A class of latin squares derived from finite abelian groups

Anthony B. Evans

Abstract. We consider two classes of latin squares that are prolongations of Cayley tables of finite abelian groups. We will show that all squares in the first of these classes are confirmed bachelor squares, squares that have no orthogonal mate and contain at least one cell though which no transversal passes, while none of the squares in the second class can be included in any set of three mutually orthogonal latin squares.

Keywords: latin squares; bachelor squares; monogamous squares; prolongation

Classification: 05B15

1. Introduction

A *latin square* of order n is an $n \times n$ array with entries from a symbol set of order n such that each symbol appears exactly once in each row and exactly once in each column. Latin squares are closely related to quasigroups. A *quasigroup* is a set with binary operation $\circ$ such that for all $a, b, c \in Q$, the equation $a \circ x = c$ has a unique solution for x and the equation $y \circ b = c$ has a unique solution for y. A *loop* is a quasigroup with a two-sided identity, i.e. an element e for which $a \circ e = e \circ a = a$ for all a. A *group* is a loop in which the binary operation is associative. For a finite quasigroup $Q = \{q_1, \dots, q_n\}$, the *Cayley table* of Q is the $n \times n$ array with (i,j)th entry $q_i \circ q_j$. The Cayley table of a finite quasigroup is a latin square and any latin square can be regarded as the Cayley table of a quasigroup.

Two latin squares on the same symbol set are *orthogonal* if when superimposed each ordered pair of symbols appears exactly once. Orthogonal latin squares are closely related to orthogonal quasigroups. Two quasigroups on the same symbol set Q with binary operations $\circ$ and $\odot$ are *orthogonal* if, for each $a, b \in Q$, the system of equations $x \circ y = a$ and $x \odot y = b$ has a unique solution for x and y. Two quasigroups on the same set of symbols are orthogonal if and only if their Cayley tables are orthogonal.

A *transversal* of a latin square of order n is a set of n cells, exactly one from each row, exactly one from each column, in which each symbol appears exactly once. For a pair of orthogonal latin squares, if we pick any symbol a, the cells in the first square corresponding to cells in the second square with entry a form a transversal of the first square: similarly cells in the second square corresponding to cells in the first square with entry a form a transversal of the second square.

There exists a latin square orthogonal to a latin square L, an *orthogonal mate* of L, if and only if the cells of L can be partitioned by some set of transversals. A latin square with no orthogonal mate is called a *bachelor square* and, if it contains a cell that is not on any transversal, then it is called a *confirmed bachelor square*. A latin square that has an orthogonal mate but which cannot be contained in a set of three pairwise orthogonal latin squares is called a *monogamous square*. A *partial transversal* of *length* k is a set of k cells, at most one from each row, at most one from each column, in which each symbol appears at most once. A *near transversal* in a latin square of order n is a partial transversal of length $n-1$. The quasigroup equivalents of transversals and near transversals are complete mappings and near complete mappings. A *complete mapping* of a quasigroup Q is a bijection $\theta\colon Q \to Q$ for which the mapping $\eta\colon x \mapsto x\theta(x)$ is also a bijection $Q \to Q$. A quasigroup that admits a complete mapping is said to be *admissible*. A *near complete mapping* of a quasigroup Q is a bijection $\theta\colon Q \setminus \{a\} \to Q \setminus \{b\}$ for which the mapping $\eta\colon x \mapsto x\theta(x)$ is a bijection $Q \setminus \{a\} \to Q \setminus \{c\}$ for some $a, b, c \in Q$. There is a one-one correspondence between complete mappings of a quasigroup and transversals of its Cayley table, and between near complete mappings of a quasigroup and near transversals of its Cayley table.

In accordance with [5], a *prolongation* of a latin square of order n is a process by which this square is extended to a latin square of order $n+1$, equivalently a process by which a quasigroup of order n is extended to a quasigroup of order $n+1$. Three classes of prolongations are described in [5]. A prolongation of the Cayley table of $\mathbb{Z}_6$ is shown in Figure 1.

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

FIGURE 1. A prolongation of the Cayley table of $\mathbb{Z}_6$.

