1-1-2011

Approximate Transversals of Latin Squares

Jon Kyle Pula
University of Denver, jpula@du.edu

Approximate Transversals of Latin Squares

A Dissertation

Presented to

the Faculty of Natural Sciences and Mathematics

University of Denver

---

in Partial Fulfillment

of the Requirements for the Degree

of Doctor of Philosophy

---

by

Jon Kyle Pula

June 2011

Advisor: Petr Vojtěchovský

Author: Jon Kyle Pula
Title: Approximate Transversals of Latin Squares
Advisor: Petr Vojtěchovský
Degree Date: June 2011

Abstract

A latin square of order n is an $n \times n$ array whose entries are drawn from an n-set of symbols such that each symbol appears precisely once in each row and column. A transversal of a latin square is a subset of cells that meets each row, column, and symbol precisely once.

There are many open and difficult questions about the existence and prevalence of transversals. We undertake a systematic study of collections of cells that exhibit regularity properties similar to those of transversals and prove numerous theorems about their existence and structure. We hope that our results and methods will suggest new strategies for the study of transversals.

The main topics we investigate are partial and weak transversals, weak orthogonal mates, integral weight functions on the cells of a latin square, applications of Alon's Combinatorial Nullstellensatz to latin squares, and complete mappings of finite loops.

Acknowledgements

I thank both family and colleagues for their support over the years. Their insights and distractions have made work possible and life enjoyable.

Firstly, I thank Melissa, whose cheerleading and partnership have been unequaled and unwavering. I thank my parents and siblings for their guidance and support. Among mathematicians, none have been so influential as Petr Vojtěchovský, my advisor at the University of Denver, and Ian Wanless, my research collaborator and host at Monash University. I also owe a great debt to the faculty, staff, and students of the mathematics department at the University of Denver, including Liane Beights, Michael Kinyon, Don Oppliger, Dan Daly, Aditya Nagrath, Jonathan Von Stroh, and Brett Werner.

The following organizations have been crucial in providing financial support for my work: the University of Denver's Mathematics Department and Office of Graduate Studies, the Australian-American Fulbright Commission, the National Science Foundation's East Asia and Pacific Summer Institutes Program, the American Mathematical Society, and the Australian Mathematical Society.

Table of Contents

Chapter 1

Introduction

This dissertation is about transversals of latin squares. More precisely, it is about collections of cells that are, in some sense, close to forming transversals. We refer to such collections as approximate transversals and prove theorems about their existence and structure.

A *latin square* of order n is an $n \times n$ array whose entries are drawn from an n-set of symbols such that no row or column contains a repeated entry. As the particular set of symbols used is not important, we will typically use the symbol set $[n] := \{1, \ldots, n\}$. Figure 1.1 depicts a latin square of order 9.

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

Figure 1.1: A latin square of order 9

We are primarily interested in collections of cells that have certain regularity properties. In particular, a *transversal* of a latin square is a subset of cells that meets each row, column, and symbol precisely once. While experimental evidence suggests that almost all latin squares have transversals, Euler showed that, for every even order n, there is a latin square of order n that has no transversal, namely, the Cayley table of $(\mathbb{Z}_{2n}, +)$ [21]. It is not known whether all latin squares of odd order have transversals, though the following conjecture has been attributed to Ryser [39].

Conjecture 1.0.1. *Every latin square of odd order has a transversal.*

Despite a diversity of attributions found in the literature, we will follow the convention of referring to Conjecture 1.0.1 as Ryser's conjecture.

There are many open and difficult questions about the existence and prevalence of transversals. We undertake a systematic study of collections of cells that exhibit regularity properties similar to those of transversals and prove numerous theorems about their existence and structure. We hope that our results and methods will suggest new strategies for the study of transversals.

In §1.1, we present the main concepts and definitions used throughout this document. In §1.2, we provide a brief summary of our main results.

1.1 Main Concepts and Definitions

We work with 2-dimensional arrays, each of whose cells contains either a single symbol or is empty. A row or column of an array is said to be *latin* if it does not contain any symbol twice. A latin row or column may contain more than one empty cell. A *partial latin square of order* n is an $n \times n$ array with latin

rows and columns and containing at most n distinct symbols. A partial latin square that contains no empty cells is called a *latin square*. The variable n will be used extensively and exclusively to refer to the order of a square array or latin square. The standard references for latin squares include the two texts of Dénes and Keedwell [13, 14] and the more recent text of Laywine and Mullen [30].

We will refer to the cell in row r and column c of an array either by writing (r, c) or (r, c, s), if it happens that cell (r, c) contains symbol s. In this way, we may also think of an array as a set of triples corresponding to its collection of non-empty cells. We will refer to the contents of the cell (r, c) of an array L by writing $L(r, c)$. For a set of cells C, we denote by $L(C)$ the set of symbols that appear in some cell in C.

Because we are interested in the combinatorial properties of latin squares, we will work with the coarsest of equivalences. For our purposes, two latin squares are equivalent if they agree up to some exchange of symbol sets, permutations of rows and columns, and permutations of the roles of rows, columns, and symbols. For latin squares, each such equivalence class is called a *main class*. With the exception of Chapter 7, in which we take a more algebraic perspective, we will deal almost exclusively with properties of latin squares that are main class invariant. The one other exception is in our study of weak transversals and weak orthogonal mates. In these cases, symbols are treated somewhat differently than rows and columns and thus it is no longer natural to permute the roles of rows, columns, and symbols.

A *diagonal* of an $n \times n$ array is a collection of n cells from distinct rows and columns. There is a natural bijection between diagonals and permutations in

$\mathrm{Sym}(n)$ by associating a permutation θ with the diagonal $\{(r, r^\theta) : 1 \leq r \leq n\}$. In this way, when there is no risk of confusion, we will at times treat θ as if it were a diagonal. We may, for example, say that θ contains the symbol s when there is a cell in the diagonal associated to θ that contains the symbol s. We will also say that a diagonal θ contains the cell (r, r^θ). The unique diagonal containing every occurrence of a fixed symbol s in a latin square is called the *symbol pattern of* s. The *main diagonal* is the diagonal associated to the identity permutation. The *deficit* of a diagonal refers to the difference between n and the number of distinct symbols contained in it. A *weak transversal* is a diagonal in which no symbol appears three times.

A *partial transversal* of a latin square of order n is a subset of cells incident with no row, column, or symbol more than once. The *length* or *size* of a partial transversal is its cardinality while its *deficit* is the number of rows (or columns or symbols) that it misses, i.e., the difference between n and its length. We refer to the minimum deficit among all partial transversals of a latin square as the *minimum deficit* of the square itself. Partial transversals are arguably the most natural candidate for an approximate transversal.

A k-plex of a latin square of order n is a collection of kn cells that meets each row, column, and symbol precisely k times. The terms *transversal* and *duplex* refer to k-plexes for $k = 1$ and $k = 2$, respectively. The first systematic study of k-plexes for $k \geq 2$ is due to Wanless [46], but numerous other works have since appeared [9, 17, 18, 19]. The most comprehensive and up-to-date reference on transversals of latin squares is due to Wanless [47].

1.2 Summary of Main Results

In Chapter 2, we focus on partial transversals of square arrays with latin rows and columns and on partial transversals of latin squares of small order. In Proposition 2.2.1, we show that every $n \times n$ array with latin rows and columns and no more than k empty cells in each row and column contains a partial transversal of length $n - \sqrt{n} - k + 1$. The importance of allowing empty cells is that the result can be applied iteratively to show the existence of mutually disjoint partial transversals. In §2.4, we describe an algorithm we developed to confirm that all latin squares of order 10 and 12 have partial transversals of lengths 9 and 10, respectively. The previous best known results were 8 and 9, respectively.

In Chapter 3, we study *weak transversals*. It is conjectured that every latin square can be partitioned into weak transversals. Our main result in this direction is Proposition 3.2.3: every latin square of order n contains about $\frac{1}{11}n$ mutually disjoint weak transversals. This result represents a major improvement given that it was previously only known that every latin square contains at least one weak transversal. In Proposition 3.4.1, we prove the surprising result that any cell of a latin square contained in a partial transversal of deficit d is contained in a weak transversal of deficit at most d. It follows that every latin square is covered by weak transversals and that the minimum deficit of any latin square is realized by some weak transversal.

In Chapter 4, we introduce the concept of weak orthogonality between pairs of latin squares. We generalize the famous result that a set of mutually orthogonal latin squares of order n can have size no larger than $n - 1$ and

construct complete sets of mutually weakly orthogonal latin squares for several non-prime power orders. For example, in contrast to the classic result that there are no pairs of orthogonal latin squares of order 6, we present a collection of 20 mutually weakly orthogonal latin squares of order 6.

In Chapter 5, we study integral weight functions on the cells of a latin square that have constant row, column, and symbol sums. We call such a function a *k-weight* when the constant row, column, and symbol sum is k. In Proposition 5.4.1, we show that every latin square contains a 2-weight and that all latin squares of odd order contain 1-weights. In Proposition 5.4.2, we show that many latin squares have no k-weights for any odd k.

In Chapter 6, we investigate applications of Alon's Combinatorial Nullstellensatz to the study of latin squares. In Proposition 6.3.2, for example, we show that every latin square of order $n \equiv 1 \mod p$ has a proper subset of cells that meets each row, column, and symbol 1 modulo p times.

In Chapter 7, we take a more algebraic perspective by studying complete mappings of finite loops. Here we develop and partially prove a non-associative analogue of the famous Hall-Paige conjecture for finite groups. We also prove a generalization of the Dénes-Hermann theorem and a weak form of the Hall-Paige conjecture.

Many of the results in Chapters 2, 3, 4, and 6 represent joint work with Ian Wanless of Monash University. Our collaboration was generously supported by the National Science Foundation's East Asia and Pacific Summer Institutes Program and the Australian-American Fulbright Commission. The remaining content, Chapters 5 and 7, has been published in peer-reviewed, international scholarly journals as [36] and [37], respectively.

Chapter 2

Partial Transversals

2.1 Background

The most important and natural questions one might ask about partial transversals are when and whether large ones exist. The following well-known conjecture proposes a simple answer. We follow the convention of referring to it as Brualdi's conjecture, though the literature records a variety of attributions including Brualdi [13, p.103], Ryser [20], and Stein [42].

Conjecture 2.1.1. *Every latin square of order n contains a partial transversal of length $n-1$.*

The conjecture is currently known to hold for $n \leq 9$ through the use of a brute force check of each main class [32]. In §2.4, we discuss computational methods we have employed to confirm the conjecture for $n = 10$ as well.

The best general results concerning Brualdi's conjecture give lower bounds on the maximum length among all partial transversals of latin squares of order n. The two most notable of such results are the following.

Proposition 2.1.2 (Brouwer *et al.* [5], Woolbright [50]). *Every latin square of order n contains a partial transversal of length at least $n - \sqrt{n}$.*

Proposition 2.1.3 (Shor [40], Hatami and Shor [28]). *Every latin square of order n contains a partial transversal of length at least $n - 11.053(\log n)^2$.*

While the latter of these bounds beats the former asymptotically, this fact is not realized until $n \geq 52{,}962{,}006$. In particular, to the extent we are interested in partial transversals of relatively small latin squares, the latter result is of little use. (The computation of the above value of n uses a slightly stronger though less compact form of Proposition 2.1.2.)

In this chapter, we present two extensions of the methods used to prove the above propositions. In §2.2, we extend the proof-method of Proposition 2.1.2 to establish an analogous result for square matrices with latin rows and columns and a bounded number of empty cells in each row and column. Our extension becomes particularly useful in Chapter 3, where we use it repeatedly to show the existence of sets of mutually disjoint weak transversals and weak k-plexes.

In §2.4, we use the central idea in Shor's proof of Proposition 2.1.3 to develop an algorithm we have used to confirm Brualdi's conjecture for $n = 10$.

2.2 Partial Transversals and Empty Cells

Recall that a row or column of a 2-dimensional array is said to be *latin* if it does not contain any repeated symbols. In our usage, a latin row or column may have multiple empty cells.

Proposition 2.2.1. *Suppose that L is an $n \times n$ array whose rows and columns are all latin and none contain more than k empty cells. Then L has a partial transversal of length t for some t satisfying $(n-t)(n-t-k) \leq t$. For $k \geq 1$, it follows that*

$$n - \sqrt{n} - k + 1 \leq t.$$

Proof. Let t be the maximum length among all partial transversals of L. Without loss of generality, we may assume that $L(i,i) = i$ for $i \in [t]$. We think of L as being partitioned into blocks A, B, C, and D as in Figure 2.1.

	1 t	t+1 n
1 t	A	B
t+1 n	C	D

Figure 2.1: General layout of L used in Proposition 2.2.1.

We call the symbols $[t] = \{1, \ldots, t\}$ small and $[n] \setminus [t] = \{t+1, \ldots, n\}$ large and denote the latter set by M. Since t is maximal, block D contains only small symbols and empty cells.

We define a sequence of sets from whose sizes we may deduce some information about t. Let S_0 be the empty set. Set $S_i = \{j : L(j, t+i) \in M \cup S_{i-1}\}$ for $1 \leq i \leq n-t$. If $L(j, t+i)$ is empty, then $j \notin S_i$.

We claim that each S_i consists entirely of small symbols. The claim is vacuously true for S_0. For S_1, the claim follows from the fact that block D cannot contain any large symbols. Working toward a contradiction, let S_i is the first of our sets to violate the claim by containing a large symbol $j \in S_i$.

By definition, $L(j, t+i) \in M \cup S_{i-1}$. Since D contains no large symbols, it follows that $L(j, t+i) \in S_{i-1}$. Set $m_0 := L(j, t+i) \in S_{i-1}$ and $m_l = L(m_{l-1}, t+i-l)$ for $1 \leq l \leq p$ where p is the first index such that $s := L(m_p, t+i-p-1) \in M$. Note that such a p must exist since the first non-empty set S_ϵ has the property that $L(S_\epsilon \times \{t+\epsilon\}) \subseteq M$. The reader should have a picture such as Figure 2.2 in mind.

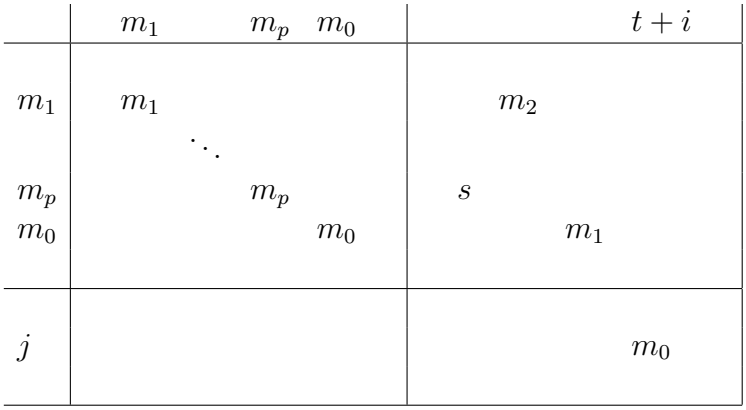

Figure 2.2: An illustration of the $(m_0, \ldots, m_p)$ sequence constructed in Proposition 2.2.1.

We will use the sequence $(m_0, \ldots, m_p)$ to construct a partial transversal of length $t+1$. First suppose that the elements in our sequence are all distinct and consider Figure 2.3. Under this assumption, the cells in the left-hand column are distinct cells in the original partial transversal and the cells in the right-hand column are distinct cells not in the original transversal. Furthermore, swapping the left-hand cells for the right-hand cells produces a partial transversal of length $t+1$, a contradiction.

Now suppose that $m_a = m_b$ for some $0 \leq a < b \leq p$. In this case, the swap described above is no longer valid as we would need to remove cell (m_a, m_a) twice. We may, however, simply discard the portion of the swap corresponding

Old Cells	Symbol	New Cells
(m_0, m_0)	m_0	$(j, t+i)$
(m_1, m_1)	m_1	$(m_0, t+i-1)$
(m_2, m_2)	m_2	$(m_1, t+i-2)$
	$\vdots$	
(m_{p-2}, m_{p-2})	m_{p-2}	$(m_{p-3}, t+i-p+2)$
(m_{p-1}, m_{p-1})	m_{p-1}	$(m_{p-2}, t+i-p+1)$
(m_p, m_p)	m_p	$(m_{p-1}, t+i-p)$
–	s	$(m_p, t+i-p-1)$

Figure 2.3: Old and new cells paired according to their common symbol. The final row contains only a new cell since its corresponding symbol does not occur in the original partial transversal.

to the subsequence $(m_{a+1}, \ldots, m_b)$. Figure 2.4 depicts this portion of the table.

