Hang Lung Mathematics Awards
Vol. 3 (2008), pp. 129–158

A CURSORY DISPROOF OF EULER'S CONJECTURE CONCERNING GRAECO-LATIN SQUARES BY MEANS OF CONSTRUCTION

TEAM MEMBER
Jun-Hou Fung[1]

SCHOOL
Canadian International School of Hong Kong

Abstract. In this report, our team has explored the mathematical structure of Graeco-Latin squares. Although we give a review of the scope of this field, our focus is on Euler's Conjecture. According to this conjecture, Graeco-Latin squares of certain orders do not exist. In this report, we disprove this conjecture by demonstrating a means to construct an infinite number of these so-called non-existent squares, following Sade. This branch of mathematics is related to group theory, combinatorics, and transversal design; therefore, we will also provide a brief overview of these topics throughout this report.

1. A Short Introduction to the Problem

Mathematics is ubiquitous in our daily world. Engineers use it to design bridges. Financial analysts use it to keep track of fluctuations in the economy. Even chefs are not immune to the necessity of math — they use it to determine how much of an ingredient is needed for a recipe and how much time to allow a stew to simmer. Even so, I cannot deny that I was mildly surprised when the Physical Education Department at my school approached the Mathematics Department October last year to solve a problem that will lead me to discover over two hundred years of mathematics produced by some of its greatest practitioners that have ever lived.

Their problem appears simple and concerns the arrangement of 30 teams during a sporting event, with the following requirements:

[1]This work is done under the supervision of the author's teacher, Mr. Jonathan Hamilton

1. There are six events that was going to occur that day; all 30 teams must attend all six events.
2. There is only time enough for six time slots; therefore, at any given time, each team must be attending one event.
3. Simple arithmetic will show that at any given time, there will be five teams at each of the six events.
4. No two teams may share a common time and event twice. This means that each team will face 24 of the 29 other teams with no duplication during the course of the day.
5. Naturally, it is absurd to suggest that a team can be at two events at the same time.

Truly, this seemed to be such a trivial problem that I did not at first try to elegantly resolve it. I had thought that brute force will yield the answer in a couple of minutes.

After three sheets of failed attempts and a broken pencil, I started to devise algorithms by analysing possible combinations of smaller size that may yield the solution. The techniques I have used, which were discovered by the great Swiss mathematician, physicist, and thinker, Leonhard Euler (1707 – 1783), included single-step and double-step arrays. (We will discuss this in chapters three and four.)

However, when that method failed too, I became so disillusioned that I began to resort to obtaining a disproof of its existence. Eventually, I was guided by my research to the peculiar mathematical structure of Latin squares and Graeco-Latin squares.

Throughout my investigation, my focus turned from sporting events to these Latin squares: their properties, their construction, and the non-existence of Graeco-Latin squares of order six. (The reader will notice the recurrence of the number six in both problems.)

Having embarked on such an investigation, I attempted my first proofs of non-existence based on some rudimentary group theory from abstract mathematics. The reason for this is because multiplication tables, indeed *Cayley tables*, of quasi-groups are by definition also Graeco-Latin squares. (See Appendix A.)

However, Henry Mann has shown in the 40's and 50's that any such attempt based on groups will be inconclusive, because although all Cayley tables of quasigroups are Graeco-Latin squares, the converse is not true: i.e. not all Graeco-Latin squares correspond to a Cayley table.

Finally, we come to the topic and purpose of this report: the disproof of Euler's conjecture (which deals with the non-existence of Graeco-Latin squares of order $4k + 2$). However, before doing so, we familiarize ourselves with the terminology and some definitions in this field. These will be covered in chapter two.

2. Some Basic Definitions

2.1. Outline

In this chapter, we will explore some basic concepts pertaining to the problem. We will begin by introducing Latin and Graeco-Latin squares and culminate in a formal statement of Euler's Conjecture.

2.2. Squares

2.2.1. Latin Squares

Definition 1. *A* Latin square *of order n is a $n \times n$ array filled with n different symbols in a way such that each symbol occurs exactly once in each row and column.*

These structures are named by Euler as such because his scheme of symbols employed the Latin alphabet: A, B, C...

We offer examples of Latin squares below.

- A Latin square of order 1 (the trivial group)
  $\begin{pmatrix} 1 \end{pmatrix}$
- A Latin square of order 2 (the binary group)
  $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
- A Latin square of order 3
  $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$
- A Latin square of order 4

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

- Another Latin square of order 4 (the Klein four-group)

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

- A Latin square of order 5

$$\begin{pmatrix} 1 & 3 & 2 & 5 & 4 \\ 4 & 2 & 1 & 3 & 5 \\ 5 & 1 & 4 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$$

2.2.2. Graeco-Latin Squares

Definition 2. *A* Graeco-Latin square *of order n is the superposition of two Latin squares of order n such that it yields all n^2 different combinations in its cells. Two Latin squares having this property are said to be* orthogonal *to each other.*

They are also called orthogonal Latin squares or Euler squares. These terms will be used interchangeably in this report.

These structures are named by Euler as such because his scheme of symbols for Graeco-Latin squares employed the Latin alphabet: A, B, C..., and the Greek alphabet: α, β, γ....

We offer examples of Graeco-Latin squares below.

- An Euler square of order 3

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

- An Euler square of order 4

$$\begin{pmatrix} (1,1) & (2,2) & (3,3) & (4,4) \\ (2,3) & (1,4) & (4,1) & (3,2) \\ (3,4) & (4,3) & (1,2) & (2,1) \\ (4,2) & (3,1) & (2,4) & (1,3) \end{pmatrix}$$

- An Euler square of order 5
$$\begin{pmatrix} (1,5) & (2,4) & (3,3) & (4,2) & (5,1) \\ (2,1) & (3,5) & (4,4) & (5,3) & (1,2) \\ (3,2) & (4,1) & (5,5) & (1,4) & (2,3) \\ (4,3) & (5,2) & (1,1) & (2,5) & (3,4) \\ (5,4) & (1,3) & (2,2) & (3,1) & (4,5) \end{pmatrix}$$

We will describe their construction in greater detail in chapter four.

2.2.3. On Mutually Orthogonal Latin Squares

Definition 3. Mutually orthogonal Latin squares *of order n, also known as MOLS of order n, are Latin squares which are pairwise orthogonal to each other. (cf.* ***Reviewer's Comment*** *1)*

Definition 4. *A* complete set of MOLS *of order n is a set of $n-1$ MOLS of order n.*

Theorem 5. *In accordance to the above theorem a Latin square of order n can have at most $n-1$ MOLS. (cf.* ***Reviewer's Comment*** *2)*

In this report, we will not go over mutually orthogonal Latin squares in detail. I include them as an extension, as there are still some fertile problems in their field. For example, the following conjecture has been regarded by some to be the next 'Fermat's Last Theorem'.

Conjecture 6. *A complete set of MOLS of order n exists for all composite n.*

It is well-known that complete sets exist for prime n.

Theorem 7. *A complete set of MOLS of order n exists for all prime n.*

See Appendix B for more information.

2.3. Euler's Conjecture

Euler's name is associated with a diverse range of mathematics. In this report, one of his works is of particular importance to us: *Recherches sur une nouvelle espèce de quarrés magiques* (1782).