We will show that, for Cayley tables of finite abelian groups, one of the classes of prolongations consists of confirmed bachelor squares, and a second class of prolongations consists of latin squares that are either bachelor squares or monogamous squares.

2. The results

We are interested in the special case of prolongations of the Cayley tables of finite abelian groups. Let $G = \{g_1, \ldots, g_n\}$, $g_1 = 0$, be an additive abelian group and let $a \notin G$. For $\theta\colon \{g_2, \ldots, g_m\} \to \{g_2, \ldots, g_m\}$ a bijection, we define $Ext_\theta(G; a, w) = \{E_{ij}\}$ by

$$E_{ij} = \begin{cases} g_i + g_j & \text{if } i, j \in \{1, \ldots, n\},\ \theta(g_i) \neq g_j, \\ a & \text{if } i, j \in \{2, \ldots, n\},\ \theta(g_i) = g_j, \\ a & \text{if } i = 1 \text{ and } j = n+1, \\ a & \text{if } i = n+1 \text{ and } j = 1, \\ g_i + \theta(g_i) & \text{if } i \in \{2, \ldots, n\},\ j = n+1, \\ g_j + \theta^{-1}(g_j) & \text{if } j \in \{2, \ldots, n\},\ i = n+1, \\ w & \text{if } i = j = n+1. \end{cases}$$

Thus

$$Ext_\theta(G; a, w) = \left(\begin{array}{c|ccc|c} g_1 & g_2 & \cdots & g_n & a \\ \hline g_2 & & & & \\ \vdots & & A & & B \\ g_n & & & & \\ \hline a & & C & & w \end{array} \right),$$

where A is an $(n-1) \times (n-1)$ array with (i, j)th entry a if $\theta(g_{i+1}) = g_{j+1}$, and $g_{i+1} + g_{j+1}$ if $\theta(g_{i+1}) \neq g_{j+1}$, B is the $(n-1) \times 1$ array with ith entry $g_{i+1} + \theta(g_{i+1})$, and C the $1 \times (n-1)$ array with jth entry $g_{j+1} + \theta^{-1}(g_{j+1})$.

When $Ext_\theta(G; a, w)$ is a latin square, then it is a prolongation of the Cayley table of G. We will call it the *extension of G by θ*. The latin square shown in Figure 1 is the extension of $\mathbb{Z}_6$ by θ, where

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}.$$

We will show that, when $Ext_\theta(G; a, w)$ is a latin square, the properties of $Ext_\theta(G; a, w)$ depend on whether G is admissible or not. Finite abelian groups that are admissible were characterized by Paige [7] in 1947.

Theorem 1 (Paige,1947)**.** *A finite abelian group is admissible if and only if it does not contain a unique involution. A finite abelian group with a unique involution admits a near complete mapping.*

Proof: See [7]. $\square$

Just as whether a finite abelian group G is admissible or not depends on whether G has a unique involution or not, the sum of the elements of a finite abelian group G also depends on whether G has a unique involution or not.

Lemma 1. *For a finite abelian group G*

$$\sum_{g \in G} g = \begin{cases} 0 & \textit{if } G \textit{ does not have a unique involution,} \\ \delta & \textit{if } G \textit{ has a unique involution } \delta. \end{cases}$$

Proof: Routine; see [7] for instance. □

In Theorem 2 we will give two characterizations of those arrays $Ext_\theta(G;a,w)$ that are latin squares, one characterization for those finite abelian groups that do not have a unique involution, and one characterization for those finite abelian groups that do have a unique involution.

Theorem 2. *Let $G=\{g_1,\dots,g_n\}$, $g_1=0$, be an abelian group and let θ be a bijection $\{g_2,\dots,g_n\}\to\{g_2,\dots,g_n\}$.*

(1) *If G has a unique involution δ, then $Ext_\theta(G;a,w)$ is a latin square if and only if $w=\delta$, and θ is a near complete mapping of G, the mapping $\eta\colon g\mapsto g+\theta(g)$ being a bijection $G\setminus\{0\}\to G\setminus\{\delta\}$.*
(2) *If G does not have a unique involution, then $Ext_\theta(G;a,w)$ is a latin square if and only if $w=0$, and, by setting $\theta(0)=0$, θ becomes a complete mapping of G.*