Old Cells	Symbol	New Cells
(m_a, m_a)	m_a	$(m_{a-1}, t+i-a)$
(m_{a+1}, m_{a+1})	m_{a+1}	$(m_a, t+i-a-1)$
	$\vdots$	
(m_{b-1}, m_{b-1})	m_{b-1}	$(m_{b-2}, t+i-b+1)$
(m_a, m_a)	m_a	$(m_{b-1}, t+i-b)$
(m_{b+1}, m_{b+1})	m_{b+1}	$(m_a, t+i-b-1)$

Figure 2.4: In the case that $m_a = m_b$ for some $a < b$, we will discard the rows corresponding to the subsequence $(m_{a+1}, \ldots, m_b)$ and keep only the first and last rows in the above table.

In this way, we pass to a subsequence with fewer repetitions. Iterating this reduction we arrive at a non-empty subsequence with no repetitions. With this final subsequence, we may apply the swap to construct a partial transversal of length $t+1$, a contradiction. Therefore, S_i contains only small symbols for $0 \leq i \leq n-t$.

We now show that $|S_i| \geq i(n-t-k)$. The claim holds trivially for $i = 0$. Suppose that $|S_i| \geq i(n-t-k)$ holds and consider $|S_{i+1}|$. Among the cells in column $t+i+1$, each cell containing either a large symbol or a symbol from

S_i will contribute 1 to $|S_{i+1}|$. Of the n cells in column $t+i+1$, there are at most $t+k-|S_i|$ cells that are neither large nor from S_i (since $S_i \subseteq [t]$). Thus, we have that

$$\begin{aligned} |S_{i+1}| &\geq n-t-k+|S_i| \\ &\geq n-t-k+i(n-t-k) \\ &= (i+1)(n-t-k). \end{aligned}$$

We have thus established that $|S_{n-t}| \geq (n-t)(n-t-k)$ but also that $|S_{n-t}| \leq t$ since $S_{n-t} \subseteq [t]$. Therefore, $(n-t)(n-t-k) \leq t$. Solving for t, we find that

$$\begin{aligned} t &\geq n - \frac{1}{2}k - \frac{1}{2}\sqrt{(k-1)^2+4\,n} + \frac{1}{2} \\ t &\geq n - \frac{1}{2}k - \frac{1}{2}|k-1| - \sqrt{n} + \frac{1}{2} \\ &= n - \sqrt{n} - k + 1. \end{aligned}$$

In this final calculation we have used the assumption that $k \geq 1$. If $k = 0$, we recover the original result of [5, 50] that $t \geq n - \sqrt{n}$. □

2.3 Using Only Prescribed Symbols

It is at times desirable to have a partial transversal that consists precisely of a set of prescribed symbols. In particular, we will use the following proposition in §3.3 to establish the existence of weak k-plexes.

Proposition 2.3.1. *Suppose that L is an $n \times n$ latin array and that D is a d-subset of symbols that each appear at least k times in L. Then L contains a partial transversal consisting precisely of the symbols from D so long as $d < \frac{1}{2}k + 1$.*

Proof. Let $D = \{s_1, \ldots, s_d\}$. Fix any cell (r_1, c_1) such that $L(r_1, c_1) = s_1$. Notice that each symbol in D can occur at most twice among row r_1 and column c_1. Therefore each symbol in D occurs at least $k - 2$ times outside of row r_1 and column c_1. Continuing in this way, once we have selected a partial transversal

$$\{(r_i, c_i) : L(r_i, c_i) = s_i \text{ and } 1 \leq i \leq t\},$$

each symbol in D appears at least $k - 2t$ times outside of the previously selected rows and columns. Therefore, to achieve $t = d$, we require only that $k - 2(d - 1) > 0$. □

We comment that Ryser's conjecture implies that the above result is much weaker than the truth for n odd since any D subset of symbols could be realized as a partial transversal simply by discarding the appropriate cells from a transversal. The result is likely far from the truth for the even case as well.

2.4 Partial Transversals of Small Latin Squares

Neither Proposition 2.1.2 nor Proposition 2.1.3 tell us much about the maximum length of partial transversals of small latin squares. For orders $n \leq 9$, the number of latin squares of order n is small enough that it is computation-

ally feasible to naively check that all such squares have partial transversals of length at least $n-1$. For larger orders, we must rely either upon theoretical lower bounds or more advanced computational methods. Figure 2.5 presents the known lower bounds for partial transversals of small latin squares based on several general results. As discussed above, we have omitted the $n - 11.053(\log n)^2$ result because it is only useful for very large n. The bounds presented in the first five rows are from [29], [16], [45], [5, 50], and [32], respectively.

n		7	8	9	10	11	12	13	14	15	16	17
$(2n+1)/3$		5	6	7	7	8	9	9	10	11	11	12
$\min(3n/4, n-2)$		5	6	7	8	9	9	10	11	12	12	13
$(9n-15)/11$		5	6	6	7	8	9	10	11	11	12	13
$n - \sqrt{n}$		5	6	7	8	9	9	10	11	12	13	14
Brute force		7	7	9	Computationally Infeasible							
Our Algorithm		6	7	8	**9**	9	**10**					
$n - \sqrt{n}$	$(k=1)$	5	6	6	7	8	9	10	11	12	12	13
	$(k=2)$	4	5	6	7	8	8	9	10	11	12	13
	$(k=3)$	4	4	5	6	7	8	9	10	10	11	12
	$(k=4)$	3	4	5	5	6	7	8	9	10	11	12
	$(k=5)$	2	3	4	5	6	6	7	8	9	10	11

Figure 2.5: Known lower bounds for maximum lengths of partial transversals among latin squares of order n. Our data for the $n - \sqrt{n}$ row comes from the slightly stronger bound of $n + 1/2 - \sqrt{n + 1/4}$. The bottom five rows record the lower bounds arising from Proposition 2.2.1 for latin squares with no more than k empty cells in each row and column.

We now describe an algorithm inspired by the method employed in [40] and report our success in using this method to improve the known lower bounds

for orders $n = 10$ and 12. In particular, we found that all such squares have partial transversals of lengths 9 and 10, respectively. The first of these results confirms Brualdi's conjecture for $n = 10$.

2.4.1 Shor's # Operation

The proof of Proposition 2.1.3 is based on two clever and well executed ideas: (1) a simple operation, called #, to move between two diagonals of a latin square that contain the same underlying symbol set and (2) a counting argument showing that this operation, when applied in all possible ways, must reach a large number of cells. It follows that the fixed underlying symbol set must be capable of filling a large number of cells and thus must contain a large number of symbols. Proposition 2.1.3 makes this argument precise and thereby shows that a partial transversal of maximum length must have length at least $n - 11.053(\log n)^2$.

We now describe the # operation used in [28] and [40]. Given L, a latin square of order n, and a diagonal π, set $S(\pi) := \{L(i, i^\pi) : 1 \leq i \leq n\}$. If $|S(\pi)| \leq n - 2$, then there are at least 3 pairs of cells in π with the property that the pair could be removed without lowering the total number of distinct symbols among the remaining $n - 2$ cells. If such a pair falls in rows r_1 and r_2, then consider the diagonal $\pi' := \pi(r_1 r_2)$. The diagonals π and π' agree on the $n - 2$ rows other than r_1 and r_2 and $S(\pi) \subseteq S(\pi')$. We will follow [40] in referring to the operation that sends π to π' as the # operation. Of course, the operation is a function not only of π but also of r_1 and r_2.

At first glance, the operation # seems arbitrarily restrictive in that it only allows the swapping of two rows at a time where one might hope to exploit a

more ambitious swap. For a diagonal $\pi \in \mathrm{Sym}(n)$, let I be a k-subset of $[n]$ such that

$$S(\pi) = \{L(i, i^\pi) : i \in [n]\} = \{L(i, i^\pi) : i \in [n] \setminus I\}.$$

That is, we may remove all the cells in π from rows indexed by I without losing any symbols. For any $\rho \in \mathrm{Sym}(I)$, we call the operation that sends π to $\pi\rho$ a *k-swap*.

Lemma 2.4.1. *Suppose that π has minimal deficit. Any k-swap on π can be decomposed into a sequence of 2-swaps, i.e. # operations.*

Proof. Consider a k-swap corresponding to $I = \{1, \ldots, k\}$ and $\rho \in \mathrm{Sym}(I)$. We may assume that π is the identity map, i.e. the main diagonal of L. Note that the symbols $\{s_i : 1 \leq i \leq k\}$ each occur at least once in $\{s_i : k{+}1 \leq i \leq n\}$ and that this fact remains true if we apply any 2-swap to π that involves only the first k rows. Otherwise, we would have introduced a new symbol, contradicting the minimality of the deficit of π.

We are, therefore, free to apply any sequence of 2-swaps we like among rows $\{1, \ldots, k\}$. In particular, if $\rho = \rho_1 \cdots \rho_m$ where each ρ_i is a 2-cycle on I, then $\pi\rho = \pi\rho_1 \cdots \rho_m$ and each operation of the right is a valid 2-swap. □

2.4.2 Our # Algorithm

From Lemma 2.4.1, we know that it suffices to focus on the # operation rather than more general k-swaps, at least among minimally deficient diagonals. With this fact in mind, we designed an algorithm based on the # operation to test Conjecture 2.1.1 for small values of n.

For $2 \leq k \leq n$, our algorithm attempts to determine whether there exists a latin square of order n with minimal deficit k. The algorithm follows a basic branching structure that, informally speaking, mimics the way one might iteratively apply the # operation to an "empty latin square." The branching occurs when the algorithm must choose which symbol is placed in a particular cell.

The algorithm begins with an $n \times n$ array whose main diagonal contains the symbols $[n-k]$ and has no empty cells as in the top-left square in Figure 2.6. All off-diagonal cells begin empty. The variable `CurrentDiagonal` is initialized to be the main diagonal. The algorithm first identifies all possible # operations that can be applied to `CurrentDiagonal`. It then records a list of the corresponding diagonals that would be achieved by these # operations. Each off-diagonal cell contained in one of these diagonals is marked as visited. Figure 2.6 depicts visited cells using the "$\circ$" symbol. The key observation is that all cells marked as visited must contain a symbol in $[n-k]$. The algorithm then selects one of the # operations (or, equivalently, one of the diagonals it recorded) to be the new value of `CurrentDiagonal`.

The algorithm should now explore # operations from `CurrentDiagonal`. Since `CurrentDiagonal` contains two empty cells, a choice must be made as to which symbols they will contain. It is this choice that forces the branching of our algorithm. The algorithm computes all possible choices for this pair of symbols (excluding symbols that have already appeared in the given row or column) and branches to explore each of these cases.

Since `CurrentDiagonal` now contains no empty cells, the algorithm can identify all possible # operations from this diagonal. The algorithm adds to its

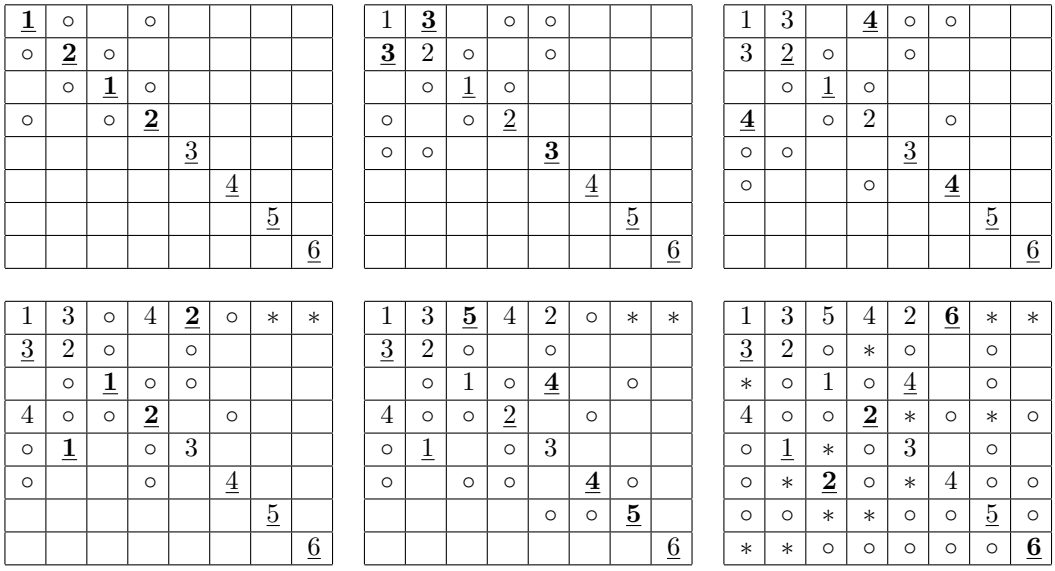

Figure 2.6: To determine whether there can exist a latin square of order 8 with minimum deficit of 2, our algorithm starts with an $n \times n$ array containing a single diagonal of deficit 2, as in the top-left square. Starting from the underlined diagonal, the # operation could potentially visit any of the ∘-cells by swapping pairs of cells containing bold symbols.

list of diagonals any of these new diagonals that contain an empty cell. It again marks all such cells as visited. The top-middle square in Figure 2.6 depicts this step in the algorithm. The underlined diagonal corresponds to the value of `CurrentDiagonal`. The algorithm now selects a new `CurrentDiagonal` from its list. If `CurrentDiagonal` no longer contains an empty cell, it is discarded and a new `CurrentDiagonal` is selected.

Iterating in this way, with each new value of `CurrentDiagonal`, we will be placing symbols in one or two previously empty cells. Such a process must terminate within $n(n-k-1)$ iterations since by that time the square would contain at least $n(n-k)$ symbols from $[n-k]$. We either reach a point where there are no viable symbols to be placed in an empty cell contained in one of our diagonals or we have no diagonals containing an empty cell.

In the first case, we have uncovered a contradiction in either an earlier symbol choice or in our original hypothesis that k was the minimal deficit. The algorithm now backtracks to explore a different branch of the search until all branches have been explored.

In the case that none of the our diagonals contains an empty cell, we have constructed a partial latin square of order n on a set of $n - k$ symbols whose main diagonal has deficit k. In the most interesting case, this square would be closed under any sequence of # operations applied to the main diagonal, though our algorithm does not guarantee this to be the case. We add this partial latin square to a list of problem cases and backtrack to explore the next branch in our search.

Let $\#(n, k)$ be the list of problem cases generated by the algorithm. If $\#(n, k) = \emptyset$, it follows that there is no latin square of order n with minimal deficit k. This is the expected output of the algorithm, and it so happens that in our tests the algorithm has never generated any other outcome.

We do need to address two points of ambiguity in the algorithm as described above. Firstly, there are several inequivalent options for how to construct the original main diagonal. It must contain the symbols $[n - k]$ but, in principle, one should run the algorithm against all of the possible multiplicities that could occur for each symbol. Put another way, there should be a separate case for each unordered partition of k corresponding to how the "extra" symbols are distributed. However, a result from Chapter 3 reduces this problem to a single case. By Proposition 3.4.1, we know that if L has a minimal deficit of k, then it contains a weak transversal of deficit k. We may, therefore, run the algorithm assuming that the main diagonal is a weak transversal.

A second point of ambiguity concerns the way in which we select the next `CurrentDiagonal` as this choice may alter $\#(n, k)$. We experimented with several criterion to choose the next diagonal. The heuristic we found most effective was that it is better to fill up rows with symbols rather than distribute the same number of symbols throughout the square. Therefore, we chose to select diagonals containing empty cells from the highest rows available. Figure 2.6 depicts this choice as the number of symbols in the first row of each square grows with each step of the algorithm.

As an illustration, we demonstrate part of this routine in Figure 2.6 using $n = 8$ and $k = 2$. In this example, visited cells are marked with the $\circ$ symbol and cells that are known to contain a symbol from $[n] \setminus [n-k]$ are marked with the $*$ symbol. Such cells are identified by the algorithm as soon as $n - k$ cells have been either filled or at least marked as visited in a given row or column. The underlined diagonal corresponds to the value of `CurrentDiagonal`.

