The Dihedral Group as the Array Stabilizer of an Augmented Set of Mutually Orthogonal Latin Squares

Margaret A. Francel*
Mathematics and
Computer Science
The Citadel
Charleston, SC 29409
email: francelm@citadel.edu

David J. John
Computer Science
Wake Forest University
Winston-Salem, NC 27109
email: djj@wfu.edu

Abstract

This paper investigates the dihedral group as the array stabilizer of an augmented k-set of mutually orthogonal latin squares. Necessary conditions for the stabilizer to be a dihedral group are established. A set of two-variable identities essential for a dihedral group to be contained in an array stabilizer are determined. Infinite classes of models that satisfy the identities are constructed.

1 Introduction

A conjugate of a k-set of mutually orthogonal tables is a second k-set of mutually orthogonal tables constructed from the first k-set through a composition mapping. A conjugate k-set may have one or more tables in common with the original k-set. Of special interest are the mappings associated with conjugates that are equal to the original k-set. These mappings form a group, represented as a subgroup of S_k, the group of all permutations acting on the set $\{1, \ldots, k\}$. Following [3], this group of mappings is called the array stabilizer of the k-set.

Past research has considered conjugates of k-sets of mutually orthogonal tables and the stabilizer group from both a local and global perspective.

*Professor Francel thanks The Citadel Foundation for its support of this research.

Although the literature contains several equivalent notations for studying these ideas, we state below all results in terms of augmented k-sets of mutually orthogonal latin squares (mols) and array stabilizers.

Questions of interest from a local standpoint (i.e., for a specific k) include: what subgroups of S_k act as an array stabilizer, for each possible stabilizer group what identities and restrictions are satisfied by the tables, and for which n do there exist models of order n with that group as stabilizer. Lindner and Steedly [9] addressed these questions for the conjugates of a single latin square (i.e., a 3-set). Lindner and others [6, 7, 8] extended the notion of a conjugate to a 4-set, again addressing the same questions. Lindner also provided an excellent overview of the 3-set and 4-set cases in [5]. Francel [4] investigated the 5-set problem.

From a global perspective, the questions of interest are slightly different. Some collection of groups is examined. Questions of interest include: for what k can a member of the collection act as an array stabilizer, can the identities associated with the collection be described, and are there models for all members of the collection. Evans and Francel [2] examined when the array stabilizer has the largest order. They showed in this situation that the collection contains the sharply doubly transitive groups. This condition limits k to prime power values.

This paper is an analysis from a global perspective, examining the case where the array stabilizer of a k-set of mutually orthogonal tables is isomorphic to the dihedral group, D_k, the subgroup of S_k which are the symmetries of a regular k-gon. In Section 2, the background material necessary to define the problem and establish its solution is presented. In Section 3, we establish when a dihedral group can act as an array stabilizer and which two-variable identities the original set of tables must satisfy in order for this to happen. In Section 4, the paper constructs an infinite class of mutually orthogonal tables whose array stabilizer contains D_k. The paper concludes with Section 5 where two applications are presented.

2 Algebras, tables and array stabilizers

This section describes the environment needed to define the problem of interest in this paper and establish its solution. The material presented in this section is not new. It is found in more detail, including the proofs of all theorems, in several sources [2, 3, 4]. Proofs for Theorems 2.3 and 2.5 are included here, giving insight into the types of arguments that are commonly used.

A latin square of order n is an $n \times n$ table on n distinct elements such that every element appears exactly once in each row and column of the table. The set of table entries is designated by $\mathcal{N}$. Recall that every $n \times n$

table on $\mathcal{N}$ represents a binary operation over $\mathcal{N}$, and vice versa. This duality of tables and binary operations allows us to freely use a single symbol to represent both the table and the corresponding operation. One way of studying $n \times n$ latin squares on $\mathcal{N}$ is by viewing them as part of the collection of all binary operations over $\mathcal{N}$. This is the approach used in this paper.

Throughout the paper assume that $\mathcal{B}$ is the set of all binary operations over some specified set $\mathcal{N}$. A ternary operation on $\mathcal{B}$ is now introduced: for $a, b, c \in \mathcal{B}$, define the composition operation $[,,]$ on $\mathcal{B}$ as the binary operation

$$[a, b, c] : (x, y) \rightarrow a(b(x, y), c(x, y)) \text{ for all } x, y \in \mathcal{N}.$$

Example 2.1 *Over $\mathcal{N} = \{0, 1, 2\}$, let $a, b, c \in \mathcal{B}$, be defined by*

$$a = \begin{array}{|c|c|c|}\hline 0 & 1 & 2 \\ \hline 1 & 2 & 0 \\ \hline 2 & 0 & 1 \\ \hline \end{array}, \quad b = \begin{array}{|c|c|c|}\hline 0 & 1 & 2 \\ \hline 2 & 0 & 1 \\ \hline 1 & 2 & 0 \\ \hline \end{array}, \text{ and } \quad c = \begin{array}{|c|c|c|}\hline 0 & 2 & 1 \\ \hline 2 & 1 & 0 \\ \hline 1 & 0 & 2 \\ \hline \end{array},$$

then the binary operation $[a, b, c]$ is represented by the table:

$$[a, b, c] = \begin{array}{|c|c|c|}\hline 0 & 0 & 0 \\ \hline 1 & 1 & 1 \\ \hline 2 & 2 & 2 \\ \hline \end{array}$$

Under the composition operation $[,,]$, $\mathcal{B}$ is a clone of binary operations over $\mathcal{N}$ [1]. Let p_1 and p_2 represent the projection maps, $p_1(x, y) = x$ and $p_2(x, y) = y$ for all $x, y \in \mathcal{N}$.

Lemma 2.2 *The clone operation $[,,]$ on $\mathcal{B}$ has the following properties:*

(1) $[[a, b, c], d, e] = [a, [b, d, e], [c, d, e]]$,

(2) $[a, p_1, p_2] = a$, *and*

(3) $[p_1, a, b] = a$, *and* $[p_2, a, b] = b$.

Two binary operations a and b in $\mathcal{B}$ are said to be orthogonal, $a \perp b$, if the mapping $(x, y) \rightarrow (a(x, y), b(x, y))$ for $x, y \in \mathcal{N}$, is a bijection. Orthogonality extends to sets of tables. A k-set of tables, $\{a_1, \ldots, a_k\}$, is said to be mutually orthogonal if every pair of distinct tables in the set is orthogonal. Figure 1 gives an example of a 3-set of mutually orthogonal tables. Note all tables in the set are latin squares.

Throughout the paper all tables are of size $n \times n$, and all table entries are from the same set $\mathcal{N}$, unless explicitly stated otherwise.

