Existence of $L_d(n)$ and $ML_d(n, k)$

by

Elizabeth Schloss

A dissertation submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Auburn, Alabama
May 6, 2023

Keywords: Latin Squares, Multi-Latin Squares

Approved by

Peter Johnson, Chair, Professor of Mathematics
Joseph Briggs, Assistant Professor of Mathematics
Jessica McDonald, Associate Professor of Mathematics
Hal Schenck, Professor of Mathematics, Rosemary Kopel Brown Chair

Abstract

We are given an $n \times n$ array, $ML(n, k)$, with integers $n, d, k \geq 1$, such that $n = mk$ and each symbol in $\{0, ..., m-1\}$ appears in each row and column of the $ML(n, k)$ exactly k times. We aim to construct an $ML_d(n, k)$ with the restrictions below. It is required that the array is filled so that every symbol $i \in \mathbb{Z}_m$ appears exactly k times in each row and column, as before. We will add the restriction that at most one of symbol i appears in each $d \times d$ block inside of the original array. What are the possible values of n, k, and d? How do we arrange the symbols? In this dissertation, we will find the answer to these questions by finding necessary conditions for an $ML_d(n, k)$ to exist: $m > d^2$, then creating a construction to produce one. We will first assess the easier case of Latin squares, where $k = 1$, then move on to multi-Latin squares, where $k \geq 2$.

Acknowledgments

I would like to express my deepest gratitude to my advisor, Dr. Dean Hoffman, for inspiring me to become a better mathematician and teacher every day. Of course, this endeavor would not have been possible without Dr. Peter Johnson stepping in as my advisor and helping me to finish this journey.

Lastly, words can not express my appreciation for my family and friends, especially my husband, David, for their constant support and belief in me.

Table of Contents

List of Figures

Chapter 1

Background

1.1 Definitions and Examples

Definition 1.1.1. An $n \times n$ array is said to be row-Latin if each cell contains one of the symbols in $\sigma_0, \sigma_1, ..., \sigma_{n-1}$, such that each row of the array contains each of the symbols in $\sigma_0, \sigma_1, ..., \sigma_{n-1}$ exactly once. Column-Latin is defined similarly.

Definition 1.1.2. A Latin square of order n is an $n \times n$ array, each cell of which contains one of the symbols in $\sigma_0, \sigma_1, ..., \sigma_{n-1}$, such that each row and each column of the array contains each of the symbols in $\sigma_0, \sigma_1, ..., \sigma_{n-1}$ exactly once. [7]

1

$n = 1$

1	2
2	1

$n = 2$

1	2	3
2	3	1
3	1	2

$n = 3$

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

$n = 4$

Figure 1.1: Latin squares of size n [7]

Definition 1.1.3. A Latin square is said to be idempotent if cell (i, i) contains symbol i for $1 \leq i \leq n$. A Latin square is said to be commutative if cells (i, j) and (j, i) contain the same symbol for all $1 \leq i, j \leq n$. [7]

1	2	3
3	2	1
2	1	3

$n = 3$

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

$n = 5$

Figure 1.2: Idempotent and commutative Latin squares of size n [7]

Definition 1.1.4. Two Latin squares L_1 and L_2 are said to be orthogonal if for each $(x, y) \in \{1, 2, ..., n\} \times \{1, 2, ..., n\}$ there is exactly one ordered pair (i, j) such that cell (i, j) of L_1 contains the symbol x and cell (i, j) of L_2 contains the symbol y. [7]

Definition 1.1.5. A set of Latin squares $L_1, ..., L_m$ is mutually orthogonal, or a set of MOLS (mutually orthogonal Latin squares), if for $1 \leq a \neq b \leq m$, L_a and L_b are orthogonal. [7]

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

L_1

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

L_2

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

L_3

Figure 1.3: Three Mutually Orthogonal Latin Squares [7]

Definition 1.1.6. A subgrid $S(s, t, u, v)$ of an $m \times n$ grid, where $1 \leq s \leq t \leq m$ and $1 \leq u \leq v \leq n$, is the intersection of rows s through t and columns u through v. [1]

Definition 1.1.7. Let $d \in \mathbb{Z}^+$ with $1 \leq d \leq n$. $B[d]$ is a subgrid $S(s, s+d-1, t, t+d-1)$ for some $s, t \in \mathbb{Z}_n$.

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

A: Latin square of order n

5	3
3	1

$B[2]$ of A: $s = 2, t = 3$

5	3	1
3	1	4
1	4	2

$B[3]$ of A: $s = 2, t = 3$

Figure 1.4: Examples of $B[d]$

Definition 1.1.8. A $L_d(n)$ is an $n \times n$ Latin square such that every $B[d]$ contains at most one of symbol i, for all $i \in \mathbb{Z}_n$, for some integer $1 < d \leq n$.

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

Figure 1.5: Example of a $L_2(5)$

Note. Figure 1.4 is not an example of an $L_2(5)$ because the $B[2]$ chosen contains the symbol 3 more than once. However, no matter what $B[2]$ you look at in Figure 1.5, no symbol will appear more than once.

Definition 1.1.9. A multi-Latin square, $ML(n, k)$, with integers $n, k \geq 2$ such that $n = mk$, is an $n \times n$ array with rows and columns labeled $0, 1, ..., n-1$ and filled with symbols $0, 1, ..., m-1$, where every symbol $i \in \mathbb{Z}_m$ appears exactly k times in each row and column.

0	1	0	1
1	0	1	0
1	1	0	0
0	0	1	1

$ML(4, 2)$

0	1	2	0	1	2
1	2	0	1	2	0
2	0	1	2	0	1
0	1	2	0	1	2
1	2	0	1	2	0
2	0	1	2	0	1

$ML(6, 2)$

Figure 1.6: Examples of Multi-Latin Squares

Definition 1.1.10. An $ML_d(n, k)$ is an $ML(n, k)$, where $n, k \geq 2$ such that $n = mk$ and every $B[d]$ contains at most one of symbol i for all $i \in \mathbb{Z}_m$, for some integer $1 < d \leq n$.

row/column	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	0	1	2	3	4
1	3	4	0	1	2	3	4	0	1	2
2	1	2	3	4	0	1	2	3	4	0
3	4	0	1	2	3	4	0	1	2	3
4	2	3	4	0	1	2	3	4	0	1
5	4	0	1	2	3	4	0	1	2	3
6	2	3	4	0	1	2	3	4	0	1
7	0	1	2	3	4	0	1	2	3	4
8	3	4	0	1	2	3	4	0	1	2
9	1	2	3	4	0	1	2	3	4	0

Figure 1.7: Example of $ML_2(10, 2)$

1.2 History of Latin Squares

1.2.1 The Euler Officer Problem

The name "Latin Square" was inspired by Leonhard Euler (1707-1783) because of his use of Latin characters in the squares. However, the first instance published of a Latin square was from Choi Seok-Jeong in 1700 to construct a magic square. [3]

In 1778, Euler introduced the following problem:

> **The Euler Officers Problem:** "Six officers from each of six different regiments are selected so that the six officers from each regiment are of six different ranks, the same six ranks being represented by each regiment. Is it possible to arrange these 36 officers in a 6 $\times$ 6 array so that each regiment and each rank is represented exactly once in each row and column of this array?" [7] [5]

If a solution exists to this problem, it would be the same as forming two mutually orthogonal Latin squares of order 6. Euler made the following conjecture based off of his research of this problem:

Euler's Conjecture (1782): A pair of orthogonal Latin squares of order n exists if and only if n is congruent to 0, 1, or 3 (mod 4). [5]

In 1900, Tarry [9] used brute force to prove that there did not exist a pair of orthogonal Latin squares of order 6, proving that the Euler Officer Problem cannot be solved. Eventually, MacNeish made the following conjecture:

MacNeish's Conjecture (1922) "Let $n = p_1^{r_1}...p_x^{r_x}$, where each of $p_1, p_2, ..., p_x$ is a distinct prime. Then the maximum number of MOLS(n) is $m(n)$ =min$\{p_1^{r_1}, ..., p_x^{r_x}\} - 1$. [8]

Euler's conjecture is a special case of MacNeish's, and they were both proved wrong in 1960 when Bose, Shrikhande, and Parker [2] proved that a pair of orthogonal Latin squares of order n exists for all n except 2 and 6. Euler provided the initial spark for the history of this problem and many others. Design theory is a field that dates back to the problems of magic squares and Latin squares, and has grown into a large field of study with many open problems and applications today.

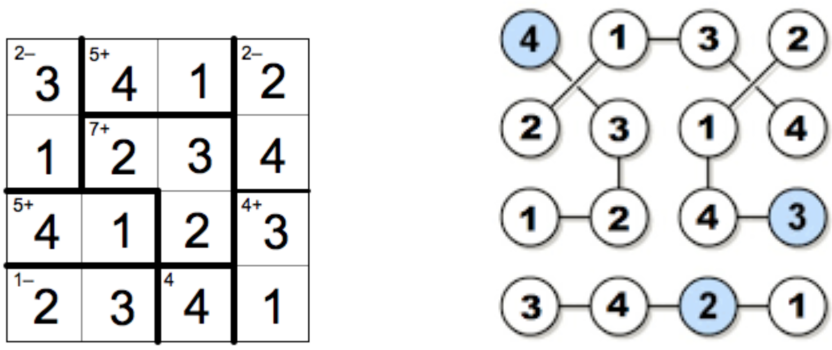
1.2.2 Applications of Latin Squares

As we have seen, Latin squares have many applications in the field of Design theory. However, it also plays a hand in many other fields. For example, in Algebra, Latin squares are related to groups. In particular, they can be characterized as the multiplication tables of quasigroups. Latin squares have also found applications in error correcting code. This application is mostly applied to noise other than basic white noise, specifically when trying to transmit internet over power lines. [4] [6] Latin squares are also found in every day puzzles. Sudoku is an example of a 9×9 Latin square with the extra condition that each of the specified blocks of size 3 needs to include every symbol in it exactly once. In the game, you are given certain placements of some of the numbers, and the player must fill in the rest. Below is an example of one where the blue numbers were given at the beginning, and the black numbers were filled in by the player.