We have used our algorithm to confirm that every latin square of order 10 and 12 has a partial transversal of length 9 and 10, respectively. In particular, working in conjunction with the theoretical bounds from Figure 2.5, we found that $\#(10, 8) = \emptyset$ and $\#(12, 9) = \emptyset$. We conducted these calculations mostly as a proof of concept, without much concern for the efficiency of our implementation or on the computational power of the machine employed. Our data was collected using an implementation of the algorithm in the computer algebra system GAP [25]. We expect that an optimized implementation would generate even stronger results.

Chapter 3

Weak Transversals

3.1 Background

In this chapter, we consider sets of cells that result from weakening the definition of transversal from requiring that every symbol be represented precisely once to requiring that no symbol be represented more than twice. In particular, a *weak transversal* is a diagonal of a latin square that contains no symbol more than twice.

We first became interested in weak transversals because of their connection to the following conjecture, due independently to Rodney [11, p.105] and Wanless [46].

Conjecture 3.1.1. *Every latin square can be partitioned into a set of transversals and duplexes.*

Recall that a duplex is another term for 2-plex, a collection of $2n$ cells that meets each row, column, and symbol twice. This conjecture appears to be quite strong since it implies both that every latin square of odd order has a

transversal (Ryser's conjecture) and that every latin square has a duplex (often referred to as Rodney's conjecture). We were, therefore, led to introduce and consider the following weaker conjecture.

Conjecture 3.1.2. *Every latin square can be partitioned into a set of weak transversals.*

It is not difficult to see how Conjecture 3.1.1 implies Conjecture 3.1.2. Any duplex belonging to such a partition can always be divided into two weak transversals. Conjecture 3.1.2 also has a natural interpretation in the area of mutually orthogonal latin squares. From that perspective, it purports that every latin square has a weak orthogonal mate, which we define and discuss in greater detail in Chapter 4.

Little was previously known about the existence and structure of weak transversals. In fact, the only two references of which we are aware are due to Brualdi and Ryser [6] and Cameron and Wanless [10]. Both works contain the following proposition.

Proposition 3.1.3. *Every latin square contains a weak transversal.*

While [6] predates [10] by 14 years, it was unknown to the latter authors and contains an incomplete proof. In §3.4, we extend the proof-method employed in [10] to give the stronger result that if a cell is contained in a partial transversal of deficit d, then it is contained in a weak transversal of deficit at most d. Two interesting facts follow immediately. Every cell is contained in a weak transversal, and there is a weak transversal with as many symbols as any partial transversal, i.e., the minimum deficit of any latin square can always be realized by one of its weak transversals.

3.2 Disjoint Weak Transversals

First, we make some initial progress towards a solution to Conjecture 3.1.2 by showing that every latin square of order n contains a collection of $\Omega(n)$ mutually disjoint weak transversals. Informally speaking, our result shows that all latin squares of order n have a collection of mutually disjoint weak transversals of size about $\frac{1}{11}n$ when n is sufficiently large.

Proposition 3.2.1. *Suppose that L is an $n \times n$ latin array with at most k empty cells in each row and column and that L contains a partial transversal of length t. Then L contains a weak transversal with deficit no larger than $\max\{4, 2n-2t\}$ so long as*

$$t \geq \max\left\{\frac{7}{8}n + \frac{3}{8}k + \frac{3}{8},\ \frac{6}{7}n + \frac{5}{14}k - \frac{18}{7}\right\}$$

The first of these expressions is greater than the second if and only if $n+k \geq 73$.

Proof. We assume that the first t cells along the main diagonal of L form a partial transversal in the natural order, i.e. $L(i,i) = i$ for $1 \leq i \leq t$. If $t = n$, then we are done. If $t = n-1$ and $L(n,n)$ is not empty, then we may add this cell to our partial transversal to form a weak transversal of deficit 1. If $L(n,n)$ is empty, then we discard any cell from our original partial transversal to place ourselves in the case $t = n-2$, which is handled below. Having effectively altered the value of t, we must accept an upper-bound on our deficit of $\max\{4, 2n-2t\}$. Had we been able to avoid altering the value of t, we would have a deficit no larger than $2n-2t$.

We will swap $m := n - t$ cells from the given partial transversal with $2m$ cells from rows and columns $t+1, \ldots, n$ to form a weak transversal. Figure 3.1 provides a schematic for our setup. The cells along the main diagonal containing symbols $a_1, \ldots, a_m$ will be swapped for m cells from each of blocks A and B. To ensure that the resulting n cells form a weak transversal, we will select cells in blocks A and B that together contain $2m$ distinct symbols and occupy distinct rows and columns. Since we will lose at most m symbols, the result holds.

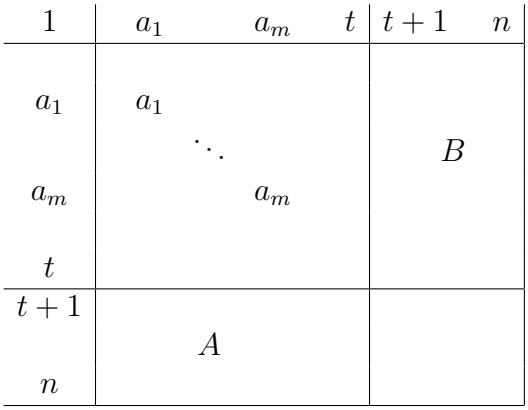

Figure 3.1: Schematic for Proposition 3.2.1

We now describe an inductive method for selecting $\{a_1, \ldots, a_m\}$ and the corresponding cells in blocks A and B. Suppose that we have selected $\{a_1, \ldots, a_j\}$ and that, for $1 \leq i \leq j$, cell (a_i, a_i, a_i) will be swapped with cells (r_i, a_i, s_i^r) and (a_i, c_i, s_i^c). To ensure that we eventually obtain a weak transversal, these

selections will be made so that each of the following sets contains no repetitions

$$R = \{r_i \in [n] \setminus [t] : 1 \leq i \leq j\}$$
$$C = \{c_i \in [n] \setminus [t] : 1 \leq i \leq j\}$$
$$S = \{s_i^r, s_i^c : 1 \leq i \leq j\}$$

Note that, given these constraints on R, C, and S, swapping cells

$$\{(a_i, a_i, a_i) : 1 \leq i \leq j\}$$

with cells

$$\{(r_i, a_i, s_i^r), (a_i, c_i, s_i^c) : 1 \leq i \leq j\}$$

will produce a collection of $t+j$ cells from distinct rows and columns that contains no symbol three times. Furthermore, the only symbols that can appear twice are those that fall both in S and in $[t]\setminus\{a_1, \ldots, a_j\}$. The unoccupied rows and columns will be $R' := [n] \setminus ([t] \cup R)$ and $C' := [n] \setminus ([t] \cup C)$, respectively.

First, assume that $0 \leq j \leq m-3$. For $i \in [t] \setminus \{a_1, \ldots, a_j\}$, we define the following sets

$$A(i) = \{r \in R' : L(r,i) \text{ is not empty and } L(r,i) \notin S\}$$
$$B(i) = \{c \in C' : L(i,c) \text{ is not empty and } L(i,c) \notin S\}.$$

Notice that if we can locate i such that $|A(i)| \geq 2$ and $|B(i)| \geq 1$ (or $|A(i)| \geq 1$ and $|B(i)| \geq 2$) then i will be a suitable choice for a_{j+1} since we would have sufficient flexibility to choose r_{j+1} and c_{j+1} appropriately.

There are at most $(k+2j)(m-j)$ cells in the $R' \times [t]$ portion of block A that are either empty or contain a symbol from the set S. Thus, there are at most $\lfloor (k+2j)(m-j)/(m-j-1) \rfloor \leq \frac{3}{2}(k+2j)$ values of i such that $|A(i)| \leq 1$ and at most $k+2j$ values of i such that $|A(i)| = 0$. Likewise for $B(i)$. It follows that there are at least $t - j - \frac{5}{2}(k+2j) = t - 6j - \frac{5}{2}k$ values of i such that both $|A(i)| \geq 2$ and $|B(i)| \geq 1$. Since $j \leq m-3$, we can find a suitable choice of i so long as the following inequality holds

$$t - 6m + 18 - \frac{5}{2}k > 0.$$

Equivalently,

$$t > \frac{6}{7}n + \frac{5}{14}k - \frac{18}{7}. \tag{3.2.1}$$

Now suppose that $j = m-2$ so that only a_{m-1} and a_m remain to be selected. The above argument will work for a_{m-1} but not for a_m since neither $|A(i)|$ nor $|B(i)|$ can ever be greater than 1 in that case. We therefore choose a_{m-1} and a_m simultaneously. Define the following set

$$I = \{i \in [t] \setminus \{a_1, \ldots, a_{m-2}\} : |A(i)|, |B(i)| \geq 2\}.$$

We will show that if $|I| \geq 17$, then there are suitable choices for a_{m-1} and a_m. Let $R' = \{r, r'\}$ and $C' = \{c, c'\}$ be the rows and columns that have not yet been utilized in blocks A and B, respectively. We define two disjoint subsets

of I as follows

$$I_{rc} = \{i \in I : L(r, i) = L(i, c)\}$$
$$I_0 = \{i \in I : L(R' \times i) \cap L(i \times C') = \emptyset\}$$

Suppose that $I_{rc} \neq \emptyset$ and $|I_0 \cup I_{rc}| \geq 5$. Fix $i_1 \in I_{rc}$. It follows that $L(r, i_1) \neq L(i_1, c')$. Let these distinct symbols be a and b, respectively. Then there are at most three values $i \in (I_0 \cup I_{rc}) \setminus i_1$ such that $L(r', i) \in \{a, b\}$ or $L(i, c) \in \{a, b\}$. Since $|I_0 \cup I_{rc}| \geq 5$, we may select $i_2 \in (I_0 \cup I_{rc}) \setminus i_1$ such that $L(r', i_2)$ and $L(i_2, c)$ are distinct from a and b. Furthermore, $L(r', i_2) \neq L(i_2, c)$ since $i_2 \in I_0 \cup I_{rc}$. The pair $\{i_1, i_2\}$ thus makes for a suitable choice of a_{m-1} and a_m. The same argument would apply for the analogous sets $I_{rc'}$, $I_{r'c}$, and $I_{r'c'}$. Now suppose instead that $I_0 = I$. The exact same argument follows here except we require that $|I_0| \geq 6$ since now there are at most four values $i \in I_0 \setminus i_1$ such that $L(r', i) \in \{a, b\}$ or $L(i, c) \in \{a, b\}$.

Thus, so long as $|I| = |I_0| + |I_{rc} \cup I_{rc'} \cup I_{r'c} \cup I_{rc}| \geq 17$, there must be a suitable choice of a_{m-1} and a_m.

As there are at most $\frac{3}{2}k + 3m - 6$ values of i such that $|A(i)| \leq 1$, there are at least

$$t - (m - 2) - (\frac{3}{2}k + 3m - 6) = 5t - 4n - \frac{3}{2}k + 8$$

many values of i such that $|A(i)| \geq 2$. Thus the value of $|I|$ is at least

$$2(5t - 4n - \frac{3}{2}k + 8) - (t - (m - 2)) = 8t - 7n - 3k + 14$$

If we want $|I| \geq 17$, then we require t such that

$$t \geq \frac{7}{8}n + \frac{3}{8}k + \frac{3}{8} \tag{3.2.2}$$

The construction can thus be completed so long as inequalities 3.2.1 and 3.2.2 both hold. It is easy to check that 3.2.2 is stronger that 3.2.1 if and only if $n + k \geq 73$. □

In light of Proposition 2.2.1, we have the following corollaries.

Corollary 3.2.2. *Suppose that L is an $n \times n$ latin array with at most k empty cells in each row and column and $n + k \geq 73$. Then L contains a weak transversal with deficit no larger than $2\sqrt{n}+2k$ so long as $k \leq \frac{1}{11}n - \frac{8}{11}\sqrt{n} - \frac{3}{11}$.*

Proof. By Proposition 3.2.1, to guarantee the existence of a weak transversal we need a partial transversal of length t such that $t \geq \frac{7}{8}n + \frac{3}{8}k + \frac{3}{8}$. By Proposition 2.2.1, L contains a partial transversal of length

$$t \geq n - \sqrt{n} - k$$

Here we have used $n - \sqrt{n} - k$ rather than $n - \sqrt{n} - k + 1$ since the latter result does not apply for $k = 0$. Thus we would like to ensure that

$$n - \sqrt{n} - k \geq \frac{7}{8}n + \frac{3}{8}k + \frac{3}{8}.$$

It is a straightforward calculation to confirm that this inequality holds at least for $0 \leq k \leq \frac{1}{11}n - \frac{8}{11}\sqrt{n} - \frac{3}{11}$. By Proposition 3.2.1, the resulting weak transversal will have deficit no larger than $2\sqrt{n} + 2k$. □

Proposition 3.2.3. *Every latin square of order $n \geq 73$ has a collection of at least $\frac{1}{11}n - \frac{8}{11}\sqrt{n} - \frac{3}{11}$ mutually disjoint weak transversals.*

Proof. Suppose that L is a latin square of order $n \geq 73$. By Corollary 3.2.2, we may iteratively remove disjoint weak transversals from L until we have reached k disjoint weak transversals where $k = \lfloor \frac{1}{11}n - \frac{8}{11}\sqrt{n} - \frac{3}{11} \rfloor$. At that point, we may remove at least one more additional weak transversal. □

3.3 Weak k-Plexes

We define a *weak k-plex* to be a collection of kn cells that meets each row and column k times and each symbol $k-1$, k, or $k+1$ times. As in the case of k-plexes, the complement of a weak k-plex is a weak $(n-k)$-plex.

Proposition 3.3.1. *All sufficiently large latin squares contain weak 2-plexes.*

Proof. Let L be a latin square of order n. By Corollary 3.2.2, L contains a weak transversal, W_1, of deficit $d_1 \leq 2\sqrt{n}$. Let $D_1, S_1 \subseteq [n]$ be the d_1-sets of symbols appearing 0 and 2 times in W_1, respectively.

By Proposition 2.3.1, we may locate a partial transversal of $L \setminus W_1$ consisting precisely of the symbols D_1 since $d_1 \leq 2\sqrt{n} \leq \frac{1}{2}n + 1$ and every symbol in D_1 appears n times in $L \setminus W_1$. We would now like to extend this partial transversal to a weak transversal of $L \setminus W_1$ that does not contain any symbol from S_1.

Consider the square latin array of order $n - d_1$ corresponding to the rows and columns not occupied by our partial transversal. Remove from this square any cells from W_1 and any cells containing symbols from S_1. The resulting

square has at most $1 + d_1$ empty cells in each row and column. By Corollary 3.2.2, this square has a weak transversal so long as

$$1 + d_1 \leq \frac{1}{11}(n - d_1) - \frac{8}{11}\sqrt{n - d_1} - \frac{3}{11}.$$

Since $d_1 \leq 2\sqrt{n}$, this inequality will hold for large n. Let W_2 be the resulting weak transversal. Notice that $W_1 \cup W_2$ is a weak 2-plex.

□

The same method can be used to show that weak k-plexes exist for larger values of k as well.

3.4 Weak Transversals of Minimum Deficit

The following method is due to Cameron and Wanless from their proof that every latin square contains a weak transversal [10]. We repurpose the method here to establish the following stronger result.

Proposition 3.4.1. *Any cell of a latin square contained in a partial transversal of deficit d is contained in a weak transversal of deficit no larger than d.*

It follows from this result that the minimum deficit of any latin square is actually realized by a weak transversal. Notice that this application would follow rather trivially from Brualdi's conjecture (Conjecture 2.1.1). If the minimum deficit among all diagonals of a latin square is 0 or 1, then such diagonals are themselves weak transversals. While this application is interesting in its own right, as discussed in §2.4.2, we also exploit it in our computations on partial transversals to confirm Brualdi's conjecture for $n = 10$.

Proof. Let L be a latin square of order n. Fix a cell $(r, r^\theta, s) \in L$ in a diagonal θ of deficit d. Select a row $r_1 \neq r$ such that $L(r_1, r_1^\theta)$ appears three or more times in θ. We will identify a row $r_2 \neq r, r_1$ such that $L(r_1, r_2^\theta)$ does not appear in θ and $L(r_2, r_1^\theta)$ appears at most once in θ.