$a_3 =$

0	2	4	1	3
4	1	3	0	2
3	0	2	4	1
2	4	1	3	0
1	3	0	2	4

$a_4 =$

0	3	1	4	2
3	1	4	2	0
1	4	2	0	3
4	2	0	3	1
2	0	3	1	4

$a_5 =$

0	4	3	2	1
2	1	0	4	3
4	3	2	1	0
1	0	4	3	2
3	2	1	0	4

Figure 1: Three 5 × 5 orthogonal latin squares on $\mathcal{N} = \{0, 1, 2, 3, 4\}$.

Theorem 2.3 *If $\mathcal{A} = \{a_1, \ldots, a_k\}$ is a k-set of mutually orthogonal tables and $u \perp v$, then $\{[a_i, u, v] \mid i = 1, \ldots, k\}$ is a k-set of mutually orthogonal tables.*

Proof. Let $a_1, \ldots, a_k, u, v \in \mathcal{B}$ with $\mathcal{A} = \{a_1, \ldots, a_k\}$ a k-set of mutually orthogonal tables and $u \perp v$. Let $x_1, y_1 \in \mathcal{N}$. Since $a_i \neq a_j$ in $\mathcal{A}$ are orthogonal, there exist $x_2, y_2 \in \mathcal{N}$ such that $a_i(x_2, y_2) = x_1$ and $a_j(x_2, y_2) = y_1$. Further, since $u \perp v$ there exists $x_3, y_3 \in \mathcal{N}$ such that $u(x_3, y_3) = x_2$ and $v(x_3, y_3) = y_2$. Thus,

$$[a_i, u, v](x_3, y_3) \quad = \quad a_i(u(x_3, y_3), v(x_3, y_3)) = a_i(x_2, y_2) = x_1$$

and

$$[a_j, u, v](x_3, y_3) \quad = \quad a_j(u(x_3, y_3), v(x_3, y_3)) = a_j(x_2, y_2) = y_1$$

which implies $[a_i, u, v] \perp [a_j, u, v]$. ■

Definition 2.4 *If $\mathcal{A} = \{a_1, \ldots, a_k\}$ is a k-set of mutually orthogonal tables and $u \perp v$, call the k-set $\{[a_1, u, v], \ldots, [a_k, u, v]\}$ a conjugate of $\mathcal{A}$, $\mathcal{A}(u, v)$.*

Finite field constructions can be used to illustrate the concept of the conjugate of a set of mutually orthogonal tables. The use of finite fields to construct orthogonal tables is a well-known technique. Define a binary operation $f(x, y) = rx + sy$ on a finite field F where r and s are elements of F. Theorem 2.5 given below gives conditions for orthogonality.

Theorem 2.5 *If r_1, r_2, r_3, r_4 are elements of some field F, then $f(x, y) = r_1x + r_2y$ and $g(x, y) = r_3x + r_4y$ are orthogonal tables if and only if $r_1r_4 - r_2r_3 \neq 0$.*

Proof. Let r_1, r_2, r_3, r_4 be elements of a field F, and define $f(x, y) = r_1x + r_2y$ and $g(x, y) = r_3x + r_4y$. If r_5, $r_6 \in F$, then $f(x, y) = r_5$

and $g(x,y) = r_6$ if and only if $x = (r_4r_5 - r_2r_6)/(r_1r_4 - r_2r_3)$ and $y = (r_1r_6 - r_3r_5)/(r_1r_4 - r_2r_3)$. ■

In the previous theorem, $f(x,y)$ and $g(x,y)$ belong to the ring of polynomials in x and y over the field F, $F[x,y]$.

Example 2.6 *Let $c_1(x,y) = 2x + y$, $c_2(x,y) = x + y$, $c_3(x,y) = y$, $c_4(x,y) = 4x+y$, and $c_5(x,y) = 3x+y$ belong to $Z_5[x,y]$. $C = \{c_1,\ldots,c_5\}$ is an orthogonal set of tables. Let $u(x,y) = x+4y$ and $v(x,y) = 4x+2y$, then $u \perp v$. Compose c_1, u and v to get, $[c_1,u,v](x,y) = c_1(u(x,y),v(x,y)) = c_1(x+4y, 4x+2y) = 2(x+4y) + (4x+2y) = x$. Compute $[c_i,u,v]$ for $i = 2,\ldots,5$ similarly; this generates the following conjugate of C,*

$$\mathcal{A} = C(u,v) = \begin{cases} p_1(x,y) &= [c_1,u,v](x,y) = x \\ p_2(x,y) &= [c_2,u,v](x,y) = y \\ a_3(x,y) &= [c_3,u,v](x,y) = 4x+2y \\ a_4(x,y) &= [c_4,u,v](x,y) = 3x+3y \\ a_5(x,y) &= [c_5,u,v](x,y) = 2x+4y \end{cases}$$

The tables for $[c_3,u,v]$, $[c_4,u,v]$ and $[c_5,u,v]$ are displayed in Figure 1, as a_3, a_4 and a_5, respectively. The binary operations $[c_1,u,v]$ and $[c_2,u,v]$ are the projections p_1 and p_2.

Next we define an important subclass of orthogonal tables and establish its relationship to the general class of orthogonal tables.

Lemma 2.7 *A table* **a** *is a latin square if and only if* **a** *is orthogonal to both p_1 and p_2.*

Theorem 2.8 *If $\mathcal{A} = \{a_1,\ldots,a_k\}$ is a k-set of mutually orthogonal tables with $a_1 = p_1$ and $a_2 = p_2$, then $\{a_3,\ldots,a_k\}$ is a k–2-set of mutually orthogonal latin squares.*

Definition 2.9 *A mutually orthogonal k-set that includes p_1 and p_2 is called an augmented set of mutually orthogonal latin squares, or an augmented set of mols.*

Theorem 2.10 *Every k-set of mutually orthogonal tables is conjugate to an augmented k-set of mols.*

Example 2.6 illustrates Theorem 2.10.

Given a k-set of mutually orthogonal tables we are interested in the collection of all $u \perp v$ such that $\mathcal{A} = \mathcal{A}(u,v)$. Associated with each such (u,v) is a permutation $\alpha_{u,v}$ of S_k defined on the indices of the tables in $\mathcal{A}$, $i\alpha_{u,v} = j$ if and only if $[a_i,u,v] = a_j$. The collection of all such permutations $\alpha_{u,v}$ is called the array stabilizer of $\mathcal{A}$, *ArrayStab* $\mathcal{A}$.

Theorem 2.11 *Let $\mathcal{A} = \{a_1, \ldots, a_k\}$ be a k-set of mutually orthogonal tables, then ArrayStab $\mathcal{A}$ is a subgroup of S_k whose order divides $k(k-1)$.*

Theorem 2.12 *Let $\mathcal{A}$ be a k-set of mutually orthogonal latin squares and $\alpha \in$ ArrayStab $\mathcal{A}$, where α is the product of non-trivial disjoint cycles $c_1, \ldots, c_m$, then each c_i has the same length, and either $| c_i |$ divides k and α has no fixed points or $| c_i |$ divides k–1 and α has a single fixed point.*

Theorem 2.13 *If $\mathcal{A}$ is a k-set of mutually orthogonal tables and $\mathcal{A}(u, v)$ is a conjugate of $\mathcal{A}$, then ArrayStab $\mathcal{A} =$ ArrayStab $\mathcal{A}(u, v)$.*

Theorems 2.10 and 2.13 together imply that without loss of generality the investigation of array stabilizers of orthogonal tables can be restricted to the investigation of array stabilizers of augmented sets of mols. This simplifies our task, as does the following theorem.