Proof: Each row, with the possible exception of the last row, contains each symbol exactly once. Similarly, each column, with the possible exception of the last column, contains each symbol exactly once. Also, the symbols in the last row are the same as the symbols in the last column. As the symbols in the last column are $\{g_2+\theta(g_2),\dots,g_n+\theta(g_n)\}\cup\{a,w\}$, $Ext_\theta(G;a,w)$ is a latin square if and only if $G=\{g_2+\theta(g_2),\dots,g_n+\theta(g_n)\}\cup\{w\}$, if and only if $\eta\colon g\mapsto g+\theta(g)$ is a bijection $G\setminus\{0\}\to G\setminus\{w\}$.

If $G=\{g_2+\theta(g_2),\dots,g_n+\theta(g_n)\}\cup\{w\}$, then, as $g_1=0$ and $\theta(g_i)\neq 0$ for $i\in\{2,\dots,n\}$,

$$\sum_{g\in G} g=\sum_{i=2}^{n}(g_i+\theta(g_i))+w=2\sum_{g\in G} g+w.$$

It follows, by Lemma 1, that

$$w=-\sum_{g\in G} g=\begin{cases}0 & \text{if } G \text{ does not have a unique involution,}\\ \delta & \text{if } G \text{ has a unique involution } \delta.\end{cases}$$

The result follows. □

If G does not have a unique involution and $Ext_\theta(G;a,w)$ is a latin square, then this prolongation is a special case of a class of prolongations of admissible quasigroups constructed by Belyavskaya [1], [2], [3]. If G has a unique involution and $Ext_\theta(G;a,w)$ is a latin square, then this prolongation is a special case of a class of prolongations constructed by Deriyenko and Dudek [5] for quasigroups that are not admissible but admit near complete mappings.

To determine possible transversals through certain cells we need to use the Δ-lemma. Let $G=\{g_1,\dots,g_n\}$ be an abelian group and let L be a latin square of order n whose entries are the elements of G. If cell C of L is in row i and column j, and its entry is g_k, then the *deviation* of C is

$$dev(C) = g_k - (g_i + g_j).$$

Lemma 2 (The Δ-lemma)**.** *Let G be an abelian group of order n, let L be a latin square of order n whose entries are the elements of G, and let $C_1, \ldots, C_n$ be the cells of a transversal of L.*

(1) *If G has a* unique involution δ, *then*

$$\sum_{i=1}^{n} dev(C_i) = \delta.$$

(2) *Otherwise*

$$\sum_{i=1}^{n} dev(C_i) = 0.$$

Proof: By Lemma 1,

$$\sum_{i=1}^{n} dev(C_i) = -\sum_{g\in G} g = \begin{cases} 0 & \text{if } G \text{ does not have a unique involution,} \\ \delta & \text{if } G \text{ has a unique involution } \delta. \end{cases}$$

□

This simple lemma has proved very useful in determining the nonexistence of orthogonal mates and the nonexistence of transversals through certain cells (see the survey by Wanless [8]). One long standing problem was the existence problem for bachelor squares of order congruent to three modulo four. This was finally settled in 2006 by Wanless and Webb [9] using the Δ-lemma for cyclic groups. They showed the existence of confirmed bachelor squares of orders congruent to three modulo four. Independently Evans [6] proved the existence of bachelor squares of orders congruent to three modulo four using a variant of the Δ-lemma.

The Δ-lemma yields a proof that $Ext_\theta(G; a, w)$ is a confirmed bachelor square for any abelian group G, that does not have a unique involution, if $Ext_\theta(G; a, w)$ is a latin square.

