AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **57** (2013), Pages 189–216

A class of orthogonal latin square graphs

Anthony B. Evans

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

Abstract

An *orthogonal latin square graph* is a graph whose vertices are latin squares of the same order, adjacency being synonymous with orthogonality. We are interested in orthogonal latin square graphs in which each square is orthogonal to the Cayley table M of a group G and is obtained from M by permuting columns. These permutations, regarded as permutations of G, are *orthomorphisms* of G and the graphs so obtained are *orthomorphism graphs.*

We will discuss the main problems in the study of orthomorphism graphs and survey bounds on the clique numbers of these graphs. We will also present several problems.

1 Introduction

A *latin square* of order n is an $n \times n$ matrix in which each symbol from an n-element set appears exactly once in each row and each column. A latin square of order 7 is shown in Figure 1. This latin square is the addition table of the group $\mathbb{Z}_7$. For a group $G = \{g_1, \ldots, g_n\}$, the *Cayley table* of G is the latin square of order n with ijth entry $g_i g_j$ ($g_i + g_j$ if the group operation is addition).

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

Figure 1: A latin square of order 7.

Two latin squares of the same order are *orthogonal* if each ordered pair of symbols appears exactly once when the squares are superimposed. Figure 2 shows an orthogonal pair of latin squares of order 4 and their superposition: in the superposition the entries from the second square are shown in bold. 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. It is known that, if $n > 1$, then

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

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 the 2007 "Handbook of Combinatorial Designs", edited by Colbourn and Dinitz [18].

$$\begin{pmatrix} 00 & 01 & 10 & 11 \\ 01 & 00 & 11 & 10 \\ 10 & 11 & 00 & 01 \\ 11 & 10 & 01 & 00 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 00 & 10 & 11 & 01 \\ 01 & 11 & 10 & 00 \\ 10 & 00 & 01 & 11 \\ 11 & 01 & 00 & 10 \end{pmatrix}$$

$$\searrow \text{superimposed} \swarrow$$

$$\begin{pmatrix} 00,\mathbf{00} & 01,\mathbf{10} & 10,\mathbf{11} & 11,\mathbf{01} \\ 01,\mathbf{01} & 00,\mathbf{11} & 11,\mathbf{10} & 10,\mathbf{00} \\ 10,\mathbf{10} & 11,\mathbf{00} & 00,\mathbf{01} & 01,\mathbf{11} \\ 11,\mathbf{11} & 10,\mathbf{01} & 01,\mathbf{00} & 00,\mathbf{10} \end{pmatrix}$$

Figure 2: A pair of orthogonal latin squares of order 4.

An *orthogonal latin square graph* is a graph whose vertices are latin squares of the same order, adjacency being synonymous with orthogonality. In 1979 Lindner, Mendelsohn, Mendelsohn, and Wolk [47] proved that any finite graph can be realized as an orthogonal latin square graph. We are interested in a special class of orthogonal latin square graphs, those based on finite groups. For our purposes an orthogonal latin square graph will be said to be *based on the group G* if each square in the graph is orthogonal to the Cayley table of G, and each square in the graph is obtained from the Cayley table of G by permuting columns. Note that in an orthogonal latin square graph based on a group, each square is uniquely determined by the entries in its first row. Figure 3 shows an orthogonal latin square graph based on the group $\mathbb{Z}_2 \times \mathbb{Z}_4$. The first rows of these squares are listed in Table 1, where L denotes the Cayley table of $\mathbb{Z}_2 \times \mathbb{Z}_4$ and the elements of $\mathbb{Z}_2 \times \mathbb{Z}_4$ are ij, $i \in \mathbb{Z}_2 = \{0, 1\}$ and $j \in \mathbb{Z}_4 = \{0, 1, 2, 3\}$.

Figure 4 shows an orthogonal latin square graph based on the group $\mathbb{Z}_{11} = \{0, 1, \ldots, 10\}$. Here $[a]$ denotes the square with first row $0, a, 2a, \ldots, 10a$, multiplication modulo 11, and $[a, b]$ denotes the square with first row 0, a, $2b$, $3a$, $4a$,

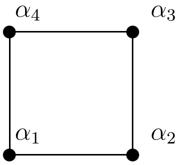

Figure 3: An orthogonal latin square graph based on $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Table 1: A 4-cycle of $Orth(\mathbb{Z}_2 \times \mathbb{Z}_4)$.

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

$5a$, $6b$, $7b$, $8b$, $9a$, $10b$, multiplication modulo 11. All the squares in Figure 4 are orthogonal to the square $[2, 6]$.

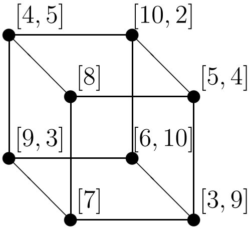

Figure 4: An orthogonal latin square graph based on $\mathbb{Z}_{11}$.

Let $G = \{g_1, \ldots, g_n\}$ be a group with $g_1 = 1$ and let L be the Cayley table of G. Let θ be a permutation of G and let L_θ denote the latin square of order n with ijth entry $g_i\theta(g_j)$. Hence $g_1, \ldots, g_n$ is the first row of L, and $\theta(g_1), \ldots, \theta(g_n)$ is the first row of L_θ. The rules for determining orthogonality are entirely algebraic.

Lemma 1 *Let $G = \{g_1, \ldots, g_n\}$ be a group and let L be the Cayley table of G.*

1. *If θ is a permutation of G, then L_θ is orthogonal to L if and only if $x \mapsto x^{-1}\theta(x)$ is a permutation.*

2. *If θ, ϕ are permutations of G, then L_θ is orthogonal to L_ϕ if and only if $x \mapsto \phi(x)^{-1}\theta(x)$ is a permutation.*

Proof. Routine. □

A permutation θ of a group G is an *orthomorphism* of G if the mapping $x \mapsto x^{-1}\theta(x)$ is a permutation. An orthomorphism θ of a group G is *normalized* if $\theta(1) = 1$. Two orthomorphisms θ, ϕ of a group G are *orthogonal* if the mapping $x \mapsto \phi(x)^{-1}\theta(x)$ is a permutation. If θ is an orthomorphism of G, then $x \mapsto \theta(x)\theta(1)^{-1}$ is a normalized orthomorphism of G. Normalization preserves orthogonality. The *orthomorphism graph* of G, denoted $Orth(G)$, has as vertices the normalized orthomorphisms of G, adjacency being orthogonality. An *orthomorphism graph* of G is a, not necessarily induced, subgraph of $Orth(G)$. An *r-clique* of $Orth(G)$ is a set of r pairwise orthogonal orthomorphisms of G. If $\mathcal{H}$ is an orthomorphism graph of G, then the *clique number* of $\mathcal{H}$, denoted $\omega(\mathcal{H})$, is the order of the largest clique in $\mathcal{H}$. We use $\omega(G)$ as a shortened form of $\omega(Orth(G))$. An r-clique of $Orth(G)$ is *maximal* if it cannot be extended to a larger clique, and a $(|G|-2)$-clique of $Orth(G)$ is a *complete* set of orthomorphisms of G. If $|G| = n > 1$, then r-cliques of $Orth(G)$ can be used to construct MOLS of order n, maximal r-cliques of $Orth(G)$ can be used to construct maximal sets of MOLS of order n, and complete sets of orthomorphisms of $Orth(G)$ can be used to construct complete sets of MOLS of order n.

Lemma 2 *Let G be a group of order $n > 1$.*

1. *From an r-clique of $Orth(G)$ we can construct a set of $r+1$ MOLS of order n.*
2. *From a maximal r-clique of $Orth(G)$ we can construct a maximal set of $r+1$ MOLS of order n.*
3. *From a complete set of orthomorphisms of G we can construct a complete set of MOLS of order n.*

Let us revisit the orthomorphism graphs shown in Figures 3 and 4. For the group $\mathbb{Z}_2 \times \mathbb{Z}_4$, its orthomorphism graph consists of twelve 4-cycles. Figure 3 shows one of these 4-cycles. The orthomorphisms in this cycle are described in Table 1. Figure 4 shows part of $Orth(\mathbb{Z}_{11})$. Let us use $[a]$ to denote the mapping $x \mapsto ax \pmod{11}$, and $[a, b]$ to denote the mapping

$$x \mapsto \begin{cases} 0 & \text{if } x = 0, \\ ax \pmod{11} & \text{if } x \text{ is a square}, \\ bx \pmod{11} & \text{if } x \text{ is a nonsquare}. \end{cases}$$

It is easily verified that $[a]$ is an orthomorphism if and only if $a \neq 0, 1$ and $[a, b]$ is an orthomorphism if and only if both ab and $(a-1)(b-1)$ are nonzero squares. Orthomorphisms of the form $[a]$ are called *linear orthomorphisms* and orthomorphisms of the form $[a, b]$ are called *quadratic orthomorphisms.* Figure 3 actually shows the neighbourhood of $[2, 6]$ in $Orth(\mathbb{Z}_{11})$.

Given a nontrivial group G and an orthomorphism graph $\mathcal{H}$ of G, the main problems that concern us are the following.

Problem 1 *Determine $\omega(\mathcal{H})$ or find good bounds for $\omega(\mathcal{H})$.*

Problem 2 *Does $\mathcal{H}$ contain complete sets of orthomorphisms? If the answer is yes, then classify these complete sets of orthomorphisms.*

Problem 3 *Find maximal cliques in $\mathcal{H}$. Are any of these maximal in $Orth(G)$?*

Problem 4 *What can we say about the structure of $\mathcal{H}$?*

One of the simplest orthomorphism graphs to study is the orthomorphism graph $\mathcal{P}(G)$ consisting of orthomorphisms of the form $x \mapsto x^r$. In Section 2 we will use this orthomorphism graph to illustrate the main problems in the study of orthomorphism graphs. For groups in general, the first question of interest is whether a group admits orthomorphisms or not: we will give a characterization of finite groups that admit orthomorphisms in Section 3. In Section 4 we will present the orders and clique numbers of the orthomorphism graphs of small groups, and in Section 5 we will survey known bounds for $\omega(G)$.