Theorem 2.14 *If $\mathcal{A} = \{a_1 = p_1, a_2 = p_2, a_3, \ldots, a_k\}$ is an augmented set of mols, then $\alpha \in$ ArrayStab $\mathcal{A}$ if and only if $a_{i\alpha} = [a_i, a_{1\alpha}, a_{2\alpha}]$.*

Example 2.15 *Revisiting Example 2.6, C is a 5-set of mols with conjugate $\mathcal{A} = C(u, v) = \{p_1, p_2, a_3, a_4, a_5\}$, where $a_1(x, y) = x = a_2(y, x)$, $a_3(x, y) = 4x + 2y = a_5(y, x)$ and $a_4(x, y) = 3x + 3y = a_4(y, x)$. Thus by Theorem 2.14, $\alpha = (1\ 2)(3\ 5)(4)$ is an element of ArrayStab $\mathcal{A}$, which by Theorem 2.13 implies $\alpha \in$ ArrayStab C. Similarly, it can be shown that $\mathcal{A}$ satisfies the identities associated with* (12345). *Therefore,* (12345) *belongs to ArrayStab C and ArrayStab $\mathcal{A}$.*

The order of the array stabilizer of an augmented k-set of mols is restricted by Theorem 2.11. As seen in Theorem 2.11 the largest order of the array stabilizer of an augmented k-set of mols is $k(k–1)$. Francel and Evans considered this largest order in [2]. They showed that if the array stabilizer of an augmented k-set of mols has order $k(k–1)$, then the array stabilizer is a sharply doubly transitive group and all the tables are idempotent. A group G is a sharply doubly transitive group of degree k if it is a permutation group on k elements and $x \neq y$ and $z \neq w$ implies there exists a unique permutation α in G with $x\alpha = z$ and $y\alpha = w$. It is well known that there exists a sharply doubly transitive group of degree k if and only if k is a prime power [10]. A table a is idempotent if for all $x \in \mathcal{N}$, $a(x, x) = x$. These results are summarized in the following theorem.

Theorem 2.16 *If the array stabilizer of a k-set of augmented mutually orthogonal tables has order $k(k–1)$, then k is a prime power, the array stabilizer is a sharply doubly transitive group on $\{1, \ldots, k\}$, and each of the tables is idempotent.*

We are interested in the case when the array stabilizer has order less than $k(k{-}1)$. Theorem 2.11 states that the order of the array stabilizer must divide $k(k{-}1)$, while Theorem 2.12 restricts the form of the permutations in the array stabilizer. This still leaves a large number of groups that potentially act as array stabilizers. For example, every cyclic group of order k or $k{-}1$ is a possible array stabilizer.

3 The dihedral group as an array stabilizer

Consider the situation where a dihedral group is a subgroup of the array stabilizer. We choose to study the dihedral groups for several reasons. First, they are an interesting class of groups. Second, they give us a infinite class of groups rather than a finite class of groups to analyze. Last, each dihedral group contains subgroups which are possible array stabilizers; for example, the subgroups of order 2 generated by the reflections, and the cyclic subgroup generated by a rotation.

The dihedral group D_k is the group of order $2k$ containing the symmetries of the regular polygon with k sides. This group is generated by two elements, a rotation and a reflection. If $k = 2t$, D_k is generated by the rotation $(1\ 2 \ldots k)$ and the reflection $(1\ 2)(3\ k)(4\ k{-}1)\ldots(t{+}1\ t{+}2)$. If $k = 2t{+}1$, D_k is generated by the rotation $(1\ 2 \ldots k)$ and the reflection $(1\ 2)(3\ k)(4\ k{-}1)\ldots(t{+}1\ t{+}3)(t{+}2)$.

To begin the study of the dihedral group as an array stabilizer necessary conditions are established.

Theorem 3.1 *Let $\mathcal{A} = \{a_1{=}p_1, a_2{=}p_2, a_3, \ldots, a_k\}$ be an augmented set of mols then*

(1) ArrayStab $\mathcal{A}$ cannot contain D_{k-1},
(2) if k is odd, then ArrayStab $\mathcal{A}$ can contain D_k, and
(3) if k is even, then ArrayStab $\mathcal{A}$ cannot contain D_k.

Proof. (1) Assume D_{k-1} is a subgroup of *ArrayStab* $\mathcal{A}$, where $\mathcal{A}$ is a k-set of augmented mols. D_{k-1}, as a group of permutations on $k{-}1$ symbols, leaves one of the indices $1, \ldots, k$ fixed, call it m. Consider the reflections in D_{k-1}. If $k{-}1$ is odd then each reflection fixes one of the indices $1, \ldots, \not m, \ldots, k$, if $k{-}1$ is even there are reflections that fix two opposite corners in the regular $k-1$-gon labelled with $1, \ldots, \not m, \ldots, k$. Both cases admit a permutation in *ArrayStab* $\mathcal{A}$ that fixes m and at least one more point. This contradicts Theorem 2.12. (2) Assume k is odd, then D_k meets the conditions of Theorems 2.11 and 2.12. So, it is possible that D_k is an array stabilizer for some k-set of mols. (3) Assume k is even, then the order of D_k is $2k$. Since 2 does not divide $k{-}1$, $2k$ does not divide $k(k{-}1)$. This is a contradiction of

Theorem 2.11 since the order of any subgroup of *ArrayStab* $\mathcal{A}$ must divide $k(k\text{--}1)$. ■

For each $\alpha \in$ *ArrayStab* $\mathcal{A}$ there exist k identities that the tables of $\mathcal{A}$ satisfy, namely, $[a_i, a_{1\alpha}, a_{2\alpha}](x,y) = a_{i\alpha}(x,y)$ for $i = 1, \ldots, k$. Conversely, if an augmented k-set of mols, $\mathcal{A}$, satisfies the identities $[a_i, a_{1\alpha}, a_{2\alpha}](x,y) = a_{i\alpha}(x,y)$ for $i = 1, \ldots, k$, and $\alpha \in S_k$, then α is an element of *ArrayStab* $\mathcal{A}$. It is desirable to reduce this set of identities associated with the permutations of the array stabilizer to a smaller subset of identities from which all the other identities can be derived. One useful reduction technique is described in the following lemma.