In *Recherches*, Euler demonstrates algorithms to create Graeco-Latin squares of odd n and of n a multiple of four. This meant that he was able to construct such squares of order 1, 3, 4, 5, 7, 8, 9, and so on.

However, unable to construct a Graeco-Latin square of order 2 (the reader may want to verify this through simple exhaustive enumeration) and order 6, he conjectured that squares of these orders do not exist.

Conjecture 8 (Euler's conjecture)**.** *Graeco-Latin squares of order* $4k + 2$ *do not exist for all integer* k*.*

It is such a simple statement that one would not believe that it would be solved only after nearly 200 years of work done by dozens of mathematicians using the cutting-edge tools of modern mathematics.

3. History and Application

3.1. Euler

Euler can be said to be the pioneer of this field in combinatorics, and his pioneering work *Recherches* has already been roughly discussed. The purpose of his paper was to investigate the '36 officers problem', which goes like this:

> How can a delegation of six regiments, each of which sends a colonel, a lieutenant-colonel, a major, a captain, a lieutenant, and a sub-lieutenant be arranged in a regular 6×6 array such that no row or column duplicates a rank or a regiment?

This is obviously isomorphic to the problem of finding a Graeco-Latin square of order six. (We shall see that it is impossible.)

In the introduction of his *Recherches*, he lays the foundations and develops the notation of Latin and Graeco-Latin squares. He also conceptualized his idea of 'formules directices', an algorithm of sorts that will complete a Latin square, i.e. find a second Latin square orthogonal to the first to create a Graeco-Latin square. His techniques of single-step and multiple-step squares are also introduced in this part. Euler opens with the statement that Euler square of order six are not possible:

> Une question fort curieuse, qui a exercé pendant quelque temps la sagacité de bien du monde, m'a engagé à faire les recherches suivantes qui semblent ouvrir une nouvelle carrière dans l'Analyse, et en particulier dans la doctine des combinaisons. Cette question rouloit sur une assemblée de 36 Officiers de six différens grades et tirés de six Régimens différens, qu'il s'agissoit de ranger dans un

> quarré, de manière que sur chaque ligne tant horizontale que verticale il se trouva six Officiers tant de différens caractères que de Régimens différens. Or, après toutes les peines qu'on s'est donné pour resoudre ce Problème, on a été obilgé de réconnoître, qu'un tel arrangement est absolument impossible; quoiqu'on ne puisse pas, en donner de démonstration rigoureuse.

In part one, he discusses his methods for single-step squares in greater detail ,giving extensive examples and description of Euler squares of order 2, 3, 5, 7, and 9. Euler also derived a set of equations pertaining to his 'guiding formulae'. In addition, he also explored the connection between Graeco-Latin squares and magic squares.

Definition 9. *A* magic square *of order n is an arrangement of n^2 numbers in a square, such that the n numbers in every row and every column have a sum of some constant k.*

Euler gives a method to transform Graeco-Latin squares of order n to magic squares of order n: simply replace (a, b) in every cell of the Graeco-Latin square with $(a-1)n+b$. It is clear that this will always produce a magic square. For example:

An Euler square of order 3
$$\begin{pmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{pmatrix}$$

becomes

A magic square of order 3
$$\begin{pmatrix} 1 & 5 & 9 \\ 6 & 7 & 2 \\ 8 & 3 & 4 \end{pmatrix}$$

(Additional requirements are needed to have the *diagonals* to sum to k.)

Part two of his work deals with double-step Graeco-Latin squares, giving such squares of order 4 and 8. He also begins to examine isotopy classes in this chapter, which is also continued in part five.

Definition 10. *An* isotopy class *is the equivalence class of Latin squares formed by isotopy relations, such as the permutation of rows, columns, and sybmols.*

In part three, Euler uses a triple-step construction to create a Graeco-Latin square of order 9. It is also in this part he begins to claim that an Euler square of order 6 is not possible. In part four, Euler uses a quadruple-step construction to create a Graeco-Latin square of order 8.

3.2. Before the 20^{th} Century

After this extensive study of Graeco-Latin squares done by Euler, the problem has been laid aside by most of the mathematical community until the 20^{th} century. However, this is not to say that there was no new advances in this period of time.

In 1842, Heinrich Schumacher in a letter to Carl Gauss wrote that his assistant, Thomas Clausen, have completed a proof of non-existence of Euler squares of order six. This was done, he said, by dividing all the Latin squares of order 6 into seven distinct isotopy classes and proving that none of them could be completed. However, the purported 'proof' was lost and never found.

3.3. The 20^{th} Century

Half a century later in 1900, a French amateur mathematician, Gaston Tarry, provided the first surviving proof. Tarry's methodology is similar to Clausen's. It included the analysis of the 17 isotopy classes. Furthermore, Tarry also hand-enumerated 9408 seperate cases, thus fulfilling Euler's wish for a proof of the non-existence of Euler squares of order 6.

After this, there was a race between mathematicians to provide a more elegant proof of Tarry's results. In 1902, Peterson published a proof using geometric arguments and Euler's polygonal formula. However, in 1910, Wernicke showed that Peterson's proof is incomplete and started to apply a group-theoretic technique to the problem.

One of the main proponents of the application of group theory to the problem at that time was MacNeish. In 1922, MacNeish managed to disprove Wernicke's results, and defined a 'direct product' of Euler squares. A direct product of two Euler squares will yield an Euler square of some greater order. (We will explore a similar constuction, the singular direct product, later.)

MacNeish also proved some general theorems in this field:

Theorem 11. *Let $N(n)$ be the maximum (cf.* ***Reviewer's Comment*** *3) number of MOLS of order n. Then*

$$N(ab) \geqslant \min\{N(a), N(b)\} \tag{1}$$

Theorem 12. *Let $p_1^{e_1}p_2^{e_2}p_3^{e_3}\cdots p_k^{e_k}$ be the prime factorization of n. Then*

$$N(n) \geqslant \min\{p_i^{e_i} - 1\} \tag{2}$$

Conjecture 13 (MacNeish's conjecture)**.**

$$N(n) = \min\{p_i^{e_i} - 1\} \tag{3}$$

Corollary 14. (Corollary to MacNeish's conjecture.) *If MacNeish's conjecture is true, then Euler's conjecture is true.*

Proof of the Corollary to MacNeish's conjecture. If MacNeish's conjecture is true, then all Euler squares of order $4k+2$ will have no orthogonal mate, because $p_i^{e_i} = 2^1$ is the smallest prime power in $4k+2$. Therefore the maximum number of MOLS of order $4k+2$ is $2-1=1$ (i.e. there are no orthogonal Latin squares of order $4k+2$, which is Euler's conjecture) (cf. **Reviewer's Comment** 4). □

Later, Fisher conjectured that

Conjecture 15. *A complete set of MOLS of order n exists for all prime n.*

This was soon proven true by Bose in 1938 using Galois fields.

Bose's other contributions to the problem included using fields and finite projective planes to construct Euler squares.

In 1942, Mann proved MacNeish's conjecture (and thus Euler's conjecture) on condition that

Condition 16. *There is a complete (cf.* ***Reviewer's Comment*** *5) bijection between the Cayley tables of quasigroups and Graeco-Latin squares.*

However, he also managed to prove that his condition was false by construction; therefore, he effectively nullified all the results of Bose and MacNeish in the last half century.