Theorem 3. *If G does not have a unique involution and $Ext_\theta(G; a, w)$ is a latin square, then $Ext_\theta(G; a, w)$ is a confirmed bachelor square.*

Proof: Suppose that there is a transversal T through the $(n+1, 1)$th cell of $E = Ext_\theta(G; a, w)$. As there is an a in the $(n+1, 1)$th cell, T must contain exactly one cell from each column of the $n \times n$ partial latin square, E', obtained from E by deleting entries a, the last row of E, and the first column of E. We next permute the columns of E' to obtain the $n \times n$ partial latin square $F = \{F_{ij}\}$

where, for the nonempty cells,

$$F_{ij} = \begin{cases} g_i + g_j & \text{if } i \in \{1,\dots,n\},\ j \in \{2,\dots,n\},\ g_j \neq \theta(g_i), \\ g_i + \theta(g_i) & \text{if } i \in \{2,\dots,n\},\ j = 1. \end{cases}$$

Now, the deviations of the cells in F are 0 for nonempty cells not in the first column, and $\theta(g_i)$, $i = 2,\dots,n$, for nonempty cells in the first column. By the Δ-lemma, the deviations of the cells of F corresponding to the transversal T of E sum to 0, an impossibility as these cells consist of exactly one nonempty cell from each column of F and the deviations of all nonempty cells in the first column are nonzero, whereas the deviations of all nonempty cells in the other columns are zero. □

Wanless and Webb [9] proved the existence of confirmed bachelor squares for all orders greater than three. Theorem 3 yields new classes of confirmed bachelor squares. If $n \equiv 0 \pmod 4$ and $G = \mathbb{Z}_2 \times \mathbb{Z}_{n/2}$, then the extension of G by any complete mapping of G is a confirmed bachelor square of order $n+1$. More generally, if $n \equiv 0 \pmod 4$, and G is an abelian group that is not of the form $\mathbb{Z}_m \times H$, $|H|$ odd, then G is admissible by Theorem 1 and the extension of G by any complete mapping of G will be a confirmed bachelor square of order $n+1$. If n is odd, G is an abelian group of order n, and $\iota\colon G \to G$ is the identity mapping, then the extension of G by ι is a confirmed bachelor square of order $n+1$. More generally, if n is odd and G is an abelian group of order n, then the extension of G by any complete mapping of G is a confirmed bachelor square of order $n+1$. Thus, Theorem 1 yields new classes of confirmed bachelor squares of all orders congruent to either 0, 1, or 2 modulo 4. Theorem 1 cannot yield confirmed bachelor squares of orders congruent to 3 modulo 4 as any abelian group of order congruent to 2 modulo 4 has a unique involution.

For abelian groups with unique involutions the situation is not as clear cut.

Theorem 4. *If, for a finite abelian group G with a unique involution, $Ext_\theta(G; a, w)$ is a latin square, then $Ext_\theta(G; a, w)$ is either a bachelor square or a monogamous square.*

Proof: Let δ be the unique involution in G and let $E = Ext_\theta(G; a, w)$ be a latin square. By Theorem 2, $w = \delta$, θ is a near complete mapping of G, and the mapping $\eta\colon g \mapsto g + \theta(g)$ is a bijection $G \setminus \{0\} \to G \setminus \{\delta\}$. As in the proof of Theorem 3, let T be a transversal through the $(n+1, 1)$th cell of E. Let E' and F be as in the proof of Theorem 3.

As in the proof of Theorem 3, the deviations of the cells in F are 0 for nonempty cells not in the first column, and $\theta(g_i)$, $i = 2,\dots,n$, for nonempty cells in the first column. By the Δ-lemma, the deviations of the cells of F corresponding to the transversal T of E sum to δ. It follows that the cells of F corresponding to cells of T must contain the unique cell in the first column of F of deviation δ. This cell is in the kth row, where $\theta(g_k) = \delta$. Thus, any transversal of E through the $(n+1, 1)$th cell must pass through the $(k, n+1)$th cell. It follows that, if

M is any latin square orthogonal to E, then the entries of M in the $(n+1,1)$th and $(k,n+1)$th cells are the same and, hence, two latin squares orthogonal to E cannot be orthogonal to each other. □

In 2011 Danziger, Wanless, and Webb [4] constructed monogamous squares for all orders $n > 6$ except when n is of the form $2p$, p prime, $p \geq 11$. Theorem 4 should yield either new classes of monogamous squares and/or new classes of bachelor squares. In what follows we will give necessary conditions for $E = Ext_\theta(G, a, w)$ to be a monogamous square when G is a finite abelian group with a unique involution and E is a latin square.

