Transversals in Latin Squares: A Survey

Ian M. Wanless

Abstract

A latin square of order n is an $n \times n$ array of n symbols in which each symbol occurs exactly once in each row and column. A transversal of such a square is a set of n entries containing no pair of entries that share the same row, column or symbol. Transversals are closely related to the notions of complete mappings and orthomorphisms in (quasi)groups, and are fundamental to the concept of mutually orthogonal latin squares.

Here we survey the literature on transversals and related notions. We cover (1) existence and enumeration results, (2) generalisations of transversals including partial transversals and plexes, (3) the special case when the latin square is a group table, (4) a connection with covering radii of sets of permutations, (5) transversals in arrays that generalise the notion of a latin square in various ways.

1 Introduction

By a *diagonal* of a square matrix we will mean a set of entries that contains exactly one representative from each row and column. A *transversal* is a diagonal in which no symbol is repeated. A *latin square* of order n is an $n \times n$ array of n symbols in which each symbol occurs exactly once in each row and in each column. The majority of this survey[1] looks at transversals (and their generalisations) in latin squares. In a transversal of a latin square every symbol must occur exactly once, although in §10 we will consider transversals of more general matrices where this property no longer holds.

Historically, interest in transversals arose from the study of orthogonal latin squares. A pair of latin squares $A = [a_{ij}]$ and $B = [b_{ij}]$ of order n are said to be *orthogonal mates* if the n^2 ordered pairs (a_{ij}, b_{ij}) are distinct. It is simple to see that if we look at all n occurrences of a given symbol in B, then the corresponding positions in A must form a transversal. Indeed,

Theorem 1.1 *A latin square has an orthogonal mate iff it has a decomposition into disjoint transversals.*

For example, below there are two orthogonal latin squares of order 8. Subscripted letters are used to mark the transversals of the left hand square which correspond

[1]The present survey extends and updates an earlier survey [123] on the same theme.

to the positions of each symbol in its orthogonal mate (the right hand square).

$$
\begin{array}{cccccccc}
1_a & 2_b & 3_c & 4_d & 5_e & 6_f & 7_g & 8_h \\
7_b & 8_a & 5_d & 6_c & 2_f & 4_e & 1_h & 3_g \\
2_c & 1_d & 6_a & 3_b & 4_g & 5_h & 8_e & 7_f \\
8_d & 7_c & 4_b & 5_a & 6_h & 2_g & 3_f & 1_e \\
4_f & 3_e & 1_g & 2_h & 7_a & 8_b & 5_c & 6_d \\
6_e & 5_f & 7_h & 8_g & 1_b & 3_a & 2_d & 4_c \\
3_h & 6_g & 2_e & 1_f & 8_c & 7_d & 4_a & 5_b \\
5_g & 4_h & 8_f & 7_e & 3_d & 1_c & 6_b & 2_a
\end{array}
\qquad
\begin{array}{cccccccc}
a & b & c & d & e & f & g & h \\
b & a & d & c & f & e & h & g \\
c & d & a & b & g & h & e & f \\
d & c & b & a & h & g & f & e \\
f & e & g & h & a & b & c & d \\
e & f & h & g & b & a & d & c \\
h & g & e & f & c & d & a & b \\
g & h & f & e & d & c & b & a
\end{array}
\qquad (1.1)
$$

It was conjectured by no less a mathematician than Euler [54] that orthogonal latin squares of order n exist iff $n \not\equiv 2 \bmod 4$. This conjecture was famously disproved by Bose, Shrikhande and Parker who in [16] showed instead that:

Theorem 1.2 *There is a pair of orthogonal latin squares of order n iff $n \notin \{2, 6\}$.*

More generally, there is interest in sets of *mutually orthogonal latin squares* (MOLS), that is, sets of latin squares in which each pair is orthogonal in the above sense. The literature on MOLS is vast (start with [31, 39, 40, 87]) and provides ample justification for studying transversals. In the interests of keeping this survey to a reasonable size, we will not discuss MOLS except as far as they bear directly and specifically on questions to do with transversals. While Theorem 1.1 remains the original motivation for studying transversals, subsequent investigations have shown that transversals are interesting objects in their own right. Despite this, a number of basic questions about their properties remain unresolved. In 1995, Alon *et al.* [6] bemoaned the fact that "There have been more conjectures than theorems on latin transversals in the literature." While there are still some frustratingly simply conjectures that remain unresolved, the progress in the last five years has finally rendered the lament from [6] untrue. Much of that progress has resulted from the discovery of a new tool called the "Delta Lemma".

2 The Delta Lemma

The deceptively simple idea behind the Delta Lemma occurred to two sets of researchers simultaneously and independently in 2005, leading eventually to the publications [49, 57]. Variants of the Lemma have also been used in [21, 37, 48, 50, 51, 101, 124].

To use the Delta Lemma it is useful to think of a latin square as being a set of *entries*, each of which is a (row, column, symbol) triple. It is convenient to index the rows, columns and symbols of a latin square of order n with $\mathbb{Z}_n$, in which case the square can be viewed as a subset of $\mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$. The latin property insists that distinct entries agree in at most one coordinate.

In its simplest form the Delta Lemma is this:

Lemma 2.1 *Let L be a latin square of order n indexed by $\mathbb{Z}_n$. Define a function $\Delta : L \to \mathbb{Z}_n$ by $\Delta(r, c, s) = r + c - s$. If T is a transversal of L then, modulo n,*

$$\sum_{(r,c,s)\in T} \Delta(r, c, s) = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ \frac{1}{2}n & \text{if } n \text{ is even.} \end{cases} \qquad (2.1)$$

The proof is a triviality, since by definition r, c and s take every value in $\mathbb{Z}_n$ once in T. Yet the simplicity of the result belies its power. The function Δ can be thought of as measuring the difference of a latin square from the cyclic group. It is uniformly zero on the addition table of $\mathbb{Z}_n$, which leads to an immediate corollary:

Theorem 2.2 *The addition table of $\mathbb{Z}_n$ has no transversals when n is even.*

This fact was proved by Euler [54], making it one of the first theorems ever proved about transversals[2]. Variants of the Delta Lemma can be used to show that many other groups lack transversals. We will revisit the question of which groups have a transversal in §6.

As Δ measures the difference of a latin square from $\mathbb{Z}_n$ it is at its most powerful when applied to latin squares where most entries agree with $\mathbb{Z}_n$. In many such cases, the few entries that have $\Delta \neq 0$ can readily be seen to have restrictions on the transversals that include them. This approach was used in [124] to show:

Theorem 2.3 *For every order $n > 3$ there exists a latin square which contains an entry that is not included in any transversal.*

Given Theorem 1.1, an immediate corollary is:

Theorem 2.4 *For every order $n > 3$ there is a latin square that has no orthogonal mate.*

The even case of this result was already known in Euler's day (Theorem 2.2), and the case of $n \equiv 1 \bmod 4$ was shown by Mann [92] in 1944 (see Theorem 4.6). However, despite prominence as an open problem [14, §3.3], [15, X.8.13], [46], [79, p.181] and [118], the $n \equiv 3 \bmod 4$ case resisted until the discovery of the Delta Lemma. With that history spanning back to the 18th century, it is remarkable that within 5 years the Delta Lemma has provided no fewer than four different proofs of Theorem 2.4, underscoring that it is the right tool for the job.

The first two proofs [57, 124] were simultaneous. Evans obtained Theorem 2.4 using a version of the Delta Lemma but without showing Theorem 2.3. In Evans' version of the Delta Lemma rows, columns and symbols have indices chosen from $\mathbb{Z}_m$ for some m smaller than the order of the square. Obviously, this necessitates some duplication of indices, but nevertheless, for any assignment of indices, there is a single value that must be the sum of the Δ function along any transversal.

Two further proofs of Theorem 2.4, both via Theorem 2.3, are given in [48, 51]. Although some of the earlier proofs are really quite neat, Egan's proof in [48] deserves recognition as the proof from "The Book". Here it is:

Proof [of Theorem 2.3] In light of Theorem 2.2, we need only consider odd $n > 3$.

[2]Euler used the name "formule directrix" for a transversal. Subsequently, in some statistical literature (e.g. [62]) a transversal was called a directrix.

Define a latin square $L = [L_{ij}]$ of order n, indexed by $\mathbb{Z}_n$, by

$$L_{ij} = \begin{cases} 1 & \text{if } (i,j) \in \{(0,0),(1,n-1)\}, \\ 0 & \text{if } (i,j) \in \{(1,0),(2,n-1)\}, \\ j+2 & \text{if } i = 0 \text{ and } j \in \{1,3,5,\dots,n-2\}, \\ j & \text{if } i = 2 \text{ and } j \in \{1,3,5,\dots,n-2\}, \\ i+j & \text{otherwise.} \end{cases}$$

To check that the entry $(1,0,0)$ is not in any transversal T of L, observe that $\Delta(1,0,0) = 1$. Any other entries which might lie in T, namely the ones that do not share any coordinate with $(1,0,0)$, have Δ value in $\{-2,0,2\}$. Since the entries with $\Delta = -2$ all share a row, at most one of them can be in any transversal. Likewise for the entries with $\Delta = +2$. As $n > 3$, it is impossible to satisfy (2.1). □

As a coda to this proof, we observe that a similar argument shows that the entry $(1, n-1, 1)$ is not in any transversal.

Evans [57] demonstrates that his variant of the Delta Lemma can be used to explain a number of classical results about transversals. In addition to the above, the Delta Lemma can be (and in many cases was) used to prove the Theorems numbered 3.1, 3.4, 3.5, 4.2, 4.3, 4.5, 4.6, 8.3, 8.4, 8.7, 8.8, 8.9, 8.10, 10.7, 10.8 and 10.11 in this survey. For such a simple device it is immensely powerful!

3 Entries not in transversals

As shown by Theorem 2.3, some latin squares have an entry that is not in any transversal. In extreme cases, such as Theorem 2.2, the latin square has no transversals at all. We now look at some further results of this nature.

A latin square of order mq is said to be of *q-step type* if it can be represented by a matrix of $q \times q$ blocks A_{ij} as follows

$$\begin{matrix} A_{11} & A_{12} & \cdots & A_{1m} \\ A_{21} & A_{22} & \cdots & A_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{mm} \end{matrix}$$

where each block A_{ij} is a latin subsquare of order q and two blocks A_{ij} and $A_{i'j'}$ contain the same symbols iff $i + j \equiv i' + j' \mod m$. The following classical theorem is due to Maillet [90] (and was rediscovered by Parker [99]).

Theorem 3.1 *Suppose that q is odd and m is even. No q-step type latin square of order mq possesses a transversal.*

As we will see in §6, this rules out many group tables having transversals. In particular, as we saw in Theorem 2.2, no cyclic group of even order has a transversal. By contrast, there is no known example of a latin square of odd order without transversals.

Conjecture 3.2 *Each latin square of odd order has at least one transversal.*

τ	Order n							
	2	3	4	5	6	7	8	9
0		1	1	1	2	54	267 932	19 270 833 530
1						11	13 165	18 066
2						26	1 427	1 853
3						12	253	54
4	1					12	508	21
5						6	89	7
6					1	8	65	7
7						3	33	1
8						4	48	1
9							25	
10						1	27	1
11						1	9	
12				1	2	6	9	
13						1	2	
14							2	
16			1		1	1	27	
18							1	
20							1	
28							1	
36					6	1		
64							33	
Total	1	1	2	2	12	147	283 657	19 270 853 541

Table 1: Species of order $n \leqslant 9$ according to their number of transversal-free entries.

This conjecture is known [94] to be true for $n \leqslant 9$. It is attributed to Ryser [104] and has been open for forty years. In fact, Ryser's original conjecture was somewhat stronger: for every latin square of order n, the number of transversals is congruent to n mod 2. In [11], Balasubramanian proved the even case.

Theorem 3.3 *In any latin square of even order the number of transversals is even.*

Despite this, it has been noted in [3, 25, 113] (and other places) that there are many counterexamples of odd order to Ryser's original conjecture. Hence the conjecture has now been weakened to Conjecture 3.2 as stated.