Mathematicians had to abandon their familiar groups and turn to other structures to shed light on Euler's conjecture. In 1959, Parker managed to use orthogonal arrays and block-designs to construct Graeco-Latin squares. This bypassed Mann's limitations. Using his methods, Parker also found a 4-MOLS of order 21, which disproved MacNeish's conjecture.

Later, Parker, Bose, and Shrikhande began to collaborate their findings. This yielded Graeco-Latin squares of order 10 and 22, which disproved Euler's conjecture once and for all.

Even though the conjecture was proven false, research in this topic never ceased. In 1960, Sade used a 'singular direct product' (SDP for short) to construct Graeco-Latin Squares. Finally, Stinston (1984) and Zhu Lie (1982), working independently, used mathematics from other fields such as graph theory and vector spaces to prove the 36 Officers problem, a full two hundred years after its initial statement by Euler in 1782.

3.4. Applications

Today, Euler squares are used in diverse fields, including algebraic coding theory (in error-correcting codes), statistical experiment designs, finite projective planes (e.g. the Bruck-Ryser theorem), and linear programming.

4. Approach and Execution

4.1. Approach

In this report, we will disprove Euler's conjecture by the construction of a Graeco-Latin square of order $4k + 2$. However, we will first go over some of Euler's methods as outlined in his *Recherches*.

4.2. Graeco-Latin Squares via Arithmetically Increasing Guiding Formulae

Before progressing any further, we must define what a guiding formula is.

Definition 17. *A* guiding formula *for a Latin square of order n is a sequence $(a_1, a_2, a_3, \dots a_n)$ such that the set of cells in the i^{th} row containing a_i form a transversal. A* transversal *of a Latin square of order n is a set of n cells, one in each row and column, such that no two cells contain the same symbol.*

For example (for sake of clarity, we will use the Latin and Greek alphabet here):

Given this Latin square of order five:

$$\begin{pmatrix} a & b & c & d & e \\ b & c & d & e & a \\ c & d & e & a & b \\ d & e & a & b & c \\ e & a & b & c & d \end{pmatrix}$$

A guiding formula for where we should place the symbol α would be (a, c, e, b, d). (cf. **Reviewer's Comment** 6) That is:

$$\begin{pmatrix} a^\alpha & b & c & d & e \\ b & c^\alpha & d & e & a \\ c & d & e^\alpha & a & b \\ d & e & a & b^\alpha & c \\ e & a & b & c & d^\alpha \end{pmatrix}$$

By permuting the guiding formula for α, we obtain the guiding formulae for β, γ, δ, and ϵ.

The final completed square is:

$$\begin{pmatrix} a^\alpha & b^\beta & c^\gamma & d^\delta & e^\epsilon \\ b^\epsilon & c^\alpha & d^\beta & e^\gamma & a^\delta \\ c^\delta & d^\epsilon & e^\alpha & a^\beta & b^\gamma \\ d^\gamma & e^\delta & a^\epsilon & b^\alpha & c^\beta \\ e^\beta & a^\gamma & b^\delta & c^\epsilon & d^\alpha \end{pmatrix}$$

Note that this is not the only possible guiding formula.

In this report, for sake of simplicity, we will only consider arithmetically increasing guiding formulae.

Definition 18. *An* arithmetically increasing guiding formula *is a guiding formula for a Latin square of order n such that $a_i \equiv n(i-1)+1$.*

4.2.1. Single-step Latin Squares

Definition 19. *A* single-step Latin square *is a Latin square such that each row and column forms a increasing sequence (*mod$n$*).*

This is a single-step Latin square of order 4.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

In his *Recherches*, Euler, citing many examples, found that all single-step Latin squares of odd order can be completed (cf. **Reviewer's Comment** 7) (that is, filled in to produce a Graeco-Latin square) via his guiding formulae, although he did not offer a rigourous proof for this. We, however, will explicitly prove this.

Proof: Any single-step Latin square of odd order can be completed. First, we note that we need only one transversal to prove this statement. This is a direct consequence from the theorems in Appendix A.

We also note that in the i^{th} row and the j^{th} column of a single-step Latin square of order n contains the symbol corresponding to $i + j - 1 \bmod n$.

Now, look at the main diagonal of such a square, that is, $i = j$, and so the diagonal elements are $2i - 1 \bmod n$. We want to show that this is a transversal, and we can do this by showing that $2i - 1 \bmod n$ takes on n different values as i takes on the numbers 1 through n.

Since there must be a value for $2i - 1 \bmod n$ for every i, we only need to show that they are all different. Now suppose that they are not all different. That is:

$$2i_u - 1 \bmod n = 2i_v - 1 \bmod n. \tag{4}$$

$$2i_u \bmod n = 2i_v \bmod n. \tag{5}$$

Since n is odd and therefore does not divide 2:

$$2(i_u \bmod n) = 2(i_v \bmod n). \tag{6}$$

$$i_u \bmod n = i_v \bmod n. \tag{7}$$

However, because $i \leqslant n$ and $u \neq v$,

$$i_u \bmod n \neq i_v \bmod n. \tag{8}$$

Proof by reductio ad absurdum.

Therefore, a tranversal exists and the Latin square can be completed. □

The above proof leads to the following theorem.

Theorem 20. *At least one Graeco-Latin square exists for each odd order.*

It would also be interesting to see why single-step construction cannot lead to a Graeco-Latin square of even order. This fact was proven by Euler.

Theorem 21. *No orthogonal mate exists for single-step Latin squares of even order.*

Proof. Suppose such a guide exists. We can denote this as $\{1, \alpha, \beta, \gamma, \ldots\}$. Since all the numbers in a row of a single-step Latin square increase by one and since α is taken from the second row (a) with the symbol a, $\alpha = a + 1$. Similarly, $\beta = b + 2$, $\gamma = c + 3$, and so on.

Now let

$$S = a + b + c + \ldots \tag{9}$$

Then,

$$\alpha + \beta + \gamma + \ldots = S + 1 + 2 + 3 + \ldots + (n - 1) \tag{10}$$

$$\alpha + \beta + \gamma + \ldots = S + \frac{1}{2}n(n - 1) \tag{11}$$

However, the difference between the two sums must be a multiple of n. Therefore,

$$\alpha + \beta + \gamma + \ldots - (a + b + c + \ldots) = \lambda n \tag{12}$$

$$\lambda n = \frac{1}{2} n(n-1) \tag{13}$$

$$\lambda = \frac{1}{2}(n-1) \tag{14}$$

Since this is an equation in integers, $n-1$ must be even, n must be odd. □

With this, I believe we have sufficiently explored single-step Latin squares.

4.2.2. Multi-step Latin squares

Since single-step Latin squares are already thoroughly discussed and are similar to multiple-step Latin squares, we will not prove the aforementioned theorems for multi-step Latin squares. We will, however, give their construction and state some theorems resulting from a particular case: double-step Latin squares.