Lemma 3. *If G is a finite abelian group with a unique involution δ and $E = Ext_\theta(G; a, w)$ is a latin square, then*

(1) *any transversal through the $(n+1,1)$th cell of E must pass through the $(i,n+1)$th cell for which $\theta(g_i) = \delta$;*
(2) *any transversal through the $(1,n+1)$th cell of E must pass through the $(n+1,j)$th cell for which $\theta^{-1}(g_j) = \delta$;*
(3) *any transversal through the $(n+1,n+1)$th cell of E must pass through the (i,j)th cell, $i,j \neq 1,n+1$, for which $g_j = \theta(g_i)$ and $g_i + g_j = 0$;*
(4) *if a transversal passes through the (s,t)th cell of E, $s \neq 1, n+1$, $g_t = \theta(g_s)$, the $(i,n+1)$th cell of E, $i \neq 1, n+1$, and the $(n+1,j)$th cell, $j \neq 1, n+1$, then*

$$\theta(g_i) + \theta^{-1}(g_j) = g_s + g_t + \delta.$$

Proof: (1) See the proof of Theorem 4.

(2) Similar to the proof of (1).

(3) Let T be a transversal through the $(n+1,n+1)$th cell of E. T must also pass through a cell with entry a: let this be the (s,t)th cell. Thus $g_t = \theta(g_s)$ and $s,t \in \{2,\ldots,n\}$. Form a partial latin square F by removing all as, replacing the sth row by the $(n+1)$th row and the tth column by the $(n+1)$th column, and then deleting the last row and column. All cells of F with nonzero deviations are in the sth row or the tth column and the deviation of the (s,t)th cell is $\delta - g_s - g_t$. As the transversal of F corresponding to T must pass through the (s,t)th cell and no other cell with nonzero deviation, $g_s + g_t = 0$ by Lemma 2.

(4) Let T be a transversal through the (s,t)th cell of E, $s \neq 1, n+1$, $g_t = \theta(g_s)$, the $(i,n+1)$th cell of E, $i \neq 1, n+1$, and the $(n+1,j)$th cell, $j \neq 1, n+1$. Form a partial latin square F from E by removing all as, replacing the sth row by the $(n+1)$th row and the tth column by the $(n+1)$th column, and then deleting the last row and column. All cells of F with nonzero deviations are in the sth row or the tth column. The deviation of the (s,j)th cell of F is $\theta^{-1}(g_j) - g_s$ if $j \neq t$ and the deviation of the (i,t)th cell of F is $\theta(g_i) - g_t$. By Lemma 2, $\theta^{-1}(g_j) - g_s + \theta(g_i) - g_t = \delta$ from which the result follows. □

Theorem 5. *If G is a finite abelian group with a unique involution δ and $E = Ext_\theta(G; a, w)$ is a monogamous square, then there exists a bijection $\alpha\colon G \setminus$*

$\{0,\delta\} \to G \setminus \{0,\delta\}$ for which the mapping $\beta\colon g \mapsto g+\alpha(g)$ is also a bijection $G \setminus \{0,\delta\} \to G \setminus \{0,\delta\}$.

Proof: Assume that E is a monogamous square. Then the cells of E can be partitioned by a set of transversals $T_1,\dots,T_{n+1}$. Let T_k be a transversal that does not pass through the $(1,n+1)$th cell of E, or the $(n+1,1)$th cell of E, or the $(n+1,n+1)$th cell of E. For some $i,j,s,t \in \{2,\dots,n\}$, $\theta(g_i) \neq \delta$, $\theta^{-1}(g_j) \neq \delta$, $\theta(g_s) = g_t$, T_k passes through the $(i,n+1)$th cell of E, the $(n+1,j)$th cell of E, and the (s,t)th cell of E, and $\theta(g_i)+\theta^{-1}(g_j) = g_s+g_t+\delta$. Set $g=\theta(g_i)$, $\phi(g_i)=g_j$, and $\alpha(g)=\theta^{-1}\phi\theta^{-1}(g)$. As T_k runs through the transversals in $\{T_1,\dots,T_{n+1}\}$ that do not pass through the $(1,n+1)$th cell of E, or the $(n+1,1)$th cell of E, or the $(n+1,n+1)$th cell of E, g runs through the elements of $G \setminus \{0,\delta\}$, $\alpha(g)$ runs through the elements of $G \setminus \{0,\delta\}$, and $g+\alpha(g)$ runs through the elements of $G \setminus \{0,\delta\}$. Hence α is a bijection $G \setminus \{0,\delta\} \to G \setminus \{0,\delta\}$ for which the mapping $g \mapsto g+\alpha(g)$ is also a bijection $G \setminus \{0,\delta\} \to G \setminus \{0,\delta\}$. □