Let x_i be the number of symbols appearing exactly i times in θ. It follows that

$$\sum_{i=0}^{n} x_i = \sum_{i=0}^{n} i x_i = n$$

and thus

$$x_0 = x_2 + 2x_3 + \cdots + (n-1)x_n > x_2 + x_3 + \cdots + x_n.$$

Row r_1 contains x_0 cells whose symbols do not appear in θ and column r_1^θ contains $\sum_{i=2}^{n} x_i - 1$ cells whose symbols appear more than once in θ, besides cell (r_1, r_1^θ). Thus, there are at least two rows r_2 such that $L(r_2, r_1^\theta)$ does not appear more than once in θ and $L(r_1, r_2^\theta)$ does not appear in θ. Select $r_2 \neq r$. Observe that the diagonal $\theta(r_1 r_2)$ has fewer cells than θ that contain symbols that appear more than twice in the diagonal, and (r, r^θ) still belongs to $\theta(r_1 r_2)$. Furthermore, $\theta(r_1 r_2)$ contains at least as many distinct symbols as θ. Iterating the construction will therefore produce a weak transversal of deficit no larger than d that contains cell (r, r^θ). □

It also follows from the above argument that there is a weak transversal of minimum deficit that does not duplicate any chosen symbol, for we could always apply the above swap to a cell containing the chosen duplicated symbol in a weak transversal.

Corollary 3.4.2. *Every latin square is covered by weak transversals. That is, each cell is contained in some weak transversal.*

This corollary is best understood in contrast to the case of transversals of latin squares. The contemporaneous but independent works of Evans [23] and Wanless and Webb [48] both established the result that for every order $n \neq 1, 3$ there exists a latin square of order n that has no orthogonal mate. This result brought to a close a century old program to establish the existence of so-called *bachelor squares*. The method used in the latter of these works was driven by a construction for latin squares that have no transversals passing through a prescribed cell. The present corollary indicates that no such proof can exist to contradict Conjecture 3.1.2.

While there are weak transversals with small deficit, the following observation shows that even relatively small partial transversals cannot always be embedded in a weak transversal.

Observation 3.4.3. *For each $n \equiv 0 \mod 4$ and $n > 4$, there exists a latin square of order n with a partial transversal of length $\frac{1}{2}n$ that is not contained in any weak transversal.*

Proof. Consider any latin square of the form

$\mathbb{Z}_{n/2}$	$*$
$*$	$\mathbb{Z}_{n/4} \times \mathbb{Z}_2$

The top-left and bottom-right blocks will contain the same symbols but will be equivalent to the Cayley tables of $\mathbb{Z}_{n/2}$ and $\mathbb{Z}_{n/4} \times \mathbb{Z}_2$, respectively. As we will see in Chapter 7, the top-left block has no transversal while the

bottom-right block does. Fix any transversal of the bottom-right block and note that to embed this partial transversal in a weak transversal, one must locate a transversal of the top-left block. □

Chapter 4

Weak Orthogonal Mates

4.1 Background

A main result of the previous chapter was that every latin square of order n contains a collection of $\Omega(n)$ mutually disjoint weak transversals. The motivation for this result was Conjecture 3.1.2 that every latin square can be partitioned into weak transversals. Here we examine this conjecture from the perspective of orthogonal latin squares.

Recall that two latin squares are *orthogonal* or *orthogonal mates* if and only if the symbol patterns of the first square form transversals of the second square. It is straightforward to check that orthogonality is a symmetric relationship.

We introduce the following notions. A *k-weak transversal* is a diagonal of a latin square that contains no symbol more than k times. Two latin squares are *k-weakly orthogonal* if the symbol patterns of the first square form k-weak transversals of the second square.

Lemma 4.1.1. *The relationship of being k-weakly orthogonal is symmetric.*

Proof. Suppose that latin squares A and B are k-weakly orthogonal. That is, the symbol patterns of A form k-weak transversals of B. Let α and β be arbitrary symbol patterns from A and B, respectively. We would like to conclude that β forms a k-weak transversal of A. Notice that if α intersects β in more than k cells, then α fails to form a k-weak transversal of B, a contradiction. □

4.2 Mutually k-Weakly Orthogonal Squares

We now investigate the possible sizes of sets of mutually k-weakly orthogonal latin squares. We denote by $N(n, k)$ the maximum size of a set of mutually weakly orthogonal latin squares of order n. The following proposition generalizes the classical result that $N(n, 1) \leq n - 1$ [30].

Proposition 4.2.1. *For $1 \leq k < n$,*

$$N(n, k) \leq \prod_{i=1}^{k} (n - i)$$

Proof. Suppose that we have a collection of k-weakly orthogonal latin squares. If we permute the symbols of any single square, it remains k-weakly orthogonal to the others. We may thus assume that the first row of each square is $(1, 2, \ldots, n)$. Note that for any of the squares there are $\Pi_{i=1}^{k}(n - i)$ possible arrangements for symbol 1 in rows 2 through $k + 1$. For two squares to be k-weakly orthogonal, they must realize distinct arrangements for symbol 1 in these k rows. □

While Proposition 4.2.1 provides an upper-bound for $N(n,k)$, the real fascinating question is when and whether this bound is attained. This innocent sounding question brings us immediately to one of the most important open problems in combinatorics, the Prime Power Conjecture.

Conjecture 4.2.2 ([30])**.** *$N(n,1) = n-1$ if and only if n is a prime power.*

Before describing our computational data for $N(n,k)$, we present the following generalization of the Prime Power Conjecture as an open problem.

Conjecture 4.2.3. *The bound from Proposition 4.2.1 is attained if and only if $n-k+1$ is a prime power.*

We have developed a small amount of computational data for $N(n,k)$. Figure 4.1 summarizes our findings. Here we explain our methods for computing this data. We anticipate that these rather rudimentary tools will lead to a general construction achieving the bound for infinitely many values of n and $k > 1$.

$k\backslash n$	2	3	4	5	6	7	8	9	10
1	–	–	–	–	$\frac{1}{5}$	–	–	–	$\frac{2}{9}$
2		–	–	–	–	$\frac{11}{30}$	–	·	·
3			–	–	$\frac{26}{60}$	$\frac{20}{120}$	·	·	·
4				–	–	–	·	·	·
5					–	–	·	·	·
6						–	·	·	·

Figure 4.1: Cell (k,n) contains symbol "–" if the bound from Proposition 4.2.1 is attained and is blank if either the parameters are out of range or only trivial information is known. If the cell contains a ratio, then the numerator is a lower-bound for $N(n,k)$ and the denominator is the known upper-bound.

Recall the classical construction used to achieve the value $N(n,1) = n-1$ for n a prime power. For each $a \in GF(n)^*$, let $f_a = ax + y \in GF(n)[x,y]$. Form a latin square L_a of order n such that $L_a(x,y) = f_a(x,y)$. It follows that L_a and L_b are orthogonal if and only if $a \neq b$ [30].

Notice that this construction begins with a single latin square, the addition table of $GF(n)$, and generates mutually orthogonal latin squares simply by permuting the non-zero rows of the original square. As a first pass at constructing k-weakly orthogonal latin squares, we began by generating the $(n-1)!$ latin squares resulting from permutations of the non-zero rows of $(\mathbb{Z}_n, +)$ and then searching for cliques of mutually k-weakly orthogonal latin squares within these sets. Since the resulting squares are determined by their first columns, we may present such cliques by rectangular arrays whose columns are the first columns of the corresponding square.

	0	1	2	3	4	5	6	7	8	9	A
0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	2	2	3	3	4	4	5	5	6
2	2	3	4	6	4	6	1	2	1	3	5
3	3	5	1	3	6	2	6	5	2	1	4
4	4	2	5	1	1	5	2	6	4	6	3
5	5	6	3	4	5	1	3	1	6	4	2
6	6	4	6	5	2	4	5	3	3	2	1

Figure 4.2: Each column corresponds to the first column of a latin square of order 7 formed by a permutation of the rows of $(\mathbb{Z}_7, +)$. This example confirms that $N(7,2) \geq 11$. Column and row dividing lines have been added to emphasize some apparent patterns and natural groupings.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	I	J
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5
2	2	3	4	5	1	4	3	5	1	5	2	4	1	3	5	2	1	2	4	3
3	3	2	5	4	4	1	5	3	5	1	4	2	3	1	2	5	2	1	3	4
4	4	5	3	2	3	5	4	1	2	4	5	1	5	2	3	1	4	3	2	1
5	5	4	2	3	5	3	1	4	4	2	1	5	2	5	1	3	3	4	1	2

	0	1	2	3	
0	0	0	0	0	
1	1	1	1	1	
2	2	3	4	5	(12)(34)
3	3	2	5	4	(13542)
4	4	5	3	2	(1452)
5	5	4	2	3	(1532)

Figure 4.3: Each column in the first table corresponds to the first column of a latin square formed by a permutation of the rows of $(\mathbb{Z}_6, +)$. This example confirms that $N(6, 2) = 20$. The second table represents this data in a more compact format. Columns 4 – J can be computed simply by applying one of the four permutations to all of the symbols in the first block.

	0	1	2	3	4	5	
0	0	0	0	0	0	0	
1	1	1	1	1	1	1	
2	2	3	4	5	6	7	(12)(35)(47)
3	3	2	6	7	4	5	(1376452)
4	4	6	5	3	7	2	(142)(567)
5	5	7	3	6	2	4	(157362)
6	6	4	7	2	5	3	(165432)
7	7	5	2	4	3	6	(172)(346)

Figure 4.4: Each column corresponds to the first column of a latin square formed by a permutation of the rows of $(\mathbb{Z}_8, +)$. An additional 36 columns can be generated by applying the listed permutations to the existing columns. Together these squares confirm that $N(8, 2) = 42$.

Chapter 5

Integral Weight Functions

5.1 Background

Any subset of cells A drawn from a latin square L may be viewed as a map $f : L \to \{0, 1\}$ such that $f^{-1}(1) = A$. From this perspective, A is a transversal of L if and only if the sum of the image of f over each row, column, and symbol pattern of L is 1, where these sums are conducted in $(\mathbb{Z}, +)$. In this chapter, we investigate the maps that arise when we allow for a larger codomain, e.g. we replace $\{0, 1\}$ with $\mathbb{Z}$, yet still require that the above sum condition holds. In Chapter 6, we examine these maps from a different perspective by investigating the sets that arise from conducting these sums in a different group, such as $(\mathbb{Z}_p, +)$.

We call an integral weight function on the cells of a latin square a *k-weight* if the sum over each row, column, and symbol is k. We will show that several important non-existence results and existence conjectures about k-plexes hold in the much weaker setting of k-weights. It is our hope for this study, therefore,

that k-weights may prove to be a useful generalization to better understand k-plexes.

In §5.3 we establish a simple lemma that is employed in several of our arguments. In §5.4 we generalize a non-existence result of Wanless for odd-plexes to show that certain latin squares have no odd-weights. We also give a construction to show that analogues of Conjectures 1.0.1 and 3.1.1 hold for k-weights. In §5.5 we generalize recent results of Stein and Szabó concerning near transversals in Abelian groups to analogous objects related to k-weights. We close this chapter with §5.6 in which we mention several open questions.

5.2 Definitions

Suppose $\theta : L \to \mathbb{Z}$ is an integral weight function on the cells of L. For $k \in \mathbb{Z}$, we call θ a *k-weight of L* if its sum over each row, column, and symbol is k. That is, for each index i, we have

$$\sum_{(r,c,i)\in L} \theta(r,c,i) = \sum_{(r,i,s)\in L} \theta(r,i,s) = \sum_{(i,c,s)\in L} \theta(i,c,s) = k.$$

We call θ a *partial k-weight* of L with length t if precisely t row, t column, and t symbol sums are k with each remaining sum being 0. We say that θ *misses* those rows, columns, and symbols whose sums are 0. When t is one less than the order of L, we call θ a *near k-weight* of L. A partial k-weight is said to be *maximal* if, as a vector in $\mathbb{Z}^{n^2}$, it is not dominated by another partial k-weight.

For latin squares L and L', we say that L *has the block pattern of* L' if L can be represented by a block matrix $[A_{i,j}]_{1\leq i,j\leq n}$ where each $A_{i,j}$ is itself a

latin square and blocks $A_{i,j}$ and $A_{i',j'}$ contain the same symbols if and only if $L'(i,j) = L'(i',j')$. In such a case, it follows that each block has the same size, say q, and we say that L has the *q-block pattern of L'*. When we are concerned only with the parity of q, we also refer to the odd-block or even-block pattern. In more classical terminology, a latin square with the q-block pattern of $(\mathbb{Z}_m, +)$ is said to be of *q-step type* and order qm.

5.3 The Delta Lemma

We now establish a lemma that has proven exceptionally useful in the study of transversals and k-plexes. Here we show that the analogous result holds in the more general context of k-weights. First recall the following result of Paige.

Lemma 5.3.1 (Paige [33])**.** *Suppose $(G,+)$ is a finite Abelian group. If G has a unique involution, then it is equal to $\sum_{g\in G} g$. Otherwise, $\sum_{g\in G} g = 0$.*

The following lemma plays a central role in several of our arguments. It is essentially another version of an argument used by Egan and Wanless to show, among many other things, that certain latin squares do not contain odd-plexes [19, 46]. Our contribution has been to show that the argument applies more generally to partial k-weights. The result is often referred to as the Delta Lemma because of the closely related map $\Delta(r,c,s) = s-r-c$, which in some sense measures the extent to which a particular square differs from the cyclic square of that order.

Lemma 5.3.2. *Suppose L is the Cayley table of an Abelian group $(G,+)$ and θ is a partial k-weight whose missing rows R sum to r, missing columns C*

sum to c, and missing symbols S sum to s. Then

$$k(s-r-c) = \begin{cases} \sum_{g\in G} g & \text{if } k \text{ is odd and } G \text{ has a unique involution} \\ 0 & \text{otherwise.} \end{cases}$$

Note that when θ is a k-weight (rather than just a partial k-weight), $r = c = s = 0$ and thus the left-hand side is always 0.

Proof. Set $u := \sum_{g\in G} g$. First we consider the sum

$$\begin{aligned} \sum_{(x,y,z)\in L} \theta(x,y,z)(z-x-y) = &\sum_{(x,y,z)\in L} \theta(x,y,z)z \\ &- \sum_{(x,y,z)\in L} \theta(x,y,z)x \\ &- \sum_{(x,y,z)\in L} \theta(x,y,z)y. \end{aligned}$$

We will evaluate the left-hand sum by examining each right-hand sum individually but first note that the result must be 0 since $z - x - y = 0$ for every triple $(x, y, z) \in L$. Grouping the first of the three sums by the z coordinate, we have

$$\begin{aligned} \sum_{(x,y,z)\in L} \theta(x,y,z)z &= \sum_{z\in G} \left(\sum_{(x,y,z)\in L} \theta(x,y,z) \right) z \\ &= \sum_{z\in G\setminus S} kz \\ &= \sum_{z\in G} kz - \sum_{z\in S} kz \\ &= ku - ks \end{aligned}$$

Likewise, we have

$$\sum_{(x,y,z)\in L} \theta(x,y,z)x = ku - kr \quad \text{and}$$
$$\sum_{(x,y,z)\in L} \theta(x,y,z)y = ku - kc.$$

Recalling that the original sum must be 0, we now have

$$\begin{aligned} 0 &= (ku - ks) - (ku - kr) - (ku - kc) \\ &= -ku + k(s - r - c). \end{aligned}$$

Thus $k(s - r - c) = ku$. By Lemma 5.3.1, if k is even or G does not have a unique involution, then $ku = 0$. Otherwise, k is odd and u is an involution. Therefore $ku = u$. □

5.4 When do k-weights Exist?

Our first result shows that the natural analogues of Ryser's and Rodney's conjectures hold for k-weights.

