplicative group G.*

4.2. Properties of left neofields. We have associated to each neofield N a normalized orthomorphism of N^* if $1+1=0$ or a normalized near orthomorphism with exdomain element t if $1+t=0$ and $t\neq 1$. Thus properties of neofields and their additive loops can, in principle, be determined from their associated normalized orthomorphisms or normalized near orthomorphisms.

For normalized orthomorphisms of a group G the following maps will prove useful. For $\alpha\in Aut(G)$ the *homology* H_α is defined by $H_\alpha[\theta]=\alpha\theta\alpha^{-1}$; the *reflection* R is defined by $R[\theta](x)=x\theta(x^{-1})$; and the *inversion* I is defined by $I[\theta](x)=\theta^{-1}(x)$. All of these mappings map normalized orthomorphisms to normalized orthomorphisms. Homologies, and reflections preserve orthogonality, but inversion does not. However, if θ is a normalized orthomorphism, then there is a one-one correspondence between the normalized orthomorphisms orthogonal to θ and the normalized orthomorphisms orthogonal to $I[\theta]$ that preserves orthogonality. For more information about these and other mappings that map orthomorphisms into orthomorphisms see [19].

For normalized near orthomorphisms these same maps will be useful. The homologies and reflection are defined as for normalized orthomorphisms, but inversion must be defined differently. If θ is a normalized near orthomorphism of a group G with exdomain element t, then $I[\theta]$ is defined by $I[\theta](x) = t^{-1}\theta^{-1}(tx)$. The exdomain element for H_α is $\alpha(t)$, and the exdomain element for both $R[\theta]$ and $I[\theta]$ is t^{-1}.

Theorem 44. *When acting on the set of normalized orthomorphisms of a group, the following relationships hold between homologies, reflection and inversion.*

(1) $H_\alpha H_\beta = H_{\alpha\beta}$,
(2) $R^2 = 1$,
(3) $H_\alpha R = RH_\alpha$,
(4) $I^2 = 1$,
(5) $H_\alpha I = IH_\alpha$,
(6) $(IR)^3 = 1$.

Proof. Routine. □

The relationships in Theorem 44 still hold for actions on the set of normalized near orthomorphisms of a group except, possibly, for the last $(IR)^3 = 1$. If θ is a normalized near orthomorphism with exdomain element t, then $(IR)^3[\theta] = \theta$ if $t \in Z(G)$ and $t^2 = 1$.

The homologies that fix the normalized orthomorphism or normalized near orthomorphism associated with a left neofield determine automorphisms of the left neofield and instances of the right distributive law.

Theorem 45. *Let θ be a normalized orthomorphism or normalized near orthomorphism of a group G, let N be the left neofield constructed from θ, and let $\alpha \in Aut(G)$.*

(1) *α extends to an automorphism of N, by setting $\alpha(0) = 0$, if and only if $H_\alpha[\theta] = \theta$.*
(2) *If $\alpha(x) = c^{-1}xc$ then $H_\alpha[\theta] = \theta$ if and only if $(a+b)c = ac + bc$ for all $a, b \in N$.*

Proof. (1). If $a, b \neq 0$ then $\alpha(a+b) = \alpha(a) + \alpha(b)$ if and only if $\alpha(a\theta(a^{-1}b)) = \alpha(a)\theta(\alpha(a^{-1}b))$ if and only if $\alpha(\theta(a^{-1}b)) = \theta(\alpha(a^{-1}b))$. By setting $x = \alpha(a^{-1}b)$, this is seen to be true if and only if $\alpha\theta\alpha^{-1}(x) = \theta(x)$. Hence the result.

(2). If any of a, b, or c is zero then $(a+b)c = ac + bc$. If $a, b, c \neq 0$ then $(a+b)c = a\theta(a^{-1}b)c$ and $ac + bc = ac\theta(c^{-1}a^{-1}bc)$ and $a\theta(a^{-1}b)c = ac\theta(c^{-1}a^{-1}bc)$ if and only if $H_\alpha[\theta] = \theta$. □

An immediate corollary.