Lemma 3.2 *Let* $\mathcal{A} = \{a_1{=}p_1, a_2{=}p_2, a_3, \ldots, a_k\}$ *be an augmented set of mols. If* $\mathcal{A}$ *satisfies the identities associated with the permutations* $\alpha, \beta \in S_k$, $[a_i, a_{1\alpha}, a_{2\alpha}] = a_{i\alpha}$ *and* $[a_i, a_{1\beta}, a_{2\beta}] = a_{i\beta}$ *for each* i, *then* $\mathcal{A}$ *satisfies the identities associated with* $\alpha\beta$, $[a_i, a_{1\alpha\beta}, a_{2\alpha\beta}] = a_{i\alpha\beta}$ *for each* i.

Proof. Let $\mathcal{A} = \{a_1{=}p_1, a_2{=}p_2, a_3, \ldots, a_k\}$ be an augmented set of mols that satisfy the identities $\alpha, \beta \in S_k$. From the above discussion and Lemma 2.2 for $i = 1, \ldots, k$

$$\begin{aligned} a_{(i\alpha)\beta} &= [a_{i\alpha}, a_{1\beta}, a_{2\beta}] = [[a_i, a_{1\alpha}, a_{2\alpha}], a_{1\beta}, a_{2\beta}] \\ &= [a_i, [a_{1\alpha}, a_{1\beta}, a_{2\beta}], [a_{2\alpha}, a_{1\beta}, a_{2\beta}]] = [a_i, a_{1\alpha\beta}, a_{2\alpha\beta}]. \end{aligned}$$

Thus, $\mathcal{A}$ satisfies the identities associated with the permutation $\alpha\beta$. ■

Example 3.3 *Continuing with Example 2.15, since the identities associated with the permutations* (12345) *and* (12)(35)(4) *are satisfied by the augmented* 5*-set of mols* $\mathcal{A} = \{p_1, p_2,\ a_3(x,y) = 4x + 2y,\ a_4(x,y) = 3x + 3y,\ a_5(x,y) = 2x + 4y\}$, *Lemma 3.2 tells us that* $\langle (12345), (12)(35)(4) \rangle$, *the group generated by the permutations* (12345) *and* (12)(35)(4), *is a subgroup of ArrayStab* $\mathcal{A}$.

Using Lemma 3.2, the next theorem isolates a minimal set of identities which the tables in $\mathcal{A}$ must satisfy when D_k is contained in *ArrayStab* $\mathcal{A}$.

Theorem 3.4 *Let* $k = 2t{+}1$ *and let* $\mathcal{A} = \{a_1{=}p_1, a_2{=}p_2, a_3, \ldots, a_k\}$ *be an augmented set of mols. The tables in* $\mathcal{A}$ *satisfy the identities*

(1) $a_i(x,y) = a_{k+3-i}(y,x)$ *for* $i = t{+}2, \ldots, k$,
(2) $a_{t+2}(x,y) = a_{t+2}(y,x)$,
(3) $a_i(x,y) = a_{i-1}(y, a_3(x,y))$ *for* $i = 4, \ldots, k$, *and*
(4) $x = a_k(y, a_3(x,y))$,

if and only if D_k *is contained in ArrayStab* $\mathcal{A}$.

Proof. D_k is generated by two permutations: the reflection, $(1\ 2)(3\ k)(4\ k\text{--}1)\ldots(t{+}1\ t{+}3)(t{+}2)$, and the rotation, $(1\ 2 \ldots k)$. The identities in (1) and (2) are those associated with the reflection generator $(1\ 2)(3\ k)(4\ k-1)\ldots(t+1\ t+3)(t+2)$. The identities in (3) and (4) are those associated with the rotation generator, $(1\ 2\ldots k)$. Lemma 3.2 guarantees that the identities associated with the other permutations in D_k are derived from the identities of (1)-(4). ∎

4 Mols with dihedral array stabilizers

In the previous section, it was shown that a k-set of mols never contains D_{k-1} in its array stabilizer, and can contain D_k only if k is odd. In this section, we construct, for all odd k, an infinite class of mols such that each k-set of mols in the class contains D_k, a dihedral group, in its array stabilizer.

For a subgroup H of S_k to be contained in the array stabilizer of a k-set of mols, it is sufficient to show that the tables of $\mathcal{A}$ satisfy all the identities associated with the permutations of H. However, to verify that H is precisely the array stabilizer is more complicated. Besides validating that the tables of $\mathcal{A}$ fulfil the identities associated with the permutations of H, it is also necessary to show that for each possible array stabilizer K in S_k that contains H, there exits a permutation $\alpha \in K-H$ such that the tables of $\mathcal{A}$ do not satisfy identically at least one of the identities associated with α.

To illustrate the difference discussed in the above paragraph and to establish the existence of both proper containment and equality to the array stabilizer, the dihedral group $D_5 = \langle(12345),(12)(35)(4)\rangle$ is considered in conjunction with two different sets of mols in this and the next two paragraphs. Francel [4] has shown the only possible array stabilizer of S_5 that properly contains D_5 is the subgroup $\langle(12345),(1325)(4)\rangle$. Thus for an augmented 5-set of mols $\mathcal{A}$ that satisfies the identities of D_5 examining the identities associated with $\alpha = (1325)(4)$ determines whether D_5 equals *ArrayStab* $\mathcal{A}$, or is a proper subgroup of it.

First examine the 5-set $\mathcal{A} = \{p_1,p_2,\ a_3(x,y) = 10x+3y,\ a_4(x,y) = 8x+8y,\ a_5(x,y) = 3x+10y\}$, where each of these polynomials belongs to $Z_{11}[x,y]$, the ring of polynomials in variables x and y over the field Z_{11}. It is straight forward to show that $\mathcal{A}$ is an augmented 5-set of mols and that D_5 is a subgroup of *ArrayStab* $\mathcal{A}$. For the tables of $\mathcal{A}$ to satisfy the identities of $\alpha = (1325)(4)$ Theorem 2.14 implies that $a_{3\alpha} = [a_3, a_{1\alpha}, a_{2\alpha}]$, simplified as $a_2 = [a_3, a_3, a_5]$, however $[a_3, a_3, a_5](x,y) = 10(10x+3y)+3(3x+10y) = 10x+5y \neq y$. Hence, $\mathcal{A}$ does not satisfy the identities of α; it follows that *ArrayStab* $\mathcal{A} = D_5$.

Next consider the augmented 5-set of mols $\mathcal{A}$ generated in Example 2.6. In Example 3.3 the array stabilizer of this set was shown to satisfy the identities of D_5. However using the method illustrated in Example 2.6, it can be shown that $\mathcal{A}$ also satisfies the identities associated with (1325)(4). Thus D_5 is a proper subgroup of *ArrayStab* $\mathcal{A} = \langle(12345), (1325)(4)\rangle$.

Since there is no one set of subgroups that represents all possible array stabilizers that contain the dihedral group, the following discussion is limited to containment.