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

Figure 1.8: Sudoku puzzle (Latin square of order 9)

There are many spin-offs of Sudoku that are similar Latin squares with different kinds of conditions on them. Below is an example of two popular spin-offs, KenKen and Strimko. In KenKen, you are given only the bold lines and the combination of the number and operation you see in the corner. You must satisfy each operation while forming a Latin square. For example, in the top right corner, there is a $2-$, meaning that for the cells contained in those bold lines, they must subtract to equal 2. In Strimko, you are given the numbers in the blue circles and the lines connecting the circles. From there, the player must fill in the rest to create a Latin square. The extra condition is that each stream (any circles connected by a single line) must contain different numbers.



KenKen Strimko

Figure 1.9: Popular Games Based off of Latin Squares

There are many more variations of puzzles on Latin squares. The main problem of this paper is similar to these puzzles as we are trying to form Latin squares with extra conditions on them.

1.3 Previous Work

1.3.1 Results from [1]

Definition 1.3.1. Let $k, d, n \in \mathbb{Z}^+$, where $1 \leq k$, $2 \leq d < n$. Then a (d,k,n)-tree planting (denoted as $TP(d,k,n)$) is a planting of exactly k trees (or a placement of exactly $k$symbols) in each row and column of n-grid such that there is at most one tree in any block $B[d]$.

The following are results from [1], numbered as they are in that dissertation.

Theorem 1.4 If $TP(d,k,n)$ exists, then $\lfloor \frac{n}{d^2} \rfloor \geq k$.

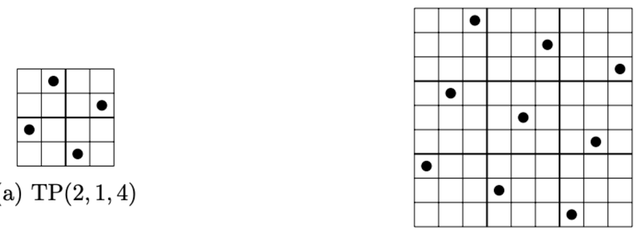
Proposition 1.6 $TP(d,k,kd^2)$ can be attained by planting trees in the cells $(jd+i, d(ki+l-k) - \lfloor \frac{jd+i-1}{kd} \rfloor$, where $1 \leq i \leq d, 0 \leq j \leq dk-1$, and $1 \leq l \leq k$.

Proposition 1.8 $TP(d,k,mdk)$ can be attained by planting trees in the cells $(jm+i, d(ki+l) - dk - \lfloor \frac{jm+i-1}{mk} \rfloor + 1$, where $1 \leq i \leq m, 0 \leq j \leq dk-1$, and $1 \leq l \leq k-1$.

1.3.2 Comparison to [1]

Chapter 1 of [1] discusses necessary and sufficient conditions for the existence of $TP(d,k,n)$. Theorem 1.4 of [1] is similar to Theorems 2.1.1 and 2.1.2 of this paper. However, since [1] is only looking at one tree (or symbol), there can exist a $TP(d,1,d^2)$, shown in Figure 1.10, whereas there does not exist an $L_d(d^2)$, which will be proven later in this dissertation. Similarly, Proposition 1.6 in [1] gives a construction for $TP(d,k,kd^2)$, but an $ML_d(kd^2,k)$ is proven to not exist by Theorem 3.1.2 of this dissertation.

Example 1.3.1.



(a) $\mathrm{TP}(2,1,4)$

(b) $\mathrm{TP}(3,1,9)$

Figure 1.10: Examples of $TP(d,1,d^2)$

Proposition 1.8 in [1] gives a construction for a $TP(d, k, mkd)$, where $m > d$. Only placing one symbol, say symbol 0 in the construction in Theorem 3.2.2 of this paper of an $ML_d(n, k)$ where $n = mk$ and $m \geq d^2 + 1$ gives a different construction of a $TP(d, k, mkd)$ than Proposition 1.8.

Example 1.3.2. Below is a picture from[1] of a $TP(d, k, mdk)$ with $d = 2, k = 3, m = 4$.

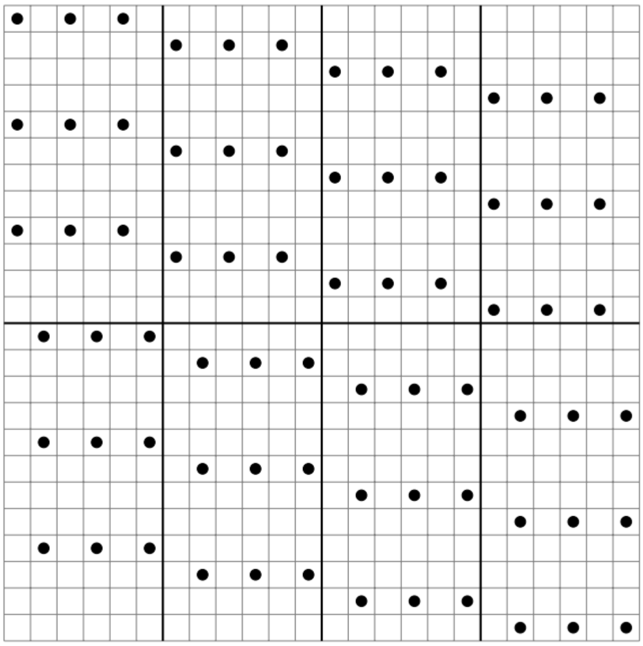


Figure 1.11: Example of a $TP(2, 3, 24)$

Chapter 2 of [1] goes on to discuss possibilities of $TP(d, k, mkd + i)$ where $1 \leq i \leq d$. This paper does not have a construction to cover this, since we are only discussing multi-Latin squares, where $k|n$.

In the following chapters, we will present results on a generalization of [1].

Chapter 2

Existence of $L_d(n)$

The previously stated problem of finding necessary and sufficient conditions of $TP(d,k,n)$ leads into the problem statement for this dissertation. In this chapter, we will discuss the existence of $L_d(n)$, which was defined in Definition 1.1.8. We will assume that $n > d \geq 2$.

2.1 Necessary and Sufficient Conditions

Theorem 2.1.1. *If an $L_d(n)$ exists, then $n \geq d^2$.*

Proof. Suppose there exists an $L_d(n)$ with blocks of size d with $2 \leq d \leq n$. Therefore, there must be at least one $B[d]$, say b. By Definitions 1.1.7 and 1.1.8, the block b must contain d^2 distinct symbols. So, $n \geq d^2$. □

Theorem 2.1.2. *If an $L_d(n)$ exists, then $n \neq d^2$.*

Proof. Assume that there exists an $L_d(n)$ of size $n = d^2$. Consider symbol $i \in \mathbb{Z}_n$ and consider just the first d rows of the $L_d(n)$. The symbol i must show up in each row, meaning that it must appear in each of the $B[d]$'s shown below:

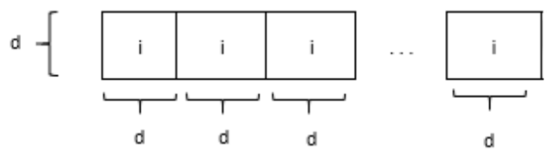


Figure 2.1: First d rows of the $L_d(n)$

This will occur for the next $d-1$ sets of d rows, too. So, the symbol i must appear exactly once in each of the $B[d]$'s shown below.

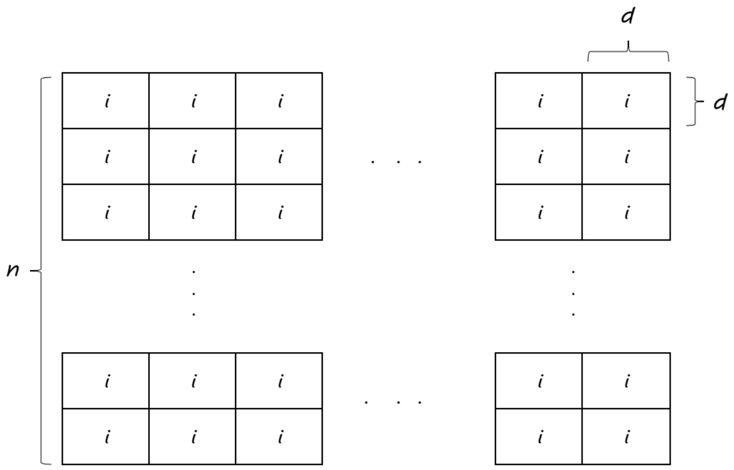


Figure 2.2: $L_d(n)$ broken down into sets of $d-1$ rows

Since this argument works for any symbol i in the Latin square, consider the symbol j such that there is a j in the cell $(d-1, d-1)$. Since the j in $S(0, d-1, 0, d-1)$ is in column $d-1$, this forces the j in the block $S(0, d-1, d, 2d-1)$ to be in column $2d-1$ in order for them to be far enough apart to not be in a $d \times d$ block together. Similarly, the j in $S(d, 2d-1, 0, d-1)$ must be in row $2d-1$.

