The Chromatic Number of Finite Group Cayley Tables

Luis Goddyn Kevin Halasz

Department of Mathematics
Simon Fraser University
Burnaby, Canada

{goddyn,khalasz}@sfu.ca

E. S. Mahmoodian

Department of Mathematical Sciences
Sharif University of Technology
Tehran, I.R. Iran

emahmood@sharif.edu

Submitted: May 18, 2018; Accepted: Jan 6, 2019; Published: Mar 8, 2019

Abstract

The chromatic number of a latin square L, denoted $\chi(L)$, is the minimum number of partial transversals needed to cover all of its cells. It has been conjectured that every latin square satisfies $\chi(L) \leqslant |L| + 2$. If true, this would resolve a long-standing conjecture—commonly attributed to Brualdi—that every latin square has a partial transversal of size $|L| - 1$. Restricting our attention to Cayley tables of finite groups, we prove two results. First, we resolve the chromatic number question for Cayley tables of finite Abelian groups: the Cayley table of an Abelian group G has chromatic number $|G|$ or $|G| + 2$, with the latter case occurring if and only if G has nontrivial cyclic Sylow 2-subgroups. Second, we give an upper bound for the chromatic number of Cayley tables of arbitrary finite groups. For $|G| \geqslant 3$, this improves the best-known general upper bound from $2|G|$ to $\frac{3}{2}|G|$, while yielding an even stronger result in infinitely many cases.

Mathematics Subject Classifications: 05B15, 05C15, 05E30

1 Introduction and preliminaries

Let n be a positive integer, let $[n] := \{0, 1, 2, \ldots, n-1\}$, and let L be a **latin square** of order n, which we define as an $n \times n$ array in which each row and each column is a permutation of some set of n symbols indexed by $[n]$. We define a **partial transversal** of L as a collection of cells which intersects each row, each column, and each symbol class at most once. A **transversal** of L is a partial transversal of size n and a **near transversal** is a partial transversal of size $n - 1$. It is well known that L possesses an orthogonal mate if and only if it can be partitioned into transversals. But when L does not have an orthogonal mate, can we still efficiently partition its cells into partial transversals?

$L =$

0	1	2
1	2	0
2	0	1

$\Gamma(L) =$

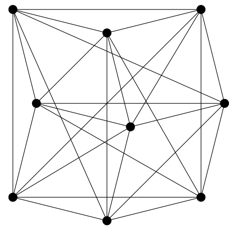

Figure 1: A latin square L and its associated latin square graph $\Gamma(L)$.

This question can be restated in terms of graph coloring. Associated with every latin square L is a strongly regular graph $\Gamma(L)$ defined on vertex set $\{(r, c, L_{r,c}) : r, c \in [n]\}$ with $(r_1, c_1, s_1) \sim (r_2, c_2, s_2)$ if and only if one of $r_1 = r_2$, $c_1 = c_2$, or $s_1 = s_2$ holds (e.g. see Figure 1). It is straightforward to check that partial transversals of L correspond to independent sets in $\Gamma(L)$. Thus, the graph chromatic number $\chi(\Gamma(L))$ is the minimum number of partial transversals needed to cover all of the cells in L.

We refer to a partition of a latin square L into k partial transversals as a (proper) ***k*-coloring** of L. The **chromatic number** of L, denoted $\chi(L)$, is the minimum k for which L has a k-coloring. As a partial transversal has size at most n, $\chi(L) \geqslant n$. On the other hand, we may bound $\chi(L)$ from above by applying Brooks' theorem to the graph $\Gamma(L)$.

Proposition 1. *Let L be a latin square of order $n \geqslant 3$. Then*

$$n \leqslant \chi(L) \leqslant 3n - 3,$$

with equality holding for the lower bound if and only if L possesses an orthogonal mate.

It is widely believed that the upper bound in Proposition 1 is far from tight. Indeed, a recent conjecture due to Cavenagh [2] proposes that the chromatic number of a latin square can differ from its order by at most 2.

Conjecture 2. Let L be a latin square of order n. Then

$$\chi(L) \leqslant \begin{cases} n+1 & \text{if } n \text{ is odd,} \\ n+2 & \text{if } n \text{ is even.} \end{cases}$$

Latin squares for which this conjecture is tight have been given by Euler [5] in the even case and by Wanless and Webb [16] in the odd case. If true, Conjecture 2 is likely difficult to prove, as it implies a pair of long-standing conjectures concerning the existence of large partial transversals in latin squares. These conjectures are attributed to Brualdi [3, 14] and Ryser [13], respectively.

Conjecture 3. Let L be a latin square of order n. Then (1) L possesses a near transversal and (2) if n is odd then L possesses a transversal.

To see that Conjecture 2 implies Conjecture 3.1, suppose there exists a latin square L in which every partial transversal has size at most $n - 2$. Any set of $n + 2$ partial transversals in L could cover at most $(n+2)(n-2) = n^2 - 4$ of L's n^2 cells. Thus, L has no proper $(n+2)$-coloring. A similar argument shows that Conjecture 2 implies Conjecture 3.2.

There is a growing body of evidence for Conjecture 2. As noted in [1], the conjecture has been verified for $n \leqslant 8$. It is also known to hold in an asymptotic sense. Using the canonical representation of latin squares as 3-uniform hypergraphs, the following is an immediate corollary of a powerful theorem due to Pippenger and Spencer [12].

Theorem 4. *As $n \to \infty$, every latin square L of order n satisfies $\chi(L) = n + o(n)$.*

Furthermore, there are several families for which Conjecture 2 is known to hold. Cavenagh and Kuhl [2] showed that Conjecture 2 holds for circulant latin squares (i.e. Cayley tables of cyclic groups) when $n \not\equiv 6 \pmod{12}$. This result was confirmed and extended in [1], where Conjecture 2 was established for circulant latin squares of every order. The present paper continues the work towards resolving Conjecture 2 in the special case where L is the Cayley table of a finite group. Parts of this work have already appeared in the M.Sc. thesis of the second author [8], which was supervised by the first author.

Observe that the chromatic number of $\Gamma := \Gamma(L)$ is not affected by relabelling the rows, columns, or symbol classes of L, nor is it affected by applying a fixed permutation to each of the triples $(r, c, s) \in V(\Gamma)$. Thus, $\chi(L)$ is a *main class invariant*, and it makes sense in this context to speak of *the* Cayley table of a group G, which we denote by $L(G)$. In a slight abuse of notation, we write $\chi(G)$ for the chromatic number of $L(G)$ and $\Gamma(G)$ for the latin square graph $\Gamma(L(G))$.