Corollary 9. *If N is the left neofield constructed from a normalized orthomorphism or a normalized near orthomorphisms θ of a group G, then*

$$Aut(N) = \{\alpha \in Aut(G) \mid H_\alpha[\theta] = \theta\}.$$

Theorem 45 yields a characterization of those normalized orthomorphisms and normalized near orthomorphisms that correspond to neofields.

Corollary 10. *Let θ be a normalized orthomorphism or normalized near orthomorphism of a group G, and let N be the left neofield constructed from θ. Then N is a neofield if and only if $H_\alpha[\theta] = \theta$ for all $\alpha \in Inn(G)$.*

Corollary 11. *If θ is a normalized near orthomorphism of a group G with exdomain element t corresponding to a neofield, then the $t \in Z(G)$.*

Proof. By Corollary 10, $H_\alpha[\theta] = \theta$ for all $\alpha \in Inn(G)$. As the exdomain element of $H_\alpha[\theta]$ is $\alpha(t)$, $\alpha(t) = t$ for all $\alpha \in Inn(G)$. The result follows. □

Let N be a left neofield. N is *commutative* if N^+ is commutative and *abelian* if N^* is abelian. N has the *right inverse property* if for all $a \in N$ there exists $(-a)_R \in N$ such that $(x + a) + (-a)_R = x$ for all $x \in N$. N has the *left inverse property* if for all $a \in N$ there exists $(-a)_L \in N$ such that $(-a)_L + (a + x) = x$ for all $x \in N$. N has the inverse property if it has both the left and right inverse properties. N has the exchange inverse property if for all $a \in N$ there exists $(-a)_L \in N$ such that $(-a)_L + (x + a) = x$ for all $x \in N$. If a left neofield N is constructed from a normalized orthomorphism or normalized near orthomorphism θ, then the properties N satisfies are determined by which elements of $\langle R, I\rangle$ fix θ.

Lemma 1. *Let N be a left neofield in which $1+t = 0$, $t \neq 1$. If N is commutative, satisfies the left inverse property, or satisfies the right inverse property, then $t^2 = 1$.*

Proof. If N is commutative, then $t + 1 = 0$ and so $t(1 + t^{-1}) = 0$, from which it follows that $t^{-1} = t$.

If N has the right inverse property then $(-t)_R = 1$ as $(1 + t) + (-t)_R = 1$ and then $(0 + t) + 1 = 0$, which again implies that $t^2 = 1$.

If N has the left inverse property then $(-1)_L = t$ as $(-1)_L + (1 + t) = t$ and then $t + (1 + 0) = 0$, which again implies that $t^2 = 1$. □

Theorem 46. *Let θ be a normalized orthomorphism of a group G, or a normalized near orthomorphism of G with exdomain element t, and let N be the left neofield constructed from θ.*

(1) *N is commutative if and only if $R[\theta] = \theta$.*

(2) *If $t \in Z(G)$ then N has the right inverse property if and only if $IRI[\theta] = \theta$.*

(3) *N has the left inverse property if and only if $I[\theta] = \theta$.*

(4) *If $t \in Z(G)$ then N has the inverse property if and only if $I[\theta] = \theta$ and $IRI[\theta] = \theta$.*

(5) *N has the exchange inverse property if and only if $RI[\theta] = \theta$.*

Proof. We will give the proof for the special case θ a normalized orthomorphism: thus $a + a = 0$ for all $a \in N$. The proof for the case θ a normalized near orthomorphism is similar except that it requires Lemma 1.

N is commutative if and only if $a + b = b + a$, for all $a, b \neq 0$, if and only if $a\theta(a^{-1}b) = b\theta(b^{-1}a)$, for all $a, b \neq 0$, if and only if $\theta(a^{-1}b) = (a^{-1}b)\theta((a^{-1}b)^{-1})$, for all $a, b \neq 0$, if and only if $R[\theta](a^{-1}b) = \theta(a^{-1}b)$, for all $a, b \neq 0$, if and only if $R[\theta] = \theta$.