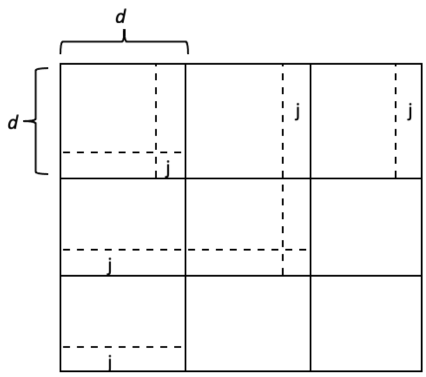


Figure 2.3: Contradiction in the middle block: $S(d, 2d-1, d, 2d-1)$

Now, consider the block $S(d, 2d-1, d, 2d-1)$. Since there is already a j in row $2d-1$ and column $2d-1$, the j in this block must be in $S(d, 2d-2, d, 2d-2)$. Therefore, the $d \times d$ block $S(d-1, 2d-2, d-1, 2d-2)$ has two of the symbols j in it, which is a contradiction to the definition of an $L_d(n)$.

□

2.2 Construction

Theorem 2.2.1. *If $n \geq d^2 + 1$, then $L_d(n)$ exists.*

Construction. Let $n, d, g, h, p,$ and q be integers such that $n \geq d^2 + 1$, $g = gcd(n, d)$, $h = \frac{n}{g}$, $0 \leq p \leq h - 1$, and $0 \leq q \leq g - 1$. Given a pair (r, c) with $r, c \in \{0, 1, ..., n - 1\}$, find p and q such that $p + qh = r$ and $q + pd + s' = c$, for some s'. Then, place symbol s in cell (r, c) where $s \cong s'$ (mod n) and $s \in \{0, ..., n - 1\}$.

Example 2.2.1. Let $n = 5$ and $d = 2$. Then $g = 1$, $h = 5$, and $0 \leq p \leq 4$, $0 \leq q \leq 0$.

Consider cell $(0, 0)$. We have that $r = 0 = p + qh$. Since $q = 0$, this forces $p = 0$. Then $c = 0 = q + pd + s' = 0 + 0 + s'$. Therefore, the symbol in cell $(0, 0)$ is $s = 0$. From the construction, the rest of row 0 is simple to fill in.

Consider cell $(1, 0)$. We have that $r = 1 = p + qh$. Again, $q = 0$, so $p = 1$. This leads to

$$c = 0 = q + pd + s' = 0 + (1 \times 2) + s'$$

$$\Rightarrow s' = -2 \Rightarrow s \cong -2(mod\, 5) \cong 3(mod\, 5)$$

Lastly, consider cell, say $(4, 2)$. Here, $r = 4 = p + qh = p$. Then

$$c = 2 = q + pd + s' = 0 + (4 \times 2) + s' = 8 + s'$$

$$\Rightarrow s' = -6 \Rightarrow s \cong -6(mod\, 5) \cong 4(mod\, 5)$$

Below is the example all filled in:

0	1	2	3	4
3	4	0	1	2
1	2	3	4	0
4	0	1	2	3
2	3	4	0	1

Figure 2.4: Example of an $L_2(5)$ using the construction above

Before we prove Theorem 2.2.1, here are some lemmas to help us out.

Lemma 2.2.2. *Suppose that* $n, d > 1$ *are integers,* $g = gcd(n, d)$*, and* $h = \frac{n}{g}$*. Then for each* $r \in \{0, ..., n-1\}$ *there is a unique pair* (p, q) *with* $0 \leq p \leq h-1, 0 \leq q \leq g-1$*, such that* $r = p + qh$*.*

Proof. There are $hg = n$ pairs (p, q) and for each pair

$$0 = 0 + 0h \leq p + qh \leq (h-1) + (g-1)h = gh - 1 = n - 1$$

So, it suffices to show that for $0 \leq q_1, q_2 \leq g-1$ and $0 \leq p_1, p_2 \leq h-1$,

$$p_1 + q_1 h = p_2 + q_2 h \ \Rightarrow \ p_1 = p_2 \, q_1 = q_2$$

Therefore, if $p_1 + q_1 h = p_2 + q_2 h$, then we have that $p_1 - p_2 = (q_1 - q_2)h$. Since $|p_1 - p_2| \leq h - 1 < h$, there is no way this would happen unless $p_1 = p_2$ and $q_1 = q_2$. $\square$

Lemma 2.2.3. *Suppose that* $0 \leq r \leq n-2$ *and* $0 \leq c \leq n-1$*.*

(a) Suppose that $r = p + qd$ *for some* $0 \leq p \leq h-1$ *and* $0 \leq q \leq g-1$*. Then* $s(r+1, c) \equiv s(r, c) - d$ *(mod n).*

(b) Suppose that $r = (h-1) + qd$ *for some* $0 \leq q \leq g-1$*. Then,* $s(r+1, c) \equiv s(r, c) - (d+1)$ *(mod n).*

Proof. (a) Let $r = p+qh$ for $0 \leq p \leq h-2, 0 \leq q \leq g-1$ and let s' be such that $c = q+pd+s'$. So, we have that:

$$c = q + pd + s' = q + (p-1)d + s' - d$$

$$\Rightarrow s(r+1, c) \equiv s' - d \ (mod\, n) \equiv s(r, c) - d \ (mod\, n)$$

(b) As in the proof of (a), we have that $r = p+qh = h-1+qh$ and $c = q+(h-1)d+s'$. Then $r + 1 = h + qh = 0 + (q+1)h$ when $q < g-1$ (we will cover this case below). So,

$$c = q + (h-1)d + s' = (q+1) + 0d + s' - 1 + (h-1)d$$

$$\Rightarrow s(r+1,c) \equiv s' - 1 + hd - d \; (mod\, n)$$

$$\equiv s(r,c) - 1 + \frac{nd}{g} - d \; (mod\, n)$$

$$\equiv s(r,c) - (d+1) \; (mod\, n)$$

As for the possibility that $p = h-1$ and $q = g-1$, we have that:

$$r = h - 1 + (g-1)h = gh - 1 = h - 1$$

whereas $r \leq h-2$, by supposition.

$\square$

Lemma 2.2.4. *Let $s(r,c)$ denote the symbol in cell (r,c). Suppose that $0 \leq r \leq n-1$ and $0 \leq c \leq n-2$. Then $s(r,c+1) \equiv s(r,c) + 1$ (mod n).*

Proof. Let $0 \leq p \leq h-1, \leq q \leq g-1$ be such that $r = p + qh$, and let s' be such that $c = q + pd + s'$. Then:

$$c + 1 = q + pd + (s'+1)$$

$$\Rightarrow s(r,c+1) \equiv s' + 1 \equiv s(r,c) + 1 \; (mod\, n)$$

$\square$

Below is a visual of Lemmas 2.2.3 and 2.2.4:

s	$s+1$	$s+2$	. . .	$s+y$
$s-d$	$s-d+1$	$s-d+2$	. . .	$s-d+y$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$s-xd+\alpha$	$s-xd+\alpha+1$	$s-xd+\alpha+2$	. . .	$s-xd+\alpha+y$

Figure 2.5: Lemmas 2.2.3 and 2.2.4 for $\alpha \in \{0,1\}$

Lemma 2.2.5. *This construction forms an $n \times n$ Latin square.*

Proof. It is obvious that this array is row-Latin (see Definition 1.1.1) due to Lemma 2.2.4. So, we will show that this array is also column-Latin. Assume that there is a symbol i that appears twice in column j in cells (k, j) and (l, j), with $k = p_1 + q_1 h$ and $l = p_2 + q_2 h$. Then,

$$j = q_1 + p_1 d + i = q_2 + p_2 d + i$$

$$q_1 + p_1 d = q_2 + p_2 d$$

$$q_1 - q_2 = d(p_1 - p_2)$$

First, assume that $p_1 - p_2 \neq 0$. This implies that $d|(q_1 - q_2)$. However, $|q_1 - q_2| < g$ and $g|d$. Therefore, $p_1 - p_2 = 0$, so $q_1 - q_2 = 0$, and $k = l$.

So we see that we cannot have one symbol appearing more than once in each column. Therefore, this array is column-Latin.

□

Lemma 2.2.6. *This construction forms an $L_d(n)$.*

Proof. Using the previous lemma, we know that we are working with an $n \times n$ Latin square. Suppose that symbol s is in cells (i, j) = $(p_1 + q_1 h,\ q_1 + p_1 d + s)$ and (k, l) = $(p_2 + q_2 h,\ q_2 + p_2 d + s)$. Note first that $h > d$ since $h = \frac{n}{g} \geq \frac{d^2+1}{d} > d$.

If $|i - k| \geq d - 1$, we are done.

Suppose $|i - k| \leq d - 1$. We will show that the columns are at least d apart, so these two s symbols do not show up in the same $d \times d$ block. We can suppose that:

$$|i - k| = |(p_1 + q_1 h) - (p_2 + q_2 h)| \leq d - 1$$

$$|(p_1 - p_2) + (q_1 - q_2)h| \leq d - 1 \tag{1}$$

- **Case 1.** Suppose $q_1 = q_2$. If $p_1 = p_2$, then $(i, j) = (k, l)$. If $p_1 \neq p_2$, then:

$$|d(p_1 - p_2)| \geq d$$

$$\Rightarrow |(q_1 - q_2) + d(p_1 - p_2)| = |j - l| \geq d$$

- **Case 2.** Suppose $q_1 \neq q_2$. If $p_1 = p_2$, then $|i-k| = |h(q_1-q_2)| \geq h > d$, a contradiction to (1).