Proposition 5.4.1. *Every latin square has a* 2*-weight and those of odd order have* 1*-weights.*

Proof. Fix any cell $(r, c, s) \in L$ and define $\theta : L \to \mathbb{Z}$ as follows:

$$\theta(x, y, z) = \begin{cases} 3 - n & \text{if } (x, y, z) = (r, c, s) \\ 1 & \text{if } (x, y, z) \text{ and } (r, c, s) \text{ agree in precisely one position} \\ 0 & \text{otherwise.} \end{cases}$$

We claim that θ is a 2-weight of L. First consider the sum of θ over row $x \neq r$. All cells in row x have been assigned 0 except for the cell in column c and the cell containing symbol s. These exceptions must be distinct cells since L is a latin square. Since these two cells both carry a weight of 1, the sum over row x is 2. Now consider the sum over row r. Every cell in row r carries weight 1 except for cell (r, c, s), which carries weight $3 - n$. Thus the sum over row r is $(n - 1) + (3 - n) = 2$.

Since our construction treats rows, columns, and symbols symmetrically, it follows that all column and symbol sums are also 2.

Now suppose $n = 2m + 1$ is odd. Note that every latin square has at least one n-weight since we may assign 1 to every cell. Let θ and γ be a 2-weight and n-weight of L, respectively. Then $\psi := \gamma - m\theta$ is a 1-weight of L. □

In light of Proposition 5.4.1, the existence question for k-weights is rather crude. Each latin square has a k-weight either for all integers k or for every even k. This fact contrasts sharply with the situation in k-plexes where the spectrum of existence can be much more subtle. Egan and Wanless, for example, have shown that for every even $n > 2$ there exists a latin square of order n that has no k-plex for any odd $k < \lfloor n/4 \rfloor$ but has a k-plex for every other $k \leq n/2$ [19]. For further results of this sort consult [18, 9, 17].

Our next result has a long history. Euler showed that $(\mathbb{Z}_{2m}, +)$ has no transversals [21], a century later Maillet showed the same result for any latin square with the odd-block pattern of $(\mathbb{Z}_{2m}, +)$ [31], and another century passed before Wanless extended the result to odd-plexes [46]. We show that the claim holds on the more general level of odd-weights.

Proposition 5.4.2. *Let L and L' be latin squares.*

1. *The Cayley table of a finite Abelian group with a unique involution has no odd-weights.*

2. *If L has no odd-weights and L' has the odd-block pattern of L, then L' has no odd-weights.*

The primary contribution of Proposition 5.4.2 is to show that the above sequence of results of Euler, Maillet, and Wanless follows from the more general setting of k-weights. However, we do show a bit more in that if there exists a latin square L that has no odd-weights but does not have the odd-block pattern of $(\mathbb{Z}_{2m}, +)$, then by part (ii) of the proposition this property persists to all squares with the odd-block pattern of L. It remains an open question whether such squares exist.

Proof. (i) Suppose θ is a k-weight of M, the Cayley table of a finite Abelian group with unique involution u. By Lemma 5.3.2, k is even since, otherwise, we immediately have the contradiction that $0 = u$.

(ii) Suppose L' has the q-block pattern of L and that L has no odd-weights. Let L' be represented by the block matrix $[A_{i,j}]_{1 \leq i,j \leq m}$ where squares $A_{i,j}$ and $A_{i',j'}$ use the same symbols if and only if $L(i,j) = L(i',j')$. Let θ be a k-weight

of L'. Define the map $\psi : L \to \mathbb{Z}$ by

$$\psi(i,j,k) := \sum_{(x,y,z)\in A_{i,j}} \theta(x,y,z).$$

We now verify that ψ is a qk-weight of L. Observe that the sum over row r of L equals the sum over q different rows of L'. Since each row of L' sums to k, the sum over row r in L equals qk. Similarly for columns and symbols. Thus ψ is a qk-weight of L but since L has no odd-weight, either q or k must be even. □

5.5 Near k-weights of Abelian Groups

In this section we generalize a recent result of Stein and Szabó to the context of k-weights.

Lemma 5.5.1 (Hall [27]). *The Cayley table of any finite Abelian group has a near transversal.*

Proposition 5.5.2 (Stein and Szabó [43]). *Suppose L is the Cayley table of an Abelian group of order n.*

1. *Then L has a transversal or a maximal near transversal but not both.*
2. *If n is prime, then there is no way to select a single cell from each row and column such that precisely two distinct symbols have been selected.*

As stated, Proposition 5.5.2 is somewhat stronger than what [43] actually contains but our form follows easily from theirs and Lemma 5.5.1, which Stein

and Szabó use and discuss in their paper. We show that this result is again a more general fact about partial k-weights.

Proposition 5.5.3. *Suppose L is the Cayley table of an Abelian group of order n.*

1. *Then L has a 1-weight or a maximal near 1-weight but not both.*

2. *If $\theta : L \to \mathbb{Z}$ whose row and column sums are all 1, then it cannot happen that $n-2$ symbol sums are 0 while the remaining sums are $n-i$ and i with $\gcd(n,i) = 1$. In particular, if n is prime, then it cannot happen that precisely $n-2$ symbol sums are 0.*

Proof. (i) Let θ be a near 1-weight that misses row r, column c, and symbol s. We know such a partial weight exists by Lemma 5.5.1. It suffices for our purposes to show that whether θ is maximal depends only on G and not the particular partial weight. Let $u := \sum_{g \in G} g$. By Lemma 5.3.2,

$$s - r - c = \begin{cases} u & \text{if } G \text{ has a unique involution (which then must be } u) \\ 0 & \text{otherwise.} \end{cases}$$

If $s-r-c = 0$, then $r+c = s$, i.e. (r,c,s) is a cell in the Cayley table of G and we may thus extend θ to a 1-weight. If $s-r-c = u$, then $r+c \neq s$ and thus θ is maximal. In the case that θ is maximal, i.e. G has a unique involution, we should also note that G could not also have a 1-weight since reducing the weight on any single cell would produce a near 1-weight that by the preceding argument must be maximal, a contradiction.

(ii) Suppose that $\theta : L \to \mathbb{Z}$ has the property described in the statement of the proposition. In particular, all row and column sums are 1 and all symbol sums are 0 with the exception of symbols g and h whose sums are i and $n-i$, respectively. As in the proof of Lemma 5.3.2, we evaluate the following trivial expression as three separate sums. Again, set $u := \sum_{g \in G} g$.

$$\begin{aligned} 0 = \sum_{(x,y,z) \in L} \theta(x,y,z)(z-x-y) &= \left(\sum_{(x,y,z) \in L} \theta(x,y,z) z \right) - 2u \\ &= \sum_{(x,y,z) \in L} \theta(x,y,z) z \\ &= \sum_{z \in G} \left(\sum_{(x,y,z) \in L} \theta(x,y,z) \right) z \\ &= ig + (n-i)h \\ &= i(g-h). \end{aligned}$$

Thus either $g = h$ or the order of the nontrivial group element $g - h$ divides both i and n. In the latter case, $\gcd(n, i) > 1$. □

5.6 Open Questions about k-weights

We introduced the concept of a k-weight of a latin square as a potentially useful generalization of a k-plex. We showed that several results about transversals and k-plexes can be seen as facts about these more general structures and that analogues of well-known conjectures about transversals and duplexes hold at least in the context of k-weights.

We have yet to resolve at least two basic questions regarding k-weights. We have seen that latin squares with the odd-block pattern of $\mathbb{Z}_{2m}$ have no odd-weights. Does the converse hold? That is, does the lack of odd-weights characterize latin squares of the odd-block pattern of $\mathbb{Z}_{2m}$? We suspect the answer is no but are not aware of any counter-example. The analogous question for plexes is also open: do there exist latin squares without odd-plexes besides those of odd-step type with an even number of blocks?

As we have seen, it was fairly straightforward to settle k-weight analogues of Ryser's and Rodney's conjectures by constructing 2-weights for all latin squares and 1-weights for the those of odd order. One might hope to find similar constructions for near 1-weights in every latin square and thereby settle the k-weight analogue of Brualdi's conjecture that every latin square has a near transversal. It is interesting that this construction, should it exist, seems to be more difficult than the 1-weight and 2-weight constructions.

Chapter 6

Combinatorial Nullstellensatz

In this chapter, we explore applications of a method called the Combinatorial Nullstellensatz to the study of latin squares.

6.1 Background

The term *Combinatorial Nullstellensatz* (CN) refers to the following proposition.

Proposition 6.1.1 (Alon [2])**.** *Let F be a field and $f \in F[x_1, \ldots, x_n]$. Suppose that* $\deg(f) = \sum_{i=1}^{n} t_i$ *where each t_i is a nonnegative integer and the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is nonzero. Then for any subsets of F, $S_1, \ldots, S_n$ with $|S_i| > t_i$, there are $s_1 \in S_1, \ldots, s_n \in S_n$ such that*

$$f(s_1, \ldots, s_n) \neq 0.$$

For the duration of this chapter, let L be a latin square of order n with symbol patterns coded by π_i, i.e. cell (j, j^{π_i}) contains symbol i. Let $x = (x_{i,j} :$

$1 \leq i, j \leq n$) be a set of indeterminates, where $x_{i,j}$ corresponds to the (i, j) cell of L. Let R_i, C_i, S_i be the sets of indeterminates corresponding to row i, column i, and symbol i, respectively.

To this date, the most notable application of Proposition 6.1.1 to latin squares is Alon's result that every square sub-block of the multiplication table of $(\mathbb{Z}_p, +)$ contains a transversal [3]. This result was the first confirmation of a special case of a conjecture of Snevily that every square sub-block of an Abelian group of odd order contains a transversal [41]. The full conjecture has recently been established in the affirmative by Arsovski using a linear algebraic method [4].

6.2 Latin Square Related Polynomials

Applications of Proposition 6.1.1 typically involve two steps: (1) identify a polynomial whose support corresponds to some type of combinatorial structure of interest and (2) use algebraic techniques to determine, or at least bound, the polynomial's degree. It is then fairly straightforward to apply Proposition 6.1.1 to show that there is a point in the support having some desired combinatorial properties.

While it is arguably the second of these steps that tends to be the most difficult, in the present section, we focus on this first step as we survey various polynomials that are interesting in the context of transversals of latin squares.

As we will deal mostly with polynomials in $GF(2)[x]$, it is helpful to understand when particular terms will appear in a given polynomial. For a collection of indeterminates $A \subseteq x$ and $f \in GF(2)[x]$, we write $f(A)$ for the value of f

under the valuation $x_i = 1$ if and only if $x_i \in A$. We write $t(A)$ for the term $\prod_{x_i \in A} x_i$.

Lemma 6.2.1. *Let $A \subseteq x$ and $f \in GF(2)[x]$. Then $t(A)$ is a term in f if and only if there are an odd number of subsets $A' \subseteq A$ such that $f(A') = 1$.*

Proof. Consider $\sum_{A' \subseteq A} f(A')$ and note that the only terms in f that contribute to this sum are those whose indeterminates form a subset of A. All other terms will evaluate to 0. Those terms whose indeterminates form an $(|A| - k)$-subset of A, say B, contribute 1 to the sum for each of the 2^k subsets of A that contain B. Therefore

$$\sum_{A' \subseteq A} f(A') = \begin{cases} 1 & \text{if } t(A) \text{ is a term in } f \\ 0 & \text{otherwise} \end{cases}$$

We are now done since the sum also counts the number of solutions to $f(x) = 1$ contained in A. □

To each $f \in GF(2)[x]$, we associate a new polynomial f^* whose terms correspond to the support of f. That is, $f^* := \sum_{f(A)=1} t(A)$ where the sum runs over all subsets $A \subseteq x$.

Lemma 6.2.2. $f = (f^*)^*$

Proof. The following conditions are equivalent.

1. $f(A) = 1$
2. $t(A)$ is a term of f^* (by definition)

3. There exists an odd number of $A' \subseteq A$ such that $f^*(A') = 1$ (Lemma 6.2.1)

4. There exists an odd number of $A' \subseteq A$ such that $t(A')$ is a term of $(f^*)^*$. (by definition)

5. $(f^*)^*(A) = 1$.

Therefore, $f(A) = (f^*)^*(A)$. □

6.2.1 Polynomials for k-plexes

We first develop polynomials whose support corresponds to the collection of k-plexes of a latin square. For the duration of this chapter, we let e_i be the ith elementary symmetric polynomial, i.e., $e_i(x_1, \ldots, x_n)$ is the sum of the $\binom{n}{i}$ terms of the form $x_{a_1}x_{a_2}\cdots x_{a_i}$ where $1 \leq a_1 < \cdots < a_i \leq n$. For $k \geq 0$, we define f_k by

$$f_k = e_k + \sum_{i>k} c_i e_i$$

where $c_i = \binom{i}{k} + \sum_{j=k+1}^{i-1} c_j \binom{i}{j} \mod 2$. Figure 6.1 presents the initial terms of f_k for small k.

$f_0 = 1 + e_1 + e_2 + e_3 + e_4 + e_5 + e_6 + e_7 + e_8 + \cdots$
$f_1 = e_1 + e_3 + e_5 + e_7 + e_9 + e_{11} + e_{13} + e_{15} + e_{17} \cdots$
$f_2 = (e_2 + e_3) + (e_6 + e_7) + (e_{10} + e_{11}) + (e_{14} + e_{15}) + (e_{18} + e_{19}) + \cdots$
$f_3 = e_3 + e_7 + e_{11} + e_{15} + e_{19} + e_{23} + e_{27} + e_{31} + e_{35} + e_{39} + e_{43} + e_{47} + \cdots$
$f_4 = (e_4 + e_5 + e_6 + e_7) + (e_{12} + e_{13} + e_{14} + e_{15}) + (e_{20} + e_{21} + e_{22} + e_{23}) + \cdots$
$f_5 = (e_5 + e_7) + (e_{13} + e_{15}) + (e_{21} + e_{23}) + (e_{29} + e_{31}) + \cdots$

Figure 6.1: Initial terms of polynomials f_k for small k. Some parenthesis have been introduced as a visual emphasis of the periodic structure of the terms for the given polynomial.

Lemma 6.2.3. *For any binary vector z with finite support, $f_k(z) \equiv 1 \mod 2$ if and only if z has exactly k nonzero entries.*

Proof. Suppose z has support of size m and note that the claim holds for $m \leq k$. For $m > k$,

$$\begin{aligned} f_k(z) &= \binom{m}{k} + \sum_{i>k}^{m} c_i \binom{m}{i} \\ &= \binom{m}{k} + \sum_{i>k}^{m-1} c_i \binom{m}{i} + c_m \binom{m}{m} \\ &= \binom{m}{k} + \sum_{i>k}^{m-1} c_i \binom{m}{i} + c_m \\ &= \binom{m}{k} + \sum_{i>k}^{m-1} c_i \binom{m}{i} + \binom{m}{k} + \sum_{i>k}^{m-1} c_i \binom{m}{i} \\ &= 0 \mod 2 \end{aligned}$$

□

Recall that R_i, C_i, S_i are the sets of indeterminates corresponding to row i, column i, and symbol i, respectively, of L, a fixed latin square of order n. For $k > 0$, we define the polynomial $g_k \in GF(2)[x]$ by

$$g_k = \prod_{i=1}^{n} f_k(R_i) f_k(C_i) f_k(S_i).$$

Proposition 6.2.4. *The support of g_k is in bijection with the k-plexes of L.*

Proof. By Lemma 6.2.3, the term $f_k(R_i)$ will be non-zero if and only if precisely k of the indeterminates in R_i have been assigned 1 while the others have been assigned 0. That is, in terms of subsets of cells, this assignment selects precisely k cells from row i. Likewise for columns and symbols. □

Before moving on, we point out that, as presented above, the naive bound on the degree of g_k is $3n^2$, which is of course a very poor bound given that the degree can be no larger than n^2, the number of indeterminates.

6.2.2 Polynomials for partial and weak transversals

We now turn our attention to polynomials related to partial and weak transversals. Let δ be the polynomial in $GF(2)[x]$ whose terms correspond to the $\{0, 1\}$ matrices of order n with odd permanent. Equivalently, the terms of δ correspond to the invertible matrixes of order n over $GF(2)$.

Lemma 6.2.5.

1. *The support of δ is the collection of diagonals.*

2. $\dim(\delta) = n^2 - n + 1$.

3. *δ has precisely $2^{\binom{n}{2}} \prod_{i=1}^{n}(2^i - 1)$ terms.*

Proof. For (i), note that the terms of δ are precisely the $n \times n$ $\{0,1\}$ matrices with odd permanent. We now apply Lemma 6.2.2 several times. Since $\delta = (\delta^*)^*$, the support of δ^* must be the odd permanent matrices. Such a polynomial could easily be constructed as the sum of all terms corresponding to diagonals. Thus, the terms of δ^* correspond to all diagonals. It follows that the support of δ is precisely the diagonals.