If N has the right inverse property, then, as $(0+a)+(-a)_R = 0$, $(-a)_R = a$. If $a, x \neq 0$, then $(x + a) + a = x$ if and only if $\theta(\theta(x^{-1}a)^{-1}x^{-1}a) = \theta(x^{-1}a)^{-1}$ if and only if $\theta(y\theta^{-1}(y^{-1})) = y$, where $y = \theta(x^{-1}a)^{-1}$, if and only if $y\theta^{-1}(y^{-1}) = \theta^{-1}(y)$ if and only if $RI[\theta](y) = I[\theta](y)$ if and only if $IRI[\theta] = \theta$.

A similar proof shows that N has the left inverse property if and only if $I[\theta] = \theta$.

N has the inverse property if and only if N has both the right and left inverse properties, if and only if $I[\theta] = \theta$ and $IRI[\theta] = \theta$.

If N has the exchange inverse property then $(-a)_L = a$. If $a, x \neq 0$, then $a + (x + a) = x$ if and only if $a\theta(a^{-1}x\theta(x^{-1}a)) = x$ if and only if $RI[\theta](a^{-1}x) = \theta(a^{-1}x)$, if and only if $RI[\theta] = \theta$. □

Further correspondences between the properties of neofields and properties of the corresponding near orthomorphisms can be found in [39]. These properties were used in Hsu [31] in 1980 to classify cyclic neofields, i.e. neofields in which the multiplicative group is cyclic.

5. Final remarks

This survey of applications of complete mappings and orthomorphisms, and the related near complete mappings and near orthomorphisms is not exhaustive. We have tended to emphasize applications in which there is a clear relationship between properties of the mappings and properties of the algebraic and combinatorial structures constructed from them.

In Section 3, there are a number of variants of group sequencings that we did not cover: symmetrically harmonious orderings, R^*-sequencings, and 2-sequencings for instance. Readers interested in pursuing these topics should consult Ollis [49] or the chapter on sequenceable and R-sequenceable groups in Dénes and Keedwell's book [13].

Readers who want to know more about neofields should consult the papers by Hsu and Keedwell [34, 35] or the more recentpaper by Keedwell [41].

A number of applications are described in the papers in the reprint volumes [32, 33], edited by Hsu, and in the papers by Hsu and Keedwell [34, 35]. Other applications include the construction of Bol loops by Niederreiter and Robinson [48], Mittenthal's [47] use of orthomorphic mappings in cryptography, Wanless' [59] use of cyclotomic orthomorphisms in the construction of atomic latin squares, and Shaheen and Winterhof's [56] use of complete permutation polynomials to construct check digit systems.

References

[1] **B.A. Anderson**, *S_5, A_5 and all non-abelian groups of order* 32 *are sequenceable*, Congr. Numer. **58** (1987), 53–68.

[2] **B.A. Anderson**, *A fast method for sequencing low order non-abelian groups*, Ann. Discrete Math. **34** (1987), 27–42.

[3] **B.A. Anderson and E.C. Ihrig**, *Every finite solvable group with a unique element of order two, except the quaternion group, has a symmetric sequencing*, J. Combin. Des. **1** (1993), 3–14.

[4] **L. Baumert and M. Hall Jr.**, *Nonexistence of certain planes of order* 10 *and* 12, J. Combin. Theory Ser. A **14** (1973), 273–280.

[5] **R. Beals, J.A. Gallian, P. Headley and D. Jungreis**, *Harmonious groups*, J. Combin. Theory Ser. A **56** (1991), 223–238.

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

[7] **J.N. Bray**, personal communication.

[8] **M.L. Cates and R.B. Killgrove**, *One-directional translation planes of order* 13, Congr. Numer. **32** (1981), 173–180.