Latin squares of moderate order are typically blessed with many transversals, although it is clear that some rare cases have restrictions. One measure of the restrictions on transversals is $\tau(L)$, the number of transversal-free entries in a latin square L. The value of τ for latin squares of order up to 9 is shown in Table 1, from [51]. The entries in the table are counts of the number of species[3]. This table, together with tests on random latin squares of larger order suggests that almost all latin squares of large order have a transversal through every entry (i.e. $\tau = 0$). Nevertheless, we have the following result, which was implicitly shown in [124] and

[3] A *species* or *main class*, is an equivalence class of latin squares each of which has essentially the same structure. See [39, 87] for the definition.

explicitly stated in [51].

Theorem 3.4 *For all $n \geqslant 4$, there exists a latin square L of order n with $\tau(L) \geqslant 7$.*

This result is likely to be far short of best possible. Clearly, τ can be as large as n^2 for even n, by Theorem 2.2. For odd n we also know the following, from [51].

Theorem 3.5 *For all odd $m \geqslant 3$ there exists a latin square of order $3m$ that contains an $(m-1) \times m$ latin subrectangle consisting of entries that are not in any transversal.*

In this example $\tau/n^2 \geqslant m(m-1)/(3m)^2 \sim 1/9$, so at least a constant fraction of the entries are transversal free as $n = 3m \to \infty$. This raises the following interesting question [51]:

Question 3.6 *Is $\liminf_{n\to\infty} \max_L \frac{1}{n^2}\tau(L) > 0$, where L ranges over squares of order n?*

4 Disjoint transversals

Motivated by Theorem 1.1, we next consider sets of disjoint transversals. Such a set will be described as *maximal* if it is not a subset of a strictly larger set of disjoint transversals. For a given latin square L we consider two measures of the number of disjoint transversals in L. Let $\lambda = \lambda(L)$ be the largest cardinality of any set of disjoint transversals in L, and let $\alpha = \alpha(L)$ be the smallest cardinality of any maximal set of disjoint transversals in L. Clearly $0 \leqslant \alpha \leqslant \lambda \leqslant n$. We will also be interested in $\beta(n)$ and $\mu(n)$, which we define to be the minimum of $\alpha(L)$ and $\lambda(L)$, respectively, among all latin squares L of order n.

Example 4.1 A latin square of order n has $\lambda = n$ iff it has an orthogonal mate, by Theorem 1.1. For $n = 6$ there is no pair of orthogonal squares (see Theorem 1.2), but we can get close. Finney [62] gives the following example which contains 4 disjoint transversals indicated by the subscripts a, b, c and d.

1_a	2	3_b	4_c	5	6_d
2_c	1_d	6	5_b	4_a	3
3	4_b	1	2_d	6_c	5_a
4	6_a	5_c	1	3_d	2_b
5_d	3_c	2_a	6	1_b	4
6_b	5	4_d	3_a	2	1_c

This square has $\lambda = 4$, and $\alpha = 3$ (the different shadings show a maximal set of 3 disjoint transversals).

Table 2 shows the species of order $n \leqslant 9$, counted according to their maximum number λ of disjoint transversals. Table 3 shows the species of order $n = 9$ categorised according to their values of λ and α. The data in both tables was computed in [51].

Evidence for small orders (such as that in Table 2) led van Rees [118] to conjecture that, as $n \to \infty$, a vanishingly small proportion of latin squares have orthogonal

λ	$n=2$	3	4	5	6	7	8	9
0	1	0	1	0	6	0	33	0
1	-	0	0	1	0	1	0	0
2	0	-	0	0	2	5	7	0
3	-	1	-	0	0	24	46	3
4	-	-	1	-	4	68	712	23
5	-	-	-	1	-	43	71 330	142 915
6	-	-	-	-	0	-	209 505	61 613
7	-	-	-	-	-	6	-	18 922 150 935
8	-	-	-	-	-	-	2 024	-
9	-	-	-	-	-	-	-	348 498 052
Total	1	1	2	2	12	147	283 657	19 270 853 541

Table 2: Latin squares of order $n \leqslant 9$ with λ disjoint transversals.

	λ						
α	3	4	5	6	7	9	Total
1	0	7	36 000	0	0	0	36 007
2	2	4	6 765	528	873	5	8 177
3	1	12	100 150	61 085	18 786 989 798	340 588 766	19 127 739 812
4		0	0	0	135 160 264	7 909 243	143 069 507
5			0	0	0	32	32
6				0	0	5	5
7					0	1	1
Total	3	23	142 915	61 613	18 922 150 935	348 498 052	19 270 853 541

Table 3: Species of order 9 categorised according to λ and α.

mates. However, the trend seems to be quite the reverse (see [93, 124]), although no rigorous way of establishing this has yet been found.

For even orders, [50] showed that λ can achieve many different values[4]:

Theorem 4.2 *For each even $n \geqslant 6$ and each $j \equiv 0 \bmod 4$ such that $0 \leqslant j \leqslant n$, there exists a latin square L of order n with $\lambda(L) = j$.*

In [51] it was shown that $\lambda = 1$ is also achievable for even $n \geqslant 10$, as a corollary of:

Theorem 4.3 *For all even $n \geqslant 10$, there exists a latin square of order n that has transversals, but in which every transversal coincides on a single entry*[5]*.*

It is not possible for a latin square of order n to have $\lambda = n-1$. Theorems 4.2 and 4.3, together with small order examples, led the authors of [51] to conjecture that for large even orders, all other values of λ are achievable:

Conjecture 4.4 *For all even $n \geqslant 10$ and each $m \in \{0, 1, \ldots, n-3, n-2, n\}$ there exists a latin square of order n such that $\lambda(L) = m$.*

[4] We will see in Theorem 6.1 that the situation is markedly different for group tables.

[5] If n is a multiple of 16 then every transversal in the construction includes two specific entries.

For odd orders n, there is not even a conjecture as to which values of λ can be achieved, except that Conjecture 3.2 predicts that λ must be positive. This leads naturally to a discussion of $\mu(n)$, the minimum value of λ among the latin squares of order n. Clearly, $\mu(n) = 0$ for all even n by Theorem 2.2, so we are concerned with the case when n is odd. If Conjecture 3.2 is true, then $\mu(n) \geqslant 1$ for all odd n. Our best general upper bound currently is:

Theorem 4.5 *If $n > 3$ then $\mu(n) \leqslant \frac{1}{2}(n+1)$.*

This result was first explicitly stated in [51], although it follows immediately from the only known proof[6] of Theorem 2.4 that does not go via Theorem 2.3. The $n \equiv 3 \bmod 4$ case of Theorem 4.5 was implicitly shown by Evans [57], 62 years after the $n \equiv 1 \bmod 4$ had been shown by Mann [92], who proved:

Theorem 4.6 *Let L be a latin square of order $4k+1$ containing a latin subsquare S of order $2k$. Let U be the set of entries in L that do not share a row, column or symbol with any element of S. Then every transversal of L contains an odd number of elements of U.*

In Theorem 4.6, simple counting shows that U has $2k+1$ elements and hence $\lambda(L) \leqslant 2k+1 = (n+1)/2$.

There appears to be room to improve on the upper bound for $\mu(n)$ stated in Theorem 4.5. The known values of $\mu(n)$ for odd n are $\mu(1) = \mu(5) = \mu(7) = 1$ and $\mu(3) = \mu(9) = 3$. It would be of interest to determine if $\mu(n) < \frac{1}{2}n$ for $n > 3$. In particular [51]:

Question 4.7 *Is $\mu(n)$ bounded as $n \to \infty$?*

Next we consider $\beta(n)$, the minimum value of α among the latin squares of order n. Although we know little about the size of $\mu(n)$ for odd n, we can narrow $\beta(n)$ down to a very small set of possible values. A result in [50] proved that

$$\beta(n) \leqslant \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4, \\ 3 & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

Even this strong restriction leaves some potential for improvement. The known values of $\beta(n)$ for odd n are $\beta(3) = 3$ and $\beta(1) = \beta(5) = \beta(7) = \beta(9) = 1$. If Conjecture 3.2 is correct then $\beta(n) \geqslant 1$ for all odd n, but at this stage it is still plausible that equality holds for odd $n > 3$.

Finally, we remark that if transversals are not disjoint then they intersect. It is obvious that two transversals of an $n \times n$ latin square can never share exactly $n-1$ or $n-2$ entries. However, [28] shows that they can intersect in any other way:

Theorem 4.8 *For all odd $n > 5$ and every integer $t \in \{0, 1, 2, \ldots, n-3, n\}$ there exist two transversals of the addition table of $\mathbb{Z}_n$ that intersect in exactly t entries.*

[6] Theorem 2.4 is a direct corollary of Theorem 4.5.

5 Partial transversals

We have seen in Theorems 2.2 and 3.1 that not all latin squares have transversals, which prompts the question of how close we can get to finding a transversal in such cases. We define a *partial transversal*[7] of *length* k to be a set of k entries, each selected from different rows and columns of a latin square such that no two entries contain the same symbol. A partial transversal is *completable* if it is a subset of some transversal, whereas it is *non-extendible* if it is not contained in any partial transversal of greater length.

Since not all squares of order n have a partial transversal of length n (i.e. a transversal), the best we can hope for is to find one of length $n-1$. Such partial transversals are called *near transversals*. The following conjecture has been attributed to Brualdi (see [39, p.103]) and Stein [111] and, in [52], to Ryser. For generalisations of it, in terms of hypergraphs, see [2].

Conjecture 5.1 *Every latin square has a near transversal.*

A claimed proof of this conjecture by Deriyenko [42] contains a fatal error, as mentioned in [40, p.40] and discussed in detail in [25]. More recently, a paper [77] appeared in the maths arXiv claiming to prove Conjecture 5.1. However, the paper was subsequently withdrawn when it was discovered that the proof was invalid. By copying the method of Theorem 3.3, Akbari and Alireza [3] managed to show that the number of non-extendible near transversals in any latin square is divisible by 4. Unfortunately in many cases that number can be zero, as we will see in Corollary 6.6.

The best reliable lower bound to date states that there must be a partial transversal of length at least $n - O(\log^2 n)$. This was shown by Shor [108], and the implicit constant in the 'big O' was very marginally improved by Fu *et al.* [64]. Subsequently Hatami and Shor [73] discovered an error in [108] (duplicated in [64]) and corrected the constant to a higher one. Nonetheless, the important thing remains that the bound is $n - O(\log^2 n)$. This improved on a number of earlier bounds including $\frac{2}{3}n + O(1)$ (Koksma [83]), $\frac{3}{4}n + O(1)$ (Drake [45]) and $n - \sqrt{n}$ (Brouwer *et al.* [17] and Woolbright [126]).

It has also been shown in [25] that every latin square possesses a diagonal in which no symbol appears more than twice. An earlier claimed proof of this result [22, Thm 8.2.3] is incomplete.

Conjecture 5.1 has been open for decades and has now gained a degree of notoriety. A much simpler problem is to consider the shortest possible length of a non-extendible partial transversal. It is easy to see the impossibility of a non-extendible partial transversal having length strictly less than $\frac{1}{2}n$, since there would not be enough 'used' symbols to fill the submatrix formed by the 'unused' rows and columns. However, for all $n > 4$, non-extendible partial transversals of length $\lceil \frac{1}{2}n \rceil$ can easily be constructed using a square of order n which contains a subsquare S of order $\lfloor \frac{1}{2}n \rfloor$ and a partial transversal containing the symbols of S but not using any of the same rows or columns as S.

The antithesis of non-extendibility is for a partial transversal to be *completable* in the sense that it is a subset of some transversal. Theorems 3.4, 3.5 and 4.3 all furnish

[7] In some papers (e.g. [64, 73, 108]) a partial transversal of length k is defined slightly differently to be a diagonal on which k different symbols appear.

examples where even some partial transversals of length 1 fail to be completable. An interesting open question concerns the completability of short partial transversals in cyclic groups. Grüttmüller [68] defined $C(k)$ to be the smallest odd integer such that it is possible to complete every partial transversal of length k in $\mathbb{Z}_n$ for any odd $n \geqslant C(k)$. He showed that $C(1) = 1$ and $C(2) = 3$. It is not proved that $C(k)$ even exists for $k \geqslant 3$, but if it does then Grüttmüller [69] showed that $C(k) \geqslant 3k - 1$. He also provided computational evidence to suggest that this bound is essentially best possible. Further evidence that $C(3) = 9$ was given by Cavenagh *et al.* [27], who proved:

Theorem 5.2 *For any prime $p > 7$, every partial transversal of length 3 in the addition table of $\mathbb{Z}_p$ is completable.*

To complement this result, [110] gives a method for completing short partial transversals in $\mathbb{Z}_n$ when n has many different prime factors.