As corollaries to Theorem 5 we see that for small abelian groups $Ext_\theta(G,a,w)$ must be a bachelor square if it is a latin square.

Corollary 1. *If $E = Ext_\theta(\mathbb{Z}_4;a,w)$ is a latin square, then E is a bachelor square.*

Proof: For any mapping $\alpha\colon \{1,3\} \to \{1,3\}$, $g+\alpha(g) \in \{0,2\}$ for $g \in \{1,3\}$. It follows that the conditions of Theorem 5 cannot be satisfied and, hence, that E is a bachelor square. □

Corollary 2. *If $E = Ext_\theta(\mathbb{Z}_6;a,w)$ is a latin square, then E is a bachelor square.*

Proof: Let $\alpha\colon \{1,2,4,5\} \to \{1,2,4,5\}$ be a bijection. For the mapping $\beta\colon g \mapsto g+\alpha(g)$ to be a bijection $\{1,2,4,5\} \to \{1,2,4,5\}$, α must map $\{1,4\}$ to $\{1,4\}$ and $\{2,5\}$ to $\{2,5\}$. But then, either $\alpha(1)=1$ and $\alpha(4)=4$ or $\alpha(1)=4$ and $\alpha(4)=1$. In the first case $\beta(1)=\beta(4)=2$ and in the second case $\beta(1)=\beta(4)=5$, a contradiction. It follows that the conditions of Theorem 5 cannot be satisfied and, hence, that E is a bachelor square. □

For $\mathbb{Z}_8$ the conditions of Theorem 5 can be satisfied. If

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 5 & 6 & 7 \\ 1 & 7 & 3 & 2 & 5 & 6 \end{pmatrix}, \text{ then } \beta = \begin{pmatrix} 1 & 2 & 3 & 5 & 6 & 7 \\ 2 & 1 & 6 & 7 & 3 & 5 \end{pmatrix}.$$

Two questions remain. For which finite abelian groups with unique involutions are the conditions of Theorem 5 satisfied? When does Theorem 4 yield bachelor squares and when does it yield monogamous squares?

Acknowledgments. I would like to thank Fedir Sokhatsky for referring me to the work on prolongations by Belyavskaya, Deriyenko, and Dudek.

References

[1] Belyavskaya G.B., *Generalized extension of quasigroups* (Russian), Mat. Issled. **5** (1970), 28–48.

[2] Belyavskaya G.B., *Contraction of quasigroups. I.* (Russian), Bul. Akad. Stiince RSS Moldoven (1970), 6–12.

[3] Belyavskaya G.B., *Contraction of quasigroups. II.* (Russian), Bul. Akad. Stiince RSS Moldoven (1970), 3–17.

[4] Danziger P., Wanless I.M., Webb B.S., *Monogamous latin squares*, J. Combin. Theory Ser. A **118** (2011), 796–807.

[5] Deriyenko I.I., Dudek W.A., *On prolongation of quasigroups*, Quasigroups and Related Systems **16** (2008), 187–198.

[6] Evans A.B., *Latin squares without orthogonal mates*, Des. Codes Crypt. **40** (2006), 121–130.

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

[8] Wanless I.M., *Transversals in latin squares: a survey*, Surveys in combinatorics 2011, pp. 403–437, London Math. Soc. Lecture Note Ser., **392**, Cambridge Univ. Press, Cambridge, 2011.

[9] Wanless I.M., Webb B.S., *The existence of latin squares without orthogonal mates*, Des. Codes Cryptogr. **40** (2006), 131–135.

Wright State University

(*Received* October 30, 2013)