  So, assume that $p_1 \neq p_2$. And, without loss of generality, that $p_1 > p_2$.

  - **Case 2.a.** If $q_1 > q_2$, then $(p_1 - p_2) + h(q_1 - q_2) > d$ since everything is positive and $h > d$. This is a contradiction to (1).
  - **Case 2.b.** Now suppose that $q_1 < q_2$. Assume that $|j - l| < d$ for a contradiction. Then we have that:

    $$-d < (q_1 - q_2) + d(p_1 - p_2) < d$$

    $$\Rightarrow d(p_1 - p_2) < d - (q_1 - q_2)$$

    Note that since $0 \leq q_1, q_2 < g$, we get that $0 < (q_2 - q_1) < g$. So:

    $$d(p_1 - p_2) < d + g \Rightarrow d(p_1 - p_2 - 1) < g \tag{2}$$

    Since $p_1 > p_2$ and $g \leq d$, if $p_1 - p_2 > 1$, then $d(p_1 - p_2 - 1) > d \geq g$, which contradicts (2).

    If $p_1 - p_2 = 1$, then we get from (1) that

    $$-d < 1 + h(q_1 - q_2) < d \Rightarrow -d - 1 < h(q_1 - q_2)$$

    Since $h > d$ and $q_1 - q_2 < 0$, we know that $h(q_1 - q_2) < -d$. So, we get that

    $$-d - 1 < h(q_1 - q_2) < -d$$

    which is a contradiction since $h(q_1 - q_2)$ is an integer.

Therefore, if $|i - k| \leq d - 1$, $|j - l| \geq d$, so we will not have any symbol appearing more than once in one $B[d]$.

$\square$

Proof. **Alternate proof of Lemma 2.2.6.** Let L be the $n \times n$ Latin square formed by the construction above. We will show that L in an $L_d(n)$ by looking at the possible blocks of size d inside.

Consider a block of size d, say B, in L. For simplicity, call the top left cell in B cell $(0, 0)$. Note that this is not necessarily cell $(0, 0)$ of L. Let i be the symbol in cell $(0, 0)$ of B. We will show that there will be no repeated values in this block due to the construction.

We know, by Lemmas 2.2.3 (a) and 2.2.4 that if cell $(0, 0)$ contains symbol i, then cell $(0, a)$ will contain symbol $i + a \ (mod\ n)$ and cell $(a, 0)$ will contain symbol $i - ad$ for some integer $0 \leq a \leq n$. Below is a figure showing B filled out in this manner.

i	$i+1$	$i+2$	$\cdot\ \cdot\ \cdot$	$i+d-1$
$i-d$	$i-d+1$	$i-d+2$	$\cdot\ \cdot\ \cdot$	$i-1$
$i-2d$	$i-2d+1$	$i-2d+2$	$\cdot\ \cdot\ \cdot$	$i-d-1$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$i-(d-1)d$	$i-(d-1)d+1$	$i-(d-1)d+2$	$\cdot\ \cdot\ \cdot$	$i-(d-1)d+d-1$

Figure 2.6: B filled out according to the Construction

Clearly, rows 1 through $d - 1$ of B will not have any repeated symbols. So, let's compare row 0 to the rest of the rows to make sure that there are no repeated symbols.

Ignoring row 0 of B, the smallest value (before being reduced modulo n is in cell $(d-1, 0)$. The symbol in this cell is $i - d^2 + d$. Since $m \geq d^2 + 1$, we get that

$$i - d^2 + d \geq i - m + 1 + d \cong i + 1 + d \ (mod\ n)$$

Therefore, rows 1 through $d-1$ of B contain all the elements between $i-d^2+d$ and $i-1$. Since the largest value in row 0 of B is $i+d-1$ and the smallest value in the rest of B is at least $i+1+d$, we will have no repeated values.

This case will work if $g=1$ or if q does not change throughout B. However, we could have a case where $g \geq 2$ and q does change inside of B. This transition will only occur one time inside of any block of size d because $0 \leq p \leq h$ and $h > b$. So, lets consider this case and call the block B_1. Let symbol i be in cell $(0,0)$ of B_1. Suppose q is incremented by 1 in row a of B_1. Lemma 2.2.3 (b) will help us with the following figure.

i	$i+1$	$\cdots$	$i+d-1$	
$i-d$	$i-d+1$	$\cdots$	$i-1$	
$\vdots$	$\vdots$		$\vdots$	
$i-(a-1)d$	$i-(a-1)d+1$	$\cdots$	$i-(a-1)d+d-1$	$p=h-1, q=q$
$i-ad-1$	$i-ad$	$\cdots$	$i-ad+d-1$	$p=0, q=q+1$
$\vdots$	$\vdots$		$\vdots$	
$i-(d-1)d-1$	$i-(d-1)d$	$\cdots$	$i-(d-1)d+d-1$	

Figure 2.7: B filled out according to the Construction

We will fill in B_1 similar to how we did before, as shown in Figure 2.6. This time, though, row a will shift everything again by 1, by the construction. We know that rows 1 through $a-1$ do not repeat any symbols, and neither do rows a through $d-1$. We also know that $i-ad+d-1 < i-(a-1)d$, so there will not be any repeated symbols in rows 1 through $d-1$. Now, let's check that row 0 does not repeat any of the symbols from the other rows. Note that rows 1 through $d-1$ contain (nearly) consecutive values from $i-(d-1)d-1$ through $i-1$. Since $n \geq d^2+1$, have that

$$i-(d-1)d-1 \geq i-n+1+d-1 \cong i+d\ (mod\ n)$$

Since row 0 contains the consecutive values i through $i + d - 1$, there are no repeated values and no repeated symbols when everything is reduced modulo n.

□

Example 2.2.2. Here, we will look at an example when $n = 12$, and $d = 3$.

row/column	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	9	10	11	0	1	2	3	4	5	6	7	8
2	6	7	8	9	10	11	0	1	2	3	4	5
3	3	4	5	6	7	8	9	10	11	0	1	2
4	11	0	1	2	3	4	5	6	7	8	9	10
5	8	9	10	11	0	1	2	3	4	5	6	7
6	5	6	7	8	9	10	11	0	1	2	3	4
7	2	3	4	5	6	7	8	9	10	11	0	1
8	10	11	0	1	2	3	4	5	6	7	8	9
9	7	8	9	10	11	0	1	2	3	4	5	6
10	4	5	6	7	8	9	10	11	0	1	2	3
11	1	2	3	4	5	6	7	8	9	10	11	0

Figure 2.8: $L_3(12)$

Example 2.2.3. Here is an example when $n = 13$, and $d = 3$.

row/column	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	2	3	4	5	6	7	8	9	10	11	12
1	10	11	12	0	1	2	3	4	5	6	7	8	9
2	7	8	9	10	11	12	0	1	2	3	4	5	6
3	4	5	6	7	8	9	10	11	12	0	1	2	3
4	1	2	3	4	5	6	7	8	9	10	11	12	0
5	11	12	0	1	2	3	4	5	6	7	8	9	10
6	8	9	10	11	12	0	1	2	3	4	5	6	7
7	5	6	7	8	9	10	11	12	0	1	2	3	4
8	2	3	4	5	6	7	8	9	10	11	12	0	1
9	12	0	1	2	3	4	5	6	7	8	9	10	11
10	9	10	11	12	0	1	2	3	4	5	6	7	8
11	6	7	8	9	10	11	12	0	1	2	3	4	5
12	3	4	5	6	7	8	9	10	11	12	0	1	2

Figure 2.9: $L_3(13)$

Chapter 3

Existence of $ML_d(n, k)$

3.1 Necessary and Sufficient Conditions for the Existence of an $ML_d(n, k)$

Theorem 3.1.1. *If $ML_d(n, k)$ exists, then $m \geq d^2$. This implies that $n \geq kd^2$.*

Proof. Suppose there exists an $ML_d(n, k)$ with blocks of size d with $1 < d \leq n$. Therefore, there must be at least one $B[d]$, say b. By Definition 1.1.10, the block b must contain d^2 distinct symbols, implying that $m \geq d^2$ and $n \geq kd^2$. □

Theorem 3.1.2. *If $ML_d(n, k)$ exists, then $m \neq d^2$.*

Proof. Suppose there exists an $ML_d(kd^2, k)$ with blocks of size d with $1 < d \leq n$ and $1 < k < n$. Consider just the first d rows of the multi-Latin square and consider symbol $i \in \mathbb{Z}_m$. The symbol i must show up exactly k times in each row, meaning that it must appear exactly kd times in just the first d rows. This implies that i must appear in each of the $B[d]$'s in Figure 3.1.

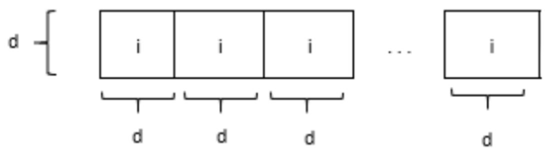


Figure 3.1: First d rows of an $ML_d(kd^2, k)$

This will occur for all of the following sets of d rows, too. So, the arbitrary symbol i must appear exactly once in each of the special blocks of size d shown in Figure 3.2.

