
# SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET


## The search for orthogonal Latin squares


av

**Nicole Saeed**



2021 - No K50

# The search for orthogonal Latin squares

Nicole Saeed

---

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Sven Raum

2021

# The search for orthogonal Latin squares

Nicole Saeed

November 22, 2021

**Abstract**

Latin squares are $n \times n$ arrays where the elements in each row and column do not repeat; mutually orthogonal Latin squares (MOLS) are sets of Latin squares such that, when their elements are superimposed on top of each other, all element combinations are unique. This thesis explains the relationship between MOLS and finite projective plane geometry by detailing how one might construct a finite projective plane from a finite field as well as how a finite projective plane may be used to construct a set of MOLS and vice-versa. With the link between MOLS and finite geometries established, some examples of proofs showing the non-existence of a finite projective plane of certain orders are discussed.

**Acknowledgement**

I would like to thank my supervisor, Sven Raum, for his patience, detail-oriented guidance, and quick and engaged responses regarding any questions or issues encountered during the writing of the thesis. I would further like to thank my cat for her emotional support.

# Contents

# 1

# Introduction

A Latin square is an $n \times n$ array whose entries consist of a set of $n$ numbers, which are arranged in such a way that each number appears exactly once in each row and each column. Readers may be familiar with the relatively modern number-placement puzzle Sudoku, which provides some easy-to-understand examples of Latin squares—each solution to a Sudoku puzzle is a Latin square.

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 2 | 3 | 1 |
| 3 | 1 | 2 |

Figure 1: An example of a Latin square of order 3.

More formally, we may define a Latin square as follows:

**Definition 1.1.** A Latin square $L \in M_n(\mathbb{Z})$ of order $n$ is an $n \times n$ array such that $L_{i,j} \in \{1, \ldots, n\}$ for all i, j and such that each of the numbers $1, \ldots, n$ appear exactly once in each row and column of L.

Note that while we may wish to represent the numbers in a Latin square with various symbols (such as letters, which has been done traditionally), for the purposes of the paper, the entries in a Latin square are defined as numbers.

An orthogonal pair of Latin squares, meanwhile, is a pair of Latin squares such that when they are superimposed, each element of each square occurs only once with the other. Formally, they are defined as such:

**Definition 1.2.** Let $L_1 = (a_{i,j})$ and $L_2 = (b_{i,j})$ be two $n \times n$ Latin squares where

each $a_{i,j}, b_{i,j} \in 1, 2, 3, ..., n$. If the $n^2$ ordered pairs $(a_{i,j}, b_{i,j})$ are distinct, then $L_1$ and $L_2$ are a pair of orthogonal Latin squares.

It is often convenient to speak in terms of *mutually orthogonal Latin squares*, and so they will henceforth be referred to as *MOLS*.

While a seemingly simplistic combinatorial design, the search for MOLS of certain orders has proven difficult, and solutions have been linked to areas of mathematics as unexpected as finite geometry.

$$\begin{array}{ccc} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{array}$$

Figure 2: An example of an orthogonal pair of Latin squares of order 3, superimposed.

## 1.1 History

In ancient times, constructions which were equivalent to Latin squares were thought to have magical qualities. However, they were not defined with mathematical terminology until Leonhard Euler started investigating their properties in the late 18th century.

In the famous problem of the 36 officers, Euler asks the following question: given a collection of 36 officers, of 6 different ranks and 6 different regiments, is it possible for the officers to line up in such a way that in each line (horizontal and vertical) there are six officers of both different ranks and regiments? In modern terminology, we would say that Euler was attempting to find a pair of orthogonal Latin squares of order 6.

In his attempts to find a solution, Euler chose to denote the regiments with the Latin letters *a, b, c, d, e, f* and the ranks with the Greek letters $\alpha$, $\beta$, $\gamma$, $\delta$, $\varepsilon$, $\zeta$. Indeed, the name *Latin square* stems from Euler's decision to have the elements of the square be represented by Latin letters, and the name Graeco-Latin square is used interchangeably with a superimposed pair of orthogonal Latin squares.

$$\begin{array}{cccc} (a,\alpha) & (b,\beta) & (c,\gamma) & (d,\delta) \\ (b,\delta) & (a,\gamma) & (d,\beta) & (c,\alpha) \\ (c,\beta) & (d,\alpha) & (a,\delta) & (b,\gamma) \\ (d,\gamma) & (c,\delta) & (b,\alpha) & (a,\beta) \end{array}$$

Figure 3: A Graeco-Latin square of order 4.

Euler was not able to find a Graeco-Latin square of order 6, and suggested that the problem of the 36 officers may have no solutions, but was unable to prove it. Yet he continued to study Latin squares, and came to define another key concept: that of a *transversal*.

**Definition 1.3.** Let $L = (a_{i,j})$ be a Latin square of order $n$. A transversal of L is a choice of pairs $(i_1, j_1), \ldots, (i_n, j_n) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ such that $\{i_1, \ldots, i_n\} = \{j_1, \ldots, j_n\} = \{a_{i_1,j_1}, \ldots, a_{i_n,j_n}\} = \{1, \ldots, n\}$.

Informally, one can think of a transversal as a set of $n$ distinct entries occurring in distinct rows and columns in a Latin square of order $n$.

Euler noted that, for a Latin square of order $n$ to have an orthogonal mate, it must have $n$ mutually disjoint transversals. He then chose to study transversals of *cyclic Latin squares*: that is, Latin squares where each successive row contains elements equivalent to those of the previous row but shifted one step to the left. More formally, they may be defined as follows:

**Definition 1.4.** A *cyclic Latin square* of order $n$ is a Latin square $L = (a_{i,j})$ such that its entries are determined according to $a_{i+1,j} = a_{i,j+1} = a_{i,j} + 1 \bmod n$.