Definition 22. *This is the form of a* double-step Latin square *of order* n*.*

$$\left(\begin{array}{cc|cc|cc|cc|cc}
1 & 2 & 3 & 4 & 5 & 6 & \cdots & \cdots & n-1 & n \\
2 & 1 & 4 & 3 & 6 & 5 & \cdots & \cdots & n & n-1 \\
\hline
3 & 4 & 5 & 6 & \cdots & \cdots & n-1 & n & 1 & 2 \\
4 & 3 & 6 & 5 & \cdots & \cdots & n & n-1 & 2 & 1 \\
\hline
5 & 6 & \cdots & \cdots & n-1 & n & 1 & 2 & 3 & 4 \\
\multicolumn{10}{c}{\textit{etc.}}
\end{array}\right)$$

Notice that we simply take each 2×2 *grouping and switch the elements on lower row.*

In his *Recherches*, Euler showed that all double-step Latin squares of orders $n = 4k$ can be completed with his other guiding formulae. Hence, the following theorem:

Theorem 23. *There exists at least one Graeco-Latin square of order* $4k$*.*

It is also interesting to note that if $n = 4k$ and $n > 8$, then an Euler square of order n can be constructed using the singular direct product to be discussed

in the next section if we take $p = k$, $m = 4$, and $q = 0$ (this is not the only possible option), except for the following cases.

Case 24. *We cannot use* $24 = (6)(4) + 0$*, because no Graeco-Latin square of order 6 exists. However, we can easily remedy this using* $24 = (5)(4) + 4$*. Also, we (at this point) cannot create Graeco-Latin squares of order* $40 = (10)(4) + 0$*, because we cannot create Graeco-Latin squares of order* $p = 4k + 2$*. However, this can be altered accordingly. (e.g.* $40 = (9)(4) + 4$*).*

This leaves us with Euler squares of order 4 and 8. Since we have already seen an Euler square of order 4, I shall present here a Graeco-Latin square of order 8 which is created by using Euler's guiding formula for double-step Latin squares.

$$\begin{pmatrix}
(1,1) & (2,8) & (3,7) & (4,6) & (5,4) & (6,5) & (7,2) & (8,3) \\
(2,2) & (1,7) & (4,8) & (3,5) & (6,3) & (5,6) & (8,1) & (7,4) \\
(3,3) & (4,2) & (5,1) & (6,8) & (7,6) & (8,7) & (1,4) & (2,5) \\
(4,4) & (3,1) & (6,2) & (5,7) & (8,5) & (7,8) & (2,3) & (1,6) \\
(5,5) & (6,4) & (7,3) & (8,2) & (1,8) & (2,1) & (3,6) & (4,7) \\
(6,6) & (5,3) & (8,4) & (7,1) & (2,7) & (1,2) & (4,5) & (3,8) \\
(7,7) & (8,6) & (1,5) & (2,4) & (3,2) & (4,3) & (5,8) & (6,1) \\
(8,8) & (7,5) & (2,6) & (1,3) & (4,1) & (3,4) & (6,7) & (5,2)
\end{pmatrix}$$

In addition, as we will see, we will need an idempotent (cf. **Reviewer's Comment** 8) square of order 4. For sake of organization, it will be presented here as well.

$$\begin{pmatrix}
(1,1) & (3,2) & (4,3) & (2,4) \\
(4,4) & (2,3) & (1,2) & (3,1) \\
(2,2) & (4,1) & (3,4) & (1,3) \\
(3,3) & (1,4) & (2,1) & (4,2)
\end{pmatrix}$$

4.3. Graeco-Latin Squares via SDP Construction

4.3.1. The Singular Direct Product

A. Sade first introduced this singular direct product (SDP) in 1960, in his *Produit direct-singulier de quasigroupes orthogonaux et anti-abéliens.*

Here, we shall first give a simple example of this construction. However, before that, we need to define an idempotent Latin square.

Definition 25. *An* idempotent Latin square *is a Latin square whose main diagonal is a transversal. (cf.* ***Reviewer's Comment*** *9)*

(*Transversals* are discussed – and defined – in more detail in Appendix A.)

To illustrate the construction, we will construct an Latin square of order 9.

The 'Ingredients'

Noting that $9 = 2(4) + 1$, we get $p = 2$, $m = 4$, and $q = 1$. Therefore we need a Latin square of order $p + q = 3$ (a subsquare of order 1 is trivial), a Latin square of order 2, and an idempotent Latin square - a Latin square whose main diagonal is a transversal - of order 4.

1. $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$
2. $A' = \begin{pmatrix} 1 \end{pmatrix}$
3. $B = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}$
4. $C = \begin{pmatrix} a & c & d & b \\ d & b & a & c \\ b & d & c & a \\ c & a & b & d \end{pmatrix}$

(The reason for the use of the Latin alphabet will become apparent.)

Note that B uses the symbols found in A but not A'.

SDP Construction

First, we construct the first q rows and columns (which is, in this case, 1) using A.

1	2	3	2	3	2	3	2	3
2								
3								
2								
3								
2								
3								
2								
3								

Notice that we take subsquare A' and place it in the top-left corner and then repeat whatever is in the other p columns (and rows) of A m times.

Then, we use the main diagonal of C (which is idempotent) to differentiate between the repeated elements.

1	$2a$	$3a$	$2b$	$3b$	$2c$	$3c$	$2d$	$3d$
$2a$								
$3a$								
$2b$								
$3b$								
$2c$								
$3c$								
$2d$								
$3d$								

We will translate the 2a's, 3a's... later.

Then, treating the remaining $pm \times pm$ squares as a $m \times m$ squares of size $p \times p$, we can continue to use C as such:.

1	$2a$	$3a$	$2b$	$3b$	$2c$	$3c$	$2d$	$3d$
$2a$	a	a	c	c	d	d	b	b
$3a$	a	a	c	c	d	d	b	b
$2b$	d	d	b	b	a	a	c	c
$3b$	d	d	b	b	a	a	c	c
$2c$	b	b	d	d	c	c	a	a
$3c$	b	b	d	d	c	c	a	a
$2d$	c	c	a	a	b	b	d	d
$3d$	c	c	a	a	b	b	d	d

Along the main left-to-right diagonal of the $m \times m$ square, we repeat whatever is left of the square of order $p + q$.

1	$2a$	$3a$	$2b$	$3b$	$2c$	$3c$	$2d$	$3d$
$2a$	$3a$	$1a$	c	c	d	d	b	b
$3a$	$1a$	$2a$	c	c	d	d	b	b
$2b$	d	d	$3b$	$1b$	a	a	c	c
$3b$	d	d	$1b$	$2b$	a	a	c	c
$2c$	b	b	d	d	$3c$	$1c$	a	a
$3c$	b	b	d	d	$1c$	$2c$	a	a
$2d$	c	c	a	a	b	b	$3d$	$1d$
$3d$	c	c	a	a	b	b	$1d$	$2d$

Then, we fill in the remaining $p \times p$ cells with array B and set $1a = 1b = 1c = 1d = 1$.

1	$2a$	$3a$	$2b$	$3b$	$2c$	$3c$	$2d$	$3d$
$2a$	$3a$	1	$2c$	$3c$	$2d$	$3d$	$2b$	$3b$
$3a$	1	$2a$	$3c$	$2c$	$3d$	$2d$	$3b$	$2b$
$2b$	$2d$	$3d$	$3b$	1	$2a$	$3a$	$2c$	$3c$
$3b$	$3d$	$2d$	1	$2b$	$3a$	$2a$	$3c$	$2c$
$2c$	$2b$	$3b$	$2d$	$3d$	$3c$	1	$2a$	$3a$
$3c$	$3b$	$2b$	$3d$	$2d$	1	$2c$	$3a$	$2a$
$2d$	$2c$	$3c$	$2a$	$3a$	$2b$	$3b$	$3d$	1
$3d$	$3c$	$2c$	$3a$	$2a$	$3b$	$2b$	1	$2d$

This is a Graeco-Latin square with the symbols $\{1, 2a, 3a, 2b, \ldots, 3d, \}$.