Given a group G, let $Syl_2(G)$ denote the isomorphism class of its Sylow 2-subgroups. The groups for which $\chi(G) = n$ were recently characterized by Bray, Evans, and Wilcox [7, 17], resolving a 50 year old conjecture due to Hall and Paige [9].

Theorem 5. *Let G be a group of order n. Then the following are equivalent:*

1. *$\chi(G) = n$,*
2. *$\chi(G) \leqslant n + 1$,*
3. *$L(G)$ has a transversal,*
4. *$Syl_2(G)$ is either trivial or non-cyclic.*

In light of this, verifying that Conjecture 2 is true for finite group Cayley tables amounts to showing that every group with nontrivial, cyclic Sylow 2-subgroups has an $(n+2)$-coloring. In Section 2 we give such a construction under the additional assumption that G is Abelian, yielding our first main result.

Theorem 6. *Let G be an Abelian group of order n. Then*

$$\chi(G) = \begin{cases} n & \text{if } Syl_2(G) \text{ is either trivial or non-cyclic,} \\ n+2 & \text{otherwise.} \end{cases} \tag{1}$$

In Section 3 we turn to the case of general (i.e. not necessarily Abelian) groups. We begin by showing that $\chi(G)$ is submultiplicative, thereby generalizing a classical result due to Hall and Paige. This allows us to establish an upper bound for $\chi(G)$ which depends only upon the largest power of 2 dividing $|G|$: every group G of order $n = 2^l m \geqslant 3$ satisfies

$$\chi(G) \leqslant n + 2m. \tag{2}$$

Previously, the best-known general upper bound for $\chi(G)$ was due to Wanless; it follows directly from his work in [15] that every finite group satisfies $\chi(G) \leqslant 2n$. This bound is improved upon by (2) except when $n \equiv 2 \pmod 4$. Dealing directly with this final case, we obtain our second main result.

Theorem 7. *Let G be a group of order $n \geqslant 3$. Then*

$$\chi(G) \leqslant \frac{3}{2}n.$$

The condition $n \geqslant 3$ is necessary because $\Gamma(\mathbb{Z}_2) \cong K_4$. It is worth noting that, by Theorem 4, the bound in Theorem 7 is not asymptotically tight. Indeed, it is likely far from tight even for relatively small fixed values of n; if Conjecture 2 is true, then (1) holds for every finite group.

2 The chromatic number of Abelian groups

Let $G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ be a finite Abelian group of order n. We say that $G = \{g_0, g_1, \ldots, g_{n-1}\}$ is ordered **lexicographically** if $g_i = (i_1, i_2, \ldots, i_k)$ precedes $g_j = (j_1, j_2, \ldots, j_k)$ (i.e. $i < j$) if and only if there is some $l \in \{1, 2, \ldots, k\}$ for which (under the natural order of $\mathbb{Z}_{m_l}$) $i_l \prec j_l$ and $i_m = j_m$ for every positive integer $m < l$. In the statement of the following technical lemma, indices are expressed modulo n.

Lemma 8. *Let $G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} = \{g_0, g_1, \ldots, g_{n-1}\}$ be a lexicographically ordered Abelian group of odd order n. If $\gcd(s+1, n) = 1$ for some positive integer s, then the map $\phi : G \to G$ given by $\phi(g_i) = g_{i+c} + g_{si+d}$ is injective for every $c, d \in [n]$.*

Proof. Suppose $G = \mathbb{Z}_n$ is cyclic and consider $g, h \in G$ such that $\phi(g) = \phi(h)$. We may treat g and h as integers in the set $[n]$, in which case the group operation is simply addition modulo n, and

$$(s+1)g + c + d \equiv \phi(g) \equiv \phi(h) \equiv (s+1)h + c + d \pmod{n}.$$

We then have $(s+1)g \equiv (s+1)h \pmod{n}$. But $\gcd(s+1, n) = 1$ tells us that $s+1$ is a generator of $G = \mathbb{Z}_n$, and therefore $g \equiv h \pmod{n}$, as desired.

Now, we may assume $G = \mathbb{Z}_{n_1} \times H$, where $H = \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ is a nontrivial Abelian group of odd order $m := n/n_1$. If $H = \{h_0, h_1, \ldots, h_{m-1}\}$ is ordered lexicographically, then for every $i \in [n]$

$$g_i = \left(\left\lfloor \frac{i}{m} \right\rfloor, h_{i \ (\mathrm{mod}\ m)} \right)$$

and, defining the map $\psi : H \to H$ by $\psi(h_i) = h_{i+c \pmod m} + h_{si+d \pmod m}$, we have

$$\phi(g_i) = \left(\left\lfloor \frac{i+c}{m} \right\rfloor + \left\lfloor \frac{si+d}{m} \right\rfloor \pmod{n_1}, \; \psi\left(h_{i \pmod m}\right) \right).$$

Consider $i, j \in [n]$ such that $\phi(g_i) = \phi(g_j)$. In this case we have $\psi(h_{i \pmod m}) = \psi(h_{j \pmod m})$. It then follows by induction on $|G|$ that $i \equiv j \pmod m$. Thus, there is some $r \in [n_1]$ such that $j = i + rm$, and

$$\begin{aligned} \left\lfloor \frac{i+c}{m} \right\rfloor + \left\lfloor \frac{si+d}{m} \right\rfloor &\equiv \left\lfloor \frac{i+rm+c}{m} \right\rfloor + \left\lfloor \frac{si+srm+d}{m} \right\rfloor \\ &\equiv \left\lfloor \frac{i+c}{m} \right\rfloor + r + \left\lfloor \frac{si+d}{m} \right\rfloor + sr \pmod{n_1}. \end{aligned}$$

We then have $(s+1)r \equiv 0 \pmod{n_1}$. But $r \in [n_1]$ and $\gcd(s+1, n_1) = 1$, forcing us to conclude that $r = 0$, in which case $i = j$. □

The **Möbius ladder** of order $2n$, denoted M_n, is the cubic graph formed from a cycle of length $2n$ by adding n edges, one between each pair of vertices at distance n in the initial cycle. We refer to this initial cycle as the *rim* of M_n, and refer to the edges between opposite vertices in the rim as *rungs*. A pair $\{u, v\} \subseteq V(M_n)$ is called **near-antipodal** if the shortest path from u to v along the rim of M_n has length $n-1$ (see Figure 2). There is a strong sense in which Möbius ladders are "nearly" bipartite.