We are now ready to construct augmented k-sets of mols such that a dihedral group is contained in each of the corresponding array stabilizers. Linear functions over finite fields are used to define the latin squares in each k-set. In Section 4.1, field properties are identified that guarantee that such a set of mols can be constructed from the field elements. In Section 4.2, two sequences of irreducible polynomials are derived which lead to fields with the properties identified in Section 4.1. Finally, the construction of the desired sets of mols is presented in Section 4.3.

4.1 Identifying sufficient field properties

Theorem 4.1 exhibits field properties that admit linear functions which generate latin squares with the desired properties, i.e. latin squares that satisfy the identities of Theorem 3.4. Here and throughout the remainder of the section assume that k is odd.

Theorem 4.1 *Let $k = 2t{+}1$. If there exists a finite field F of characteristic two ($\forall z \in F, z{+}z = 0$) and order 2^n that contains a sequence of elements $s_1 = 1, s_2, \ldots, s_{k-1}$ such that (1) s_i is non-zero for $1 \leq i \leq k{-}1$, (2) $s_i = s_{i-2} + s_2 s_{i-1}$ for $3 \leq i \leq k{-}1$, and (3) $s_t = s_{t+1}$, then $\mathcal{A} = \{a_1{=}p_1(x,y){=} x,\ a_2{=}p_2(x,y){=}y,\ a_3(x,y) = s_1 x + s_2 y, \ldots,\ a_k(x,y) = s_{k-2}x + s_{k-1}y\}$ is an augmented set of mols of order 2^n such that $D_k \subseteq$ ArrayStab $\mathcal{A}$.*

The proof of Theorem 4.1 is divided into four pieces, each addressed in a separate lemma. Lemma 4.2 shows that $\mathcal{A} - \{p_1, p_2\}$ is a set of mutually orthogonal latin squares. Each of Lemmas 4.3, 4.4 and 4.5 shows that one of the identities of Theorem 3.4 is satisfied. For each of the four lemmas assume $k = 2t{+}1$, F is a finite field of characteristic two having order 2^n, and there exists a sequence of elements $s_1 = 1, s_2, \ldots, s_{k-1}$ with properties (1) s_i is non-zero for $1 \leq i \leq k{-}1$, (2) $s_i = s_{i-2} + s_2 s_{i-1}$ for $3 \leq i \leq k{-}1$, and (3) $s_t = s_{t+1}$.

Lemma 4.2 *$\{a_3, \ldots, a_k\}$ is a set of mols.*

Proof. Since, for $i = 4, \ldots, k$,

$$\begin{aligned} s_1 s_{i-1} + s_2 s_{i-2} &= 1(s_{i-3} + s_2 s_{i-2}) + s_2 s_{i-2} \\ &= s_{i-3} \neq 0, \end{aligned}$$

it follows from Theorem 2.5 that a_3 is orthogonal to a_i.

Assume that $\{a_3, \dots, a_{m-1}\}$, $4 \le m{-}1 \le k{-}1$, is a set of mols. Consider a_m and a_j, $4 \le j \le m{-}1$.

$$\begin{aligned} s_{m-2}s_{j-1} + s_{m-1}s_{j-2} &= s_{m-2}(s_{j-3} + s_2 s_{j-2}) + (s_{m-3} + s_2 s_{m-2})s_{j-2} \\ &= s_{m-2}s_{j-3} + s_2 s_{m-2}s_{j-2} + \\ &\qquad s_{m-3}s_{j-2} + s_2 s_{m-2} s_{j-2} \\ &= s_{m-2}s_{j-3} + s_{m-3}s_{j-2} \neq 0 \end{aligned}$$

by the induction assumption and Theorem 2.5. Thus, $a_m \perp a_j$. ■

Lemma 4.3 *For* $3 \le i \le k{-}1$, $a_{i+1}(x,y) = [a_i, p_2, a_3](x,y)$.

Proof. By assumption $s_1 = 1$ and $s_i = s_{i-2} + s_2 s_{i-1}$ for $3 \le i \le k{-}1$. Thus,

$$\begin{aligned} [a_i, p_2, a_3](x,y) &= a_i(p_2(x,y), a_3(x,y)) = a_i(y, s_1 x + s_2 y) \\ &= s_{i-2}y + s_{i-1}(x + s_2 y) = s_{i-1}x + (s_{i-2} + s_2 s_{i-1})y \\ &= s_{i-1}x + s_i y = a_{i+1}(x,y). \quad ■ \end{aligned}$$

Lemma 4.4 *For* $3 \le i \le t{+}1$, $a_{t+i}(x,y) = a_{t+4-i}(y,x)$.

Proof.

Initially consider when $i = 3$. Examining the sequence element s_{t+2} shows

$$\begin{aligned} s_{t+2} &= s_t + s_2 s_{t+1} = s_{t+1} + s_2 s_t \\ &= s_{t-1} + s_2 s_t + s_2 s_t = s_{t-1}. \end{aligned}$$

Hence,

$$\begin{aligned} a_{t+3}(x,y) &= s_{t+1}x + s_{t+2}y = s_t x + s_{t-1}y \\ &= a_{t+1}(y,x) = a_{t+4-3}(y,x). \end{aligned}$$

Assume for $3 \le i \le m-1$ that $a_{t+i}(x,y) = a_{t+4-i}(y,x)$. As a consequence of this assumption, $s_{t+i-2}x + s_{t+i-1}y = s_{t+2-i}y + s_{t+3-i}x$ for $3 \le i \le m{-}1$, which implies $s_{t+i-2} = s_{t+3-i}$ and $s_{t+i-1} = s_{t+2-i}$ for $3 \le i \le m{-}1$ or $s_{t+j} = s_{t+1-j}$ for $1 \le j \le m{-}2$.

Finally, consider when $i = m$. Examining the sequence element s_{t+m-1} shows

$$\begin{aligned} s_{t+m-1} &= s_{t+m-3} + s_2 s_{t+m-2} = s_{t+1-(m-3)} + s_2 s_{t+1-(m-2)} \\ &= s_{t+4-m} + s_2 s_{t+3-m} \\ &= (s_{t+2-m} + s_2 s_{t+3-m}) + s_2 s_{t+3-m} = s_{t+2-m}. \end{aligned}$$

Hence,

$$\begin{aligned} a_{t+m}(x,y) &= s_{t+m-2}x + s_{t+m-1}y = s_{t+1-(m-2)}x + s_{t+1-(m-1)}y \\ &= s_{t+2-m}y + s_{t+3-m}x = a_{t+4-m}(y,x) \quad ■ \end{aligned}$$

Lemma 4.5 $[a_k, p_2, a_3](x,y) = x$.

