# LATIN SQUARES AND THEIR APPLICATIONS TO CRYPTOGRAPHY

by

Nathan O. Schmidt

A thesis
submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Mathematics
Boise State University

December 2016

BOISE STATE UNIVERSITY GRADUATE COLLEGE

## DEFENSE COMMITTEE AND FINAL READING APPROVALS

of the thesis submitted by

Nathan O. Schmidt

Thesis Title: Latin Squares and Their Applications to Cryptography

Date of Final Oral Examination: 28 October 2016

The following individuals read and discussed the thesis submitted by student Nathan O. Schmidt, and they evaluated his presentation and response to questions during the final oral examination. They found that the student passed the final oral examination.

| | |
|---|---|
| Liljana Babinkostova, Ph.D. | Chair, Supervisory Committee |
| Samuel Coskey, Ph.D. | Member, Supervisory Committee |
| Marion Scheepers, Ph.D. | Member, Supervisory Committee |
| Jyh-Haw Yeh, Ph.D. | Member, Supervisory Committee |

The final reading approval of the thesis was granted by Liljana Babinkostova, Ph.D., Chair, Supervisory Committee. The thesis was approved by the Graduate College.

I dedicate this work to my family, and especially to my Marissa!

# ACKNOWLEDGMENTS

A special thanks to my adviser Dr. Liljana Babinkostova for her invaluable knowledge, insight, and guidance on this great subject. I am honored to have worked under her advisement and have learned much.

Thanks to Will Unger for helping to design and implement the software for generating latin squares and counting their transversals. Our joint research operations primarily consisted of eating pizza, drinking coffee, programming computers, and solving math problems, which led us to consider super-symmetric latin squares and Conjecture 2.100. Good times.

Thanks to Dr. Samuel Coskey, Dr. Marion Scheepers, and Dr. Jyh-Haw Yeh for their helpful comments that improved the thesis.

Thanks to Sam Dworetzky for his collaboration during the "Square Bandits" project.

Thanks to Dr. Ian Wanless for answering my questions on latin square transversals.

And last, but surely not least, thanks to my wife Marissa, for everything.

# AUTOBIOGRAPHICAL SKETCH

Nathan Schmidt was born and raised in Kenai, Alaska. He has always enjoyed doing activities with family and friends, such as fishing, hunting, snowboarding, and competitive athletics. His upbringing led him to develop a strong appreciation of the significance of family, the mathematical sciences, hard work, and the great outdoors. Through discipline, perseverance, and creativity, he firmly believes that the tools of science and mathematics can be used to build a successful future.

The first computer that Nathan used was his family's Apple Macintosh 128K. In those early days, one of his favorite things to do on the computer was to draw black-and-white pictures using MacDraw. At age 13 he began to teach himself the basics of HTML, computers, networking, the Internet, and cyber security. At age 15 his friend handed him the Red Hat 7 Linux install disk during biology class and he has been addicted to Linux ever since.

In 2004 Nathan graduated high school after being recognized as Science Student of the Year, an All-State Football Player, and the new record holder in the 200-meter dash. Thereafter, he attended Eastern Oregon University. While doing research in robotics and artificial intelligence, he tutored in computer programming, helped maintain the Linux lab, and sprinted for the track and field team. He was on the school-record breaking 4x100-meter dash relay team that provisionally qualified for the USA NAIA Championships. In 2008 he earned a B.S. in computer science and a minor in mathematics.

Thereafter, Nathan pursued a M.S. in computer science at Boise State University to study bioinformatics and artificial intelligence. He worked as a research assistant on the DNA Safeguard Project and as a teaching assistant. Since then he has also published research work in disciplines such as quantum gravity and sustainable energy. He has also worked various jobs as a computer technician, computer programmer, construction laborer, teacher, and commercial fisherman. In 2014 he married his beloved wife Marissa. Thereafter, he pursued a M.S. in mathematics to study cryptography and cyber security, while researching and teaching at Boise State.

Today Nathan continues to program computers, solve math problems, research, teach, and train in Jeet Kune Do and Kali in Idaho while commercial fishing in Alaska. He continues to be firm believer in the methods of science and mathematics, the power of creativity, freedom of speech, privacy, and self-defense.

# ABSTRACT

A *latin square* of order-$n$ is an $n \times n$ array over a set of $n$ symbols such that every symbol appears exactly once in each row and exactly once in each column. Latin squares encode features of algebraic structures. When an algebraic structure passes certain "latin square tests", it is a candidate for use in the construction of cryptographic systems. A *transversal* of a latin square is a list of $n$ distinct symbols, one from each row and each column. The question regarding the existence of transversals in latin squares that encode the Cayley tables of finite groups is far from being resolved and is an area of active investigation. It is known that counting the pairs of permutations over a Galois field $\mathbb{F}_{p^d}$ whose point-wise sum is also a permutation is equivalent to counting the transversals of a latin square that encodes the addition group of $\mathbb{F}_{p^d}$. We survey some recent results and conjectures pertaining to latin squares and transversals. We create software tools that generate latin squares and count their transversals. We confirm previous results that cyclic latin squares of prime order-$p$ possess the *maximum* transversal counts for $3 \leq p \leq 9$. Furthermore, we create a new algorithm that uses these prime order-$p$ cyclic latin squares as "building blocks" to construct *super-symmetric* latin squares of prime power order-$p^d$ with $d > 0$; using this algorithm we accurately predict that super-symmetric latin squares of order-$p^d$ possess the confirmed maximum transversal counts for $3 \leq p^d \leq 9$ and the estimated lower bound on the maximum transversal counts for $9 < p^d \leq 17$. Also, we give some conjectures regarding the number of transversals in a super-symmetric latin square. Lastly, we use the super-symmetric latin square for the additive group of the Galois field $(\mathbb{F}_{3^2}, +)$ to create a simplified version of Grøstl, an iterated hash function, where the compression function is built from two fixed, large, distinct permutations.

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

# CHAPTER 1

# INTRODUCTION

**Definition 1.1.** A *latin square* $L$ of order-$n$ is an $n \times n$ array of symbols in which each symbol occurs exactly once in each row and once in each column. We let $\mathcal{L}^n$ denote the *set of all order-n latin squares.* We let $|\mathcal{L}^n|$ denote the *total number of all order-n latin squares.*

**Table 1.1: An example of an order-3 latin square with symbols from the set $\mathbb{Z}_3 = \{0, 1, 2\}$ of integers modulo 3 [left] and an example of an order-4 latin square with symbols from the set $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ of integers modulo 4 [right].**

| | | |
|---|---|---|
| 0 | 1 | 2 |
| 1 | 2 | 0 |
| 2 | 0 | 1 |

| | | | |
|---|---|---|---|
| 0 | 1 | 2 | 3 |
| 3 | 2 | 1 | 0 |
| 2 | 0 | 3 | 1 |
| 1 | 3 | 0 | 2 |

**Definition 1.2.** A *magic square* $M$ of order-$n$ is an $n \times n$ array of integers from the set $\{0, 1, 2, \ldots, n^2 - 1\}$, where the integers in each row, in each column, in the main diagonal, and in the main anti-diagonal all add up to the same number called the *magic constant.*

Latin squares (and their close relatives magic squares) have been studied by mathematicians since ancient times. The origin of the latin square is not known for certain. The name “latin square” was inspired by some work conducted by Euler in the late 18th century, who used Latin characters as the symbols [9, 10, 11]. The latin square concept might have originated with problems concerning the motion and placement of pieces on a chessboard; see Example 1.3. It might also have originated from problems concerning the placement of denominations and suits in a deck of playing cards which are arranged in specific $4 \times 4$ arrays; see Example 1.5. To the best of our knowledge, the earliest *written reference* (that has survived history) includes the solutions to the card problem, which was published in 1723; we recommend [12, 13] for additional information. Furthermore, there is evidence indicating that magic squares were also known to mathematicians in much earlier times. For example, magic squares were known by ancient cultures located in places such as China, India, the Middle East, and Europe [14, 15, 16].

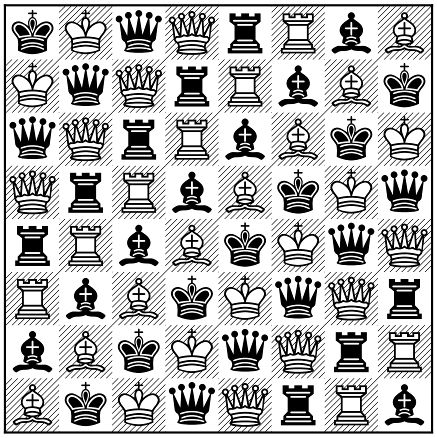
**Table 1.2: An example of an order-3 magic square with symbols from the set $\mathbb{Z}_9$ of integers modulo 9 and the magic constant $12$ [left] and an example of an order-4 magic square with symbols from the set $\mathbb{Z}_{16}$ of integers modulo $16$ with the magic constant 30 [right].**

| | | |
|---|---|---|
| 3 | 8 | 1 |
| 2 | 4 | 6 |
| 7 | 0 | 5 |

| | | | |
|---|---|---|---|
| 6 | 11 | 0 | 13 |
| 1 | 12 | 7 | 10 |
| 15 | 2 | 9 | 4 |
| 8 | 5 | 14 | 3 |

**Example 1.3.** Consider the following old chessboard problem [17]: *Given eight kings, eight queens, eight rooks, and eight bishops in black and white, place the (64 total) game pieces on an* $8 \times 8$ *chessboard so that each of the eight distinct pieces appears only once in each row and each column.* See Figure 1.1 for a latin square example solution.

**Figure 1.1: An example solution to the $8 \times 8$ latin square chessboard problem of Example 1.3.**



Euler is credited for initiating the systematic development of latin squares and “graeco-latin squares” [9, 10, 11].

**Definition 1.4.** Let $\mathcal{A}$ and $\mathcal{B}$ be sets of $n$ symbols. A *graeco-latin square* (or *Euler square*) of order-$n$ is an $n \times n$ array of ordered pairs of the form $(a, b)$ where $a \in \mathcal{A}$ and $b \in \mathcal{B}$, such that every row and every column contains each element of $\mathcal{A}$ and each element of $\mathcal{B}$ exactly once, where each ordered pair appears exactly once in the array.

**Example 1.5.** Consider the old card problem [18]: *given a deck of playing cards, arrange the 16 face cards in a* $4 \times 4$ *array so that each denomination symbol in the set* $\mathcal{A} = \{A, K, Q, J\}$ *and each suit symbol in the set* $\mathcal{B} = \{♣, ♥, ♦, ♠\}$ *appears only once in each row and each column.* See Figure 1.2 for an example solution with latin squares.

Not all pairs of latin squares can be super-imposed to construct a graeco-latin square; for this, the pair of latin squares must have the following property:

**Figure 1.2: An example solution to the old playing card problem of Example 1.5 with a denomination latin square, a suit latin square, and a super-imposed suit-denomination graeco-latin square.**

| | | | |
|---|---|---|---|
| ♠ | ♥ | ♦ | ♣ |
| ♦ | ♣ | ♠ | ♥ |
| ♣ | ♦ | ♥ | ♠ |
| ♥ | ♠ | ♣ | ♦ |

**Latin Square of Suits**

| | | | |
|---|---|---|---|
| A | K | Q | J |
| J | Q | K | A |
| K | A | J | Q |
| Q | J | A | K |

**Latin Square of Denominations**

| | | | |
|---|---|---|---|
| ♠A | ♥K | ♦Q | ♣J |
| ♦J | ♣Q | ♠K | ♥A |
| ♣K | ♦A | ♥J | ♠Q |
| ♥Q | ♠J | ♣A | ♦K |

**Graeco-Latin Square of Suits-Denominations**

**Definition 1.6.** Let $\mathcal{A}$ and $\mathcal{B}$ be sets of $n$ symbols with $n \geq 2$. Let $L^{\mathcal{A}}, L^{\mathcal{B}} \in \mathcal{L}^n$ denote order-$n$ latin squares with symbols from $\mathcal{A}$ and $\mathcal{B}$, respectively. Let $\otimes$ be the *super-imposition* operation, where $L^{\mathcal{A}} \otimes L^{\mathcal{B}}$ is the super-imposition of $L^{\mathcal{A}}$ and $L^{\mathcal{B}}$; $L^{\mathcal{A}} \otimes L^{\mathcal{B}}$ is an $n \times n$ array of ordered pairs. Then $L^{\mathcal{A}}$ and $L^{\mathcal{B}}$ are said to be *orthogonal* if $L^{\mathcal{A}} \otimes L^{\mathcal{B}}$ is a graeco-latin square.

Thus, in the playing card puzzle solution of Figure 1.2 we observe that the "suit latin square" and the "denomination latin square" are in fact a pair of orthogonal latin squares because they satisfy Definition 1.6 and can therefore be super-imposed to construct a graeco-latin square of Definition 1.4. Figure 1.2 is a classic illustration of a historical connection between orthogonal latin squares, graeco-latin squares, and puzzle games. However, in [9, 10, 11] Euler goes beyond such games by applying the concept of orthogonal latin squares to develop new approaches for constructing graeco-latin squares (including the specific case of magic squares). For instance, he proposed the Thirty-Six Officers problem (a practical application of order-6 graeco-latin squares) and investigated general rules for constructing such graeco-latin squares with even and odd orders [9, 10, 11]. In [11] Euler conjectured that: *orthogonal latin squares of order-$n$ exist if and only if $n \not\equiv 2 \mod 4$.* Thereafter, in [19] Bose, Shrikhande, and Parker famously disproved this conjecture by instead proving the following result:

**Theorem 1.7.** *There is a pair of orthogonal latin squares of order-$n$ if and only if $n \neq \{2, 6\}$.*

Although not all of Euler's conjectures were correct, his inquiries and work eventually led to important future developments in fields such as combinatorics, algebra, and number theory.

A *Cayley table* [20, 21, 22] encodes the structure of a finite group by rearranging all the possible products of the group's elements in a square table that is similar to the addition tables and multiplication tables that many young students learn about in elementary school. Cayley was aware of Euler's work [9, 10, 11], and while he was examining such groups [20, 21, 22] he discovered that the *unbordered* Cayley table of an order-$n$ group is actually an order-$n$ latin square, where each row (or column) of the latin square encodes a permutation of the group's elements.

**Definition 1.8.** Let $\mathcal{G} = (\mathcal{G}, +)$ be a finite group of order-$n$ and let $L$ be a latin square of order-$n$. If $L$ encodes the unbordered Cayley table of $(\mathcal{G}, +)$, then we write $L = L^{(\mathcal{G},+)}$ (or equivalently $L = L^{\mathcal{G}}$) and say that $L^{(\mathcal{G},+)}$ *encodes* $(\mathcal{G}, +)$.