Proposition 9. *For $n \geqslant 3$, let $M_n = (V, E)$ be the Möbius ladder of order $2n$, and let $\{u, v\} \in V$ be a near-antipodal pair. Then the induced subgraph $M_n[V \setminus \{u, v\}]$ is bipartite.*

Proof. Observe that the greedily coloring of $M_n[V \setminus \{u, v\}]$ with vertices ordered clockwise around the rim of M_n uses exactly 2 colors. □

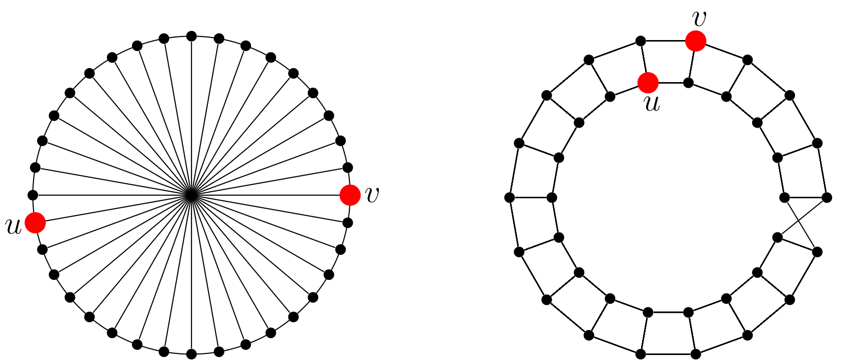

Figure 2: Two drawings of the Möbius ladder M_{18} with a near-antipodal pair of vertices highlighted.

Let $G = \{g_0, g_1, \ldots, g_{n-1}\}$ be a group satisfying $\chi(G) > n$. We construct an $(n+2)$-coloring of $\Gamma = \Gamma(G)$ in two steps. First, we show that Γ can be partitioned into $\frac{n}{2}$ induced copies of M_n. Second, we find a bipartite induced subgraph $\Lambda \subseteq \Gamma$ which contains a near-antipodal pair from each copy of M_n. By Proposition 9, we then have a partition of Γ into $\frac{n}{2} + 1$ bipartite induced subgraphs. Using a disjoint pair of colors for each of these subgraphs, we obtain an $(n+2)$-coloring of Γ.

Before formally presenting our construction, we introduce some notation which will be utilized both here and in Section 3. Letting $L = L(G)$ and fixing an integer $d \in [n]$, we define the **dth right diagonal of L** as the set

$$T_d^L := \{L_{i,i+d} : i \in [n]\},$$

where indices are expressed modulo n. When it is clear which latin square we are discussing, we drop the superscript and simply write T_d. We also define the maps $R, C : L \to [n]$ and $S : L \to G$ by

$$R(L_{ij}) = i, C(L_{ij}) = j, \text{ and } S(L_{ij}) = g_i g_j. \tag{3}$$

These maps send a cell of L to its row index, its column index, and its symbol, respectively. We then extend these functions to sets of cells. For $A \subseteq L$, let $R(A) = \{R(a) : a \in A\}$ be the multiset containing the row-index of every cell in A (counted with multiplicity), and define $C(A)$ and $S(A)$ similarly.

Theorem 10. *Let G be an Abelian group of order n. If $Syl_2(G)$ is cyclic and nontrivial then*

$$\chi(G) \leqslant n + 2.$$

Proof. Because $Syl_2(G)$ is nontrivial, n is even and the constant

$$q := n/2 \tag{4}$$

is well-defined. We may assume $n \geqslant 4$, as $\Gamma(\mathbb{Z}_2) \cong K_4$ has chromatic number $4 = 2 + 2$. Moreover, letting $t := |Syl_2(G)|$, there is some integer $l \geqslant 1$ such that $t = 2^l$. By the fundamental theorem of finite Abelian groups $G = \mathbb{Z}_t \times \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$, where $m := \prod_{i=1}^{k} m_k$ is odd. Letting $H := \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$, we order $H = \{h_0, h_1, \ldots, h_{m-1}\}$ lexicographically. We then impose an ordering on G by setting

$$g_i := \left(i \pmod{t}, h_{i \pmod{m}}\right) \text{ for every } i \in [n]. \tag{5}$$

Arrange the rows and columns of $L = L(G)$ according to this ordering and, for every $i \in [q]$, define the set

$$D_i := T_{2i} \cup T_{2i+1}.$$

Letting $\Gamma := \Gamma(G)$, recall that $V = V(\Gamma)$ corresponds to the set of cells in L, and that two cells are adjacent if they lie in the same row, they lie in the same column, or they contain the same symbol. By definition, two cells in a latin square can satisfy at most one of these conditions. We therefore have a natural partition of $E = E(\Gamma)$ into the sets E_R, E_C, and E_S, corresponding to "row-edges," "column-edges," and "symbol-edges," respectively.

Claim 11. *The induced subgraph $\Gamma_i := \Gamma[D_i]$ is isomorphic to the Möbius ladder M_n for every $i \in [q]$.*

Expressing indices modulo n, let $A_j := L_{j,j+2i}$ and $B_j := L_{j,j+2i+1}$ for every $j \in [n]$. It is not hard to see that the only row-edges in Γ_i are $\{A_jB_j : j \in [n]\}$ (see Figure 3). Similarly, the only column-edges in Γ_i are $\{A_{j+1}B_j : j \in [n]\}$. Thus, the vertex sequence

$$A_0, B_0, A_1, B_1, \ldots, A_{n-1}, B_{n-1} \tag{6}$$

corresponds to a Hamilton cycle in Γ_i that uses all of the edges in $E(\Gamma_i) \cap (E_R \cup E_C)$. To prove the claim, it is left to show that $E(\Gamma_i) \cap E_S$ contains exactly n edges, each of which connects opposite vertices (i.e. vertices at distance n) in the cycle given by (6).

