

RESOLVABLE MENDELSON DESIGNS AND FINITE FROBENIUS GROUPS

D. F. HSU and SANMING ZHOU[✉]

(Received 12 February 2018; accepted 27 March 2018; first published online 30 May 2018)

Abstract

We prove the existence and give constructions of a $(p(k) - 1)$ -fold perfect resolvable $(v, k, 1)$ -Mendelsohn design for any integers $v > k \geq 2$ with $v \equiv 1 \pmod k$ such that there exists a finite Frobenius group whose kernel K has order v and whose complement contains an element ϕ of order k , where $p(k)$ is the least prime factor of k . Such a design admits $K \rtimes \langle \phi \rangle$ as a group of automorphisms and is perfect when k is a prime. As an application we prove that for any integer $v = p_1^{e_1} \cdots p_t^{e_t} \geq 3$ in prime factorisation and any prime k dividing $p_i^{e_i} - 1$ for $1 \leq i \leq t$, there exists a resolvable perfect $(v, k, 1)$ -Mendelsohn design that admits a Frobenius group as a group of automorphisms. We also prove that, if k is even and divides $p_i - 1$ for $1 \leq i \leq t$, then there are at least $\varphi(k)^t$ resolvable $(v, k, 1)$ -Mendelsohn designs that admit a Frobenius group as a group of automorphisms, where φ is Euler's totient function.

2010 Mathematics subject classification: primary 05B05.

Keywords and phrases: Mendelsohn design, balanced directed cycle design, resolvable Mendelsohn design, perfect Mendelsohn design, Frobenius group, fixed-point-free automorphism.

1. Introduction

The purpose of this paper is to explore connections between resolvable Mendelsohn designs and Frobenius groups. We will show that Frobenius groups provide a natural means for constructing resolvable Mendelsohn designs with $\lambda = 1$.

All sets and groups considered in the paper are finite. Let $v \geq k \geq 2$ and $\lambda \geq 1$ be integers. A (v, k, λ) -Mendelsohn design [24], or a (v, k, λ) -MD for short, consists of a set X (of points) of cardinality v and a collection \mathcal{B} of cyclically ordered subsets of X (called blocks) each with cardinality k , such that every ordered pair of elements of X are consecutive in exactly λ blocks. In a block (a_1, a_2, \dots, a_k) with cyclic order $a_1 < a_2 < \dots < a_k < a_1$, the points a_i and a_{i+t} are said to be t -apart for $i = 1, \dots, k$ with subscripts modulo k . A (v, k, λ) -MD (X, \mathcal{B}) is called ℓ -fold perfect [21] if, for $t = 1, \dots, \ell$, every ordered pair of elements of X appears t -apart in exactly λ blocks. A (v, k, λ) -MD is said to be perfect [24], denoted by (v, k, λ) -PMD, if it is $(k - 1)$ -fold perfect. It is not difficult to see that any (v, k, λ) -MD has $\lambda v(v - 1)/k$ blocks and

The second author was supported by a Future Fellowship (FT110100629) of the Australian Research Council.

© 2018 Australian Mathematical Publishing Association Inc.

thus satisfies $\lambda v(v-1) \equiv 0 \pmod{k}$. A (v, k, λ) -MD is called *resolvable* [7], denoted (v, k, λ) -RMD, if either $v \equiv 0 \pmod{k}$ and the set of blocks can be partitioned into $\lambda(v-1)$ parts each containing v/k pairwise disjoint blocks, or $v \equiv 1 \pmod{k}$ and the set of blocks can be partitioned into λv parts each containing $(v-1)/k$ pairwise disjoint blocks. We denote a resolvable perfect (v, k, λ) -MD by (v, k, λ) -RPMD. A (v, k, λ) -MD can be equivalently defined as a decomposition of $\lambda \vec{K}_v$ into edge-disjoint directed cycles of length k , where $\lambda \vec{K}_v$ is the directed complete multigraph of v vertices with λ directed edges between each ordered pair of vertices. From this viewpoint a (v, k, λ) -MD is also called a *balanced directed cycle design* with parameters (v, k, λ) or a $(v, k, \lambda)\vec{C}_k$ -*design* (see, for example, [26, 27]).

Mendelsohn designs are very well studied and many results about them have been produced since the 1970s. Here we mention only a few results on PMDs and RMDs. As mentioned above, a necessary condition for the existence of a (v, k, λ) -MD is that $\lambda v(v-1) \equiv 0 \pmod{k}$. This condition has been proved to be sufficient for the existence of a (v, k, λ) -PMD when: (i) $k = 3$, except for the nonexisting $(6, 3, 1)$ -PMD [5, 23]; (ii) $k = 4$, except for $v = 4$ and λ odd, $v = 8$ and $\lambda = 1$ [4, Theorem 1.2]; (iii) $k = 5$, except for $\lambda = 1$, $v \in \{6, 10\}$, and possibly for $\lambda = 1$ and $v \in \{15, 20\}$ [4, Theorem 1.3]. See [1, 4, 6, 25] for more results on PMDs.

In [7] it was proved that a $(v, k, 1)$ -RMD exists if there is an algebra of order v in a certain quasivariety, that a $(q, k, 1)$ -RPMD exists whenever q is a prime power with $q \equiv 1 \pmod{k}$, and that a $(v, k, 1)$ -RPMD exists for sufficiently large v with $v \equiv 1 \pmod{k}$. A $(v, 3, 1)$ -RMD exists if and only if $v \equiv 0$ or $1 \pmod{3}$ and $v \neq 6$ [8, 10]. A $(v, 4, 1)$ -RMD exists if and only if $v \equiv 0, 1 \pmod{4}$ and $v \neq 4$ except possibly when $v = 12$ [9]. A $(v, 4, 1)$ -RPMD exists for all $v \equiv 0 \pmod{4}$ other than $v = 4, 8$ with at most 27 possible exceptions [34, 35]. A $(v, k, 1)$ -RPMD exists for all sufficiently large v with $v \equiv 0 \pmod{k}$ [34]. A $(v, 5, 1)$ -RPMD with $v \equiv 1 \pmod{5}$ exists for all $v > 6$ except possibly $v = 26$ [2], and a $(v, 5, 1)$ -RPMD with $v \equiv 0 \pmod{5}$ exists for all $v \geq 215$ with two known exceptions plus at most 17 possible exceptions below this value [3]. In [33] it was proved that for $\lambda > 1$ the necessary condition $v \equiv 0, 1 \pmod{4}$ is also sufficient for the existence of a $(v, 4, \lambda)$ -RPMD with the exception when $v = 4$ and λ is odd.