2 The orthomorphism graph $\mathcal{P}(G)$

To illustrate the main problems in the study of orthomorphism graphs, let us look at one of the easiest orthomorphism graphs to study. Let G be a finite group and let $\mathcal{P}(G)$ be the orthomorphism graph of G whose elements are orthomorphisms of the form $\phi_r\colon x \mapsto x^r$. The rules for membership and orthogonality in $\mathcal{P}(G)$ are easily established.

Lemma 3 *If $|G| = n > 1$, then*

1. *ϕ_r is a permutation if and only if $\gcd(n, r) = 1$,*

2. *ϕ_r is an orthomorphism if and only if $\gcd(n, r) = \gcd(n, r-1) = 1$, and*

3. *If $\phi_r, \phi_s \in \mathcal{P}(G)$, then ϕ_r is orthogonal to ϕ_s if and only if $\gcd(n, r-s) = 1$.*

Proof. Routine. □

As a consequence of Lemma 3, the structure of $\mathcal{P}(G)$ depends only on the order of the group G, not on its structure. The clique number of $\mathcal{P}(G)$ is readily determined.

Theorem 1 *If $|G| = n > 1$ and p is the smallest prime divisor of n, then*

$$\omega(\mathcal{P}(G)) = p - 2.$$

Proof. The mappings $\phi_2, \ldots, \phi_{p-1}$ form a $(p-2)$-clique in $\mathcal{P}(G)$ and, if $\phi_{r_1}, \ldots, \phi_{r_k}$ is a k-clique in $\mathcal{P}(G)$, then $0, 1, r_1, \ldots, r_k$ must be in distinct residue classes modulo p. □

As an immediate corollary we can determine when $\omega(\mathcal{P}(G)) = n-2$ for a group of order n.

Corollary 1 *If $|G| = n > 1$, then*

$$\omega(\mathcal{P}(G)) = n-2$$

if and only if n is a prime.

In the case when $\mathcal{P}(G)$ does contain a complete set of orthomorphisms, $G = \mathbb{Z}_p$, p a prime, $\mathcal{P}(\mathbb{Z}_p) = \{\phi_2, \ldots, \phi_{p-1}\}$ is the only complete set of orthomorphisms in $\mathcal{P}(\mathbb{Z}_p)$. Are there other complete sets of orthomorphisms in $Orth(\mathbb{Z}_p)$?

Problem 5 *Does $Orth(\mathbb{Z}_p)$, p a prime, contain a second complete set of orthomorphisms?*

A positive answer to Problem 5 would have geometric implications as, in 1984 Evans and McFarland [36] proved that, if $Orth(\mathbb{Z}_p)$, p a prime, contains more than one complete set of orthomorphisms, then there exists a non-Desarguesian projective plane of prime order, p. It is a long-standing conjecture that such projective planes do not exist.

The maximal cliques in $\mathcal{P}(G)$ are easily determined.

Theorem 2 *If $|G| = n > 1$ and p is the smallest prime divisor of n, then every maximal clique in $\mathcal{P}(G)$ is a $(p-2)$-clique.*

Proof. If $\phi_{r_1}, \ldots, \phi_{r_k}$ is a k-clique in $\mathcal{P}(G)$, then $0, 1, r_1, \ldots, r_k$ must be in distinct residue classes modulo any prime divisor of n. Using the chinese remainder theorem, we can extend this to $0, 1, r_1, \ldots, r_{p-2}$, a complete set of residues modulo p that are also in distinct residue classes modulo any prime divisor of n. Then $\phi_{r_1}, \ldots, \phi_{r_{p-2}}$ is a $(p-2)$-clique in $\mathcal{P}(G)$, which is maximal by Theorem 1. □

When is a maximal clique in $\mathcal{P}(G)$ also maximal in $Orth(G)$? When the smallest prime divisor of $|G|$ is 2, this question reduces to"Is $Orth(G) = \emptyset$?" This is a question that we will answer in Section 3. One special case was dealt with by Evans [24] in 1991, cyclic groups of prime-power order.

Theorem 3 (Evans, 1991) *If p is a prime, then any maximal $(p-2)$-clique in $\mathcal{P}(\mathbb{Z}_{p^k})$ is maximal in $Orth(\mathbb{Z}_{p^k})$.*

In [24] a more general result was proved from which we can prove the maximality in $Orth(G)$ of maximal cliques of $\mathcal{P}(G)$ when the Sylow p-subgroup of G is cyclic. This proof needs to be given in a difference matrix setting. If $|G| = n$, 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 can be expressed λ times in the form $d_{ij}^{-1} d_{kj}$: λ is the *index* of D. From a difference matrix D over a group G we can form other difference matrices over G by permuting its rows, permuting its columns, multiplying each entry in a row on the right by an element $g \in G$, and multiplying each entry in a column on the left by an element $g \in G$. Using these operations, any difference matrix can be transformed into a *normalized* difference matrix, a difference matrix in which each entry in the first row and the first column is the identity. If $|G| = n$ and D is a normalized $(n, r+2; 1)$-difference matrix over G, then each entry of the first row of D is the identity, each element of G appears exactly once in the second row, and the remaining r rows, regarded as permutations of the second row, form an r-clique of $Orth(G)$. Similarly, from an r-clique of $Orth(G)$ we can construct a normalized $(n, r+2; 1)$-difference matrix over G. Homomorphic images of difference matrices are difference matrices.

Lemma 4 *If $D = \{d_{ij}\}$ is a difference matrix over G and $f\colon G \to H$ is a homomorphism, then $f(D) = \{f(d_{ij})\}$ is a difference matrix over H.*

Proof. Routine. □

We say that a difference matrix over G is *maximal* if it cannot be extended to a larger difference matrix over G by adding rows. Maximal $(n, r+2; 1)$-difference matrices over G correspond to maximal r-cliques in $Orth(G)$. While maximality of difference matrices is not preserved by homomorphisms, only maximal difference matrices can be mapped by homomorphisms onto maximal difference matrices.

Lemma 5 *If D is a difference matrix over G, $f\colon G \to H$ is a homomorphism, and $f(D)$ is a maximal difference matrix over H, then D is a maximal difference matrix over G.*

Proof. Routine. □

Theorem 4 *If p is the smallest prime divisor of $|G|$ and the Sylow p-subgroup of G is cyclic, then any $(p-2)$–clique of $\mathcal{P}(G)$ is a maximal set of orthomorphisms of G.*

Proof. Let $G = \{g_1, \ldots, g_n\}$, $g_1 = 1$, $n = p^r m$, $\gcd(m, p) = 1$, let $\phi_{k_1}, \ldots, \phi_{k_{p-2}}$ be a clique in $\mathcal{P}(G)$, and let $S = \mathbb{Z}_{p^r} = \{h_1, \ldots, h_{p^r}\}$. Let $D_G = \{d_{ij}\}$ be the $(n, p; 1)$–difference matrix over G defined by

$$d_{ij} = \begin{cases} 1 & \text{if } i = 1, \\ g_j & \text{if } i = 2, \\ g_j^{k_{i-2}} & \text{if } i > 2. \end{cases}$$

Let $D_p = \{d'_{ij}\}$ be the $(p^r, p; 1)$–difference matrix over S defined by

$$d'_{ij} = \begin{cases} 1 & \text{if } i = 1, \\ h_j & \text{if } i = 2, \\ h_j^{k_{i-2}} & \text{if } i > 2. \end{cases}$$

As p is the smallest prime dividing $|G|$ and the Sylow p-subgroup of G is cyclic, by, for example, Corollary 1.4.18 in [50], there is a homomorphism f from G onto S. Each column of D_p appears exactly m times in $f(D_G)$. Thus $f(D_G)$ is mD_p with the columns permuted, and hence, by Theorem 3 of [24], $f(D_G)$ is maximal, from which it follows, by Lemma 5, that D_G is maximal and, hence, that $\phi_{k_1}, \dots, \phi_{k_{p-2}}$ is a maximal set of orthomorphisms of G. □

What if p is the smallest prime divisor of $|G|$ and the Sylow p-subgroup of G is noncyclic? We know that, if G is an elementary abelian p-group other than $\mathbb{Z}_p$, then any maximal clique of $\mathcal{P}(G)$ can be extended. We conjecture the following.

Conjecture 1 *If the Sylow p-subgroup of a group G is noncyclic and p is the smallest prime divisor of $|G|$, then no $(p-2)$-clique of $\mathcal{P}(G)$ is maximal in $Orth(G)$.*

For $p = 2$, this conjecture is the Hall-Paige conjecture, whose proof will be discussed in Section 3. For $p = 3$, the mapping ϕ_{-1} is an orthomorphism of G that forms a maximal clique in $\mathcal{P}(G)$. This is relevant to the existence problem for strong complete mappings. A *complete mapping* of a group G is a bijection $\theta\colon G \to G$ for which the mapping $x \mapsto x\theta(x)$ is also a bijection. A *strong complete mapping* of a group G is a complete mapping of G that is also an orthomorphism of G. It is easy to see that any orthomorphism orthogonal to ϕ_{-1} is a strong complete mapping. The existence of strong complete mappings was proved for abelian groups whose Sylow 2-subgroups and Sylow 3-subgroups are trivial or noncyclic by Evans [30] in 2012: this encompasses a special case of Conjecture 1. The existence problem for strong complete mappings of nonabelian groups is still open. See [31] for a survey of work done on the existence problem for strong complete mappings. There is reason to believe that a proof of Conjecture 1 is within reach. While a proof of the special case $p = 2$, given in 2009, required the classification of finite simple groups, its proof for solvable groups was obtained much earlier by Hall and Paige [39] in 1955. For $p \geq 3$ we are only dealing with solvable groups as, by the Feit-Thompson Theorem, all odd-order groups are solvable.