Finally, we rewrite $2a = 2$, $3a = 3$, $2b = 4$, $\ldots$, $3d = 9$, and we end up with:

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

The usefulness of this construction is reflected in the fact if we repeat the construction with Latin squares that are orthogonal to those listed in 'Ingredients', we get a Latin square that is orthogonal to the one above. Hence, the SDP allows us to construct larger Graeco-Latin squares from smaller ones. This idea is formalized in the following theorem.

Theorem 26. *Given an orthogonal pair of Latin squares of order $p + q$, with an orthogonal subsquare of order q; an orthogonal pair of order p, and an idempotent orthogonal pair of order m, a Graeco-Latin square of order $pm + q$ can be constructed using the SDP.*

Remark 27. *Since idempotent squares of order n exist if and only if there are three MOLS of order n, the SDP requires three MOLS of order m.*

Remark 28. *Via the SDP, we can construct Euler squares of order $4k + 2$, $n \geqslant 22$.*

There are certain restrictions on p, m, and q. We will go over this in the next section.

4.3.2. A Pair of MOLS of Order 22

In this section, we will disprove Euler's conjecture by creating a Graeco-Latin square of order $4k + 2$.

The 'Ingredients' Pt. 1

We have to first note the restrictions on p, m, and q.

1. p, m, $p + q$, $q \bmod 4 \neq 2$
   Since we need to have orthogonal mates of order p, m, $p + q$, and q, they must be constructible via other methods (e.g. Euler's methods).
2. $p \geqslant q$
   Obviously, we cannot have a Latin square of order $p + q$ with a subsquare of order q with $q > p$. In fact, we will see from this and point 5 that $p \neq 1$ (only applicable for constructing squares of order $4k + 2$).
3. $m > 3$
   Since the Latin square of order m needs to be idempotent, we need to have 3 MOLS of order m. Because the greatest number of MOLS of order n is $n - 1$, $m > 3$.

4. If $q \bmod 4 = 2$, then either $m \bmod 4 = 0$ or $p \bmod 2 = 0$ and $m \bmod 2 = 0$. Of course, $p \bmod 4 \neq 0$. (This is only applicable for constructing squares of order $4k + 2$.)
5. If $q \bmod 4 = 1$, then $p \bmod 4 = 3$ and $m \bmod 2 = 1$. (This is only applicable for constructing squares of order $4k + 2$.)
6. If $q \bmod 4 = 3$, then $p \bmod 4 = 1$ and $m \bmod 2 = 1$ (This is only applicable for constructing squares of order $4k + 2$.)
7. If $q \bmod 4 = 0$, then $p \bmod 4 \neq 2$. (This is only applicable for constructing squares of order $4k + 2$.)

Given these restrictions, $n \geqslant 3(4) + 1$, $n \geqslant 13$. So, we are only considering squares of order 14, 18, 22, and so on.

If $n = 14$, then $q = 1$ because $pm \geqslant 12$ and $q \neq 2$. However, this leaves $pm = 13$, which factors to 1×13. But neither p nor m can equal 1. (Generally, pm cannot be prime.) Therefore, we cannot construct $n = 14$.

If $n = 18$, then $q = 1, 3, 4$, or 5. If $q = 1$, then $pm = 17$, which is prime. Similarly, $q \neq 5$. If $q = 3$, then $pm = 15 = 3 \times 5$. (Factorization into 1×15 does not work.) In this case, we have $p = 3$, because $m > 3$. However, this violates point six above. Also, $q \neq 4$ because 14 factors into 2×7, and orthogonal latin squares of order two do not exist. Therefore, we cannot construct $n = 18$.

However, we *can* construct $n = 22 = 4(5) + 2$ using $p = 3, m = 7$, and $q = 1$.

The 'Ingredients' Pt. 2

In this section, we list A, B, and C necessary to construct a Latin square of order 22 using the SDP. These squares can all be obtained via other methods.

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$B = \begin{pmatrix} 2 & 3 & 4 \\ 3 & 4 & 2 \\ 4 & 2 & 3 \end{pmatrix}$$

$$C = \begin{pmatrix} a & e & b & f & c & g & d \\ e & b & f & c & g & d & a \\ b & f & c & g & d & a & e \\ f & c & g & d & a & e & b \\ c & g & d & a & e & b & f \\ g & d & a & e & b & f & c \\ d & a & e & b & f & c & g \end{pmatrix}$$

The 'Ingredients' Pt. 3

In this section, we list A, B, and C necessary to construct a Latin square of order 22 orthogonal to the previous Latin square of order 22 using the SDP. These squares can all be obtained via other methods. Note that these squares are also orthogonal to the counterparts above. Therefore, by the previous theorem, the resulting squares of order 22 will be orthogonal to each other.

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$B = \begin{pmatrix} 2 & 3 & 4 \\ 4 & 2 & 3 \\ 3 & 4 & 2 \end{pmatrix}$$

$$C = \begin{pmatrix} a & e & b & f & c & g & d \\ g & d & a & e & b & f & c \\ f & c & g & d & a & e & b \\ e & b & f & c & g & d & a \\ d & a & e & b & f & c & g \\ c & g & d & a & e & b & f \\ b & f & c & g & d & a & e \end{pmatrix}$$

The Pair of MOLS of Order 22

The steps and procedure will be too tedious and complex to work out here. However, the methodology is identical to the one for the square of order 9 given in the last section.

Readers are welcome to verify that they are indeed orthogonal.