For (ii), note that $Per(E_n)$ is odd for

$$E_n = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & 1 \\ \vdots & 1 & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}$$

since we may add the top row to all of the lower rows and then add each of the lower rows to the top row to attain the identity matrix. Therefore, E_n corresponds to a term of degree $n^2 - n + 1$ in δ. However, any matrix with $n^2 - n + 2$ non-zero coordinates must have two all 1 rows and cannot, therefore, be invertible.

For (iii), observe that we are counting the number of invertible matrices of order n over $GF(2)$. See, for example, sequence A002884 in [1]. □

For $0 \leq k \leq n$, define the following polynomial in $GF(2)[x]$

$$t_k = \delta \prod_{i=1}^{n-k} e_1(S_i).$$

Lemma 6.2.6. *The support of t_k corresponds to diagonals of L in which symbols $1, \ldots, n-k$ appear an odd number of times. Furthermore,* $\deg(t_k) \leq n^2 - k + 1$.

Note that $t_0 = t_1 = g_1$, where g_1 was defined in §6.2.1. It may be useful that with t_1 we now have a way to write the polynomial whose support corresponds to the collection of transversals with degree bounded by n^2. Of course, our other representations will always reduce to something less than or equal to n^2 but the naive bound for $\deg(g_1)$ was $3n^2$.

Lastly, we define the following polynomial in $GF(2)[x]$ by

$$w = \delta \prod_{i=1}^{n} (f_0 + f_1 + f_2)(S_i).$$

Lemma 6.2.7. *The support of w corresponds to the weak transversals of L.*

Proof. Observe that $w(z) = 1$ if and only if the support of z is a diagonal that meets each symbol either $0, 1$, or 2 times. □

6.3 Applying Combinatorial Nullstellensatz

We now apply Proposition 6.1.1 using several polynomials similar to those discussed above to show that certain classes of latin squares possess structured subsets of prescribed sorts.

Proposition 6.3.1. *Every latin square of order* 11 *has a proper subset of cells meeting each row, column, and symbol* $3, 7,$ *or* 11 *times.*

Proof. Consider the following polynomial in $GF(2)[x]$

$$f = \prod_{i=1}^{11} e_3(R_i)e_3(C_i)e_3(S_i).$$

Note that $e_3(z) = \binom{k}{3} \mod 2$ where z has support of size k. Since $\binom{k}{3} \equiv 1 \mod 2$ implies $k = 3, 7, 11$ whenever $k \leq 11$, the support of f corresponds to selections meeting each row, column, and symbol 3, 7, or 11 times. Given that $f(L) = 1$ and $\deg(f) \leq 99$, the result follows by Proposition 6.1.1. □

6.3.1 Polynomials in $GF(p)[x]$

Thus far we have only considered polynomials in $GF(2)[x]$. In these cases, there was always a natural correspondence between valuations of the indeterminates and subsets of L. In this section, when working in $GF(p)[x]$, we think of the binary valuations as corresponding to subsets of L and simply ignore all other valuations. The following trick will help us focus only on the binary valuations.

Suppose $f \in GF(p)[x]$. Let $\prod x_{i,j}^{\beta_{i,j}}$ be a term in f with $\sum \beta_{i,j} = \deg(f)$. Proposition 6.1.1 allows us to conclude that for any $S_{i,j} \subseteq GF(p)$ with $|S_{i,j}| > \beta_{i,j}$, there are $s_{i,j} \in S_{i,j}$ such that $f(s_{i,j} : 1 \leq i, j \leq n) = 1$. Unfortunately, if some $\beta_{i,j} \geq 2$, we cannot set $S_{i,j} = \{0, 1\}$ and cannot, therefore, guarantee that $s_{i,j} \in \{0, 1\}$.

To fix this problem, let g be the polynomial resulting from f by replacing each occurrence of $x_{i,j}^d$ with $x_{i,j}$ for $1 \leq i, j \leq n$ and $d \geq 2$. Polynomials g and

f will typically have dramatically different supports but notice that they will always agree on binary valuations. Furthermore, note that $\deg(g) \leq \deg(f)$. Let $\prod_{i,j} x_{i,j}^{\beta_{i,j}}$ be a term in g with $\sum \beta_{i,j} = \deg(g)$. Since $\beta_{i,j} \in \{0,1\}$, we may set $S_{i,j} = \{0,1\}$ for $\beta_{i,j} = 1$ and $S_{i,j} = \{0\}$ for $\beta_{i,j} = 0$.

Proposition 6.3.2. *Let p be prime and $n = kp + 1$ for $k \geq 3$. Every latin square of order n has a subset of cells no larger than $3(p-1)n < n^2$ that meets each row, column, and symbol $1 \mod p$ times.*

Proof. Consider the polynomial $f \in GF(p)[x]$ defined by

$$f = \prod_{i=1}^{n} \prod_{j=2}^{p} (e_1(R_i) - j)(e_1(C_i) - j)(e_1(S_i) - j).$$

Observe that $e_1(R_i) - j = 0$ if and only if $j \mod p$ cells have been selected in row i. Thus $f(z) = 0$ if and only if z meets some row, column, or symbol a number of times not congruent to $1 \mod p$. Since $f(L) = 1$ and $\deg(f) \leq 3(p-1)n$, we may employ the trick outlined above to reduce to a polynomial g with the same binary support as f. The claim now follows from Proposition 6.1.1. □

Chapter 7

Complete Mappings

7.1 Background

In this chapter, we take a much more algebraic perspective on the study of transversals of latin squares. Every latin square may be viewed as the multiplication table of a quasigroup, and conversely. Here we study the topic of transversals of a latin square from the perspective of quasigroups. In particular, for a quasigroup $(Q, \cdot)$ a *complete mapping* is a permutation $\theta : Q \to Q$ such that the map $x \mapsto x \cdot \theta(Q)$ is also a permutation. Notice that θ is a complete mapping of $(Q, \cdot)$ if and only if the entries $\{(x, \theta(x), x \cdot \theta(x)) : x \in Q\}$ form a transversal of the multiplication table of Q.

We say that a quasigroup has a transversal if it has a complete mapping. The most important result in the study of complete mappings is the following proposition.

Proposition 7.1.1. *Suppose that G is a finite group. The following are equivalent:*

(1) G has a complete mapping,

(2) the Sylow 2-subgroups of G are trivial or non-cyclic, and

(3) there is an ordering of the elements of G such that $g_1 \cdots g_n = 1$.

Hall and Paige [26] first proposed the general conjecture and established it for the solvable, symmetric, and alternating cases in 1955. Over the following 30 years little headway was made until the late 1980s when transversals were shown to exist for large classes of finite groups (consult Evans [22] for an excellent survey of progress up to 1992). In 2001, Dalla Volta and Gavioli [12] proved that a minimal-counterexample to the conjecture must either be almost simple or posses a list of restrictive technical properties.

Wilcox [49] built upon this result to show that a minimal-counterexample must be a sporadic simple group or the Tits group. Many of these groups were already known to possess transversals, thus reducing the conjecture to identifying transversals in just 22 groups. Building upon this progress, Evans [24] constructed transversals in all remaining cases other than the Janko group J_4. John Bray has reportedly resolved this final case, thereby establishing the Hall-Paige conjecture.

It is the goal of the present chapter to initiate the study of the Hall-Paige conjecture in more general varieties of loops. We begin with the modest task of making sense of the above conditions in non-associative settings. While (1) translates directly, (2) and (3) present difficulties since it is not clear what a

Sylow 2-subloop should be and any product in a non-associative loop requires the specification of some association.

We propose natural generalizations of these conditions and establish several universal implications between them. As described in §7.2, we prove a number of related results including a generalization of the Dénes-Hermann theorem and provide an elementary proof of a weak form of the Hall-Paige conjecture.

7.1.1 Definitions

We call a subset $C = \{(x_i, y_i, z_i) : 1 \leq i \leq m\} \subseteq L$ *column-entry regular*, or just *regular* for short, if for each symbol s we have $|\{i : y_i = s\}| = |\{i : z_i = s\}|$. That is, s appears as an entry the same number of times it appears as a column. We denote by C_r the multiset of symbols appearing as rows in C. For example, if C is a k-plex, then C_r contains precisely k copies of each symbol. We will be primarily interested in regular row transversals, i.e. selections of a single cell from each row so that each symbol appears as a column the same number of times as an entry (Figure 7.1 depicts such a selection in the multiplication table of a loop).

A set with a binary operation, say $(Q, \cdot)$, is a *quasigroup* if for each $x, z \in Q$, the equations $x \cdot y_1 = z$ and $y_2 \cdot x = z$ have unique solutions $y_1, y_2 \in Q$. A quasigroup with a neutral element is called a *loop*. We will always denote the neutral element by 1. A *group* is an associative loop. We assume in all cases that Q is finite and typically write Q rather than $(Q, \cdot)$. We write $A(Q)$ for the associator subloop of Q, the smallest normal subloop of Q such that $Q/A(Q)$ is a group. Likewise, we write Q' for the derived subloop of Q, the smallest normal subloop of Q such that Q/Q' is an Abelian group. Note that $A(Q) \trianglelefteq Q'$

and thus cosets of Q' are partitioned by cosets of $A(Q)$. When Q is a group, $A(Q) = \{1\}$.

The *multiplication table* of a loop Q is the set of triples $\{(x, y, xy) : x, y \in Q\}$. Multiplication tables of loops are latin squares and, up to the reordering of rows and columns, every latin square is the multiplication table of some loop. It thus makes sense to say that a loop has a k-plex or more generally a regular row k-plex whenever its multiplication table does.

Most literature on the Hall-Paige conjecture focuses on the concept of a complete mapping of a group rather than a transversal of its multiplication table, though the two are completely equivalent [14, p. 7]. In the general loop setting, we prefer the latter concept as it emphasizes the combinatorial nature of the problem and generalizes more naturally to the concepts of k-plexes and regular k-plexes.

For $H \subseteq Q$ and $k \geq 1$, let $P^k(H)$ be the set of elements in Q that admit factorizations containing every element of H precisely k times. We call these elements *full k-products of H*. When $k = 1$, we write just $P(H)$ and refer to its elements as *full products of H*. We work primarily in the case $H = Q$ and simply refer to these elements as *full k-products*. While in the group case, the set $P(G)$ has been well-studied (see the commentary preceding Theorem 7.2.4 for some background), to the best of our knowledge, the present chapter contains the first investigation of the general loop case.

Although we assume a basic familiarity with both loops and latin squares, we provide references for any non-trivial results that we employ. For standard references for loops, consult Bruck [7] and Pflugfelder [35].

7.2 Summary of Results

Conjecture 7.2.1 (Hall-Paige conjecture 1955 [26])**.** *In every group G, the following are equivalent:*

(1) G has a transversal,

(2) Sylow 2-subgroups of G are trivial or non-cyclic, and

(3) $1 \in P(G)$.

We propose the following condition as a fruitful interpretation of the Hall-Paige conjecture in varieties of loops in which associativity need not hold.

Definition 7.2.2 (HP-condition)**.** *A class of loops $\mathcal{Q}$ satisfies the* HP-condition *if for each $Q \in \mathcal{Q}$ the following are equivalent:*

(A) Q has a transversal,

(B) there does not exist $N \trianglelefteq Q$ such that $|N|$ is odd and $Q/N \cong \mathbb{Z}_{2^m}$ for $m \geq 1$, and

(C) $A(Q)$ intersects $P(Q)$ nontrivially.

When $\mathcal{Q}$ is the variety of groups, satisfaction of the HP-condition reduces to the Hall-Paige conjecture. The equivalence of (1) and (A) is clear; as is that of (3) and (C), given that when Q is a group, $A(Q) = \{1\}$. We take an indirect approach to showing (2) $\iff$ (B) by showing (B) $\iff$ (C), a corollary of Propositions 7.2.5 and 7.2.6. In 2003, Vaughan-Lee and Wanless [44] provided the first elementary proof of (2) $\iff$ (3). Their paper also

provides some background on this result (whose initial proof invoked the Feit-Thompson theorem).

As corollaries of our main results, we show that in all loops (B) $\iff$ (C) and (A) $\implies$ (B) $\wedge$ (C).

The following easy observation sets the context for our main results. It is well-known in the group case and follows in the loop case for the same simple reasons. We include it in Lemma 7.3.1 for completeness.

Observation 7.2.3. *$P^k(Q)$ is contained in a single coset of Q'.*

At least as far back as 1951, authors have asked whether, in the group case, this observation can be extended to show that $P^k(Q)$ in fact coincides with this coset. For a history of this line of investigation, see [13, p. 35] and [14, p. 40]. This result now bears the names of Dénes and Hermann who first established the claim for all groups.

Proposition 7.2.4 (Dénes, Hermann [15] 1982)**.** *If G is a group, then $P(G)$ is a coset of G'. It follows that $P^k(G)$ is also a coset of G'.*

A more general way to read this statement is that $P(G)$ intersects every coset of $A(G)$ that is contained in the relevant coset of G'. Since $A(G) = \{1\}$ and these cosets partition cosets of G', this overly technical phrasing reduces to the proposition as stated. We extend the Dénes-Hermann theorem to show that this more general phrasing holds in all loops. Although the result is more general, our proof of Proposition 7.2.5 does rely upon the Dénes-Hermann theorem. In §7.7, we discuss the possibility of generalizing the theorem completely.

Proposition 7.2.5. *If $P(Q) \subseteq xQ'$, then $P(Q) \cap yA(Q) \neq \emptyset$ for all $y \in xQ'$. That is, $P(Q)$ intersects every coset of $A(Q)$ contained in xQ' and, in particular, if $P(Q) \subseteq Q'$, then $P(Q)$ intersects $A(Q)$. It follows that $P^k(Q)$ also intersects every coset of $A(Q)$ in the corresponding coset of Q'.*

Coupled with Proposition 7.2.5, our next result establishes (B) $\iff$ (C).

Proposition 7.2.6. *$P(Q) \subseteq Q'$ if and only if (B) holds.*

In 1951, Paige [34] showed that if a group G has a transversal, then $1 \in P(G)$. We extend this result to a much wider class of structures.

Proposition 7.2.7. *If C is a regular subset of the multiplication table of Q, then $P(C_r)$ intersects $A(Q)$. In particular, if Q has a k-plex (or just a regular row k-plex), then $P^k(Q)$ intersects $A(Q)$.*

Applying these results, we establish that for all loops:

- (A) $\implies$ (C) by Proposition 7.2.7 and
- (B) $\iff$ (C) by Propositions 7.2.5 and 7.2.6.

By 1779, Euler had shown that a cyclic group of even order has no transversal and in 1894 Maillet extended his argument to show that all loops for which condition (B) fails lack transversals [13, p. 445]. In 2002, Wanless [46] showed that such loops lack not just transversals, i.e. 1-plexes, but contain no odd-plexes at all. While their arguments are quite nice, our proof of (A) $\implies$ (B) provides an alternative, more algebraic proof of these results.

Corollary 7.2.8. *If a loop fails to satisfy (B), then it has no regular row odd-plexes.*

It is not true in general that (B) $\wedge$ (C) $\implies$ (A) (for a smallest possible counter-example, see Figure 7.1). We are however interested in identifying nonassociative classes of loops in which the equivalence holds. In a separate paper still in preparation [38], we show that the HP-condition is satisfied by several technical varieties of loops that include non-assoicative members and provide both computational and theoretical evidence suggesting that the variety of Moufang loops also satisfies the HP-condition.

Q	1	2	3	4	5	6
1	[1]	2	3	4	5	6
2	2	1	4	[3]	6	5
3	3	5	[1]	6	2	4
4	[4]	6	2	5	1	3
5	5	3	6	2	4	[1]
6	[6]	4	5	1	3	2

Figure 7.1: Loop Q with no transversal and yet $P(Q) = Q' = Q$. Q contains 168 regular row transversals, one of which has been bracketed.

The Hall-Paige conjecture is typically stated with the additional claim that G can be partitioned into n mutually disjoint transversals, i.e. G has an orthogonal mate. In the group case, it is easy to show that having an orthogonal mate is equivalent to having at least one transversal. While this equivalence may extend to other varieties of loops (for example, we believe it holds in at least Moufang loops), the argument seems unrelated to the difficult part of the conjecture, which the HP-condition seeks to capture.

