On parity vectors of Latin squares

D. M. Donovan[1], M. J. Grannell[2], T. S. Griggs[2] and J. G. Lefevre[1*]

1. Centre for Discrete Mathematics and Computing
University of Queensland
St Lucia 4072, Australia

2. Department of Mathematics and Statistics
The Open University
Walton Hall
Milton Keynes MK7 6AA, UK

Abstract

The parity vectors of two Latin squares of the same side n provide a necessary condition for the two squares to be biembeddable in an orientable surface. We investigate constraints on the parity vector of a Latin square resulting from structural properties of the square, and show how the parity vector of a direct product may be obtained from the parity vectors of the constituent factors. Parity vectors for Cayley tables of all Abelian groups, some non-Abelian groups, Steiner quasigroups and Steiner loops are determined. Finally, we give a lower bound on the number of main classes of Latin squares of side n that admit no self-embeddings.

Keywords: Latin square, Orientable surface, Biembedding, Parity vector, Group, Steiner quasigroup, Steiner loop.

AMS classifications: 05B15, 05C10.

[*]Donovan and Lefevre supported by grants DP0664030 and LX0453416

1 Introduction

A triangular embedding of a complete regular tripartite graph $K_{n,n,n}$ in a surface is face two-colourable if and only if the surface is orientable [5]. In this case, the faces of each colour class can be regarded as the triples of a *transversal design* $TD(3,n)$, of order n and block size 3. Such a design comprises a triple $(V, \mathcal{G}, \mathcal{B})$, where V is a $3n$-element set (the points), $\mathcal{G}$ is a partition of V into three parts (the groups) each of cardinality n, and $\mathcal{B}$ is a collection of 3-element subsets (the blocks) of V such that each 2-element subset of V is either contained in exactly one block of $\mathcal{B}$, or in exactly one group of $\mathcal{G}$, but not both. Two $TD(3,n)$s , $(V, \{G_1, G_2, G_3\}, \mathcal{B})$ and $(V', \{G'_1, G'_2, G'_3\}, \mathcal{B}')$ are said to be *isomorphic* if, for some permutation π of $\{1,2,3\}$, there exist bijections $\alpha_i : G_i \to G'_{\pi(i)}$, $i = 1,2,3$, that map blocks of $\mathcal{B}$ to blocks of $\mathcal{B}'$. A Latin square of side n determines a $TD(3,n)$ by assigning the row labels, the column labels, and the entries as the three groups of the design. Two Latin squares are said to be in the same *main class* if the corresponding transversal designs are isomorphic. A question that naturally arises is: which pairs of (main classes of) Latin squares may be biembedded?

This question seems to be difficult. On the existence side, recursive constructions are given in [3, 6, 7]. Of particular interest are biembeddings of Latin squares which are the Cayley tables of groups and other algebraic structures. An infinite class of biembeddings of Latin squares representing the Cayley tables of cyclic groups of order n is known for all $n \geq 2$. This is the family of regular biembeddings constructed using a voltage graph based on a dipole with n parallel edges embedded in a sphere [12], or alternatively directly from the Latin squares defined by $C_n(i,j) = i + j \pmod{n}$, and $C'_n(i,j) = i + j - 1 \pmod{n}$ [5]. A regular biembedding of a Latin square of side n has the greatest possible symmetry, with full automorphism group of order $12n^2$, the maximum possible value. Recently the present authors [3] constructed another family of biembeddings of the Latin squares representing the Cayley tables of cyclic groups of order $2n$, $n \geq 3$, also with a high degree of symmetry. Enumeration results for biembeddings of Latin squares of side 3 to 7 are given in [5] and for groups of order 8 in [8]. More recently still, in [9] it has been shown that with the single exception of the group C_2^2, the Cayley table of each Abelian group appears in some biembedding.

In the context of non-existence results, some small Latin squares do not appear in any biembeddings [5]. In [11], the present authors introduced the concept of the parity vector of a main class of Latin squares. Using this concept, it was shown that for $n \geq 2$, there is no biembedding of two Latin squares both lying in the same main class as the Latin square obtained from the Cayley table of the Abelian 2-group C_2^n.

The purpose of the current paper is two-fold. First we calculate the parity vectors of the Latin squares which are the Cayley tables of Abelian groups, as well as various classes of non-Abelian groups. We also deal with Steiner quasigroups and loops. Secondly we use our calculations to show that there exists a set H of main classes of Latin squares of even side n such that each class admits no self-embeddings, that is to say no biembeddings of any pair of Latin squares belonging to that main class, and for which

$$|H| \geq \begin{cases} n^{\frac{n^2}{4}(1-o(1))} & \text{if } n \equiv 0, 4 \text{ or } 8 \pmod{12}, \\ n^{\frac{n^2}{6}(1-o(1))} & \text{if } n \equiv 2 \text{ or } 10 \pmod{12}, \\ n^{\frac{n^2}{36}(1-o(1))} & \text{if } n \equiv 6 \pmod{12}. \end{cases}$$

Before doing this we give some definitions and then briefly recall the relevant material on Latin squares and parity vectors (taken from [11]).