6 Finite Groups

By using the symbols of a latin square to index its rows and columns, each latin square can be interpreted as the Cayley table of a quasigroup [39]. In this section we consider the important special case when that quasigroup is associative; in other words, it is a group. The extra structure in this case allows for much stronger results. For example, let L_G be the Cayley table of a finite group G. Suppose that we know of a transversal of L_G that comprises a choice from each row i of an element g_i. Let g be any fixed element of G. Then if we select from each row i the element $g_i g$ this will give a new transversal. Moreover, as g ranges over G the transversals so produced will be mutually disjoint. Hence:

Theorem 6.1 *If the Cayley table of a finite group has a single transversal then it has a decomposition into disjoint transversals.*

In other words, using the notation of §4, the only two possibilities if $|G| = n$ are that $\lambda(L_G) = 0$ or $\lambda(L_G) = n$.

6.1 Complete Mappings and Orthomorphisms

Much of the study of transversals in groups has been phrased in terms of the equivalent concepts of complete mappings and orthomorphisms[8]. Mann [91] introduced complete mappings for groups, but the definition works just as well for quasigroups. It is this: a permutation θ of the elements of a quasigroup $(Q, \oplus)$ is a *complete mapping* if $\eta : Q \mapsto Q$ defined by $\eta(x) = x \oplus \theta(x)$ is also a permutation. The permutation η is known as an *orthomorphism* of $(Q, \oplus)$, following terminology introduced in [78]. All of the results of this paper could be rephrased in terms of complete mappings and/or orthomorphisms because of our next observation.

Theorem 6.2 *Let $(Q, \oplus)$ be a quasigroup and L_Q its Cayley table. Then $\theta : Q \mapsto Q$ is a complete mapping iff we can locate a transversal of L_Q by selecting, in each row*

[8] These two concepts are so closely related that some references (e.g. [75, 107]) confuse them.

x, the entry in column $\theta(x)$. Similarly, $\eta : Q \mapsto Q$ is an orthomorphism iff we can locate a transversal of L_Q by selecting, in each row x, the entry containing symbol $\eta(x)$.

There are also notions of near complete mappings and near orthomorphisms that correspond naturally to near transversals [12, 40, 55].

Orthomorphisms and complete mappings have been used to build a range of different combinatorial designs and algebraic structures including MOLS [12, 55, 91], generalized Bhaskar Rao designs [1], diagonally cyclic latin squares [27, 121], left neofields [12, 40, 55], Bol loops [96] and atomic latin squares [122]. This wide applicability and the intimate connection with transversals, as demonstrated by Theorem 6.2, justifies a closer look at orthomorphisms (or equivalently, at complete mappings). Various special types of orthomorphisms have been considered, with the focus often on orthomorphisms with a particularly nice algebraic structure. Such orthomorphisms have the potential to be exploited in a variety of applications, so we now examine them in some detail.

An orthomorphism of a group is *canonical* [12, 13, 40, 110] (also called *normalized* [31] or *standard* [75]) if it fixes the identity element[9]. In the following we will suppose that θ is an orthomorphism in a group G with identity ε. For the sake of simplicity we will assume that G is abelian and θ is canonical, although in some of the following categories these restrictions may be relaxed if so desired.

1. *Linear orthomorphisms*: θ is linear if $\theta(x) = \lambda x$ for some fixed $\lambda \in G$. Clark and Lewis [30] show that the number of such linear orthomorphisms of $\mathbb{Z}_n$ is

$$\prod_{p|n} p^{a-1}(p-2),$$

   where the product is over prime divisors of n and $a = a(p,n)$ is the greatest integer such that p^a divides n.

2. *Quadratic orthomorphisms*: Suppose G is the additive group of a finite field F and let $\square$ denote the set of non-zero squares in F. If there are constants $\lambda_1, \lambda_2 \in F$ such that θ can be defined as $x \mapsto \lambda_1 x$ for $x \in \square$ and $x \mapsto \lambda_2 x$ for $x \notin \square$, then we say θ is a quadratic orthomorphism. Linear orthomorphisms are a special case of quadratic orthomorphisms for which $\lambda_1 = \lambda_2$. Note that $\square$ is an index 2 subgroup of the multiplicative group of F, and the non-squares form a coset of $\square$.

3. *Cyclotomic orthomorphisms*: These generalise the quadratic orthomorphisms. Take any non-trivial subgroup H of the multiplicative group of F and choose a multiplier λ_i for each coset of H. Multiply every element in the coset (sometimes called a cyclotomy class) by the chosen multiplier. If the resulting map is an orthomorphism then we say it is a cyclotomic orthomorphism. See [55] for more information on cyclotomic orthomorphisms, including the special cases of linear and quadratic orthomorphisms.

[9] Some references (e.g. [55]) define all "orthomorphisms" to be canonical, but that is undesirable since it leaves no easy way to talk about the orthomorphisms which are not canonical.

4. *Regular orthomorphisms*: Let θ' be the restriction of θ to $G \setminus \{\varepsilon\}$. The orthomorphism θ is k-regular if the permutation θ' is regular in the sense that it permutes all elements of $G \setminus \{\varepsilon\}$ in cycles of length k. This notion was introduced in [63] and later studied in [107]. The special case when θ' has a single cycle of length $|G| - 1$ corresponds to the idea of an R-sequencing of G (see [40, Chap.3]).

5. *Involutory orthomorphisms*: If $\theta = \theta^{-1}$ then $\big\{\{x, \theta(x)\} : x \in G \setminus \{\varepsilon\}\big\}$ is a starter[10] in G. Conversely every starter in G defines an orthomorphism of G that is its own inverse.

6. *Strong orthomorphisms*: A permutation that is both an orthomorphism and a complete mapping is called a strong orthomorphism [8] (alternatively, a strong complete mapping [59] or a strong permutation [74]). They exist in an abelian group G if and only if the Sylow 2-subgroups and Sylow 3-subgroups of G are either trivial or non-cyclic [59]. Strong orthomorphisms are connected to strong starters, see [31, 74] for definitions and details.

7. *Polynomial orthomorphisms*: If G is the additive group of a ring R and there exists any polynomial $p(x)$ over R such that $\theta(x) = p(x)$ for all $x \in G$ then we say that θ is a polynomial orthomorphism. For example, linear orthomorphisms are polynomial, as is any orthomorphism of a finite field. In fact, [97, 119] any orthomorphism of a field of order $q \geqslant 4$ is realised by a polynomial of degree at most $q - 3$. In contrast, [110] showed that for any odd composite n there is a non-polynomial orthomorphism of $\mathbb{Z}_n$. The polynomials of small degree that produce orthomorphisms are classified in [97]. Note that quadratic orthomorphisms are polynomial, but are not produced by quadratic polynomials (indeed no orthomorphism is produced by a quadratic polynomial).

8. *Compound orthomorphisms*: Let d be a divisor of n. An orthomorphism θ of $\mathbb{Z}_n$ is defined to be d-compound if $\theta(i) \equiv \theta(j)$ whenever $i \equiv j \bmod d$. This notion was introduced in [110] where compound orthomorphisms were used, among other things, for completing partial orthomorphisms.

9. *Compatible orthomorphisms*: An orthomorphism θ of $\mathbb{Z}_n$ is compatible if it is d-compound for all divisors d of n. Every polynomial orthomorphism is necessarily compatible. The converse holds only for certain values of n, as characterised in [110]. The same paper contains a formula for the number of compatible orthomorphisms of $\mathbb{Z}_n$ expressed in terms of the number of orthomorphisms of $\mathbb{Z}_p$ for prime divisors p of n.

Having seen in Theorem 6.2 that transversals, orthomorphisms and complete mappings are essentially the same thing, we will adopt the practice of expressing our remaining results in terms of transversals even when the original authors used one of the other notions.

[10] A *starter* is a pairing of the non-zero elements of an additive group such that every non-zero element can be written as the difference of the two elements in some pair. Starters are useful for creating numerous different kinds of designs [31].

6.2 Which groups have transversals?

We saw in §3 that the question of which latin squares have transversals is far from settled. However, if we restrict our attention to group tables, the situation is a lot clearer.

Consider these five propositions for the Cayley table L_G of a finite group G:

(i) L_G has a transversal.

(ii) L_G can be decomposed into disjoint transversals.

(iii) There exists a latin square orthogonal to L_G.

(iv) There is some ordering of the elements of G, say $a_1, a_2, \ldots, a_n$, such that $a_1 a_2 \cdots a_n = \varepsilon$, where ε denotes the identity element of G.

(v) The Sylow 2-subgroups of G are trivial or non-cyclic.

The fact that (i), (ii) and (iii) are equivalent comes directly from Theorem 1.1 and Theorem 6.1. Paige [98] showed that (i) implies (iv). Hall and Paige [72] then showed[11] that (iv) implies (v). They also showed that (v) implies (i) if G is a soluble, symmetric or alternating group. They conjectured that (v) is equivalent to (i) for all groups.

It was subsequently noted in [41] that both (iv) and (v) hold for all non-soluble groups, which proved that (iv) and (v) are equivalent. A much more direct and elementary proof of this fact was given in [117]. Thus the Hall-Paige Conjecture could be rephrased as the statement that all five conditions (i)–(v) are equivalent.

For decades there was incremental progress, as the Hall-Paige Conjecture was shown to hold for various groups, including the linear groups $GL(2, q)$, $SL(2, q)$, $PGL(2, q)$ and $PSL(2, q)$ (see [56] and the references therein). Then a very significant breakthrough was obtained by Wilcox [125] who reduced the problem to showing it for the sporadic simple groups (of which the Mathieu groups have already been handled in [36]). Evans [58] then showed that the only possible counterexample was Janko's group J_4. Finally, in unpublished work Bray claims to have showed that J_4 has a transversal, thereby proving the important theorem:

Theorem 6.3 *Conditions* (i), (ii), (iii), (iv), (v) *are equivalent for all finite groups.*

An interesting first step towards finding non-associative analogues of Theorem 6.3 was taken by Pula [100]. Regarding the non-associative analogue of condition (iv) above, it was shown in [19] that for all $n \geqslant 5$ there exists a loop[12] of order n in which every element can be obtained as a product of all n elements in some order and with some bracketing.

While Theorem 6.3 settles the question of which groups have a transversal[13], it remains an interesting open question as to whether Conjecture 5.1 holds for groups. A related concept is the idea of a sequenceable group. A group of finite order n is

[11] As shown in [120], the fact that (i) implies (v) is actually a special case of Theorem 3.1.

[12] A *loop* is a quasigroup with an identity element [39].

[13] From now on we will sometimes refer to groups having transversals (or near transversals etc.) when strictly speaking it is the Cayley table of the group that has these structures.

called *sequenceable* if its elements can be labelled in an order $a_1, a_2, \ldots, a_n$ such that the products a_1, a_1a_2, $a_1a_2a_3$, $\ldots$, $a_1a_2\cdots a_n$ are distinct. This idea was introduced by Gordon [67] who showed that abelian groups are sequenceable iff they have a non-trivial cyclic Sylow 2-subgroup (in other words if condition (v) above fails). Since then, many non-abelian groups have been shown to be sequenceable as well (see [40, Chap 3] or [31, p.350] for details). The importance of this idea for our purposes is that the entries $(a_1a_2\cdots a_i,\ a_{i+1},\ a_1a_2\cdots a_{i+1})$ for $i = 1, 2, \ldots, n-1$ form a near transversal of a sequenceable group. Hence we have this folklore result:

Theorem 6.4 *If a finite group is sequenceable then it has a near transversal.*

The converse of Theorem 6.4 is false. For example, the dihedral groups of order 6 and 8 have near transversals but are not sequenceable. All larger dihedral groups are sequenceable [88]. Indeed, it has been conjectured by Keedwell [80] that all non-abelian groups of order at least 10 are sequenceable.