We do however introduce a weakening of the orthogonal mate condition in the following proposition. While this result follows directly from a combination of the Hall-Paige conjecture and Proposition 7.2.7, we provide an elementary proof.

Proposition 7.2.9. *If G is a group of order n, then the following are equivalent:*

1. *G has a regular row transversal,*
2. *G can be partitioned into n mutually disjoint regular row transversals,*
3. *Sylow 2-subgroups of G are trivial or non-cyclic, and*
4. *$1 \in P(G)$.*

Corollary 7.2.10. *The Hall-Paige conjecture is equivalent to the claim that a group has a transversal if and only if it has a regular row transversal.*

We make the following two observations not to suggest that our methods may be useful in tackling these important problems but rather to indicate their theoretical context.

Observation 7.2.11. *When $\mathcal{Q}$ is the class of odd ordered loops, condition (B) always holds and thus satisfaction of the HP-condition is equivalent to Ryser's conjecture [46, p. 11], that every latin square of odd order has a transversal.*

One natural extension of the HP-condition might be that Q has a 2-plex if and only if $A(Q)$ intersects $P^2(Q)$. Since this latter condition is satisfied in all loops, this formulation is equivalent to Rodney's conjecture [11, p. 105], that every latin square has a 2-plex.

7.3 Properties of the sets $P^k(Q)$

We begin with a sequence of easy observations about the sets $P^k(Q)$.

Lemma 7.3.1. *For $i, j, k \geq 1$,*

1. $1 \in P^2(Q)$,
2. $P^i(Q)P^j(Q) \subseteq P^{i+j}(Q)$ *and* $|P^k(Q)| \leq |P^{k+1}(Q)|$,
3. $P^k(Q)$ *is contained in a coset of* Q',
4. $P^k(Q) \subseteq P^{k+2}(Q)$,
5. $P^2(Q) \subseteq Q'$, *and*
6. $P(Q) \subseteq aQ'$ *where* $a^2 \in Q'$.

Proof. 1 Let q^ρ be the right inverse of q. Then $1 = \prod_{q \in Q} qq^\rho \in P^2(Q)$.

2 Observe that $P^i(Q)P^j(Q) = \{ab : a \in P^i(Q), b \in P^j(Q)\}$. Thus ab is a full $(i+j)$-product. It then follows that $|P^k(Q)| \leq |P^{k+1}(Q)|$ since for $q \in P(Q)$, $qP^k(Q) \subseteq P^{k+1}(Q)$ and $|P^k(Q)| = |qP^k(Q)|$.

3 Any two elements of $P^k(Q)$ have factors that differ only in their order and association. In other words, if $x, y \in P^k(Q)$, then $xQ' = yQ'$.

4 By 1, we have $1 \in P^2(Q)$; thus $P^k(Q) = P^k(Q) \cdot 1 \subseteq P^k(Q)P^2(Q)$. By 2 we have $P^k(Q)P^2(Q) \subseteq P^{k+2}(Q)$. Thus $P^k(Q) \subseteq P^{k+2}(Q)$.

5 The claim follows immediately from 1 and 3.

6 By 3, $P(Q) \subseteq aQ'$ for some $a \in Q$ and thus $P(Q)^2 \subseteq a^2Q'$. By 2, $P(Q)^2 \subseteq P^2(Q)$ and by 5 $P^2(Q) \subseteq Q'$. It follows that $a^2Q' = Q'$ and thus $a \in Q'$. □

Our next lemma uses the idea that Q/N is a set of cosets of N and thus $P(Q/N)$ is a subset of these cosets.

Lemma 7.3.2. *If $N \trianglelefteq Q$, $|N| = k$, and $a_1N, \ldots, a_kN \in P(Q/N)$, then $P(Q) \cap (a_1N \cdots a_kN) \neq \emptyset$. That is, $P(Q)$ intersects every member of $P(Q/N)^k$.*

Proof. Let $|Q| = mk$. For any $aN \in P(Q/N)$, we may select a system of coset representatives of N in Q, say $\{x_1, \ldots, x_m\}$, and some association of the left hand side such that

$$x_1N \cdots x_mN = aN \tag{7.3.1}$$

and thus using the same association pattern $x_1 \cdots x_m \in aN$. Furthermore, since (7.3.1) depends only on the order and association of the cosets of N (rather than the specific representatives chosen), we may select k disjoint sets of coset representatives of N in Q, say $\{x_{(i,1)}, \ldots, x_{(i,m)} : 1 \leq i \leq k\}$, and corresponding association patterns such that

$$(x_{(1,1)} \cdots x_{(1,m)}) \cdots (x_{(k,1)} \cdots x_{(k,m)}) \in a_1N \cdots a_kN \in P(Q/N)^k$$

for any selection of $a_iN \in P(Q/N)$ for $1 \leq i \leq k$. Having selected each element of Q as a coset representative precisely once, the left-hand side falls in $P(Q)$ and we are done. □

7.4 When does $P^k(Q)$ intersect $A(Q)$?

For $x \in Q$, we write L_x (R_x) for the left (right) translation of Q by x. Our notation for the left translation is not to be confused with the convention of using L for a latin square.

The *multiplication group of* Q, written $\mathrm{Mlt}(Q)$, is the subgroup of S_Q generated by all left and right translations, i.e. $\langle L_x, R_x : x \in Q \rangle$, while the *left multiplication group of* Q, written $\mathrm{LMlt}(Q)$, is generated by all left translations. If $H \trianglelefteq Q$ and $\rho \in \mathrm{Mlt}(Q)$, we may define the map $\rho_H(xH) := \rho(x)H$, which is said to be induced by ρ. It is straightforward to verify that the map is well-defined and that $\rho_H \in \mathrm{Mlt}(Q/H)$.

To prove Proposition 7.2.7 in the group case one would like to use the fact that from an identity of the form $a_1(a_2(\cdots(a_k x)\cdots) = x$ we may conclude that $a_1(a_2(\cdots(a_k)\cdots) = 1$, which is trivial in the presence of associativity but typically false otherwise. In the general loop case, the following lemma shows we can at least conclude that $a_1(a_2(\cdots(a_k)\cdots) \in A(Q)$.

Lemma 7.4.1.

1. *If $\rho \in LMlt(Q)$, then $\rho_{A(Q)} = L_{\rho(1)A(Q)}$.*

2. *If $\rho \in Mlt(Q)$, then $\rho_{Q'} = L_{\rho(1)Q'}$.*

3. *If $a_1(a_2(\cdots(a_k x)\cdots) = x$, then $a_1(a_2(\cdots(a_k)\cdots) \in A(Q)$.*

Proof. Set $A := A(Q)$.

(i) Let $\rho = L_{a_1} \cdots L_{a_k}$. Then $\rho_A(qA) = a_1(a_2 \cdots (a_k q) \cdots)A$. Since Q/A is a group, we may reassociate to get $\rho_A(qA) = a_1(a_2 \cdots (a_k) \cdots)A \cdot qA = \rho(1)A \cdot qA$. Thus $\rho_A = L_{\rho(1)A}$.

(ii) Let $\rho = T_{a_1}^{\epsilon_1} \cdots T_{a_k}^{\epsilon_k}$ where $T^{\epsilon_i} \in \{L, R\}$. Since Q/Q' is an Abelian group, we may reassociate and commute to get $\rho_{Q'}(qQ') = a_1(a_2 \cdots (a_k) \cdots)Q' \cdot qQ' = \rho(1)Q' \cdot qQ'$. Thus $\rho_{Q'} = L_{\rho(1)Q'}$.

(iii) Let $\rho(z) := a_1(a_2(\cdots(a_k z)\cdots)$. Since $\rho_A(xA) = \rho(x)A = xA$, the map ρ_A has a fixed point. As it is a left translation, it must be constant. Thus $\rho_A(A) = A$ and in particular $\rho(1) = a_1(a_2(\cdots(a_k)\cdots) \in A$. □

Lemma 7.4.1 is stated somewhat more generally then we actually need. If the translation notation feels cumbersome, the idea is very basic. Given the product $a_1(a_2(\cdots(a_k x)\cdots) = x$, we may reduce both sides mod A to get

$$a_1 A a_2 A \cdots a_k A x A = xA$$

$$a_1 A a_2 A \cdots a_k A = 1A$$

$$a_1 a_2 \cdots a_k \in A$$

.

Lemma 7.4.2. *If $C \neq \emptyset$ is regular, then there exists C' such that*

1. *$\emptyset \neq C' \subseteq C$,*
2. *$P(C'_r)$ intersects $A(Q)$, and*
3. *$C \setminus C'$ is regular.*

It follows that $P(C_r)$ intersects $A(Q)$.

Proof. Let $[k] := \{1, \ldots, k\}$. Suppose $C = \{(x_i, y_i, z_i) : i \in [k]\}$ is regular. Select $i_1 \in [k]$ at random. Having selected $i_1, \cdots, i_m \in [k]$, pick $i_{m+1} \in [k]$

such that $y_{i_m} = z_{i_{m+1}}$. Since C is regular, such a selection can always be made. If $i_{m+1} \notin \{i_1, \ldots, i_m\}$, continue.

Otherwise, stop and consider the set $\{i_j, \ldots, i_m\}$ where $i_j = i_{m+1}$. Reindex C such that $\langle i_j, \ldots, i_m \rangle = \langle 1, \cdots, s \rangle$ and set $C' := \{(x_i, y_i, z_i) : 1 \leq i \leq s\}$. Note that $y_s = z_1$. By construction, C' has the following form:

$$\begin{aligned} C' = \{&(x_1, y_1, y_s), \\ &(x_2, y_2, y_1), \\ &(x_3, y_3, y_2), \\ &\cdots \\ &(x_{s-1}, y_{s-1}, y_{s-2}), \\ &(x_s, y_s, y_{s-1})\}. \end{aligned}$$

C' is clearly regular and thus so too is $C \setminus C'$. Furthermore, by construction we have $x_1(x_2(\cdots(x_s z_1)\cdots)) = z_1$.

By Lemma 7.4.1, $x_1(x_2(\cdots(x_s)\cdots)) \in A(Q)$. Since this product is in $P(C'_r)$ as well, $P(C'_r) \cap A(Q) \neq \emptyset$. Iterating this construction we have $P(C_r)$ intersects $A(Q)$.

□

Proof of Proposition 7.2.7. If C is a k-plex, then C_r consists of k copies of each element of Q and thus $P(C_r) = P^k(Q)$. By Lemma 7.4.2, $P^k(Q)$ intersects $A(Q)$. □

7.5 A Weaker Hall-Paige Theorem

Lemma 7.5.1. *If G is a group and $g_1, \ldots, g_k \in G$ such that $g_1 \cdots g_k = 1$ and no proper contiguous subsequence evaluates to 1, then G admits a regular set C such that $C_r = \{g_1, \ldots, g_k\}$ and no column (and thus no entry) is selected more than once.*

Proof. Set $h_i := g_{i+1} \cdots g_k$ for $1 \leq i \leq k-1$ and $h_0 = h_k := 1$. Note that we have $g_i h_i = h_{i-1}$ for $1 \leq i \leq k$. We claim that $C := \{(g_i, h_i, h_{i-1}) : 1 \leq i \leq k\}$ is the desired regular set. It is clear that C is regular and that $C_r = \{g_1, \ldots, g_k\}$. To see that no column is selected more than once, suppose that $h_i = h_{i+j}$ for $j \geq 1$. That is, $g_{i+1} \cdots g_k = g_{i+j+1} \cdots g_k$. Canceling on the right, we have $g_{i+1} \cdots g_{i+j} = 1$, a contradiction. □

Proof of Proposition 7.2.9.

(i) $\Longrightarrow$ (ii) In this case we may use the standard argument from the group case showing that a single transversal extends to n disjoint transversals. Let $T = \{(x_i, y_i, z_i) : 1 \leq i \leq n\}$ be a regular row transversal of G. For each $g \in G$, form $T_g := \{(x, yg, zg) : (x, y, z) \in T\}$. It is easy to check that the family $\{T_g : g \in G\}$ partitions the multiplication table of G into regular row transversals.

(i) $\Longleftarrow$ (ii) If G admits a partition into regular row transversals, then it certainly has a regular row transversal.

(i) $\Longrightarrow$ (iv) Let T be a regular row transversal. By Proposition 7.2.7, $P(G) \cap A(G) \neq \emptyset$ and thus $1 \in P(G)$.

(i) $\Longleftarrow$ (iv) Let $g_1 \cdots g_n = 1$. We partition G as follows:

- If no proper contiguous subsequence of $g_1 \cdots g_n$ evaluates to 1, stop.
- Otherwise, extract the offending subsequence $g_i \cdots g_j = 1$ and note that $g_1 \cdots g_{i-1} g_{j+1} \cdots g_n = 1$.
- Iterate this process with these shortened products.

Suppose we have thus partitioned G into k disjoint sequences $\{g_{(i,1)}, \ldots, g_{(i,n_i):1 \leq i \leq k}\}$ such that $g_{(i,1)} \cdots g_{(i,n_i)} = 1$ for $1 \leq i \leq k$ and no proper contiguous subsequence of $g_{(i,1)}, \ldots, g_{(i,n_i)}$ evaluates to 1. Now we apply Lemma 7.5.1 to each subsequence to get regular sets C_i for $1 \leq i \leq k$. Then $\bigcup_{i=1}^{k} C_i$ is a regular row transversal of G.

(iii) $\Longleftrightarrow$ (iv) As noted earlier, this is an established equivalence in the Hall-Paige conjecture.

□

7.6 An equivalence for $P(Q) \subseteq Q'$

Lemma 7.6.1. (2) $\Longleftrightarrow$ (3) *holds for Abelian groups.*

Proof. As mentioned above Vaughan-Lee and Wanless [44] give a direct, elementary proof of this result for all groups. For an earlier though indirect proof, Paige [33] showed that (1) $\Longleftrightarrow$ (2) holds in Abelian groups and Hall and Paige [26] showed that (1) $\Longleftrightarrow$ (3) in solvable groups. □

Lemma 7.6.2. *If a group G has a cyclic Sylow 2-subgroup S, then there exists $N \trianglelefteq G$ such that $G/N \cong S$.*

Proof. This is a direct application of Burnside's Normal Complement theorem that can be found in most graduate level group theory texts (see [52] for example). □

Proof of Proposition 7.2.6. ($\Longleftarrow$) We show the contrapositive. Suppose $P(Q) \subseteq aQ' \neq Q'$. Since $G := Q/Q'$ is an Abelian group, $P(G) = \{bQ'\}$ such that $b^2 \in Q'$. By Lemma 7.3.2, $P(Q)$ intersects every element of $P(G)^{|Q'|} = \{b^{|Q'|}Q'\}$ and thus $aQ' = b^{|Q'|}Q'$. Since $aQ' \neq Q'$ and $b^2 \in Q'$, it follows that $aQ' = bQ'$ and $|Q'|$ is odd.

Since $P(G) \neq \{1Q'\}$, by Lemmas 7.6.1 and 7.6.2 there is $N \trianglelefteq G$ such that $|N|$ is odd and $G/N \cong \mathbb{Z}_{2^m}$. N is a collection of coset of Q'. Letting H be their union, we have $Q/H \cong G/N \cong \mathbb{Z}_{2^m}$ and $|H| = |N||Q'|$ is odd.

($\Longrightarrow$) Again we argue the contrapositive. Suppose $N \trianglelefteq Q$ such that $|N| = q$ is odd and $Q/N \cong \mathbb{Z}_{2^m}$ for $m \geq 1$. Since $Q/N \cong \mathbb{Z}_{2^m}$, $P(Q/N) = \{aN\} \neq \{N\}$ such that $a^2 \in N$. By Lemma 7.3.2, $P(Q)$ intersects every element of $P(Q/N)^{|N|} = \{aN\}^{|N|} = \{aN\}$.