A Latin square may be thought of as a set of ordered triples, where the triple (i, j, k) represents the occurrence of entry k in cell (i, j) of the Latin square. A Latin square L, of side n, is said to be *symmetric* if whenever $(i, j, k) \in L$ then $(j, i, k) \in L$. A Latin square L is said to be *idempotent* if, for all $i \in \{1, \ldots, n\}$, $(i, i, i) \in L$ and *unipotent* if, for some $k \in \{1, \ldots, n\}$ and all $i \in \{1, \ldots, n\}$, $(i, i, k) \in L$. A Latin square L, of even side $2n$, is said to be *half-idempotent* if, for all $1 \leq i \leq n$, $(i, i, 2i), (n+i, n+i, 2i) \in L$. The direct product of two Latin squares A and B is given by $A \times B = \{((i, i'), (j, j'), (k, k')) \mid (i, j, k) \in A \text{ and } (i', j', k') \in B\}$. It will be useful to distinguish between the row labels, column labels and entry symbols of a Latin square. So, given a Latin square L of side n, we denote the set of entries by $E = \{e_1, \ldots, e_n\}$, the set of rows labels by $R = \{r_1, \ldots, r_n\}$ and the set of column labels by $C = \{c_1, \ldots, c_n\}$. We take arbitrary but fixed orderings on R, C and E; we will use $(r_1, \ldots, r_n)$, $(c_1, \ldots, c_n)$ and $(e_1, \ldots, e_n)$.

For each row r_i, column c_j and entry e_k of L, define bijections $\beta^L_{r,i} : C \to E$ with $\beta^L_{r,i}(c_j) = e_k$, $\beta^L_{c,j} : E \to R$ with $\beta^L_{c,j}(e_k) = r_i$, and $\beta^L_{e,k} : R \to C$, with $\beta^L_{e,k}(r_i) = c_j$ if and only if $(r_i, c_j, e_k) \in L$. Define permutations $\gamma^L_{r,i} : E \to E$, $\gamma^L_{c,j} : R \to R$ and $\gamma^L_{e,k} : C \to C$ by $\gamma^L_{r,i}(e_j) = \beta^L_{r,i}(c_j)$, $\gamma^L_{c,j}(r_k) = \beta^L_{c,j}(e_k)$ and $\gamma^L_{e,k}(c_i) = \beta^L_{e,k}(r_i)$, respectively. We make the following definition.

Definition 1.1 *For a Latin square L of side n, let*

$$\begin{aligned} x_L &= |\{i \in N \mid \gamma^L_{r,i} \text{ has odd parity}\}|, \\ y_L &= |\{j \in N \mid \gamma^L_{c,j} \text{ has odd parity}\}|, \\ z_L &= |\{k \in N \mid \gamma^L_{e,k} \text{ has odd parity}\}|. \end{aligned}$$

Then the vector (x_L, y_L, z_L) will be called the parity vector *of L.*

We remark that the above definition refers to the Latin square L, as it is presented. If (x, y, z) is the parity vector of L, the parity vector of any Latin square in the same main class as L is one of (x, y, z), $(x, n-y, n-z)$, $(n-x, y, n-z)$ or $(n-x, n-y, z)$, or some reordering of one of these. Of the resulting 24 parity vectors, there are at most four distinct ones that have a common minimal first entry. Of these, there is precisely one distinct vector that has a minimal second entry. We call this vector the *main class parity vector* and denote it by $[p, q, r]$, using square brackets to distinguish it from the original parity vectors. If $[p, q, r]$ is a main class parity vector, then $p \leq q \leq \min\{r, n-r\}$.

The main theorem of [11] is:

Theorem 1.1 [11] *Let A and B be two Latin squares of side n, with main class parity vectors $[x_A, y_A, z_A]$ and $[x_B, y_B, z_B]$ respectively. If there exist Latin squares A' and B' which are in the same main class as A and B respectively and which can be biembedded, then*

- $[x_A, y_A, z_A] = [x_B, y_B, z_B]$ *if n is odd;*
- $[x_A, y_A, z_A] = [x_B, y_B, n - z_B]$ *if n is even.*

2 Parity vectors

We begin this section with some general results about parity vectors of Latin squares. We go on to show how the main class parity vector of the direct product $A \times B$ of two Latin squares can be calculated from the main class parity vectors of the constituent squares A and B.