Euler proposed and proved the following:

**Theorem 1.5.** *Let L be a cyclic Latin square of order* n. *For even* n, *L lacks a transversal.*

*Proof.* Reenumerating rows and columns, we may assume that the entries of the first column of L are $1, 2, \ldots, n$ (that is, that $L_{i,1} = i$ for all $i$). Since L is cyclic, this implies that $L_{i,j} = i + j - 1 \mod n$ for all $i$ and $j$. Now assume that

$$(1, j_1), (2, j_2), \ldots, (n, j_n)$$

is a transversal of L. Then, we find that

$$\begin{aligned}
\frac{(n+1)n}{2} &= 1 + 2 + \ldots + n \\
&= L_{1,j_1} + L_{2,j_2} + \ldots + L_{n,j_n} \\
&= (1 + j_1 - 1) + (2 + j_2 - 1) + \ldots + (n + j_n - 1) \\
&= (j_1 + j_2 + \ldots + j_n) + (0 + 1 + \ldots + n - 1) \\
&= (1 + \ldots + n) + (1 + \ldots + n - 1) \\
&= \frac{(n+1)n}{2} + \frac{(n-1)n}{2} \mod n.
\end{aligned}$$

Hence it follows that $\frac{(n-1)n}{2} \equiv 0 \mod n$, which means that L can not have even order (that is, it has odd order). □

We now know that cyclic Latin squares of even order do not have orthogonal mates. For odd $n$, conversely, the main diagonal is a transversal, and so one can find a set of $n$ disjoint transversals. Therefore, cyclic Latin squares of odd order have orthogonal mates (and, more generally, so do Latin squares of odd orders).

In his paper, Euler proceeded to investigate transversals of cyclic Latin squares of orders 2, 3, and 4. During his investigation of these transversals, he proved that there are orthogonal Latin squares of all sides$n$ divisible by 4. This proof led Euler to his now-famous conjecture on orthogonal Latin squares:

**Conjecture 1.6.** If $n \equiv 2 \mod 4$, then there are no MOLS of order $n$.

He knew this was the case for $n = 2$, but could not prove it in the general case. It was not until the year 1901 that Tarry was able to prove the conjecture held for n = 6 by examining squares relatively case-by-case (thereby also proving Euler's 36 officers indeed had no solution, as he had suspected). However, it would later be shown that Graeco-Latin squares of order $10, 14, 18, \ldots$ and so on exist. Euler's conjecture, though long accepted as a reasonable theory, would turn out to be incorrect.

# 2

# Finite planes and finite fields

We now aim to turn our attention to a field of mathematics which would come to be of great importance to the search for orthogonal Latin squares: *finite projective planes*. Before delving into these, let us briefly recall the definition of an *affine plane*. Affine planes are a system of points and lines that satisfy the following axioms:

- Any two distinct points lie on a unique line,
- Lines have at least two points,
- Given a line and a point not on said line, there is a unique, separate line that contains the given point and is parallel to (never meeting) the given line,
- There exist three points not on any single line at once.

The familiar-to-most Euclidean plane, with lines given as solution sets to linear equations, is merely one example of an affine plane.

Now let us study the related concept of projective plane geometry. The axioms for projective plane geometry are defined as such:

- Any two distinct points lie on a unique line,
- Any two distinct lines have in common exactly one point,
- Every line contains at least three points,
- There are at least two lines.

As lines must intersect in one point, these axioms tell us that parallel lines do not exist in projective plane geometry, a contrast to (for instance) Euclidean geometry. Nevertheless, an affine plane can be constructed from a projective plane by removing a line and its contained points, and a projective plane can be constructed from an affine plane by adding a line at infinity, as we shall see later.

## 2.1 Finite projective plane geometry

Let us examine the mathematical field of finite projective plane geometry: in other words, projective plane geometries with a finite number of points. The figure below is an example of a finite projective plane geometry:

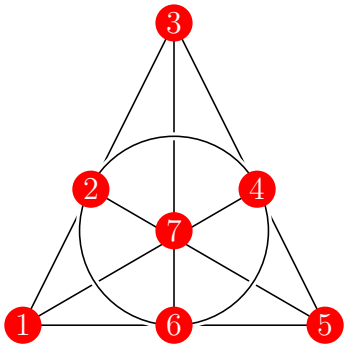



Figure 4: A finite projective plane with seven points, also known as a Fano plane.

We may wish to briefly ensure that the axioms are satisfied. We can trivially see that any two lines we choose will share just one point in common. It is further possible to intuit that any two points we choose will lie on a unique line: with the exception of the line that draws a circle, each line in the figure can be thought of as having two extreme points and a third point in-between. Hence if we choose the two extremes as our points, then our distinct line is completed by the in-between point; if we choose an extreme and an in-between point, then it is completed by the remaining extreme. If we select any two of the points (2, 4, 6), then we have instead chosen the line which draws a circle enclosed in the triangle. It is further clear that each line in the Fano plane contains exactly three points—the minimum amount required to satisfy the third axiom. There are seven lines in total, and so we can conclude all axioms hold.

Incidence matrices provide an alternative way to represent a finite projective plane.

**Definition 2.1.** An incidence matrix is a matrix whose entries lie in $\{0, 1\}$.

An incidence matrix is typically used to show a relation between two classes of objects—in this case, points and lines. We may represent the above finite projective plane with a $7 \times 7$ incidence matrix as follows:

| Line \ Point | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| (1, 2, 3) | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| (3, 4, 5) | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| (1, 5, 6) | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| (1, 4, 7) | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| (3, 6, 7) | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| (2, 5, 7) | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| (2, 4, 6) | 0 | 1 | 0 | 1 | 0 | 1 | 0 |

If a line contains a certain point, we enter a 1 in the corresponding row and column; otherwise, we enter a 0. As has been mentioned previously, each line contains three points, but we can also note from the incidence matrix that each point appears on exactly three lines. These observations lead us to the following theorem:

**Theorem 2.2.** *For every finite projective plane* P*, there is a positive integer* n *(known as the order of P) such that each line of P contains exactly* $n + 1$ *points and each point of P is contained in exactly* $n + 1$ *lines. Furthermore, P has exactly* $n^2 + n + 1$ *points and exactly* $n^2 + n + 1$ *lines.*

In this instance, we have a seven-point projective plane of order 2: each line contains $2 + 1$ points and is contained in $2 + 1$ lines, and there are exactly $2^2 + 2 + 1$ points and exactly $2^2 + 2 + 1$ lines.