As a result of Cayley's discoveries, the subject of latin squares began to attract the serious attention of mathematicians. The cause of this serious interest was the

**Table 1.3: Let $(\mathbb{Z}_5, +)$ be the finite group over the set $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ of integers modulo 5 under addition. Then the Cayley table of $(\mathbb{Z}_5, +)$ [left] and the corresponding order-5 latin square $L^{(\mathbb{Z}_5,+)}$ [right] can be written as such.**

| + | **0** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|---|
| **0** | 0 | 1 | 2 | 3 | 4 |
| **1** | 1 | 2 | 3 | 4 | 0 |
| **2** | 2 | 3 | 4 | 0 | 1 |
| **3** | 3 | 4 | 0 | 1 | 2 |
| **4** | 4 | 0 | 1 | 2 | 3 |

**Cayley Table of $(\mathbb{Z}_5, +)$**

| | | | | |
|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 |
| 1 | 2 | 3 | 4 | 0 |
| 2 | 3 | 4 | 0 | 1 |
| 3 | 4 | 0 | 1 | 2 |
| 4 | 0 | 1 | 2 | 3 |

**Latin Square of $(\mathbb{Z}_5, +) : L^{(\mathbb{Z}_5,+)}$**

realization that latin squares were not just applicable to certain puzzle games, but that latin squares were fundamentally relevant to fields such as combinatorics and algebra. Schröder made additional latin square developments, where he wrote a series of papers on formal algebra and logic, which he termed “formal arithmetics” [12, 23]. Schröder focused heavily on the development of algebraic systems with a generalized identity element and a binary operation such that both the left and right inverse operations could be uniquely defined [12, 23]. In fact, these algebraic systems that Schröder had discovered are what we refer to today as *quasi-groups*, which are a generalization of groups that satisfy the *latin square property*. Evidently, much of Schröder’s work was “forgotten” but was rediscovered some decades later; a list of Schröder’s papers and a discussion of his significant accomplishments is exemplified in Ibragimov’s historical review [23]. This rediscovery of Schröder’s work was initiated when mathematicians began to generalize group theory to quasi-group theory [12]. For example, a major result of this generalization was achieved by Moufang in [24], where she established a fundamental connection between non-associative quasi-groups and non-desarguesian projective planes.

The combined results of groups and quasi-groups discovered by Euler [9, 10, 11], Cayley [20, 21], Schröder [23], and Moufang [24] built a "latin square bridge" between the fields of combinatorics and algebra; it then became possible to simultaneously view latin squares from both combinatoric and algebraic standpoints. For the reader who is interested in a stronger discussion of such relationships, we recommend the literature of Dénes and Keedwell [12], Dénes [25], Dénes and Pásztor [26], Barra [27], Guérin [28], Fog [29], Schönhardt [30], and Wielandt and Huppert [31]. Such achievements have built the foundation for a legion of historical and modern applications throughout the 20th and 21st centuries. Some examples of modern applications of latin squares are in experimental design in statistics [32], programming language compiler testing [33], and telecommunications [34].

It turns out that quasi-groups and groups play a big role in *information security*, which is the discipline and practice of defending information from unauthorized access, usage, modification, disruption, or destruction. *Cyber security* (or *computer security*) is information security for computing systems and the data in which they store, transceive, and/or access. An imperative component of both information and computer security is *cryptology*, which includes:

- *Cryptography*: the science of making codes for secure communication in the presence of adversaries.

- *Cryptanalysis*: the science of breaking codes by hunting for weaknesses that would enable adversaries to circumvent "secure" communication without necessarily knowing the secret key(s).

Thus, cryptology plays an extensive role in the protection of information and data that is either in transit or in storage. Hence, in order to maintain and increase the privacy, integrity, and protection of such information and computing systems against adversaries in an era of rapidly advancing technology with cyber warfare [35, 36, 37] and numerous cyber security threats [38, 39, 40, 41, 42, 43], the theory and practice of cryptology must be thoroughly researched and developed via the scientific method and the mathematical method.

Since the development of electro-mechanical rotor machines during World War I (ex. the Enigma machines [44, 45, 46]) and the development of programmable, electronic, digital computers during World War II (ex. the Colossus computers [47, 48]), the methods of cryptography have become increasingly complex with a rapidly expanding application domain. Modern cryptography is based heavily on the disciplines of mathematics, computer science, and electrical engineering. The design of a cryptographic algorithm is based on assumptions of computational hardness, where the primary objective is to make such algorithmically-based systems computationally infeasible for an attacker to break in practice. Thus, although it is theoretically feasible to break such a cryptographic system, it must be practically infeasible to do so in any known workable situation or context; in this case, the system is considered to be *computationally secure*.

The computational security of a cryptographic system depends greatly on the underlying algebraic structures and operations that are used to build its algorithm and implementation. Finite groups and Galois fields [49, 50, 51] are fundamental algebraic structures that are used to construct cryptographic systems. Therefore, in order to assess the degree of protection, strength, and reliability that such a system offers, it is crucial to rigorously evaluate the underlying finite groups and Galois fields via the scientific method and the mathematical method.

Thus, given that the structure of any finite group is encoded with a Cayley table (and a corresponding latin square), and given that the structure of a Galois field (a specific type of finite ring equipped with two binary operations) is encoded with two Cayley tables (and two corresponding latin squares), then many key properties of a given finite group or Galois field can be obtained by evaluating its representative latin square(s). This implies that latin squares are elemental to cyber security because they can be directly utilized to evaluate the computational security of cryptographic systems.

**Example 1.9.** Galois fields of prime power order-$2^d$ are important algebraic structures for constructing cryptographic systems for digital computers with a binary numeral system. Here we give an example of how to construct such a Galois field $\mathbb{F}_{2^2} \cong \mathbb{F}_{2^2}[x]$, whose addition group $(\mathbb{F}_{2^2}, +) \cong (\mathbb{F}_{2^2}[x], +)$ is encoded by an order-4 latin square $L^{(\mathbb{F}_{2^2},+)} \in \mathcal{L}^4$. First, let $\mathbb{Z}_2 = (\mathbb{Z}_2, +) = \{0, 1\}$ be the group of integers with addition modulo 2. Then the Cayley table of $(\mathbb{Z}_2, +)$ and the corresponding order-2 latin square $L^{(\mathbb{Z}_2,+)}$ can be respectively written as

| $+$ | **0** | **1** |
|---|---|---|
| **0** | 0 | 1 |
| **1** | 1 | 0 |

**Cayley Table of** $(\mathbb{Z}_2, +)$

and

| | |
|---|---|
| 0 | 1 |
| 1 | 0 |

.

$L^{(\mathbb{Z}_2,+)}$

Now let $\mathbb{Z}_2[x]$ be the set of polynomials with coefficients from $\mathbb{Z}_2$. Next, we choose a polynomial $P(x) \in \mathbb{Z}_2[x]$ of degree 2 with coefficients $p_0, p_1, p_2 \in \mathbb{Z}_2$ given by the binary string

$$P(x) = p_2 x^2 + p_1 x + p_0 = 1 \bullet x^2 + 0 \bullet x + 1 = 101 \in \mathbb{Z}_2[x],$$

where $p_2 = 1, p_1 = 0, p_0 = 1 \in \mathbb{Z}_2$, such that $P(x)$ is irreducible in $\mathbb{Z}_2[x]$. Then we obtain the Galois field $\mathbb{F}_{2^2}[x] = \mathbb{Z}_2[x]/\langle P(x)\rangle$ where the 4 distinct polynomial elements of $\mathbb{F}_{2^2}[x]$ are encoded as the binary strings

$$\begin{array}{lclcl@{\qquad}lclcl} a_0(x) & = & 0 & = & 00 \in \mathbb{F}_{2^2}[x] & a_2(x) & = & x & = & 10 \in \mathbb{F}_{2^2}[x] \\ a_1(x) & = & 1 & = & 01 \in \mathbb{F}_{2^2}[x] & a_3(x) & = & x+1 & = & 11 \in \mathbb{F}_{2^2}[x]. \end{array} \tag{1.1}$$

Moreover, we can input $x = 2$ into the above equations to obtain the equivalent enumeration

$$\begin{array}{lclcl@{\qquad}lclcl} a_0(2) & = & 0 & = & 00 \in \mathbb{F}_{2^2} & a_2(2) & = & 2 & = & 10 \in \mathbb{F}_{2^2} \\ a_1(2) & = & 1 & = & 01 \in \mathbb{F}_{2^2} & a_3(2) & = & 3 & = & 11 \in \mathbb{F}_{2^2}. \end{array} \tag{1.2}$$

Therefore, we can write the addition Cayley table of $(\mathbb{F}_{2^2}[x], +)$ in the equivalent polynomial and integer representations

| $+$ | $\mathbf{0}$ | $\mathbf{1}$ | $\boldsymbol{x}$ | $\boldsymbol{x+1}$ |
|---|---|---|---|---|
| $\mathbf{0}$ | $0$ | $1$ | $x$ | $x+1$ |
| $\mathbf{1}$ | $1$ | $0$ | $x+1$ | $x$ |
| $\boldsymbol{x}$ | $x$ | $x+1$ | $0$ | $1$ |
| $\boldsymbol{x+1}$ | $x+1$ | $x$ | $1$ | $0$ |

and

| $+$ | $\mathbf{0}$ | $\mathbf{1}$ | $\mathbf{2}$ | $\mathbf{3}$ |
|---|---|---|---|---|
| $\mathbf{0}$ | 0 | 1 | 2 | 3 |
| $\mathbf{1}$ | 1 | 0 | 3 | 2 |
| $\mathbf{2}$ | 2 | 3 | 0 | 1 |
| $\mathbf{3}$ | 3 | 2 | 1 | 0 |

,

respectively. If we remove the top and left borders of the above Cayley tables, then we obtain the corresponding equivalent latin squares

| | | | |
|---|---|---|---|
| $0$ | $1$ | $x$ | $x+1$ |
| $1$ | $0$ | $x+1$ | $x$ |
| $x$ | $x+1$ | $0$ | $1$ |
| $x+1$ | $x$ | $1$ | $0$ |

$L^{(\mathbb{F}_{2^2}[x],+)}$

and

| | | | |
|---|---|---|---|
| 0 | 1 | 2 | 3 |
| 1 | 0 | 3 | 2 |
| 2 | 3 | 0 | 1 |
| 3 | 2 | 1 | 0 |

$L^{(\mathbb{F}_{2^2},+)}$

that encode $L^{(\mathbb{F}_{2^2}[x],+)} \cong L^{(\mathbb{F}_{2^2},+)}$, which is "built from" a $2 \times 2$ array of order-2 latin sub-squares that are each equivalent to $L^{(\mathbb{Z}_2,+)}$.

**Definition 1.10.** Let $\mathcal{C} \subset \mathcal{L}^n$ be a set of order-$n$ latin squares and let $L^{\mathcal{A}}, L^{\mathcal{B}} \in \mathcal{C}$ be two distinct latin squares. $\mathcal{C}$ is said to be a *set of mutually orthogonal latin squares* if each super-imposition $L^{\mathcal{A}} \otimes L^{\mathcal{B}}$ is a graeco-latin square for all $L^{\mathcal{A}}, L^{\mathcal{B}} \in \mathcal{C}$.

A well-known connection between mutually orthogonal latin squares and Galois fields is [52]:

**Proposition 1.11.** *Let $p^d \in \mathbb{N}$ be a prime power. Then there exists the following:*

- *A Galois field $\mathbb{F}_{p^d}$ of order-$p^d$.*
- *A set $\mathcal{C} \subset \mathcal{L}^{p^d}$ of mutually orthogonal latin squares with $|\mathcal{C}| = p^d - 1$.*

*See Appendix A (and the references therein) for more information on Galois fields.*

**Example 1.12.** Here we give an example of a connection between orthogonal latin squares, graeco-latin squares, magic squares, and Galois fields. Let $\mathcal{G} = (\mathcal{G}, \oplus)$ and $\mathcal{H} = (\mathcal{H}, \odot)$ be finite groups over the set of symbols $\mathbb{Z}_3 = \{0, 1, 2\}$ such that their (unbordered) Cayley tables are the order-3 latin squares

$$L^{\mathcal{G}} = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{bmatrix} \quad \text{and} \quad L^{\mathcal{H}} = \begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix},$$

where $L^{\mathcal{G}}$ and $L^{\mathcal{H}}$ are orthogonal. Then $L^{\mathcal{G}}$ and $L^{\mathcal{H}}$ can be super-imposed to obtain the graeco-latin square

$$L^{\mathcal{G}} \otimes L^{\mathcal{H}} = \begin{bmatrix} (1,0) & (2,2) & (0,1) \\ (0,2) & (1,1) & (2,0) \\ (2,1) & (0,0) & (1,2) \end{bmatrix}$$

where each ordered pair of

$$\mathcal{G} \otimes \mathcal{H} \equiv \mathcal{G} \times \mathcal{H} = \{(0,0), (1,1), (2,2), (1,2), (2,0), (0,1), (2,1), (0,2), (1,0)\}$$

is unique. Then, for each ordered pair $(a, b) \in \mathcal{G} \times \mathcal{H} = \mathbb{Z}_3 \times \mathbb{Z}_3$, there exists a unique linear polynomial $ax+b \in \mathbb{F}_{3^2}[x] = \mathbb{Z}_3[x]/\langle P(x)\rangle$ for some degree 2 irreducible polynomial $P(x) = x^2 + 1 \in \mathbb{Z}_3[x]$, such that we obtain

$$\begin{bmatrix} (1,0) & (2,2) & (0,1) \\ (0,2) & (1,1) & (2,0) \\ (2,1) & (0,0) & (1,2) \end{bmatrix} \leftrightarrow \begin{bmatrix} x & 2x+2 & 1 \\ 2 & x+1 & 2x \\ 2x+1 & 0 & x+2 \end{bmatrix}$$

where

$$\begin{array}{ccccccc} (0,0) & \leftrightarrow & 0x+0 & = & 0 & \in & \mathbb{F}_{3^2}[x] \\ (0,1) & \leftrightarrow & 0x+1 & = & 1 & \in & \mathbb{F}_{3^2}[x] \\ (0,2) & \leftrightarrow & 0x+2 & = & 2 & \in & \mathbb{F}_{3^2}[x] \\ (1,0) & \leftrightarrow & 1x+0 & = & x & \in & \mathbb{F}_{3^2}[x] \\ (1,1) & \leftrightarrow & 1x+1 & = & x+1 & \in & \mathbb{F}_{3^2}[x] \\ (1,2) & \leftrightarrow & 1x+2 & = & x+2 & \in & \mathbb{F}_{3^2}[x] \\ (2,0) & \leftrightarrow & 2x+0 & = & 2x & \in & \mathbb{F}_{3^2}[x] \\ (2,1) & \leftrightarrow & 2x+1 & = & 2x+1 & \in & \mathbb{F}_{3^2}[x] \\ (2,2) & \leftrightarrow & 2x+2 & = & 2x+2 & \in & \mathbb{F}_{3^2}[x]. \end{array}$$

Then we let $x = 3$ to obtain

$$\begin{bmatrix} (1,0) & (2,2) & (0,1) \\ (0,2) & (1,1) & (2,0) \\ (2,1) & (0,0) & (1,2) \end{bmatrix} \leftrightarrow \begin{bmatrix} 3 & 2\bullet 3+2 & 1 \\ 2 & 3+1 & 2\bullet 3 \\ 2\bullet 3+1 & 0 & 3+2 \end{bmatrix} \leftrightarrow \begin{bmatrix} 3 & 8 & 1 \\ 2 & 4 & 6 \\ 7 & 0 & 5 \end{bmatrix},$$

which is a magic square with a magic constant of 12.