Proof. From Lemma 4.4, $a_k(x,y) = a_3(y,x)$. Thus,

$$\begin{aligned} [a_k, p_2, a_3](x,y) &= a_k(p_2(x,y), a_3(x,y)) \\ &= a_3(a_3(x,y), p_2(x,y)) = x + s_2 y + s_2 y = x. \quad ■ \end{aligned}$$

Proof. (of Theorem 4.1) By Lemma 4.2 it follows that $\mathcal{A}$ is an augmented set of mols. By assumption, Property (2) of Theorem 3.4 is true. Properties (1), (3) and (4) of Theorem 3.4 follow from Lemmas 4.3, 4.4 and 4.5, respectively. Thus, Theorem 3.4 implies that D_k is contained in the array stabilizer of $\mathcal{A}$. ∎

4.2 Generating an appropriate field

In Theorem 4.1 the values of $s_3, \ldots, s_k$ are dependent solely on s_2. Finding a field element s_2 which generates a sequence satisfying the hypothesis of Theorem 4.1 is the next step in the process of constructing sets of mols with a dihedral group in their stabilizer. Not all field elements are suitable choices for s_2. In this subsection a field is identified by way of an irreducible polynomial that leads in Section 4.3 to an appropriate choice for s_2.

Two sets of polynomials will be shown to be irreducible, ${}_1p_i(x)$ where $i \neq 1 \bmod 3$, and ${}_3p_i(x)$ where $i = 1 \bmod 3$. These irreducible polynomials over Z_2 will be used to construct fields whose elements will produce linear equations that define a set of mols with array stabilizer containing a dihedral group.

The following polynomials $q_i(x)$ will play important roles in the definitions of polynomials ${}_1p_i(x)$ and ${}_2p_i(x)$, and later the field elements s_i.

Definition 4.6 *In $Z_2[x]$ define the sequence of polynomials $q_i(x)$ as follows: $q_1(x) = 1$, $q_2(x) = x$, and for $i \geq 3$ $q_i(x) = q_{i-2}(x) + xq_{i-1}(x)$.*

The degree of $q_i(x)$ is $i - 1$. The next two lemmas establish the roots of $q_i(x)$ in Z_2.

Lemma 4.7 *$q_i(0) = 0$ if and only if i is even.*

Proof. Since $q_1(0) = 1$, $q_2(0) = 0$, and $q_i(0) = q_{i-2}(0) + 0q_{i-1}(0) = q_{i-2}(0)$ the result follows. ∎

Lemma 4.8 *$q_i(1) = 0$ if and only if $i = 0 \bmod 3$.*

Proof. Since $q_1(1) = 1$, $q_2(1) = 1$, $q_i(1) = q_{i-2}(1) + 1q_{i-1}(1)$ for $i \geq 3$, and $1 + 1 = 0$, the result follows. ∎

Using the $q_i(x)$ polynomials, we construct irreducible polynomials in Theorems 4.12 and 4.14 which lead to fields that satisfy the properties of Theorem 4.1.

Definition 4.9 *For $i \geq 2$, define two sequences of polynomials as follows: ${}_1p_i(x) = q_{i-1}(x) + (1 + x)q_i(x)$, and ${}_2p_i(x) = q_i(x) + q_{i+1}(x)$.*

The degrees of the polynomials ${}_1p_i(x)$ and ${}_2p_i(x)$ are i.

Lemma 4.10 *For $i \geq 2$, ${}_1p_i(0) ={}_2 p_i(0) = 1$.*

Proof. For $i \geq 2$, ${}_1p_i(0) = q_{i-1}(0)+(1+0)q_i(0)$ and ${}_2p_i(0) = q_i(0)+q_{i+1}(0)$. Thus the result follows from Lemma 4.7. ■

Lemma 4.11 *For $i \geq 2$, ${}_1p_i(1) ={}_2 p_i(1) = 1$ if and only if $i \neq 1 \bmod 3$.*

Proof. For $i \geq 2$, ${}_1p_i(1) = q_{i-1}(1) + (1+1)q_i(1) = q_{i-1}(1)$, and ${}_2p_i(1) = q_{i-1}(1) + q_i(1)$, the lemma follows from Lemma 4.8. ■

Theorem 4.12 *For $i \geq 2$, ${}_1p_i(x)$ is irreducible over Z_2 if and only if $i \neq 1 \bmod 3$.*

Proof. Lemmas 4.10 and 4.11 establish this result. ■

The next lemma leads to Theorem 4.14 which defines the set of irreducible polynomials ${}_3p_i(x)$ over Z_2. In $Z_2[x]$, the polynomial x^2+1 equals the polynomial $(x+1)^2$.

Lemma 4.13 *If $i \geq 4$ and $i = 1 \bmod 3$ then $x+1$ divides ${}_2p_i(x)$ but $(x+1)^2$ does not divide ${}_2p_i(x)$.*

Proof. Assume $i = 3r+1$ for some $r \geq 1$. Lemma 4.8 implies ${}_2p_i(1) = q_i(1) + q_{i+1}(1) = 1+1 = 0$, hence $x+1$ divides ${}_2p_i(x)$.

Since

$$\begin{aligned} {}_2p_i(x) &= q_i(x) + q_{i+1}(x) \\ &= q_i(x) + (q_{i-1}(x) + xq_i(x)) \\ &= q_i(x) + q_{i-1}(x) + x(q_{i-2}(x) + xq_{i-1}(x)) \\ &= q_i(x) + q_{i-1}(x) + xq_{i-2}(x) + x^2q_{i-1}(x)) \\ &= q_i(x) + xq_{i-2}(x) + (1+x^2)q_{i-1}(x) \\ &= q_{i-2}(x) + xq_{i-1}(x) + xq_{i-2}(x) + (1+x^2)q_{i-1}(x) \\ &= (1+x)q_{i-2}(x) + x(q_{i-3}(x) + xq_{i-2}(x)) + (1+x^2)q_{i-1}(x) \\ &= (1+x^2)(q_{i-2}(x) + q_{i-1}(x)) + x(q_{i-3}(x) + q_{i-2}(x)) \end{aligned}$$

it follows that $1+x^2$ divides ${}_2p_i(x)$ if and only if $(1+x^2)$ divides $q_{i-3}(x) + q_{i-2}(x)$. Continuing the reduction shows that $(1+x^2)$ divides ${}_2p_i(x)$ if and only if $1+x^2$ divides $q_1(x)+q_2(x) = 1+x$. Therefore $1+x^2$ does not divide ${}_2p_i(x)$. ■

Theorem 4.14 *If $i \geq 4$ and $i = 1 \bmod 3$ then ${}_2p_i(x) = (x+1){}_3p_i(x)$ where ${}_3p_i(x)$ is an irreducible polynomial over Z_2.*

4.3 Constructing the mols

Theorems 4.12 and 4.14 establish for every positive odd integer a set of irreducible polynomials over Z_2. In this subsection, these polynomials will be used to build augmented sets of mols whose array stabilizer contains a dihedral group.