An *automorphism* of an MD is a permutation of its point set that permutes its blocks among themselves. The (full) *automorphism group* of an MD is the group of all its automorphisms with operation the usual composition of permutations. In general, for a group G , an MD (X, \mathcal{B}) is said to *admit* G as a group of automorphisms if G acts (not necessarily faithfully) on the point set X and preserves the block set \mathcal{B} . An MD is said to be *based on* G [11, 13, 26, 27] if its point set can be identified with G in such a way that the MD admits the left regular representation of G as a group of automorphisms. A useful construction, called the ‘difference method’, for constructing MDs based on groups was discussed in [11] and further developed in [13, 26, 27]. A similar construction was also developed in [21] using the language of generalised complete mappings (and generalised Mendelsohn designs). In [13] all MDs admitting a one-dimensional affine group $\text{AGL}(1, q)$ as a group of automorphisms were classified, and

in [26] all MDs admitting the holomorph of a cyclic group were classified. In [27, Section 5] MDs based on a group G that admit as automorphisms elements of a certain subgroup of the automorphism group $\text{Aut}(G)$ of G were studied.

In this paper we give constructions of RMDs and RPMDs with $\lambda = 1$ using Frobenius groups. Our research was motivated by the first author's work [20, 21] (with Keedwell) on generalised complete mappings and the second author's work [28–30, 36] (partly with Thomson) on Frobenius circulant graphs. We refined the methods in [20, 21] (see the first version of this paper at <https://arxiv.org/abs/1307.7455v1>), but later we found that our constructions are also in line with the difference method [13, 26, 27] as all RMDs and RPMDs obtained in our paper are based on the kernels of Frobenius groups. It turns out that Frobenius groups are proper choices because the Mendelsohn designs obtained from them are always resolvable. As mentioned above, much is known about the existence of MDs with $\lambda = 1$ in the literature. The benefit of our results is that they give natural constructions of some RMDs and RPMDs with $\lambda = 1$ having the additional property that an automorphism group is regular on the point set.

The main results in the paper are as follows. We first prove (see Theorem 3.1) that, if there exists a Frobenius group $K \rtimes H$ with Frobenius kernel K and complement H such that $v = |K|$ and H contains an element ϕ of order $k \geq 2$, then a $(p(k) - 1)$ -fold perfect $(v, k, 1)$ -RMD based on K exists, where $p(k)$ is the smallest prime factor of k . In particular, this $(v, k, 1)$ -RMD is a $(v, k, 1)$ -RPMD when k is a prime. Moreover, such a $(v, k, 1)$ -RMD can be easily constructed from ϕ and the action of H on K . This result enables us to construct various point-transitive RMDs and RPMDs systematically using Frobenius groups. To illustrate this method, we will use Theorem 3.1 and a known result [12] on Ferrero pairs to prove the existence and give an explicit construction of a $(v, k, 1)$ -RPMD, for any integer with prime factorisation $v = p_1^{e_1} \cdots p_t^{e_t}$ and any prime k dividing every $p_i^{e_i} - 1$ (see Theorem 3.8). We will also use Theorem 3.1 and a recent result from network design [30] to construct $(v, k, 1)$ -RMDs for any $v = p_1^{e_1} \cdots p_t^{e_t}$ and any even k dividing every $p_i - 1$ (see Theorem 4.1).

All results obtained in this paper can be stated in terms of regular orthomorphisms or complete mappings of groups, owing to the close connections between MDs and orthomorphisms and complete mappings of groups as shown in [21, Theorem 5.1] (see also Lemma 3.3 and Remark 3.4). Beginning with [22] and motivated by the study of Latin squares, there is a long history of studying complete mappings. Hall and Paige [19] proved that a finite group with a nontrivial, cyclic Sylow 2-subgroup does not admit complete mappings. The converse, which was a long-standing conjecture [19], was proved in 2009 by Wilcox [31], Evans [15] and Bray (see [15]).

2. Notation and terminology

To make the paper self-contained we collect here some basic definitions on orthomorphisms, complete mappings and Frobenius groups. Undefined group-theoretic definitions can be found in [14, 18].

Let G be a group. A bijection $\theta : G \rightarrow G$ is called a *complete mapping* [19, 22] of G if the mapping $\hat{\theta}$ defined by $\hat{\theta}(x) = x\theta(x)$ is also a bijection, and an *orthomorphism* [16] if the mapping $\bar{\theta}$ defined by $\bar{\theta}(x) = x^{-1}\theta(x)$ is also a bijection. Thus, θ is a complete mapping if and only if $\hat{\theta}$ is an orthomorphism, and θ is an orthomorphism if and only if $\bar{\theta}$ is a complete mapping. Obviously, if θ is a complete mapping or orthomorphism of G , then so is the bijection $x \mapsto \theta(x)a$ for every fixed $a \in G$. Hence, we may require θ to fix 1_G , and in this case θ is said to be in *canonical form*. As a permutation of G , θ can be decomposed into a product of cycles. A complete mapping or orthomorphism θ in canonical form is *k-regular* [20], where $k \geq 2$, if all cycles in this decomposition other than the trivial cycle (1_G) have length k . If in addition $\theta, \theta^2, \dots, \theta^\ell$ are all k -regular, then θ is said to be *ℓ -fold perfect* [21, Definition 5.7], where ℓ is a positive integer less than k and θ^i is the composition of θ with itself i times. In particular, θ is called *perfect* [21] if it is $(k - 1)$ -fold perfect.

An *action* of a group G on a set Ω is a mapping $G \times \Omega \rightarrow \Omega$, $(x, \alpha) \mapsto x(\alpha)$ such that $1_G(\alpha) = \alpha$ and $x(y(\alpha)) = (xy)(\alpha)$ for $\alpha \in \Omega$ and $x, y \in G$, where 1_G is the identity element of G . Call $G(\alpha) := \{x(\alpha) : x \in G\}$ the *G-orbit* containing α , and $G_\alpha := \{x \in G : x(\alpha) = \alpha\}$ the *stabiliser* of α in G . We say that G is *semiregular* on Ω if $G_\alpha = \{1_G\}$ for all $\alpha \in \Omega$, *transitive* on Ω if $G(\alpha) = \Omega$ for some (and hence all) $\alpha \in \Omega$, and *regular* on Ω if it is both transitive and semiregular on Ω .

If a group H acts on a group K such that $x(uw) = x(u)x(w)$ for $x \in H$ and $u, w \in K$, then H acts on K as a group. This is equivalent to saying that the mapping defined by $x \mapsto \psi_x$ is a homomorphism from H to $\text{Aut}(K)$, where $\psi_x \in \text{Aut}(K)$ is defined by $\psi_x(u) = x(u)$. In this case the semidirect product [14] of K by H with respect to the action, denoted by $K \rtimes H$, is the group whose elements are ordered pairs (u, x) , $u \in K$, $x \in H$, with operation defined by $(u_1, x_1)(u_2, x_2) = (u_1x_1(u_2), x_1x_2)$. If in addition H is semiregular on $K \setminus \{1_K\}$, then $K \rtimes H$ is called a *Frobenius group* [14, 18]. It is well-known [14, 18] that, for a finite Frobenius group $G = K \rtimes H$, the group K is a nilpotent normal subgroup of G called the *Frobenius kernel* of G , and $|H|$ is a divisor of $|K| - 1$. Here, H is called a *Frobenius complement* [14, 18] of K in G .