There is interest in sets of mutually orthogonal latin squares with much information in the literature; for the reader who wishes to learn more details on mutually orthogonal latin squares, we recommend [12, 53, 54, 55] as a good starting point. It turns out that the notion of mutually orthogonal latin squares justifies the importance of examining latin square "transversals" [6]; a latin square feature that is of primary interest for this thesis.

**Definition 1.13.** A *transversal* of a latin square is a set of entries which includes exactly one entry from each row and column, and one of each symbol.

**Definition 1.14.** A permutation of a set $\mathcal{G}$ is a function $P : \mathcal{G} \to \mathcal{G}$ that is both one-to-one and onto.

**Table 1.4: A latin square $L^{(\mathbb{Z}_5,+)}$ which encodes the finite group $(\mathbb{Z}_5,+)$ has 15 transversals. One of these transversals is marked in green parentheses. Can the reader find any of the other transversals?**

| $+$ | **0** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|---|
| **0** | 0 | 1 | (2) | 3 | 4 |
| **1** | 1 | 2 | 3 | (4) | 0 |
| **2** | 2 | 3 | 4 | 0 | (1) |
| **3** | (3) | 4 | 0 | 1 | 2 |
| **4** | 4 | (0) | 1 | 2 | 3 |

**Definition 1.15.** Let $(\mathcal{G},\oplus)$ be a finite group of order-$n$. Let $P_1$ and $P_2$ be permutations over $(\mathcal{G},\oplus)$. Then $P_1=(a_1,...,a_n)$ and $P_2=(b_1,...,b_n)$, where $a_i,b_i\in\mathcal{G}$ for all $i\in\mathbb{Z}_n$. We define point-wise addition between $P_1$ and $P_2$ as

$$P_1\oplus P_2=(a_1\oplus b_1,a_2\oplus b_2,...,a_n\oplus b_n)=P_3.$$

If $P_3=P_1\oplus P_2$ is a permutation over $(\mathcal{G},\oplus)$, then $P_3$ is said to be an *additive permutation* or "*good permutation*".

It turns out that not all permutations are additive permutations. The question regarding the existence of transversals in latin squares that encode finite algebraic structures (ex. groups, quasi-groups, Galois fields, etc.) is far from being resolved and is an area of active investigation. The following known fact is of fundamental importance to this thesis [56, 57, 58, 59]:

**Theorem 1.16.** *Counting the pairs of permutations over a finite group whose point-wise sum is also a permutation is equivalent to counting the transversals of a latin square that encodes the group.*

**Example 1.17.** The transversal marked across the latin square $L^{(\mathbb{Z}_5,+)}$ in Table 1.4

is equivalent to an additive permutation; let $P_3$ be this permutation, which can be written "from left to right" as

$$\begin{aligned} P_3 &= (3,0,2,4,1) \\ &= (3+0,4+1,0+2,1+3,2+4) \\ &= (3,4,0,1,2)+(0,1,2,3,4) \\ &= P_1+P_2. \end{aligned}$$

In this thesis, our primary objective is to find latin squares that possess the *maximum* number of transversals for a given order-$n$; can we make accurate predictions? In other words, we wish to determine which order-$n$ algebraic structures possess the maximum number of additive permutations; any such structures that "pass" such "latin square tests" will be candidates for the construction of computationally secure cryptographic systems that operate with additive permutations. For example, a cryptographic hash function that operates with additive permutations will have a greater collision resistance to attacks if we use algebraic structures that possess the maximum number of additive permutations (when compared to structures with relatively few additive permutations). Therefore, the main points of this thesis are summarized as follows:

- In Sections 2.1–2.4 we discuss some additional pertinent notions of latin squares.
- In Sections 2.5 and 2.7 we discuss our software tools for generating latin square data sets and counting transversals.
- In Section 2.6 we survey some recent results and conjectures related to transversals.
- In Section 2.8 we search for latin squares with maximum transversal counts:
  - We confirm previous results [5, 6, 8] that cyclic latin squares of prime order-$p$ possess the maximum transversal counts for $3 \leq p \leq 9$.

  - We create a new algorithm that uses these prime order-$p$ cyclic latin squares as “building blocks” to construct “super-symmetric latin squares” of prime power order-$p^d$, which is a generalization of the order-$2^d$ algorithm proposed in [60].
  - Using this algorithm we accurately predict that super-symmetric latin squares of order-$p^d$ with $d > 0$ possess the confirmed maximum transversal counts for $3 \leq p^d \leq 9$ from [5, 6, 8] and the estimated lower bound on the maximum transversal counts for $9 < p^d \leq 17$ from [5, 6, 8].
  - Based on the said evidence, we give some conjectures regarding the number of transversals in super-symmetric latin squares.

- Lastly, in Chapter 3 we give an example application of how our algorithms and results can be applied to cryptography for cyber security:
  - We create a new generalized version of Grøstl [61], an iterated cryptographic hash function, where the compression function is built from two fixed, large, distinct permutations.
  - In particular, we use the super-symmetric latin square for the additive group of the Galois field $(\mathbb{F}_{3^2}, +)$, which possesses the confirmed maximum transversal count for order-9, to build our “*Simplified-Grøstl*” (S-Grøstl).

Note: the latest versions of our latin square tools are open source and are available at: https://sourceforge.net/projects/latin-square-toolbox/.

# CHAPTER 2

# LATIN SQUARES

## 2.1 How Many Exist?

Before we begin to explore latin squares, one of the first questions that may come to mind is: *for a given order-$n$, how many $n \times n$ latin squares exist?* Mathematicians and scientists have worked on this challenging problem for many generations. To date of writing, the short answer is: the counts are known up to order-11 [1, 2], but beyond that nobody knows for sure!

Let $|\mathcal{L}^{n'}|$ be the number of *reduced* order-$n$ latin squares. Based on Definition 2.1, it is not difficult to show that in fact $|\mathcal{L}^n| = |\mathcal{L}^{n'}|n!(n-1)!$. Thus, in the attempt to answer this question for a given order-$n$, one may begin to hunt for $|\mathcal{L}^{n'}|$ and then use it to compute $|\mathcal{L}^n|$.

**Definition 2.1.** A latin square is said to be in *reduced form* if both its first row and first column are in their natural order. Note: by "natural order" we mean ordered like the natural numbers $\mathbb{N}$.

The chronology of results for which the exact values of $|\mathcal{L}^n|$ are known is as follows:

- In 1782 Euler [11] determined $|\mathcal{L}^5|$, which was independently determined in 1890 by Cayley [22].

**Figure 2.1: An example of a latin square in non-reduced form [left] and reduced form [right], where the second and fourth rows of the non-reduced latin square are swapped to transform it into a reduced latin square that encodes the cyclic group. Any latin square can be reduced by permuting its rows and columns to yield the natural order.**

| | | | |
|---|---|---|---|
| 0 | 1 | 2 | 3 |
| 3 | 2 | 1 | 0 |
| 2 | 0 | 3 | 1 |
| 1 | 3 | 0 | 2 |

**Non-Reduced Form**

| | | | |
|---|---|---|---|
| 0 | 1 | 2 | 3 |
| 1 | 3 | 0 | 2 |
| 2 | 0 | 3 | 1 |
| 3 | 2 | 1 | 0 |

**Reduced Form**

- In the period of 1890–1900 Frolov [62] and Tarry [63] determined $|\mathcal{L}^6|$. Thereafter in 1915 McMahon found roughly the same numbers with an alternative approach [64].
- In the period of 1939–1951 Norton [65], Sade [66], and Saxena [67] determined $|\mathcal{L}^7|$.
- In 1967 Wells determined $|\mathcal{L}^8|$ [68].
- In 1975 Bammel and Rothstein determined $|\mathcal{L}^9|$ [69].
- In the period of 1990-1995 Rogoyoski and McKay determined $|\mathcal{L}^{10}|$ (Rogoyoski was an amateur mathematician working on his home computer) [70].
- In 2005 (armed with more computational power) McKay and Wanless determined $|\mathcal{L}^{11}|$ [71].

Note: for the above results, one finds $|\mathcal{L}^{n'}|$ and then computes $|\mathcal{L}^n| = |\mathcal{L}^{n'}|n!(n-1)!$.

In Table 2.1 we observe that (as $n$ increases) $|\mathcal{L}^{n'}|$ increases at an astronomical rate: observe the table below, which displays all known values of $|\mathcal{L}^n|$ and $|\mathcal{L}^{n'}|$ for $1 \leq n \leq 11$ [1, 2].

**Table 2.1: The number of latin squares up to order-11; the $|\mathcal{L}^{n'}|$ column contains the OEIS Sequence A000315 [1] while the $|\mathcal{L}^{n}|$ column contains the OEIS Sequence A002860 [2].**

| $n$ | **# Reduced Latin Squares ($|\mathcal{L}^{n'}|$)** | **# All Latin Squares ($|\mathcal{L}^{n}|$)** |
|---|---:|---:|
| 1 | 1 | 1 |
| 2 | 1 | 2 |
| 3 | 1 | 12 |
| 4 | 4 | 576 |
| 5 | 56 | 161 280 |
| 6 | 9408 | 812 851 200 |
| 7 | 16 942 080 | 61 479 419 904 000 |
| 8 | 535 281 401 856 | 108 776 032 459 082 956 800 |
| 9 | 377 597 570 964 258 816 | 5 524 751 496 156 892 842 531 225 600 |
| 10 | 7 580 721 483 160 132 811 489 280 | 9 982 437 658 213 039 871 725 064 756 920 320 000 |
| 11 | 5 363 937 773 277 371 298 119 673 540 771 840 | 776 966 836 171 770 144 107 444 346 734 230 682 311 065 600 000 |
| 12 | ? | ? |

To date, as it turns out, an *easily computable* explicit formula for answering this fundamental question does not yet exist, as the most accurate upper and lower bounds that are known for large $n$ still remain far apart. For example, one well-known result for computing the full $|\mathcal{L}^n|$ is [72]

$$\frac{(n!)^{2n}}{n^{n^2}} \leq |\mathcal{L}^n| \leq \prod_{k=1}^{n} (k!)^{n/k}.$$

In the literature there are a handful of explicit formulas for computing $|\mathcal{L}^n|$ [71, 73]. For instance, a relatively simple and explicit formula for the number of latin squares was determined in 1992 by Shao and Wei [73]

$$|\mathcal{L}^n| = n! \sum_{A \in B_n} (-1)^{\sigma_0(A)} \binom{\mathrm{per}(A)}{n}, \tag{2.1}$$

where $B_n$ is the set of $n \times n$ binary permutation matrices (each row and column contain exactly one nonzero element), $\sigma_0(A)$ is the number of zero entries in $A$, and $\mathrm{per}(A)$ is the permanent of $A$. Unfortunately, the number of terms in (2.1) exponentially increases, so it quickly becomes difficult to compute $|\mathcal{L}^n|$ as the order-$n$ increases.

In any case, this problem remains open for $n \geq 12$ [1, 2] and stands as one of the greatest challenges in latin square research. For the reader who is further interested in the enumeration of latin squares, we recommend the literature [71, 74, 75] and the references therein.

## 2.2 Basic Notation

For the purposes of this thesis, we will now give a more formal notation for encoding latin squares. It is important to establish these notational clarifications now because we'll be referring to latin squares with three distinct but equivalent notations, which will depend on the context.

**Definition 2.2.** Let $L \in \mathcal{L}^n$ be an order-$n$ latin square over a set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ of symbols (the integers modulo $n$). We say that $L$ is encoded in the $n \times n$ *symbol matrix form* if we write

$$L = \begin{bmatrix} z_{0,0} & z_{0,1} & \cdots & z_{0,n-1} \\ z_{1,0} & z_{1,1} & \cdots & z_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ z_{n-1,0} & z_{n-1,1} & \cdots & z_{n-1,n-1} \end{bmatrix} = \begin{bmatrix} L_{0,0} & L_{0,1} & \cdots & L_{0,n-1} \\ L_{1,0} & L_{1,1} & \cdots & L_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ L_{n-1,0} & L_{n-1,1} & \cdots & L_{n-1,n-1} \end{bmatrix} \in \mathcal{L}^n \subset \mathbb{Z}_n^{n \times n},$$

where $\mathbb{Z}_n^{n \times n}$ is the set of all $n \times n$ matrices over $\mathbb{Z}_n$, and $x, y, z_{x,y} \in \mathbb{Z}_n$ such that each $z_{x,y} = L_{x,y}$ is the symbol inscribed in the entry of the $x$th row and $y$th column of $L$. Moreover, we say that the $x$th *row* of $L$ and the $y$th *column* of $L$ are respectively written as

$$L_{x,*} = \begin{pmatrix} z_{x,0} & z_{x,1} & \ldots & z_{x,n-1} \end{pmatrix} \quad \text{and} \quad L_{*,y} = \begin{pmatrix} z_{0,y} \\ z_{1,y} \\ \vdots \\ z_{n-1,y} \end{pmatrix}$$

so

$$L = \begin{bmatrix} z_{0,0} & z_{0,1} & \cdots & z_{0,n-1} \\ z_{1,0} & z_{1,1} & \cdots & z_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ z_{n-1,0} & z_{n-1,1} & \vdots & z_{n-1,n-1} \end{bmatrix} = \begin{bmatrix} L_{0,*} \\ L_{1,*} \\ \cdots \\ L_{n-1,*} \end{bmatrix} = \begin{bmatrix} L_{*,0} & L_{*,1} & \ldots & L_{*,n-1} \end{bmatrix}.$$

**Example 2.3.** Let $L \in \mathcal{L}^4$ be the reduced latin square in Figure 2.1. Then the symbol matrix form of $L$ is

$$L = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 3 & 0 & 2 \\ 2 & 0 & 3 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix} \in \mathcal{L}^4 \subset \mathbb{Z}_4^{4\times 4},$$

where the rows of $L$ are

$$\begin{aligned} L_{0,*} &= (0\ 1\ 2\ 3), \\ L_{1,*} &= (1\ 3\ 0\ 2), \\ L_{2,*} &= (2\ 0\ 3\ 1), \quad \text{and} \\ L_{3,*} &= (3\ 2\ 1\ 0), \end{aligned}$$

and the columns of $L$ are

$$L_{*,0} = \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix}, \quad L_{*,1} = \begin{pmatrix} 1 \\ 3 \\ 0 \\ 2 \end{pmatrix}, \quad L_{*,2} = \begin{pmatrix} 2 \\ 0 \\ 3 \\ 1 \end{pmatrix}, \quad \text{and} \quad L_{*,3} = \begin{pmatrix} 3 \\ 2 \\ 1 \\ 0 \end{pmatrix}.$$

**Remark 2.4.** Depending on the context, we may write the symbol inscribed in the $x$th row and $y$th column of $L$ as either $L_{x,y}$ or $z_{x,y}$, which are equivalent notations that mean exactly the same thing. For example, if we're referring to $L$ in a permutation context, then we may write the inscribed symbol as $L_{x,y}$ because it will be consistent with our notation of the $x$th row permutation $L_{x,*}$ and the $y$th column permutation $L_{*,y}$ in upcoming sections. Alternatively, if we're referring to $L$ in a 3D Cartesian-coordinate context, then we may write the inscribed symbol as $z_{x,y}$ because it will be consistent with our ordered 3-tuple notation $(x, y, z_{x,y})$ as defined below.