$$\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 \\
2 & 1 & 4 & 3 & 14 & 15 & 16 & 5 & 6 & 7 & 17 & 18 & 19 & 8 & 9 & 10 & 20 & 21 & 22 & 11 & 12 & 13 \\
3 & 4 & 1 & 2 & 15 & 16 & 14 & 6 & 7 & 5 & 18 & 19 & 17 & 9 & 10 & 8 & 21 & 22 & 20 & 12 & 13 & 11 \\
4 & 3 & 2 & 1 & 16 & 14 & 15 & 7 & 5 & 6 & 19 & 17 & 18 & 10 & 8 & 9 & 22 & 20 & 21 & 13 & 11 & 12 \\
5 & 14 & 15 & 16 & 1 & 7 & 6 & 17 & 18 & 19 & 8 & 9 & 10 & 20 & 21 & 22 & 11 & 12 & 13 & 2 & 3 & 4 \\
6 & 15 & 16 & 14 & 7 & 1 & 5 & 18 & 19 & 17 & 9 & 10 & 8 & 21 & 22 & 20 & 12 & 13 & 11 & 3 & 4 & 2 \\
7 & 16 & 14 & 15 & 6 & 5 & 1 & 19 & 17 & 18 & 10 & 8 & 9 & 22 & 20 & 21 & 13 & 11 & 12 & 4 & 2 & 3 \\
8 & 5 & 6 & 7 & 17 & 18 & 19 & 1 & 10 & 9 & 20 & 21 & 22 & 11 & 12 & 13 & 2 & 3 & 4 & 14 & 15 & 16 \\
9 & 6 & 7 & 5 & 18 & 19 & 17 & 10 & 1 & 8 & 21 & 22 & 20 & 12 & 13 & 11 & 3 & 4 & 2 & 15 & 16 & 14 \\
10 & 7 & 5 & 6 & 19 & 17 & 18 & 9 & 8 & 1 & 22 & 20 & 21 & 13 & 11 & 12 & 4 & 2 & 3 & 16 & 14 & 15 \\
11 & 17 & 18 & 19 & 8 & 9 & 10 & 20 & 21 & 22 & 1 & 13 & 12 & 2 & 3 & 4 & 14 & 15 & 16 & 5 & 6 & 7 \\
12 & 18 & 19 & 17 & 9 & 10 & 8 & 21 & 22 & 20 & 13 & 1 & 11 & 3 & 4 & 2 & 15 & 16 & 14 & 6 & 7 & 5 \\
13 & 19 & 17 & 18 & 10 & 8 & 9 & 22 & 20 & 21 & 12 & 11 & 1 & 4 & 2 & 3 & 16 & 14 & 15 & 7 & 5 & 6 \\
14 & 8 & 9 & 10 & 20 & 21 & 22 & 11 & 12 & 13 & 2 & 3 & 4 & 1 & 16 & 15 & 5 & 6 & 7 & 17 & 18 & 19 \\
15 & 9 & 10 & 8 & 21 & 22 & 20 & 12 & 13 & 11 & 3 & 4 & 2 & 16 & 1 & 14 & 6 & 7 & 5 & 18 & 19 & 17 \\
16 & 10 & 8 & 9 & 22 & 20 & 21 & 13 & 11 & 12 & 4 & 2 & 3 & 15 & 14 & 1 & 7 & 5 & 6 & 19 & 17 & 18 \\
17 & 20 & 21 & 22 & 11 & 12 & 13 & 2 & 3 & 4 & 14 & 15 & 16 & 5 & 6 & 7 & 1 & 19 & 18 & 8 & 9 & 10 \\
18 & 21 & 22 & 20 & 12 & 13 & 11 & 3 & 4 & 2 & 15 & 16 & 14 & 6 & 7 & 5 & 19 & 1 & 17 & 9 & 10 & 8 \\
19 & 22 & 20 & 21 & 13 & 11 & 12 & 4 & 2 & 3 & 16 & 14 & 15 & 7 & 5 & 6 & 18 & 17 & 1 & 10 & 8 & 9 \\
20 & 11 & 12 & 13 & 2 & 3 & 4 & 14 & 15 & 16 & 5 & 6 & 7 & 17 & 18 & 19 & 8 & 9 & 10 & 1 & 22 & 21 \\
21 & 12 & 13 & 11 & 3 & 4 & 2 & 15 & 16 & 14 & 6 & 7 & 5 & 18 & 19 & 17 & 9 & 10 & 8 & 22 & 1 & 20 \\
22 & 13 & 11 & 12 & 4 & 2 & 3 & 16 & 14 & 15 & 7 & 5 & 6 & 19 & 17 & 18 & 10 & 8 & 9 & 21 & 20 & 1
\end{pmatrix}$$

$$\begin{pmatrix}
1 & 2 & 3 & 4 & 11 & 12 & 13 & 20 & 21 & 22 & 8 & 9 & 10 & 17 & 18 & 19 & 5 & 6 & 7 & 14 & 15 & 16 \\
3 & 4 & 1 & 2 & 14 & 15 & 16 & 5 & 6 & 7 & 17 & 18 & 19 & 8 & 9 & 10 & 20 & 21 & 22 & 11 & 12 & 13 \\
4 & 3 & 2 & 1 & 16 & 14 & 15 & 7 & 5 & 6 & 19 & 17 & 18 & 10 & 8 & 9 & 22 & 20 & 21 & 13 & 11 & 12 \\
2 & 1 & 4 & 3 & 15 & 16 & 14 & 6 & 7 & 5 & 18 & 19 & 17 & 9 & 10 & 8 & 21 & 22 & 20 & 12 & 13 & 11 \\
12 & 20 & 21 & 22 & 13 & 1 & 11 & 2 & 3 & 4 & 14 & 15 & 16 & 5 & 6 & 7 & 17 & 18 & 19 & 8 & 9 & 10 \\
13 & 22 & 20 & 21 & 12 & 11 & 1 & 4 & 2 & 3 & 16 & 14 & 15 & 7 & 5 & 6 & 19 & 17 & 18 & 10 & 8 & 9 \\
11 & 21 & 22 & 20 & 1 & 13 & 12 & 3 & 4 & 2 & 15 & 16 & 14 & 6 & 7 & 5 & 18 & 19 & 17 & 9 & 10 & 8 \\
21 & 17 & 18 & 19 & 8 & 9 & 10 & 22 & 1 & 20 & 11 & 12 & 13 & 2 & 3 & 4 & 14 & 15 & 16 & 5 & 6 & 7 \\
22 & 19 & 17 & 18 & 10 & 8 & 9 & 21 & 20 & 1 & 13 & 11 & 12 & 4 & 2 & 3 & 16 & 14 & 15 & 7 & 5 & 6 \\
20 & 18 & 19 & 17 & 9 & 10 & 8 & 1 & 22 & 21 & 12 & 13 & 11 & 3 & 4 & 2 & 15 & 16 & 14 & 6 & 7 & 5 \\
9 & 14 & 15 & 16 & 5 & 6 & 7 & 17 & 18 & 19 & 10 & 1 & 8 & 20 & 21 & 22 & 11 & 12 & 13 & 2 & 3 & 4 \\
10 & 16 & 14 & 15 & 7 & 5 & 6 & 19 & 17 & 18 & 9 & 8 & 1 & 22 & 20 & 21 & 13 & 11 & 12 & 4 & 2 & 3 \\
8 & 15 & 16 & 14 & 6 & 7 & 5 & 18 & 19 & 17 & 1 & 10 & 9 & 21 & 22 & 20 & 12 & 13 & 11 & 3 & 4 & 2 \\
18 & 11 & 12 & 13 & 2 & 3 & 4 & 14 & 15 & 16 & 5 & 6 & 7 & 19 & 1 & 17 & 8 & 9 & 10 & 20 & 21 & 22 \\
19 & 13 & 11 & 12 & 4 & 2 & 3 & 16 & 14 & 15 & 7 & 5 & 6 & 18 & 17 & 1 & 10 & 8 & 9 & 22 & 20 & 21 \\
17 & 12 & 13 & 11 & 3 & 4 & 2 & 15 & 16 & 14 & 6 & 7 & 5 & 1 & 19 & 18 & 9 & 10 & 8 & 21 & 22 & 20 \\
6 & 8 & 9 & 10 & 20 & 21 & 22 & 11 & 12 & 13 & 2 & 3 & 4 & 14 & 15 & 16 & 7 & 1 & 5 & 17 & 18 & 19 \\
7 & 10 & 8 & 9 & 22 & 20 & 21 & 13 & 11 & 12 & 4 & 2 & 3 & 16 & 14 & 15 & 6 & 5 & 1 & 19 & 17 & 18 \\
5 & 9 & 10 & 8 & 21 & 22 & 20 & 12 & 13 & 11 & 3 & 4 & 2 & 15 & 16 & 14 & 1 & 7 & 6 & 18 & 19 & 17 \\
15 & 5 & 6 & 7 & 17 & 18 & 19 & 8 & 9 & 10 & 20 & 21 & 22 & 11 & 12 & 13 & 2 & 3 & 4 & 16 & 1 & 14 \\
16 & 7 & 5 & 6 & 19 & 17 & 18 & 10 & 8 & 9 & 22 & 20 & 21 & 13 & 11 & 12 & 4 & 2 & 3 & 15 & 14 & 1 \\
14 & 6 & 7 & 5 & 18 & 19 & 17 & 9 & 10 & 8 & 21 & 22 & 20 & 12 & 13 & 11 & 3 & 4 & 2 & 1 & 16 & 15
\end{pmatrix}$$

5. Conclusions and Reflections

In the previous chapter, we have followed the paths that mathematicians has lain for us decades ago. Euler has provided the first construction method, while Sade has given us the most recent (along with Parker, Bose, and Shrikhande and their transversal designs).