For abelian groups, an important result was proved by Hall [71]. Recast into the form most useful to us, it is this:

Theorem 6.5 *Let L_G be the Cayley table of an abelian group G of finite order n, with identity 0. Suppose $b_1, b_2, \ldots, b_n$ is a list of (not necessarily distinct) elements of G. A necessary and sufficient condition for L_G to possess a diagonal on which the symbols are $b_1, \ldots, b_n$ (in some order), is that $\sum b_i = 0$.*

Since the sum of the elements in an abelian group is the identity if condition (v) above holds, and is the unique involution in the group otherwise, we have:

Corollary 6.6 *If a finite abelian group has a non-trivial cyclic Sylow 2-subgroup then it possesses non-extendible near transversals, but no transversals. Otherwise it has transversals but no non-extendible near transversals.*

This corollary has been rediscovered several times, most recently by Stein and Szabó [113]. They also show that for p prime, $\mathbb{Z}_p$ has no diagonal with exactly two distinct symbols on it. Again, this is a direct corollary of Theorem 6.5. We will see yet a third result that follows easily from Theorem 6.5 in Theorem 10.8.

6.3 How many transversals does a group have?

We turn next to the question of how many transversals a given group may have. In this subsection and the next, we will be concerned with estimating the number of transversals, as well as demonstrating that it must satisfy certain congruences. Analogous questions for more general latin squares will be considered in §7.

Using theoretical methods it seems very difficult to find accurate estimates for the number of transversals in a latin square (unless, of course, that number is zero). This difficulty is so acute that there are not even good estimates for z_n, the number of transversals of the cyclic group of order n. Clark and Lewis [30] conjecture that $z_n \geqslant n(n-2)(n-4)\cdots 3\cdot 1 = n!\,o(\sqrt{e/n}^{\,n})$ for odd n, while Vardi [116] makes a stronger prediction:

Conjecture 6.7 *There exist real constants* $0 < c_1 < c_2 < 1$ *such that*

$$c_1^n n! \leqslant z_n \leqslant c_2^n n!$$

for all odd $n \geqslant 3$.

Vardi makes this conjecture[14] while considering a variation on the toroidal n-queens problem. The toroidal n-queens problem is that of determining in how many different ways n non-attacking queens can be placed on a toroidal $n \times n$ chessboard. Vardi considered the same problem using semiqueens in place of queens, where a semiqueen is a piece which moves like a toroidal queen except that it cannot travel on right-to-left diagonals. The solution to Vardi's problem provides an upper bound on the toroidal n-queens problem. The problem can be translated into one concerning latin squares by noting that every configuration of n non-attacking semiqueens on a toroidal $n \times n$ chessboard corresponds to a transversal in a cyclic latin square L of order n, where $L_{ij} \equiv i - j \bmod n$. Note that the toroidal n-queens problem is equivalent to counting diagonals which simultaneously yield transversals in L and L', where $L'_{ij} = i + j \bmod n$.

Cooper and Kovalenko [34] were the first to prove the upper bound in Conjecture 6.7 by showing $z_n = o(0.9154^n n!)$, and this was subsequently improved to $z_n = o(0.7072^n n!)$ in [84]. In Theorem 7.2 we will see a stronger bound, that applies to all latin squares, not just to cyclic groups.

Finding a lower bound of the form given in Conjecture 6.7 is still an open problem. However, [32, 103, 107] do give some lower bounds, each of which applies only for some n. The following better bound was found in [28], although it is still a long way short of proving Vardi's Conjecture:

Theorem 6.8 *If* n *is odd and sufficiently large then* $z_n > (3.246)^n$.

Estimates for the rate of growth of z_n are given by Cooper *et al.* [33], who arrived at a value around $0.39^n n!$ and Kuznetsov [85, 86] who favours the slightly smaller $0.37^n n!$. Acting on a hunch, the present author proposes:

Conjecture 6.9

$$\lim_{n\to\infty} \frac{1}{n} \log(z_n/n!) = -1.$$

Of course, at this stage it is not even known that this limit exists.

6.4 Congruences and divisors

We next consider congruences satisfied by the number of transversals in a group table. An immediate corollary of the proof of Theorem 6.1 is that for any group the number of transversals through a given entry of the Cayley table is independent of the entry chosen. Hence (see Theorem 3.5 of [40]) we get:

Theorem 6.10 *The number of transversals in the Cayley table of a group* G *is divisible by* $|G|$*, the order of* G.

[14]Vardi's actual statement is not very concrete. Conjecture 6.7 is the present author's interpretation of Vardi's intention.

McKay *et al.* [94] also showed the following simple results, in the spirit of Theorem 3.3:

Theorem 6.11 *The number of transversals in any symmetric latin square of order n is congruent to n modulo* 2*.*

Corollary 6.12 *Let G be a group of order n. If G is abelian or n is even then the number of transversals in G is congruent to n modulo* 2*.*

Corollary 6.12 cannot be generalised to non-abelian groups of odd order, given that the non-abelian group of order 21 has 826 814 671 200 transversals.

Theorem 6.13 *If G is a group of order $n \not\equiv 1 \bmod 3$ then the number of transversals in G is divisible by* 3*.*

We will see below that the cyclic groups of small orders $n \equiv 1 \bmod 3$ have a number of transversals which is not a multiple of three.

Let z_n be the number of transversals in the cyclic group of order n and let $z'_n = z_n/n$ denote the number of transversals through any given entry of the cyclic square of order n. Since $z_n = z'_n = 0$ for all even n by Theorem 2.2 we shall assume for the following discussion that n is odd. The initial values of z'_n are known from [105] and [106]. They are

$$z'_1 = z'_3 = 1, \quad z'_5 = 3, \quad z'_7 = 19, \quad z'_9 = 225, \quad z'_{11} = 3\,441, \quad z'_{13} = 79\,259,$$
$$z'_{15} = 2\,424\,195, \quad z'_{17} = 94\,471\,089, \quad z'_{19} = 4\,613\,520\,889, \quad z'_{21} = 275\,148\,653\,115,$$
$$z'_{23} = 19\,686\,730\,313\,955, \quad z'_{25} = 1\,664\,382\,756\,757\,625.$$

Interestingly, if we take these numbers modulo 8 we find that this sequence begins 1,1,3,3,1,1,3,3,1,1,3,3,1. We know from Theorem 6.11 that z'_n is always odd for odd n, but it is an open question whether there is any deeper pattern modulo 4 or 8. The initial terms of z'_n mod 3 are 1,1,0,1,0,0,2,0,0,1,0,0,2. We know from Theorem 6.13 that z'_n is divisible by 3 when $n \equiv 2 \bmod 3$. In fact we can say more:

Theorem 6.14 *Let n be an odd number. If $n \geqslant 5$ and $n \not\equiv 1 \bmod 3$ then z'_n is divisible by* 3*. If n is a prime of the form $2 \times 3^k + 1$ then $z'_n \equiv 1 \bmod 3$.*

Theorem 6.14 is from [110]. In the same paper, the sequence $z'_n \bmod n$ was completely determined:

Theorem 6.15 *If n is prime then $z'_n \equiv -2 \bmod n$, whereas if n is composite then $z'_n \equiv 0 \bmod n$.*

A nice fact about z_n is that it is the number of *diagonally cyclic latin squares* of order n. Equivalently, z_n is the number of quasigroups on the set $\{1, 2, \ldots, n\}$ which have the transitive automorphism $(123 \cdots n)$. Moreover, z'_n is the number of such quasigroups which are idempotent. See [20, 121] for more details and a survey of the many applications of such objects.

n	Number of transversals in groups of order n
3	3
4	0, 8
5	15
7	133
8	0, 384, 384, 384, 384
9	2 025, 2 241
11	37 851
12	0, 198 144, 76 032, 46 080, 0
13	1 030 367
15	36 362 925
16	0, 235 765 760, 237 010 944, 238 190 592, 244 744 192, 125 599 744, 121 143 296, 123 371 520, 123 895 808, 122 191 872, 121 733 120, 62 881 792, 62 619 648, 62 357 504
17	1 606 008 513
19	87 656 896 891
20	0, 697 292 390 400, 140 866 560 000, 0, 0
21	5 778 121 715 415, 826 814 671 200
23	452 794 797 220 965

Table 4: Transversals in groups of order $n \leqslant 23$.

6.5 Groups of small order

We now discuss the number of transversals in general groups of small order. For groups of order $n \equiv 2 \bmod 4$ there can be no transversals, by Theorem 6.3. For each other order $n \leqslant 23$ the number of transversals in each group is given in Table 4. The groups are ordered according to the catalogue of Thomas and Wood [115]. The numbers of transversals in abelian groups of order at most 16 and cyclic groups of order at most 21 were obtained by Shieh *et al.* [107]. The remaining values in Table 4 were computed by Shieh [105]. McKay *et al.* [94] then independently confirmed all counts except those for cyclic groups of order $\geqslant 21$, correcting one misprint in Shieh [105].

Bedford and Whitaker [13] offer an explanation for why all the non-cyclic groups of order 8 have 384 transversals. The groups of order 4, 9 and 16 with the most transversals are the elementary abelian groups of those orders. Similarly, for orders 12, 20 and 21 the group with the most transversals is the direct sum of cyclic groups of prime order. It is an open question whether such a statement generalises.

Question 6.16 *Is it true that a direct sum of cyclic groups of prime order always has at least as many transversals as any other group of the same order?*

By Corollary 6.12 we know that in each case covered by Table 4 (except the non-abelian group of order 21), the number of transversals must have the same parity as the order of the square. It is remarkable though, that the groups of even order have a number of transversals which is divisible by a high power of 2. Indeed, any 2-group of order $n \leqslant 16$ has a number of transversals which is divisible by 2^{n-1}. It would be interesting to know if this is true for general n. Theorem 6.10 does provide a partial answer, but there seems to be more to the story.

7 Number of transversals

In this section we consider the question of how many transversals a general latin square can have. We define $t(n)$ and $T(n)$ to be respectively the minimum and maximum number of transversals among the latin squares of order n.

In §6 we have already considered z_n, the number of transversals in the addition table of $\mathbb{Z}_n$, which is arguably the simplest case. Since $t(n) \leqslant z_n$, Theorem 2.2 tells us that $t(n) = z_n = 0$ for even n. It is unknown whether there is any odd n for which $t(n) = 0$, although Conjecture 3.2 asserts there is not. In any case, for lower bounds on $t(n)$ we currently can do no better than to observe that $t(n) \geqslant 0$, and to note that $t(1) = 1$, $t(3) = t(5) = t(7) = 3$ and $t(9) = 68$. A related question, for which no work seems to have been published, is to find an upper bound on $t(n)$ when n is odd.

Turning to the maximum number of transversals, we have $z_n \leqslant T(n)$ and hence Theorem 6.8 gives a lower bound on $T(n)$ for odd n. In fact, the bound applies for even n as well [28]:

Theorem 7.1 *Provided n is sufficiently large, $T(n) > (3.246)^n$.*

It is clear that $T(n) \leqslant n!$ since there are only $n!$ different diagonals. An exponential improvement on this trivial bound was obtained by McKay *et al.* [94], who showed:

Theorem 7.2 *For $n \geqslant 5$,*

$$15^{n/5} \leqslant T(n) \leqslant c^n \sqrt{n}\, n!$$

where $c = \sqrt{\frac{3-\sqrt{3}}{6}}\, e^{\sqrt{3}/6} \approx 0.6135.$

As a corollary of Theorem 7.2 we can infer that the upper bound in Conjecture 6.7 is true (asymptotically) with $c_2 = 0.614$. This also yields an upper bound for the number of solutions to the toroidal n-queens problem.

The lower bound in Theorem 7.2 is very simple and is weaker than Theorem 7.1. The upper bound took considerably more work, although it too is probably far from the truth.

The same paper [94] reports the results of an exhaustive computation of the transversals in latin squares of orders up to and including 9. Table 5 lists the minimum and maximum number of transversals over all latin squares of order n for $n \leqslant 9$, and the mean and standard deviation to 2 decimal places.