The irreducible polynomials of Section 4.2 serve two purposes. They are used to identify a field in which to build mols, and each polynomial provides a field identity that is essential to showing that a sequence of field elements exists satisfying the properties of Theorem 4.1 and hence the identities of Theorem 3.4. The irreducible polynomials ${}_1p_i(x)$ yield an identity, namely $s_{t+1} = s_{t-1} + s_2 s_t$, that is related to the identities associated with the dihedral group reflection permutation. As a consequence, when using ${}_1p_i(x)$ to define the field, the elements s_i are defined to satisfy the identities associated with the rotation, then it is proven that they satisfy the associated reflection identities. On the other hand, the polynomial ${}_2p_i(x)$ yields an identity, namely $s_{t+1} = s_t$, that is related to the identities associated with the dihedral group rotation permutation. Using ${}_2p_i(x)$, the elements s_i are defined to satisfy the dihedral group reflection, and then identities related to the dihedral group rotation are proven.

First consider the case where $k=2t+1$ and $t \neq 1 \bmod 3$. From Theorem 4.12, ${}_1p_t(x)$ is an irreducible polynomial over Z_2 with degree t. Let α be an element in a splitting field for ${}_1p_t(x)$ where α is a root of ${}_1p_t(x)$.

Definition 4.15 *Define a sequence of 2t field elements in $Z_2(\alpha)$ as follows: for $i = 1, \ldots, t$, let $s_i = q_i(\alpha)$, and for $j = 1, \ldots, t$, let $s_{t+j} = s_{t+1-j}$.*

Lemma 4.16 *Let $k = 2t+1$ where $t \neq 1 \bmod 3$, then the sequence of elements $s_1 = 1, \ldots, s_{k-1}$ satisfy:*

(1) each s_i is non-zero,

(2) $s_i = s_{i-2} + s_2 s_{i-1}$ for $3 \leq i \leq k-1$, and

(3) $s_{t+1} = s_t$,

Proof. (1) $Z_2(\alpha)$ is a vector space over Z_2 with a basis $< 1, \alpha, \ldots, \alpha^{t-1} >$. This implies for $1 \leq i \leq t$ that $s_i = q_i(\alpha)$ is non-zero since each $q_i(x)$ has degree $i-1$. By the symmetric definition of the s_i's it follows that all the s_i's are non-zero.

(2) This argument is split into three cases corresponding to the initial, middle and final s_i terms.

Case 1: For $3 \leq i \leq t$, $s_i = q_i(\alpha)$, and $s_2 = q_2(\alpha) = \alpha$. From Definition 4.6 $q_i(x) = q_{i-2}(x) + xq_{i-1}(x)$. This yields $s_i = q_i(\alpha) = q_{i-2}(\alpha) + \alpha q_{i-1}(\alpha) = s_{i-2} + s_2 s_{i-1}$.

Case 2: Assume $i = t+1$. Since ${}_1p_t(\alpha) = q_{t-1}(\alpha) + (1+\alpha)q_t(\alpha) = 0$, it follows $s_{t-1} + (1+s_2)s_t = 0$. Simplifying, we get $s_{t-1} + s_2 s_t = s_t$. Since $s_t = s_{t+1}$, the result follows.

Case 3: For $t+2 \leq i \leq k-1$ write i as $t+1+j$ where $1 \leq j \leq t-1$. Using cases 1 and 2 and Definition 4.15,

$$\begin{aligned} s_i &= s_{t+1+j} = s_{(t+1)-(1+j)} = s_{t-j} \\ &= s_{t-j} + 0 = s_{t-j} + (s_2 s_{t+1-j} + s_2 s_{t+1-j}) \\ &= (s_{t-j} + s_2 s_{t+1-j}) + s_2 s_{t+1-j} \\ &= s_{t+2-j} + s_2 s_{t+1-j} = s_{(t+1)-(j-1)} + s_2 s_{(t+1)-j} \\ &= s_{t+j-1} + s_2 s_{t+j} = s_{i-2} + s_2 s_{i-1} \end{aligned}$$

(3) From Definition 4.15, $s_{t+1} = s_t$. ■

Second consider the case where $k = 2t+1$ and $t = 1 \bmod 3$. As established in Theorem 4.14, ${}_3p_t(x)$ is an irreducible polynomial over Z_2 with degree $t-1$. Let β be an element in a splitting field for ${}_3p_t(x)$ where β is a root of ${}_3p_t(x)$.

Definition 4.17 *Define a sequence of 2t field elements in $Z_2[\beta]$ as follows: for $i = 1, \ldots, 2t$, let $s_i = q_i(\beta)$.*

Lemma 4.18 *Let $k = 2t+1$ and $t = 1$ mod 3, then the sequence of elements $s_1 = 1, \ldots, s_{k-1}$ of $Z_2[\beta]$ satisfy the following:*

(1) each s_i is non-zero,
(2) $s_i = s_{i-2} + s_2 s_{i-1}$ for $3 \leq i \leq k-1$, and
(3) $s_{t+1} = s_t$.

Proof. (1) This argument is split into four cases corresponding to the initial, two middle and final s_i terms.

Case 1: Assume $1 \leq i \leq t-2$. By Theorem 4.14, ${}_3p_t(x)$ is an irreducible polynomial of degree $t-1$. Thus $Z_2(\beta)$ is a vector space over Z_2 with basis $< 1, \beta, \ldots, \beta^{t-2} >$. This implies that for $1 \leq i \leq t-2$, $s_i = q_i(\beta)$ is non-zero.

Case 2: Assume $i = t-1$. If $s_{t-1} = 0$ then $s_{t-3} + \beta s_{t-2} = q_{t-3}(\beta) + \beta q_{t-2}(\beta) = 0$, which implies that β^{t-2} can be written as a linear combination of $1, \beta, \ldots, \beta^{t-3}$. Hence it must be $s_{t-1} \neq 0$.

Case 3: Assume $i = t$. If $s_t = 0$ then it further follows that $s_{t+1} = 0$. Since $s_{t+1} = s_{t-1} + s_2 s_t$, it then follows that $s_{t-1} = 0$ which contradicts Case 2.

Case 4: Assume $t+1 \leq i \leq 2t$, and write i as $t+j$. It will be established that $s_i = s_{t+j} = s_{t+1-j}$ and then the result follows from the previous cases.

From (2) $s_{t+1} = s_t = s_{t+1-1}$. Now assume for $1 \leq j \leq m-1$ that $s_{t+j} = s_{t+1-j}$. Considering s_{t+m}:

$$\begin{aligned} s_{t+m} &= s_{t+m-2} + s_2 s_{t+m-1} = s_{t+(m-2)} + s_2 s_{t+(m-1)} \\ &= s_{t+1-(m-2)} + s_2 s_{t+1-(m-1)} = s_{t+3-m} + s_2 s_{t+2-m} \\ &= (s_{t+1-m} + s_2 s_{t+2-m}) + s_2 s_{t+2-m} = s_{t+1-m} \end{aligned}$$

(2) This follows directly from Definition 4.17.