**Definition 2.5.** Let $L \in \mathcal{L}^n$ be a latin square. We say that $L$ is encoded in the $n$-by-$n$ *ordered 3-tuple matrix form* if we write

$$L = \begin{bmatrix} (0,0,z_{0,0}) & (0,1,z_{0,1}) & \dots & (0,n-1,z_{0,n-1}) \\ (1,0,z_{1,0}) & (1,1,z_{1,1}) & \dots & (1,n-1,z_{1,n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ (n-1,0,z_{n-1,0}) & (n-1,1,z_{n-1,1}) & \dots & (n-1,n-1,z_{n-1,n-1}) \end{bmatrix} \in (\mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n)^{n \times n},$$

where $L$ is written as an $n \times n$ array of ordered 3-tuples $(x, y, z) = (x, y, z_{x,y}) \in \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$, such that each ordered triple encodes a 3D cartesian-coordinate coordinate in $\mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$.

**Example 2.6.** Let $L \in \mathcal{L}^4$ be the reduced form latin square in Figure 2.1. Then the ordered 3-tuple matrix form of $L$ is

$$L = \begin{bmatrix} (0,0,0) & (0,1,1) & (0,2,2) & (0,3,3) \\ (1,0,1) & (1,1,3) & (1,2,0) & (1,3,2) \\ (2,0,2) & (2,1,0) & (2,2,3) & (2,3,1) \\ (3,0,3) & (3,1,2) & (3,2,1) & (3,3,0) \end{bmatrix} \in (\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4)^{4 \times 4}.$$

**Definition 2.7.** Let $L \in \mathcal{L}^n$ be a latin square. We say that a set ${}^{\{\}}L$ of $n^2$ ordered triples is the *ordered 3-tuple set form* of $L$ if

$${}^{\{\}}L = \{\ (x, y, z) \in \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n\ \},$$

where each entry of $L$ is encoded as an ordered triple.

**Example 2.8.** Let $L \in \mathcal{L}^4$ be the reduced latin square in Figure 2.1. Then the ordered 3-tuple set form of $L$ is

$$\begin{aligned} {}^{\{\}}L \quad = \quad \{ \quad & (0,0,0), (0,1,1), (0,2,2), (0,3,3) \\ & (1,0,1), (1,1,3), (1,2,0), (1,3,2) \\ & (2,0,2), (2,1,0), (2,2,3), (2,3,1) \\ & (3,0,3), (3,1,2), (3,2,1), (3,3,0) \ \ \}, \end{aligned}$$

which is a set of coordinates in $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$ that encodes $L$.

**Remark 2.9.** If we're referring to $L$ in a context that requires us to identify subsets of entries of $L$, then we will use the ordered 3-tuple set notation ${}^{\{\}}L$. For example, in Sections 2.6–2.8 we'll be referring to diagonals, transversals, and disjoint subsets of latin squares so we'll need the ordered 3-tuple set notation.

Consequently, we have the notational equivalence $L \equiv {}^{\{\}}L$ by definition.

**Example 2.10.** Let $\mathcal{A}$ and $\mathcal{B}$ both be sets of $n$ symbols for the latin squares $L^{\mathcal{A}}$, $L^{\mathcal{B}} \in \mathcal{L}^n$, respectively. Then the super-imposition of $L^{\mathcal{A}}$ and $L^{\mathcal{B}}$ is the $n \times n$ array of ordered pairs of symbols $L^{\mathcal{A}} \otimes L^{\mathcal{B}}$ written as

$$\begin{aligned} L^{\mathcal{A}} \otimes L^{\mathcal{B}} &= \begin{bmatrix} L^{\mathcal{A}}_{0,0} & L^{\mathcal{A}}_{0,1} & \cdots & L^{\mathcal{A}}_{0,n-1} \\ L^{\mathcal{A}}_{1,0} & L^{\mathcal{A}}_{1,1} & \cdots & L^{\mathcal{A}}_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ L^{\mathcal{A}}_{n-1,0} & L^{\mathcal{A}}_{n-1,1} & \cdots & L^{\mathcal{A}}_{n-1,n-1} \end{bmatrix} \otimes \begin{bmatrix} L^{\mathcal{B}}_{0,0} & L^{\mathcal{B}}_{0,1} & \cdots & L^{\mathcal{B}}_{0,n-1} \\ L^{\mathcal{B}}_{1,0} & L^{\mathcal{B}}_{1,1} & \cdots & L^{\mathcal{B}}_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ L^{\mathcal{B}}_{n-1,0} & L^{\mathcal{B}}_{n-1,1} & \cdots & L^{\mathcal{B}}_{n-1,n-1} \end{bmatrix} \\ &= \begin{bmatrix} (L^{\mathcal{A}}_{0,0}, L^{\mathcal{B}}_{0,0}) & (L^{\mathcal{A}}_{0,1}, L^{\mathcal{B}}_{0,1}) & \cdots & (L^{\mathcal{A}}_{0,n-1}, L^{\mathcal{B}}_{0,n-1}) \\ (L^{\mathcal{A}}_{1,0}, L^{\mathcal{B}}_{1,0}) & (L^{\mathcal{A}}_{1,1}, L^{\mathcal{B}}_{1,1}) & \cdots & (L^{\mathcal{A}}_{1,n-1}, L^{\mathcal{B}}_{1,n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ (L^{\mathcal{A}}_{n-1,0}, L^{\mathcal{B}}_{n-1,0}) & (L^{\mathcal{A}}_{n-1,1}, L^{\mathcal{B}}_{n-1,1}) & \cdots & (L^{\mathcal{A}}_{n-1,n-1}, L^{\mathcal{B}}_{n-1,n-1}) \end{bmatrix}, \end{aligned}$$

where $\otimes$ is the super-imposition operator, such that the set

$$\mathcal{A} \otimes \mathcal{B} \equiv \mathcal{A} \times \mathcal{B} = \{(L^{\mathcal{A}}_{x,y}, L^{\mathcal{B}}_{x,y}) : L^{\mathcal{A}}_{x,y} \in \mathcal{A} \ \text{ and } \ L^{\mathcal{B}}_{x,y} \in \mathcal{B}\}$$

is the Cartesian product.

## 2.3 Encoding Cayley Tables of Finite Groups and Quasi-groups

In this section we demonstrate how latin squares can be applied to encode algebraic structures that are fundamental to disciplines such as cryptography and cyber security. For this, we'll discuss finite groups (ex. Galois field addition), finite quasi-groups, and permutation groups.

### 2.3.1 Connecting Groups and Permutations

Since we're interested in how latin squares apply to cryptography, then it will behoove us to connect latin squares and group Cayley tables to permutations and permutation groups; this is our objective here.

In [20, 21] Cayley achieved the following result.

**Theorem 2.11.** *If $\mathcal{G} = (\mathcal{G}, \oplus)$ is an order-$n$ finite group and $L^{\mathcal{G}}$ is the unbordered Cayley table of $\mathcal{G}$, then $L^{\mathcal{G}} \in \mathcal{L}^n$ (is an order-$n$ latin square).*

***Proof*.** Suppose that $\mathcal{G} = (\mathcal{G}, \oplus)$ is an order-$n$ finite group and $L^{\mathcal{G}}$ is the unbordered Cayley table of $\mathcal{G}$. We wish to show that $L^{\mathcal{G}} \in \mathcal{L}^n$. Choose a row $L^{\mathcal{G}}_{g_i,*}$ of $L^{\mathcal{G}}$ indexed by $g_i \in \mathcal{G}$. Next, suppose that two elements in $L^{\mathcal{G}}_{g_i,*}$ are equal. Then there exist two columns of $L^{\mathcal{G}}$, denoted $L^{\mathcal{G}}_{*,g_j}$ (indexed by $g_j \in \mathcal{G}$) and $L^{\mathcal{G}}_{*,g_k}$ (indexed by $g_k \in \mathcal{G}$), such that

$$L^{\mathcal{G}}_{g_i,g_j} = g_i \oplus g_j \quad \text{and} \quad L^{\mathcal{G}}_{g_i,g_k} = g_i \oplus g_k.$$

Therefore

$$\begin{array}{rcl} L^{\mathcal{G}}_{g_i,g_j} & = & L^{\mathcal{G}}_{g_i,g_k} \\ g_i \oplus g_j & = & g_i \oplus g_k \\ g_i^{-1} \oplus g_i \oplus g_j & = & g_i^{-1} \oplus g_i \oplus g_k \\ (g_i^{-1} \oplus g_i) \oplus g_j & = & (g_i^{-1} \oplus g_i) \oplus g_k \\ e \oplus g_j & = & e \oplus g_k \\ g_j & = & g_k, \end{array}$$

which implies that $L^{\mathcal{G}}_{*,g_j} = L^{\mathcal{G}}_{*,g_k}$. So there are no repetitions of elements in $L^{\mathcal{G}}_{g_i,*}$ because the two columns $L^{\mathcal{G}}_{*,g_j}$ and $L^{\mathcal{G}}_{*,g_k}$ are the same. Henceforth, using the same argument for columns, there are no repetitions of elements for any $L^{\mathcal{G}}_{*,g_i}$, because the two rows $L^{\mathcal{G}}_{g_j,*}$ and $L^{\mathcal{G}}_{g_k,*}$ are the same. Consequently $L^{\mathcal{G}} \in \mathcal{L}^n$ is a latin square. ■

**Definition 2.12.** Let $\mathcal{G} = (\mathcal{G}, \oplus)$ and $\mathcal{H} = (\mathcal{H}, \star)$ be groups. Then a function $\alpha : \mathcal{G} \to \mathcal{H}$ is said to be a *group homomorphism* if

$$\alpha(g_i \oplus g_j) = \alpha(g_i) \star \alpha(g_j), \quad \forall g_i, g_j \in \mathcal{G}.$$

**Definition 2.13.** Let $\mathcal{G} = (\mathcal{G}, \oplus)$ and $\mathcal{H} = (\mathcal{H}, \star)$ be groups. Then a group homomorphism $\alpha : \mathcal{G} \to \mathcal{H}$ is said to be a *group isomorphism* if and only if it is bijective. In this case $\mathcal{G}$ and $\mathcal{H}$ are said to be *isomorphic*, which is denoted by $\mathcal{G} \cong \mathcal{H}$.

**Definition 2.14.** Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a group. Then an isomorphism $\alpha$ is said to be an *automorphism* if $\alpha : \mathcal{G} \to \mathcal{G}$. If $\mathcal{G}$ is a finite group of order-$n$, then $\alpha$ is said to be a *permutation* of the set of $\mathcal{G}$, which may be written in *two-line notation* as

$$\alpha = \begin{pmatrix} e & g_1 & g_2 & \dots & g_{n-1} \\ \downarrow & \downarrow & \downarrow & \dots & \downarrow \\ \alpha(e) & \alpha(g_1) & \alpha(g_2) & \dots & \alpha(g_{n-1}) \end{pmatrix} = \begin{pmatrix} e & g_1 & g_2 & \dots & g_{n-1} \\ \alpha(e) & \alpha(g_1) & \alpha(g_2) & \dots & \alpha(g_{n-1}) \end{pmatrix},$$

or equivalently in *one-line notation* as

$$\alpha = [\alpha(e) \;\; \alpha(g_1) \;\; \alpha(g_2) \;\; \dots \;\; \alpha(g_{n-1})]$$

by assuming a natural order for the elements and omitting the first row of the two-line notation.

**Remark 2.15.** In addition to using two-line and one-line notation, we'll also write permutations using *cycle notation* (see the example below).

**Example 2.16.** Let $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ be the set of integers modulo 5. Then examples of two permutations of the elements of $\mathbb{Z}_5$ written in two-line notation are

$$\alpha = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ \alpha(0) & \alpha(1) & \alpha(2) & \alpha(3) & \alpha(4) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 3 & 0 & 2 & 4 \end{pmatrix} \quad \text{and}$$

$$\beta = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ \beta(0) & \beta(1) & \beta(2) & \beta(3) & \beta(4) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 & 0 \end{pmatrix},$$

which can equivalently be written in the corresponding one-line notation

$$\alpha = [1 \;\; 3 \;\; 0 \;\; 2 \;\; 4] \quad \text{and} \quad \beta = [4 \;\; 3 \;\; 2 \;\; 1 \;\; 0],$$

and furthermore can equivalently be written in *cycle notation*

$$\alpha = (0 \;\; 1 \;\; 3 \;\; 2) \quad \text{and} \quad \beta = (0 \;\; 4)(1 \;\; 3).$$

**Definition 2.17.** A finite group $\mathcal{P} = (\mathcal{P}, \circ)$ is said to be a *permutation group* if:

- the elements of $\mathcal{P}$ are permutations of a given set $\mathcal{G} = \{e, g_1, g_2, ..., g_{n-1}\}$, and
- the group operation $\circ$ of $\mathcal{P}$ is the composition of such permutations of $\mathcal{G}$.