Given an integer z, let $\overline{z}$ be the corresponding residue modulo t. It follows from (5) that, for every $j \in [n]$,

$$S(A_j) = \left(\overline{2j+2i}, h_j + h_{j+2i \ (\mathrm{mod}\ m)}\right) \text{ and } S(B_j) = \left(\overline{2j+2i+1}, h_j + h_{j+2i+1 \ (\mathrm{mod}\ m)}\right). \tag{7}$$

Because t is even, for every $j, k \in [n]$ the first coordinates of $S(A_j)$ and $S(B_k)$ have different values modulo 2. Thus, E_S contains no edges of the form A_jB_k.

Fixing an arbitrary $j \in [n]$, we want to find all nonzero $x \in [n]$ for which $S(A_j) = S(A_{j+x})$. For all such x, it follows from (7) that $2j + 2i \equiv 2j + 2x + 2i \pmod{t}$. Recalling that $t = 2^l$, we may conclude that x is divisible by 2^{l-1}. On the other hand, (7) also implies $h_j + h_{j+2i} = h_{j+x} + h_{j+x+2i}$ (where indices are here expressed modulo m). Applying Lemma 8 with $c = 0$, $d = 2i$, and $s = 1$, we have $j \equiv j + x \pmod{m}$, so that x is divisible by m. But, as m is odd, the only nonzero integer in $[n]$ which is divisible by both m and 2^{l-1} is $q = m2^{l-1} = n/2$. Thus, for every $j \in [n]$, we have $S(A_j) = S(A_{j+x})$ if and only if $x = q$.

We now see that each A_j is incident to exactly one edge in $E_S \cap E(\Gamma_i)$: the edge connecting it to the opposite vertex in the cycle given by (6). A similar argument shows that, for every $j \in [n]$, the only edge in $E_S \cap E(\Gamma_i)$ incident to B_j is B_jB_{j+q}. This establishes the claim.

We complete the proof (of Theorem 10) by finding a pair of independent sets $X, Y \subseteq V$ such that $\Gamma_i' := \Gamma[D_i \setminus (X \cup Y)]$ is bipartite for every $i \in [q]$. Given such X and Y, we can define $D_i' := D_i \setminus (X \cup Y)$ for every $i \in [q]$ and properly $(n+2)$-color Γ using a distinct pair of colors for each of the $\frac{n}{2} + 1$ sets $D_0', D_1', \ldots, D_{q-1}', X \cup Y$.

Towards a definition of X and Y, let

$$p := \left\lceil \frac{n}{4} \right\rceil \text{ and } (q_0, q_1) := \begin{cases} (q, q+1) & \text{if } q \equiv 0 \pmod{3}, \\ (q-1, q) & \text{otherwise.} \end{cases} \tag{8}$$

Keeping in mind that indices are here considered modulo n, for each $i \in [p]$ define

$$x_i := L_{i,\,3i},\ x_i' := L_{q_0+i,\,q_1+3i},\ \text{and } X := \{x_i, x_i' : i \in [p]\}. \tag{9}$$

Similarly, for every $j \in [q-p]$, define

$$y_j := L_{j,\,3j+2p},\ y_j' := L_{q_0+j,\,q_1+3j+2p},\ \text{and } Y := \{y_j, y_j' : j \in [q-p]\}. \tag{10}$$

$\widetilde{\mathbf{000}}$	**101**	002	110	011	112	020	121	022	100	*001*	102	010	111	012	120	021	122
101	**002**	**100**	$\widetilde{011}$	112	010	121	022	120	001	102	000	111	*012*	110	021	122	020
002	100	**001**	**112**	010	111	$\widetilde{022}$	120	021	102	000	101	012	110	011	122	*020*	121
110	*011*	112	**020**	**121**	022	100	001	102	$\widetilde{010}$	111	012	120	021	122	000	101	002
011	112	010	121	**022**	**120**	001	102	000	111	012	110	$\widetilde{021}$	122	020	101	002	100
112	010	111	022	120	**021**	**102**	000	101	012	110	011	122	020	121	002	100	001
020	121	022	100	001	102	**010**	**111**	012	120	021	122	000	101	002	110	011	112
121	022	120	001	102	000	111	**012**	**110**	021	122	020	101	002	100	011	112	010
022	120	021	102	000	101	012	110	**011**	**122**	020	121	002	100	001	112	010	111
100	001	*102*	010	111	012	120	021	122	**000**	$\widetilde{\mathbf{101}}$	002	110	011	112	020	121	022
001	102	000	111	012	*110*	021	122	020	101	**002**	**100**	011	$\widetilde{112}$	010	121	022	120
102	000	101	012	110	011	122	020	*121*	002	100	**001**	**112**	010	111	022	$\widetilde{120}$	021
010	$\widetilde{111}$	012	120	021	122	000	101	002	110	011	*112*	**020**	**121**	022	100	001	102
111	012	110	021	$\widetilde{122}$	020	101	002	100	011	112	010	121	**022**	**120**	001	102	000
012	110	011	122	020	121	002	100	001	112	010	111	022	120	**021**	**102**	000	101
120	021	122	000	101	002	110	011	112	020	121	022	100	001	102	**010**	**111**	012
021	122	020	101	002	100	011	112	010	121	022	120	001	102	000	111	**012**	**110**
122	020	121	002	100	001	112	010	111	022	120	021	102	000	101	012	110	**011**

Figure 3: A Cayley table of $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ with elements of $\mathbf{D_0}$, $\widetilde{X}$, and Y highlighted.

Figure 3 exhibits D_0, X and Y in highlighted fonts for the group $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Observe that $x_i \in T_{2i} \subseteq D_i$ and $x'_i \in T_{2i+1} \subseteq D_i$ for each $i \in [p]$. Similarly, $y_j, y'_j \in D_{p+j}$ for each $j \in [q-p]$.

Recall that the edges on the rim of Γ_i are exactly $E(\Gamma_i) \cap (E_R \cup E_C)$. It follows from the definition of D_i that the shortest path from x_i to x'_i along the rim of Γ_i has length $n-1$. Similarly, the shortest path from y_j to y'_j along the rim of Γ_{p+j} has length $n-1$. Thus, (x_i, x'_i) and (y_j, y'_j) are near-antipodal pairs for every $i, j \in [p]$. Proposition 9 then implies that Γ'_i is bipartite for every $i \in [q]$.