To summarise their contributions: Euler has proven that Euler squares of odd order or of an order that is a multiple of four exists (He also proved the obvious non-existence of Euler squares of order 2), while Parker, Bose, and Shrikhande constructed Graeco-Latin squares of all orders, including those of form $4k + 2$, with the exception of $n = 2$ and $n = 6$. On the other hand, Tarry has shown that Graeco-Latin squares of order 6 are not possible.

Theorem 29. *Euler squares exist for every order n except when $n = 2$ or 6.*

But the research does not stop here. Recently, more elegant proofs have brought forward by Stinson, Dougherty, and Zhu Lie. Also, research in this area has taken on a greater scope. Mathematicians working in this field are now researching self-orthogonal Latin squares — squares that are orthogonal to its transpose. Some error-correcting codes in algebraic coding theory are also based on MOLS. Speaking of which, perhaps the most exciting developments come from finite projective planes, to which the following theorem will link MOLS.

Theorem 30. *A complete set of MOLS of order n implies a finite projective plane of order n.*

This had all started out as the simple riddle of 36 officers. After leading to developments in combinatorics, group theory, field theory, transversal design, and work done by many mathematicians around the globe, we finally begin to draw the close to this problem. Yet, the future of Latin squares is still vast to explore.

Where do we go from here? I list here a few open problems and conjectures yet to be solved.

1. **Problem 1.** How many MOLS of order 10 are there? (We already know that there are more than three but less than seven MOLS of order 10.)
2. **Conjecture 2.** (Ryser's conjecture) Any Latin square of odd order has a transversal.

3. **Conjecture 3.** (Brualdi's conjecture) Any Latin square of order n has a partial transversal of size at least $n - 1$.

By this we hope to have achieved the purpose of this report: to bring about a basic understanding of this particular area of research and to describe its vibrant history and mathematical developments throughout the centuries.

As for me, this project has led me to discover many mathematical tools and techniques. It has sparked my interests in this area, particularly in group theory.

Finally, it is time to give thanks to all those who have supported me throughout the course of this project, notably my advisor Jonathon Hamilton and my parents, and to bid our reader farewell.

Appendix A. A Group-Theoretic Attempt

A.1. Group Theory 101

Group theory is the cornerstone of the abstraction mathematics was going through in the 19^{th} and 20^{th} centuries. In its purest sense, group theory is the study of algebraic structures called groups and their properties.

A group $(G, \circ)$ satisfies four basic axioms:

Axiom 31 (Closure)**.** *For any $a \in G$ and $b \in G$, $a \circ b \in G$.*

Axiom 32 (Identity)**.** *For all $a \in G$, there exists a element $e \in G$, such that $a \circ e = a$ and $e \circ a = a$.*

Axiom 33 (Inverse)**.** *Given $a \in G$, there exists a unique $a^{-1} \in G$, such that $a \circ a^{-1} = e$ and $a^{-1} \circ a = e$.*

Axiom 34 (Associativity)**.** *For any $a, b, c \in G$, $a \circ (b \circ c) = (a \circ b) \circ c$.*

From these axioms, it is possible to deduce some general theorems in group theory.

Theorem 35 (Left Cancellation Law)**.** *If for some $a, b, c \in G$, $a \circ b = a \circ c$, then $b = c$.*

Proof of the Left Cancellation Law.

$$a \circ b = a \circ c \tag{15}$$

$$a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c) \tag{16}$$
$$(a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c \tag{17}$$
$$e \circ b = e \circ c \tag{18}$$
$$b = c \tag{19}$$

In (A.2), we multiplied both sides of the equation by a^{-1}, which we know exists because of the inverse axiom.

In (A.3), we used the associativity axiom.

In (A.4), we used the inverse axiom to arrive at the identity element.

In (A.5), we simplified the expression using the identity axiom. □

Since groups are not generally commutative, i.e. $a \circ b \neq b \circ a$, we have to prove the right cancellation law separately. The methodology is identical with some change in notation, so we omit it.

Theorem 36 (Right Cancellation Law)**.** *If for some $a, b, c \in G$, $b \circ a = c \circ a$, then $b = c$.*

Before moving on, the pigeonhole principle should also be stated because it will be used.

Theorem 37 (The Pigeonhole Principle)**.** *There does not exist an injective function on finite sets whose codomain is smaller than its domain.*

A.2. Some Theorems

Below are some results I proved using elementary group theory.

Definition 38. *A* quasigroup $(Q, \circ)$ *is a groupoid that satisfies closure and for any $a, b \in Q$, there exists unique $c, d \in Q$ such that $a \circ c = b$ and $d \circ a = b$.*

Definition 39. *A* Cayley table *is the multiplication table of a group or groupoid.*

Theorem 40. *The Cayley table of a quasigroup is a Latin square.*

Proof. For the Cayley table to be a Latin square, each column and row must contain every element once and only once.

Now, suppose that such a table contains a column a where b appears twice, i.e. $a \circ c = b$ and $a \circ d = b$. By the definition of quasigroups above, $c = d$. However, in the construction of the table, it is assumed that $c \neq d$.

Similarly, there is no element that can occurs twice in the same column.

Since each of the n elements can appear at most once in each of the n rows and columns, then by the pigeonhole principle, each element must occur exactly once in each row and column. □

Definition 41. *A* transversal *of a Latin square of order n is a set of n cells, one in each row, one in each column, such that no two cells contain the same symbol. (cf.* ***Reviewer's Comment*** *10)*

Theorem 42. *If a Latin square of order n which is the multiplication table of a group and possesses at least one transversal, then it has a decomposition into n disjoint transversals.*

Proof. Let $(G, \circ)$ be the group that produces the Latin square L . Construct a transversal T_1 in L by selecting symbol a_1 in the first row, a_2 in the second row, ..., and a_n in the n^{th} row.

Another set T_2 can be constructed by selecting elements $a_i \circ b$ from each of the n rows, where b is an element of the group. By closure and the cancellation law, $a_i \circ b$ will each take on a different symbol. Thus, T_2 is a transversal.

One more condition that needs to be proven is that $a_i \circ b$ are all in different columns. Suppose a_i is in the i^{th} row and $\mathbf{P}(i)^{\text{th}}$ column, i.e. $a_i = (b_i, b_{\mathbf{P}(i)})$, where $\mathbf{P}(x)$ is a permutation. As the two symbols were originally in different columns, $\mathbf{P}(i) \neq \mathbf{P}(j)$, on condition that $i \neq j$. Then, $a_i \circ b = (b_i, b_{\mathbf{P}(i)}) \circ b = (b_i, b_{\mathbf{P'}(i)}$ where $\mathbf{P'}(x)$ is another permutation. Therefore, $\mathbf{P'}(i) \neq \mathbf{P'}(j)$ if $i \neq j$.