What can we say about the structure of $\mathcal{P}(G)$? The graph $\mathcal{P}(G)$ is closely related to the *unitary Cayley graph* of order n, denoted X_n, which has vertices $0, 1, \dots, n-1$, i adjacent to j if $\gcd(n, i-j) = 1$. In 1994 Evans, Fricke, Maneri, McKee, and Perkel [34], described X_n as a tensor product of graphs. The *tensor product* of graphs $\Gamma_1 \times \cdots \times \Gamma_r$ has vertices the r-tuples $(v_1, v_2, \dots, v_r)$, v_i a vertex of Γ_i, $(u_1, u_2, \dots, u_r)$ adjacent to $(v_1, v_2, \dots, v_r)$ if u_i is adjacent to v_i for each i. The tensor product of graphs has also been called the categorical product of graphs, the Kronecker product of graphs, and the conjunction of graphs. We will use $K_{k(t)}$ to denote the complete k-partite graph with each partite class of order t.

Theorem 5 *If $n = p_1^{k_1} \times \cdots \times p_r^{k_r}$, $p_1, \dots, p_r$ distinct primes, then*

$$X_n \cong K_{p_1\left(p_1^{k_1-1}\right)} \times \cdots \times K_{p_r\left(p_r^{k_r-1}\right)}.$$

Proof. See Lemma 2.1 in [34]. □

From Theorem 5 we can determine the structure of $\mathcal{P}(G)$, as $\mathcal{P}(G)$ is isomorphic to an induced subgraph of X_n.

Theorem 6 *If $|G| = n > 1$, then $\mathcal{P}(G)$ is isomorphic to the common neighbourhood of 0 and 1 in X_n.*

Proof. The mapping $\phi_r \mapsto r$ establishes the isomorphism. □

Which graphs can be induced subgraphs of $\mathcal{P}(G)$? To answer this question we first need to answer the question, Which graphs can be induced subgraphs of X_n? In 1989 Erdős and Evans [23] proved that any finite graph can be realized as an induced subgraph of X_n for some n.

Theorem 7 (Erdős and Evans, 1989) *Any finite graph can be realized as an induced subgraph of X_n for some n.*

As a corollary to Theorem 7, we obtain a similar result for $\mathcal{P}(G)$.

Corollary 2 *Any finite graph can be realized as an induced subgraph of $\mathcal{P}(G)$ for some group G.*

Proof. Let the vertices of a graph Γ be $v_1, \ldots, v_k$ and form a new graph Γ_1 by adjoining two vertices u and w to Γ, u and w being adjacent to each other as well as to each of $v_i, \ldots, v_k$. By Theorem 7, Γ_1 can be realized as an induced subgraph of X_n for some n. Let $a_1, \ldots, a_k, b, c$ be a realization of Γ_1 as an induced subgraph of X_n, a_i corresponding to v_i for $i = 1, \ldots, k$, b corresponding to u, and c corresponding to w. If $\gcd(d, n) = 1$ and e is any integer, then $da_1+e \pmod{n}, \ldots, da_k+e \pmod{n}, db+e \pmod{n}, dc + e \pmod{n}$ is also a realization of Γ_1 as an induced subgraph of X_n. Thus, by an appropriate choice of d and e, we may, without loss of generality, assume $b = 0$ and $c = 1$, in which case, $a_1, \ldots, a_k$ yields a realization of Γ as an induced subgraph of $\mathcal{P}(\mathbb{Z}_n)$. □

From Corollary 2, Erdős and Evans obtained a new proof of Lindner, Mendelsohn, Mendelsohn, and Wolk's [47] result that any finite graph can be realized as an orthogonal latin square graph.

While we may be interested in the question, "Given a graph Γ, for which groups G can Γ be realized as an induced subgraph of $\mathcal{P}(G)$?", it is easier to answer the related question, "Given a graph Γ, for which values n can Γ be realized as an induced subgraph of X_n?". A realization of a graph as an induced subgraph of X_n is called a *representation modulo n*: if $\Gamma = \{v_1, \ldots, v_m\}$ is a graph and $a_1, \ldots, a_m \in \{0, \ldots, n-1\}$ are distinct integers, then $\{a_1, \ldots, a_m\}$ is a *representation* of Γ modulo n if $\gcd(a_i - a_j, n) = 1$ if and only if v_i is adjacent to v_j. A representation of a graph may also be regarded as a labeling of the graph. As an example Figure 5 shows a graph represented modulo $105 = 3 \times 5 \times 7$.

The development of a theory of graph representations was begun by Evans, Fricke, Maneri, McKee, and Perkel [34] in 1994. The following are some of the results from this paper that have implications for the realizability of a graph Γ as an induced subgraph of $\mathcal{P}(G)$ for some group G. The easiest question to answer is, When is a graph representable modulo a prime?

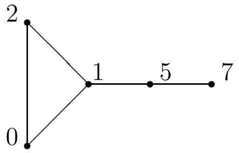

Figure 5: A graph represented modulo 105.

Theorem 8

A graph Γ is representable modulo a prime if and only if Γ is a complete graph.

Proof. See Example 1.2 in [34]. □

As $\mathcal{P}(\mathbb{Z}_p)$, p a prime, is isomorphic to K_{p-2}, the complete graph on $p-2$ vertices, the following is an immediate corollary.

Corollary 3 *A graph Γ can be realized as an induced subgraph of $\mathcal{P}(\mathbb{Z}_p)$, for some prime p, if and only if Γ is a complete graph.*

More generally, we might ask, When is a graph representable modulo a power of a prime?

Theorem 9 *A graph Γ is representable modulo a prime power if and only if Γ is a complete multipartite graph.*

Proof. See Corollary 2.1 in [34]. □

As, by Theorem 5, $\mathcal{P}(G)$, G of prime power order, is a complete multipartite graph, the following is an immediate corollary.

Corollary 4 *A graph Γ can be realized as an induced subgraph of $\mathcal{P}(G)$, for some p-group G and some prime p, if and only if Γ is a complete multipartite graph.*

When is a graph representable modulo a product of two distinct primes? The characterization of graphs representable modulo a product of two distinct primes is a forbidden subgraph characterization. The *union* of two graphs G and H, $G \cup H$, has as its vertex set the disjoint union of the vertex sets of G and H, and as its edge set the disjoint union of the edge sets of G and H. We use kH to denote the union of k copies of H: in particular kK_t denotes the union of k copies of K_t. The notation $G + H$ is sometimes used instead of $G \cup H$. A *cycle* of *length* $m \geq 3$ is a graph with vertex set $\{v_1, \ldots, v_m\}$ and edge set $\{\{v_1, v_2\}, \ldots, \{v_{m-1}, v_m\} \cup \{\{v_m, v_1\}\}$. A cycle of length m is an *odd cycle* if m is odd. The *complement*, Γ^C, of a graph Γ has the same vertex set as Γ, two vertices being adjacent in Γ^C if and only if they are not adjacent in Γ.

Theorem 10 *A graph* Γ *is representable modulo a product of two distinct primes if and only if* Γ *does not contain an induced subgraph isomorphic to* $K_2 \cup 2K_1$*,* $K_3 \cup K_1$*, or the complement of an odd cycle of length at least* 5*.*

Proof. See Theorem 4.1 in [34]. □

Several alternative characterizations of graphs that do not contain an induced subgraph isomorphic to $K_2 \cup 2K_1$, $K_3 \cup K_1$, or the complement of an odd cycle of length at least 5 were given by Peterson [53] in 2003. As a corollary to Theorem 10, we obtain a similar result for realizability as an induced subgraph of $\mathcal{P}(G)$.

Corollary 5 *A graph* Γ *can be realized as an induced subgraph of* $\mathcal{P}(G)$*,* $|G| = pq$ *for some pair of distinct primes* p *and* q*, if and only if* Γ *does not contain an induced subgraph isomorphic to* $K_2 \cup 2K_1$*,* $K_3 \cup K_1$*, or the complement of an odd cycle of length at least* 5*.*

Proof. If Γ can be realized as an induced subgraph of $\mathcal{P}(G)$, $|G| = pq$ for some pair of distinct primes p and q, then Γ is representable modulo pq and hence, by Theorem 10, does not contain an induced subgraph isomorphic to $K_2 \cup 2K_1$, $K_3 \cup K_1$, or the complement of an odd cycle of length at least 5.

Next, suppose that $\Gamma = \{v_1, \ldots, v_m\}$ does not contain an induced subgraph isomorphic to $K_2 \cup 2K_1$, $K_3 \cup K_1$, or the complement of an odd cycle of length at least 5. Form a new graph Γ_1 by adjoining vertices u and w adjacent to each other and to each vertex $v_i \in \Gamma$. Γ_1 will also not contain an induced subgraph isomorphic to $K_2 \cup 2K_1$, $K_3 \cup K_1$, or the complement of an odd cycle of length at least 5, and hence, by Theorem 10, will be representable modulo pq for some pair of distinct primes p and q. Let $\{a_1, \ldots, a_m, b, c\}$ be a representation of Γ_1 modulo pq. By the argument used in the proof of Corollary 2, we may assume that $b = 0$ and $c = 1$. The mapping $v_i \mapsto a_i$ then yields an isomorphism between Γ and an induced subgraph of $\mathcal{P}(\mathbb{Z}_{pq})$. □

No characterization of graphs representable modulo a product of three distinct primes has been found.