[9] **A. Cayley**, *On the theory of groups as depending on the symbolical equation $\theta^n = 1$*, Phil. Mag. **7** (1854), 40–47.

[10] **A. Cayley**, *On the theory of groups*, Proc. London Math. Soc. **9** (1877/78), 126–133.

[11] **C.J. Colbourn and J.H. Dinitz (ed.)**, *Handbook of combinatorial designs*, 2nd ed. Chapman and Hall, CRC, Florida (2007).

[12] **J.Dénes and A.D. Keedwell**, *Latin squares and their applications*, English Universities Press, London (1974).

[13] **J.Dénes and A.D. Keedwell**, *Latin squares: New developments in the theory and applications*, Annals Discrete Math. **46**, North Holland (1991).

[14] **A.B. Evans**, *Orthomorphisms of Z_p*, Discrete Math. **64** (1987), 147–156.

[15] **A.B. Evans**, *On planes of prime order with translations and homologies*, J. Geom. **34** (1989), 36–41.

[16] **A.B. Evans**, *On strong complete mappings*, Congr. Numer. **70** (1990), 241–248.

[17] **A.B. Evans**, *Maximal sets of mutually orthogonal Latin squares I*, Europ. J. Combinatorics **12** (1991), 477–482.

[18] **A.B. Evans**, *Maximal sets of mutually orthogonal Latin squares II*, Europ. J. Combinatorics **13** (1992), 345–350.

[19] **A.B. Evans**, *Orthomorphism graphs of groups*, Lecture Notes Math. **1535**, Springer-Verlag (1992).

[20] **A.B. Evans**, *The admissibility of sporadic simple groups*, J. Algebra **321** (2009), 105–116.

[21] **A.B. Evans**, *The existence of strong complete mappings*, Electronic J. Combin. **19** (2012), # P34.

[22] **A.B. Evans**, *The strong admissibility of finite groups: an update*, submitted.

[23] **A.B. Evans and R.L. Mcfarland**, *Planes of prime order with translations*, Congr. Numer. **44** (1984), 41–46.

[24] **R.J. Friedlander, B. Gordon and M.D. Miller**, *On a group sequencing problem of Ringel*, Congr. Numer. **21** (1978), 307?-321.

[25] **B. Gordon**, *Sequences in groups with distinct partial products*, Pacific J. Math. **11** (1961), 1309–1313.

[26] **M. Hall and L.J. Paige**, *Complete mappings of finite groups*, Pacific J. Math. **5** (1955), 541–549.

[27] **A. Hedayat**, *A complete solution to the existence and non-existence of Knut Vic designs and orthogonal Knut Vic designs*, J. Combin. Theory Ser. A **22** (1977), 331–337.

[28] **A. Hedayat and W.T. Federer**, *On the non-existence of Knut Vic designs for all even orders*, Ann. Statist. **3** (1975), 445–447.

[29] **J.D. Horton**, *Orthogonal starters in finite abelian groups*, Discrete Math. **79** (1990), 265–278.

[30] **J. Hsiang, D.F. Hsu, and Y.-P. Shieh**, *On the hardness of computing problems of complete mappings*, Discrete Math. **277** (2004), 87–100.

[31] **D.F. Hsu**, *Cyclic neofields and combinatorial designs*, Springer-Verlag, Lecture Notes Math. **824** (1980).

[32] **D.F. Hsu (ed.)**, *Advances in discrete mathematics and computer science*, vol I, *Neofields and combinatorial designs*, Hadronic Press (1985).

[33] **D.F. Hsu (ed.)**, *Advances in discrete mathematics and computer science*, vol. II, *Generalized complete mappings*, Hadronic Press (1987).

[34] **D.F. Hsu and A.D. Keedwell**, *Generalized complete mappings, neofields, sequenceable groups and block designs. I*, Pacific J. Math. **111** (1984), 317–332.