A method to prove whether a finite projective plane for an arbitrary order $n$ exists has not yet been found. However, in 1906, Veblen and Bussey proved that there exists a projective plane of order $n$ if $n$ is a power of a prime number. It follows that there are infinitely many $n$ which are orders of finite projective planes. One known $n$ for which there is no order of a finite projective plane, however, is $n = 6$, a fact which followed from Tarry's laborious 1901 proof that there are no pairs of orthogonal Latin squares of order 6; another example of such an order is $n = 10$. These proofs are touched upon in section 4.

## 2.2 Finite fields

How do we go about constructing finite projective planes? To do this, we must first consider *fields*. We will explain them through the related concept of rings:

**Definition 2.3.** A set of elements R is said to form a *ring* when there exist two binary operators $+$, for addition, and $\cdot$, for multiplication, such that the following axioms are satisfied for all $a, b, c \in R$:

- **Associativity of addition and multiplication:** $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- **Commutativity of addition:** $a + b = b + a$.
- **Distributivity of multiplication over addition:** $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.
- **Existence of an additive identity:** there exists an element 0 in R such that $a + 0 = a$.
- **Existence of an additive inverse:** for every $a$ in R, there exists an element $-a$ such that $a + (-a) = 0$.

A field, then, is defined as such:

**Definition 2.4.** A ring F is said to form a *field* when it satisfies the following additional axioms for all $a, b \in R$:

- **Commutativity of multiplication:** $a \cdot b = b \cdot a$.
- **Existence of a multiplicative identity:** there exists an element 1 in F such that $a \cdot 1 = a$.
- **Existence of a multiplicative inverse:** for every $a \neq 0$ in F, there exists an element $\frac{1}{a} \in F$ such that $a \cdot \frac{1}{a} = 1$.

It is easy to see that these rules are upheld by the infinite set of elements containing all rational numbers or the infinite set of elements containing all real numbers, hence they provide examples of fields.

More relevant to the topic of finite projective planes are *finite fields*, also known as *Galois fields*, which are defined as fields containing only a finite number of elements. A classic example of a finite field is the field provided by the numbers which are remnants modulo $p$, where $p$ is a positive prime integer, that is $0, 1, 2, \ldots, (p - 1)$. For this field, addition and multiplication are defined as in modular arithmetic.

For instance, if $p = 5$, we have the elements $\{0, 1, 2, 3, 4\}$. It is quite trivial to note that associativity, commutativity, and distributivity hold, and the existence of an additive and multiplicative identity is equally obvious. For our inverses, we have (all modulo 5):

$$1 + 4 \equiv 0, \quad 2 + 3 \equiv 0;$$
$$1 \cdot 1 \equiv 1, \quad 2 \cdot 3 = 6 \equiv 1, \quad 4 \cdot 4 = 16 \equiv 0.$$

Hence the set of elements $\{0, 1, 2, 3, 4\}$ with addition and multiplication mod 5 is a finite field.

Let us examine a method by which one may construct finite fields of orders which are prime powers, rather than merely primes (and, indeed, all finite fields are of prime power order):

**Theorem 2.5.** *a) Taking all polynomials of degree lesser than deg s(x), where* s(x) *belongs to the ring* F*, the operations of polynomial addition and polynomial multiplication modulo s(x) defines a commutative ring with multiplicative identity, which is denoted by* $F[x]/(s(x))$.

*b) If s(x) is not a product of two polynomials of positive degree (i.e. it is irreducible in F[x]), then* $F[x]/(s(x))$ *has multiplicative inverses and is hence a field.*

*c) If* $|F| = q$*, then* $|F[x]/(s(x))| = q^{deg(s(x))}$.

For instance, we may choose the polynomial $s(x) = x^2 + x + 1$ belonging to the ring $\mathbb{Z}_2[x]$ and use it to construct a field of order 4 (that is, $|\mathbb{Z}_2|^{deg(x^2+x+1)}$). We know $s(x) = x^2 + x + 1$ is irreducible as $s(0) = 1$, $s(1) = 1$, and $s(2) = 1$ (modulo 2). The elements of the field are then $[0], [1], [x], [x + 1]$. Now we have the following multiplicative inverses modulo $x^2 + x + 1$:

$$1 \cdot 1 \equiv 1, \quad x \cdot (x + 1) = x^2 + x \equiv 1.$$

And so we see $\mathbb{Z}_2[x]/(x^2 + x + 1)$ is a finite field.

## 2.3 Constructing finite projective planes from finite fields

Henceforth $F_n$ will refer to a field of order $n$. Given a finite field $F_n$, we may now use it to construct a projective plane:

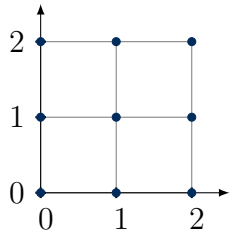
**Theorem 2.6.** *a) Consider $F_n^2$ as a set of points with the solution sets to $ax + by + c = 0$ in $F_n$, $(a, b, c) \neq (0, 0, 0)$, as lines.*

*b) Add points parameterized by the slopes of the lines, that is, $-\frac{a}{b}$ $(b \neq 0)$, and add one more for when $b = 0$. Extend these lines to contain their point at infinity.*

*c) Add a line at infinity connecting all $(n + 1)$ points at infinity.*

*Then this defines a projective plane.*

Let us consider an example. We may represent the set of points associated with the finite field $F_3$ as follows:




According to the above theorem, we see that, for instance, {(0, 1), (1, 0), (2, 2)} is a line in the projective plane, because its equation is $x + y + 2$, and:

$$\begin{aligned} 0 + 1 + 2 = 3 \equiv 0 \mod 3, \\ 1 + 0 + 2 = 3 \equiv 0 \mod 3, \\ 2 + 2 + 2 = 6 \equiv 0 \mod 3, \end{aligned}$$

and so the points on the line are a solution set to the equation described by $ax + by + c = 0$ in $F_3$.