Lemma 2.1 *Let A and B be Latin squares of the same side n with parity vectors (x_A, y_A, z_A) and (x_B, y_B, z_B) respectively. Then*

$$x_A + y_A + z_A \equiv x_B + y_B + z_B \pmod 2.$$

Proof. Define bijections $\rho_r, \rho_c, \rho_e : A \to B$ by

$$\begin{aligned}
\rho_r(r_i, c_j, e_k) &= (\beta^B_{c,j}(e_k), c_j, e_k), \\
\rho_c(r_i, c_j, e_k) &= (r_i, \beta^B_{e,k}(r_i), e_k), \\
\rho_e(r_i, c_j, e_k) &= (r_i, c_j, \beta^B_{r,i}(c_j)),
\end{aligned}$$

for all $(r_i, c_j, e_k) \in A$. Then

$$\begin{aligned}
\rho_r^{-1}(r_i, c_j, e_k) &= ((\beta^A_{e,k})^{-1}(c_j), c_j, e_k), \\
\rho_c^{-1}(r_i, c_j, e_k) &= (r_i, (\beta^A_{r,i})^{-1}(e_k), e_k), \\
\rho_e^{-1}(r_i, c_j, e_k) &= (r_i, c_j, (\beta^A_{c,j})^{-1}(r_i)),
\end{aligned}$$

for all $(r_i, c_j, e_k) \in B$. To see this note that, for example, if $(r_i, c_j, e_k) \in A$ then $r_i = \beta^A_{c,j}(e_k)$. Thus ρ_r maps $(\beta^A_{c,j}(e_k), c_j, e_k)$ to $(\beta^B_{c,j}(e_k), c_j, e_k)$, and so ρ_r^{-1} maps $(\beta^B_{c,j}(e_k), c_j, e_k)$ to $(\beta^A_{c,j}(e_k), c_j, e_k)$. But by the definition of the bijections $\beta^A_{\alpha,i}$, we have $\beta^A_{c,j}(e_k) = (\beta^A_{e,k})^{-1}(c_j)$.

We form the compositions

$$\begin{aligned}
\rho_c^{-1}\rho_e(r_i, c_j, e_k) &= (r_i, (\beta^A_{r,i})^{-1}\beta^B_{r,i}(c_j), \beta^B_{r,i}(c_j)), \\
\rho_e^{-1}\rho_r(r_i, c_j, e_k) &= (\beta^B_{c,j}(e_k), c_j, (\beta^A_{c,j})^{-1}\beta^B_{c,j}(e_k)), \\
\rho_r^{-1}\rho_c(r_i, c_j, e_k) &= ((\beta^A_{e,k})^{-1}\beta^B_{e,k}(r_i), \beta^B_{e,k}(r_i), e_k),
\end{aligned}$$

each of which is a permutation on A. If we consider the action of $\rho_c^{-1}\rho_e$ on a fixed row i of A, we have a permutation of that row which is isomorphic to $(\beta^A_{r,i})^{-1}\beta^B_{r,i}$. Thus this row permutation has even parity if and only if $\gamma^A_{r,i}$ and $\gamma^B_{r,i}$ have the same parity. Now the entire permutation $\rho_c^{-1}\rho_e$ is simply the composition of each of these row permutations, so it will have the same parity as $x_A + x_B$. Likewise $\rho_e^{-1}\rho_r$ and $\rho_r^{-1}\rho_c$ will have the same parity as $y_A + y_B$ and $z_A + z_B$ respectively. But $(\rho_c^{-1}\rho_e)(\rho_e^{-1}\rho_r)(\rho_r^{-1}\rho_c)$ is the identity. Hence $x_A + x_B + y_A + y_B + z_A + z_B$ is even. □

Lemma 2.2 *Let L be a symmetric Latin square of side n with parity vector (x, y, z). Then the following must hold.*

(1) $x = y$.

(2) If L is idempotent then n must be odd and

$$z = \begin{cases} 0, & \textit{if } n \equiv 1 \pmod 4, \\ n, & \textit{if } n \equiv 3 \pmod 4. \end{cases}$$

(3) If L is half-idempotent then n must be even and $z = n/2$.

(4) If L is unipotent then n must be even and

$$z = \begin{cases} 0, & \textit{if } n \equiv 0 \pmod 4, \\ n-1, & \textit{if } n \equiv 2 \pmod 4. \end{cases}$$