Table 5 confirms Conjecture 3.2 for $n \leqslant 9$. The following semisymmetric[15] latin squares are representatives of the unique species with $t(n)$ transversals for

[15]A latin square is semisymmetric if it is invariant under cyclically permuting the roles of rows, columns and symbols. See [39] for more details.

n	$t(n)$	Mean	Std Dev	$T(n)$
2	0	0	0	0
3	3	3	0	3
4	0	2	3.46	8
5	3	4.29	3.71	15
6	0	6.86	5.19	32
7	3	20.41	6.00	133
8	0	61.05	8.66	384
9	68	214.11	15.79	2241

Table 5: Transversals in latin squares of order $n \leqslant 9$.

$n \in \{5, 7, 9\}$. In each case the entries in the largest subsquares are shaded.

1	2	3	4	5
2	1	4	5	3
3	5	1	2	4
4	3	5	1	2
5	4	2	3	1

3	2	1	5	4	7	6
2	1	3	6	7	4	5
1	3	2	7	6	5	4
5	6	7	4	1	2	3
4	7	6	1	5	3	2
7	4	5	2	3	6	1
6	5	4	3	2	1	7

2	1	3	6	7	8	9	5	4
1	3	2	5	4	9	6	7	8
3	2	1	4	9	5	7	8	6
9	5	4	3	2	1	8	6	7
8	4	6	2	5	7	1	9	3
4	7	9	8	3	6	5	1	2
5	8	7	9	6	2	3	4	1
6	9	8	7	1	4	2	3	5
7	6	5	1	8	3	4	2	9

n	Lower Bound	Upper Bound
10	5 504	75 000
11	37 851	528 647
12	198 144	3 965 268
13	1 030 367	32 837 805
14	3 477 504	300 019 037
15	36 362 925	2 762 962 210
16	244 744 192	28 218 998 328
17	1 606 008 513	300 502 249 052
18	6 434 611 200	3 410 036 886 841
19	87 656 896 891	41 327 486 367 018
20	697 292 390 400	512 073 756 609 248
21	5 778 121 715 415	6 803 898 881 738 477

Table 6: Bounds on $T(n)$ for $10 \leqslant n \leqslant 21$.

In Table 6 we reproduce from [94] bounds on $T(n)$ for $10 \leqslant n \leqslant 21$. The upper bound is somewhat sharper than that given by Theorem 7.2, though proved by the same methods. The lower bound in each case is constructive and likely to be of the same order as the true value. When $n \not\equiv 2 \bmod 4$ the lower bound comes from the group with the highest number of transversals (see Table 4). When $n \equiv 2 \bmod 4$ the lower bound comes from a so-called turn-square, many of which were analysed in [94]. A *turn-square* is obtained by starting with the Cayley table of a group (typically a group of the form $\mathbb{Z}_2 \oplus \mathbb{Z}_m$ for some m) and "turning" some of the intercalates (that is, replacing a subsquare of order 2 by the other possible subsquare on the same symbols). For example,

$$\begin{array}{ccccc|ccccc}
5 & 6 & 2 & 3 & 4 & 0 & 1 & 7 & 8 & 9 \\
6 & 2 & 3 & 4 & 0 & 1 & 7 & 8 & 9 & 5 \\
2 & 3 & 4 & 0 & 1 & 7 & 8 & 9 & 5 & 6 \\
3 & 4 & 0 & 1 & 2 & 8 & 9 & 5 & 6 & 7 \\
4 & 0 & 1 & 2 & 3 & 9 & 5 & 6 & 7 & 8 \\
\hline
0 & 1 & 7 & 8 & 9 & 5 & 6 & 2 & 3 & 4 \\
1 & 7 & 8 & 9 & 5 & 6 & 2 & 3 & 4 & 0 \\
7 & 8 & 9 & 5 & 6 & 2 & 3 & 4 & 0 & 1 \\
8 & 9 & 5 & 6 & 7 & 3 & 4 & 0 & 1 & 2 \\
9 & 5 & 6 & 7 & 8 & 4 & 0 & 1 & 2 & 3
\end{array} \tag{7.1}$$

has 5504 transversals. The 'turned' entries have been shaded. The study of turn-squares was pioneered by Parker (see [18] and the references therein) in his unsuccessful quest for a triple of MOLS of order 10. He noticed that turn-squares often have many more transversals than is typical for squares of their order, and used this as a heuristic in the search for MOLS.

It is has long been suspected that $T(10)$ is achieved by (7.1). This suspicion was strengthened by McKay *et al.* [93] who examined several billion squares of order 10, including every square with a non-trivial symmetry, and found none had more than 5504 transversals. Parker was indeed right that the square (7.1) is rich in orthogonal mates[16]. However, using the number of transversals as a heuristic in searching for MOLS is not fail-safe. For example, the turn-square of order 14 with the most transversals (namely, 3 477 504) does not have any orthogonal mates [94]. Meanwhile there are squares of order n with orthogonal mates but which possess only the bare minimum of n transversals (the left hand square in (1.1) is one such).

Nevertheless, the number of transversals does provide a useful species invariant for squares of small orders where this number can be computed in reasonable time (see, for example, [82] and [120]). It is straightforward to write a backtracking algorithm to count transversals in latin squares of small order, though this method currently becomes impractical if the order is much over 20. See [75, 76, 107] for some algorithms and complexity theory results[17] on the problem of counting transversals.

8 Generalised transversals

There are several ways to generalise the notion of a transversal. We have already seen one of them, namely the partial transversals in §5. In this section we collect results on another generalisation, namely plexes.

[16] It has 12 265 168 orthogonal mates [89], which is an order of magnitude greater than Parker estimated.

[17] An unfortunate feature of the analysis in [75] of the complexity of counting transversals in cyclic groups is that it hinges entirely on a technicality as to what constitutes the input for the algorithm. The authors consider the input to be a single integer that specifies the order of group. However, their conclusions would be very different if the input was considered to be a Cayley table for the group in question, which in the context of counting transversals is a more natural approach.

A *k-plex* in a latin square of order n is a set of kn entries which includes k representatives from each row and each column and of each symbol. A transversal is a 1-plex.

Example 8.1 The shaded entries form a 3-plex in the following square:

1	2	3	**4**	5	**6**
2	1	4	**3**	**6**	5
3	**5**	1	6	**2**	**4**
4	6	**2**	5	**3**	**1**
5	**4**	**6**	2	1	3
6	**3**	**5**	**1**	4	2

The name k-plex was coined in [120] only fairly recently. It is a natural extension of the names duplex, triplex, and quadruplex which have been in use for many years (principally in the statistical literature, such as [62]) for 2, 3 and 4-plexes.

The entries not included in a k-plex of a latin square L of order n form an $(n-k)$-plex of L. Together the k-plex and its complementary $(n-k)$-plex are an example of what is called an *orthogonal partition* of L. For discussion of orthogonal partitions in a general setting see Gilliland [66] and Bailey [10]. For our purposes, if L is decomposed into disjoint parts $K_1, K_2, \ldots, K_d$ where K_i is a k_i-plex then we call this a $(k_1, k_2, \ldots, k_d)$-partition of L. A case of particular interest is when all parts have the same size. We call a $(k, k, \ldots, k)$-partition more briefly a *k-partition*. For example, the marked 3-plex and its complement form a 3-partition of the square in Example 8.1. By Theorem 1.1, finding a 1-partition of a square is equivalent to finding an orthogonal mate.

Some results about transversals generalise directly to other plexes, while others seem to have no analogue. Theorem 3.3 and Theorem 6.1 seem to be in the latter class, as observed in [94] and [120] respectively. However, Theorem 6.10 does generalise to the following [50]:

Theorem 8.2 *Let m be the greatest common divisor of positive integers n and k. Suppose L is the Cayley table of a group of order n. The number of k-plexes in L is a multiple of n/m.*

Also, Theorems 3.1 and 6.3 showed that not every square has a transversal, and similar arguments work for any k-plex where k is odd [120]:

Theorem 8.3 *Suppose that q and k are odd integers and m is even. No q-step type latin square of order mq possesses a k-plex.*

Theorem 8.4 *Let G be a group of finite order n with a non-trivial cyclic Sylow 2-subgroup. The Cayley table of G contains no k-plex for any odd k but has a 2-partition and hence contains a k-plex for every even k in the range $0 \leqslant k \leqslant n$.*

The situation for even k is quite different to the odd case. Rodney [31, p.143] conjectured that every latin square has a duplex. He subsequently strengthened this conjecture, according to Dougherty [44], to the following:

Conjecture 8.5 *Every latin square has the maximum possible number of disjoint duplexes. In particular, every latin square of even order has a* 2*-partition and every latin square of odd order has a* $(2, 2, 2, \ldots, 2, 1)$*-partition.*

Conjecture 8.5 was stated independently in [120]. It implies Conjecture 3.2 and also that every latin square has k-plexes for every even value of k up to the order of the square. Thanks to [50], Conjecture 8.5 is now known to be true for all latin squares of orders $\leqslant 9$. It is also true for all groups[18], as can be seen by combining Theorem 6.3 and Theorem 8.4.

If a group has a trivial or non-cyclic Sylow 2-subgroup then it has a k-plex for all possible k. Otherwise it has k-plexes for all possible even k but for no odd k. It is worth noting that other scenarios occur for latin squares which are not based on groups. For example, the square in Example 8.1 has no transversal but clearly does have a 3-plex. It is conjectured in [120] that there exist arbitrarily large latin squares of this type.

Conjecture 8.6 *For all even* $n > 4$ *there exists a latin square of order* n *which has no transversal but does contain a* 3*-plex.*

Another possibility was shown by a family of squares constructed in [49].

Theorem 8.7 *For all even* n *there exists a latin square of order* n *that has* k*-plexes for every odd value of* k *between* $\lfloor n/4 \rfloor$ *and* $\lceil 3n/4 \rceil$ (*inclusive*)*, but not for any odd value of* k *outside this range.*

Interestingly, there is no known example of odd integers $a < b < c$ and a latin square which has an a-plex and a c-plex but no b-plex.

The union of an a-plex and a disjoint b-plex of a latin square L is an $(a+b)$-plex of L. However, it is not always possible to split an $(a+b)$-plex into an a-plex and a disjoint b-plex. Consider a duplex which consists of $\frac{1}{2}n$ disjoint intercalates (latin subsquares of order 2). Such a duplex does not contain a partial transversal of length more than $\frac{1}{2}n$, so it is a long way from containing a 1-plex.

We say that a k-plex is *indivisible* if it contains no c-plex for $0 < c < k$. The duplex just described is indivisible[19]. Indeed, for every k there is an indivisible k-plex in some sufficiently large latin square. This was first shown in [120], but "sufficiently large" in that case meant at least quadratic in k. This was improved to linear as a corollary of our next result, from [21, 50]. An *indivisible partition* is a partition of a latin square into indivisible plexes.

Theorem 8.8 *For every* $k \geqslant 2$ *and* $m \geqslant 2$ *there exists a latin square of order* mk *with an indivisible* k*-partition.*

In particular, for all even $n \geqslant 4$ there is a latin square of order n composed of two indivisible $\frac{1}{2}n$-plexes. Egan [48] recently showed an analogous result for odd orders.

[18] For an alternative proof that Cayley tables of groups have at least one duplex, see [117].

[19] In contrast, it is known that any 3-plex that forms a latin trade is divisible; in fact it must divide into 3 disjoint transversals. See [26] for details.

Theorem 8.9 *If $n = 2k + 1 \geqslant 5$ then there is a latin square of order n with an indivisible $(k, k, 1)$-partition and an indivisible $(k, k + 1)$-partition.*

The previous two theorems mean that some squares can be split in "half" in a way that makes no further division possible. This is slightly surprising given that latin squares typically have a vast multitude of partitions into various plexes. For a detailed study of the indivisible partitions of latin squares of order up to 9, see [50].

It is an open question for what values of k and n there is a latin square of order n containing an indivisible k-plex. However, Bryant *et al.* [21] found the answer when k is small relative to n.