Intuitively, we can think of the line from (0, 1) to (1, 0) as wrapping around to its third point (2, 2) due to the properties of modulo arithmetic, as the "expected" point (2, -1) is equivalent to (2, 2) in $F_3^2$. Conversely, {(0, 1), (1, 0), (1, 2)} would not be

a line in the plane, because through every pair of points there is a unique line, and we already have the line {(0, 1), (1, 0), (2, 2)}.

Continuing in this manner, we will find $n^2 + n$ of the $n^2 + n + 1$ lines in the desired finite projective plane of order $n$. We have now constructed an affine plane. To produce the projective plane, we must add the aforementioned points at infinity and line at infinity: the addition of the line at infinity fulfills the axiom for a projective plane stating that "any two distinct lines have in common exactly one point", which would otherwise not hold true.

Note that parallel lines share the same points at infinity, and so there are only *(n + 1)* points at infinity to add. For instance, in the above coordinate system, the lines containing the points {(0, 0), (0, 1), (0, 2)}, {(1, 0), (1, 1), (1, 2)}, {(2, 0), (2, 1), (2, 2)} are all parallel and share a point at infinity, because they are all vertical and so have the same slope.

# 3

# Connecting finite geometries to orthogonal Latin squares

Let us recall that each finite projective plane has an order $n$. We will now show that the existence of such a finite projective plane is directly equivalent to the existence of $n-1$ MOLS.

## 3.1 From a finite projective plane to a set of MOLS

Given any prime number $p$ and a positive integer $m$, the corresponding finite field allows us to construct a projective plane with order $n = p^m$, as well as its corresponding $n$-sided $n-1$ MOLS. The construction is done as follows:

Take any of the $n^2+n+1$ lines in the plane and call it the *line at infinity* $(l)$. Through each of the $n+1$ points on $(l)$, exactly $n$ lines pass through. Other than $(l)$ itself, these $n(n+1)$ lines make up, together with $(l)$, the total amount of $n^2+n+1$ lines in the finite plane. Now choose any two points X and Y on $(l)$. The intersections of the $n$ lines passing through X and the $n$ lines passing through Y yield $n^2$ points (which, together with the $n+1$ points on $(l)$, make up the total $n^2+n+1$ points). Let us call the $n^2$ points not on the line at infinity *finite points*, and let us call the $n^2+n$ lines other than the line at infinity *finite lines*.

Now let $U_1, U_2, \ldots, U_{n-1}$ be the points other than X and Y on $(l)$. The set of finite lines passing through the points on $(l)$ may be denoted (X), (Y), $(U_i)$ $(i = 1, 2, \ldots, n-1)$. For the $n$ lines in (X) and (Y), we may attach the numbers $1, 2, \ldots, n$—one for each line. Now let us consider a finite point $P$. Let x be the

number of a line of (X) passing through $P$ and let y be the number of a line of (Y) passing through $P$. Then ($x$, $y$) are the coordinates of $P$. There are only $n^2$ ordered pairs ($x$, $y$) corresponding to the $n^2$ finite points. If we think of the $x$-coordinates as row numbers and the $y$-coordinates as the column numbers, then the finite points correspond to the $n^2$ elements in an $n$-sided square.

Let us consider the finite lines passing through $(U_1)$. As before, we may attach the numbers $1, 2, \ldots, n$ to these. Through every finite point, one and only one line of $(U_1)$ passes through. Let $\ell_k^{u_1}$ be a line of $(U_1)$ passing through ($x$, $y$) with $k$ as its assigned number. For each coordinate ($x$, $y$) in our $n$-sided square, we put the corresponding element $k$. This gives us a Latin square, because each row of the square corresponds to a line of (X), each column of the square corresponds to a line of (Y), and, further, through the $n$ finite points of each of these lines there pass $n$ different lines of $(U_1)$. We may call the unique Latin square associated with $(U_1)$ $[L_1]$, and we may construct further Latin squares $[L_2]$, $[L_3]$, ..., $[L_{(n-1)}]$ associated with the lines $(U_2)$, $(U_3)$, ..., $(U_{(n-1)})$.

**Theorem 3.1.** *The $n-1$ Latin squares constructed above are mutually orthogonal.*

*Proof.* Let $\ell_k^{u_i}$ denote a line of $U_i$ with $k = 1, 2, \ldots, n$ as the element of the $n \times n$ Latin square $[L_i]$ in row $x$ and column $y$. This line intersects with the n different lines of $(U_j)$, $i \neq j$, in the $n$ finite points on it. Hence a given element of $[L_i]$ occurs only once with every element of $[L_j]$. Further, these elements are not the same, for in a finite projective plane, two lines have in common exactly one point. The element pair (a, b) appears in $[L_i]$ and $[L_j]$ respectively only if line $a$ from $(U_1)$ and line $b$ from $(U_2)$ intersect—but there is at most one such intersection point, and so each element pair may appear only once. □

By superimposing the $n-1$ MOLS obtained, we may create a Hyper-Graeco-Latin square (or, for $n = 3$, a Graeco-Latin square).

## 3.2 Constructing a set of MOLS from a finite projective plane

Let us consider an example for the case where $n = 3$; that is, let us construct a Graeco-Latin square from the finite projective plane of order 3.

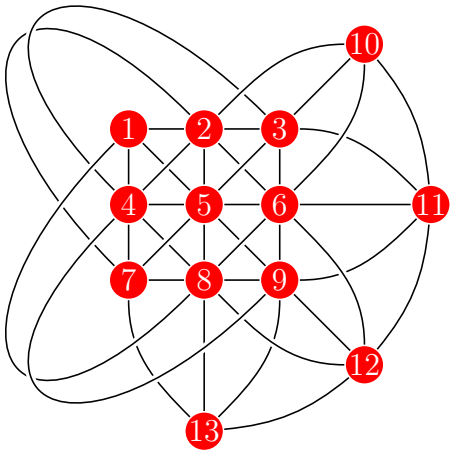



Figure 5: The finite projective plane of order 3.