Proof. Since L is symmetric, for each i, row i has the same parity as column i (that is, $\gamma_{r,i}^L$ and $\gamma_{c,i}^L$ have the same parity), and therefore $x = y$, which proves (1). If $(i,j,k) \in L$ then by symmetry $(j,i,k) \in L$; hence $\gamma_{e,k}^L(c_i) = c_j$ and $\gamma_{e,k}^L(c_j) = c_i$, implying that the column permutation $\gamma_{e,k}^L$ consists entirely of fixed points and involutions, for each k. A fixed point in $\gamma_{e,k}^L$ corresponds to an occurrence of entry k on the main diagonal. If we subtract the number of such occurrences from n and then divide by two, we obtain the number of involutions in $\gamma_{e,k}^L$, and the parity of this number is the parity of $\gamma_{e,k}^L$. If L is idempotent then every permutation $\gamma_{e,k}^L$ contains precisely one fixed point. Hence n is odd and the parity of $\gamma_{e,k}^L$ is even if $n \equiv 1 \pmod 4$ and odd if $n \equiv 3 \pmod 4$. If L is half-idempotent then, by definition, n is even, half of the permutations $\gamma_{e,k}^L$ consist of two fixed points and $(n-2)/2$ involutions, and the other half consist of $n/2$ involutions. If L is unipotent then one permutation $\gamma_{e,k}^L$ is the identity and all the others consist of $n/2$ involutions. Hence n must be even and the parity of $\gamma_{e,k}^L$ must be even if $n \equiv 0 \pmod 4$ and odd if $n \equiv 2 \pmod 4$. Results (2), (3) and (4) follow. □

Lemma 2.3 *Let $[x,y,z]$ be the main class parity vector of a Latin square of side n. Then $x+y+z$ is even if $n \equiv 0$ or $1 \pmod 4$, and odd if $n \equiv 2$ or $3 \pmod 4$.*

Proof. For all odd n there exists a symmetric, idempotent Latin square of side n, and for all even n there exists a symmetric, half-idempotent Latin square of side n. Thus by Lemma 2.2 for all $n \equiv 0$ or $1 \pmod 4$ there exists a Latin square of side n, with parity vector (x,y,z), where $x+y+z$ is even and for all $n \equiv 2$ or $3 \pmod 4$ there exists a Latin square of side n, with parity vector (x,y,z), where $x+y+z$ is odd. Therefore, by Lemma 2.1, the result holds for every Latin square of side n. □

Lemma 2.4 *Let A and B be Latin squares of side a and b respectively, with parity vectors (x_A, y_A, z_A) and (x_B, y_B, z_B) respectively. Then the parity vector of $A \times B$ is*

$$\begin{cases} (0,0,0), & a \text{ even}, \quad b \text{ even}, \\ (bx_A, by_A, bz_A), & a \text{ even}, \quad b \text{ odd}, \\ (ax_B, ay_B, az_B), & a \text{ odd}, \quad b \text{ even}, \\ (bx_A + ax_B - 2x_Ax_B, & \\ \quad by_A + ay_B - 2y_Ay_B, & \\ \quad bz_A + az_B - 2z_Az_B), & a \text{ odd}, \quad b \text{ odd}. \end{cases}$$

Proof. In order for the parity vectors to be well defined we must have arbitrary but fixed orderings of the rows, column and entry sets of A and B.

Take $(r_1, r_2, \cdots r_a)$, $(c_1, c_2, \cdots c_a)$, and $(e_1, e_2, \cdots e_a)$ for A, and $(r'_1, r'_2, \cdots r'_b)$, $(c'_1, c'_2, \cdots c'_b)$, and $(e'_1, e'_2, \cdots e'_b)$ for B. Then

$$A \times B = \left\{((r_i, r'_p), (c_j, c'_q), (e_k, e'_s)) \mid (r_i, c_j, e_k) \in A,\ (r'_p, c'_q, e'_s) \in B\right\}.$$

Using the orderings in A and B, we can order the rows, columns and entries of $A \times B$; take $((r_1, r'_1), (r_1, r'_2), \cdots, (r_1, r'_b), (r_2, r'_1), \cdots, (r_a, r'_{b-1}), (r_a, r_b))$ for the rows, and similarly for the columns and entries. Thus the β and γ functions are well defined on $A \times B$.

From the definition of $A \times B$ we have

$$\beta^{A\times B}_{(r_i,r'_p)}(c_j, c'_q) = (\beta^A_{r,i}(c_j), \beta^B_{r',p}(c'_q)),$$

hence

$$\gamma^{A\times B}_{(r_i,r'_p)}(e_j, e'_q) = (\gamma^A_{r,i}(e_j), \gamma^B_{r',p}(e'_q)).$$

Thus we see that the permutation corresponding to row (r_i, r'_p) of $A \times B$ consists of the composition of b copies of $\gamma^A_{r,i}$ and a copies of $\gamma^B_{r',p}$.