Theorem 8.10 *Let n and k be positive integers satisfying $5k \leqslant n$. Then there exists a latin square of order n containing an indivisible k-plex.*

It is also interesting to ask how large k can be relative to n. Define $\kappa(n)$ to be the maximum k such that some latin square of order n contains an indivisible k-plex. From Theorems 8.8 and 8.9 we know $\kappa(n) \geqslant \lceil n/2 \rceil$. Even though the numerical evidence (e.g. from [50]) suggests that latin squares typically contain many plexes, we are currently unable to improve on the trivial upper bound $\kappa(n) \leqslant n$. A proof of even the weak form of Conjecture 8.5 would at least show $\kappa(n) < n$ for $n > 2$. The values of $\kappa(n)$ for small n, as calculated in [50], are shown in Table 7.

n	1	2	3	4	5	6	7	8	9
$\kappa(n)$	1	2	1	2	3	4	5	5	6 or 7

Table 7: $\kappa(n)$ for $n \leqslant 9$.

So far we have examined situations where we start with a latin square and ask what sort of plexes it might have. To complete the section we consider the reverse question. We want to start with a potential plex and ask what latin squares it might be contained in. We define[20] a *k-protoplex* of order n to be an $n \times n$ array in which each cell is either blank or filled with a symbol from $\{1, 2, \ldots, n\}$, and which has the properties that (i) no symbol occurs twice within any row or column, (ii) each symbol occurs k times in the array, (iii) each row and column contains exactly k filled cells. We can then sensibly ask whether this k-protoplex is a k-plex. If it is then we say the partial latin square is *completable* because the blank entries can be filled in to produce a latin square. Donovan [43] asks for which k and n there exists a k-protoplex of order n that is not completable. The following partial answer was shown in [120].

Theorem 8.11 *If $1 < k < n$ and $k > \frac{1}{4}n$ then there exists a k-protoplex of order n that is not completable.*

Grüttmüller [69] showed a related result by constructing, for each k, a non-completable k-plex of order $4k - 2$ with the additional property that the plex is the union of k disjoint transversals. Daykin and Häggkvist [38] and Burton [23] independently conjectured that if $k \leqslant \frac{1}{4}n$ then every k-protoplex is completable. It

[20]Our definition of protoplex is very close to what is known as a "k-homogeneous partial latin square", except that such objects are usually allowed to have empty rows and columns [26].

seems certain that for k sufficiently small relative to n, every k-protoplex is completable. This has already been proved when $n \equiv 0 \bmod 16$ in [38]. Alspach and Heinrich [7] ask more specifically whether there exists an $N(k)$ with the property that if k transversals of a partial latin square of order $n \geqslant N(k)$ are prescribed then the square can always be completed. Grüttmüller's result just mentioned shows that $N(k) \geqslant 4k-1$, if it exists. A related result due to Burton [23] is this:

Theorem 8.12 *For $k \leqslant \frac{1}{4}n$ every k-protoplex of order n is contained in some $(k+1)$-protoplex of order n.*

An interesting generalisation of plexes was recently introduced by Pula [101]. A k-plex can be viewed as a function from the entries of a latin square to the set $\{0,1\}$, such that the function values add to k along any row, any column or for any symbol. Pula generalises this idea to a *k-weight*, which he defines exactly the same way, except that the function is allowed to take any integer value. He shows that the Delta Lemma still works with this more general definition and uses it to obtain analogues of several classical results, including Theorem 3.1. Perhaps more tantalisingly, he shows that Ryser's Conjecture (Conjecture 3.2) and the weak form of Rodney's Conjecture (Conjecture 8.5) are simple to prove for k-weights; every latin square has a 2-weight and all latin squares of odd order have a 1-weight. However, the analogue of Conjecture 5.1 for 1-weights is still an open question.

9 Covering radii for sets of permutations

Several years ago, a novel approach to Conjecture 3.2 and Conjecture 5.1 was opened up by Andre Kézdy and Hunter Snevily in unpublished notes. These notes were then utilised in the writing of [25], from which the material in this section is drawn. To explain the Kézdy-Snevily approach, we need to introduce some terminology.

Consider the *symmetric group* S_n as a metric space equipped with *Hamming distance*. That is, the distance between two permutations $g, h \in S_n$ is the number of points at which they disagree (n minus the number of fixed points of gh^{-1}). Let P be a subset of S_n. The *covering radius* $\mathrm{cr}(P)$ of P is the smallest r such that the balls of radius r with centres at the elements of P cover the whole of S_n. In other words every permutation is within distance r of some member of P, and r is chosen to be minimal with this property. The next result is proved in [24] and [25].

Theorem 9.1 *Let $P \subseteq S_n$ be a set of permutations. If $|P| \leqslant n/2$, then $\mathrm{cr}(P) = n$. However, there exists P with $|P| = \lfloor n/2 \rfloor + 1$ and $\mathrm{cr}(P) < n$.*

This result raises an obvious question. Given n and s, what is the smallest set S of permutations with $\mathrm{cr}(S) \leqslant n-s$? We let $f(n,s)$ denote the cardinality of the smallest such set S. This problem can also be interpreted in graph-theoretic language. Define the graph $G_{n,s}$ on the vertex set S_n, with two permutations being adjacent if they agree in at least s places. Now the size of the smallest dominating set in $G_{n,s}$ is $f(n,s)$.

Theorem 9.1 shows that $f(n,1) = \lfloor n/2 \rfloor + 1$. Since any two distinct permutations have distance at least 2, we see that $f(n,n-1) = n!$ for $n \geqslant 2$. Moreover, $f(n,s)$ is a monotonic increasing function of s (by definition).

The next case to consider is $f(n,2)$. Kézdy and Snevily made the following conjecture:

Conjecture 9.2 *If n is even, then $f(n,2) = n$; if n is odd, then $f(n,2) > n$.*

The Kézdy–Snevily Conjecture has several connections with transversals [25].

Theorem 9.3 *Let S be the set of n permutations corresponding to the rows of a latin square L of order n. Then S has covering radius $n-1$ if L has a transversal and has covering radius $n-2$ otherwise.*

Corollary 9.4 *If there exists a latin square of order n with no transversal, then $f(n,2) \leqslant n$. In particular, this holds for n even.*

Hence Conjecture 9.2 implies Conjecture 3.2, as Kézdy and Snevily observed. They also showed:

Theorem 9.5 *Conjecture* 9.2 *implies Conjecture* 5.1.

In other words, to solve the longstanding Ryser and Brualdi conjectures it may suffice to answer this: How small can we make a subset $S \subset S_n$ which has the property that every permutation in S_n agrees with some member of S in at least two places?

In Corollary 9.4 we used latin squares to find an upper bound for $f(n,2)$ when n is even. For odd n we can also find upper bounds based on latin squares. The idea is to choose a latin square with few transversals, or whose transversals have a particular structure, and add a small set of permutations meeting each transversal twice. For $n \in \{5,7,9\}$, we now give a latin square for which a single extra permutation (shaded) suffices, showing that $f(n,2) \leqslant n+1$ in these cases.

1	2	3	4	5
2	1	4	5	3
3	5	1	2	4
4	3	5	1	2
5	4	2	3	1
1	3	4	2	5

1	2	3	4	5	6	7
2	3	1	5	4	7	6
3	1	2	6	7	4	5
4	5	6	7	1	2	3
5	4	7	1	6	3	2
6	7	4	2	3	5	1
7	6	5	3	2	1	4
3	2	1	7	6	5	4

1	3	2	4	6	5	7	9	8
2	1	3	5	4	6	8	7	9
3	2	1	7	9	8	4	6	5
4	6	5	9	8	7	1	3	2
5	4	6	8	7	9	3	2	1
6	5	4	2	1	3	9	8	7
7	9	8	1	3	2	5	4	6
8	7	9	3	2	1	6	5	4
9	8	7	6	5	4	2	1	3
5	4	6	1	3	2	9	8	7

In general, we have the following [25]:

Theorem 9.6 $f(n,2) \leqslant \frac{4}{3}n + O(1)$ *for all n.*

The reader is encouraged to seek out [25] and the survey by Quistorff [102] for more information on covering radii for sets of permutations.

10 Generalisations of latin squares

There are a number of different ways in which the definition of a latin square can be relaxed. In this section we consider such generalisations, and what can be said about their transversals. In this context, it is worth clarifying exactly what we mean by a transversal. For a rectangular matrix we will always assume that there are no more rows than there are columns. In such a case, a *diagonal* will mean a selection of cells that includes one representative from each row and at most one representative from each column. As before, a *transversal*[21] will mean a diagonal in which no symbol is repeated. Of course, in situations where the number of symbols in the matrix exceeds the number of rows, this no longer means that every symbol must occur within the transversal. A *partial transversal of length* ℓ will be a selection of ℓ cells no two of which share their row, column or symbol. In an $m \times n$ matrix, a *near transversal* is a partial transversal of length $m - 1$.

A matrix is said to be *row-latin* if it has no symbol that occurs more than once in any row. Similarly, it is *column-latin* if no symbol is ever repeated within a column. Stein [111] defines an $n \times n$ matrix to be an *equi-n-square* if each of n symbols occurs n times within the matrix. In this terminology, a latin square is precisely a row-latin and column-latin equi-n-square. Stein [111] was able to show a number of interesting results including these:

Theorem 10.1 *In an equi-n-square there is a row or column that contains at least* $\sqrt{n}$ *distinct symbols.*

Theorem 10.2 *An equi-n-square has a partial transversal of length at least*

$$n\Big(1 - \frac{1}{2!} + \frac{1}{3!} - \cdots \pm \frac{1}{n!}\Big) \approx (1 - 1/e)n \approx 0.63n.$$

Theorem 10.3 *Suppose a positive integer* q *divides* $n > 2$. *If each of* n^2/q *symbols occurs* q *times in an* $n \times n$ *matrix then there is a partial transversal of length exceeding* $n - \frac{1}{2}q$.

Stein [111] also makes the following conjectures, some of which are special cases of others in the list:

1. An equi-n-square has a near transversal.
2. Any $n \times n$ matrix in which no symbol appears more than $n - 1$ times has a transversal.
3. Any $(n - 1) \times n$ matrix in which no symbol appears more than n times has a transversal.
4. Any $(n - 1) \times n$ row-latin matrix has a transversal.
5. For $m < n$, any $m \times n$ matrix in which no symbol appears more than n times has a transversal.

[21] Usage in this article follows the majority of the latin squares literature. For more general matrices the word 'transversal' has been used (for example, in [5, 6, 111, 114]) to mean what we are calling a diagonal. Other papers call diagonals 'sections' [113, 61] or '1-factors' [3]. When 'transversal' is used to mean diagonal, 'latin transversal' is used to mean what we are calling a transversal.

6. Any $(n-1)\times n$ matrix in which each symbol appears exactly n times has a transversal.
7. For $m<n$, any $m\times n$ matrix in which no symbol appears more than $m+1$ times has a transversal.

Example 10.4 Drisko [47] gives counterexamples to Stein's Conjecture 5, whenever $m<n\leqslant 2m-2$. The construction is simply to take $m-1$ columns that have the symbols in order $[1,2,3,\ldots,m]^T$ and the remaining columns to be $[2,3,\ldots,m,1]^T$. It is easy to argue directly that the resulting matrix has no transversal[22]. Taking $m=n-1$ we see immediately that Stein's Conjectures 3, 6 and 7 also fail.

A weakened form of Stein's Conjecture 5 can be salvaged. Stein's response to Example 10.4 was to propose a new conjecture [112] that all column-latin matrices have a near transversal. For "thin" matrices we can do even better. In Drisko's original paper [47] he proved the following result, which was subsequently generalised to matroids by Chappell [29], and later proved in a slightly different way by Stein [112]:

Theorem 10.5 *Let $n\geqslant 2m-1$. Any $m\times n$ column-latin matrix has a transversal.*

Häggkvist and Johansson [70] showed that every large enough and thin enough latin rectangle[23] not only has a transversal, but has an orthogonal mate:

Theorem 10.6 *Suppose $0<\varepsilon<1$. If n is sufficiently large and $m<\varepsilon n$ then every $m\times n$ latin rectangle can be decomposed into transversals.*

m	$n=2$	3	4	5	6	7
2	1	5	7	9	11	13
3		2	3	7	8	10
4			3	4	5	8
5				3	5	
6					4	

Table 8: $L(m,n)$ for small m,n.