Problem 6 *Characterize graphs representable modulo a product of three distinct primes.*

Much of the work on graph representations has involved determining the representation numbers of graphs. For a graph Γ, *rep*(Γ), the *representation number* of Γ, is the smallest n for which Γ can be represented modulo n. Let us revisit the graph depicted in Figure 5. If the representation number of this graph is n, then n must be odd as K_3 is a subgraph; by Lemma 2.2 of [34], n must be a product of distinct primes as no two vertices of this graph share a common neighborhood; and, by Theorem 10, n must be divisible by at least three distinct primes as $K_3 \cup K_1$ is an induced subgraph. Hence $n \geq 105$. As Figure 5 shows a representation of this graph modulo 105, it follows that the representation number of this graph is 105.

There are a number of papers on the determination of representation numbers: see [37] for a survey and a list of problems. Determining representation numbers of closely related classes of graphs can require very different techniques. Stars and their complements provide instructive examples. A star is a complete bipartite graph of the form $K_{1,m}$. In 2010 Akhtar, Evans, and Pritikin [9] described the representation numbers of stars in terms of Euler's phi-function, $\phi(n) = |\{k \leq n \mid \gcd(k,n) = 1\}|$.

Theorem 11 (Akhtar, Evans, Pritikin, 2010)

$$rep(K_{1,m}) = \min\{k \mid k \ \textit{even}, \phi(k) \geq m\}.$$

Proof. See Theorem 7 in [9]. □

Using Theorem 11 to compute $rep(K_{1,m})$ for small m suggested the following conjecture.

Conjecture 2 *$rep(K_{1,m})$ is of the form 2^{t+1} or $2^{t+1}p$, p an odd prime.*

Conjecture 2 was proved for small m in [9]. It was proved in [9] that asymptotically $rep(K_{1,m})$ is of the form 2^{t+1}, $2^{t+1}p$, or $2^{t+1}pq$, p and q, not necessarily distinct, odd primes. We could rule out the form $2^{t+1}pq$ if it can be proved that there always exists a prime between x and $x+\sqrt{x}$ for x sufficiently large.

By contrast, the representation numbers of complements of stars were completely determined by Evans, Isaak, and Narayan [35] in 2000: they actually proved a more general result.

Theorem 12 (Evans, Isaak, Narayan, 2000) *If $2 \leq k \leq m-1$, then*

$$rep(K_m - K_{1,k}) = p_i \dots p_{i+k-1},$$

where p_i is the smallest prime greater than or equal to $m-1$, and $p_i, \dots, p_{i+k-1}$ are consecutive primes.

Proof. See Theorem 3.6 in [35]. □

As a corollary we obtain the representation numbers of complements of stars.

Corollary 6 *If $m \geq 2$, then*

$$rep\left(K_{1,m}^C\right) = p_i \dots p_{i+m-1},$$

where p_i is the smallest prime greater than or equal to m, and $p_i, \dots, p_{i+m-1}$ are consecutive primes.

Proof. $K_{1,m}^C \equiv K_m - K_{1,m-1}$. The result then follows from Theorem 12. □

Recently, Agarwal, and Lopez [8] generalized Theorem 12.

Theorem 13 (Agarwal, Lopez, preprint)

$$rep\left(K_r - \bigcup_{i=1}^{s} K_{1,m_i}\right) = p_i \dots p_{i+m_1-1},$$

where $m_1 \geq \cdots \geq m_s$, p_i is the smallest prime greater than or equal to $r - s$, and $p_i, \dots, p_{i+m_1-1}$ are consecutive primes.

Our last example of a graph representation result establishes a surprising connection between representation numbers and MOLS. In 2000 Evans, Isaak, and Narayan [35] established a connection between the representation numbers of the union of disjoint copies of complete graphs and the existence of MOLS.

Theorem 14 (Evans, Isaak, Narayan, 2000) *If $k, m \geq 2$ and $p_i, \dots, p_{i+m-1}$ are the first m consecutive primes greater than or equal to m, then $rep(kK_m) = p_i \dots p_{i+m-1}$ if and only if $N(m) \geq k - 1$.*

Proof. See Theorem 4.3 in [35]. □

As an example, consider $rep(4K_{10})$. It is not known if there exists a set of 3 MOLS of order 10 or not. If such a set of MOLS exists then $rep(4K_{10})$ is the product of ten consecutive primes starting with 11. If no such set of MOLS exists, then we know that $rep(4K_{10})$ must be a product of at least ten distinct primes, none smaller than 11. We also known that $4K_{10}$ is isomorphic to an induced subgraph of $4K_{11}$ and that $rep(4K_{11})$ is the product of eleven consecutive primes starting with 11, giving us an upper bound on $rep(4K_{10})$.

3 Existence

In the study of orthomorphism graphs, a natural first question to ask is, "Which groups admit orthomorphisms?" The existence question has been studied in terms of complete mappings of groups. Recall that we called a permutation $\theta\colon G \to G$ a complete mapping of a group G if the mapping $x \mapsto x\theta(x)$ is a permutation of G. Orthomorphisms and complete mappings are closely related as if θ is an orthomorphism of G, then the mapping $x \mapsto x^{-1}\theta(x)$ is a complete mapping of G, and if θ is a complete mapping of G, then the mapping $x \mapsto x\theta(x)$ is an orthomorphism of G. Hence, a group admits orthomorphisms if and only if it admits complete mappings. Groups that admit complete mappings are said to be *admissible.*

The strongest nonexistence result was obtained by Hall and Paige [39] in 1955.

Theorem 15 (Hall and Paige, 1955) *If the Sylow 2-subgroup of a finite group G is nontrivial and cyclic, then G is* not *admissible.*

Theorem 15 suggested that the structure of a group's Sylow 2-subgroup might play a crucial role in determining whether a finite group is admissible. Hall and Paige conjectured its converse.

Conjecture 3 (Hall-Paige conjecture) *If the Sylow* 2*-subgroup of a finite group* G *is trivial or noncyclic, then* G *is admissible.*

Admissible finite abelian groups had already been characterized by Paige [52] in 1947. A finite abelian group is admissible if and only if its Sylow 2-subgroup is trivial or noncyclic. Any group of odd order is admissible as the identity mapping is a complete mapping. Hall and Paige [39] proved their conjecture true for alternating groups, symmetric groups, certain Frobenius groups, and solvable groups. In the intervening years the Hall-Paige conjecture has been proved for several classes of groups. The Mathieu groups were proved to be admissible by Dalla Volta and Gavioli [19] in 1993. The Suzuki groups, $Sz\,(2^{2n+1})$, $n \geq 1$, the unitary groups, $SU(3,q)$ and $PSU(3,q)$, q even, and the Frobenius groups, with Frobenius subgroups being noncyclic Sylow 2 subgroups, were proved to be admissible by Di Vincenzo [22] in 1989. Note that an alternative notation for $SU(3,q)$ and $PSU(3,q)$ is $SU(3,q^2)$ and $PSU(3,q^2)$ as is used in [22]. $SL(2,q)$, $q \neq 2$, was proved to be admissible for q even by Saeli [56] in 1989, for $q \equiv 1 \pmod 4$ by Evans [26] in 2001, and for $q \equiv 3 \pmod 4$ by Evans [27] in 2005. $PSL(2,q)$, q odd, was proved to be admissible by Dalla Volta and Gavioli [19, 20], the case $q \equiv 3 \pmod 4$ in 1993, and the case $q \equiv 1 \pmod 4$ in 1997. $SL(n,q)$, $GL(n,q)$, $PSL(n,q)$, and $PGL(n,q)$, q even, $n \geq 2$, n and q not both 2, were proved admissible by Dalla Volta and Gavioli [19] in 1993. $PGL(2,q)$, q odd, was proved admissible by Dalla Volta and Gavioli [20] in 1997; and $GL(n,q)$ and $PGL(n,q)$, $n \geq 2$, q odd, were proved admissible by Dalla Volta and Gavioli [20] in 1997.

A different approach to tackling the Hall-Paige conjecture was used by Aschbacher [10]. In unpublished lectures given at NSA in the summer of 1990 he considered possible minimal counterexamples to the Hall-Paige conjecture. He showed that any minimal counterexample to the Hall-Paige conjecture must be close to being simple.

Theorem 16 (Aschbacher, 1990) *If* G *is a minimal counterexample to the Hall-Paige conjecture, then the following hold.*

1. *G has a normal subgroup H.*

2. *$H/Z(H)$ is a nonabelian simple group.*

3. *$H = H'$.*

4. *$C_G(H)$, and G/H are cyclic* 2*-groups.*

The group H in Theorem 16 is a *quasi simple* group. A result of Hall and Paige [39] was the main tool used by Aschbacher.

Theorem 17 (Hall and Paige, 1955) *If* D *is a dual system of coset representatives for* H *in* G*,* θ *and* η *are permutations of* D *such that* $x\theta(x)H = \eta(x)H$ *for all* $x \in D$*, and* H *is admissible, then* G *is admissible.*

For G, H, D, θ, and η as in Theorem 17, we call (H, D, θ, η) an *HP-system*, a term coined by Aschbacher. A number of constructions of complete mappings of finite groups use HP-systems. Aschbacher conjectured the existence of HP-systems for a class of almost simple groups. A group G is *almost simple* if there exists a nonabelian simple group H for which $H \leq G \leq Aut(H)$.

Conjecture 4 (HP-system conjecture) *If G is an almost simple group, $F^*(G)$ is the generalized Fitting subgroup of G, and $G/F^*(G)$ is a cyclic 2-group, then there exists an HP-system (H, D, θ, η), $H \neq G$, the Sylow 2-subgroup of H being noncyclic.*

See [11] for the definition and properties of the generalized Fitting subgroup. Aschbacher showed that the HP-system conjecture implied the Hall-Paige conjecture and proved the HP-system conjecture true for several classes of groups.