We can also define a Frobenius group as a transitive group G on a set Ω that is not regular but has the property that 1_G is the only element of G that fixes two points of Ω . The Frobenius kernel K of G then consists of 1_G and the elements of G fixing no point of Ω , and the stabiliser H in G of a point of Ω is a complement of G (see, for example, [14, page 86]). Since K is regular on Ω , we may identify Ω with K in such a way that K acts on itself by right multiplication, and we may choose H to be the stabiliser of the identity element of K so that H acts on K by conjugation.

If K is a nontrivial group and H a nontrivial fixed-point-free subgroup of $\text{Aut}(K)$, then $K \rtimes H$ (with respect to the natural action of H on K) is a Frobenius group with kernel K and complement H . (An element $\phi \in \text{Aut}(G)$ is fixed-point-free if $\phi(x) \neq x$ for every $x \in G \setminus \{1_G\}$, and a subgroup H of $\text{Aut}(G)$ is fixed-point-free if every nonidentity element of H is fixed-point-free.) When the operation of K is written additively (but K is not necessarily abelian), such a pair (K, H) is called a *Ferrero pair* [12] in the literature.

The *left regular representation* [18] of a group G is the permutation group $L(G) = \{\lambda(g) : g \in G\}$, where $\lambda(g)$ is the permutation of G defined by $\lambda(g) : x \mapsto gx$, $x \in G$. This group acts regularly on G in the obvious way and is isomorphic to G when $\lambda(g)$ is identified with g .

3. Resolvable Mendelsohn designs and regular orthomorphisms

We use $p(k)$ to denote the smallest prime factor of an integer $k \geq 2$. As usual, for an element ϕ of a group, $\langle \phi \rangle$ denotes the cyclic subgroup generated by ϕ .

THEOREM 3.1. *Let $v \geq 3$ and $k \geq 2$ be integers with $v \equiv 1 \pmod k$ such that there exists a Frobenius group $K \rtimes H$ with $|K| = v$ and H containing an element ϕ of order k . Then a $(p(k) - 1)$ -fold perfect $(v, k, 1)$ -RMD exists and can be constructed based on K . Moreover, this $(v, k, 1)$ -RMD admits $K \rtimes \langle \phi \rangle$ as a group of automorphisms. In particular, if k is a prime, then it is a $(v, k, 1)$ -RPMD. Furthermore, the $(v, k, 1)$ -RMDs constructed by using conjugate elements of H with order k are isomorphic to each other.*

In general, unfortunately, we do not know when two nonconjugate elements of H with the same order produce isomorphic $(v, k, 1)$ -RMDs.

To prove Theorem 3.1 we need the following two lemmas.

LEMMA 3.2. *Let $K \rtimes H$ be a Frobenius group. Let ϕ be a nonidentity element of H with order k . Then ϕ gives rise to a $(p(k) - 1)$ -fold perfect k -regular orthomorphism of K in canonical form. Moreover, ϕ gives rise to a perfect k -regular orthomorphism of K if and only if k is a prime.*

PROOF. Since $K \rtimes H$ is a Frobenius group, H is semiregular on $K \setminus \{1\}$, where 1 is the identity element of K . That is, $\phi(x) = x$ implies $x = 1$, for any $x \in K$. Thus, for $x, y \in K$, we have $x^{-1}\phi(x) = y^{-1}\phi(y) \Leftrightarrow \phi(x)\phi(y)^{-1} = xy^{-1} \Leftrightarrow \phi(x)\phi(y^{-1}) = xy^{-1} \Leftrightarrow \phi(xy^{-1}) = xy^{-1} \Leftrightarrow xy^{-1} = 1 \Leftrightarrow x = y$. In other words, the mapping from K to K defined by $\bar{\phi}(x) = x^{-1}\phi(x)$ is injective and so must be bijective as K is finite. Note that ϕ fixes 1 . Therefore, ϕ is an orthomorphism of K in canonical form.

Since ϕ has order k , we have $\phi^j \neq 1_H$ for $1 \leq j \leq k - 1$. Since H is semiregular on $K \setminus \{1\}$, it follows that $\phi^j(x) \neq x$ for every $x \in K \setminus \{1\}$. Thus, $(x, \phi(x), \phi^2(x), \dots, \phi^{k-1}(x))$ is a cycle in the decomposition of the permutation ϕ of K into disjoint cycles. This implies that every nontrivial cycle in the cycle decomposition of ϕ has length k . Therefore, ϕ is a k -regular orthomorphism of K .

We prove further that ϕ is $(p(k) - 1)$ -fold perfect. Fix i with $1 \leq i \leq p(k) - 1$. Then i and k are coprime, since $p(k)$ is the smallest prime factor of k . Hence, the order of ϕ^i is equal to k . It follows from what we proved above that ϕ^i is a k -regular orthomorphism of K . Since this holds for $i = 1, \dots, p(k) - 1$, we conclude that ϕ is a $(p(k) - 1)$ -fold perfect k -regular orthomorphism of K .

In the special case when k is a prime, we have $p(k) = k$ and therefore ϕ is a perfect k -regular orthomorphism of K . Conversely, suppose ϕ is a perfect k -regular

orthomorphism of K . Then $\phi, \phi^2, \dots, \phi^{k-1}$ are all k -regular orthomorphisms of G . Thus, for any $1 \leq i, j \leq k - 1$ and any $x \in K \setminus \{1\}$, we have $\phi^{ij}(x) \neq x$ and so ij cannot be a multiple of k . Therefore, k must be a prime. \square

The following result is similar to its counterpart for complete mappings (see [21, Theorems 5.1, 5.3 and 5.4]), and the proof is similar to that of [21, Theorem 5.1]. We give its proof for completeness.

LEMMA 3.3. *Let G be a group of order v that admits an ℓ -fold perfect k -regular orthomorphism θ (in canonical form) and suppose that the cycle decomposition of θ is given by $(g_{11}, g_{12}, \dots, g_{1k}) \dots (g_{r1}, g_{r2}, \dots, g_{rk})$, where $k \geq 2$ and $rk = v - 1$. Let*

$$\mathcal{B} = \bigcup_{g \in G} \mathcal{B}_g,$$

where

$$\mathcal{B}_g = \{(gg_{11}, gg_{12}, \dots, gg_{1k}), \dots, (gg_{r1}, gg_{r2}, \dots, gg_{rk})\}$$

with each block $(gg_{i1}, gg_{i2}, \dots, gg_{ik})$ equipped with the cyclic order $gg_{i1} < gg_{i2} < \dots < gg_{ik} < gg_{i1}$. Then (G, \mathcal{B}) is an ℓ -fold perfect $(v, k, 1)$ -RMD with point set G . Moreover, (G, \mathcal{B}) admits the left regular representation of G as a group of automorphisms.