We may select any line as our line at infinity ($l$), so let us choose {10, 11, 12, 13}. We must now select two points X and Y on the line. Let us choose point 10 for X and point 11 for Y. We see that the set of finite points is {1, 2, 3, 4, 5, 6, 7, 8, 9}, and the set of finite lines is

$$\{\{1,6,8,10\},\{2,4,9,10\},\{3,5,7,10\},$$
$$\{1,2,3,11\},\{4,5,6,11\},\{7,8,9,11\},$$
$$\{1,5,9,12\},\{2,6,7,12\},\{3,4,8,12\},$$
$$\{1,4,7,13\},\{2,5,8,13\},\{3,6,9,13\}\}.$$

Now $U_1, U_2, \ldots, U_{(n-1)}$ are the points other than X and Y on ($l$); that is, 12 and 13. Let us choose point 12 for $U_1$ and point 13 for $U_2$. The finite lines passing through X, denoted (X), are $\ell_1^x = \{1, 6, 8, 10\}$, $\ell_2^x = \{2, 4, 9, 10\}$, $\ell_3^x = \{3, 5, 7, 10\}$; the finite lines passing through Y, denoted (Y), are $\ell_1^y = \{1, 2, 3, 11\}$, $\ell_2^y = \{4, 5, 6, 11\}$,

$\ell_3^y = \{7, 8, 9, 11\}$; the finite lines passing through $U_1$, denoted $(U_1)$, are $\ell_1^{u_1} = \{1, 5, 9, 12\}$, $\ell_2^{u_1} = \{2, 6, 7, 12\}$, $\ell_3^{u_1} = \{3, 4, 8, 12\}$; and the finite lines passing through $U_2$, denoted $(U_2)$, are $\ell_1^{u_2} = \{1, 4, 7, 13\}$, $\ell_2^{u_2} = \{2, 5, 8, 13\}$, $\ell_3^{u_2} = \{3, 6, 9, 13\}$.

Recall that for a finite point $P$, its coordinate $(x,\ y)$ is defined by letting x be the number of a line of (X) passing through $P$ and letting y be the number of a line of (Y) passing through $P$. We see that our finite points have the following coordinates: (1, 1) for 1, (2, 1) for 2, (3, 1) for 3, (2, 2) for 4, (3, 2) for 5, (1, 2) for 6, (3, 3) for 7, (1, 3) for 8, and (2, 3) for 9.

If $\ell_k^{u_1}$ is the line in the set $(U_1)$ passing through a coordinate $(x,\ y)$, we insert the element $k$ in row $x$, column $y$. For instance, the line $\ell_1^{u_1}$ passes through point 1, and so we insert the element 1 at coordinate (1, 1). Continuing in this manner with all $3^2$ coordinates $(x,\ y)$, we obtain the Latin square $[L_1]$:

$$\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array}$$

Figure 6: The Latin square associated with $(U_1)$, denoted $[L_1]$.

The Latin square $[L_2]$, which is associated with the set of lines $(U_2)$, is constructed equivalently, but now we instead look at the lines of $(U_2)$ passing through each coordinate:

$$\begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{array}$$

Figure 7: The Latin square associated with $(U_2)$, denoted $[L_2]$.

By superimposing the elements of these Latin squares onto each other, we obtain the desired Graeco-Latin square of order 3:

$$\begin{array}{ccc} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{array}$$

Figure 8: A Graeco-Latin square of order 3. Compare Figure 2.

## 3.3 From a set of MOLS to a finite projective plane

Let us now assume we have the $n-1$ Latin squares $L_1, L_2, \ldots, L_{n-1}$ which are mutually orthogonal. From these Latin squares, we may construct a finite projective plane of order $n$.

The set of points in the finite projective plane will be $P = \{x, y, 1, \ldots, n-1\} \cup n \times n$, where $n \times n$ is the Cartesian product of the set $\{1, \ldots, n\}$ with itself and where $x$, $y$ are formal symbols. The lines L of the plane will be

$$\begin{aligned} l_\infty &= \{x, y, 1, \ldots, n-1\}, \\ l_{x,i} &= \{x, (i,1), ..., (i,n)\} \quad for\ i\ \in \{1, \ldots, n\}, \\ l_{y,j} &= \{y, (1,j), ..., (n,j)\} \quad for\ j\ \in \{1, \ldots, n\}, \\ l_{k,b} &= \{k\} \cup \{(i,j), \in n \times n \,|\, (L_k)_{ij} = b\} \quad for\ k\ \in \{1, \ldots, n-1\}, b \in \{1, \ldots, n\}. \end{aligned}$$

Then (P, L) is a finite projective plane. Note that we have $n^2 + n + 1$ points and $n(n-1) + 2n + 1 = n^2 + n + 1$ lines, and so we would be constructing a finite projective plane of order $n$, in accordance with Theorem 2.2.

*Proof.* It is trivial to see that every line contains at least three points and that there is more than one line, fulfilling two of the axioms for a projective plane. To prove that the axiom stating that every pair of points lies on a unique line is also fulfilled, consider the following:

If one of the points is x or y, it is clear from the above construction of the lines in the plane that, given a second point, the pair of points will lie on a unique line. If the pair of points are from $\{1, \ldots, n-1\} \subseteq P$, it is also clear they lie on a unique line. In the case where $k \in \{1, \ldots, n-1\}$ and $(i,j) \in n \times n$, the entry $(L_k)_{ij} = b \in \{1, \ldots, n\}$ is uniquely determined by the choice of the Latin square $L_k$

and its entry $(i, j)$. Hence $k$ and $(i, j)$ lie on the line $l_{k,b}$, and this is the unique line in the plane containing these two points.

It remains to prove that the last remaining axiom, stating that any two lines have in common exactly one point, is fulfilled. If one of the lines is $l_\infty$, this is obvious. For all other cases, let us consider the intersections

$$l_{x,i} \cap l_{k,b}$$
$$l_{y,j} \cap l_{k,b}$$
$$l_{k,b} \cap l_{k',b'}.$$

For $b, i \in \{1, \ldots, n\}$ and $k \in \{1, \ldots, n-1\}$, there is only one entry labeled $b$ in the $i$-th row of $L_k$. This tells us that $|\, l_{x,i} \cap l_{k,b} \,| = 1$; that is, $l_{x,i}$ and $l_{k,b}$ share in common only one point. Similarly, $|\, l_{y,j} \cap l_{k,b} \,| = 1$ for all $j, b \in \{1, \ldots, n\}$ and all $k \in \{1, \ldots, n-1\}$, because there is only one entry labeled $b$ in the $j$-th column of $L_k$.