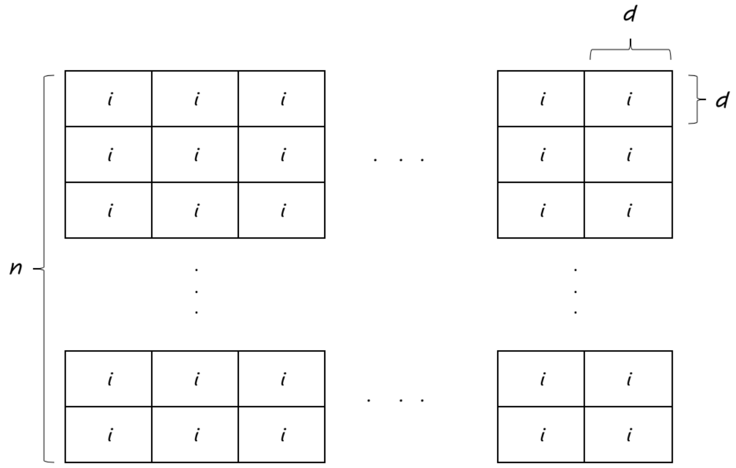


Figure 3.2: $ML_d(kd^2, k)$ broken down into sets of $d-1$ rows

Since this argument works for any symbol i in the multi-Latin square, consider the symbol j such that there is a j in the cell $(d-1, d-1)$. Since the j in $S(0, d-1, 0, d-1)$ is in row $d-1$, this forces the j in the block $S(0, d-1, d, 2d-1)$ to be in column $2d-1$ in order for them to be far enough apart to not be in a $B[d]$ together. Similarly, the j in $S(d, 2d-1, 0, d-1)$ must be in row $2d-1$.

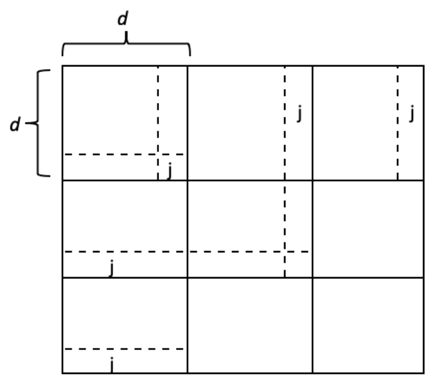


Figure 3.3: Special blocks in $ML_d(kd^2, k)$

Consider two adjacent special blocks in the first d rows $S(0, d-1, (x-1)d, xd-1)$ and $S(0, d-1, xd, (x+1)d-1)$ such that the first one has a j in row $d-1$ and the next one does not. Similarly, consider two adjacent special blocks in the first d columns $S((y-1)d, yd-1, 0, d-1)$ and $S(yd, (y+1)d-1, 0, d-1)$ such that the first one has a j in column $d-1$ and the next one does not. Note that the first block could be $S(0, d-1, 0, d-1)$ if needed. This is shown in Figure 3.4.

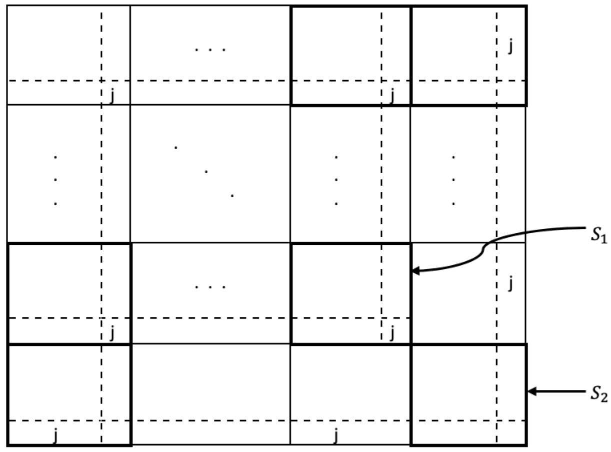


Figure 3.4: S_1 and S_2 $ML_d(kd^2, k)$

Consider the blocks $S_1 = S((y-1)d, yd-1, (x-1)d, xd-1)$ and $S_2 = S(yd, (y+1)d-1, xd, (x+1)d-1)$. Because of the j in $S(0, d-1, (x-1)d, xd-1)$, the j in S_1 must be in row $yd-1$. Similarly, because of the j in $S((y-1)d, yd-1, 0, d-1)$, the j in S_1 must be in column $xd-1$, forcing it to be in cell $(yd-1, xd-1)$ which is in the bottom right corner of S_1. This will force the j in S_2 to be in row $(y+1)d-1$, column $(x+1)d-1$, or cell $((y+1)d-1, (x+1)d-1)$ because this must be an $ML_d(n, k)$.

Consider row $(y+1)d-1$. Note that since this is an $ML(n, k)$, j will appear k times in row $d-1$, which will push the j in the special blocks below it to be in the bottom row of the special blocks, as shown below. Similarly with column $d-1$.

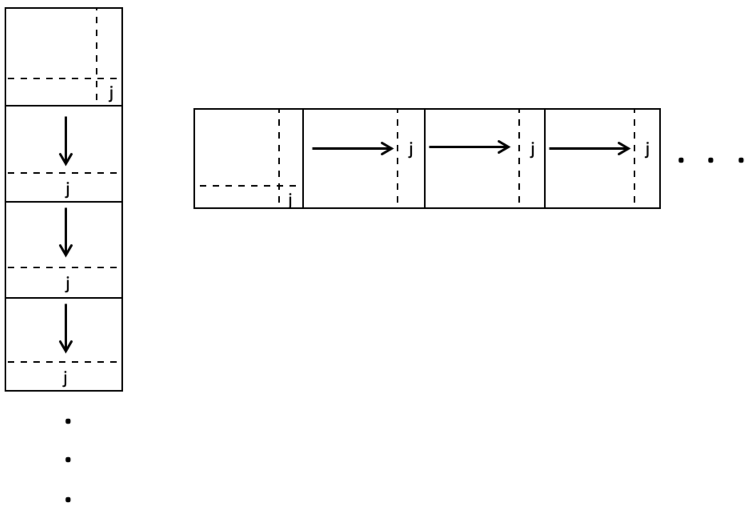


Figure 3.5: j gets pushed in the $ML_d(kd^2, k)$

This implies that j appears k times in row $(y+1)d-1$. Since j is not in row $d-1$ in $S(0, d-1, xd, (x+1)d-1)$, if the j is in row $(y+1)d-1$ in S_2, j would appear $k+1$ times in this row, creating a contradiction that this is an $ML(n, k)$.

Similarly, we can conclude that j cannot be in column $(x+1)d-1$ in S_2. This implies that there is no j in S_2, which is a contradiction. Therefore, we cannot get an $ML_d(n, k)$ where $m = d^2$.

□

Proof. **Alternate Proof of Theorem 3.1.2:** For a contradiction, assume that A is an $ML_d(kd^2, k)$ such that $d, k \geq 2$. Since there are exactly d^2 symbols and each symbol may appear at most once in each $d \times d$ block, each symbol will occur exactly once in each $d \times d$ block. Let $B_d(a, b)$ represent the subgrid $S(a, a+d-1, b, b+d-1)$ such that $0 \leq a, b \leq kd^2 - d$.

Consider the top row of the $d \times d$ block $B_d(r, b)$, and call it $R(r, b) = S(r, r, b, b+d-1)$ where $0 \leq r \leq kd^2 - d - 1$. $B_d(r, d)$ shares $d-1$ rows with $B_d(r+1, b)$, the bottom row of which is $R(r+d, b)$. Since each symbols appears exactly once in each of $B_d(r, b)$ and $B_d(r+d, b)$, it follows that the set of d symbols in $R(r, b)$ must be exactly the same as the set of symbols appearing in $R(r+d, b)$. Applying similar logic to the columns, we get that $C(a, c) = S(a, a+d-1, c, c)$ must contain exactly the same set of symbols as $C(a, c+d)$.

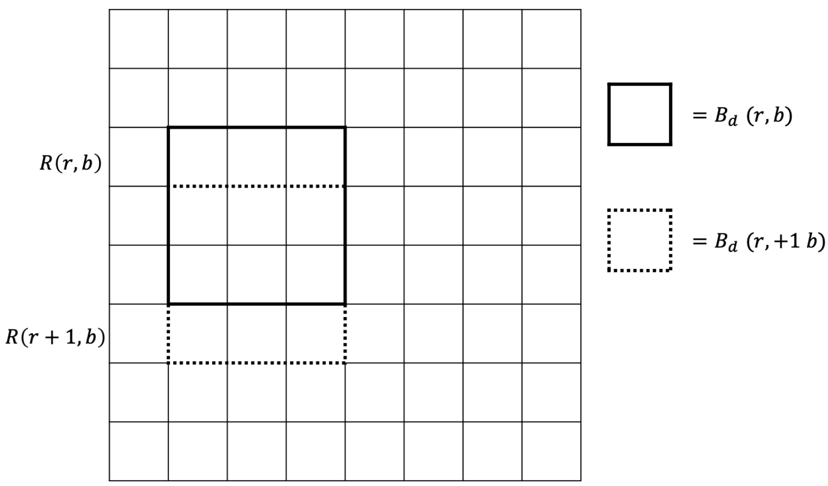


Figure 3.6: $R(r, b)$ from $B_d(r, b)$

Therefore, for any d consecutive cells in A, whether horizontal or vertical, any set of cells in A obtained by transLating the given cells vertically or horizontally, respectfully, by an integer multiple of d spaces will have the same set of entries as the given cells.

Let z be the symbol in cell $(0, 0)$ of A. Then in the rows $0, ..., d-1$, the symbol z must appear only in columns numbered $0, d, ..., (kd-1)d$. In each of the rows $0, ..., d-1$, z will appear k times. Therefore, as x varies over $0, ..., d-1$, the number of the row that z appears in in column xd will vary over $0, ..., d-1$, starting with 0 when $x = 0$.