If a and b are both even, then every row of $A \times B$ will have even parity, so $x_{A\times B} = 0$. If a is even and b is odd, then $\gamma^{A\times B}_{(r_i,r'_p)}$ will have the same parity as $\gamma^A_{r,i}$, thus $x_{A\times B} = bx_A$; similarly if a is odd and b is even, $x_{A\times B} = ax_B$. Finally, if a and b are both odd, then $\gamma^{A\times B}_{(r_i,r'_p)}$ will be odd if $\gamma^A_{r,i}$ is odd and $\gamma^B_{r,p'}$ is even, or vice-versa; thus

$$x_{A\times B} = x_A(b - x_B) + (a - x_A)x_B = bx_A + ax_B - 2x_Ax_B.$$

The proofs for $y_{A\times B}$ and $z_{A\times B}$ are similar. □

3 Steiner quasigroups and Steiner loops

First we recall the definitions of a Steiner quasigroup and a Steiner loop. A *Steiner triple system* of order n is a pair $(V, \mathcal{B})$ where V is an n-element set (the points) and $\mathcal{B}$ is a collection of 3-element subsets (the blocks) of V such that each 2-element subset of V is contained in exactly one block of $\mathcal{B}$. It is well known that a Steiner triple system of order n (briefly STS(n)) exists if and only if $n \equiv 1$ or 3 (mod 6) [10]. Given an STS(n), $(V, \mathcal{B})$, we may define a binary operation $*$ on V by $x * x = x$, $x \in V$ and $x * y = z$ if $\{x, y, z\} \in \mathcal{B}$. Then $(V, *)$ is a *Steiner quasigroup* or *squag* of order n. Alternatively define on $V \cup \{\infty\}$ an operation $\circ$ by $x \circ x = \infty$, $\infty \circ x = x \circ \infty = x$, $x \in V \cup \{\infty\}$ and $x \circ y = z$ if $\{x, y, z\} \in \mathcal{B}$. Then $(V \cup \{\infty\}, \circ)$ is a *Steiner loop* or *sloop* of order $n + 1$.

Theorem 3.1 *Let $(V, \mathcal{B})$ be an STS(n) and let $(V, *)$ be the associated Steiner quasigroup. Further, let L be the Latin square formed from the Cayley table of $(V, *)$. Then the main class parity vector of L is*

$$\begin{array}{rl} [0,0,n] & \textit{if} \quad n \equiv 3 \textit{ or } 7 \pmod{12}, \\ [0,0,0] & \textit{if} \quad n \equiv 1 \textit{ or } 9 \pmod{12}. \end{array}$$

Proof. Let (x, y, z) be the parity vector of L. Since a Steiner quasigroup is symmetric and idempotent, Lemma 2.2 implies that $x = y$ and that $z = n$ if $n \equiv 3 \pmod 4$ and $z = 0$ if $n \equiv 1 \pmod 4$. Let $\{a, b, c\} \in \mathcal{B}$, then $a*b = c$ and $a * c = b$, further $\gamma^L_{r,a}(e_b) = e_c$ and $\gamma^L_{r,a}(e_c) = e_b$. Hence $\gamma^L_{r,a}$ has even parity if $(n-1)/2$ is even and odd parity otherwise. Thus $x = y = 0$ if $n \equiv 1 \pmod 4$, and $x = y = n$ if $n \equiv 3 \pmod 4$. Consequently the parity vector of L is given by $(0, 0, 0)$ if $n \equiv 1 \pmod 4$, and by (n, n, n) if $n \equiv 3 \pmod 4$. After noting that when $n \equiv 3 \pmod 4$ the main class parity vector is given by $[n - x, n - y, z]$, the result follows. □

Theorem 3.2 *Let $(V, \mathcal{B})$ be an STS$(n-1)$ and let $(V \cup \{\infty\}, \circ)$ be the associated Steiner loop. Further, let L be the Latin square formed from the Cayley table of $(V \cup \{\infty\}, \circ)$. Then the main class parity vector of L is*

$$\begin{array}{rl} [0,0,0] & \textit{if} \quad n \equiv 4 \textit{ or } 8 \pmod{12}, \\ [1,1,n-1] & \textit{if} \quad n \equiv 2 \textit{ or } 10 \pmod{12}. \end{array}$$

Proof. Let (x, y, z) be the parity vector of L. We note that L is a symmetric unipotent Latin square. Hence Lemma 2.2 implies that $x = y$ and that $z = 0$ if $n \equiv 0 \pmod 4$ and $z = n - 1$ if $n \equiv 2 \pmod 4$. The bijection $\gamma^L_{r,\infty}$ is the identity permutation. Further, $\gamma^L_{r,a}(e_\infty) = e_a$ and $\gamma^L_{r,a}(e_a) = e_\infty$, while if $\{a, b, c\} \in \mathcal{B}$, then $\gamma^L_{r,a}(e_b) = e_c$ and $\gamma^L_{r,a}(e_c) = e_b$. Hence $\gamma^L_{r,a}$ has even parity if $n/2$ is even and odd parity otherwise. Thus $x = y = 0$ if $n \equiv 0 \pmod 4$, and $x = y = n - 1$ if $n \equiv 2 \pmod 4$. When $n \equiv 2 \pmod 4$ the main class parity vector is given by $[n - x, n - y, z]$ and the result follows. □

4 Groups

We begin this section with a general result concerning the parity vector of the Cayley table of any group, and then use this result to determine the main class parity vector of the Latin square formed from the Cayley table of the cyclic group and, ultimately, of any Abelian group. But first let G be any group of order n. If $g \in G$ is an element of order m, then the *index* of g is defined to be the integer n/m.