**Definition 2.18.** The finite group $\mathcal{S}_n = (\mathcal{S}_n, \circ)$ is said to be the *symmetric group* on the finite set $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ of $n$ symbols if:

- each element $\alpha \in \mathcal{S}_n$ is a permutation $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$, and
- the group operation $\circ$ of $\mathcal{S}_n$ is the *composition* of such permutations of $\mathbb{Z}_n$.

The following result was proved by Cayley [76].

**Theorem 2.19** (***Cayley***)**.** *Every finite group $\mathcal{G} = (\mathcal{G}, \oplus)$ of order-$n$ is isomorphic to a subgroup of the symmetric group $\mathcal{S}_n$.*

**Definition 2.20.** An ordered 4-tuple $(a, b, c, d)$ of entries from a latin square $L \in \mathcal{L}^n$ is said to be a *quadrangle* if it is of the form $(z_{i,j}, z_{i,k}, z_{l,k}, z_{l,j})$. In other words, $(a, b, c, d)$ is a quadrangle if the four entries are the corners of a rectangular block in $L$, with at least two rows and two columns, such that $a$ and $c$ lie on one of the diagonals of the rectangular block.

**Table 2.2: An example of a quadrangle $(z_{1,1}, z_{1,3}, z_{4,3}, z_{4,1}) = (2, 4, 2, 0)$ in the latin square $L^{(\mathbb{Z}_5,+)}$ which encodes the finite group $(\mathbb{Z}_5, +)$. The four entries of the quadrangle are marked in blue parentheses.**

| $+$ | **0** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|---|
| **0** | 0 | 1 | 2 | 3 | 4 |
| **1** | 1 | (2) | 3 | (4) | 0 |
| **2** | 2 | 3 | 4 | 0 | 1 |
| **3** | 3 | 4 | 0 | 1 | 2 |
| **4** | 4 | (0) | 1 | (2) | 3 |

**Definition 2.21.** A latin square $L \in \mathcal{L}^n$ is said to satisfy the *quadrangle criterion* if, whenever $(a, b, c, d)$ and $(a', b', c', d')$ are two quadrangles satisfying $a = a'$, $b = b'$, and $c = c'$, then $d = d'$.

We obtain the following result from [12].

**Theorem 2.22.** *Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite group of order-$n$ and let $L^{\mathcal{G}} \in \mathcal{L}^n$ encode $\mathcal{G}$. Then $L^{\mathcal{G}}$ has the following properties:*

*(i) Each row $L^{\mathcal{G}}_{x,*}$ and each column $L^{\mathcal{G}}_{*,y}$ of $L^{\mathcal{G}}$ is a permutation of the elements of $\mathcal{G}$.*

*(ii) The quadrangle criterion is satisfied.*

***Proof.*** ($\Longrightarrow$) Suppose that $\mathcal{G} = (\mathcal{G}, \oplus)$ is a finite group of order-$n$ and that $L^{\mathcal{G}} \in \mathcal{L}^n$ is the unbordered Cayley table of $\mathcal{G}$. We wish to show that properties $(i)$ and $(ii)$ are satisfied.

***Claim:*** *property $(i)$ holds.* From Theorem 2.11 it immediately follows that each row $L^{\mathcal{G}}_{x,*}$ and each column $L^{\mathcal{G}}_{*,y}$ is a permutation of the elements of $\mathcal{G}$. So $(i)$ is satisfied.

***Claim:*** *property* $(ii)$ *holds.* Suppose that $(z_{i,j}, z_{i,k}, z_{l,k}, z_{l,j})$ and $(z_{i',j'}, z_{i',k'}, z_{l',k'}, z_{l',j'})$ are two quadrangles of $L$ where

$$z_{i,j} = z_{i',j'}, \quad z_{i,k} = z_{i',k'}, \quad \text{and} \quad z_{l,k} = z_{l',k'}.$$

Then we obtain

$$\begin{aligned} z_{l,j} &= z_l \oplus z_j \\ &= z_l \oplus (z_k \oplus z_k^{-1}) \oplus (z_i^{-1} \oplus z_i) \oplus z_j \\ &= (z_l \oplus z_k) \oplus (z_i \oplus z_k)^{-1} \oplus (z_i \oplus z_j) \\ &= z_{l,k} \oplus z_{i,k}^{-1} \oplus z_{i,j} \\ &= z_{l',k'} \oplus z_{i',k'}^{-1} \oplus z_{i',j'} \\ &= (z_{l'} \oplus z_{k'}) \oplus (z_{i'} \oplus z_{k'})^{-1} \oplus (z_{i'} \oplus z_{j'}) \\ &= z_{l'} \oplus (z_{k'} \oplus z_{k'}^{-1}) \oplus (z_{i'}^{-1} \oplus z_{i'}) \oplus z_{j'} \\ &= z_{l'} \oplus z_{j'} \\ &= z_{l',j'}. \end{aligned}$$

So the quadrangle criterion is satisfied for $L^{\mathcal{G}}$; so $(ii)$ is satisfied.

Therefore, both properties $(i)$ and $(ii)$ are satisfied in $L^{\mathcal{G}}$ since it is the unbordered Cayley table of $\mathcal{G}$. ☑

$(\Longleftarrow)$ Conversely, suppose that $L \in \mathcal{L}^n$ is a latin square where properties $(i)$ and $(ii)$ are satisfied. We wish to show that $L = L^{\mathcal{G}}$ is the unbordered Cayley table of $\mathcal{G}$. For this, we will start by choosing borders for $L$ that will become the borders of the Cayley table of $\mathcal{G}$. First, we choose the top border; we denote this by ${}^{top}L$ and without loss of generality we choose the row ${}^{top}L = L_{e,*}$ (the identity permutation). Second, we choose the left border; we denote this by ${}^{left}L$ and without loss of generality we choose the column ${}^{left}L = L_{*,e}$. Now that the top-left border of $L$ is chosen, it follows that $L_{e,e} = e$ is the identity of $\mathcal{G}$. Since $L$ is a latin square, then

$$\begin{aligned} \forall g_x \in \mathcal{G}, \quad \exists! g_y \in \mathcal{G}, \quad L_{g_x,g_y} &= e \Longrightarrow g_x \oplus g_y &= e \\ \forall g'_y \in \mathcal{G}, \quad \exists! g'_x \in \mathcal{G}, \quad L_{g'_x,g'_y} &= e \Longrightarrow g'_x \oplus g'_y &= e, \end{aligned}$$

meaning that the equations are soluble for every $g_x, g'_y \in \mathcal{G}$ by property $(i)$. Next, we wish to use the assumed quadrangle criterion of property $(ii)$ to show that $\oplus$, which is associative in $\mathcal{G}$, is associative among the entries $L$. So take any $g_i, g_j, g_k \in \mathcal{G}$. If $g_i = e$, $g_j = e$, or $g_k = e$ then $g_i \oplus (g_j \oplus g_k) = (g_i \oplus g_j) \oplus g_k$ is trivial. Henceforth, we may assume that $g_i, g_j, g_k \neq e$. Then the subsquare of $L$ determined by the rows $L_{e,*}$ and $L_{g_i,*}$, and the columns $L_{*,g_j}$ and $L_{*,g_b \oplus g_k}$ has the Cayley table

| $\oplus$ | $\boldsymbol{g_j}$ | $\boldsymbol{g_j \oplus g_k}$ |
|---|---|---|
| $\boldsymbol{e}$ | $g_j$ | $g_j \oplus g_k$ |
| $\boldsymbol{g_i}$ | $g_i \oplus g_j$ | $g_i \oplus (g_j \oplus g_k)$ |

while the subsquare of $L$ determined by the rows $L_{g_j,*}$ and $L_{g_i \oplus g_j,*}$, and the columns $L_{*,e}$ and $L_{*,g_k}$ has the Cayley table

| $\oplus$ | $\boldsymbol{e}$ | $\boldsymbol{g_k}$ |
|---|---|---|
| $\boldsymbol{g_j}$ | $g_j$ | $g_j \oplus g_k$ |
| $\boldsymbol{g_i \oplus g_j}$ | $g_i \oplus g_j$ | $(g_i \oplus g_j) \oplus g_k$ |

.

Consequently, in the bottom right entry of the above two subsquares we see that we've obtained the associativity $g_i \oplus (g_j \oplus g_k) = (g_i \oplus g_j) \oplus g_k$ by the quadrangle criterion of property $(ii)$. So we have $L = L^{\mathcal{G}}$ since it is the unbordered Cayley table of $\mathcal{G}$; by appending the borders ${}^{top}L$ and ${}^{left}L$ to $L^{\mathcal{G}}$ we obtain the Cayley table of $\mathcal{G}$.

☑

■

The result of Theorem 2.22 yields the following.

**Corollary 2.23.** *Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite group of order-$n$. If $e, g_1, g_2, ..., g_{n-1}$ are the elements of $\mathcal{G}$ and $h \in \mathcal{G}$ is fixed, then the sets of products*

$$h \oplus e, h \oplus g_1, h \oplus g_2, ..., h \oplus g_{n-1} \quad \textit{and} \quad e \oplus h, g_1 \oplus h, g_2 \oplus h, ..., g_{n-1} \oplus h$$

*comprise all $n$ (possibly permuted) elements of $\mathcal{G}$.*

**Remark 2.24.** For the reader who is interested in a more in-depth historical explanation of Theorem 2.22 and Corollary 2.23, we recommend pg. 19 of [12] and the references therein.

At this point, let us briefly recapitulate the main results obtained thus far in this subsection, which pertain to cryptography. Given a finite group $\mathcal{G} = (\mathcal{G}, \oplus)$ of order-$n$, we can encode its unbordered Cayley table with a latin square $L^{\mathcal{G}} \in \mathcal{L}^n$, where $\mathcal{G}$ is isomorphic to a subgroup of $\mathcal{S}_n$, while each row and column of $L^{\mathcal{G}}$ is a permutation of the elements $\{e, g_1, g_2, ..., g_{n-1}\}$ of $\mathcal{G}$. We can elaborate on this as follows.

- $L^{\mathcal{G}}$'s "$x$th row permutation" that transforms the ordered list of $\{e, g_1, g_2, ..., g_{n-1}\}$ into $L^{\mathcal{G}}$'s $x$th row may be written as

$$\begin{aligned} L^{\mathcal{G}}_{x,*} &= \begin{pmatrix} e & g_1 & g_2 & \cdots & g_{n-1} \\ L^{\mathcal{G}}_{x,*}(e) & L^{\mathcal{G}}_{x,*}(g_1) & L^{\mathcal{G}}_{x,*}(g_2) & \cdots & L^{\mathcal{G}}_{x,*}(g_{n-1}) \end{pmatrix} \\ &= \begin{pmatrix} e & g_1 & g_2 & \cdots & g_{n-1} \\ z_{x,0} & z_{x,1} & z_{x,2} & \cdots & z_{x,n-1} \end{pmatrix}. \end{aligned}$$

- $L^{\mathcal{G}}$'s "$y$th column permutation" that transforms the ordered list of $\{e, g_1, g_2, ..., g_{n-1}\}$ into $L^{\mathcal{G}}$'s $y$th column may be written as

$$\begin{aligned} L^{\mathcal{G}}_{*,y} &= \begin{pmatrix} e & g_1 & g_2 & \cdots & g_{n-1} \\ L^{\mathcal{G}}_{*,y}(e) & L^{\mathcal{G}}_{*,y}(g_1) & L^{\mathcal{G}}_{*,y}(g_2) & \cdots & L^{\mathcal{G}}_{*,y}(g_{n-1}) \end{pmatrix} \\ &= \begin{pmatrix} e & g_1 & g_2 & \cdots & g_{n-1} \\ z_{0,y} & z_{1,y} & z_{2,y} & \cdots & z_{n-1,y} \end{pmatrix}. \end{aligned}$$

So in other words, the permutation $L^{\mathcal{G}}_{x_i,*} \circ L^{\mathcal{G}-1}_{x_j,*}$ leaves no symbol unchanged for $x_i \neq x_j$ because, otherwise, one column would contain a symbol twice. Therefore, a sequence of $n$ permutations $(L^{\mathcal{G}}_{0,*}, L^{\mathcal{G}}_{1,*}, L^{\mathcal{G}}_{2,*}, \ldots, L^{\mathcal{G}}_{n-1,*})$, where $L^{\mathcal{G}}_{x_i,*} \circ L^{\mathcal{G}-1}_{x_j,*}$ leaves no symbol unchanged for all $x_i, x_j \in \mathcal{G}$, generates the entire $L^{\mathcal{G}}$.

**Definition 2.25.** Let $L^{\mathcal{G}} \in \mathcal{L}^n$ be a latin square that encodes the group $\mathcal{G} = (\mathcal{G}, \oplus) = \{e, g_1, g_2, ..., g_{n-1}\}$. A proper subset of the entries of $L^{\mathcal{G}}$, denoted by $D^{L^{\mathcal{G}}} \subset {}^{\{\}}L^{\mathcal{G}}$, is said to be a *diagonal of* $L^{\mathcal{G}}$ if each $(g_x, g_y, g_z) \in D^{L^{\mathcal{G}}}$ encodes a unique $g_x \in \mathcal{G}$ and a unique $g_y \in \mathcal{G}$, where the order of $D^{L^{\mathcal{G}}}$ is $|D^{L^{\mathcal{G}}}| = n$. For each $(g_x, g_y, g_z) \in D^{L^{\mathcal{G}}}$, we say that $D^{L^{\mathcal{G}}}$ *passes through* the entry $(g_x, g_y, g_z)$. The *set of all diagonals of* $L^{\mathcal{G}}$ is denoted by $\mathcal{D}^{L^{\mathcal{G}}}$, so the number of diagonals of $L^{\mathcal{G}}$ is always given by $|\mathcal{D}^{L^{\mathcal{G}}}| = n!$ (i.e. the number of elements of $\mathcal{S}_n$).