It remains to show that X and Y are independent sets in Γ. We begin by showing that there are no row-edges and no column-edges between cells in X. Recalling the definitions in (3) and (9), we see that the multiset of row-indices of cells in X is

$$R(X) = [p] \cup \{q_0 + i \,:\, i \in [p]\}.$$

But, having assumed $n \geqslant 4$, we have $p - 1 < q_0$ and $q_0 + p - 1 < n$. It follows that $R(X)$ is *simple*, that is, it contains no repeated entries. Now, define

$$\widehat{X} := \{x_i \,:\, i \in [p]\} \text{ and } X' := \{x'_i \,:\, i \in [p]\}.$$

Again looking to (9), we see that

$$C(\widehat{X}) = \{3i \,:\, i \in [p]\} \text{ and } C(X') = \{q_1 + 3i \pmod{n} \,:\, i \in [p]\}.$$

Because $3(p-1) < n$, both $C(\widehat{X})$ and $C(X')$ are simple sets. Thus, $C(X) = C(\widehat{X}) \cup C(X')$ is simple unless $C(\widehat{X}) \cap C(X') \neq \emptyset$. Suppose there were some $c \in C(\widehat{X}) \cap C(X')$. As $c \in C(\widehat{X})$, there is an $i_0 \in [p]$ such that $c = 3i_0$, which implies $c \equiv 0 \pmod{3}$. On the other hand, $c \in C(X')$ implies $c \equiv q_1 + 3i_1 \pmod{n}$ for some $i_1 \in [p]$. We claim that this implies $c \not\equiv 0 \pmod{3}$, which will yield a contradiction.

To prove this claim, first suppose that n is a multiple of 3. In this case q is also divisible by 3, and (8) tells us that $q_1 = q + 1 \equiv 1 \pmod{3}$. But then $c \equiv q_1 + 3i_1 \equiv 1 \pmod{3}$ as claimed. Now suppose n is not divisible by 3. In this case (8) tells us that $q_1 = q \not\equiv 0 \pmod{3}$. When $q + 3i_1 < n$ this implies $c \equiv q + 3i_1 \not\equiv 0 \pmod{3}$, while when $q + 3i_1 \geqslant n$ we have

$$c \equiv q + 3i_1 - n \equiv q - n = -q \not\equiv 0 \pmod{3}.$$

Now, observe that X and Y have the same "shape" in L in the sense that $R(Y) \subseteq R(X)$ and $C(Y) \subseteq \{c + 2p : c \in C(X)\}$. Thus, having shown that $R(X)$ and $C(X)$ are simple, we may conclude that $R(Y)$ and $C(Y)$ are also simple. In other words, there are no row-edges or column-edges between cells in Y.

We next show that $S(X)$ is a simple set. From here to the end of the proof indices are expressed modulo m. Recalling (8), observe that $q_0 + q_1 \in \{n-1, n+1\}$. Combinined with (5), (9), and the fact that t divides n, this implies the existence of some $w \in \{-1, 1\}$ such that, for every $i \in [p]$,

$$S(x_i) = (\overline{4i}, h_i + h_{3i}) \text{ and } S(x_i') = (\overline{4i + w}, h_{i+q_0} + h_{3i+q_1}).$$

Considering the parity of entries in the first coordinate, we immediately see that $S(x_i) \neq S(x_j')$ for every $i, j \in [p]$. Thus, $S(\widehat{X}) \cap S(X') = \emptyset$.

To see that $S(\widehat{X})$ is simple, consider $x_i, x_j \in \widehat{X}$ such that $S(x_i) = S(x_j)$. We then have $h_i + h_{3i} = h_j + h_{3j}$, and applying Lemma 8 with $c = d = 0$ and $s = 3$ tells us that $i \equiv j \pmod{m}$. We also have

$$4i \equiv 4j \pmod{t}. \tag{11}$$

Suppose $t \leqslant 4$. In this case (11) is trivially satisfied. However, because $0 \leqslant i, j \leqslant p - 1$,

$$|i - j| < p = \left\lceil \frac{tm}{4} \right\rceil \leqslant \left\lceil \frac{4m}{4} \right\rceil = m.$$

As distinct numbers are congruent modulo m only if their difference is at least m, we may conclude that $i = j$. So, recalling that $t = 2^l$ for some integer $l \geqslant 1$, we may assume $t \geqslant 8$. It then follows from (11) that $i - j \equiv 0 \pmod{2^{l-2}}$. Because m is odd, $\gcd\left(m, 2^{l-2}\right) = 1$ and the Chinese Remainder Theorem tells us that $x = 0$ is the unique $x \in [2^{l-2}m]$ satisfying $x \equiv 0 \pmod{2^{l-2}}$ and $x \equiv 0 \pmod{m}$. But we have just shown that $|i - j| \equiv 0 \pmod{m}$ and $|i - j| \equiv 0 \pmod{2^{l-1}}$. Thus, as $0 \leqslant |i - j| < p = 2^{l-2}m$, we have $i = j$.

A similar argument shows that $S(X')$ is simple. Indeed, when $S(x_i') = S(x_j')$, applying Lemma 8 with $c = q_0$, $d = q_1$, and $s = 3$ yields $i \equiv j \pmod{m}$, while $4i + w \equiv 4j + w \pmod{t}$ implies $4i \equiv 4j \pmod{t}$. From here we may proceed exactly as above.

The proof that $S(Y)$ is simple is nearly identical. By (5) and (10), there is some $w \in \{-1, 1\}$ such that

$$S(y_i) = (\overline{4i + 2p}, h_i + h_{3i+2p}) \text{ and } S(y_i') = (\overline{4i + 2p + w}, h_{i+q_0} + h_{3i+q_1+2p})$$

for every $i \in [q-p]$. Considering the parity of entries in the first coordinate, we see $S(\widehat{Y}) \cap S(Y') = \emptyset$. We then check that $S(\widehat{Y})$ and $S(Y')$ are both simple by applying Lemma 8 and noting that for $z \in \mathbb{Z}$ we have $4i + z \equiv 4j + z \pmod{t}$ if and only if $4i \equiv 4j \pmod{t}$. □

Proof of Theorem 6. By Theorem 5, if $Syl_2(G)$ is trivial or non-cyclic, then $\chi(G) = n$. Otherwise $\chi(G) \geqslant n + 2$, from which Theorem 10 implies $\chi(G) = n + 2$. □

3 A general upper bound

Consider a finite group G and a normal subgroup $H \triangleleft G$. In [9], Hall and Paige showed that a sufficient condition for the existence of a transversal in $L(G)$ is that both $L(H)$ and $L(G/H)$ possess transversals. This turns out to be a special case of a more general result concerning colorings of finite group Cayley tables.