Let us consider the intersection $l_{k,b} \cap l_{k',b'}$ for $b, b' \in \{1, \ldots, n\}$ and $k, k' \in \{1, \ldots, n-1\}$ such that $(k, b) \neq (k', b')$. Assume that $k = k'$. Then we know that $b \neq b'$, and we have $l_{k,b} \cap l_{k,b'} = \{k\}$, since $(i, j) \in l_{k,b} \cap l_{k,b'}$ implies that $b = (L_k)_{i,j}$ and $b' = (L_k)_{i,j}$, which is a contradiction.

Now assume that $k \neq k'$. Since $L_k$ and $L_{k'}$ are orthogonal Latin squares, there is only one entry $(i, j)$ such that $((L_{ki,j}), (L_{k'i,j})) = (b, b')$. Thus, we have that $l_{k,b} \cap l_{k',b'} = \{(i, j)\}$, verifying the final axiom of a finite projective plane. □

## 3.4 Constructing a finite projective plane from a set of MOLS

Let us construct a finite projective plane from the two earlier $3 \times 3$ MOLS $[L_1]$ and $[L_2]$, as seen in section 3.2. We have the set of points $P = \{x, y, 1, 2\} \cup 3 \times 3$, where $3 \times 3$ symbolizes the set $\{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)\}$. This gives us $n^2 + n + 1 = 13$ points in P, as expected. Now, in accordance with the

construction above, the set of lines L in the plane are

$$l_\infty = \{x, y, 1, 2\},$$
$$l_{x,1} = \{x, (1,1), (1,2), (1,3)\}, l_{x,2} = \{x, (2,1), (2,2), (2,3)\}, l_{x,3} = \{x, (3,1), (3,2), (3,3)\},$$
$$l_{y,1} = \{y, (1,1), (2,1), (3,1)\}, l_{y,2} = \{y, (1,2), (2,2), (3,2)\}, l_{y,3} = \{y, (1,3), (2,3), (3,3)\},$$
$$l_{1,1} = \{1, (1,1), (2,3), (3,2)\}, l_{1,2} = \{1, (1,2), (2,1), (3,3)\}, l_{1,3} = \{1, (1,3), (2,2), (3,1)\},$$
$$l_{2,1} = \{2, (1,1), (2,2), (3,3)\}, l_{2,2} = \{1, (1,2), (2,3), (3,1)\}, l_{2,3} = \{1, (1,3), (2,1), (3,2)\}.$$

We can easily verify that there are $n^2 + n + 1 = 13$ lines, that each line contains $n + 1 = 4$ points, and that each point is contained in $n + 1 = 4$ lines. (P, L) is our desired finite projective plane.

Referring back to Figure 5, we see that the points {10, 11, 12, 13} correspond to the points {1, y, 2, x}, respectively, in (P, L) (these points represent the lines at infinity); 1 corresponds to (1, 1), 2 corresponds to (2, 1), 3 corresponds to (3, 1), 4 corresponds to (1, 2), 5 corresponds to (2, 2), 6 corresponds to (3, 2), 7 corresponds to (1, 3), 8 corresponds to (2, 3), and, finally, 9 corresponds to (3, 3). Note here how the lines $l_{x,1}$, $l_{x,2}$, and $l_{x,3}$ correspond to the "vertical" lines in the original figure, which connect to the point at infinity drawn at the bottom (labeled 13), whereas the lines $l_{y,1}$, $l_{y,2}$, and $l_{y,3}$ correspond to the "horizontal" lines connecting to the point at infinity directly to the right of points 1 through 9 in the original figure (labeled 11).

# 4

# Proving the nonexistence of some finite projective planes

The search for orthogonal Latin squares is equally concerned with proving the nonexistence of certain orthogonal Latin squares. In this section, we will examine some such proofs.

## 4.1 The Bruck-Ryser theorem

In 1948, Bruck and Ryser published a paper stating the following:

**Theorem 4.1.** *If* $n \equiv 1 \mod 4$ *or* $n \equiv 2 \mod 4$*, then a necessary condition for the existence of a finite projective plane of order* n *is that there exist integers* $x$ *and* $y$ *such that* $n = x^2 + y^2$*.*

Since from a complete set of MOLS of order $n$ we can construct a finite projective plane of the same order, the above theorem tells us that we will not find a complete set for any such $n$. (However, it may still be possible to find an incomplete set of MOLS for the given order.)

To sketch a proof of the theorem, let us recall that finite projective planes may be represented by an incidence matrix, where we enter a 1 in the corresponding row and column if a line contains a certain point and enter a 0 otherwise.

**Theorem 4.2.** *Given a finite projective plane geometry* $P$ *with* $n + 1$ *points on a line, there exists an incidence matrix* $A$ *of order* $n^2 + n + 1$*. If* $A^T$ *denotes the transpose of the matrix* A*, then* $A \cdot A^T = A^T \cdot A$ *is a matrix with* $n + 1$ *down the main diagonal and ones elsewhere.*

*Proof.* Let the $n^2+n+1$ points of P be ordered $1, 2, \ldots, n^2+n+1$ and listed in a row. Let the lines be equivalently ordered and listed in a column. Now let a table of size $(n^2+n+1)^2$ be formed by inserting a 1 in position (i, j) if line i contains point j and a 0 otherwise. It follows that the table yields an incidence matrix $A$ which satisfies $A \cdot A^T = A^T \cdot A$. □

We may wish to consider an example to illustrate the above. Recall the incidence matrix associated with the Fano plane, here referred to as $A$. Indeed, we see the theorem holds, as

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}, A^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix},$$

and therefore (with $n+1=3$):

$$A \cdot A^T = A^T \cdot A = \begin{bmatrix} 3 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 3 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 3 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 3 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 3 \end{bmatrix}.$$