Taking T_2, T_3 can be constructed, until T_n, after which $a_i \circ b^n$ cycles back to T_1. □

Note that the converse is not true.

Theorem 43. *If a Latin square has n disjoint transversals, we can create its orthogonal mate by assigning each of the n transversal an element of the*

orthogonal mate. (cf. ***Reviewer's Comment*** *11)*

Conclusion 44. *A given Latin square possesses an orthogonal mate if it has a transversal.*

This is a clear conclusion from the above theorems and the definition of orthogonality.

1. Here is an example from the Klein four-group. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}$
2. Here is a transversal. $\begin{pmatrix} \mathbf{1} & 2 & 3 & 4 \\ 2 & 1 & \mathbf{4} & 3 \\ 3 & 4 & 1 & \mathbf{2} \\ 4 & \mathbf{3} & 2 & 1 \end{pmatrix}$
3. Therefore, we may conclude that this Latin square can be completed to form a Graeco-Latin square, because there is a transversal.
4. Here is the completed Euler square. $\begin{pmatrix} (1,1) & (2,2) & (3,3) & (4,4) \\ (2,3) & (1,4) & (4,1) & (3,2) \\ (3,4) & (4,3) & (1,2) & (2,1) \\ (4,2) & (3,1) & (2,4) & (1,3) \end{pmatrix}$

Appendix B. More on MOLS and other Topics

As we have already mentioned, MOLS have been very important in experimental design and the theory of finite projective planes. Therefore, we will provide a list of useful theorems in this field that have not been discussed.

Theorem 45. *Suppose that there exist r MOLS of order n and r MOLS of order m, then there exist r MOLS of order mn.*

Theorem 46. *If a Latin square of order $4k+2$ contains a Latin subsquare of order $2k+1$, then it has no orthogonal mate.*

Theorem 47. *A Latin square of order mq and of q-step type has no transversals if m is even and q is odd.*

Theorem 48. *There exist unipotent symmetric Latin squares of order n for every even integer n, but none exists if n is any odd order greater than 1.*

Theorem 49. *An $(n, q^2, n-1)$ q-ary code is equivalent to a set of $n-2$ MOLS of order q.*

Theorem 50. *k-MOLS of order n is equivalent to $k+2$-net of order n.*

Proofs of these theorems require group theory, general field theory, and algebraic coding theory.

Appendix C. Regarding the Use of Computer-Aided Proof

In recent years, proofs involving computers, e.g. the proof of the Four Colour Theorem, have spurred on some controversy. Do they qualify as proof? And how are they different from the exhaustive enumeration by hand (like as done by Tarry)?

In Parker, Bose, and Shrikhande's work, the actual construction relied somewhat on computers. But fortunately, this is a proof of existence (indeed, by finding a counterexample to Euler's conjecture), and therefore is not hampered by this philosophical debate on the nature of mathematical proof. Given a counterexample, humans can always check that it does refute the conjecture.

Even proofs of non-existence of Graeco-Latin squares of order 2 and 6 have been found in elegant ways without resorting to brute force attack.

Therefore, Graeco-Latin squares are free (for now) of the plague of computer aided proof.

(Computers were used minimally in this project, in order to facilitate the construction of some of the Euler squares.)

REFERENCES

[1] Andersen, Lars D., *Chapter on the History of Latin Squares*. Ed. Robin J. Wilson. Department of Mathematical Sciences, Aalborg University. 11 Apr. 2008 [http://www.math.aau.dk/research/reports/R-2007-32.pdf].

[2] Cameron, Peter J. "Encyclopedia of Design Theory: Latin Squares." *Encyclopedia of Design Theory*. 5 July 2006. Queen Mary, University of London. 11 Apr. 2008 ⟨http://designtheory.org/library/encyc/latinsq/m/⟩.

[3] Cherowitzo, Bill. Reading. University of Colorado, Denver. 11 Apr. 2008 [http://www-math.cudenver.edu/ wcherowi/courses/m6406/].

[4] Dougherty, S. T. "A Coding Theoretic Solution to the 36 Officer Problem." *Designs, Codes, and Cryptography* (1994). 11 Apr. 2008 [http://academic.scranton.edu/faculty/doughertys1/euler.tex].

[5] Euler, Leonhard. "Recherches sur une nouvelle espéce de quarrès magiques." Verhandelingen Uitgegeven Door Het Zeeuwsch Genootschap Der Wetenschappen Te Vlissingen 9 (1782): 85-239. *The Euler Archive*. Hong Kong. 11 Apr. 2008.

[6] Hedayat, A., and W. T. Federer. *Annals of Mathematical Statistics* 42.2 (1971): 509-516. *Project Euclid*. 11 Apr. 2008.
[7] Klyve, Dominic, and Lee Stemkoski. *Graeco-Latin Squares and a Mistaken Conjecture of Euler*. Eötvös Loránd Tudományegyetem. 11 Apr. 2008 [http://compalg.inf.elte.hu/ tony/Kutatas/PerfectArrays/ GraecoLatinSquares.pdf].
[8] Mann, Henry B. "On Orthogonal Latin Squares." *Bulletin of the American Mathematical Society* 50 (1950): 249-257. *Project Euclid*. Hong Kong. 11 Apr. 2008.
[9] Mann, Henry B. "On the Construction of Sets of Orthogonal Latin Squares." *Annals of Mathematical Statistics* 14.4 (1943): 401-414. *Project Euclid*. Hong Kong. 11 Apr. 2008.
[10] Mann, Henry B. "The Construction of Orthogonal Latin Squares." *Annals of Mathematical Statistics* 13 (1942): 418-423. *Project Euclid*. Hong Kong.

Reviewer's Comments

1. In the statement of Definition 3, the meaning of the word "orthogonal" is not specified. After the review, the author then quotes

   Theorem 51. *A Latin square of order n can have at most $n-1$ Latin squares that are both orthogonal to it and to each other.*

2. In the statement the reference theorem is not clearly stated. What is the meaning of "a Latin square of order n *can have* at most $n-1$ MOLS"? Reviewer suggests the author may mean "there are at most $n-1$ MOLS of order n".

3. In the statement of Theorem 11, the word "maximum" was missing.

4. On page 7, in the last sentence of the proof of Corollary 14, reviewer asks how Euler conjecture follows.

5. On page 7, in the statement of Condition 16, the meaning of the word "complete" is not specified.

6. On page 9, line 3, what is the meaning of the symbol α? Reviewer doubts if it is a Latin square according to **Definition 17**. Furthermore, what is the meaning of a^{α}?

7. On page 10, line 2, the meaning of the word "completed" is not clear. One can perhaps guess what the term means, but a clear definition is helpful. It seems not clear how the "single-step property" of the Latin square is involved here.

8. On page 12, last paragraph, line 1, the meaning of the word "idempotent" is not specified.

9. On page 13, the statement of Definition 25 is then deleted by the author.

10. On page 21, the statement of Definition 41 is then deleted by the author.

11. In the statement of Theorem 43, the meaning of "orthogonal mate" of a Latin square is not specified.