[35] **D.F. Hsu and A.D. Keedwell**, *Generalized complete mappings, neofields, sequenceable groups and block designs. II*, Pacific J. Math. **117** (1985), 291–312.

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

[37] **D. Jungnickel and G. Grams**, *Maximal difference matrices of order* $\leqslant 10$, Discrete Math. **58** (1986), 199–203.

[38] **A.D. Keedwell**, *Latin squares P-quasigroups and graph decompositions*, Recueil des Travaux de l'Institute Mathématique, Belgrade, N.S. **1(9)** (1976), 41–48.

[39] **A.D. Keedwell**, *The existence of pathological left neofields*, Ars Combinatoria **16B** (1983), 161–170.

[40] **A.D. Keedwell**, *Sequenceable groups, generalized complete mappings, neofields and block designs*, Lecture Notes Math. **1036** (1983), 49–71.

[41] **A.D. Keedwell**, *Construction, properties and applications of finite neofields*, Comment. Math. Univ. Carolin. **41** (2000), 283–297.

[42] **A.D. Keedwell**, *Latin squares and their applications*, 2nd edition (in press).

[43] **F. Lazebnik and A. Thomason**, *Orthomorphisms and the construction of projective planes*, Math. Comp. **73** (2004), 1547–1557.

[44] **H.B. Mann**, *On orthogonal latin squares*, Bull. Amer. Math. Soc. **50** (1944), 249–257.

[45] **B.D. McKay, J.C. McLeod and I.M. Wanless**, *The number of transversals in a latin square*, Des. Codes Cryptogr. **40** (2006), 269–284.

[46] **N.S. Mendelsohn and B. Wolk**, *A search for a nondesarguesian plane of prime order*, Lecture Notes Pure and Appl. Math. **103** (1985), 199–208.

[47] **L. Mittenthal**, *Block substitutions using orthomorphic mappings*, Adv. in Appl. Math. **16** (1995), 59–71.

[48] **H. Niederreiter and K.H. Robinson**, *Bol loops of order pq*, Math. Proc. Camb. Phil. Soc. **89** (1981), 241–256.

[49] **M. A. Ollis**, *Sequenceable groups and related topics. Dynamic survey*, Electronic J. Combin. **20**(2) (2013), #DS10v2.

[50] **T.G. Ostrom**, *Replaceable nets, net collineations, and net extensions*, Canad. J. Math. **18** (1966), 666–672.

[51] **L.J. Paige**, *Neofields*, PhD dissertation, University of Wisconsin, 1947.

[52] **L.J. Paige**, *Neofields*, Duke Math. J. **16** (1949), 39–60.

[53] **L.J. Paige**, *Complete mappings of finite groups*, Pacific J. Math. **1** (1951), 111–116.

[54] **A. Pott**, *Maximal difference matrices of order q*, J. Combin. Des. **1** (1993), 171–176.

[55] **G. Ringel**, *Cyclic arrangements of the elements of a group*, Notices Amer. Math. Soc. **21** (1974), A95–96.

[56] **R. Shaheen and A. Winterhof**, *Permutations of finite fields for check digit systems*, Des. Codes Cryptogr. **57** (2010), 361–371.

[57] **Y.-P. Shieh, J. Hsiang, and D.F. Hsu**, *On the existence problems of complete mappings*, preprint.

[58] **I. Studicka**, *Non-existence of Cartesian groups of order $2p^m$*, Comment. Math. Univ. Carolin. **13** (1972), 721–725.

[59] **I.M. Wanless**, *Atomic latin squares based on cyclotomic orthomorphisms*, Electronic J. Combin. **12** (2005), # R22.

[60] **S. Wilcox**, *Reduction of the Hall-Paige conjecture to sporadic simple groups*, J. Algebra **321** (2009), 1407–1428.

Received May 15, 2015

Department of Mathematics and Statistics, Wright State University, Dayton, Ohio, USA
E-mail: anthony.evans@wright.edu