Theorem 18 (Aschbacher, 1990) *Let G be an almost simple group whose minimal normal subgroup H is of Lie type over $GF(q)$. If G does not satisfy the HP-system conjecture, then one of the following holds.*

1. *H is of Lie rank 1, q is odd, and G induces inner diagonal automorphisms on H.*
2. *$H = L_n(q)$, $n \geq 3$, G nontrivial on the Dynkin diagram of H.*
3. *$H = Sp_4(q)$ or $F_4(q)$, q even, G nontrivial on the Dynkin diagram of H.*
4. *$H = {}^2F_4(q)$, q even.*

Theorem 19 (Aschbacher, 1990) *An almost simple group whose minimal normal subgroup is a Mathieu group satisfies the HP-system conjecture.*

The breakthrough, that led to the proof of the Hall-Paige conjecture, came in 2009 with the work of Wilcox [58]. Using more elementary methods than Aschbacher, Wilcox significantly reduced the set of possible minimal counterexamples to the Hall-Paige conjecture.

Theorem 20 (Wilcox, 2009) *Any minimal counterexample to the Hall-Paige conjecture must be a finite nonabelian simple group.*

Proof. See Theorem 12 in [58]. □

As the Hall-Paige conjecture had already been proved for alternating groups by Hall and Paige, to complete the proof of the Hall-Paige conjecture it sufficed to prove that none of the simple groups of Lie type or the sporadic simple groups could be minimal counterexamples to the Hall-Paige conjecture. Wilcox proved that none of the simple groups of Lie type, with the possible exception of the Tits group, could be minimal counterexamples to the Hall-Paige conjecture.

Theorem 21 (Wilcox, 2009) *Any minimal counterexample to the Hall-Paige conjecture must be either the Tits group or a sporadic simple group.*

Proof. See Theorem 24 in [58]. □

In proving Theorem 21, Wilcox made extensive use of double cosets, specifically the following tool.

Theorem 22 (Wilcox, 2009) *Let H be a subgroup of a group G and let $\mathcal{D}$ be the set of double cosets of H in G. If H is admissible and there exist permutations ϕ, ψ of $\mathcal{D}$ satisfying*

$$|D| = |\phi(D)| = |\psi(D)| \text{ and } \psi(D) \subseteq D\phi(D)$$

for all $D \in \mathcal{D}$, then G is admissible.

Proof. See Corollary 15 in [58]. □

We call the set $(\mathcal{D}, \phi, \psi)$ in Theorem 22 a *W-system.* Given a W-system for a subgroup H of G, if the Sylow 2-subgroup of H is noncyclic, then G cannot be a minimal counterexample to the Hall-Paige conjecture. One class of W-sytems proved particularly useful, the simple W-systems: we say that a W-system is *simple* if both ϕ and ψ are the identity mapping.

Corollary 7 *If $D \subseteq D^2$ for every $D \in \mathcal{D}$, then $(\mathcal{D}, \iota, \iota)$ is a W-system, where ι is the identity map.*

Proof. See Corollary 16 in [58]. □

The Mathieu groups had already been proved admissible by Dalla Volta and Gavioli [19] in 1993. Thus Theorem 21 reduced the number of possible minimal counterexamples to the Hall-Paige conjecture to just 22. In 2009 Evans [29] made extensive use of W-systems, many of them simple W-systems, to reduce the number of potential minimal counterexamples to the Hall-Paige conjecture to just one, J_4, Janko's fourth group.

Theorem 23 (Evans, 2009) *If G is a minimal counterexample to the Hall-Paige conjecture, then $G \cong J_4$.*

In the proof of Theorem 23, W-sytsems were constructed from collapsed adjacency matrices: see [54] for the definition. In 1997 Praeger and Soicher [54] computed a number of collapsed adjacency matrices for the sporadic simple groups. These matrices, as well as collapsed adjacency matrices in the GAP database [15], proved essential in proving Theorem 23.

Bray [16] has a proof that J_4 is not a minimal counterexample to the Hall-Paige conjecture, thus completing a proof of the Hall-Paige conjecture. Bray's proof was obtained by computing collapsed adjacency matrices for the permutation representation of J_4 of degree 3,980,549,947 with point-stabiliser isomorphic to $2_+^{1+12}{\cdot}3M_{22} : 2$, from which the existence of a W-system could be determined. Bray's proof has not been published yet.

4 Data for small groups

Our knowledge of $|Orth(G)|$ and $\omega(G)$ for groups of order at most 23 is summarized in Table 2. Any group whose Sylow 2-subgroup is nontrivial and cyclic is omitted from this table as, by Theorem 15, these groups do not admit orthomorphisms. Recent computer searches have confirmed and extended earlier results. In particular in 2004 Hsiang, Hsu, and Shieh [40] computed $|Orth(\mathbb{Z}_n)|$ for $n \leq 23$; in 2006 McKay, McLeod, and Wanless [49] computed $|Orth(G)|$ for all groups of order at most 23; and in 2004 Lazebnik and Thomason [45] computed $\omega(G)$ for all abelian groups of order at most 16. A more complete explanation for the entries in Table 2 can be found in a monograph [33] currently in preparation.

Group G	Order G	$\lvert Orth(G)\rvert$	$\omega(G)$	Group G	Order G	$\lvert Orth(G)\rvert$	$\omega(G)$
1	1	1	∞	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$	16	14,886,912	6
$GF(3)^+$	3	1	1	$GF(16)^+$	16	15,296,512	14
$GF(4)^+$	4	2	2	$D_8 \times \mathbb{Z}_2$	16	7,849,984	≥ 2
$GF(5)^+$	5	3	3	$Q_8 \times \mathbb{Z}_2$	16	7,571,456	≥ 2
$GF(7)^+$	7	19	5	$Pauli$	16	7,710,720	≥ 2
$\mathbb{Z}_2 \times \mathbb{Z}_4$	8	48	2	$G_{4,4}$	16	7,743,488	≥ 2
D_8	8	48	1	$\mathbb{Z}_4 \rtimes \mathbb{Z}_4$	16	7,636,992	≥ 2
Q_8	8	48	1	Mod_{16}	16	7,608,320	≥ 2
$GF(8)^+$	8	48	6	D_{16}	16	3,930,112	≥ 3
$\mathbb{Z}_9$	9	225	1	SD_{16}	16	3,913,728	≥ 1
$GF(9)^+$	9	249	7	Q_{16}	16	3,897,344	≥ 1
$GF(11)^+$	11	3441	9	$GF(17)^+$	17	94,471,089	15
$\mathbb{Z}_2 \times \mathbb{Z}_6$	12	16,512	4	$GF(19)^+$	19	4,613,520,889	17
D_{12}	12	6,336	2	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$	20	34,864,619,520	≥ 3
A_4	12	3,840	1	D_{20}	20	7,043,328,000	≥ 2
$GF(13)^+$	13	79,259	11	$\mathbb{Z}_{21}$	21	275,148,653,115	≥ 4
$\mathbb{Z}_{15}$	15	2,424,195	3	$\mathbb{Z}_7 \rtimes \mathbb{Z}_3$	21	39,372,127,200	≥ 1
$\mathbb{Z}_2 \times \mathbb{Z}_8$	16	14,735,360	3	$GF(23)^+$	23	19,686,730,313,955	21
$\mathbb{Z}_4 \times \mathbb{Z}_4$	16	14,813,184	6				

Table 2: Data for small groups.

Some of the values for $|Orth(G)|$ in Table 2 have also been determined theoretically. Clearly the only orthomorphism of the trivial group is the identity mapping. For elementary abelian groups any orthomorphism can be represented by a permutation polynomial. A *permutation polynomial* of a field $GF(q)$ is a polynomial, f, over $GF(q)$ for which the mapping $x \mapsto f(x)$ is a permutation of $GF(q)$. As any mapping $GF(q) \to GF(q)$ can be represented by a polynomial, any orthomorphism of $GF(q)^+$ can be represented by an orthomorphism polynomial. An *orthomorphism polynomial* of $GF(q)^+$ is a permutation polynomial, f, of $GF(q)$ for which the mapping $x \mapsto f(x) - x$ is also a permutation polynomial. A complete list of permutation polynomials of degree at most 5 can be found in [46]. As any orthomorphism of $GF(q)^+$ can be represented by an orthomorphism polynomial of degree at most $q-3$, this list enables us to determine all orthomorphisms of elementary abelian groups of order at most 8. Recently Shallue and Wanless [57] extended the list in [46] by determining all permutation polynomials of degree 6, from which they computed all orthomorphism polynomials of $GF(9)^+$. In 1999 Bedford and Whitaker [13] gave a theoretical proof that all noncyclic groups of order 8 have 48 normalized orthomorphisms. Other than for the trivial group, elementary abelian groups of order at most 9, and groups of order 8, all other values of $|Orth(G)|$ in Table 2 have only been obtained via computer searches. As the identity mapping is orthogonal to itself, we set $\omega(1) = \infty$. For the elementary abelian groups, $GF(q)^+$, the linear orthomorphisms, $[a]\colon x \mapsto ax$, $a \neq 0, 1$, form a complete set of orthomorphisms of $GF(q)^+$, from which it follows that $\omega(GF(q)^+) = q - 2$. Other than for the trivial group and the elementary abelian groups, all other values of $\omega(G)$ in Table 2 have only been obtained via computer searches.