Lemma 4.1 *Let A be a Latin square formed from the Cayley table of a group G of order n. Let $H = \{g \in G \mid g$ has even order and odd index$\}$. Let $K = \{g \in G \mid g$ has order 3 or greater$\}$. Then $|K|$ is even, and*

$$(x_A, y_A, z_A) = \begin{cases} (|H|, |H|, |H|), & \text{if } |K|/2 \text{ is even}, \\ (|H|, |H|, n - |H|), & \text{if } |K|/2 \text{ is odd}. \end{cases}$$

In particular,

$$(x_A, y_A, z_A) = \begin{cases} (0, 0, 0), & \text{if } n \equiv 1 \pmod 4, \\ (0, 0, n), & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

Proof. Let g be any element of G, with order m and index n/m. Then $\gamma^A_{r,g}(e_x) = e_{gx}$, $\gamma^A_{c,g}(r_x) = r_{xg^{-1}}$ and $\gamma^A_{e,g}(c_x) = c_{x^{-1}g}$. Thus, for $\alpha \in \{r, c\}$, the permutation $\gamma^A_{\alpha,g}$ can be written as n/m cycles of length m, with one of the cycles being $(g, g^2, g^3, \ldots, g^m)$ if $\alpha = r$, or $(g^m, g^{m-1}, g^{m-2}, \ldots, g)$ if $\alpha = c$. Thus the parity of $\gamma^A_{\alpha,g}$ is odd if and only if m is even and n/m is odd; that is, if and only if $g \in H$. If the order of G is odd, then the order of each element in G is odd and so H is empty.

This leaves only the calculation of z_A. Note that $\gamma^A_{e,g} = \mathcal{P}_g \circ \mathcal{Q}$, where $\mathcal{Q}(c_x) = c_{x^{-1}}$ and $\mathcal{P}_g(c_x) = c_{xg}$. By the reasoning above, $\mathcal{P}_g$ will have odd parity if and only if $g \in H$. The permutation $\mathcal{Q}$, which is independent of g, consists of one or more fixed points, and cycles of length 2 involving pairs of elements from K. It follows that $|K|$ will be even, and the parity of $\mathcal{Q}$ will be the parity of $|K|/2$. We have the parity of $\mathcal{P}_g$, $\mathcal{Q}$ and hence $\gamma^A_{e,g}(c_x)$, and the result follows. □

Note that if G is any group of even order whose Sylow 2-subgroups are not cyclic, then $|H| = 0$. To see this, suppose that G has order $n = 2^s t$ where $s, t \geq 1$ and t is odd. Then for $g \in G$ to have even order and odd index, it must have order $2^s r$ where $r \mid t$. But then g^r has order 2^s and so the subgroup $\langle g^r \rangle$ of order 2^s is cyclic, a contradiction. Hence $H = \emptyset$.

Using the preceding lemma, the main class parity vector for any cyclic group can be determined.

Theorem 4.1 *For any $n \in \mathbb{N}$, let C_n denote the Latin square formed from the Cayley table of the cyclic group of order n. Then the main class parity vector of C_n is:*

$$[x_{C_n}, y_{C_n}, z_{C_n}] = \begin{cases} [\frac{n}{2}, \frac{n}{2}, \frac{n}{2}], & \text{if } n \text{ is even}, \\ [0, 0, 0], & \text{if } n \equiv 1 \pmod 4, \\ [0, 0, n], & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

Proof. If n is odd then the result follows directly from the previous lemma. If n is even, let $n = 2m$, $m \geq 1$, and suppose that the cyclic group is generated by an element g. Then the elements g^{2i-1}, $1 \leq i \leq m$, have even order and index $\gcd(2i-1, n)$ which is odd. On the other hand the elements g^{2i}, $0 \leq i \leq m-1$, have index $\gcd(2i, n)$ which is even. Hence $|H| = m = n/2$, and the result follows. □

We can now determine the main class parity vector for any Abelian group.

Theorem 4.2 *Let A be a Latin square formed from the Cayley table of an Abelian group G of order n. Then the main class parity vector of A is*

$$[x_A, y_A, z_A] = \begin{cases} [0,0,0], & \text{if } n \equiv 1 \pmod 4, \\ [0,0,n], & \text{if } n \equiv 3 \pmod 4, \\ [\frac{n}{2}, \frac{n}{2}, \frac{n}{2}], & \text{if } n \equiv 2 \pmod 4, \\ [0,0,0], & \text{if } n \equiv 0 \pmod 4 \text{ and } G \text{ is isomorphic} \\ & \text{to the product of two groups of even order,} \\ [\frac{n}{2}, \frac{n}{2}, \frac{n}{2}], & \text{if } n \equiv 0 \pmod 4 \text{ and } G \text{ is not isomorphic} \\ & \text{to the product of two groups of even order.} \end{cases}$$

Proof. By the Fundamental Theorem of finite Abelian groups, G may be regarded as the direct product of cyclic groups. The result follows from Theorem 4.1 and Lemma 2.4. The result also follows directly from Lemma 4.1 for n odd. □

Using Lemma 4.1 we may also classify the main class parity vectors for the dihedral groups and the generalized quaternion groups.