Given such an incidence matrix, we may also use it to arrive at its corresponding projective plane:

**Theorem 4.3.** *If a matrix* A *with non-negative integer elements of order* $n^2+n+1, n \geq 2$, *satisfies* $A \cdot A^T = A^T \cdot A$, *which is constant along the diagonal and has ones elsewhere, then* A *is an incidence matrix that defines a projective plane geometry with* $n+1$ *points on a line.*

*Proof.* $A$ must be composed entirely of ones and zeroes; if an element of $A$, $a_{i,j}$, were to be greater than 1, then given $A \cdot A^T = A^T \cdot A$, all elements in column $j$ of $A$ except $a_{i,j}$ would be zero and all elements in row $i$ of $A$ except $a_{i,j}$ would also be zero. This would mean $A \cdot A^T$ contains an element zero, which is impossible since $A \cdot A^T = A^T \cdot A$. From the conditions given in the theorem, it follows that $A$ is an incidence matrix which can be used to define a finite projective plane. □

We now outline the strategy of Bruck-Ryser. Let us first briefly recall the definition of *matrix congruence*.

**Definition 4.4.** If $A$ and $B$ are symmetric matrices of order $n$ with elements in $\mathbb{R}$, then $A$ and $B$ are *congruent* (written $A \sim B$) if there exists a non-singular matrix $C$ with elements in $\mathbb{R}$ such that $A = C^T BC$.

Suppose that $A$ is a symmetric matrix with elements in $\mathbb{N}$ of order and rank $n$. Then we can construct a diagonal matrix $D = [d_1, d_2, \ldots, d_n]$ where $d_i \neq 0$ for $i = 1, 2, \ldots, n$ such that $D \sim A$. The number of negative terms $\iota$ in the diagonal is called the *index* of $A$, and it is an invariant of $A$ according to Sylvester's law of inertia.

Let $d = (-1)^{\iota}\delta$, where $\delta$ is the determinant $|A|$ of $A$ with the square factors removed. From $B = C^T AC$, it follows that $|B| = |C|^2|A|$, and so $d$ is the second invariant of A.

Now let us consider the third invariant $c_p$, which completes the system alongside $\iota$ and $d$. The Hilbert norm-residue symbol $(m, n)_p$ is defined for every prime $p$ and arbitrary $m$ and $n$, $m, n \neq 0, m, n \in \mathbb{Z}$. While it is outside the scope of this paper, it is provable that $c_p = -1$ for only a finite number of $p$, and is defined for every odd prime $p$ by the equation

$$c_p = c_p(A) = (-1, -D_n)_p \prod_{i=1}^{n-1} (D_{i'}, -D_{i+1})_p. \tag{1}$$

Let us now state, without proof, another theorem: the Minkowski-Hasse theorem.

**Theorem 4.5.** *Let $A$ and $B$ be two symmetric matrices of order and rank $n$ with integer elements. Suppose the principal minor determinants of $A$ and $B$ are not zero.*

*Then $A \sim B$ iff $A$ and $B$ have the same invariants $\iota$, $d$, and $c_p$ for every odd prime $p$.*

With this information, we may proceed to sketch the proof for the Bruck-Ryser theorem.

*Proof.* Let $N$ be a positive integer and let $B_n$ be a matrix of order $n$ with $N+1$ down the main diagonal and with ones in all other positions. By subtracting the first column of $B_n$ from all other columns and adding the first row to all other rows, we get

$$|B_n| = N^{n-1}(N+n). \tag{2}$$

Note that if $n = N^2 + N + 1$, then $B_n$ is equivalent to the matrix referred to as $A \cdot A^T$ in Theorem 4.3 and its determinant is the square of an integer.

If instead row $n$ of $B_n$ is subtracted from all other rows and column $n$ is subtracted from all other columns, we receive a matrix $Q_n$ with $2N$ down the main diagonal save for in position $(n, n)$, where we have $N+1$. Further, all other elements in the matrix are $N$ save for the elements in row and column $n$, which are $-N$.

The matrix $Q_n$ is congruent to $B_n$, and so for every odd prime $p$, we have that $c_p(B_n) = c_p(Q_n)$. If $E_i$ denotes the determinant of order $i$ with $2N$ down the main diagonal and N in all other positions, then $E_i = N^i(i+1)$.

If $n = N^2 + N + 1$ and if $p$ is an odd prime, then the invariant $c_p(B) = c_p(Q_n)$ of the matrix $B$ is given by

$$c_p(B) = (E_{n-1}, -1)_p \prod_{i=1}^{n-2} (E_i, -E_{i+1})_p.$$

We state now, without proof, that

$$c_p(B) = (-1, N)_p^{\frac{N(N+1)}{2}}.$$

Now let $\pi$ be a finite projective plane with $N+1$ points on a line. Then according to Theorem 4.2, the matrix $B$ is congruent to the identity matrix $I$. Given that

$c_p(I) = +1$ for every odd prime $p$, it follows that if $\pi$ exists, then for all odd primes $p$,

$$c_p(B) = (-1, N)^{\frac{N(N+1)}{2}} = +1.$$

If $n \equiv 1 \mod 4$ or $n \equiv 2 \mod 4$, then $\frac{N(N+1)}{2}$ is odd. Further, if a prime $p$ of the form $4k + 3$ divides the squarefree part of n, then $(-1, N)_p = -1$. This contradicts the above equation, and so the sketch of the proof is complete. □

## 4.2 The non-existence of a finite projective plane of order 6

Recall Theorem 4.1 (the Bruck-Ryser theorem). From this, it is clear that no projective plane of order 6 exists, because $6 \equiv 2 \mod 4$, and there are no integers $x$ and $y$ for which $x^2 + y^2 = 6$.

It is worth nothing that the Bruck-Ryser theorem was not used in the first proof to show there is no finite projective plane of order 6, and it also does not help solve Euler's problem of the 36 officers. For this reason, we may wish to briefly expound on the previously-mentioned proof provided by Gaston Tarry, which stated that a Graeco-Latin square of order 6 does not exist.