**Table 2.3: An example of an order-5 diagonal $\{(3,0,3),(1,1,2),(0,2,2),(2,3,0),(4,4,3)\}$ (written "from left to right") across the latin square $L^{(\mathbb{Z}_5,+)}$. The five entries of the diagonal are marked in blue parentheses.**

| + | **0** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|---|
| **0** | 0 | 1 | (2) | 3 | 4 |
| **1** | 1 | (2) | 3 | 4 | 0 |
| **2** | 2 | 3 | 4 | (0) | 1 |
| **3** | (3) | 4 | 0 | 1 | 2 |
| **4** | 4 | 0 | 1 | 2 | (3) |

**Definition 2.26.** Let $L^{\mathcal{G}} \in \mathcal{L}^n$ be a latin square that is the unbordered Cayley table of the group $\mathcal{G} = (\mathcal{G}, \oplus) = \{e, g_1, g_2, ..., g_{n-1}\}$. Without loss of generality we may assume that $L^{\mathcal{G}}$ is in reduced form. The set of entries

$$\{(g_{x_0}, g_{y_0}, g_{x_0,y_0}), (g_{x_1}, g_{y_1}, g_{x_1,y_1}), (g_{x_2}, g_{y_2}, g_{x_2,y_2}), \ldots, (g_{x_{n-1}}, g_{y_{n-1}}, g_{x_{n-1},y_{n-1}})\}$$

is said to be the *main diagonal* of $L^{\mathcal{G}}$ if it connects the top-left entry and the bottom-right entry, which are

$$(g_{x_0}, g_{y_0}, g_{x_0,y_0}) \text{ and } (g_{x_{n-1}}, g_{y_{n-1}}, g_{x_{n-1},y_{n-1}}),$$

respectively. Similarly, the set of entries

$$\{(g_{x_0}, g_{y_{n-1}}, g_{x_0,y_{n-1}}), (g_{x_1}, g_{y_{n-2}}, g_{x_1,y_{n-2}}), (g_{x_2}, g_{y_{n-3}}, g_{x_2,y_{n-3}}), \ldots, (g_{x_{n-1}}, g_{y_0}, g_{x_{n-1},y_0})\}$$

is said to be the *main anti-diagonal* of $L^{\mathcal{G}}$ if it connects the top-right entry and the bottom-left entry, which are

$$(g_{x_0}, g_{y_{n-1}}, g_{x_0,y_{n-1}}) \text{ and } (g_{x_{n-1}}, g_{y_0}, g_{x_{n-1},y_0}),$$

respectively.

**Table 2.4: The entries of the main diagonal** $\{(0,0,0),(1,1,2),(2,2,4),(3,3,1),(4,4,0)\}$ **and the main anti-diagonal** $\{(4,0,4),(3,1,4),(2,2,4),(1,3,4),(0,4,4)\}$ **across the latin square** $L^{(\mathbb{Z}_5,+)}$ **are marked in blue parentheses and red square brackets, respectively.**

| $+$ | **0** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|---|
| **0** | (0) | 1 | 2 | 3 | [4] |
| **1** | 1 | (2) | 3 | [4] | 0 |
| **2** | 2 | 3 | [(4)] | 0 | 1 |
| **3** | 3 | [4] | 0 | (1) | 2 |
| **4** | [4] | 0 | 1 | 2 | (3) |

We obtain the following result from [12].

**Theorem 2.27.** *Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite group of order-$n$ and let $L^{\mathcal{G}} \in \mathcal{L}^n$ be a latin square that encodes $\mathcal{G}$. Then $\mathcal{G}$ is an abelian group if and only if $L^{\mathcal{G}}$ has the property that products located symmetrically, with respect to the main diagonal, encode the same group element.*

***Proof.*** Suppose that $\mathcal{G} = (\mathcal{G}, \oplus)$ is a finite group of order-$n$ and let $L^{\mathcal{G}} \in \mathcal{L}^n$ encode $\mathcal{G}$.

($\Longrightarrow$) Suppose that $\mathcal{G}$ is an abelian group. Take any $g_i, g_j \in \mathcal{G}$. Then by the commutative property of $\oplus$ there exists some $g_k \in \mathcal{G}$ such that

$$g_i \oplus g_j = g_k = g_j \oplus g_i$$

implies

$$L^{\mathcal{G}}_{g_i,g_j} = g_k = L^{\mathcal{G}}_{g_j,g_i}. \quad \boxed{\checkmark}$$

($\Longleftarrow$) Suppose, on the contrary, that (with respect to the main diagonal of $L^{\mathcal{G}}$) the products of $L^{\mathcal{G}}$ that are located symmetrically do not encode the same group element. Then there exists some $g_i, g_j \in \mathcal{G}$ such that

$$g_i \oplus g_j \neq g_j \oplus g_i$$

implies

$$L^{\mathcal{G}}_{g_i,g_j} \neq L^{\mathcal{G}}_{g_j,g_i}.$$

Consequently, the commutative property of $\oplus$ does not hold in $\mathcal{G}$; so $\mathcal{G}$ is not an abelian group. ☑ ■

**Definition 2.28.** Let $p \in \mathbb{N}$ be a prime number. An abelian group $\mathcal{G}$ is said to be an *elementary abelian group* if $|g| = p$ for every non-trivial element $g \in \mathcal{G}$.

**Remark 2.29.** In upcoming sections we will explore a crucial connection between the Cayley table of any finite elementary abelian group, the number of additive permutations of the group, and the number of transversals in the group's representative latin square.

**Table 2.5: An example illustration of Theorem 2.27 for the latin square $L^{(\mathbb{Z}_5,+)}$ that encodes the abelian group $(\mathbb{Z}_5,+)$. The entries of $L^{(\mathbb{Z}_5,+)}$'s main diagonal $\{(0,0,0),(1,1,2),(2,2,4),(3,3,1),(4,4,0)\}$ are marked in blue parentheses. The products located symmetrically, with respect to $L^{(\mathbb{Z}_5,+)}$'s main diagonal, encode the same group element, where the same group elements have the same coloring.**

| $+$ | **0** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|---|
| **0** | (0) | 1 | 2 | 3 | 4 |
| **1** | 1 | (2) | 3 | 4 | 0 |
| **2** | 2 | 3 | (4) | 0 | 1 |
| **3** | 3 | 4 | 0 | (1) | 2 |
| **4** | 4 | 0 | 1 | 2 | (3) |

### 2.3.2 Generalizing from Groups to Quasi-groups

**Definition 2.30.** A set $\mathcal{G} = (\mathcal{G}, \star)$ equipped with a binary operation is said to be a *quasi-group* if the following conditions are satisfied:

- $\mathcal{G}$ is *closed* under the operation: $q_i \star q_j \in \mathcal{G}, \quad \forall q_i, q_j \in \mathcal{G}$.
- The *latin square property* holds: $\forall q_i, q_j \in \mathcal{G}, \quad \exists! x, y \in \mathcal{G}, \quad q_i \star x = q_j$ and $y \star q_i = q_j$.

If $\mathcal{G}$ contains a finite number of elements, then $\mathcal{G}$ is said to be a *finite quasi-group.*

**Remark 2.31.** The unique solution property of Definition 2.30 is known as *the* latin square property because it ensures that each element of $\mathcal{G}$ occurs exactly once in each row and exactly once in each column of the $\mathcal{G}$'s Cayley table; *it is the defining property of all quasi-groups and an elementary property of all groups.* Recall from Chapter 1 that much of the credit for many of the initial results pertaining to this fundamental relationship between quasi-groups and latin squares is given to Schröder and Moufang;

for the reader who is interested in further details we recommend [12, 23, 24] and the references therein. The following quasi-group Theorem 2.32 (as given in [12]) is a generalization of the group Theorem 2.11.

**Theorem 2.32.** *If $\mathcal{G} = (\mathcal{G}, \star)$ is a finite quasi-group and $L^{\mathcal{G}}$ is the unbordered Cayley table of $\mathcal{G}$, then $L^{\mathcal{G}}$ is a latin square.*

***Proof.*** Suppose that $\mathcal{G} = (\mathcal{G}, \star)$ is a finite quasi-group and $L^{\mathcal{G}}$ is the unbordered Cayley table of $\mathcal{G}$. We wish to show that $L^{\mathcal{G}}$ is a latin square. Choose a row $L^{\mathcal{G}}_{q_i,*}$ of $L^{\mathcal{G}}$ indexed by $q_i \in \mathcal{G}$. Now suppose, on the contrary, that two elements in $L^{\mathcal{G}}_{q_i,*}$ are equal. Then there exist two distinct columns of $L^{\mathcal{G}}$, denoted $L^{\mathcal{G}}_{*,q_j}$ and $L^{\mathcal{G}}_{*,q_k}$, such that

$$L^{\mathcal{G}}_{q_i,q_j} = q_i \star q_j = y = q_i \star q_k = L^{\mathcal{G}}_{q_i,q_k}.$$

But then there would exist two distinct solutions to the equation $q_i \star x = y$, which contradicts the axiom of a quasi-group. So it follows that there are no repetitions of the elements in $L^{\mathcal{G}}_{q_i,*}$. Using the same argument for columns, it further follows that there are no repetitions for elements in any $L^{\mathcal{G}}_{*,q_i}$. Consequently $L^{\mathcal{G}}$ is a latin square. ■

**Table 2.6: An example of the Cayley table of the finite quasi-group $\mathcal{G} = (\mathbb{Z}_3, \star)$ of order-3 over the set $\mathbb{Z}_3 = \{0, 1, 2\}$ of integers modulo 3, where $q_i \star q_j = 2q_i + q_j + 1$ for all $q_i, q_j \in \mathcal{G}$.**

| $\star$ | **0** | **1** | **2** |
|---|---|---|---|
| **0** | 1 | 2 | 0 |
| **1** | 0 | 1 | 2 |
| **2** | 2 | 0 | 1 |

.

As we will see in Section 2.4, this fundamental connection between latin squares and quasi-groups is essential for classifying these structures via equivalence classes.

## 2.4 Equivalence Classes

In this section we will consider operations applied to a latin square that yield another latin square. Here, many of the results are from [12].

**Definition 2.33.** Let $\mathcal{G} = (\mathcal{G}, \star)$ and $\mathcal{H} = (\mathcal{H}, \odot)$ be quasi-groups. Let $\alpha, \beta$, and $\gamma$ be one-to-one mappings from $\mathcal{G}$ to $\mathcal{H}$. Then the ordered triple $(\alpha, \beta, \gamma)$ is said to be an *isotopism* if

$$\alpha(g_x) \odot \beta(g_y) = \gamma(g_x \star g_y), \quad \forall g_x, g_y \in \mathcal{G}.$$

In this case $\mathcal{G}$ and $\mathcal{H}$ are said to be *isotopic quasi-groups*.

**Definition 2.34.** Let $\mathcal{G} = (\mathcal{G}, \star)$ and $\mathcal{H} = (\mathcal{H}, \odot)$ be finite isotopic quasi-groups of order-$n$ that are encoded by the respective latin squares $L^{\mathcal{G}}, L^{\mathcal{H}} \in \mathcal{L}^n$. Then $L^{\mathcal{G}}$ and $L^{\mathcal{H}}$ are said to be *isotopic latin squares*, where:

- $\alpha$ is a permutation that operates on the rows of $L^{\mathcal{G}}$,
- $\beta$ is a permutation that operates on the columns of $L^{\mathcal{G}}$, and
- $\gamma$ is a permutation that operates on the elements of $L^{\mathcal{G}}$.

In this case we say that $L^{\mathcal{G}}$ and $L^{\mathcal{H}}$ are in the same *isotopy class*; there exist permutations $\alpha$, $\beta$, and $\gamma$ that transform $L^{\mathcal{G}}$ into $L^{\mathcal{H}}$.

To the best of our knowledge, the age and origin of the concept of isotopy is not known for certain. It is said that this old concept is so “natural” to the subject of latin squares that it often goes unnoticed [12]. The isotopy of latin squares was intentionally applied by Schönhardt in [30] and Baer in [77, 78], and also by Albert [79, 80] working independently (who introduced the isotopy of algebras and borrowed the concept from topology for linear algebra applications) [12].

**Example 2.35.** Let $(\mathbb{Z}_4, +)$ be the finite cyclic group over the set $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ of integers modulo 4 under addition. Then the Cayley table of $(\mathbb{Z}_4, +)$ and the corresponding representative latin square $L^{(\mathbb{Z}_4,+)} \in \mathcal{L}^4$ can be respectively written as

| + | **0** | **1** | **2** | **3** |
|---|---|---|---|---|
| **0** | 0 | 1 | 2 | 3 |
| **1** | 1 | 2 | 3 | 0 |
| **2** | 2 | 3 | 0 | 1 |
| **3** | 3 | 0 | 1 | 2 |

and

| | | | |
|---|---|---|---|
| 0 | 1 | 2 | 3 |
| 1 | 2 | 3 | 0 |
| 2 | 3 | 0 | 1 |
| 3 | 0 | 1 | 2 |

.

Now suppose that

$$\alpha = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 1 & 3 & 0 \end{pmatrix}, \quad \beta = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 3 & 2 & 0 \end{pmatrix}, \quad \text{and} \quad \gamma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

are applied to $L^{(\mathbb{Z}_4,+)}$ to transform it into the latin square $L^{\mathcal{H}} \in \mathcal{L}^4$ that encodes the order-4 quasi-group $\mathcal{H}$, where the Cayley table of $\mathcal{H}$ and the corresponding $L^{\mathcal{H}}$ are respectively written as

| + | **0** | **2** | **3** | **1** |
|---|---|---|---|---|
| **3** | 2 | 0 | 1 | 3 |
| **0** | 3 | 1 | 2 | 0 |
| **2** | 1 | 3 | 0 | 2 |
| **1** | 0 | 2 | 3 | 1 |

and

| | | | |
|---|---|---|---|
| 2 | 0 | 1 | 3 |
| 3 | 1 | 2 | 0 |
| 1 | 3 | 0 | 2 |
| 0 | 2 | 3 | 1 |

.

Then $(\mathbb{Z}_4, +)$ and $\mathcal{H}$ are isotopic quasi-groups while $L^{(\mathbb{Z}_4,+)}$ and $L^{\mathcal{H}}$ are isotopic latin squares.

**Definition 2.36.** Let $\mathcal{G} = (\mathcal{G}, \star)$ and $\mathcal{H} = (\mathcal{H}, \odot)$ be quasi-groups that are isotopic with respect to $(\alpha, \beta, \gamma)$. We say that $(\alpha, \beta, \gamma)$ is an *isomorphism* if $\alpha = \beta = \gamma$. In this case we say that the corresponding latin squares $L^{\mathcal{G}}, L^{\mathcal{H}} \in \mathcal{L}^n$ (that encode $\mathcal{G}$ and $\mathcal{H}$) are *isomorphic* and are in the same *isomorphism class.*

**Example 2.37.** Let $L^{(\mathbb{Z}_4,+)} \in \mathcal{L}^4$ be the latin square from Example 2.35. Now suppose that the permutations $\alpha$, $\beta$, and $\gamma$ with

$$\alpha = \beta = \gamma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$

are applied to $L^{(\mathbb{Z}_4,+)}$ to transform it into the latin square $L^{\mathcal{K}} \in \mathcal{L}^4$ that encodes the order-4 quasi-group $\mathcal{K}$, where the Cayley table of $\mathcal{K}$ and the corresponding $L^{\mathcal{K}}$ are respectively written as

| $+$ | **2** | **3** | **0** | **1** |
|---|---|---|---|---|
| **2** | 3 | 0 | 1 | 2 |
| **3** | 0 | 1 | 2 | 3 |
| **0** | 1 | 2 | 3 | 0 |
| **1** | 2 | 3 | 0 | 1 |

and

| | | | |
|---|---|---|---|
| 3 | 0 | 1 | 2 |
| 0 | 1 | 2 | 3 |
| 1 | 2 | 3 | 0 |
| 2 | 3 | 0 | 1 |

.