Stein and Szabó [113] introduce the function $L(m,n)$ which they define as the largest integer i such that there is a transversal in every $m\times n$ matrix that has no symbol occurring more than i times. Table 8, reproduced from [113], shows the value of $L(m,n)$ for small m and n. The examples that show $L(5,5)<4$ and $L(6,6)<5$ yield counterexamples to Stein's Conjecture 2. So of the seven conjectures listed above, only Conjectures 1 and 4 remain. In addition to the values in Table 8, Stein and Szabó show that $L(2,n)=2n-1$ for $n\geqslant 3$ and $L(3,n)=\lfloor(3n-1)/2\rfloor$ for $n\geqslant 5$ and prove the lower bound $L(m,n)\geqslant n-m+1$. Akbari *et al.* [4] showed that $L(m,n)=\lfloor(mn-1)/(m-1)\rfloor$ if $m\geqslant 2$ and $n\geqslant 2m^3$. Parker is attributed in [112, 113] with a construction proving the following result, which also follows from Example 10.4:

[22] This can also easily be proved by a variant of the Delta Lemma.

[23] A *latin rectangle* is row-latin and column-latin and also must use the same symbols in each row.

Theorem 10.7 *If $n \leqslant 2m-2$ then $L(m,n) \leqslant n-1$.*

Various results have been shown using the probabilistic method. Erdős and Spencer [53] showed that $L(n,n) \geqslant (n-1)/16$. Fanaï [60] took the direct generalisation to rectangular matrices, showing $L(m,n) \geqslant \frac{1}{8}n(n-1)/(m+n-2)+1$. Alon *et al.* [6] showed that there is a small $\varepsilon > 0$ such that if no symbol occurs more than $\varepsilon 2^m$ times in a $2^m \times 2^m$ matrix, then the matrix can be decomposed into transversals. They claim the same method can be adapted to show the existence of a number of pairwise disjoint transversals in matrices of a similar type, but whose order need not be a power of 2.

Akbari and Alireza [3] define $l(n)$ to be the smallest integer such that there is a transversal in every $n \times n$ matrix that is row-latin and column-latin and contains at least $l(n)$ different symbols. They show that $l(1) = 1$, $l(2) = l(3) = 3$, $l(4) = 6$, and $l(5) \geqslant 7$. Theorem 2.2 shows that $l(n) > n$ for all even n. Establishing a meaningful upper bound on $l(n)$ remains an interesting open challenge. The authors of [3] conjecture that $l(n)-n$ is not bounded as $n \to \infty$. They also prove that $l(2^a-2) > 2^a$ for $a \geqslant 3$, which follows from:

Theorem 10.8 *Let a, b be any two elements of an elementary abelian 2-group G, of order $2^m \geqslant 4$. Let M be the matrix of order $2^m - 2$ formed from the Cayley table of G by deleting the rows and columns indexed by a and b. Then M has no transversal.*

Although Akbari and Alireza did not do so, it is simple to derive this result from Theorem 6.5, given that the sum of all but two elements of an elementary abelian group can never be the identity. A related new result by Arsovski [9] is this:

Theorem 10.9 *Any square submatrix of the Cayley table of an abelian group of odd order has a transversal.*

This result was originally conjecture by Snevily [109]. He also conjectured that in Cayley tables of cyclic groups of even order, the only submatrices without a transversal are subgroups of even order or "translates" of such subgroups. This conjecture (which remains open) does not generalise directly to all abelian groups of even order, as Theorem 10.8 shows.

Theorem 10.9 was first proved[24] for prime orders by Alon [5] and for all cyclic groups by Dasgupta *et al.* [35]. Gao and Wang [65] then showed it is true in arbitrary abelian groups for submatrices whose order is less than $\sqrt{p}$, where p is the smallest prime dividing the order of the group. In related work, Fanaï [61] showed that there is a transversal in any square submatrix of the addition table of $\mathbb{Z}_n$ (for arbitrary n)[25], provided the rows selected to form the submatrix are sufficiently close together relative to n. He also showed existence of a partial transversal in certain submatrices satisfying a slightly weaker condition.

Finally, we briefly consider arrays of dimension higher than two. A *latin hypercube* of order n is an $n \times n \times \cdots \times n$ array filled with n symbols in such a way that no symbol is repeated in any *line* of n cells parallel to one of the axes. A 3-dimensional

[24] In fact Alon showed a stronger result that allows rows to be repeated when selecting the submatrix. His proof uses the fascinating combinatorial nullstellensatz. For related work, see [81].

[25] Although, given [35], this result is only of interest when n is even.

latin hypercube is a *latin cube* and a 2-dimensional latin hypercube is a latin square. Furthermore, any 2-dimensional "slice" of a latin hypercube is a latin square. By a transversal of a latin hypercube of order n we mean a selection of n cells no two of which agree in any coordinate or share the same symbol. The literature contains some variation on the definitions of both latin hypercubes and transversals thereof [95]. Perhaps the most interesting work in this area is by Sun [114], who conjectured that all latin cubes have transversals[26]. Generalising this conjecture (and Conjecture 3.2) on the basis of the examples catalogued in [95], we propose:

Conjecture 10.10 *Every latin hypercube of odd dimension or of odd order has a transversal.*

The restriction to odd dimension or odd order is required. Let $Z_{n,d}$ denote the d-dimensional hypercube whose entry in cell $(x_1, x_2, \dots, x_d)$ is $x_1+x_2+\cdots+x_d \bmod n$. Then, by direct generalisation of Theorem 2.2, we have:

Theorem 10.11 *If n and d are even, there are no transversals in $Z_{n,d}$.*

Sun [114] showed that if d is odd and n is arbitrary then $Z_{n,d}$ has a transversal. In fact, any $k \times k \times \cdots \times k$ subarray of $Z_{n,d}$ has a transversal, where $1 \leqslant k \leqslant n$.

11 Concluding Remarks

We have only been able to give a brief overview of the fascinating subject of transversals in this survey. Space constraints have forced the omission of much worthy material, including proofs of most of the theorems quoted. However, even this brief skim across the surface has shown that many basic questions remain unanswered and much work remains to be done.

The subject is peppered with tantalising conjectures. Even the theorems in many cases seem to be far from best possible, leaving openings for future improvements. It is hoped that this survey may motivate and assist such improvements.

References

[1] R. J. R. Abel, D. Combe, G. Price and W. D. Palmer, Existence of generalized Bhaskar Rao designs with block size 3, *Discrete Math.* **309** (2009), 4069–4078.

[2] R. Aharoni and E. Berger, Rainbow matchings in r-partite r-graphs, *Electron. J. Combin.* **16** (2009), R119.

[3] S. Akbari and A. Alireza, Transversals and multicolored matchings, *J. Combin. Des.* **12** (2004), 325–332.

[4] S. Akbari, O. Etesami, H. Mahini, M. Mahmoody and A. Sharifi, Transversals in long rectangular arrays, *Discrete Math.* **306** (2006), 3011–3013.

[5] N. Alon, Additive Latin transversals, *Israel J. Math.* **117** (2000), 125-130.

[6] N. Alon, J. Spencer and P. Tetali, Covering with latin transversals, *Discrete Appl. Math.* **57** (1995), 1–10.

[26] Sun defined a transversal to be n cells no two of which lie in the same line. However, this seems too broad a definition. It includes some examples where, say, all cells in the transversal share the same first coordinate. However, Sun's results all relate to transversals as we have defined them.

[7] B. Alspach and K. Heinrich, Matching designs, *Australas. J. Combin.* **2** (1990), 39–55.

[8] B. A. Anderson, Sequencings and houses, *Congr. Numer.* **43** (1984), 23–43.

[9] B. Arsovski, A proof of Snevily's conjecture, *Israel J. Math.*, to appear.

[10] R. A. Bailey, Orthogonal partitions in designed experiments (Corrected reprint), *Des. Codes Cryptogr.* **8** (1996), 45–77.

[11] K. Balasubramanian, On transversals in latin squares, *Linear Algebra Appl.* **131** (1990), 125–129.

[12] D. Bedford, Orthomorphisms and near orthomorphisms of groups and orthogonal Latin squares: a survey, *Bull. Inst. Combin. Appl.* **15** (1995), 13–33.

[13] D. Bedford and R. M. Whitaker, Enumeration of transversals in the Cayley tables of the non-cyclic groups of order 8, *Discrete Math.* **197/198** (1999), 77–81.

[14] T. Beth, D. Jungnickel and H. Lenz, *Design theory*, Cambridge University Press, Cambridge, 1986.

[15] T. Beth, D. Jungnickel and H. Lenz, *Design theory* (2nd ed., Vol II), Cambridge University Press, Cambridge, 1999.

[16] R. C. Bose, S. S. Shrikhande and E. T. Parker. Further results on the construction of mutually orthogonal latin squares and the falsity of Euler's conjecture, *Canad. J. Math.* **12** (1960), 189–203.

[17] A. E. Brouwer, A. J. de Vries and R. M. A. Wieringa, A lower bound for the length of partial transversals in a latin square, *Nieuw Arch. Wisk. (3)* **26** (1978), 330–332.

[18] J. W. Brown and E. T. Parker, More on order 10 turn-squares, *Ars Combin.* **35** (1993), 125–127.

[19] J. Browning, P. Vojtěchovský and I. M. Wanless, Overlapping latin subsquares and full products, *Comment. Math. Univ. Carolin.* **51** (2010), 175–184.

[20] D. Bryant, M. Buchanan and I. M. Wanless, The spectrum for quasigroups with cyclic automorphisms and additional symmetries, *Discrete Math.* **309** (2009), 821–833.

[21] D. Bryant, J. Egan, B. M. Maenhaut and I. M. Wanless, Indivisible plexes in latin squares, *Des. Codes Cryptogr.* **52** (2009), 93–105.

[22] R. A. Brualdi and H. J. Ryser, *Combinatorial matrix theory*, Encyclopedia of Mathematics and its Applications **39**, Cambridge University Press, 1991.

[23] B. Burton, *Completion of partial latin squares*, honours thesis, University of Queensland, 1996.

[24] P. J. Cameron and C. Y. Ku, Intersecting families of permutations, *European J. Combin.* **24** (2003), 881–890.

[25] P. J. Cameron and I. M. Wanless, Covering radius for sets of permutations, *Discrete Math.* **293** (2005), 91–109.

[26] N. J. Cavenagh, A uniqueness result for 3-homogeneous Latin trades, *Comment. Math. Univ. Carolin.* **47** (2006), 337-358.

[27] N. J. Cavenagh, C. Hämäläinen and A. M. Nelson, On completing three cyclically generated transversals to a Latin square, *Finite Fields Appl.* **15** (2009), 294–303.

[28] N. J. Cavenagh and I. M. Wanless, On the number of transversals in Cayley tables of cyclic groups, *Disc. Appl. Math.* **158** (2010), 136–146.

[29] G. G. Chappell, A matroid generalization of a result on row-Latin rectangles, *J. Combin. Theory Ser. A* 88 (1999), 235–245.

[30] D. Clark and J. T. Lewis, Transversals of cyclic latin squares, *Congr. Numer.* **128** (1997), 113–120.

[31] C. J. Colbourn and J. H. Dinitz (eds), *Handbook of combinatorial designs* (2nd ed.), Chapman & Hall/CRC, Boca Raton, 2007.

[32] C. Cooper, A lower bound for the number of good permutations, Data Recording, Storage and Processing (Nat. Acad. Sci. Ukraine) **2** (2000), 15–25.

[33] C. Cooper, R. Gilchrist, I. Kovalenko and D. Novakovic, Deriving the number of good permutations, with applications to cryptography, *Cybernet. Systems Anal.* **5** (2000), 10–16.

[34] C. Cooper and I. M. Kovalenko, The upper bound for the number of complete mappings, *Theory Probab. Math. Statist.* **53** (1996), 77–83.

[35] S. Dasgupta, G. Károlyi, O. Serra and B. Szegedy, Transversals of additive Latin squares, *Israel J. Math.* **126** (2001), 17–28.

[36] F. Dalla Volta and N. Gavioli, Complete mappings in some linear and projective groups, *Arch. Math. (Basel)* **61** (1993), 111–118.

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

[38] D. E. Daykin and R. Häggkvist, Completion of sparse partial latin squares, *Graph theory and combinatorics*, 127–132, Academic Press, London, 1984.