So, we can find $x \in \{0, ..., kd-2\}$ and $0 \le i_1 < i_2 \le d-1$ such that z appears in cells (i_1, xd) and $(i_2, (x+1)d)$. Similarly, we can find $y \in \{0, ..., kd-2\}$ and $0 \le j_1 < j_2 \le d-1$ such that z appears in cells (yd, j_1) and $((y+1)d, j_2)$.

Let $S_1 = S(yd, yd+d-1, xd, xd+d-1)$

$S_2 = S(yd, yd+d-1, (x+1)d, (x+1)d+d-1)$

$S_3 = S((y+1)d, (y+1)d+d-1, xd, xd+d-1)$

$S_4 = S((y+1)d, (y+1)d+d-1, (x+1)d, (x+1)d+d-1)$

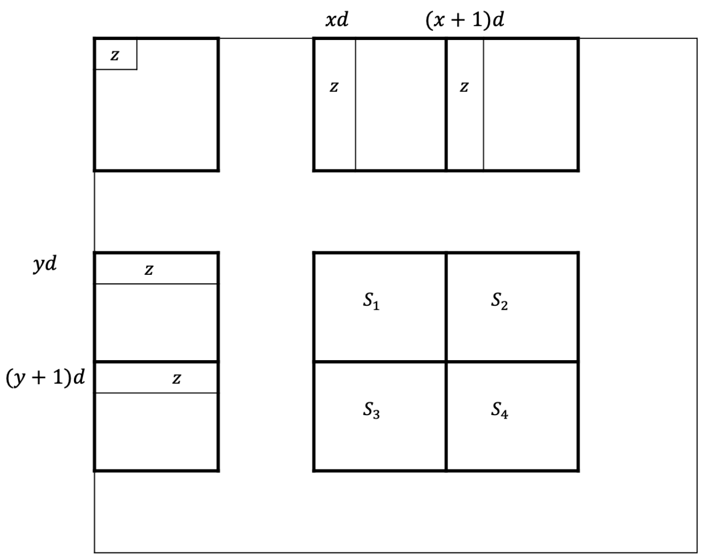


Figure 3.7: S_1, S_2, S_3, S_4

We can see that S_1 and S_2 are horizontal translates of $B_d(yd, 0) = S(yd, yd{+}d{-}1, 0, d{-}1)$ by xd and $(x+1)d$, respectively. Similarly, S_3 and S_4 are horizontal translates of $B_d(0, xd)$ by xd and $(x+1)d$. Also, S_1 and S_3 are vertical translates of $B_d(0, xd)$ by yd and $(y+1)d$, respectively. Finally, S_2 and S_4 are vertical translates of $B_d(0,(x+1)d)$ by yd and $(y+1)d$, respectively.

Therefore, z appears in S_1 in column $xd+j_1$ and row $yd+i_1$.

So, in S_1, z is in cell $(yd+i_1, xd+j_1)$

in S_2, z is in cell $(yd+i_2,(x+1)d+j_1)$

in S_3, z is in cell $((y+1)d+i_1, xd+j_2)$

in S_4, z is in cell $((y+1)d+i_2,(x+1)d+j_2)$

The distance between the row containing z in S_2 and the row containing z in S_3 is:

$$(y+1)d+i_1-[yd+i_2]=i_1-i_2+d$$

Since $0 \leq i_1 < i_2 \leq d-1$, we have that $-1 \leq i_1-i_2+d < d$. So, since the distance between the rows is not at least d, we will see if the columns will be far enough apart.

The distance between the column containing z in S_2 and the column containing z in S_3 is:

$$xd+j_2-[(x+1)d+j_1]=j_2-j_1-d$$

Since $0 \leq j_1 < j_2 \leq d-1$, we have that $-d < j_2-j_1-d \leq -1$.

Since neither the distance between the rows nor the distance between the columns of the cells containing z in S_2 and S_3 are at least d apart, we have that z will appear twice in the same B_d.

□

3.2 Construction

Theorem 3.2.1. *If $m \geq d^2+1$, then $ML_d(n,k)$ exists.*

Construction. Let n, m, d, g, h, p, q, and t be integers such that $n = mk$, $0 \leq p \leq h-1$, $m \geq d^2+1$, $0 \leq q \leq g-1$, $g = gcd(n,d)$, $0 \leq t \leq k-1$, and $h = n/g$. Given a pair (r,c) with $r, c \in \{0,...,n-1\}$, find p, q, and t such that $p+qh = r$, and $q+pd+tm+s' = c$. Then, place symbol s in cell (r,c) such that $s \cong s' \ (mod\, m)$ and $s \in \{0,...,m-1\}$.

Example 3.2.1. Here, we will look at an example when $n = 10$, $k = 2$, $m = 5$, and $d = 2$. So, $g = 2$, $h = 5$, $0 \leq p \leq 4$, $0 \leq q \leq 1$, and $0 \leq t \leq 1$. Similarly to the construction in chapter two, let's pick a few cells to fill in.

Consider cell $(0, 0)$. We have that $r = 0 = p + qh$, forcing p and q to be 0. Then, $c = 0 = q + pd + tm + s' = tm + s'$, so $t = s' = 0$.

Now, look at cell $(2, 5)$. $r = 2 = p + qh$. Since $h = 5$, q must be zero and p must be 2. The we get: $c = 5 = q + pd + tm + s' = (2 \times 2) + (t \times 5) + s'$. Since $m = 5$, $t = 0$:, and we get: $4 + s' = 5 \Rightarrow s \cong 1\ (mod\ 5)$.

Let's walk through one more: cell $(8, 3)$. $r = 8 = p + qh$. Since $p \leq 4$, we need $q = 1$ and $p = 3$. Therefore, $c = 3 = q + pd + tm + s' = 1 + (3 \times 2) + (t \times 5) + s'$. In order to make this work, $t = 0$, and $s' = -4$. Then we get that $s \cong -4\ (mod\ 5) \cong 1\ (mod\ 5)$.

The example below shows the rest of the cells filled in similarly.

row/column	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	0	1	2	3	4
1	3	4	0	1	2	3	4	0	1	2
2	1	2	3	4	0	1	2	3	4	0
3	4	0	1	2	3	4	0	1	2	3
4	2	3	4	0	1	2	3	4	0	1
5	4	0	1	2	3	4	0	1	2	3
6	2	3	4	0	1	2	3	4	0	1
7	0	1	2	3	4	0	1	2	3	4
8	3	4	0	1	2	3	4	0	1	2
9	1	2	3	4	0	1	2	3	4	0

Figure 3.8: $ML_2(10, 2)$ formed by the construction above

Before we prove our main theorem of this dissertation, we will cover some helpful notation and lemmas. Consider an $n \times n$ array with each of the n^2 cells occupied by one of the symbols $0, ..., m-1$, such that $n = mk$. For $(r, c) \in \{0, 1, ..., n-1\}^2$, an index of a cell in the array, let p and q be the unique elements of $\{0, 1, ..., h-1\}$ and $\{0, 1, ..., g-1\}$, respectively, such that $r = p + qh$. Note that Lemma 2.2.2 proves that every $r \in \{0, ..., n-1\}$ is able to be represented by p and q as stated. Then let s' and t be integers such that $0 \leq t \leq k-1$ and $c = q + pd + tm + s'$. Then, let (r, c) be occupied by the symbol $s \in \{0, 1, ..., m-1\}$ such that $s \equiv s'\ (mod\ m)$ and $s \in \{0, ..., m-1\}$. Let this s be denoted $s(r, c)$.

Lemma 3.2.2. *Suppose that* $0 \leq r \leq n-2$ *and* $0 \leq c \leq n-1$.

(a) Suppose that $r = p + qd$ *for some* $0 \leq p \leq h-1$ *and* $0 \leq q \leq g-1$. *Then* $s(r+1, c) \equiv s(r, c) - d\ (mod\ m)$*.*

(b) Suppose that $r = (h-1) + qd$ *for some* $0 \leq q \leq g-1$. *Then,* $s(r+1, c) \equiv s(r, c) - (d+1)\ (mod\ m)$*.*

Proof. (a) Let $r = p + qh$ for $0 \leq p \leq h-2, 0 \leq q \leq g-1$ and let s' and t be such that $c = q + pd + tm + s'$. So, we have that:

$$c = q + pd + tm + s' = q + (p+1)d + tm + s' - d$$

$$\Rightarrow s(r+1, c) \equiv s' - d\ (mod\ m) \equiv s(r, c) - d\ (mod\ m)$$

(b) As in the proof of (a), we have that $r = p + qh = h - 1 + qh$ and $c = q + (h-1)d + tm + s'$. Then $r + 1 = h + qh = 0 + (q+1)h$ when $q < g - 1$ (we will cover this case below). So,

$$c = q + (h-1)d + tm + s' = (q+1) + 0d + tm + s' - 1 + (h-1)d$$

$$\begin{aligned} \Rightarrow s(r+1, c) &\equiv s' - 1 + hd - d\ (mod\ m) \\ &\equiv s(r, c) - 1 + \frac{nd}{g} - d\ (mod\ m) \\ &= s(r, c) - (d+1) + mk\left(\frac{d}{g}\right) \end{aligned}$$

$$\equiv s(r,c) - (d+1) \ (mod\, m)$$

As for the possibility that $p = h-1$ and $q = g-1$, we have that:

$$r = h - 1 + (g-1)h = gh - 1 = h - 1$$

whereas $r \leq h-2$, by supposition.