Our proof of this fact relies upon a modification the mappings R, C, and S—introduced just before Theorem 10—which map sets of cells in a latin square to *multi*sets of rows indices, column indices, and symbols, respectively. Given a multiset X, let $\mathrm{Supp}(X)$ be the underlying simple set. For every set of cells $X \subseteq L(G)$, we set $R'(X) := \mathrm{Supp}(R(X))$, $C'(X) := \mathrm{Supp}(C(X))$, and $S'(X) := \mathrm{Supp}(S(X))$.

Lemma 12. *Let G be a finite group and let $H \triangleleft G$ be a normal subgroup. Then*

$$\chi(G) \leqslant \chi(H)\chi(G/H).$$

Proof. Letting $n := |G|$ and $m := |H|$, set $k := \frac{n}{m}$. We begin by constructing a block representation

$$L(G) = \begin{pmatrix} A_{00} & A_{01} & \cdots & A_{0,k-1} \\ A_{10} & A_{11} & \cdots & A_{1,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ A_{k-1,0} & A_{k-1,1} & \cdots & A_{k-1,k-1} \end{pmatrix} \tag{12}$$

where each block A_{ij} is a latin subsquare satisfying $\chi(A_{ij}) = \chi(H)$. Let $\{f_0, f_1, \ldots, f_{k-1}\}$ be a collection of coset representatives for H in G, so that $G/H = \{f_0H, f_1H, \ldots, f_{k-1}H\}$. We may assume that f_0 is the identity element of G. To build the block representation (12), fix an ordering of $H = \{h_0, h_1, \ldots, h_{m-1}\}$ and order the rows and columns of $L(G)$ by

$$h_0, h_1, \ldots, h_{m-1}, f_1h_0, \ldots, f_1h_{m-1}, f_2h_0, \ldots, f_2h_{m-1}, \ldots, f_{k-1}h_0, \ldots, f_{k-1}h_{m-1}. \tag{13}$$

Fixing arbitrary $i, j \in [k]$, we define A_{ij} as the unique $m \times m$ subsquare of $L(G)$ satisfying

$$R'(A_{ij}) = \{im + x \,:\, x \in [m]\} \text{ and } C'(A_{ij}) = \{jm + x \,:\, x \in [m]\}.$$

Because H is normal in G there is a permutation $\pi \in S_m$ such that $h_r f_j = f_j h_{\pi(r)}$ for every $r \in [m]$. Thus $S'(A_{ij}) = f_i f_j H$, and it follows that A_{ij} is a latin subsquare of $L(G)$.

$\mathbf{1}$	h	h^2	s	sh	sh^2	s^2	s^2h	s^2h^2	s^3	s^3h	s^3h^2
h	$\mathbf{h^2}$	1	sh^2	s	sh	s^2h	s^2h^2	s^2	s^3h^2	s^3	s^3h
h^2	1	$\mathbf{h}$	sh	sh^2	s	s^2h^2	s^2	s^2h	s^3h	s^3h^2	s^3
s	sh	sh^2	$\mathbf{s^2}$	s^2h	s^2h^2	s^3	s^3h	s^3h^2	1	h	h^2
sh	sh^2	s	s^2h^2	s^2	$\mathbf{s^2h}$	s^3h	s^3h^2	s^3	h^2	1	h
sh^2	s	sh	s^2h	$\mathbf{s^2h^2}$	s^2	s^3h^2	s^3	s^3h	h	h^2	1
s^2	s^2h	s^2h^2	s^3	s^3h	s^3h^2	1	h	h^2	$\mathbf{s}$	sh	sh^2
s^2h	s^2h^2	s^2	s^3h^2	s^3	s^3h	h	h^2	1	sh^2	s	$\mathbf{sh}$
s^2h^2	s^2	s^2h	s^3h	s^3h^2	s^3	h^2	1	h	sh	$\mathbf{sh^2}$	s
s^3	s^3h	s^3h^2	1	h	h^2	s	sh	sh^2	s^2	s^2h	s^2h^2
s^3h	s^3h^2	s^3	h^2	1	h	sh	sh^2	s	s^2h^2	s^2	s^2h
s^3h^2	s^3	s^3h	h	h^2	1	sh^2	s	sh	s^2h	s^2h^2	s^2

Figure 4: $L(Dic_3)$, divided into blocks as per (12), with a color class from the proof of Lemma 12 in bold.

To establish $\chi(A_{ij}) = \chi(H)$, we provide a graph isomorphism between $\Gamma(A_{ij})$ and $\Gamma(H)$. Indeed, for every $v_{ab} = (a, b, h_a h_b) \in V(\Gamma(H))$, let $\phi(v_{ab}) = (\pi^{-1}(a), b, f_i f_j h_a h_b) \in V(\Gamma(A_{ij}))$. It then follows from the definition of a group that the triples $v_{ab} = (a, b, h_a h_b)$ and $v_{cd} = (r, s, h_r h_s)$ match in exactly one coordinate if and only if the corresponding triples $\phi(v_{ab})$ and $\phi(v_{rs})$ match in exactly one coordinate.

Let K be the $k \times k$ array formed from (12) by identifying blocks with the symbols therein contained. Having shown above that $S'(A_{ij}) = f_i f_j H$, we see that K is a latin square which is equivalent to the Cayley table $L(G/H)$. Letting $y := \chi(G/H)$, we may select some y-coloring $f_\infty : K \to [y]$. Furthermore, letting $x := \chi(H)$, we may also select an x-coloring $c_{ij} : A_{ij} \to [x]$.

We now use the colorings f_∞ and $\{f_{ij} : i, j \in [k]\}$ to construct (xy)-coloring of L, say $f : L \to [x] \times [y]$. For each $i, j \in [k]$ and for every cell $c \in A_{ij} \subseteq L$, set $f(c) := (f_\infty(A_{ij}), f_{ij}(c))$. See Figure 4 for an example of a color class of f when $G = \langle h, s \,|\, h^3 = s^4 = 1, s^{-1}hs = h^{-1} \rangle$ is the dicyclic group of order 12 and $H = \mathbb{Z}_3$. To see that f is indeed a proper coloring, consider $c, c' \in L$ such that $f(c) = f(c')$. Because f_∞ is a proper coloring, c and c' cannot lie in adjacent blocks of $V(\Gamma(K))$. They could lie in the same block, say A_{ij}, but because f_{ij} is also a proper coloring, it is nonetheless impossible for c and c' to be adjacent in $\Gamma(L)$. □

Recall from Theorem 5 that, in determining an upper bound for the chromatic number of *all* finite groups, we need only consider groups whose Sylow 2-subgroups are nontrivial and cyclic. The following structural theorem for such groups was observed in [9] as a direct corollary of a classical result due to Burnside ([10] Theorem 14.3.1).