Then $(\mathbb{Z}_4, +)$ and $\mathcal{K}$ are isomorphic quasi-groups while $L^{(\mathbb{Z}_4,+)}$ and $L^{\mathcal{K}}$ are isomorphic latin squares.

**Definition 2.38.** A set $\mathcal{G}$ is said to be a *groupoid* if $\mathcal{G}$ has a unary operation ${}^{-1} : \mathcal{G} \to \mathcal{G}$ and a partial function $\star : \mathcal{G} \times \mathcal{G} \rightharpoonup \mathcal{G}$ such that the following properties hold for all $g_1, g_2, g_3 \in \mathcal{G}$:

- *Associativity*: if $g_1 \star g_2$ and $g_2 \star g_3$ are defined, then $(g_1 \star g_2) \star g_3$ and $g_1 \star (g_2 \star g_3)$ are defined and equal.
- *Inverse*: $g_1^{-1} \star g_1$ and $g_1 \star g_1^{-1}$ are defined.
- *Identity*: if $g_1 \star g_2$ is defined, then $g_1 \star g_2 \star g_2^{-1} = g_1$ and $g_1^{-1} \star g_1 \star g_2 = g_2$.

We prove the following four results from [12].

**Theorem 2.39.** *If $\mathcal{G} = (\mathcal{G}, \star)$ is a quasi-group that is isotopic to a groupoid $\mathcal{H} = (\mathcal{H}, \odot)$, then $\mathcal{H}$ is also a quasi-group.*

***Proof.*** Let $\mathcal{G} = (\mathcal{G}, \star)$ be a quasi-group and let $\mathcal{H} = (\mathcal{H}, \odot)$ be a groupoid. Suppose that $\mathcal{G}$ and $\mathcal{H}$ are isotopic. Then by definition

$$\alpha(g_x) \odot \beta(g_y) = \gamma(g_x \star g_y), \quad \forall g_x, g_y \in \mathcal{G}.$$

Take any $a, b \in \mathcal{H}$.

***Claim:*** *There exists a unique $h_x \in \mathcal{H}$ for*

$$a \odot h_x = b. \tag{2.2}$$

Since $\mathcal{G}$ and $\mathcal{H}$ are isotopic, then $\alpha^{-1}(a), \gamma^{-1}(b) \in \mathcal{G}$. Moreover, since $\mathcal{G}$ is a quasi-group, then for arbitrary $a, b \in \mathcal{H}$ there exists a unique $c \in \mathcal{G}$ that is a solution to $\alpha^{-1}(a) \star g_y = \gamma^{-1}(b)$ with $g_y = c \in \mathcal{G}$. Now suppose that $h_x = \beta(c) \in \mathcal{H}$. Then we obtain

$$\begin{aligned} a \odot h_x &= a \odot \beta(c) \\ &= \alpha(\alpha^{-1}(a)) \odot \beta(c) \\ &= \gamma(\alpha^{-1}(a) \star c) \\ &= \gamma(\gamma^{-1}(b)) \\ &= b, \end{aligned}$$

which implies that there always exists a solution $h_x \in \mathcal{H}$ to (2.2). Next, to prove uniqueness, we take $h'_x \in \mathcal{H}$ for (2.2) such that $a \odot h'_x = b$ implies

$$\gamma(\alpha^{-1}(a) \star \beta^{-1}(h'_x)) = b \iff \alpha^{-1}(a) \star \beta^{-1}(h'_x) = \gamma^{-1}(b) \tag{2.3}$$

so $\alpha^{-1}(a) \star g_y = \gamma^{-1}(b)$ is solvable and has a unique solution $g_y = c = \alpha^{-1}(h'_x)$ where $h'_x = \beta(c)$. Therefore, $h'_x = h_x = \beta(c)$ implies that there always exists a unique solution $h'_x = h_x$ to (2.2); so (2.2) is solvable in $\mathcal{H}$. ☑

***Claim:*** *There exists a unique $h_z \in \mathcal{H}$ for*

$$h_z \odot a = b. \tag{2.4}$$

Using a similar argument to the previous claim, we can show that there exists a unique solution $h_z \in \mathcal{H}$ to (2.4); so (2.4) is solvable in $\mathcal{H}$. ☑

Consequently $\mathcal{H}$ is a quasi-group. ■

**Definition 2.40.** Let $\mathcal{G} = (\mathcal{G}, \star)$ be a quasi-group (or groupoid). Let $\sigma$ and $\tau$ be one-to-one mappings where $\sigma, \tau : \mathcal{G} \to \mathcal{G}$. Then the isotope $\mathcal{G}^* = (\mathcal{G}, \otimes)$ given by $g_x \otimes g_y = \sigma(g_x) \star \tau(g_y)$ is said to be a *principal isotope* of $\mathcal{G}$.

**Remark 2.41.** In Definition 2.40 the mappings $\alpha$, $\beta$, and $\gamma$ from Definition 2.33 are replaced with $\sigma^{-1}$, $\tau^{-1}$, and the identity mapping, respectively.

**Theorem 2.42.** *Let $\mathcal{G} = (\mathcal{G}, \star)$ be a quasi-group (or groupoid) and let $\mathcal{H} = (\mathcal{H}, \odot)$ be isotopic to $\mathcal{G}$. Then $\mathcal{H}$ is isomorphic to a principal isotope of $\mathcal{G}$.*

***Proof.*** Let $\mathcal{G} = (\mathcal{G}, \star)$ be a quasi-group (or groupoid) and let $\mathcal{H} = (\mathcal{H}, \odot)$ be isotopic to $\mathcal{G}$. Then there exist the one-to-one, onto mappings $\alpha, \beta, \gamma : \mathcal{G} \to \mathcal{H}$ which define the isotopism between $\mathcal{G}$ and $\mathcal{H}$ such that

$$\alpha(g_x) \odot \beta(g_y) = \gamma(g_x \star g_y), \quad \forall g_x, g_y \in \mathcal{G}.$$

Thus, the fact that $\alpha$, $\beta$, and $\gamma$ are one-to-one, onto mappings (with inverses) implies that $\alpha^{-1} \circ \gamma$ and $\beta^{-1} \circ \gamma$ are also one-to-one, onto mappings.

***Claim:*** *There exists an isotope $\mathcal{G}^* = (\mathcal{G}, \otimes)$ of $\mathcal{G}$.* Now the operation $\otimes$ is given as

$$g_x \otimes g_y = \alpha^{-1}(\gamma(g_x)) \star \beta^{-1}(\gamma(g_y)), \tag{2.5}$$

which implies the existence of a principal isotope $\mathcal{G}^* = (\mathcal{G}, \otimes)$ of $\mathcal{G}$. ☑

***Claim:*** *$(\mathcal{H}, \odot)$ and $(\mathcal{G}^*, \otimes)$ are isomorphic with respect to $\mathcal{G} \overset{\gamma}{\to} \mathcal{H}$.* From (2.5) we obtain

$$\begin{aligned}\gamma(g_x) \odot \gamma(g_y) &= \alpha(\alpha^{-1}(g_x)) \odot \beta(\beta^{-1}(g_y)) \\ &= \gamma(\alpha^{-1}(\gamma(x)) \star \beta^{-1}(\gamma(g_y))) \\ &= \gamma(g_x \otimes g_y),\end{aligned}$$

which implies that $\mathcal{H}$ and $\mathcal{G}^*$ are isomorphic under the mapping $\mathcal{G} \overset{\gamma}{\to} \mathcal{H}$. ☑

Consequently, $\mathcal{H}$ is isomorphic to a principal isotope $\mathcal{G}^*$ of $\mathcal{G}$. ■

**Definition 2.43.** A set $\mathcal{G}$ is said to be a *semi-group* if $\mathcal{G}$ has a binary operation $\star : \mathcal{G} \times \mathcal{G} \to \mathcal{G}$ such that satisfies associativity:

$$(g_1 \star g_2) \star g_3 = g_1 \star (g_2 \star g_3), \quad \forall g_1, g_2, g_3 \in \mathcal{G}.$$

**Lemma 2.44.** *Let $\mathcal{G} = (\mathcal{G}, \star)$ be a groupoid with an identity element and let $\mathcal{H} = (\mathcal{H}, \odot)$ be a semi-group. If $\mathcal{G}$ and $\mathcal{H}$ are isotopic, then $\mathcal{G}$ and $\mathcal{H}$ are also isomorphic.*

**Theorem 2.45.** *If $\mathcal{G} = (\mathcal{G}, \star)$ and $\mathcal{H} = (\mathcal{H}, \odot)$ are isotopic groups, then $\mathcal{G}$ and $\mathcal{H}$ are isomorphic.*

***Proof.*** Let $\mathcal{G} = (\mathcal{G}, \star)$ and $\mathcal{H} = (\mathcal{H}, \odot)$ be isotopic groups. Then by Definition 2.38 it follows that $\mathcal{G}$ is a groupoid with an identity element. Furthermore, by Definition 2.43 it follows that $\mathcal{H}$ is a semi-group. Therefore, Lemma 2.44 implies that $\mathcal{G}$ and $\mathcal{H}$ are isomorphic. ■

**Remark 2.46.** Based on these results, we observe that isotopy is an equivalence relation between quasi-groups (or groupoids) and their representative latin squares. Therefore, for all $n \in \mathbb{N}$, the set $\mathcal{L}^n$ of all order-$n$ latin squares can be partitioned into isotopy classes, such that any two squares in the same class are isotopic, while any two squares that appear in different classes are not isotopic. In [12] it is furthermore shown that, in terms geometry, isotopic quasi-groups are quasi-groups that coordinatize the same 3-net.

The following definition and example figure are based on [55].

**Definition 2.47.** Let $L^{\mathcal{G}} \in \mathcal{L}^n$ be a latin square that encodes the quasi-group $\mathcal{G} = (\mathcal{G}, \star)$ where each ordered triple is of the form $(g_x, g_y, g_z)$ for $g_x, g_y, g_z \in \mathcal{G}$. Let $\mathcal{C} = \{(g_x, g_y, g_z) : L_{g_x,g_y} = g_z\}$. The $(x, y, z)$-*conjugate* of $L^{\mathcal{G}}$ is defined by $L^{\mathcal{G}:(x,y,z)}_{g_x,g_y} = g_z$ for each $(g_x, g_y, g_z) \in \mathcal{C}$. In this case we say that $L^{\mathcal{G}}$ and any such $L^{\mathcal{G}:(x,y,z)}$ are *conjugate equivalent*, where they are in the same *conjugacy class*.

**Figure 2.2: Let $L^{(\mathbb{Z}_4,\star)}$ be an order-4 latin square that encodes the quasi-group $(\mathbb{Z}_4, \star)$ over the symbol set $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. These are the six conjugates of $L^{(\mathbb{Z}_4,\star)}$.**

| | | | |
|---|---|---|---|
| 0 | 3 | 1 | 2 |
| 1 | 2 | 0 | 3 |
| 3 | 0 | 2 | 1 |
| 3 | 1 | 3 | 0 |

$(x, y, z)$-conjugate

| | | | |
|---|---|---|---|
| 0 | 1 | 3 | 2 |
| 3 | 2 | 0 | 1 |
| 1 | 0 | 2 | 3 |
| 2 | 3 | 1 | 0 |

$(y, x, z)$-conjugate

| | | | |
|---|---|---|---|
| 0 | 2 | 1 | 3 |
| 1 | 3 | 0 | 2 |
| 3 | 1 | 2 | 0 |
| 2 | 0 | 3 | 1 |

$(z, y, x)$-conjugate

| | | | |
|---|---|---|---|
| 0 | 1 | 3 | 2 |
| 2 | 3 | 1 | 0 |
| 1 | 0 | 2 | 3 |
| 3 | 2 | 0 | 1 |

$(y, z, x)$-conjugate

| | | | |
|---|---|---|---|
| 0 | 2 | 3 | 1 |
| 2 | 0 | 1 | 3 |
| 1 | 3 | 2 | 0 |
| 3 | 1 | 0 | 2 |

$(x, z, y)$-conjugate

| | | | |
|---|---|---|---|
| 0 | 2 | 1 | 3 |
| 2 | 0 | 3 | 1 |
| 3 | 1 | 2 | 0 |
| 1 | 3 | 0 | 2 |

$(z, x, y)$-conjugate

A latin square has 1, 2, 3, or 6 distinct conjugates [55]. By combining Definitions 2.33, 2.34 and 2.47 one can define the following equivalence relation.

**Definition 2.48.** Let $L^{\mathcal{G}}, L^{\mathcal{H}} \in \mathcal{L}^n$ be latin squares. We say that $L^{\mathcal{G}}$ and $L^{\mathcal{H}}$ are *main class isotopic* if one of them is isotopic to some $L^{\mathcal{K}} \in \mathcal{L}^n$ that is conjugate equivalent to the other. In this case we say that $L^{\mathcal{G}}$ and $L^{\mathcal{H}}$ are *main class equivalent*, where they are in the same *main class*.

**Remark 2.49.** Since each latin square contains either 1, 2, 3, or 6 distinct conjugates, then each conjugacy class contains at either 1, 2, 3, or 6 latin squares. So it follows that each main class contains either 1, 2, 3, or 6 isotopy classes.

From Section 2.1 we recall that $|\mathcal{L}^{n'}|$ is the number of reduced order-$n$ latin squares. The following result was proved in [71].