If we compare $\omega(G)$, G a direct product of elementary abelian groups, in Table 2 with the table of lower bounds for $N(n)$ given in [18], we see that in each case the lower bounds match, that is, $\omega(G) + 1$ yields the current lower bound for $N(n)$ if $|G| = n \leq 23$, $n \not\equiv 2 \pmod 4$, and G is a direct product of elementary abelian groups. A number of the lower bounds for $N(n)$ have been obtained by improving lower bounds for $\omega(G)$, G a direct product of elementary abelian groups. We list some of the known lower bounds for $\omega(G)$ for groups that are direct products of elementary abelian groups in Table 3. Some of these lower bounds do not exceed the MacNeish bound. In 1922 MacNeish [48] proved that, if $n = q_1 \dots q_m$, $q_1, \dots, q_m$ powers of distinct primes, then $N(n) \geq \min\{q_1 - 1, \dots, q_m - 1\}$: this is the *MacNeish bound.*

Group G	Order G	$\omega(G) \geq$	Group G	Order G	$\omega(G) \geq$
$GF(8)^+ \times GF(3)^+$	24	$6^\dagger$	$GF(8)^+ \times GF(7)^+$	56	$6^\dagger$
$GF(7)^+ \times GF(4)^+$	28	$4^\dagger$	$GF(3)^+ \times GF(19)^+$	57	$6^\dagger$
$GF(11)^+ \times GF(3)^+$	33	$4^\dagger$	$GF(4)^+ \times GF(3)^+ \times GF(5)^+$	60	$3^\dagger$
$GF(7)^+ \times GF(5)^+$	35	$4^\dagger$	$GF(9)^+ \times GF(7)^+$	63	$5^{*\dagger}$
$GF(9)^+ \times GF(4)^+$	36	$7^\dagger$	$GF(5)^+ \times GF(13)^+$	65	3^*
$GF(13)^+ \times GF(3)^+$	39	$4^\dagger$	$GF(4)^+ \times GF(17)^+$	68	2^*
$GF(8)^+ \times GF(5)^+$	40	$6^\dagger$	$GF(3)^+ \times GF(23)^+$	69	3
$GF(11)^+ \times GF(4)^+$	44	$4^\dagger$	$GF(8)^+ \times GF(9)^+$	72	$6^{*\dagger}$
$GF(9)^+ \times GF(5)^+$	45	$5^\dagger$	$GF(3)^+ \times GF(25)^+$	75	$6^\dagger$
$GF(16)^+ \times GF(3)^+$	48	$7^\dagger$	$GF(4)^+ \times GF(19)^+$	76	2^*
$GF(17)^+ \times GF(3)^+$	51	$4^\dagger$	$GF(7)^+ \times GF(11)^+$	77	5^*
$GF(13)^+ \times GF(4)^+$	52	$4^\dagger$	$GF(16)^+ \times GF(5)^+$	80	$8^\dagger$
$GF(11)^+ \times GF(5)^+$	55	$5^\dagger$	$GF(4)^+ \times GF(3)^+ \times GF(7)^+$	84	4

* Does not exceed the MacNeish bound.
† Agrees with current lower bounds for $N(n)$.

Table 3: Some lower bounds for $\omega(G)$.

Most of the current lower bounds for $\omega(G)$ in Table 3 yield current lower bounds for $N(n)$. A number of the entries in Table 3 are the result of computer searches, establishing that $\omega(G) \geq r$ by finding a $(|G|, r + 2; 1)$-difference matrix over G. In 2008 Abel [1] found a $(28, 6; 1)$-difference matrix over $GF(7)^+ \times GF(4)^+$, a $(44, 6; 1)$-

difference matrix over $GF(11)^+ \times GF(4)^+$, and a $(52,6;1)$-difference matrix over $GF(13)^+ \times GF(4)^+$. In 2003 Abel and Bennett [2] found a $(45,7;1)$-difference matrix over $GF(9)^+ \times GF(5)^+$. In 2007 Abel and Cavenagh [3] found a $(48,9;1)$-difference matrix over $GF(16)^+ \times GF(3)^+$. In 1994 Abel and Cheng [4] found a $(40,8;1)$-difference matrix over $GF(8)^+ \times GF(5)^+$, and an $(80,9;1)$-difference matrix over $GF(16)^+ \times GF(5)^+$. In 2004 Abel and Colbourn and Wojta [5] found a $(24,8;1)$-difference matrix over $GF(8)^+ \times GF(3)^+$, a $(36,9;1)$-difference matrix over $GF(9)^+ \times GF(4)^+$, and a $(75,8;1)$-difference matrix over $GF(3)^+ \times GF(25)^+$. In 2005 Abel and Ge [7] found a $(33,6;1)$-difference matrix over $GF(11)^+ \times GF(3)^+$, a $(39,6;1)$-difference matrix over $GF(13)^+ \times GF(3)^+$, and a $(51,6;1)$-difference matrix over $GF(17)^+ \times GF(3)^+$. In 1977 Mills [51] found a $(56,8;1)$-difference matrix over $GF(8)^+ \times GF(7)^+$. In 1996 Wojta [59] found a $(35,6;1)$-difference matrix over $GF(7)^+ \times GF(5)^+$, and in 2000 Wojta [60] found a $(55,7;1)$-difference matrix over $GF(11)^+ \times GF(5)^+$.

The remaining entries in Table 3 can be derived from general results that will be given in Section 5. The bound $\omega(GF(3)^+ \times GF(19)^+) \geq 6$ is derived from Theorem 34 with $q = 7$, and the bound $\omega(GF(3)^+ \times GF(23)^+) \geq 3$ is derived from Theorem 33. The bounds $\omega(GF(4)^+ \times GF(3)^+ \times GF(5)^+) \geq 3$ and $\omega(GF(4)^+ \times GF(3)^+ \times GF(7)^+) \geq 4$ are derived from Theorem 28, and the bounds that do not exceed the MacNeish bound, $\omega(GF(9)^+ \times GF(7)^+) \geq 5$, $\omega(GF(5)^+ \times GF(13)^+) \geq 3$, $\omega(GF(4)^+ \times GF(17)^+) \geq 2$, $\omega(GF(8)^+ \times GF(9)^+) \geq 6$, $\omega(GF(4)^+ \times GF(19)^+) \geq 2)$, and $\omega(GF(7)^+ \times GF(11)^+) \geq 5$ are all derived from Corollary 9.

5 Bounds on $\omega(G)$

In Section 4 we gave known bounds on $\omega(G)$ for groups of order at most 23. In this section we will describe more general bounds on $\omega(G)$. The most general bounds on $\omega(G)$, G nontrivial, are given in the following theorem and its corollary.

Theorem 24 *If G is a group of order $n > 1$ and if p is the smallest prime divisor of n, then*

$$p - 2 \leq \omega(G) \leq n - 2.$$

Proof. By Theorem 1, $p - 2 = \omega(\mathcal{P}(G)) \leq \omega(G)$. Further $\omega(G) + 1 \leq N(n) \leq n - 1$. □

The following is an almost immediate corollary.

Corollary 8 *If G is a group of order $n > 1$, whose Sylow 2-subgroup is noncyclic, then*

$$1 \leq \omega(G) \leq n - 2.$$

Proof. The proof that $\omega(G) \geq 1$ was outlined in Section 3. □

For many groups the bounds in Theorem 24 and Corollary 8 are the best available bounds. The question arises as to when the upper bound is achieved.

Problem 7 *For which groups G is $\omega(G) = |G| - 2$?*

The only groups for which $\omega(G)$ is known to be $|G|-2$ are the elementary abelian groups.

Theorem 25 *If G is elementary abelian, then $\omega(G) = |G| - 2$.*

Proof. Without loss of generality $G = GF(q)^+$ for some prime power q. The linear orthomorphisms $[a]\colon x \mapsto ax$, $a \neq 0, 1$, form a $(q-2)$-clique of $Orth(G)$. □

The well-known prime power conjecture asserts that the order of a projective plane is always a prime power. As a projective plane of order n corresponds to a complete set of MOLS of order n, the prime power conjecture for projective planes naturally yields a prime power conjecture for complete sets of orthomorphisms.

Conjecture 5 (Prime power conjecture) *If $\omega(G) = |G|-2$, then $|G|$ is a power of a prime.*

By Theorem 25, for all prime powers there exist groups admitting complete sets of orthomorphisms, the elementary abelian groups, but no groups of prime power order, other than the elementary abelian groups, are known to admit complete sets of orthomorphisms.

Problem 8 *Does there exist a group of prime power order, that is not elementary abelian, for which $\omega(G) = |G| - 2$?*

In 1949 Bruck and Ryser [17] proved the Bruck-Ryser theorem, establishing the nonexistence of projective planes of certain orders. The only improvement to their result is the 1986 proof by Lam, Thiel, and Swiercz [44] that no projective plane of order 10 exists. The Bruck-Ryser theorem yields a nonexistence result for complete sets of orthomorphisms for groups of certain orders.

Theorem 26 (Bruck and Ryser, 1949) *Let G be a group of order n. If $n \equiv 1$ or $2 \pmod 4$ and n is not a sum of two squares, then $\omega(G) < n - 2$.*

It should be noted that, if $|G| = n$ and n satisfies the conditions of Theorem 26, then the upper bound can be improved as $\omega(G)$ cannot then exceed the Bruck bound or the Metsch bound: see Theorem 3.32, section III.3 of [18]. If $|G| = n$ and $\omega(G)+1$ exceeds either of these bounds, then $N(n) = n - 2$.

In 1984 De Launey [21] proved the nonexistence of certain generalized Hadamard matrices. A *generalized Hadamard matrix*, $GH(n, \lambda)$, of *index* λ over a group G, of order n, is an $(n, \lambda n; \lambda)$-difference matrix over G. A complete set of orthomorphisms of G, of order n, corresponds to a $GH(n, 1)$ over G.

Theorem 27 (De Launey, 1984) *If $H \lhd G$, $|G| = n$, $|H| = m$, then $\omega(G) < n-2$ if*

- *$n/m = 3$, $n = 3^t p_1^{k_1} \dots p_s^{k_s}$, where $p_1, \dots, p_s$ are distinct primes, and, for some i, $p_i \equiv 5 \pmod 6$ and k_i is odd,*

- *$n/m = 5$, $n = 3^t 7^k s$, where s is odd, $\gcd(s, 21) = 1$, and one of t, k is odd, or*

- *$n/m = 7$, $n = 3^t s$, where $\gcd(s, 3) = 1$, and t and s are both odd.*

There are several quotient group constructions in the literature for abelian groups. In 1999 Quinn [55] established a quotient group construction for nonabelian as well as abelian groups.