PROOF. By our assumption, θ is defined by $\theta(1_G) = 1_G$ and $\theta(g_{ij}) = g_{i,j+1}$, for $1 \leq i \leq r$, $1 \leq j \leq k$, with the second subscripts modulo k . In general, for $1 \leq t \leq \ell$, $\theta^t(1) = 1$ and $\theta^t(g_{ij}) = g_{i,j+t}$.

Fix t with $1 \leq t \leq \ell$. Let (x, y) be an arbitrary pair of distinct elements of G , so that $x^{-1}y \neq 1$. Then $(x, y) = (gg_{ij}, gg_{i,j+t})$ if and only if $x^{-1}y = g_{ij}^{-1}g_{i,j+t}$ and $g = xg_{ij}^{-1}$. However, since by our assumption θ^t is an orthomorphism of G , there is exactly one pair (i, j) satisfying the first equation. Therefore, the ordered pair of elements (x, y) are t -apart in exactly one block of \mathcal{B} . Since this holds for any (x, y) and any t with $1 \leq t \leq \ell$, it follows that (G, \mathcal{B}) is an ℓ -fold perfect $(v, k, 1)$ -MD with point set G . Moreover, (G, \mathcal{B}) is resolvable because of the obvious partition $\{\mathcal{B}_g : g \in G\}$ of \mathcal{B} into v parts each containing $(v - 1)/k$ pairwise disjoint blocks. Clearly, (G, \mathcal{B}) admits the left regular representation of G as a group of automorphisms. \square

REMARK 3.4.

- (a) Similar to [21, Theorem 5.1], the converse of Lemma 3.3 is also true. That is, from an ℓ -fold perfect $(v, k, 1)$ -RMD on G that admits $L(G)$ as a group of automorphisms, we can recover an ℓ -fold perfect k -regular orthomorphism.
- (b) In Lemma 3.3, $\mathcal{B}_1 = \{(g_{11}, g_{12}, \dots, g_{1k}), \dots, (g_{r1}, g_{r2}, \dots, g_{rk})\}$ is a *basis*, and its blocks are *base blocks*, of the $(v, k, 1)$ -RMD in the sense that all other blocks are obtained from them by applying $L(G)$. This fact is usually expressed as $\mathcal{B} = \text{dev}(\mathcal{B}_1)$ [6].

PROOF OF THEOREM 3.1. Let $v, k, K \rtimes H$ and ϕ be as in Theorem 3.1. By Lemma 3.2, ϕ gives rise to a $(p(k) - 1)$ -fold perfect k -regular orthomorphism of K in canonical

form, whose cycles in the cycle decomposition are $B(x) = (x, \phi(x), \phi^2(x), \dots, \phi^{k-1}(x))$, for $x \in K \setminus \{1\}$, where 1 is the identity element of K . Note that $B(x) = B(y)$ as sets if and only if $y = \phi^i(x)$ for some i . Regard $B(x)$ as a block with cyclic order $x < \phi(x) < \phi^2(x) < \dots < \phi^{k-1}(x) < x$, and define $\mathcal{B}_1(\phi) = \{B(x) : x \in K \setminus \{1\}\}$ with duplicated blocks counted only once. More explicitly, letting the $\langle \phi \rangle$ -orbits on $K \setminus \{1\}$ be $\langle \phi \rangle(x_1), \dots, \langle \phi \rangle(x_r)$, where $x_1, \dots, x_r \in K \setminus \{1\}$ and $r = (v - 1)/k$,

$$\mathcal{B}_1(\phi) = \{B(x_1), \dots, B(x_r)\}.$$

Define

$$\mathcal{B}(\phi) = \text{dev}(\mathcal{B}_1(\phi)) = \bigcup_{g \in K} \mathcal{B}_g(\phi),$$

where

$$\mathcal{B}_g(\phi) = g\mathcal{B}_1(\phi) = \{gB(x_1), \dots, gB(x_r)\}$$

and

$$gB(x_i) = (gx_i, g\phi(x_i), g\phi^2(x_i), \dots, g\phi^{k-1}(x_i)), \quad i = 1, \dots, r.$$

By Lemma 3.3, $(K, \mathcal{B}(\phi))$ is a $(p(k) - 1)$ -fold perfect $(v, k, 1)$ -RMD. Since $\langle \phi \rangle$ leaves each block of $\mathcal{B}_1(\phi)$ invariant and permutes its elements cyclically, one can verify that $(K, \mathcal{B}(\phi))$ admits $\langle \phi \rangle$ as a group of automorphisms. Since by Lemma 3.3, $(K, \mathcal{B}(\phi))$ also admits $L(K)$ as a group of automorphisms, it admits $K \rtimes \langle \phi \rangle$ as a group of automorphisms (with K identified with $L(K)$).

If k is a prime, then by Lemma 3.2, ϕ gives rise to a perfect k -regular orthomorphism of K , and hence $(K, \mathcal{B}(\phi))$ is a $(v, k, 1)$ -RPMD by Lemma 3.3.

Finally, assume that $\phi' = \psi^{-1}\phi\psi$ is a conjugate of ϕ , where $\psi \in H$. Then a typical base block in $\mathcal{B}_1(\phi')$ is $(x, \psi^{-1}\phi\psi(x), \dots, \psi^{-1}\phi^{k-1}\psi(x))$, which can be expressed as

$$(\psi^{-1}(y), \psi^{-1}\phi(y), \dots, \psi^{-1}\phi^{k-1}(y)) = \psi^{-1}(y, \phi(y), \dots, \phi^{k-1}(y)),$$

where we set $y = \psi(x)$. From this one can verify that ψ (viewed as a bijection of K) is an isomorphism from $(K, \mathcal{B}(\phi))$ to $(K, \mathcal{B}(\phi'))$. □

In Theorem 3.1 and Lemma 3.2 we essentially dealt with the Frobenius group $K \rtimes \langle \phi \rangle$. Thus, we have the following corollary of Theorem 3.1.

COROLLARY 3.5. *Let $v \geq 3$ and $k \geq 2$ be integers such that there exists a group K with order v that admits a fixed-point-free automorphism ϕ of order k . Then there exists a $(p(k) - 1)$ -fold perfect $(v, k, 1)$ -RMD based on K that admits $K \rtimes \langle \phi \rangle$ as a group of automorphisms. If in addition k is a prime, then this $(v, k, 1)$ -RMD is a $(v, k, 1)$ -RPMD.*

The assumption in this corollary (as well as the next one) implies $v \equiv 1 \pmod k$. The well-known Cauchy theorem in group theory asserts that for any group H and any prime divisor k of $|H|$, H contains an element of order k . Combining this with Theorem 3.1 we obtain the following result.