Lemma 13. *Let G be a finite group and let P be a Sylow 2-subgroup of G. If P is cyclic and nontrivial then there is a normal subgroup of odd order $H \triangleleft G$ for which $G/H \cong P$.*

Combining Lemmas 12 and 13, we obtain an upper bound for $\chi(G)$ which depends only upon the largest power of 2 dividing $|G|$.

Theorem 14. *Let l and m be nonnegative integers such that m is odd, and let $t = 2^l$. If G is a group of order $n = mt$, then*

$$\chi(G) \leqslant n + 2m.$$

Proof. We may assume $t \geqslant 2$ and $Syl_2(G) = \mathbb{Z}_t$, as otherwise Theorem 5 implies $\chi(G) = n \leqslant n + \frac{2n}{t}$. Lemma 13 then tells us that G has a normal subgroup H of order m satisfying $G/H \cong \mathbb{Z}_t$. With $\chi(H)$ and $\chi(\mathbb{Z}_t)$ determined by Theorem 5 and Theorem 10, respectively, it follows from Lemma 12 that

$$\chi(G) \leqslant \chi(H)\chi(\mathbb{Z}_t) = n + 2m. \qquad \square$$

Recall that the previously best-known general upper bound, proven in [15], was $\chi(G) \leqslant 2n$. Theorem 14 improves significantly upon this bound for general groups whose order is divisible by large powers of 2. Indeed, as t grows with respect to m, Theorem 14 approaches the conjectured best possible bound of $\chi(G) \leqslant n + 2$.

Given a (full) transversal T in a latin square L of order n, there is a unique bijection $\phi : [n] \to [n]$, known as the **index map of $\boldsymbol{T}$**, which sends the row index $x \in [n]$ to the column index of the unique cell in T with row index x, so that

$$T = \{L_{i,\phi(i)} \,:\, i \in [n]\}.$$

If L is the Cayley table of a group $G = \{g_0, g_1, \ldots, g_{n-1}\}$, then $\phi \in S_n$ is the index map of some transversal if and only if $g_i g_{\phi(i)}$ is an enumeration of G (or, in the language of [7], $g_i \mapsto g_{\phi(i)}$ is a *complete mapping*).

We end by proving our second main result, Theorem 7, which states that every finite group G of order n satisfies

$$\chi(G) \leqslant \frac{3}{2}n.$$

Proof of Theorem 7. Let P be a Sylow 2-subgroup of G. We may assume $P = \langle p \rangle \cong \mathbb{Z}_2$; indeed, if P is trivial then Theorem 5 implies $\chi(G) = n \leqslant \frac{3}{2}n$, while if $|P| \geqslant 4$ then it follows from Theorem 14 that

$$\chi(G) \leqslant n + 2\frac{n}{|P|} \leqslant n + \frac{2n}{4} = \frac{3}{2}n.$$

Letting $m := \frac{n}{2}$, Lemma 13 tells us that G has a normal subgroup H of order m satisfying $G/H \cong P$. As in the proof of Lemma 12, we fix an arbitrary enumeration of $H = \{h_0, h_1, \ldots, h_{m-1}\}$ and order the rows and columns of $L = L(G)$ by

$$h_0, h_1, \ldots, h_{m-1}, ph_0, ph_1, \ldots, ph_{m-1}.$$

Breaking L into four $m \times m$ subsquares, we obtain the block representation

$$L = \begin{pmatrix} A_0 & A_2 \\ A_1 & A_3 \end{pmatrix}.$$

Observe that each A_i is a latin subsquare with $A_0 = L(H)$.

Because $m = |H|$ is odd, Theorem 5 implies $\chi(A_0) = m = |A_0|$. Let $\{T_0, T_1, \ldots, T_{m-1}\}$ be an m-coloring of A_0. For each $i \in [m]$, let ϕ_i be the index map corresponding to the transversal T_i, so that

$$T_i = \{L_{j,\phi_i(j)} \,:\, j \in [m]\}.$$

We want to use ϕ_i to define m-colorings of A_1, A_2, and A_3. Fixing an arbitrary $i \in [m]$, define the set

$$T_i' := \{L_{m+j,\phi_i(j)} \,:\, j \in [m]\},$$

and note that $T_i' \subseteq A_1$. To see that T_i' is a transversal of A_1, note that ϕ_i is a bijection and $ph_j h_{\phi_i(j)}$ is an enumeration of pH. It is then easy to check that $\{T_i' \,:\, i \in [m]\}$ is an m-coloring of A_1.

To find m-colorings for A_2 and A_3, we use the fact that H is normal in G to define a permutation $\pi \in S_m$ for which $h_j p = ph_{\pi(j)}$ for every $j \in [m]$. Fixing an arbitrary $i \in [m]$, define the map $\psi_i : [m] \to ([2m] \setminus [m])$ by

$$\psi_i(j) := m + \phi_i(\pi(j)) \text{ for every } j \in [m].$$

As both π and ϕ_i are permutations of $[m]$, their composition is also a permutation. Thus, ψ_i is a bijection. We then define the sets

$$Q_i := \{L_{j,\psi_i(j)} \,:\, j \in [m]\} \text{ and } Q_i' := \{L_{m+j,\psi_i(j)} \,:\, j \in [m]\}.$$

Observing that $S(L_{j,\psi_i(j)}) = h_j ph_{\phi_i(\pi(j))} = ph_{\pi(j)} h_{\phi_i(\pi(j))}$ and $S(L_{m+j,\psi_i(j)}) = h_{\pi(j)} h_{\phi_i(\pi(j))}$, it is easy to check that $\{Q_i \,:\, i \in [m]\}$ and $\{Q_i' \,:\, i \in [m]\}$ are m-colorings of A_2 and A_3, respectively.