Theorem 28 (Quinn, 1999) *If $H \lhd G$, then $\omega(G) \geq \min(\omega(H), \omega(G/H))$.*

Quotient group constructions yield many examples of improved lower bounds for $\omega(G)$. Theorem 28 explains two entries in Table 3,

$$\omega(GF(4)^+ \times GF(3)^+ \times GF(5)^+) \geq \min\{\omega(GF(4)^+ \times GF(3)^+), \omega(GF(5)^+)\} \geq \min\{4, 3\} = 3,$$

and

$$\omega(GF(4)^+ \times GF(3)^+ \times GF(7)^+) \geq \min\{\omega(GF(4)^+ \times GF(3)^+), \omega(GF(7)^+)\} \geq \min\{4, 5\} = 4.$$

A special case of the quotient group construction is the direct product construction that corresponds to the Kronecker product construction for latin squares.

Theorem 29 *If $\theta \in Orth(G)$ and $\phi \in Orth(H)$, then the mapping $\theta \times \phi \colon G \times H \to G \times H$, defined by $\theta \times \phi(g, h) = (\theta(g), \phi(h))$, is an orthomorphism of $G \times H$. Further if $\theta, \theta' \in Orth(G)$ are orthogonal and $\phi, \phi' \in Orth(H)$ are orthogonal, then $\theta \times \phi$ and $\theta' \times \phi'$ are orthogonal.*

Proof. Routine. □

An immediate corollary.

Corollary 9 *If G and H are finite groups, then $\omega(G \times H) \geq \min(\omega(G), \omega(H))$.*

We turn now to the problem of improving the lower bounds in Theorem 24 and Corollary 8 for finite abelian groups. This requires a class of orthomorphisms that are also automorphisms. A *fixed-point-free automorphism* of a group is an automorphism that fixes only the identity. An automorphism of a group is an orthomorphism of the group if and only if it is fixed-point-free. Fixed-point-free automorphisms are used in the construction of translation nets. Using fixed-point-free automorphisms, in 1990 Bailey and Jungnickel [12] derived a lower bound for $\omega(G)$ when G is a finite abelian group. First, in 1989, Jungnickel [43] derived a lower bound for $\omega(G)$ when G is a finite abelian group of prime power order.

Theorem 30 (Jungnickel, 1989) *If p is a prime and $G = m_1\mathbb{Z}_{p^{k_1}} \times \cdots \times m_r\mathbb{Z}_{p^{k_r}}$, then*

$$\omega(G) \geq p^m - 2,$$

where $m = \min\{m_i \mid i = 1, \ldots, k\}$.

Proof. The proof involves constructing a pairwise orthogonal set of $p^m - 2$ fixed-point-free automorphisms of G. □

In 1990 Theorem 30 was generalized by Bailey and Jungnickel [12] to finite abelian groups in general.

Theorem 31 (Bailey and Jungnickel, 1990) *Let G be an abelian group, $p_1, \ldots,$ p_m the distinct prime divisors of $|G|$, and let S_{p_i} denote the Sylow p_i-subgroup of G. Then*

$$\omega(G) \geq \min(\omega(S_{p_1}), \ldots, \omega(S_{p_m})).$$

Proof. The proof uses Theorem 30 and direct product constructions. □

In Theorem 31, if we restrict ourselves to the orthomorphism graph $\mathcal{A}(G)$, consisting of fixed-point-free automorphisms of G, then

$$\omega(\mathcal{A}(G)) = \min(\omega(S_{p_1}), \ldots, \omega(S_{p_m})).$$

For many abelian groups, the bound in Theorem 31 has not been improved upon.

Problem 9 *Improve the lower bounds for $\omega(G)$, G abelian.*

A number of results have been obtained for cyclic groups. In 2005 Ge [38] established a general lower bound for cyclic groups.

Theorem 32 (Ge, 2005) *If $n \geq 5$ is odd and $\gcd(n, 27) = 1$ or 27, then $\omega(\mathbb{Z}_n) \geq 3$.*

Note that, if $n > 1$ is odd and not divisible by 3 or 5, then Theorem 24 yields a better lower bound for $\omega(\mathbb{Z}_n)$. Ge's result was extended to the case $n = 3m$, m not divisible by 2 or 3, by Evans [28] in 2007.

Theorem 33 (Evans, 2007) *If $n = 3m$, $m > 1$, m odd and not divisible by 3, then $\omega(\mathbb{Z}_n) \geq 3$.*

This leaves the case $n = 9m$, m not divisible by 2 or 3.

Problem 10 *For which m, $\gcd(m, 6) = 1$, is $\omega(\mathbb{Z}_{9m}) \geq 3$?*

It is known that $\omega(\mathbb{Z}_{9m}) \geq 3$, $\gcd(m, 6) = 1$, for many values of m: see [6]. In 1980 and 1981 Jungnickel [41, 42] gave a number of constructions of difference matrices using difference sets, relative difference sets, difference families, and relative difference families.

Theorem 34 (Jungnickel, 1980) *If q is a prime power, then*

$$\omega(\mathbb{Z}_{q^2+q+1}) \geq N(q+1) - 1.$$

Proof. The proof uses planar difference sets to construct $(q^2+q+1, r+1; 1)$-difference matrices over $\mathbb{Z}_{q^2+q+1}$ from sets of r MOLS of order $q+1$. □

Theorem 35 (Jungnickel, 1980) *If q is a prime power, then*

$$\omega(\mathbb{Z}_{q^2-1}) \geq \omega(\mathbb{Z}_{q-1}).$$

Proof. The proof uses relative difference sets to construct $(q^2-1, r+1; 1)$-difference matrices over $\mathbb{Z}_{q^2-1}$ from $(q-1, r+1; 1)$-difference matrices over $\mathbb{Z}_{q-1}$. □

Theorem 36 (Jungnickel, 1981) *If q is a prime power, then*

$$\omega(\mathbb{Z}_{q^n+\cdots+q+1}) \geq \begin{cases} N(q+1)-1 & \textit{if } n \textit{ is even,} \\ \omega(\mathbb{Z}_{q-1}) & \textit{if } n \textit{ is odd.} \end{cases}$$

Proof. The proof uses difference families to construct $(q^n + \cdots + q + 1, r+1; 1)$-difference matrices over $\mathbb{Z}_{q^n+\cdots+q+1}$ from sets of r MOLS of order $q+1$ when n is even, and to construct $(q^n + \cdots + q + 1, r+1; 1)$-difference matrices over $\mathbb{Z}_{q^n+\cdots+q+1}$ from $(q-1, r+1; 1)$-difference matrices over $\mathbb{Z}_{q-1}$ when n is odd. □

Theorem 37 (Jungnickel, 1981) *If q is a prime power, then*

$$\omega(\mathbb{Z}_{q^n-1}) \geq \omega(\mathbb{Z}_{q-1}).$$

Proof. The proof uses relative difference families to construct $(q^n-1, r+1; 1)$-difference matrices over $\mathbb{Z}_{q^n-1}$ from $(q-1, r+1; 1)$-difference matrices over $\mathbb{Z}_{q-1}$. □

Problem 11 *Improve lower bounds for $\mathbb{Z}_n$.*

Except for groups of small order and results obtained through quotient group constructions, very little is known about the value of $\omega(G)$ when G is nonabelian. For dihedral groups of doubly even order, $GL(2,q)$ and $SL(2,q)$, q even, and $GL(n,q)$, q even, reasonable lower bounds for $\omega(G)$ have been obtained. For the dihedral groups we will use D_n to denote the dihedral group of order n. The first improvement for $\omega(D_n)$ was given by Bowler [14] in 1997.

Theorem 38 (Bowler, 1997) *If $n \equiv 1, 5 \pmod 6$, then $\omega(D_{4n}) \geq 2$.*

In 1999 Quinn [55] improved this lower bound.

Lemma 6 (Quinn, 1999) *If $n = 2^k m$, m odd, then*

$$\omega(D_{2n}) \geq \min(\omega(\mathbb{Z}_m), \omega(D_{2^{k+1}})).$$

Table 4: Lower bounds for $\omega(D_{2^{k+1}})$

k	1	2	3	≥ 4
$\omega(D_{2^{k+1}})$	2	1	≥ 3	≥ 1

Proof. This follows from Theorem 28. □

Quinn improved the bound in Theorem 38 for D_{16}.

Theorem 39 (Quinn, 1999) *$\omega(D_{16}) \geq 3$.*

The known lower bounds for $\omega(D_{2^{k+1}})$ are given in Table 4.

For $k \geq 4$, the current lower bound for $\omega(D_{2^{k+1}})$, namely 1, is that given in Corollary 8.

Problem 12 *Improve lower bounds for $\omega(D_{2^{k+1}})$.*

For linear groups, the first improvement on the lower bound of Corollary 8 was given by Evans [25] in 1993.

Theorem 40 (Evans,1993) *If q is even, $q \neq 2$, then*

$$\omega(GL(2,q)) \text{ and } \omega(SL(2,q)) \geq \min(\omega(\mathbb{Z}_{q-1}), \omega(\mathbb{Z}_{q+1})).$$

Proof. The proof is obtained by partitioning the elements of a group G into equivalence classes, $x \equiv y$ if $C_G(x) = C_G(y)$, and then stitching together orthomorphisms of these equivalence classes. □

As examples,

$$\omega(GL(2,16)), \omega(SL(2,16)) \geq \min(\omega(\mathbb{Z}_{15}), \omega(\mathbb{Z}_{17})) = \min(3,15) = 3,$$

and

$$\omega(GL(2,32)), \omega(SL(2,32)) \geq \min(\omega(\mathbb{Z}_{31}), \omega(\mathbb{Z}_{33})) \geq \min(29,4) = 4.$$

The lower bound of Theorem 40 has recently been extended to $\omega(GL(n,q))$, q even, by Evans [32].