COROLLARY 3.6. *Let $v \geq 3$ be an integer and $k \geq 2$ a prime such that there exists a Frobenius group $K \rtimes H$ with $|K| = v$ and with k dividing $|H|$. Then there exists a $(v, k, 1)$ -RPMD based on K that admits $K \rtimes \langle \phi \rangle$ as a group of automorphisms, where ϕ is an element of H with order k .*

Applying Theorem 3.1, Corollary 3.5 or Corollary 3.6 to various Frobenius groups, we can obtain point-transitive Mendelsohn designs with specific parameters. In the special case when the group is $\text{AGL}(1, q)$, we obtain the following well-known construction (see, for example, [6, 25, 32]) which is included for illustration only. (A related result that generalises [13, Theorem 2.3] is the classification [27, Theorem 5.4] of all $(q, k, 1)$ -MDs based on $(\mathbb{F}_q, +)$ admitting a subgroup of (\mathbb{F}_q^*, \cdot) as a group of automorphisms.)

EXAMPLE 3.7. $\text{AGL}(1, q)$ consists of all affine transformations $t_{\alpha, \beta} : \xi \mapsto \alpha\xi + \beta$ of \mathbb{F}_q , $\alpha \in \mathbb{F}_q^*, \beta \in \mathbb{F}_q$, where q is a prime power. It is well-known that $\text{AGL}(1, q) = K \rtimes H$ is sharply 2-transitive on \mathbb{F}_q [14] and hence $\text{AGL}(1, q)$ is a Frobenius group, where $K = \{t_{1, \beta} : \beta \in \mathbb{F}_q\} \cong (\mathbb{F}_q, +)$ and $H = \{t_{\alpha, 0} : \alpha \in \mathbb{F}_q^*\} \cong (\mathbb{F}_q^*, \cdot)$. Since H is a cyclic group of order $q - 1$, for every divisor $k \geq 2$ of $q - 1$, H has a unique element $\phi = t_{\alpha, 0}$ of order k , where $\alpha = \omega^r$ with ω a primitive element of \mathbb{F}_q and $r = (q - 1)/k$. Moreover, $\langle \phi \rangle$ is isomorphic to the subgroup $\langle \alpha \rangle$ of \mathbb{F}_q^* , and so we may identify these two cyclic groups. By Theorem 3.1, a $(q, k, 1)$ -RMD $(K, \mathcal{B}(\phi))$ exists and can be constructed explicitly. A typical base block in $\mathcal{B}_1(\phi)$ is of the form $(x, x\alpha, \dots, x\alpha^{k-1})$. Hence, $\mathcal{B}_1(\phi) = \{(1, \omega^r, \dots, \omega^{r(k-1)}), \dots, (\omega^{r-1}, \omega^{2r-1}, \dots, \omega^{r(k-1)+(r-1)})\}$ and so the blocks of $\mathcal{B}(\phi)$ are $(\omega^i, \omega^{i+r}, \dots, \omega^{i+r(k-1)}), \dots, (\omega^{i+r-1}, \omega^{i+2r-1}, \dots, \omega^{i+r(k-1)+(r-1)})$, $i = 0, 1, \dots, r$. In the case when k is a prime factor of $q - 1$, by Theorem 3.1, $(K, \mathcal{B}(\phi))$ is a $(q, k, 1)$ -RPMD.

In [12, Theorem 1], Boykett proved the following: let $v = p_1^{e_1} \cdots p_t^{e_t}$ (prime factorisation) and k be positive integers. Then there exists a Ferrero pair (K, H) such that $|K| = v$ and $|H| = k$ if and only if k divides $p_i^{e_i} - 1$ for $1 \leq i \leq t$. Using this, we obtain the following special case of Theorem 3.1. In the statement, gcd stands for the greatest common divisor.

THEOREM 3.8. *Let $v = p_1^{e_1} \cdots p_t^{e_t} \geq 3$ be an integer in prime factorisation, and let k be a prime factor of $\text{gcd}(p_1^{e_1} - 1, \dots, p_t^{e_t} - 1)$. Then there exists a $(v, k, 1)$ -RPMD that admits a Frobenius group $K \rtimes H$ with $|K| = v$ and $|H| = k$ as a group of automorphisms.*

PROOF. Since k divides $\text{gcd}(p_1^{e_1} - 1, \dots, p_t^{e_t} - 1)$, by the result of Boykett mentioned above there exists a Ferrero pair (K, H) with $|K| = v$ and $|H| = k$. Since k is a prime, H is a cyclic group and every nonidentity element of it has order k . The result follows from Theorem 3.1. □

Theorem 3.8 is in the same spirit as the following known results:

- (a) a $(v, k, 1)$ -RPMD exists for any prime power v and any divisor $k \geq 2$ of $v - 1$ [7];
- (b) a $(v, k, 1)$ -PMD exists for any integer $v = p_1^{e_1} \cdots p_t^{e_t} \geq 3$ and any divisor $k \geq 2$ of $\text{gcd}(p_1^{e_1} - 1, \dots, p_t^{e_t} - 1)$ [24, Corollary 2.5].

Nevertheless, neither of these results implies Theorem 3.8.

CONSTRUCTION 3.9. Following the line of proof of Theorem 3.1, we can construct the $(v, k, 1)$ -RPMD in Theorem 3.8 explicitly. Denote $q_i = p_i^{e_i}$ and let $K = \bigoplus_{i=1}^t \mathbb{F}_{q_i}$ be the direct sum of the additive groups of the finite fields \mathbb{F}_{q_i} . Since k divides $q_i - 1$, for each i , $r_i = (q_i - 1)/k$ is an integer. Let ω_i be a primitive element of \mathbb{F}_{q_i} and $H_i = \langle \omega_i^{r_i} \rangle$ be the subgroup of $\mathbb{F}_{q_i}^*$ with order k . We denote a copy of $H_1 \cong \dots \cong H_t$ by $H = \langle \omega \rangle$. Then H acts on K by $\omega^j(x_1, \dots, x_t) = (\omega_1^{j r_1} x_1, \dots, \omega_t^{j r_t} x_t)$, for $(x_1, \dots, x_t) \in K$ and $\omega^j \in H$. It can be verified that H acts fixed-point-freely on K as a group and H is isomorphic to a subgroup of $\text{Aut}(K)$. Thus, (K, H) is a Ferrero pair with $|K| = v$ and $|H| = k$. Since k is a prime, every nonidentity element of H has order k . For $i = 1, \dots, k - 1$, the $(v, k, 1)$ -RPMD $(K, \mathcal{B}(\omega^i))$ obtained from ω^i is as follows: the basis $\mathcal{B}_0(\omega)$ consists of blocks of the form $B(x_1, \dots, x_t) = ((x_1, \dots, x_t), (\omega_1^{i r_1} x_1, \dots, \omega_t^{i r_t} x_t), \dots, (\omega_1^{(k-1)i r_1} x_1, \dots, \omega_t^{(k-1)i r_t} x_t))$, for $(x_1, \dots, x_t) \in K \setminus \{(0, \dots, 0)\}$. We have $\mathcal{B}(\omega) = \bigcup_{(y_1, \dots, y_t) \in K} (\mathcal{B}_0(\omega) + (y_1, \dots, y_t))$, where $\mathcal{B}_0(\omega) + (y_1, \dots, y_t)$ consists of all blocks

$$B(x_1, \dots, x_t) + (y_1, \dots, y_t) = ((x_1 + y_1, \dots, x_t + y_t), (\omega_1^{i r_1} x_1 + y_1, \dots, \omega_t^{i r_t} x_t + y_t), \dots, (\omega_1^{(k-1)i r_1} x_1 + y_1, \dots, \omega_t^{(k-1)i r_t} x_t + y_t)).$$