Let $\Gamma := \Gamma(L)$. Expressing indices modulo m, define for every $i \in [m]$ the set

$$X_i := T_i \cup T_{i+1}' \cup Q_i \cup Q_i'.$$

Because X_i is the union of four subsquare transversals, it contains exactly two cells from each row, column, and symbol class of L. Thus, the induced subgraph $\Gamma_i := \Gamma[X_i]$ is cubic. Noticing that $\{X_i \,:\, i \in [m]\}$ partitions L, if we can show that $\chi(\Gamma_i) \leqslant 3$ for every $i \in [m]$, then we may conclude that $\chi(L) \leqslant \frac{3}{2}n$. Fixing an arbitrary $i \in [m]$, Brooks' Theorem tells us that Γ_i is 3-colorable unless it contains a connected component isomorphic to the complete graph K_4.

Suppose we could find a connected component $\Lambda \subseteq \Gamma_i$ which is isomorphic to K_4. As $V(\Gamma_i)$ is the union of four independent sets—one corresponding to each subsquare A_j—we may assume $V(\Lambda) = \{v_j \in A_j \,:\, j \in [4]\}$. Moreover, the row and column edges of Λ must form a 4-cycle. Thus, if $R(v_0) = j$, we must have $C(v_0) = \phi_i(j)$ and $R(v_2) = j$. It then follows from the definition of Q_i that $C(v_2) = \psi_i(j)$. But this implies $C(v_3) = \psi_i(j)$, so that $R(v_3) = m + \psi_i^{-1}(\psi_i(j)) = m + j$. We then have $R(v_1) = m + j$ and $C(v_1) = \phi_{i+1}(j)$. If v_0, v_2, v_3, v_1 is to form a 4-cycle, we must have $C(v_0) = C(v_1)$. However, this would mean $\phi_i(j) = \phi_{i+1}(j)$, contradicting the fact that $T_i \cap T_{i+1} = \emptyset$. □

4 Concluding remarks and open problems

While the restriction of Cavenagh's Conjecture 2 to finite group Cayley tables remains open, even for groups as basic as dihedral groups with order congruent to 2 modulo 4, we believe that the restriction of Brualdi's Conjecture 3 to Cayley tables may be within reach.

Conjecture 15. For every finite group G, its Cayley table $L(G)$ possesses a near transversal.

Conjecture 15 is related to the notion of sequenceable groups, and is known to hold true for many groups that are not known to satisfy Cavenagh's conjecture [4, Chapter 3] (including all dihedral groups [11]).

One strengthening of Conjecture 2 is worth mentioning. Cavenagh and Kuhl [2] have conjectured that latin squares should possess optimal colorings that are *equitable*, i.e. colorings in which any two color classes differs in size by at most one.

Conjecture 16. Every latin square L possesses an equitable $\chi(L)$-coloring.

This obviously holds true if $\chi(L) = n$, while Mehdi Esmaili [6] has recently verified Conjecture 16 for *all* latin squares of order at most 8. Cavenagh and Kuhl prove that Conjecture 16 also holds for $L(\mathbb{Z}_n)$ when n is congruent to 2 or 10 modulo 12. They do this by starting with a construction similar to that in our proof of Theorem 10, then extending the two smaller color classes by carefully transferring cells from several of the larger color classes. Can a similar process be done with our colorings?

Finally, we mention a natural generalization of chromatic number to the class of orthogonal arrays. Following [3, §11.1], an **orthogonal array** is a $k \times n^2$ matrix in which every $2 \times n^2$ submatrix contains every pair in $[n] \times [n]$ as a column. Let $OA(n, k)$ be the set of orthogonal arrays with fixed n and k. For $k \geqslant 3$, a member of $OA(n, k)$ (with two rows designated as index sets) is equivalent to a set of $k - 2$ mutually orthogonal latin squares (MOLS) of order n. Let $\mathcal{O} \in OA(n, k)$. We may define $\chi(\mathcal{O})$ to be the least number of parts into which the columns of $\mathcal{O}$ can be partitioned such that the submatrix induced by each part has no row with a repeated entry. It is easy to show that $\chi(\mathcal{O}) \geqslant n$ and that $\chi(\mathcal{O}) = n$ if and only if $\mathcal{O}$ extends to a member of $OA(n, k + 1)$. Thus $\chi(\mathcal{O})$ serves as a measure of how close a set of $k - 2$ MOLS is to being extendable to a set of $k - 1$ MOLS. A number questions regarding the chromatic number of orthogonal arrays can be formulated, few of which have been investigated to our knowledge.

Acknowledgements

We would like to thank the anonymous "Reviewer B" for their many helpful suggestions.

References

[1] N. Besharati, L. Goddyn, E. S. Mahmoodian, and M. Mortezaeefar, On the chromatic number of Latin square graphs, *Discrete Math.* **339** (2016), 2613–2619.

[2] N. J. Cavenagh and J. Kuhl, On the chromatic index of Latin squares, *Contrib. Discrete Math.* **10** (2015), 22–30.

[3] J. Dénes and A. D. Keedwell, *Latin squares and their applications*, Elsevier/North-Holland, Amsterdam, second edition, 2015.

[4] J. Dénes and A. D. Keedwell, *Latin squares: New developments in the theory and applications*, Ann. Discrete Math., **46**, North-Holland, Amsterdam, 1991.

[5] L. Euler, Recherches sur une nouvelle espece de quarres magiques, *Verh. Zeeuwsch. Gennot. Weten. Vliss.* **9** (1782), 85–239.

[6] Mehdi Esmaili, Personal communication.

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

[8] K. C. Halasz, *Coloring Cayley tables of finite groups*, MSc thesis, Simon Fraser University, 2017.

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

[10] M. Hall, *The theory of groups*, Macmillan, New York, 1959.

[11] P. Li, Sequencing the dihedral groups D_{4k}, *Discrete Math.* **175** (1997), 271–276.

[12] N. Pippenger and J. Spencer, Asymptotic behavior of the chromatic index for hypergraphs, *J. Combin. Theory Ser. A* **51** (1989), 24–42.

[13] H. J. Ryser, Neuere probleme der kombinatorik, *Vorträge über Kombinatorik Oberwolfach*, 24–29 Juli (1967), 69–91.

[14] S. K. Stein, Transversals of Latin squares and their generalizations, *Pacific J. Math.* **59** (1975), 567–575.

[15] I. M. Wanless, A generalisation of transversals for Latin squares, *Electron. J. Combin.* **9**(1) (2002), #R12.

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

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