Theorem 41 (Evans, 2012) *If q is even, $q \neq 2$, then*

$$\omega(GL(n,q)) \geq \min(\omega(\mathbb{Z}_{quot_1(q)}), \ldots, \omega(\mathbb{Z}_{quot_n(q)})),$$

where

$$quot_n(q) = \begin{cases} q-1 & \text{if } n = 1, \\ (q^n - 1)/lcm\{q^i - 1 \mid i \text{ divides } n,\ i \neq n\} & \text{if } n > 1. \end{cases}$$

Proof. The proof is obtained by combining pairwise orthogonal sets of orthomorphisms of U the set of 2-elements of $GL(n,q)$ and S the set of odd-order elements of $GL(n,q)$ to obtain pairwise orthogonal sets of orthomorphisms of $GL(n,q)$. □

As a corollary we obtain a simple lower bound for the special case $n = 3$.

Corollary 10 *If q is even, $q \neq 2$, then*

$$\omega(GL(3,q)) \geq \min(\omega(\mathbb{Z}_{q-1}), \omega(\mathbb{Z}_{q+1}), \omega(\mathbb{Z}_{q^2+q+1})).$$

As examples

$$\omega(GL(3,16)) \geq \min(\omega(\mathbb{Z}_{15}), \omega(\mathbb{Z}_{17}), \omega(\mathbb{Z}_{307})) = \min(3, 15, 305) = 3,$$

and

$$\omega(GL(3,32)) \geq \min(\omega(\mathbb{Z}_{31}), \omega(\mathbb{Z}_{33}), \omega(\mathbb{Z}_{1{,}057})) \geq \min(29, 4, 5) = 4.$$

Problem 13 *Improve the lower bounds for $\omega(G)$ for more classes of nonabelian groups.*

References

[1] R. J. R. Abel, Some $V(12,t)$ vectors and other designs from difference and quasi-difference matrices, *Australas. J. Combin.* **40** (2008), 69–85.

[2] R. J. R. Abel and F. E. Bennett, The existence of 2-SOLSSOMs, in *"Designs 2002"*, W. D. Wallis (ed.), 1–21, Kluwer, Boston, 2003.

[3] R. J. R. Abel and N. J. Cavenagh, Concerning eight mutually orthogonal latin squares, *J. Combin. Des.* **15** (2007), 255–261.

[4] R. J. R. Abel and Y. W. Cheng, Some new MOLS of order $2^n p$ for p a prime power, *Australas. J. Combin.* **10** (1994), 175–186.

[5] R. J. R. Abel, C. J. Colbourn and M. Wojtas, Concerning seven and eight mutually orthogonal latin squares, *J. Combin. Des.* **12** (2004), 123–131.

[6] 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** (2006), 1649–1673.

[7] R. J. R. Abel and G. Ge, Some difference matrix constructions and an almost completion for the existence of triplewhist tournaments $TWh(v)$, *Europ. J. Combin.* **26** (2005), 1094–1104.

[8] A. Agarwal and M. Lopez, Representation number for complete graphs minus stars, preprint.

[9] R. Akhtar, A. B. Evans and D. Pritikin, Representation numbers of stars, *Integers* **10** (2010), A54, 733–745.

[10] M. Aschbacher, Lectures delivered at NSA (1990).

[11] M. Aschbacher, *Finite group theory*, 2nd ed., Cambridge University Press, Cambridge, 2000.

[12] R. A. Bailey and D. Jungnickel, Translation nets and fixed-point-free group automorphisms, *J. Combin. Theory Ser. A* **55** (1990), no. 1, 1–13.

[13] D. Bedford and R. M. Whitaker, Enumeration of transversals in the Cayley tables of the non-cyclic groups of order 8, *Discrete Math.* **197/198** (1999), 77–81.

[14] A. Bowler, Orthomorphisms of dihedral groups, *Discrete Math.* **167/168** (1997), 141–144.

[15] T. Breuer and J. Müller, Character tables of endomorphism rings of multiplicity-free permutation modules in GAP, `http://www.math.rwth-aachen.de/∼Juergen.Mueller/mferctbl/mferctbl.html`.

[16] J. N. Bray, personal communication.

[17] R.H. Bruck and H. J. Ryser, The nonexistence of certain finite projective planes, *Canad. J. Math.* **1** (1949), 88–93.

[18] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs*, 2nd. ed., Chapman & Hall/CRC, Florida, 2007.

[19] F. Dalla Volta and N. Gavioli, Complete mappings in some linear and projective groups, *Arch. Math.* (Basel) **61** (1993), no. 2, 111–118.

[20] F. Dalla Volta and N. Gavioli, On the admissibility of some linear and projective groups in odd characteristic, *Geom. Ded.* **66** (1997), 245–254.

[21] W. De Launey, On the nonexistence of generalized Hadamard matrices, *J. Statist. Plann. Inference* **10** (1984), 385–396.

[22] O. M. Di Vincenzo, On the existence of complete mappings of finite groups, *Rend. Mat. Appl.* (7) **9** (1989), 189–198.

[23] P. Erdős and A. B. Evans, Representations of graphs and orthogonal latin square graphs, *J. Graph Theory* **13** (1989), no. 5, 593–595.

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

[25] A. B. Evans, Mutually orthogonal Latin squares based on linear groups, in *Coding theory, design theory, group theory* (Burlington, VT, 1990), 171–175, Wiley-Intersci. publ., 1993.

[26] A. B. Evans, The existence of complete mappings of $\mathrm{SL}(2, q)$, $q \equiv 1 \pmod 4$, *Finite Fields Applic.* **7** (2001), no. 3, 373–381.

[27] A. B. Evans, The Existence of Complete Mappings of $SL(2, q)$, $q \equiv 3 \pmod 4$, *Finite Fields Applic.* **11** (2005), 151–155.

[28] A. B. Evans, On orthogonal orthomorphisms of cyclic and non-abelian groups. II, *J. Combin. Des.* **15** (2007), 195–209.

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

[30] A. B. Evans, The existence of strong complete mappings, *Electron. J. Combin.* **19** (2012), no. 1, Paper 34, 10 pp.

[31] A. B. Evans, The existence of strong complete mappings of finite groups: a survey, *Discrete Math.* **313** (2013), 1191-1196.

[32] A. B. Evans, Mutually orthogonal latin squares based on general linear groups, *Des. Codes Cryptogr.* DOI 10.1007/s10623-012-9752-9.

[33] A. B. Evans, Orthogonal latin squares based on groups, monograph in preparation.

[34] A. B. Evans, G. H. Fricke, C. C, Maneri, T. A. McKee and M. Perkel, Representations of graphs modulo n, *J. Graph Theory* **18** (1994), no. 8, 801–815.

[35] A. B. Evans, G. Isaak and D. A. Narayan, Representations of graphs modulo n, *Discrete Math.* **223** (2000), no. 1-3, 109–123.

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

[37] A. B. Evans, D. A. Narayan and J. Urick, Representations of graphs modulo n: some problems, *Bull. Inst. Combin. Applic.* **56** (2009), 85–97.

[38] G. Ge, On $(g, 4; 1)$-difference matrices, *Discrete Math.* **301** (2005), 164–174.

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

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

[41] D. Jungnickel, On difference matrices and regular latin squares, *Abh. Math. Sem. Univ. Hamburg* **50** (1980), 219–231.

[42] D. Jungnickel, Einige neue Differenzenmatrizen, *Mitt. Math. Sem. Giessen* **149** (1981), 47–57.

[43] D. Jungnickel, Partial spreads over $\mathbb{Z}_q$, *Linear Algebra Appl.* **114** (1989), 95–102.

[44] C. W. H. Lam, L. H. Thiel and S. Swiercz, A computer search for a projective plane of order 10, in *Algebraic, extremal and metric combinatorics*, 1986 (Montreal, PQ, 1986), 155–165, London Math. Soc. Lec. Note Ser. 131, Cambridge Univ. Press, Cambridge, 1988.

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

[46] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of mathematics and its applications **20**, Addison-Wesley, Reading, 1983.

[47] C. C. Lindner, E. Mendelsohn, N. S. Mendelsohn and B. Wolk, Orthogonal latin square graphs, *J. Graph Theory* **3** (1979), 325–338.

[48] H. F. MacNeish, Euler squares, *Annals Math.* **23** (1922), 221–227.

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

[50] G. O. Michler, *Theory of finite simple groups*, Cambridge University Press, Cambridge, 2006.

[51] W. H. Mills, Some mutually orthogonal latin squares, *Congr. Numer.* **19** (1977), 473–487.

[52] L. J. Paige, A note on finite abelian groups, *Bull. Amer. Math. Soc.* **53** (1947), 590–593.

[53] D. Peterson, Gridline graphs: a review in two dimensions and an extension to higher dimensions, *Discrete Appl. Math.* **126** (2003), 223–239.

[54] C. E. Praeger and L. H. Soicher, *Low rank representations and graphs for sporadic groups*, Cambridge University Press, Cambridge, 1997.

[55] K. A. S. Quinn, Difference matrices and orthomorphisms over non-abelian groups, *Ars Combin.* **52** (1999), 289–295.

[56] D. Saeli, Complete mappings and difference ratio in double loops, *Riv. Mat. Univ. Parma* (4) **15** (1989), 111–117.

[57] C. J. Shallue and I. M. Wanless, Permutation polynomials and orthomorphism polynomials of degree six, *Finite Fields Applic.* **20** (2013), 84–92.

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

[59] M. Wojtas, Five mutually orthogonal latin squares of order 35, *J. Combin. Des.* **4** (1996), 153–154.

[60] M. Wojtas, Three new constructions of mutually orthogonal latin squares, *J. Combin. Des.* **8** (2000), 218–220.

(Received 23 Aug 2012; revised 21 May 2013)