There has been extensive research on the existence of (v, k, λ) -PMDs for a fixed (especially small) integer k (see [6] for a survey). Theorem 3.8 asserts that, for a fixed prime k , a $(p_1^{e_1} \dots p_t^{e_t}, k, 1)$ -RPMD exists for any prime powers $p_i^{e_i}$ as long as k divides all $p_i^{e_i} - 1$, $1 \leq i \leq t$. In particular, for any primes $p_1, \dots, p_t \equiv 1 \pmod k$ and any integers $e_1, \dots, e_t \geq 1$, there exists a $(p_1^{e_1} \dots p_t^{e_t}, k, 1)$ -RPMD.

4. Constructing resolvable Mendelsohn designs from cyclic groups

In this section we construct RMDs from cyclic groups by using Theorem 3.1 and recent results [28–30, 36] on first-kind Frobenius circulant graphs. As usual we denote the additive group of integers modulo n by \mathbb{Z}_n and the multiplicative group of units of the ring \mathbb{Z}_n by $\mathbb{Z}_n^* = \{[u] : 1 \leq u \leq n - 1, \text{gcd}(n, u) = 1\}$. Then $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$ and \mathbb{Z}_n^* acts on \mathbb{Z}_n by the usual multiplication: $[x][u] = [xu]$, $[x] \in \mathbb{Z}_n$, $[u] \in \mathbb{Z}_n^*$. The semidirect product $\mathbb{Z}_n \rtimes \mathbb{Z}_n^*$ acts on \mathbb{Z}_n by $[x]^{([y], [u])} = [(x + y)u]$ for $[x], [y] \in \mathbb{Z}_n$ and $[u] \in \mathbb{Z}_n^*$.

Let φ denote Euler’s totient function. The main result in this section is as follows.

THEOREM 4.1. *Let $v = p_1^{e_1} \dots p_t^{e_t} \geq 3$ be an odd integer in prime factorisation. Then for every even divisor k of $\text{gcd}(p_1 - 1, \dots, p_t - 1)$, there exist at least $\varphi(k)^t$ $(v, k, 1)$ -RMDs based on \mathbb{Z}_v , and each of them can be constructed from some $[a] \in \mathbb{Z}_v^*$ of the form $a = \sum_{i=1}^t (v/p_i^{e_i}) a_i b_i$ and admits $\mathbb{Z}_v \rtimes \langle [a] \rangle$ as a group of automorphisms, where b_i is the inverse of $v/p_i^{e_i}$ in $\mathbb{F}_{p_i^{e_i}}$ and a_i satisfies $a_i \equiv \eta_i^{m_i \varphi(p_i^{e_i})/k} \pmod{p_i^{e_i}}$ for a fixed primitive element η_i of $\mathbb{F}_{p_i^{e_i}}$ and an integer m_i coprime to k .*

REMARK 4.2.

- (a) It would be interesting to understand whether and when some of these $\varphi(k)^t$ $(v, k, 1)$ -RMDs are isomorphic to each other. A construction of such RMDs will be given in the proof of Theorem 4.1.

- (b) In [26, Corollary 2] it was shown that a $(v, k, 1)$ -MD admitting the holomorph $\text{Hol}(\mathbb{Z}_v) \cong \mathbb{Z}_v \rtimes \mathbb{Z}_v^*$ of \mathbb{Z}_v as a group of automorphisms exists if and only if one of the following holds: (i) $k = 2$; (ii) $p \equiv 1 \pmod k$ for every prime factor p of v ; (iii) k is the least prime factor of v , k^2 does not divide v , and $p \equiv 1 \pmod k$ for every prime factor p of v other than k . Theorem 4.1 implies that under condition (ii) many $(v, k, 1)$ -RMDs based on \mathbb{Z}_v exist and can be easily constructed. Neither of Theorem 4.1 and [26, Corollary 2] is implied by the other.
- (c) Similar to Lemma 3.2, the result in Theorem 4.1 can be stated in terms of orthomorphisms: under the same assumption, \mathbb{Z}_v admits at least $\varphi(k)^t$ k -regular orthomorphisms. Hsu conjectured that, for every odd integer $n \geq 3$ and every divisor k of $n - 1$, a k -regular complete mapping of \mathbb{Z}_n exists, or equivalently a k -regular orthomorphism exists. This was confirmed when $k = 2$ or $(n - 1)/2$ (see [17, Theorem 3]). The following corollary of Theorem 4.1 provides further support to Hsu’s conjecture.

COROLLARY 4.3. *Let $n \geq 3$ be an odd integer and k a divisor of $n - 1$. If k divides $p - 1$ for every prime factor p of n , then a k -regular complete mapping of \mathbb{Z}_n exists.*

PROOF OF THEOREM 4.1. Let v and k be as in Theorem 4.1. Let $[a]$ be an element of \mathbb{Z}_v^* with order k such that $H = \langle [a] \rangle$ is semiregular on $\mathbb{Z}_v \setminus \{[0]\}$. (See below for the existence of such elements $[a]$.) Then $\mathbb{Z}_v \rtimes H$ is a Frobenius group. It can be verified (see [28, Lemma 4]) that the semiregularity of H on $\mathbb{Z}_v \setminus \{[0]\}$ is equivalent to saying that $[a^i - 1] \in \mathbb{Z}_v^*$ for $1 \leq i \leq k - 1$.