□

Lemma 3.2.3. *Suppose that* $0 \leq r \leq n-1$ *and* $0 \leq c \leq n-2$. *Then* $s(r, c+1) \equiv s(r,c) + 1$ *(mod m).*

Proof. Let $0 \leq p \leq h-1, \leq q \leq g-1$ be such that $r = p + qh$, and let s' and t, with $0 \leq t \leq k-1$, be such that $c = q + pd + tm + s'$. Then:

$$c + 1 = q + pd + tm + (s'+1)$$

$$\Rightarrow s(r, c+1) \equiv s' + 1 \equiv s(r,c) + 1 \ (mod\, m)$$

□

Below is a visual of Lemmas 3.2.2 and 3.2.3:

s	$s+1$	$s+2$	. . .	$s+y$
$s-d$	$s-d+1$	$s-d+2$	. . .	$s-d+y$
. . .	. . .	. . .	. . .	. . .
$s-xd+\alpha$	$s-xd+\alpha+1$	$s-xd+\alpha+2$	. . .	$s-xd+\alpha+y$

Figure 3.9: Lemmas 3.2.2 and 3.2.3 for $\alpha \in \{0, 1\}$

Note that Lemmas 3.2.2 and 3.2.3 are mirrors of Lemmas 2.2.3 and 2.2.4.

Lemma 3.2.4. *This construction forms an $n \times n$ k-Latin square.*

Proof. Let ML be the $n \times n$ array formed from the construction.

Based on Lemma 3.2.2, we know that ML is row-Latin. So, we will show now that it is column-Latin.

Note first that each column $0 < j < n$ is the translate of column 0 by adding j $(mod\ m)$ to each entry in columns 0. Therefore, it suffices to show that each $s \in \{0, ..., m-1\}$ appears exactly k times in row 0.

Let n and d be positive integers such that $g = gcd(n, d)$ and $h = \frac{n}{g}$. We will now prove that the n numbers $q + pd$, as q ranges from 0 to $g-1$ and p ranges from 0 to $h-1$, represent all n of the congruence classes modulo n.

Note that the following proof is not dependent upon m or k and has no restrictions on n and d other than needing to be positive integers. Therefore, as long as $n = mk$, even if $m \leq d^2$, if ML is formed according to the construction, it will be an $ML(n, k)$ even if it is not an $ML_d(n, k)$.

Let $d' = \frac{d}{g}$. Then n and d' are relatively prime. Also, let $a_1, a_2, ..., a_z \in \mathbb{Z}$ be representatives of different congruence classes modulo n. Therefore, $a_1d', a_2d', ..., a_zd'$ are also representatives of different congruence classes modulo n.

As p ranges from 0 to $h-1$, pg ranges over $0, g, ..., (h-1)g = n-g$, which are representatives of h distinct congruence classes modulo n. Note that these congruence classes are precisely the elements of the additive subgroup, H, of $\mathbb{Z}_n$ generated by the congruence class of g, let's call it $\bar{g}$.

Therefore, as p varies, $pd = (pg)d'$ varies over h distinct congruence classes modulo n. Since g divides every representative of each of these congruence classes, they must be the elements of H. (Note that they may be in a different order than $\bar{0}, \bar{g}, \bar{2g}, ..., (h \bar{-} 1)g$.

The cosets of H in $\mathbb{Z}_n$ are $H = \bar{0} + H$, $H = \bar{1} + H$, $H = \bar{2} + H$, ..., $H = \bar{g} + H$ and thus the congruence classes of the n integers $q + pd$ as q ranges from 0 to $g-1$ and p ranges from 0 to $h-1$ are the n distinct congruence classes modulo n. This finishes the proof. $\square$

Lemma 3.2.5. *This construction forms an $ML_d(n,k)$.*

Proof. As stated in the construction, let n, m, d, g, h, q, t, s, and s' be integers such that $n = mk$, $m \geq d^2 + 1$ is the number of symbols. Let $g = gcd(n,d)$, $h = \frac{n}{g}$, $0 \leq p \leq h-1$, $0 \leq q \leq g-1$, and $0 \leq t \leq k-1$. We can prove that no symbol appears twice in any B_d in the $ML(n,k)$ using the construction if $m \geq d^2 + 1$.

Two cells (r,c) and $(r+x, c+y)$ are in the same B_d if and only if $0 \leq |x|, |y| \leq d-1$. Assuming this and that $|x| + |y| \geq 1$, it suffices to show that $s(r+x, c+y) - s(r,c) \not\equiv 0 \ (mod\, m)$. Note that if both $x, y < 0$, then $(r+x, c+y) = (r', c')$ and $(r,c) = (r'+x, r'+y)$. So, we can assume that they won't both be negative, but they could both be positive.

Given Lemmas 3.2.3 and 3.2.4, we have that:

$$s(r+x,c+y) - s(r,c) = (s(r+x,c+y) - s(r+x,c)) + (s(r+x,c) - s(r,c))$$

$$= y - (xd + \alpha) \ (mod\, m)$$

where $\alpha \in \{0,1\}$ is the number of integers $z \in \{0,1,...,|x|-1\}$ such that $r+z = h-1+qd$ for some $q \in \{0,1,...,g-1\}$. So, it suffices to show that $-m+1 \leq y - (xd+\alpha) \leq -1$ or that $1 \leq y - (xd+\alpha) \leq m-1$ which will imply that $s(r+x,c+y) - s(r,c) \not\equiv 0 \ (mod\, m)$.

- If $x = 0$, then $\alpha = 0$, $0 < |y| \leq d-1$, and we get that

$$s(r+x,c+y) - s(r,c) \equiv y \not\equiv 0 \ (mod\, m)$$

- If $0 < x \leq d-1$, then since $-d+1 \leq y \leq d-1$,

$$-m+1 \leq -d^2 = (-d+1) - ((d-1)d+1) \leq y - (xd+\alpha) \leq d-1-(d) = -1$$

$$\Rightarrow s(r+x,c+y) - s(r,c) \neq 0$$

- If $-d+1 \leq x < 0$, then $0 \leq y \leq d-1$

$$d-1 = 0-(-d+1) \leq y-(xd+\alpha) \leq (d-1)+(d-1)d = d^2-1 \leq m-2$$

$\square$

Note that this proof, with $k = 1$, will also suffice for the proof that the construction in Theorem 2.2.1 will create an $L_d(n)$.

Example 3.2.2. Here, we will look at an example when $n = 20, k = 2, m = 10$, and $d = 3$

r/c	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
1	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
2	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3
3	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
4	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
5	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4
6	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
7	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8
8	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
9	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2
10	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
11	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
12	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3
13	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
14	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
15	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4
16	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
17	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8
18	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
19	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2

Figure 3.10: $ML_3(20, 2)$

Chapter 4

Multi-Latin Squares Versus Latin Squares

4.1 Definitions [10]

Definition 4.1.1. A graph G is a triple consisting of a vertex set $V(G)$, an edge set $E(G)$, and a relation that associates to each edge two vertices called its endpoints.

Definition 4.1.2. A simple graph is a graph with no loops or multiple edges.

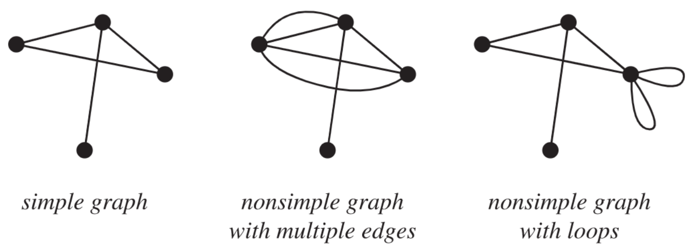


Figure 4.1: Examples of graphs with 4 vertices.

Definition 4.1.3. A vertex is incident with an edge if the vertex is one of the two vertices the edge connects.

Definition 4.1.4. The degree of a vertex is the number of edges incident with the vertex.

Definition 4.1.5. A graph is k-regular if each vertex has degree k.

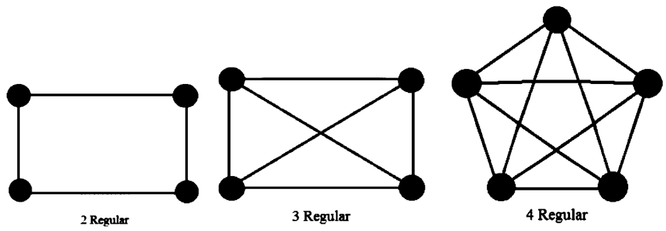


Figure 4.2: Examples of regular graphs.

Definition 4.1.6. Two vertices in a graph are said to be adjacent if an edge connects them.

Definition 4.1.7. An independent set is a set of vertices, no two of which are adjacent.

Definition 4.1.8. A graph G is bipartite if $V(G)$ is the union of two disjoint (possibly empty) independent sets called partite sets of G.

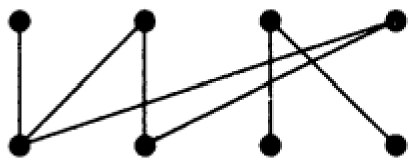
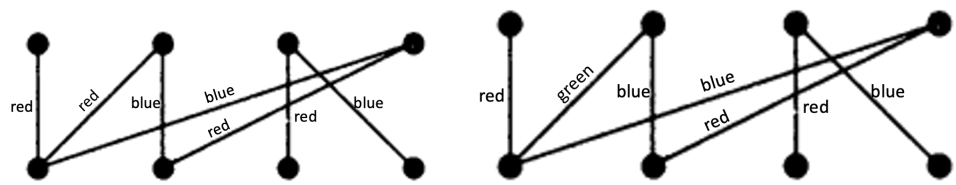


Figure 4.3: Example of a properly 2-edge-colored bipartite graph.