[39] J. Dénes and A. D. Keedwell, *Latin squares and their applications*, Akadémiai Kiadó, Budapest, 1974.

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

[41] J. Dénes and A. D. Keedwell, A new conjecture concerning admissibility of groups, *European J. Combin.* **10** (1989), 171–174.

[42] I. I. Deriyenko, On a conjecture of Brualdi (in Russian), *Mat. Issled.* No. 102, Issled. Oper. i Kvazigrupp, (1988), 53–65, 119.

[43] D. Donovan, The completion of partial Latin squares, *Australas. J. Combin.* **22** (2000), 247–264.

[44] S. Dougherty, Planes, nets and codes, *Math. J. Okayama Univ.* **38** (1996), 123–143.

[45] D. A. Drake, Maximal sets of latin squares and partial transversals, *J. Statist. Plann. Inference* **1** (1977), 143–149.

[46] D. A. Drake, G. H. J. van Rees and W. D. Wallis, Maximal sets of mutually orthogonal latin squares, *Discrete Math.* **194** (1999), 87–94.

[47] A. A. Drisko, Transversals in row-Latin rectangles, *J. Combin. Theory Ser. A* **84** (1998), 181–195.

[48] J. Egan, Bachelor latin squares with large indivisible plexes, *J. Combin. Designs*, to appear.

[49] J. Egan and I. M. Wanless, Latin squares with no small odd plexes, *J. Combin. Designs* **16** (2008), 477–492.

[50] J. Egan and I. M. Wanless, Indivisible partitions of latin squares, *J. Statist. Plann. Inference* **141** (2011), 402–417.

[51] J. Egan and I. M. Wanless, Latin squares with restricted transversals, submitted.

[52] P. Erdős, D. R. Hickerson, D. A. Norton and S. K. Stein, Unsolved problems: Has every latin square of order n a partial latin transversal of size $n-1$? *Amer. Math. Monthly* **95** (1988), 428–430.

[53] P. Erdős and J. Spencer, Lopsided Lovász local lemma and latin transversals, *Discrete Appl. Math.* **30** (1991), 151–154.

[54] L. Euler, Recherches sur une nouvelle espéce de quarrés magiques, *Verh. Zeeuwsch. Gennot. Weten. Vliss.* **9** (1782), 85–239. Eneström E530, Opera Omnia OI7, 291–392.

[55] A. B. Evans, *Orthomorphism Graphs of Groups*, Springer, 1992.

[56] A. B. Evans, The existence of complete mappings of $\mathrm{SL}(2, q)$, $q \equiv 3$ modulo 4, *Finite Fields Appl.* **11** (2005), 151–155.

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

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

[59] A. B. Evans, The existence of strong complete mappings, submitted.

[60] H.-R. Fanaï, A note on transversals, *Ars Combin.* **91** (2009), 83–85.

[61] H.-R. Fanaï, Existence of partial transversals, *Linear Algebra Appl.* **432** (2010), 2608–2614.

[62] D. J. Finney, Some orthogonal properties of the 4×4 and 6×6 latin squares. *Ann. Eugenics* **12** (1945), 213–219.

[63] R. J. Friedlander, B. Gordon and P. Tannenbaum, Partitions of groups and complete mappings, *Pacific J. Math.* **92** (1981), 283–293.

[64] H.-L. Fu, S.-C. Lin and C.-M. Fu, The length of a partial transversal in a latin square, *J. Combin. Math. Combin. Comput.* **43** (2002), 57–64.

[65] W. D. Gao and D. J. Wang, Additive Latin transversals and group rings, *Israel J. Math.* **140** (2004), 375–380.

[66] D. C. Gilliland, A note on orthogonal partitions and some well-known structures in design of experiments, *Ann. Statist.* **5** (1977), 565–570.

[67] B. Gordon, Sequences in groups with distinct partial products, *Pacific J. Math.* **11** (1961), 1309–1313.

[68] M. Grüttmüller, Completing partial Latin squares with two cyclically generated prescribed diagonals, *J. Combin. Theory Ser. A* **103** (2003), 349–362.

[69] M. Grüttmüller, Completing partial Latin squares with prescribed diagonals, *Discrete Appl. Math.* **138** (2004), 89–97.

[70] R. Häggkvist and A. Johansson, Orthogonal Latin rectangles, *Combin. Probab. Comput.* **17** (2008), 519–536.

[71] M. Hall, A combinatorial problem on abelian groups, *Proc. Amer. Math. Soc.* **3** (1952), 584–587.

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

[73] P. Hatami and P. W. Shor, Erratum to: A lower bound for the length of a partial transversal in a latin square, *J. Combin. Theory Ser. A* **115** (2008), 1103–1113.

[74] J. D. Horton, Orthogonal starters in finite abelian groups, *Discrete Math.* **79** (1990), 265–278.

[75] J. Hsiang, D. F. Hsu and Y. P. Shieh, On the hardness of counting problems of complete mappings, *Disc. Math.* **277** (2004), 87–100.

[76] J. Hsiang, Y. Shieh and Y. Chen, The cyclic complete mappings counting problems, *PaPS: Problems and problem sets for ATP workshop in conjunction with CADE-18 and FLoC 2002*, Copenhagen, (2002).

[77] L. Hu and X. Li, Color degree condition for large heterochromatic matchings in edge-colored bipartite graphs, http://arxiv.org/abs/math.CO/0606749.

[78] D. M. Johnson, A. L. Dulmage and N. S. Mendelsohn, Orthomorphisms of groups and orthogonal latin squares I, *Canad. J. Math.* **13** (1961), 356–372.

[79] D. Jungnickel, "Latin squares, their geometries and their groups. A survey", in *Coding theory and design theory. Part II. Design theory* (Ed. Dijen Ray-Chaudhuri), Springer-Verlag, New York, 1990 (pp. 166–225).

[80] A. D. Keedwell, Sequenceable groups, generalized complete mappings, neofields and block designs, Combinatorial mathematics X (Adelaide, 1982), 49–71, Lecture Notes in Math. **1036**, Springer, Berlin, 1983.

[81] A. E. Kézdy and H. S. Snevily, Distinct sums modulo n and tree embeddings, *Combin. Probab. Comput.* **11** (2002), 35–42.

[82] R. Killgrove, C. Roberts, R. Sternfeld, R. Tamez, R. Derby and D. Kiel, Latin squares and other configurations, *Congr. Numer.* **117** (1996), 161–174.

[83] K. K. Koksma, A lower bound for the order of a partial transversal in a latin square, *J. Combinatorial Theory* **7** (1969), 94–95.

[84] I. N. Kovalenko, Upper bound for the number of complete maps, *Cybernet. Systems Anal.* **32** (1996), 65–68.

[85] N. Yu. Kuznetsov, Applying fast simulation to find the number of good permutations, *Cybernet. Systems Anal.* 43 (2007), 830–837.

[86] N. Yu. Kuznetsov, Estimating the number of good permutations by a modified fast simulation method, *Cybernet. Systems Anal.* 44 (2008), 547–554.

[87] C. F. Laywine and G. L. Mullen, *Discrete mathematics using latin squares*, Wiley, New York, 1998.

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

[89] B. M. Maenhaut and I. M. Wanless, Atomic latin squares of order eleven, *J. Combin. Des.* **12** (2004), 12–34.

[90] E. Maillet, Sur les carrés latins d'Euler, *Assoc. Franc. Caen.* **23** (1894), 244–252.

[91] H. B. Mann, The construction of orthogonal latin squares, *Ann. Math. Statistics* **13** (1942), 418–423.

[92] H. B. Mann, On orthogonal latin squares, *Bull. Amer. Math. Soc.* **50** (1944), 249–257.

[93] B. D. McKay, A. Meynert and W. Myrvold, Small latin squares, quasigroups and loops, *J. Combin. Des.* **15** (2007), 98–119.

[94] B. D. McKay, J. C. McLeod and I. M. Wanless, The number of transversals in a latin square, *Des. Codes Cryptogr.* **40** (2006), 269–284.

[95] B. D. McKay and I. M. Wanless, A census of small latin hypercubes, *SIAM J. Discrete Math.* **22** (2008), 719–736.

[96] H. Niederreiter and K. H. Robinson, Bol loops of order pq, *Math. Proc. Cambridge Philos. Soc.* **89** (1981), 241–256.

[97] H. Niederreiter and K. H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc. Ser. A* **33** (1982), 197–212.

[98] L. J. Paige, Complete mappings of finite groups, *Pacific J. Math.* **1** (1951), 111–116.

[99] E. T. Parker, Pathological latin squares, *Proceedings of symposia in pure mathematics*, Amer. Math. Soc. (1971), 177–181.

[100] K. Pula, Products of all elements in a loop and a framework for non-associative analogues of the Hall-Paige conjecture, *Electron. J. Combin.* **16** (2009), R57.

[101] K. Pula, A generalization of plexes of latin squares, *Disc. Math.* **311** (2011), 577–581.

[102] J. Quistorff, A survey on packing and covering problems in the Hamming permutation space, *Electron. J. Combin.* **13** (2006), A1.

[103] I. Rivin, I. Vardi and P. Zimmerman, The n-Queens Problem, *Amer. Math. Monthly* **101** (1994), 629–639.

[104] H. J. Ryser, Neuere Probleme der Kombinatorik, *Vortrage über Kombinatorik Oberwolfach*, 24–29 Juli (1967), 69–91.

[105] Y. P. Shieh, *Partition strategies for #P-complete problem with applications to enumerative combinatorics*, PhD thesis, National Taiwan University, 2001.

[106] Y. P. Shieh, private correspondence, (2006).

[107] Y. P. Shieh, J. Hsiang and D. F. Hsu, On the enumeration of abelian K-complete mappings, *Congr. Numer.* **144** (2000), 67–88.

[108] P. W. Shor, A lower bound for the length of a partial transversal in a latin square, *J. Combin. Theory Ser. A* **33** (1982), 1–8.

[109] H. S. Snevily, The Cayley addition table of $\mathbb{Z}_n$, *Amer. Math. Monthly* **106** (1999), 584–585.

[110] D. S. Stones and I. M. Wanless, Compound orthomorphisms of the cyclic group, *Finite Fields Appl.* **16** (2010), 277–289.

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

[112] S. K. Stein, Transversals in rectangular arrays, *Amer. Math. Monthly* **117** (2010), 424–433.

[113] S. K. Stein and S. Szabó, The number of distinct symbols in sections of rectangular arrays, *Discrete Math.* **306** (2006), 254–261.

[114] Z.-W. Sun, An additive theorem and restricted sumsets, *Math. Res. Lett.* **15** (2008), 1263-1276.

[115] A. D. Thomas and G. V. Wood, *Group tables*, Shiva Mathematics Series 2, Shiva Publishing, Nantwich, 1980.

[116] I. Vardi, *Computational Recreations in Mathematics*, Addison-Wesley, Redwood City, CA, 1991.

[117] M. Vaughan-Lee and I. M. Wanless, Latin squares and the Hall-Paige conjecture, *Bull. London Math. Soc.* **35** (2003), 1–5.

[118] G. H. J. van Rees, Subsquares and transversals in latin squares, *Ars Combin.* **29**B (1990), 193–204.

[119] D. Q. Wan, On a problem of Niederreiter and Robinson about finite fields, *J. Austral. Math. Soc. Ser. A* **41** (1986), 336–338.

[120] I. M. Wanless, A generalisation of transversals for latin squares, *Electron. J. Combin.* **9** (2002), R12.

[121] I. M. Wanless, Diagonally cyclic latin squares, *European J. Combin.* **25** (2004), 393–413.

[122] I. M. Wanless, Atomic Latin squares based on cyclotomic orthomorphisms, *Electron. J. Combin.* **12** (2005), R22.

[123] I. M. Wanless, Transversals in latin squares, *Quasigroups Related Systems* **15** (2007), 169–190.

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

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

[126] D. E. Woolbright, An $n \times n$ latin square has a transversal with at least $n - \sqrt{n}$ distinct symbols, *J. Combin. Theory Ser. A* **24** (1978), 235–237.

School of Mathematical Sciences
Monash University
Vic 3800, Australia
ian.wanless@monash.edu