Let $H[x_1] = H, H[x_2], \dots, H[x_r]$ be the H -orbits on $\mathbb{Z}_v \setminus \{[0]\}$, where we assume $[x_1] = [1]$ without loss of generality. Then each $H[x_i]$ has length k and $kr = v - 1$. Define the function $\phi_a : \mathbb{Z}_v \rightarrow \mathbb{Z}_v$ by $\phi_a([0]) = [0]$ and $\phi_a([a^s x_i]) = [a^{s+1} x_i]$, for $1 \leq i \leq r, 0 \leq s \leq k - 1$. In line with the proof of Lemma 3.2, since $[a - 1] \in \mathbb{Z}_v^*$ as noted above, one can verify that the mapping from \mathbb{Z}_v to itself defined by $\bar{\phi}_a([0]) = [0]$ and $\bar{\phi}_a([a^s x_i]) = \phi_a([a^s x_i]) - [a^s x_i] = [a^s(a - 1)x_i]$ is bijective. Hence, ϕ_a is a k -regular orthomorphism of \mathbb{Z}_v . Thus, by Theorem 3.1 and its proof, ϕ_a produces a $(v, k, 1)$ -RMD, $\mathcal{B}(a)$, whose base blocks are $B_{a,i} = ([x_i], [ax_i], [a^2 x_i], \dots, [a^{k-1} x_i])$, $1 \leq i \leq r$. More explicitly, $\mathcal{B}(a) = \{[x] + B_{a,i} : [x] \in \mathbb{Z}_m, 1 \leq i \leq r\}$, where we set $[x] + B_{a,i} = ([x + x_i], [x + ax_i], [x + a^2 x_i], \dots, [x + a^{k-1} x_i])$.

It was proved in [30, Theorem 2.7] that every element $[a]$ of \mathbb{Z}_v^* with order k such that $\langle [a] \rangle$ is semiregular on $\mathbb{Z}_v \setminus \{[0]\}$ can be constructed as stated in the theorem, and vice versa. Since k divides each $p_i - 1$, it divides $p_i^{e_i} - 1$ and so $\mathbb{Z}_{p_i^{e_i}}^*$ has exactly one subgroup of order k . Thus, as noted in the proof of [30, Theorem 2.7], without loss of generality, we may fix the primitive element η_i of $\mathbb{F}_{p_i^{e_i}}$. There are exactly $\varphi(k)$ values a_i satisfying $a_i \equiv \eta_i^{m_i \varphi(p_i^{e_i})/k} \pmod{p_i^{e_i}}$, each corresponding to a different value of m_i . Since this is true for $i = 1, \dots, t$ and since each $b_i \pmod{p_i^{e_i}}$ is unique, it follows that there are exactly $\varphi(k)^t$ different elements $[a]$ of \mathbb{Z}_v^* with order k such that $\langle [a] \rangle$ is semiregular on $\mathbb{Z}_v \setminus \{[0]\}$. (Note that if $[a]$ is such an element, then so is $[a^j]$ provided $\text{gcd}(j, k) = 1$. In this case, $\langle [a] \rangle = \langle [a^j] \rangle$ but the $(v, k, 1)$ -RMD $\mathcal{B}(a^j)$ is not necessarily

identical to $\mathcal{B}(a)$.) Therefore, there exist at least $\varphi(k)^t$ $(v, k, 1)$ -RMDs each with the stated properties. \square

The following is a corollary of Theorem 4.1 and [28, Theorem 2].

COROLLARY 4.4. *Let $v = p_1^{e_1} \cdots p_t^{e_t} \geq 5$ be an integer in prime factorisation such that each $p_i \equiv 1 \pmod{4}$. Then there are at least 2^t $(v, 4, 1)$ -RMDs based on \mathbb{Z}_v , and each of them is produced by a solution a to the congruence equation $x^2 + 1 \equiv 0 \pmod{v}$ and admits $\mathbb{Z}_v \rtimes \langle [a] \rangle$ as a group of automorphisms.*

PROOF. Since each $p_i \equiv 1 \pmod{4}$, 4 is a divisor of $\gcd(p_1 - 1, \dots, p_t - 1)$. Since $\varphi(4) = 2$, by Theorem 4.1 there are at least 2^t $(v, 4, 1)$ -RMDs. Moreover, each of them is constructed from an element $[a] \in \mathbb{Z}_v^*$ of order 4 such that $\langle [a] \rangle$ is semiregular on $\mathbb{Z}_v \setminus \{[0]\}$ and admits the corresponding $\mathbb{Z}_v \rtimes \langle [a] \rangle$ as a group of automorphisms. It can be verified (see [28, Theorem 2]) that such elements a are in one-to-one correspondence with the solutions of $x^2 + 1 \equiv 0 \pmod{v}$. \square

In [29, Theorem 2] it was proved that, if every prime factor of an integer $v \geq 7$ is congruent to 1 modulo 6, then there are exactly 2^t ($= \varphi(6)^t$) elements $[a]$ of \mathbb{Z}_v^* of order 6 such that $\langle [a] \rangle$ is semiregular on $\mathbb{Z}_v \setminus \{[0]\}$, and moreover they are in one-to-one correspondence with the solutions of $x^2 - x + 1 \equiv 0 \pmod{v}$. Thus, similar to Corollary 4.4, we obtain the following special case of Theorem 4.1.

COROLLARY 4.5. *Let $v = p_1^{e_1} \cdots p_t^{e_t} \geq 7$ be an integer in prime factorisation such that each $p_i \equiv 1 \pmod{6}$. Then there are at least 2^t $(v, 6, 1)$ -RMDs based on \mathbb{Z}_v , and each of them is produced by a solution a to the congruence equation $x^2 - x + 1 \equiv 0 \pmod{v}$ and admits $\mathbb{Z}_v \rtimes \langle [a] \rangle$ as a group of automorphisms.*

We conclude this paper by an example which illustrates how the RMDs in Corollary 4.4 can be constructed following the proof of Theorem 4.1.

EXAMPLE 4.6. Consider $v = 53$. Then $x = 23$ is a solution to $x^2 + 1 \equiv 0 \pmod{53}$. Let $H = \langle [23] \rangle \leq \mathbb{Z}_{53}^*$. Then the H -orbits on $\mathbb{Z}_{53} \setminus \{[0]\}$ are as follows:

$$\begin{aligned} H &= \{[1], [23], [52], [30]\}, H[2] = \{[2], [46], [51], [7]\}, H[3] = \{[3], [16], [50], [37]\}, \\ H[4] &= \{[4], [39], [49], [14]\}, H[24] = \{[24], [22], [29], [31]\}, \\ H[25] &= \{[25], [45], [28], [8]\}, H[26] = \{[26], [15], [27], [38]\}, \\ H[47] &= \{[47], [21], [6], [32]\}, H[48] = \{[48], [44], [5], [9]\}, \\ H[17] &= \{[17], [20], [36], [33]\}, H[18] = \{[18], [43], [35], [10]\}, \\ H[40] &= \{[40], [19], [13], [34]\}, H[41] = \{[41], [42], [12], [11]\}. \end{aligned}$$

Thus, in view of the proof of Lemma 3.2, the permutation

$$(1\ 23\ 52\ 30)(2\ 46\ 51\ 7) \cdots (41\ 42\ 12\ 11)$$

is a 4-regular orthomorphism of \mathbb{Z}_{53} . In view of the proof of Theorem 4.1, this orthomorphism gives rise to the (53, 4, 1)-RMD $\mathcal{B}(53)$ whose basis $\mathcal{B}_0(53)$ consists of (1, 23, 52, 30), (2, 46, 51, 7), \dots , (41, 42, 12, 11). Note that

$$\mathcal{B}(53) = \text{dev}(\mathcal{B}_0(53)) = \bigcup_{i=0}^{52} (\mathcal{B}_0(53) + i),$$

where $\mathcal{B}_0(53) + i$ is obtained from $\mathcal{B}_0(53)$ by adding i to each block of $\mathcal{B}_0(53)$ coordinate-wise with addition modulo 53. For example, $\mathcal{B}_0(53) + 1$ consists of (2, 24, 0, 31), (3, 47, 52, 8), \dots , (42, 43, 13, 12).