Definition 4.1.9. A k-edge-coloring is a labeling $f : E(G) \to S$, where $|S| = k$. The labels are colors.

Definition 4.1.10. A k-edge-coloring is proper if incident edges have different labels.



2-Edge-Colored Bipartite Graph Proper 2-Edge-Colored Bipartite Graph

Figure 4.4: Bipartite Graph

4.2 Theorems

4.2.1 Latin Squares to Multi-Latin Squares

Theorem 4.2.1. *If L is an $n \times n$ Latin square and k is a real integer such that $k|n$, then an $n \times n$ multi-Latin square, $ML(n,k)$, exists.*

Construction

Let L be an $n \times n$ Latin square and let k be a real integer such that $k|n$. For each symbol i in L, replace it with the symbol $j \in \{0, 1, ..., m-1\}$ such that $j = i$ $(mod\ m = \frac{n}{k})$.

Lemma 4.2.2. *This construction forms a multi-Latin square.*

Proof. Let L be a Latin square as described above. Since $k|n$, let $n = mk$ for some integer $m \geq 1$. For each symbol $i \in \{0, 1, ...n-1\}$ in L, replace it with the symbol $j \in \{0, 1, ...m-1\}$ such that $j \equiv i$ $(mod\ k)$. To prove that this creates a multi-Latin square, ML, we will prove the following: Each symbol appears exactly k times in each (a) row and (b) columns

(a) Since each symbol $i \in \{0, 1, ..., n-1\}$ appeared in each row of L exactly once and $k|n$, when we reduce the symbols modulo m, each new symbol $j \in \{0, 1, ...m-1\}$ appears exactly k times in each row.

(b) This proof is similar to (a). □

Example 4.2.1. Using the above construction, we can turn the following 6×6 Latin square into the $ML(6, 2)$ shown.

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

6×6 Latin square

0	1	2	0	1	2
1	2	0	1	2	0
2	0	1	2	0	1
0	1	2	0	1	2
1	2	0	1	2	0
2	0	1	2	0	1

$ML(6, 3)$

Figure 4.5: Transition from an $n \times n$ Latin square to a $ML(n, k)$

Theorem 4.2.3. *Using the construction from Theorem 4.2.1, we can turn an $L_d(n)$ into an $ML_d(n,k)$, assuming that $k|n$ and $\frac{n}{k} = m \geq d^2 + 1$.*

Proof. Since the proof of Lemma 3.2.5 where $k = 1$ also proves the construction for an $L_d(n)$ in chapter 2, we know that for any two cells (r,c) and $(r+x, c+y)$ in the $L_d(n)$ formed by the construction in chapter 2,

$$0 < |s(r+x, c+y) - s(r,c)| \leq d^2$$

Let k be a positive integer such that $k|n$ and $\frac{n}{k} = m \geq d^2 + 1$. Therefore, if we use the construction from Theorem 4.2.1 on this $L_d(n)$, we know that:

$$0 < |s(r+x, c+y) - s(r,c)| \leq d^2 < m$$

Therefore, this construction will produce an $ML_d(n,k)$. □

4.2.2 Multi-Latin Squares to Latin Squares

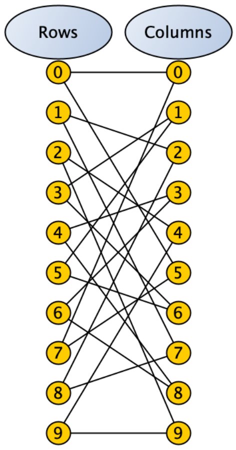
Theorem 4.2.4. *If $ML(n,k)$ is an $n \times n$ multi-Latin square and k is a real integer such that $k|n$, then an $n \times n$ Latin square, L, exists.*

Construction

Let $ML(n,k)$ be an $n \times n$ multi-Latin square. For each symbol i in $0, 1, ...m = n/k$, create a simple bipartite graph, G_i, where one set of vertices, $r_0, r_1, ..., r_{n-1}$, represents the rows and the other set of vertices, $c_0, c_1, ..., c_{n-1}$, represents the columns of $ML(n,k)$. Let the edges of G_i correspond to the cells containing symbol i. See Figure 4.6 for an example of this process.

row/column	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	0	1	2	3	4
1	3	4	0	1	2	3	4	0	1	2
2	1	2	3	4	0	1	2	3	4	0
3	4	0	1	2	3	4	0	1	2	3
4	2	3	4	0	1	2	3	4	0	1
5	4	0	1	2	3	4	0	1	2	3
6	2	3	4	0	1	2	3	4	0	1
7	0	1	2	3	4	0	1	2	3	4
8	3	4	0	1	2	3	4	0	1	2
9	1	2	3	4	0	1	2	3	4	0

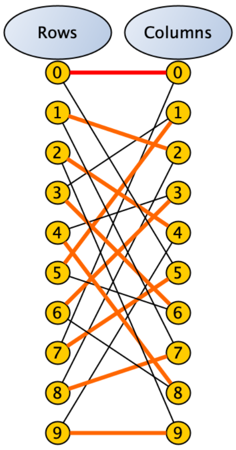
$ML_2(10, 2)$



G_0

Figure 4.6: Creating G_0 from the $ML_2(10, 2)$

Since each symbol appears exactly k times in each row and column, each of the graphs, G_i will be k-regular. Properly edge color G_i with k colors and assign each color a symbol, $ki, ki+1, ki+2, ..., k(i+1)-1$. Now, replace each occurrence of symbol i in $ML(n, k)$ with the corresponding symbol from proper edge coloring of G_i. Figure 4.7 below properly edge colors G_0 from Figure 4.6 into red and black edges. Then we can create the Latin square in Figure 4.7 by corresponding the red edges to 0 and the black edges to 1. Figure 4.7 shows the entire Latin square filled in, according to this construction.



Properly Edge Colored G_0

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

$L_2(10)$

Figure 4.7: Forming $L_2(10)$

Lemma 4.2.5. *This construction forms a Latin square.*

Proof. Clearly, with the way the reassigning works, each symbol $0, 1, ..., km = n$ appears at least once in each row and column since each color from each graph G_i will appear on every vertex. Since we created a proper coloring, no symbol will appear in each row or column more than once.

□

Note. The Latin square in Figure 4.7 is an $L_2(10)$. This leads us to the following theorem.

Theorem 4.2.6. *Using the construction from Theorem 4.2.3, we can turn an $ML_d(n, k)$ into an $L_d(n)$.*

Proof. Let ML be an $ML_d(n, k)$ as described, and let L be the Latin square which results from using the construction from Theorem 4.2.4 on ML. For a contradiction, suppose L is not an $L_d(n)$. Then there exists some B_d, say B, and a symbol i in L such that i appears at least twice in B.

Consider the corresponding block, B, in ML. Let $c_1$and c_2 in ML correspond to the locations of the two cells in B in L containing the symbols i. By the construction above, the only way that two symbols would be the same in L is if they were originally the same in ML. This comes from the way we form each graph G_i. Therefore, c_1 and c_2 contain the same symbol and are in the same block B. This results in a contradiction to ML being an $ML_d(n, k)$. □

Chapter 5

Summary and Path Forward

5.1 Summary

We have shown that we can construct an $L_d(n)$ and an $ML_d(n, k)$ given that the number of symbols is at least $d^2 + 1$, for integers $0 < d < m \leq n$. We have also created a construction for forming an $ML_d(n, k)$ given an $L_d(n)$ and integers k, m such that $k|n$ and $m \geq d^2 + 1$. Finally, given an $ML_d(n, k)$, we have found a construction that forms an $L_d(n)$.

5.2 Path Forward

A possible extension to this problem would be considering blocks of size $c \times d$ where $c \neq d$. Using rectangular blocks like this would be similar to square blocks, but has not been looked into yet.

There is a possible application to this problem in error correcting code, specifically on power lines transmitting internet. [4] [6]

References

[1] Aliyev, N. (2019). *Existence of TP(d, k, n)* [Doctoral dissertation, Auburn University].

[2] Bose, R. C.; Shrikhande, S. S.; Parker, E. T. *Further Results on the Construction of Mutually Orthogonal Latin Squares and the Falsity of Euler's Conjecture.* Canadian. J. Math., 1 (1949): 88-93.

[3] Colbourn, C. J.; Dinitz, J. H. (2006). *Handbook of Combinatorial Design (Second Edition)*. CRC Press. p. 12.

[4] Colbourn, C. J.; Kove, T.; Ling, A. C. H. (2004). "Permutation Arrays for Powerline Communication". *IEEE Trans. Inf. Theory.* 50: 1289-1291.

[5] Euler, L. *Recherches sur une nouvelie espece de quarres magiques.* Vehandlingen Zeeuwach Genootchap Wetenshapper Vlissengen, 9 (1782): 85-239.

[6] Huczynska, Sophie (2006). "Powerline Communication and the 36 Officers Problem". *Philosophical Transactions of the Royal Society A.* 364 (1849): 3199-3214.

[7] Lindner, C. C.; Rodger, C.; *Design Theory, Second Edition*

[8] MacNeish, H. F. *Euler Squares.* Ann. Math., 23 (1922): 221-227

[9] Tarry, G. *Le probleme des 36 officers* C. R. Assoc. Fr. Av. Sci., 29 (1900): 170-203.

[10] West, D. (2015) *Introduction to Graph Theory, Second Edition.*