Given that Q/N is an Abelian group, $Q' \subseteq N$ but since $P(Q)$ intersects $aN \neq N$, it is therefore disjoint from Q'. □

7.7 A Generalization of the Dénes-Hermann Theorem

The *left*, *right*, and *middle inner mappings* are defined as $L(x,y) = L_{yx}^{-1}L_yL_x$, $R(x,y) = R_{xy}^{-1}R_yR_x$, and $T(x) = R_x^{-1}L_x$, respectively. A subloop S of a loop Q is said to be *normal*, written $S \trianglelefteq Q$, if S is invariant under all inner mappings

of Q. A loop Q is *simple* if it has no normal subloops except for $\{1\}$ and Q. An *A-loop* is a loop in which all inner mappings are automorphisms. The variety of A-loops is larger than that of groups but is certainly not all loops. Bruck and Paige [8] conducted the earliest extensive study of A-loops.

Before proving Proposition 7.2.5, we make several additional observations about the sets $P^k(Q)$. While none of these results will be used directly in our proof, we hope they are of some interest in that they may suggest an alternative proof of the Dénes-Hermann theorem.

Lemma 7.7.1. *Set* $P^\omega := \bigcup_{i=1}^{\infty} P^i(Q)$.

1. $P^\omega \leq Q$,
2. $P^\omega = P^k(Q) \cup P^{k+1}(Q)$ *for sufficiently large* k,
3. *If* $P^\omega \trianglelefteq Q$, *then* $P^\omega = Q'$ *or* $P^\omega = Q' \cup aQ'$ *where* $a^2 \in Q'$, *and*
4. P^ω *is fixed by all automorphisms of* Q. *Thus, if* Q *is an A-loop, then* $P^\omega \trianglelefteq Q$.

Proof. (i) Since Q is finite, we need only verify that P^ω is closed under multiplication. If $x, y \in P^\omega$, then $x \in P^i(Q)$ and $y \in P^j(Q)$ for some $i, j \geq 1$. Thus $xy \in P^{i+j}(Q) \subseteq P^\omega$.

(ii) Again, since Q is finite, the nested sequence $(P^{2i}(Q) : 1 \leq i < \infty)$ must terminate at some step, say $P^{k_1}(Q)$. Likewise $(P^{2i+1}(Q) : 1 \leq i < \infty)$ must terminate at some step, say $P^{k_2}(Q)$. Thus letting $k = \max\{k_1, k_2\}$, we have $P^\omega = P^k(Q) \cup P^{k+1}(Q)$. (In fact, by Lemma 7.3.1 part (ii), the sequences terminate at the same time.)

(iii) Suppose $P^\omega \trianglelefteq Q$. We show that Q/P^ω is an Abelian group and thus $Q' \subseteq P^\omega$. To see that Q/P^ω is a group, note that $aP^\omega bP^\omega \cdot cP^\omega = (ab \cdot c)P^\omega$. We would like to show that $(ab \cdot c)P^\omega = (a \cdot bc)P^\omega$.

To that end, let $a' \in P(Q \setminus \{a\})$ and likewise for b' and c'. We translate both $(ab \cdot c)P^\omega$ and $(a \cdot bc)P^\omega$ by $(a'b' \cdot c')P^\omega$ on the left to get

$$(a \cdot bc)P^\omega \cdot (a'b' \cdot c')P^\omega = [(a \cdot bc) \cdot (a'b' \cdot c')]P^\omega$$
$$(ab \cdot c)P^\omega \cdot (a'b' \cdot c')P^\omega = [(ab \cdot c) \cdot (a'b' \cdot c')]P^\omega$$

Note that both $(a \cdot bc) \cdot (a'b' \cdot c')$ and $(ab \cdot c) \cdot (a'b' \cdot c')$ are elements of $P(Q)$ and thus both right-hand sides reduce to P^ω. Thus both $(ab \cdot c)P^\omega$ and $(a \cdot bc)P^\omega$ are left inverses of $(a'b' \cdot c')P^\omega$. Since left inverses are unique, we have $(ab \cdot c)P^\omega = (a \cdot bc)P^\omega$ and Q/P^ω is a group.

To see that Q/P^ω is Abelian, consider $aP^\omega bP^\omega$ and $bP^\omega aP^\omega$. Again let $a' \in P(Q \setminus \{a\})$ and $b' \in P(Q \setminus \{b\})$. We then have

$$abP^\omega \cdot a'b'P^\omega = (ab \cdot a'b')P^\omega$$
$$baP^\omega \cdot a'b'P^\omega = (ba \cdot a'b')P^\omega$$

Since $(ab \cdot a'b')$ and $(ba \cdot a'b')$ are both members of $P(Q)$, the right-hand sides reduce to P^ω. As above, it follows that $aP^\omega bP^\omega = bP^\omega aP^\omega$. Since Q' is the smallest normal subloop of Q such that Q/Q' is an Abelian group, $Q' \subseteq P^\omega$.

(iv) First note that for $i \geq 1$, $P^i(Q)$ is always fixed by automorphisms of Q and thus so is P^ω. If Q is an A-loop, then P^ω is fixed by every inner-mapping. $\square$

In the spirit of the observations made in Lemma 7.7.1, Yff [51, p. 269] showed that when G is a group, $P^3(G)$ coincides with a coset of G'. Although this fact is an easy application of the Dénes-Hermann theorem, his proof applies directly to all finite groups and avoids the use of the Feit-Thompson theorem.

To our knowledge, Proposition 7.2.5 is the first extension beyond groups of the Dénes-Hermann theorem. Although our generalization is rather modest, we suspect the result extends completely.

Problem 7.7.2. *For larege $|Q|$, is $P(Q)$ always a coset of Q'?*

The Dénes-Hermann theorem is equivalent to the claim that for any finite group G we have that $|\{g_1 \cdots g_n : \text{ ranging over all orderings }\}| = |G'|$.

To establish Conjecture 7.7.2, it would suffice to show the perhaps stronger claim that given any fixed ordering of the elements of Q, we have

$$|\{q_1 \cdots q_n : \text{ ranging over all associations }\}| = |A(Q)|.$$

Observation 7.7.3. *Proposition 7.7.4 is motivated by the following question: if G is a group and $a \in P(G)$, does it follow that $a \in P(G_2)$ where G_2 is the set of involutions in G? That is, does $P(G) = P(G_2)$?*

Proposition 7.7.4. *Let Q_2 be the set of involutions in Q. If Q has two-sided inverses, then $P^k(Q_2) \subseteq P^k(Q)$.*

Proof. Note that $^{-1}$ is an involution in S_Q whose fixed points are precisely the elements of Q_2 and the identity element. We thus have that $1 \in P(Q \setminus Q_2) \subseteq Q'$. Since $P(Q_2)P(Q \setminus Q_2) \subseteq P(Q)$, we are done. □

We recall the following special case of the correspondence and isomorphism theorems, proofs of which can be found in most standard universal algebra texts.

Lemma 7.7.5. *If $N \trianglelefteq Q$ and $N \leq H \leq Q$, then*

1. *$H \trianglelefteq Q$ if and only if $H/N \trianglelefteq Q/N$ and*
2. *when $H \trianglelefteq Q$, $Q/H \cong (Q/N)/(H/N)$.*

We employ the following lemma in our proof of Proposition 7.2.5.

Lemma 7.7.6. $(Q/A(Q))' = Q'/A(Q)$.

Proof. Set $A := A(Q)$. By definition, $(Q/A)'$ is the smallest normal subloop of Q/A such that the factor loop is an Abelian group. Since $A \leq Q' \trianglelefteq Q$, by the correspondence theorem we have $(Q'/A) \trianglelefteq (Q/A)$ and $(Q/A)/(Q'/A) \cong Q/Q'$, an Abelian group. Thus $(Q/A)' \leq (Q'/A)$.

We now show $(Q'/A) \leq (Q/A)'$. Fix $N/A \trianglelefteq Q/A$ such that $(Q/A)/(N/A)$ is an Abelian group. Again by the correspondence theorem, $N \trianglelefteq Q$ and $Q/N \cong (Q/A)/(N/A)$. Since Q/N is an Abelian group, $Q' \leq N$ and thus $Q'/A \leq N/A$. It follows that $(Q'/A) \leq (Q/A)'$

□

Proof of Proposition 7.2.5. Let $A := A(Q)$ and $k := |A|$. Since $P(Q)$ is contained in a single coset of Q', it suffices to show that $P(Q)$ intersects at least $[Q' : A]$ cosets of A (the maximum possible).

By Theorem 7.2.4, $P(Q/A) = \{xA(Q/A)'\}$ such that $x^2A \in (Q/A)'$. By Lemma 7.7.6, $xA(Q/A)' = xA(Q'/A) = (xQ')A$. Thus we have $P(Q/A) =$

$\{(xQ')A\}$. By Lemma 7.3.2, $P(Q)$ intersects each of the $[Q' : A]$ elements of $P(Q/A)^k = \{(x^kQ')A\} = \{qA : q \in x^kQ'\}$. □

7.8 Concluding Remarks

We have proposed the HP-condition as a fruitful extension of the Hall-Paige conjecture from groups into the larger world of non-associative loops. Having shown several universal implications between the points of the HP-condition, we leave open the difficult problem of identifying interesting varieties of loops in which conditions (B) and (C) imply the existence of a transversal.

It would also be of interest to identify classes of loops in which the existence of a regular row transversal implies the existence of a transversal. As noted above, this implication in groups is equivalent to Proposition 7.2.1, the Hall-Paige conjecture.

Bibliography

[1] The on-line encyclopedia of integer sequences. http://oeis.org. 2010.

[2] Noga Alon. Combinatorial Nullstellensatz. *Combin. Probab. Comput.*, 8(1-2):7–29, 1999. Recent trends in combinatorics (Mátraháza, 1995).

[3] Noga Alon. Additive Latin transversals. *Israel J. Math.*, 117:125–130, 2000.

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

[5] 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(2):330–332, 1978.

[6] Richard A. Brualdi and Herbert J. Ryser. *Combinatorial matrix theory*, volume 39 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1991.

[7] R. H. Bruck. *A survey of binary systems*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge, Heft 20. Reihe: Gruppentheorie. Springer Verlag, Berlin, 1958.

[8] R. H. Bruck and Lowell J. Paige. Loops whose inner mappings are automorphisms. *Ann. of Math. (2)*, 63:308–323, 1956.

[9] Darryn Bryant, Judith Egan, Barbara Maenhaut, and I. M. Wanless. Indivisible plexes in latin squares. *Designs, Codes and Cryptography*, 52(1), July 2009.

[10] Peter J. Cameron and Ian M. Wanless. Covering radius for sets of permutations. *Discrete Math.*, 293(1-3):91–109, 2005.

[11] C. J. Colbourn and J. H. Dinitz. *The CRC Handbook of Combinatorial Designs*. CRC Press, Boca Raton, FL, 1996.

[12] F. Dalla Volta and N. Gavioli. Minimal counterexamples to a conjecture of Hall and Paige. *Arch. Math. (Basel)*, 77(3):209–214, 2001.

[13] J. Dénes and A. D. Keedwell. *Latin squares and their applications*. Academic Press, New York, 1974.

[14] J. Dénes and A. D. Keedwell. *Latin squares*, volume 46 of *Annals of Discrete Mathematics*. North-Holland Publishing Co., Amsterdam, 1991.

[15] József Dénes and Péter Hermann. On the product of all elements in a finite group. In *Algebraic and geometric combinatorics*, volume 65 of *North-Holland Math. Stud.*, pages 105–109. North-Holland, Amsterdam, 1982.

[16] David A. Drake. Maximal sets of Latin squares and partial transversals. *J. Statist. Plann. Inference*, 1(2):143–149, 1977.

[17] Judith Egan. Bachelor latin squares with large indivisible plexes. *Journal of Combinatorial Designs*, 2010.

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

[19] Judith Egan and Ian M. Wanless. Latin squares with no small odd plexes. *Journal of Combinatorial Designs*, 16(6):477–492, 2008.

[20] P. Erdös, 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(5):428–430, 1988.

[21] Leonhard Euler. Recherches sur une nouvelle espèces de quarrés magique. *Verh. uitgegeven door het Zeeuwsch Genootschap d. Wetensch. te Vlissingen*, pages 9:85–232, 1782.

[22] Anthony B. Evans. The existence of complete mappings of finite groups. In *Proceedings of the Twenty-third Southeastern International Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1992)*, volume 90, pages 65–75, 1992.

[23] Anthony B. Evans. Latin squares without orthogonal mates. *Des. Codes Cryptogr.*, 40(1):121–130, 2006.

[24] Anthony B. Evans. The admissibility of sporadic simple groups. *J. Algebra*, 321:1407–1428, 2009.

[25] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.

[26] Marshall Hall and L. J. Paige. Complete mappings of finite groups. *Pacific J. Math.*, 5:541–549, 1955.

[27] Marshall Hall, Jr. A combinatorial problem on abelian groups. *Proc. Amer. Math. Soc.*, 3:584–587, 1952.

[28] Pooya Hatami and Peter W. Shor. A lower bound for the length of a partial transversal in a Latin square. *J. Combin. Theory Ser. A*, 115(7):1103–1113, 2008.

[29] Klaas K. Koksma. A lower bound for the order of a partial transversal in a Latin square. *J. Combinatorial Theory*, 7:94–95, 1969.

[30] Charles F. Laywine and Gary L. Mullen. *Discrete mathematics using Latin squares*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons Inc., New York, 1998. A Wiley-Interscience Publication.

[31] E. Maillet. Sur les carrés latins d'euler. *C. R. Assoc. France Av. Sci*, 23(2):244–252, 1894.

[32] Brendan D. McKay, Jeanette C. McLeod, and Ian M. Wanless. The number of transversals in a Latin square. *Des. Codes Cryptogr.*, 40(3):269–284, 2006.

[33] L. J. Paige. A note on finite Abelian groups. *Bull. Amer. Math. Soc.*, 53:590–593, 1947.

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

[35] Hala O. Pflugfelder. *Quasigroups and loops: introduction*, volume 7 of *Sigma Series in Pure Mathematics*. Heldermann Verlag, Berlin, 1990.

[36] K. Pula. A Generalization of Plexes of Latin Squares. *Discrete Math.*, 311(8-9):577–581, May 2011.

[37] Kyle 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.

[38] Kyle Pula. Complete mappings of finite Moufang loops. preprint.

[39] H. J. Ryser. Neure probleme der kombinatorik in vortrdge uber kombinatorik. *Oberwolfach*, pages 24–29, 1967.

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

[41] Hunter S. Snevily. Unsolved Problems: The Cayley Addition Table of Z_n. *Amer. Math. Monthly*, 106(6):584–585, 1999.

[42] S. K. Stein. Transversals of Latin squares and their generalizations. *Pacific J. Math.*, 59(2):567–575, 1975.

[43] Sherman K. Stein and Sándor Szabó. The number of distinct symbols in sections of rectangular arrays. *Discrete Math.*, 306(2):254–261, 2006.

[44] M. Vaughan-Lee and I. M. Wanless. Latin squares and the Hall-Paige conjecture. *Bull. London Math. Soc.*, 35(2):191–195, 2003.

[45] Shinmin Patrick Wang. *ON SELF-ORTHOGONAL LATIN SQUARES AND PARTIAL TRANSVERSALS OF LATIN SQUARES*. ProQuest LLC, Ann Arbor, MI, 1978. Thesis (Ph.D.)–The Ohio State University.

[46] Ian M. Wanless. A generalisation of transversals for Latin squares. *Electron. J. Combin.*, 9(1):Research Paper 12, 15 pp. (electronic), 2002.

[47] Ian M. Wanless. Transversals in Latin squares: a survey. In R. Chapman, editor, *Surveys in Combinatorics 2011*, volume 392 of *London Math. Soc. Lecture Note Series*, pages pp403–437. Cambridge University Press, 2011.

[48] Ian M. Wanless and Bridget S. Webb. The existence of Latin squares without orthogonal mates. *Des. Codes Cryptogr.*, 40(1):131–135, 2006.

[49] Stewart Wilcox. Reduction of the hall-paige conjecture to sporadic simple groups. *J. Algebra*, 321(5):1407–1428, March 2009.

[50] David E. Woolbright. An $n \times n$ Latin square has a transversal with at least $n - \sqrt{n}$ distinct symbols. *J. Combinatorial Theory Ser. A*, 24(2):235–237, 1978.

[51] Peter Yff. On the Dénes-Hermann theorem: a different approach. *European J. Combin.*, 12(3):267–270, 1991.

[52] H. Zassenhaus. *The theory of groups*. Chelsea Publishing Co., New York, New York, 1949.