References

- [1] R. J. R. Abel and F. E. Bennett, 'The existence of $(v, 6, \lambda)$ -perfect Mendelsohn designs with $\lambda > 1$ ', *Des. Codes Cryptogr.* **40** (2006), 211–224.
- [2] R. J. R. Abel, F. E. Bennett and G. Ge, 'Almost resolvable perfect Mendelsohn designs with block size five', *Discrete Appl. Math.* **116** (2002), 1–15.
- [3] R. J. R. Abel, F. E. Bennett and G. Ge, 'Resolvable perfect Mendelsohn designs with block size five', *Discrete Math.* **247**(1–3) (2002), 1–12.
- [4] R. J. R. Abel, F. E. Bennett and H. Zhang, 'Perfect Mendelsohn designs with block size six', *J. Stat. Plan. Inference* **86** (2000), 287–319.
- [5] F. E. Bennett, 'Direct constructions for perfect 3-cyclic designs', *Ann. Discrete Math.* **15** (1982), 63–68.
- [6] F. E. Bennett, 'Recent progress on the existence of perfect Mendelsohn designs', *J. Stat. Plan. Inference* **94** (2001), 121–138.
- [7] F. E. Bennett, E. Mendelsohn and N. S. Mendelsohn, 'Resolvable perfect cyclic designs', *J. Combin. Theory Ser. A* **29** (1980), 142–150.
- [8] F. E. Bennett and D. Soiteau, 'Almost resolvable decomposition of K_n^* ', *J. Combin. Theory Ser. B* **30**(2) (1981), 228–232.
- [9] F. E. Bennett and X. Zhang, 'Resolvable Mendelsohn designs with block size 4', *Aequationes Math.* **40**(2–3) (1990), 248–260.
- [10] J.-C. Bermond, A. Germa and D. Soiteau, 'Resolvable decomposition of K_n^* ', *J. Combin. Theory Ser. A* **26**(2) (1979), 179–185.
- [11] J.-C. Bermond and D. Soiteau, 'Graph decompositions and G -designs', in: *Proc. 5th British Combin. Conf.* (Univ. Aberdeen, Aberdeen, 1975), Congressus Numerantium, XV (Utilitas Math., Winnipeg, Man., 1976), 53–72.
- [12] T. Boykett, 'Construction of Ferrero pairs of all possible orders', *SIAM J. Discrete Math.* **14**(3) (2001), 283–285.
- [13] N. Brand and W. C. Huffman, 'Mendelsohn designs admitting the affine group', *Graphs Combin.* **3** (1987), 313–324.
- [14] J. D. Dixon and B. Mortimer, *Permutation Groups* (Springer, New York, 1996).
- [15] A. B. Evans, 'The admissibility of sporadic simple groups', *J. Algebra* **321** (2009), 1407–1428.
- [16] A. B. Evans, 'The existence of strong complete mappings of finite groups: A survey', *Discrete Math.* **313**(11) (2013), 1191–1196.
- [17] R. J. Friedlander, B. Gordon and P. Tannenbaum, 'Partitions of groups and complete mappings', *Pacific J. Math.* **92**(2) (1981), 283–293.
- [18] D. Gorenstein, *Finite Groups*, 2nd edn (Chelsea, New York, 1980).
- [19] M. Hall and L. J. Paige, 'Complete mappings of finite groups', *Pacific J. Math.* **5** (1955), 541–549.
- [20] D. F. Hsu and A. D. Keedwell, 'Generalized complete mappings, neofields, sequenceable groups and block designs I', *Pacific J. Math.* **111** (1984), 317–332.

- [21] D. F. Hsu and A. D. Keedwell, 'Generalized complete mappings, neofields, sequenceable groups and block designs II', *Pacific J. Math.* **117** (1985), 291–312.
- [22] H. B. Mann, 'The construction of orthogonal latin squares', *Ann. Math. Statist.* **12** (1942), 418–423.
- [23] N. S. Mendelsohn, 'A natural generalization of Steiner triple systems', in: *Computers in Number Theory* (Academic Press, New York, 1971), 323–338.
- [24] N. S. Mendelsohn, 'Perfect cyclic designs', *Discrete Math.* **20** (1977), 63–68.
- [25] Y. Miao and L. Zhu, 'Perfect Mendelsohn designs with block size six', *Discrete Math.* **143** (1995), 189–207.
- [26] C. Nilrat and C. E. Praeger, 'Balanced directed cycle designs based on cyclic groups', *J. Aust. Math. Soc.* **58** (1995), 210–218.
- [27] C. E. Praeger, 'Balanced directed cycle designs based on groups', *Discrete Math.* **92** (1991), 275–290.
- [28] A. Thomson and S. Zhou, 'Frobenius circulant graphs of valency four', *J. Aust. Math. Soc.* **85** (2008), 269–282.
- [29] A. Thomson and S. Zhou, 'Frobenius circulant graphs of valency six, Eisenstein–Jacobi networks, and hexagonal meshes', *European J. Combin.* **38** (2014), 61–78.
- [30] A. Thomson and S. Zhou, 'Rotational circulant graphs', *Discrete Appl. Math.* **162** (2014), 296–305.
- [31] S. Wilcox, 'Reduction of the Hall–Paige conjecture to sporadic simple groups', *J. Algebra* **321**(5) (2009), 1407–1428.
- [32] J. Yin, 'The existence of $(v, 6, 3)$ -PMDs', *Math. Appl.* **6** (1993), 457–462.
- [33] X. Zhang, 'Constructions of resolvable Mendelsohn designs', *Ars Combin.* **34** (1992), 225–250.
- [34] X. Zhang, 'On the existence of $(v, 4, 1)$ -RPMD', *Ars Combin.* **42** (1996), 3–31.
- [35] X. Zhang, 'A few more RPMDs with $k = 4$ ', *Ars Combin.* **74** (2005), 187–200.
- [36] S. Zhou, 'A class of arc-transitive Cayley graphs as models for interconnection networks', *SIAM J. Discrete Math.* **23** (2009), 694–714.

D. F. HSU, Department of Computer and Information Sciences,
Fordham University, New York, NY 10023, USA
e-mail: hsu@cis.fordham.edu

SANMING ZHOU, School of Mathematics and Statistics,
The University of Melbourne, Parkville, VIC 3010, Australia
e-mail: sanming@unimelb.edu.au