Lemma 4.2 *Let $n = 2m$ and let A be a Latin square formed from the Cayley table of the dihedral group D_m of order n. Then the parity vector of A is*

$$[x_A, y_A, z_A] = \begin{cases} [0,0,2m], & \text{if } m \equiv 0 \pmod 4, \\ [m,m,m], & \text{if } m \equiv 1 \pmod 4, \\ [0,0,0], & \text{if } m \equiv 2 \pmod 4, \\ [m,m,m], & \text{if } m \equiv 3 \pmod 4. \end{cases}$$

Proof. The group presentation for the dihedral group D_m can be written as $\langle \sigma, \tau \mid \sigma^m = e, \tau^2 = e, \tau\sigma\tau = \sigma^{-1} \rangle$, where e is the identity element. We assume that the ordering of the rows, columns and entries of D_m is given by $(\sigma^0, \sigma^1, \ldots, \sigma^{m-1}, \tau, \sigma^1\tau, \ldots, \sigma^{m-1}\tau)$.

Let H and K be defined as in the statement of Lemma 4.1. Elements of the form σ^i, $0 \leq i \leq m-1$, have order $m/\gcd(i, m)$, and hence have even index. Thus none of these elements are in H, but all elements of this form are in K except for e and, if m is even, $\sigma^{m/2}$. The elements of the form $\sigma^i\tau$, $0 \le i \le m-1$, have order 2 and thus index m. Hence none of these elements are in K, and if m is even then none of these elements occur in H either; however, if m is odd then all of these elements occur in H.

It follows that if m is even then $|K| = m-2$ and $|H| = 0$, while if m is odd then $|K| = m-1$ and $|H| = m$. The result follows from Lemma 4.1. □

Lemma 4.3 *Let $n = 2^m$, $m \ge 3$ and let A be a Latin square formed from the Cayley table of the generalized quaternion group Q_m of order n. Then the main class parity vector of A is*

$$[0, 0, n].$$

Proof. The group presentation for the generalized quaternion group Q_m can be written as $\langle \sigma, \tau \mid \sigma^{n/2} = e, \tau^2 = \sigma^{n/4}, \tau\sigma\tau^{-1} = \sigma^{-1}\rangle$, where e is the identity element. All elements of the group have even index, and all elements have order greater than 2 except for the identity and $\sigma^{n/4}$. The result follows directly from Lemma 4.1. □

5 Main classes admitting no self-embeddings

We now briefly investigate those main classes of Latin squares which admit no self-embeddings. In particular, we establish a lower bound on the number of such main classes of Latin squares of side n for every even n.

Lemma 5.1 *Let A and B be Latin squares of even side m. Then there is no biembedding of two Latin squares from the main classes of $A \times C_2$ and $B \times C_2$.*

Proof. This result follows from Theorem 1.1 and Lemma 2.4. □

Lemma 5.2 *Let A and B be Latin squares of odd side m, and let C and D be Latin squares of side 6 from the main classes 6.3, 6.4 or 6.10, using the enumeration in [1]. Then there is no biembedding of two Latin squares from the main classes of $A \times C$ and $B \times D$.*

Proof. By Table 3 of [11], C and D will have main class parity vectors $[0, 0, 5]$, $[1, 2, 4]$ or $[1, 1, 1]$. Therefore, by Lemma 2.4, $A \times C$ and $B \times D$ will have main class parity vectors $[0, 0, 5m]$, $[m, 2m, 4m]$ or $[m, m, m]$. Since $A \times C$ and $B \times D$ have side $6m$, the result follows from Theorem 1.1. □

Lemma 5.3 *Let A and B be Latin squares formed from the Cayley tables of Steiner loops of order n. Then there is no biembedding of two Latin squares from the main classes of A and B.*

Proof. This result follows from Theorem 1.1 and Theorem 3.2. $\square$

Using known results on the number of distinct Latin squares of side n and the number of distinct Steiner triple systems of order n, the following estimate may be obtained.