(3) Since β is a root of ${}_3p_t(x)$, β is also a root of ${}_2p_t(x)$, which gives $q_t(\beta) + q_{t+1}(\beta) = 0$. Hence $s_{t+1} = q_{t+1}(\beta) = q_t(\beta) = s_t$. ■

Lemmas 4.16 and 4.18 immediately yield the main result, Theorem 4.19.

Theorem 4.19 *Let $k = 2t+1 \geq 5$, then for $n \geq t+1$, there exists an augmented set of mols $\mathcal{A}$ of order 2^n such that $D_k \subseteq$ ArrayStab $\mathcal{A}$.*

5 Applications

We conclude the paper with two specific applications of the results discussed in the previous sections. In the first application, an augmented 7-set of mols with array stabilizer D_7 is constructed using the methods in Section 4.

Example 5.1 *Let $k = 7$, writing k as $2t+1$ yields $t = 3 \neq 1 \bmod 3$. Using Definition 4.6, $q_1(x) = 1$, $q_2(x) = x$ and $q_3(x) = 1 + x^2$. The polynomial ${}_1p_3(x) = q_2(x) + (1 + x)q_3(x) = 1 + x^2 + x^3$ is irreducible over Z_2. Let α be a root of ${}_1p_3(x)$ over some splitting field. As prescribed in Definition 4.15, define $s_1, \ldots, s_6$: $s_1 = 1$, $s_2 = q_2(\alpha) = \alpha$, $s_3(\alpha) = q_3(\alpha) = 1 + \alpha^2$, $s_4 = s_3 = 1 + \alpha^2$, $s_5 = s_2 = \alpha$, and $s_6 = s_1 = 1$.*

It follows immediately from the statement of Theorem 4.1 that the set of polynomials, $\mathcal{A} = \{p_1(x,y) = x, p_2(x,y) = y, a_3(x,y) = x + \alpha y, a_4(x,y) = \alpha x + (1 + \alpha^2)y, a_5(x,y) = (1 + \alpha^2)x + (1 + \alpha^2)y, a_6(x,y) = (1 + \alpha^2)x + \alpha y, a_7(x,y) = \alpha x + y\}$, is an augmented 7-set of mols of order 8 with D_7 in ArrayStab $\mathcal{A}$.

By Theorem 2.12, the order of the array stabilizer of a 7-set of augmented mols must divide 42. Since D_7 has order 14 and is a subgroup of ArrayStab $\mathcal{A}$, this implies ArrayStab $\mathcal{A}$ is either D_7 or has order 42. However, if ArrayStab $\mathcal{A}$ has order 42, then Theorem 2.16 implies the mols in $\mathcal{A}$ with this "largest" array stabilizer must be idempotent, i.e. $a_i(x,x) = x$. Examining $a_3(x,y)$, one sees that $a_3(x,x) \neq x$. Thus it must be the case that ArrayStab $\mathcal{A} = D_7$.

All of the latin squares constructed in Section 4 had order 2^n for some $n \in Z^+$. The final application shows that this is not a necessary condition for an augmented set of mols to contain a dihedral group in its array stabilizer.

Example 5.2 *Consider the following latin squares defined by polynomials over Z_{17}, $a_3(x,y) = a_9(y,x) = 16x + 7y$, $a_4(x,y) = a_8(y,x) = 10x + 14y$, $a_5(x,y) = a_7(y,x) = 3x + 6y$ and $a_6(x,y) = 11x + 11y$. Using Theorem 2.5, it is straightforward to show that $\mathcal{A} = \{p_1, p_2, a_3, \ldots, a_9\}$ is a 9-set of augmented mols.*

Considering the permutation $\alpha = (123456789)$, *we find*

$$a_{i\alpha}(x,y) = [a_i, p_{1\alpha}, p_{2\alpha}](x,y)$$

yields:

$$\begin{array}{rcl}
[p_1, p_2, a_3](x,y) & = & p_2(x,y) \\
[p_2, p_2, a_3](x,y) & = & a_3(x,y) \\
[a_3, p_2, a_3](x,y) & = & 16y + 7(16x + 7y) = a_4(x,y) \\
[a_4, p_2, a_3](x,y) & = & 10y + 14(16x + y) = a_5(x,y) \\
[a_5, p_2, a_3](x,y) & = & 3y + 6(16x + 7y) = a_6(x,y) \\
[a_6, p_2, a_3](x,y) & = & 11y + 11(16x + 7y) = a_7(x,y) \\
[a_7, p_2, a_3](x,y) & = & 6y + 3(16x + 7y) = a_8(x,y) \\
[a_8, p_2, a_3](x,y) & = & 14y + 10(16x + 7y) = a_9(x,y) \\
[a_9, p_2, a_3](x,y) & = & 7y + 16(16x + 7y) = p_1(x,y)
\end{array}$$

Hence by Theorem 2.14, $\alpha \in$ *ArrayStab* $\mathcal{A}$. *Similarly, consideration of the permutation* $\beta = (12)(39)(48)(57)(6)$ *shows that* $\beta \in$ *ArrayStab* $\mathcal{A}$. *Thus* $D_9 \subseteq$ *ArrayStab* $\mathcal{A}$.

The authors thank the reviewer for constructive suggestions that significantly improved this paper.

References

[1] T. Evans, *Some Remarks on the General Theory of Clones, Proceedings on the Conference on Finite Algebra and Multiple-Valued Logic*, August 1979, North Holland.

[2] T. Evans and M. Francel, *Some Connections between Steiner Systems and Self-Conjugate Sets of M.O.L.S., Annals of Discrete Mathematics*, 15 (1982), 143-159.

[3] M. Francel, *Self-conjugate sets of mutually orthogonal latin squares*, Ph.D. Thesis, Emory University, 1981.

[4] Margaret Ann Francel, *Possible Orders for the Stabilizer of a Set of M.O.L.S, Discrete Mathematics*, 84 (1990), 119-134.

[5] C. C. Lindner, *Quasigroup identities and orthogonal arrays, Surveys in Combinatorics*, (1983), 77-105.

[6] C. C. Lindner, N. S. Mendelsohn, and S. R. Sun, *On the construction of Schroeder quasigroups, Discrete Math.*, 32 (1980), 281-289.

[7] C. C. Lindner and E. Mendelsohn, *On the conjugates of an* $n^2 \times 4$ *orthogonal array, Discrete Math.*, 20 (1977), 123-132.

[8] C. C. Lindner, R. C. Mullin and D. G. Hoffman, *The spectra for the conjugate invariant subgroups of n^2 orthogonal arrays*, *Canad. J. Math.*, 32 (1980), no. 5, 1126-1139.

[9] C. C. Lindner and D. Steedly, *On the number of conjugates of a quasigroup*, *Algebra Universalis*, 5 (1975), 191-196.

[10] Donald Passman. *Permutation Groups.* W. A. Benjamin, Inc, New York. 1968.