There are over 800 million unique Latin squares of order 6, and so it was not feasible to compare them all by hand; instead, Tarry considers only *reduced Latin squares*—that is, Latin squares of order $n$ whose entries in the first row and column are the integers $1, 2, \ldots, n$—as any Latin square can be transformed into such a reduced form by permuting the rows and columns without affecting whether or not it has an orthogonal mate. This narrowed down the amount of unique Latin squares to study to 9408.

Tarry then further narrowed down the problem by defining 17 families of Latin squares and proving that any reduced Latin square of order 6 is in one of these families. Finally, he proved that any reduced Latin square that belongs to one of the 17 families can not be mutually orthogonal. Curious readers may wish to refer to [Hor16] for a more detailed recount of the proof.

## 4.3 The non-existence of a finite projective plane of order 10

It was not until 1989 that Lam, Thiel, and Swiercz showed, with the aid of a computer, that finite projective planes of order 10 do not exist. Much as Bruck and Ryser had previously, they came to study incidence matrices, as well as *codewords*.

**Definition 4.6.** Let A be an incidence matrix of size $(n^2 + n + 1)^2$ representing a projective plane of order n and let $S$ be the vector space generated by the rows of A over $F_2$. A vector in $S$ is called a *codeword*.

The *weight* of a codeword is the number of 1s in the codeword, and the *weight enumerator* of S is

$$\sum_{i=0}^{n^2+n+1} w_i x^i,$$

where $w_i$ is the number of codewords of weight $i$.

Previous research had shown that the weight enumerator of $S$ is uniquely determined once $w_{12}$, $w_{15}$, and $w_{16}$ are known. $w_{15}$ proved unusually quick to find by way of a computer search, requiring a mere 3 hours of computer time, and was found to be 0.

Finding the number codewords of weight 12, on the other hand, was an arduous task: the associated search tree had an estimated $4 \times 10^{11}$ nodes, and with the program's creators expecting to process $10^5$ nodes per second, the required computing time would be around 50 days. However, in actuality, the search took 183 days, as the computer was only able to process $3 \times 10^4$ nodes per second. $w_{12}$ also turned out to be 0. By the time they searched for $w_{16}$, the programs were more carefully optimized, resulting in a computing time of 80 days. Yet again, the result was 0.

Hence, for a projective plane of order 10, $w_{12} = 0$, $w_{15} = 0$, and $w_{16} = 0$, and so the weight enumerator is indeed computable. It was further determined that $w_{19} = 24\,675$: that is to say, for a projective plane of order 10 to exist, it must contain 24 675 codewords of weight 19. If these 19-point configurations could be proven to not exist, then neither would a projective plane of order 10, and so this was the method used to prove the plane's non-existence.

It was expected that this would take considerably longer than finding $w_{12}$ and $w_{16}$. Initially, the researchers were only able to proceed at 60 nodes per second, meaning a full search at the same pace would have required around 100 years of computing time.

Evidently, the program needed to be drastically sped-up, and so the CRAY supercomputer was used to ensure faster calculation. The search required around 80 days of computing time, and nodes were processed at a rate of $2 \times 10^4$ per second. The slower computing time compared to the earlier codeword searches is explained by the fact that it is simply more difficult to find codewords of weight 19—part of the issue lies in 19 being an odd number, which complicated calculations.

The data from the search performed by the CRAY supercomputer was compiled into two tables. While the full contents of these tables are outside the scope of the paper, they show that, even after trying every possible case, a completion to a full incidence matrix could not be found. Therefore, a finite projective plane of order 10 does not exist.

## 4.4 The open case of finding a finite projective plane of order 12

While it is in theory possible to extend the methods used by Lam, Thiel, and Swiercz to find a projective plane of order 10 in order to find planes of higher orders, such as 12, this has not yet been done. As the search space for a finite projective plane of order 12 would be considerably larger than the search space for a plane of order 10, one might surmise that such a computer search is simply not feasible, even with the technology available today.

There has nevertheless been some research done into the topic. Most intriguingly, in 2011, Bashir and Rajah stated the following conjecture, which investigates the matter through the link between finite projective planes and MOLS:

**Conjecture 4.7.** Let $n$ be an integer and let $\sigma(n)$ denote the sum of all positive divisors of $n$ (including itself). If $\sigma(n) > 2n$, then there is no complete set of n - 1 MOLS that corresponds to a finite projective plane. From this, it follows that there is no finite projective plane of order $n$.

Here we note that $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$, and indeed, $28 > 24$—hence the conjecture implies there is no finite projective plane of order 12. Could this conjecture be proven, it would effect a great step forward in the search for finite projective planes.

# References


[And07] L. D. Andersen. *Chapter on The history of Latin squares.* Aalborg University, Research Report Series No. R-2007-32.

[Bas11] M. A. Bashir, A. Rajah. *On projective planes of order 12..* World Applied Sciences Journal, Vol. 14, No. 4, pages 957-972, 2011.

[Bos38] R. C. Bose. *On the Application of the Properties of Galois Fields to the Problem of Construction of Hyper-Græco-Latin Squares.* Sankhyā: The Indian Journal of Statistics, Vol. 3, No. 4, pages 323-338, 1938.

[Bot61] T. Botts. *Finite planes and latin squares.* The Mathematics Teacher, Vol 54, No. 5, pages 300-306, 1961.

[Bru48] R. H. Bruck, H. J. Ryser. *The Nonexistence of Certain Finite Projective Planes.* Canadian Journal of Mathematics, Vol. 1, pages 88–93, 1949.

[Hor16] H. Horner. *Even Famous Mathematicians Make Mistakes!.* Whitman College, Bachelor's Thesis, 2016.

[Lam89] C. W. H. Lam, L. Thiel, and S. Swiercz. *The non-existence of finite projective planes of order 10.* Canadian Journal of Mathematics, Vol 16, No. 6, pages 1117-1123, 1989.

[Lam91] C. W. H. Lam. *The search for a finite projective plane of order 10.* The American Mathematical Monthly, Vol. 98, No. 4, pages 305-318, 1991.

[Ral89] R. P. Grimaldi. *Discrete and Combinatorial Mathematics, Second Edition.* Addison-Wesley Publishing Company, 1989.