Theorem 5.1 *Let n be a positive even integer. Then there exists a set H_n of Latin squares of side n, such that no two squares from H_n may be biembedded together and for which*

$$|H_n| \geq \begin{cases} n^{\frac{n^2}{4}(1-o(1))} & \text{if } n \equiv 0 \pmod 4, \\ n^{\frac{n^2}{36}(1-o(1))} & \text{if } n \equiv 0 \pmod 6, \\ n^{\frac{n^2}{6}(1-o(1))} & \text{if } n \equiv 2 \text{ or } 4 \pmod 6. \end{cases}$$

Proof. We deal first with the case $n \equiv 0 \pmod 4$. The number $L(m)$ of distinct Latin squares of side m satisfies $L(m) \geq (m!)^{2m} m^{-m^2}$ ([1], page 141). Using the estimate $m! > (2\pi m)^{\frac{1}{2}} m^m e^{-m}$ gives $L(m) > m^{m^2(1-o(1))}$. Now take m even and apply Lemma 5.1 to obtain $L(m)$ distinct Latin squares of side $n = 2m$, no two of which can be biembedded together. Hence for $n \equiv 0 \pmod 4$,

$$|H_n| \geq \left(\frac{n}{2}\right)^{\frac{n^2}{4}(1-o(1))} = n^{\frac{n^2}{4}(1-o(1))}.$$

The case $n \equiv 0 \pmod 6$ is dealt with similarly using Lemma 5.2. Finally, the case $n \equiv 2$ or $4 \pmod 6$ follows from Lemma 5.3 together with the estimate $N(m) = m^{\frac{m^2}{6}(1-o(1))}$ for the number $N(m)$ of distinct Steiner triple systems of order m ([2], page 70 et seq.). $\square$

We remark that the cardinality of H_n should be compared with the total number of distinct Latin squares of side n, namely $n^{n^2(1-o(1))}$.

Corollary 5.1 *Let n be a positive even integer, and let $f(n)$ be the number of main classes of Latin squares of side n which admit no self-embeddings. Then*

$$f(n) \geq \begin{cases} n^{\frac{n^2}{4}(1-o(1))} & \text{if } n \equiv 0, 4 \text{ or } 8 \pmod{12}, \\ n^{\frac{n^2}{6}(1-o(1))} & \text{if } n \equiv 2 \text{ or } 10 \pmod{12}, \\ n^{\frac{n^2}{36}(1-o(1))} & \text{if } n \equiv 6 \pmod{12}. \end{cases}$$

Proof. The cardinality of a main class of Latin squares of side n is at most $3!(n!)^3$ and for any positive constant a, $n^{an^2}/3!(n!)^3 = n^{an^2(1-o(1))}$. Applying Theorem 5.1 and writing the results modulo 12 gives the stated inequalities.

$\square$

In conclusion, we note that the number of nonisomorphic biembeddings of Latin squares of side n is known to be at least $n^{\frac{n^2}{144}(1-o(1))}$ for an infinite set of values of n [4]. An obvious upper bound for this quantity is $n^{2n^2(1-o(1))}$, obtained by considering the number of pairs of Latin squares of side n. For self-embeddings, the corresponding obvious upper bound is $n^{n^2(1-o(1))}$, but no comparable lower bound is currently known.

References

[1] C. J. Colbourn and J. H. Dinitz (editors), "The CRC Handbook of Combinatorial Designs", 2nd Edition, CRC Press, Boca Raton (ISBN: 9781584885061), 2006.

[2] C. J. Colbourn and A. Rosa, "Triple Systems", Oxford University Press, New York (ISBN: 9780198535768), 1999.

[3] D. M. Donovan, A. Drápal, M. J. Grannell, T. S. Griggs and J. G. Lefevre, *Quarter-regular biembeddings of Latin squares*, Discrete Math. **310** (2010), 692–699.

[4] D. M. Donovan, M. J. Grannell, T. S. Griggs, J. G. Lefevre and T. McCourt, *Self-embeddings of cyclic and projective Steiner quasigroups*, J. Combin. Des., to appear.

[5] M. J. Grannell, T. S. Griggs and M. Knor, *Biembeddings of Latin squares and Hamiltonian decompositions*, Glasgow Math. J. **46** (2004), 443–457.

[6] M. J. Grannell, T. S. Griggs and M. Knor, *On biembeddings of Latin squares*, Electron. J. Combin. **16** (2009), R106, 12pp.

[7] M. J. Grannell, T. S. Griggs and J. Širáň, *Recursive constructions for triangulations*, J. Graph Theory **39** (2002), 87-107.

[8] M. J. Grannell, T. S. Griggs and M. Knor, *Biembeddings of Latin squares of side 8*, Quasigroups Related Systems **15** (2007), 273–278.

[9] M. J. Grannell and M. Knor, *Biembeddings of Abelian groups*, J. Combin. Des. **18** (2010), 71–83.

[10] T. P. Kirkman, *On a problem in combinations*, Cambridge and Dublin Math. J. **2** (1847), 191-204.

[11] J. G. Lefevre, D. M. Donovan, M. J. Grannell and T. S. Griggs, *A constraint on the biembedding of Latin squares*, European J. Combin. **30** (2009), 380–386.

[12] S. Stahl and A. T. White, *Genus embeddings for some complete tripartite graphs*, Discrete Math. **14** (1976), 279-296.