**Corollary 2.50.** *The number of isomorphism classes, isotopy classes, and main classes of order-$n$ latin squares will be asymptotic to* $\frac{|\mathcal{L}^{n'}|}{n!}$, $\frac{|\mathcal{L}^{n'}|}{n!^3}$, *and* $\frac{|\mathcal{L}^{n'}|}{6n!^3}$, *respectively.*

**Table 2.7: The number of isotopy classes and main classes for latin squares up to order-11; the isotopy class column contains the OEIS Sequence A040082 [3] while the main class column contains the OEIS Sequence A003090 [4].**

| **Order-$n$** | **# Isotopy Classes** | **# Main Classes** |
|---|---:|---:|
| 1 | 1 | 1 |
| 2 | 1 | 1 |
| 3 | 1 | 1 |
| 4 | 2 | 2 |
| 5 | 2 | 2 |
| 6 | 22 | 12 |
| 7 | 564 | 147 |
| 8 | 1 676 267 | 283 657 |
| 9 | 115 618 721 533 | 19 270 853 541 |
| 10 | 208 904 371 354 363 006 | 34 817 397 894 749 939 |
| 11 | 12 216 177 315 369 229 261 482 540 | 2 036 029 552 582 883 134 196 099 |
| 12 | ? | ? |

## 2.5 Computational Construction of Latin Squares

In order to search for latin squares with maximum transversal counts, we first need the ability to efficiently generate data sets of latin squares. More specifically, given some order-$n$ and currently available computational power, we need to develop our own algorithms to rapidly generate:

- The entire $\mathcal{L}^n$ for relatively low orders (ex. for order-($n \leq 5$)).
- A "practical sized" proper subset of $\mathcal{L}^n$ for relatively high orders (ex. data set sizes of no more than 1-4 GB for orders for order-($n \leq 21$)).

There are numerous latin square generation algorithms in the literature [81, 82, 83, 84, 85], but for investigative and learning purposes we create our own algorithms from scratch.

For our attack of the said objectives we design, implement, and test numerous versions of both non-recursive and recursive generation algorithms. Given the current computational and time constraints, we put forth our best effort to continually improve the efficiency, capability, and overall performance of our algorithms in order to obtain bigger latin square data sets of progressively higher orders. Here we discuss our latest (and personal best) algorithms for the generation of latin square data sets, namely:

- the *Non-Preloading Selection-Based Latin Square Generation Algorithm* (NPS-LS-GA), and
- the *Preloading Selection-Based Latin Square Generation Algorithm* (PS-LS-GA).

Note: the NPS-LS-GA and the PS-LS-GA are given in Appendix B.1.1.

The recursive NPS-LS-GA of Algorithm 2.1 (in Appendix B.1.1) is our latest algorithm that is capable of generating data sets of latin squares without skipping any. We implement the NPS-LS-GA in the Java programming language and use it as our primary tool to generate subsets of $\mathcal{L}^n$ up to order-21 on a laptop computer with an Intel® Core™ M-5Y71 1.2 GHz Processor and 8 GB DDR3L SD-RAM equipped with a Linux operating system. Given our current computational resources, we find that the NPS-LS-GA implementation is capable of generating the complete $\mathcal{L}^n$ up to order-5. Beyond that, we use the NPS-LS-GA to generate proper subsets of $\mathcal{L}^n$ up to order-21. We find that the NPS-LS-GA generates 607 order-21 latin squares per second. In Table 2.8 we report the number of latin squares (up to order-21) that we generate using the NPS-LS-GA, which are compared to all known values of the total number of latin squares $|\mathcal{L}^n|$ that are known to exist up to order-11 (i.e. recall Table 2.1) [1, 2]. To assess NPS-LS-GA's generation rate performance, we also use it to generate 100,000 latin square subsets of $\mathcal{L}^n$ up to order-21; see the performance benchmark results in Appendix B.1.3.

After achieving order-21, we continue our computational experiments by adjusting the NPS-LS-GA to see if we could increase generation rates for subsets of $|\mathcal{L}^n|$ up to order-21 and beyond. Given that the symbol selection strategy of the NPS-LS-GA is (theoretically) designed to generate the complete $\mathcal{L}^n$ for a given order-$n$ (without skipping any), we observe the following: the NPS-LS-GA's (non-preloading) symbol selection strategy requires a relatively significant computational cost because it searches for the next available symbol (to insert into the latin square being generated) in order to ensure that no latin squares of $\mathcal{L}^n$ are skipped during the generation process. Upon realizing that the majority of the NPS-LS-GA's computational cost is spent on selecting the next symbol, we come up with a hypothesis on how to possibly modify the NPS-LS-GA with a symbol "preloading" strategy to increase generation rates at the cost of "skipping over" some of the latin squares in $\mathcal{L}^n$ that are appended to the data set; the result of this experimental modification is the PS-LS-GA of Algorithm 2.2 (in Appendix B.1.1).

**Table 2.8: The sizes of the latin square data sets generated by the NPS-LS-GA Java implementation up to order-21.**

| Order-$n$ | Data Set Size<br># Bytes | Data Set Size<br># Latin Squares | # All Latin Squares: $\lvert\mathcal{L}^n\rvert$ |
|---|---:|---:|---:|
| 1 | 9 $B$ | 1 | 1 |
| 2 | 62 $B$ | 2 | 2 |
| 3 | 804 $B$ | 12 | 12 |
| 4 | 66 $KB$ | 576 | 576 |
| 5 | 28 $MB$ | 161 280 | 161 280 |
| 6 | 989 $MB$ | 4 000 000 | 812 851 200 |
| 7 | 1.0 $GB$ | 3 000 000 | 61 479 419 904 000 |
| 8 | 1.2 $GB$ | 2 750 000 | 108 776 032 459 082 956 800 |
| 9 | 1.4 $GB$ | 2 500 000 | 5 524 751 496 156 892 842 531 225 600 |
| 10 | 679 $MB$ | 1 000 000 | 9 982 437 658 213 039 871 725 064 756 920 320 000 |
| 11 | 851 $MB$ | 1 000 000 | 776 966 836 171 770 144 107 444 346 734 230 682 311 065 600 000 |
| 12 | 1.1 $GB$ | 1 000 000 | ? |
| 13 | 1.3 $GB$ | 1 000 000 | ? |
| 14 | 1.5 $GB$ | 1 000 000 | ? |
| 15 | 1.7 $GB$ | 1 000 000 | ? |
| 16 | 2.0 $GB$ | 1 000 000 | ? |
| 17 | 2.3 $GB$ | 1 000 000 | ? |
| 18 | 2.6 $GB$ | 1 000 000 | ? |
| 19 | 2.9 $GB$ | 1 000 000 | ? |
| 20 | 3.2 $GB$ | 1 000 000 | ? |
| 21 | 3.6 $GB$ | 1 000 000 | ? |

Hence, by modifying the selection strategy of the NPS-LS-GA to obtain the PS-LS-GA, we discover that our "preloading hypothesis" is correct: the preloading strategy of the PS-LS-GA enables it to outperform the NPS-LS-GA (in terms of generating subsets of $|\mathcal{L}^n|$) by a significant margin; see the performance benchmark results of the NPS-LS-GA versus the PS-LS-GA in Appendix B.1.3. Interestingly enough, we test the PS-LS-GA up to order-30 and find that it continues to perform relatively well. In practice we find that the PS-LS-GA implementation is capable of generating 2,801 order-21 latin squares per second. Thus, although the PS-LS-GA is approximately 4.6 times faster (and achieves much higher orders) than the NPS-LS-GA, we find that the NPS-LS-GA is the most applicable to this research because it doesn't skip any of the latin squares in $\mathcal{L}^n$. In future work, it would be interesting to further investigate when the PS-LS-GA decides to skip a latin square and which types of latin squares that it may tend to skip.

Upon considering the challenges associated with the task of generating latin squares, let us briefly acknowledge the complexity. Suppose that we have a partially filled latin square where at most $k$ cells of the square remain unfilled in any row or column. *What is the complexity of deciding if such a partially filled latin square is completable?* This is known as the *latin square completion problem* (LS-CP) [86, 87], which concerns the generation of latin squares. In [86] Colbourn proved that if $k$ is free, then the LS-CP is $\mathscr{NP}$-complete. This means that the LS-CP is both $\mathscr{NP}$ (a decision problem that is solvable in polynomial time by a theoretical non-deterministic Turing machine [88]) and $\mathscr{NP}$-hard (every decision problem $\mathscr{A}$ that is in $\mathscr{NP}$ can be reduced to the LS-CP in polynomial time, where one can verify that a given solution to $\mathscr{A}$ is also a solution to the LS-CP in polynomial time [89]). In [87] Easton and Parker tighten Colbourn's result by proving that the LS-CP remains in $\mathscr{NP}$-hard for $k = 3$.

## 2.6 Transversals and Conditions for Existence

Latin square transversals also play a critical role in the important concept of latin square orthogonality and they are a major topic of examination in latin square research [8, 12]. However, a number of basic questions about their properties remain unresolved. For instance, the question regarding the existence of transversals in latin squares is far from being resolved and is an area of active investigation (even if strong additional assumptions are made about the structure of the latin square [8]). Here we survey some known results and conjectures related to transversals. If one is building a cryptographic system, then such results may help one determine which algebraic structures may (or may not) be useful for cryptographic applications. Using our latin square notation, we can restate the transversal Definition 1.13 as follows.

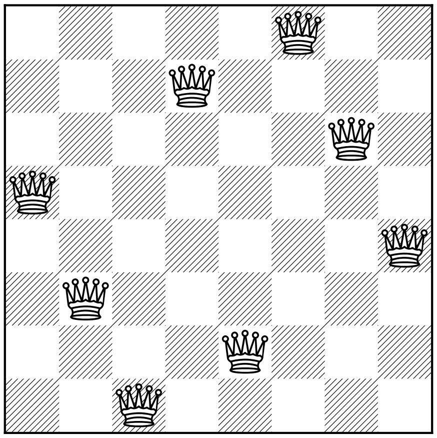
**Definition 2.51.** Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite quasi-group of order-$n$ and let $L^{\mathcal{G}}$ the latin square that encodes $\mathcal{G}$. A diagonal $T \in \mathcal{D}^{L^{\mathcal{G}}}$ of $L^{\mathcal{G}}$ is said to be a *transversal* if each entry $(g_x, g_y, g_z) \in T$ encodes a unique $g_x \in \mathcal{G}$, a unique $g_y \in \mathcal{G}$, and a unique $g_z \in \mathcal{G}$, where the order of $T$ is $|T| = n$. The *set of all transversals of* $L^{\mathcal{G}}$ is denoted by $\mathcal{T}(L^{\mathcal{G}})$, so the *number of transversals of* $L^{\mathcal{G}}$ is denoted by $|\mathcal{T}(L^{\mathcal{G}})|$. For each $(g_x, g_y, g_z) \in T$, we say that $T$ *passes through* the entry $(g_x, g_y, g_z)$.

**Table 2.9: A latin square $L^{(\mathbb{Z}_5,+)}$ which encodes the finite group $(\mathbb{Z}_5, +)$ has 15 transversals. The entries for three of these transversals are marked in red parentheses, blue square brackets, and green angled brackets.**

| + | **0** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|---|
| **0** | (0) | 1 | <2> | 3 | [4] |
| **1** | 1 | [2] | 3 | <(4)> | 0 |
| **2** | 2 | (3) | 4 | [0] | <1> |
| **3** | <[3]> | 4 | 0 | 1 | (2) |
| **4** | 4 | <0> | [(1)] | 2 | 3 |

**Example 2.52.** Consider the classic Eight Queens Puzzle [90]: *Given eight queens, place them on an* $8 \times 8$ *chessboard so that no two queens threaten each other (in other words, no two queens share the same row, column, or diagonal).* See Figure 2.3 for an example solution, where we observe that the placement of the queens (if labeled with eight distinct symbols) represent a transversal of the chessboard.

**Figure 2.3: The only symmetrical solution to the eight queens puzzle of Example 2.52 (except for rotations and reflections of itself). We observe that the placement of the eight queens (if labeled with eight distinct symbols) represent a transversal of the chessboard.**



The following result was initially conjectured by Snevily [91] and proved by Alon [57].

**Theorem 2.53.** *Let $p \in \mathbb{N}$ be an odd prime for the group $(\mathbb{Z}_p, +)$. Take $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_p$ given by $\mathcal{A} = \{a_0, a_1, a_2, \ldots, a_{k-1}\}$ and $\mathcal{B} = \{b_0, b_1, b_2, \ldots, b_{k-1}\}$. Then there exists a permutation $\alpha \in S_k$ such that the sums $a_i + b_{\alpha(i)} \mod p$ for $0 \leq i < k$ are pairwise distinct.*

Theorem 2.53 was further extended in [56]. From this we obtain the following:

**Definition 2.54.** Let $n \in \mathbb{N}$ and let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ be a set of symbols. Take $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_n$ given by $\mathcal{A} = \{a_0, a_1, a_2, \ldots, a_{k-1}\}$ and $\mathcal{B} = \{b_0, b_1, b_2, \ldots, b_{k-1}\}$. Then a permutation $\alpha \in S_k$ is said to be a *good permutation* if the sums $a_i + b_{\alpha(i)}$ mod $p$ for $0 \leq i < k$ are pairwise distinct.

In [58, 59] the authors propose methods for estimating the number of good permutations of a given set of $n$ symbols. When $n$ is odd the number of good permutations is not well understood [58]. For instance, is it possible to accurately predict the number of transversals in latin squares that encode odd order finite groups? This is an example of an open question regarding the number of additive permutations in finite groups.

As we will soon see, a major objective of this section is to show that the number of good permutations of a given finite quasi-group (or group) $\mathcal{G}$ of order-$n$ is equal to the number of transversals across the latin square $L^{\mathcal{G}}$ that encodes $\mathcal{G}$. In other words, we wish to show that a good permutation of a given $\mathcal{G}$ is equivalent to a transversal of $L^{\mathcal{G}}$. Counting the number of good permutations of a given set or group is particularly important for developing computationally secure cryptographic systems for cyber security. Theorem 2.53 and Definition 2.54 indicate that if algebraic structures with "not good permutations" are used to construct a system such as a cryptographic hash function, then there will be more collisions than a system built with good permutations. This motivates us to find latin squares with maximum transversal counts.

**Example 2.55.** Let $L^{(\mathbb{Z}_5,+)}$ be the latin square that encodes the cyclic group $\mathbb{Z}_5 = (\mathbb{Z}_5,+)$ of integers with addition modulo 5. Suppose that we have two permutations $\alpha$ and $\beta$ given by

$$\alpha = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 3 & 1 & 4 & 2 \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 0 & 4 \end{pmatrix},$$

which both encode a distinct transversal of $L^{(\mathbb{Z}_5,+)}$; these are equivalent to the red transversal

$$\{(0,0,0),(2,1,3),(4,2,1),(1,3,4),(3,4,2)\}$$

and the blue transversal

$$\{(3,0,3),(1,1,2),(4,2,1),(2,3,0),(0,4,4)\}$$

marked in Table 2.9. Then the (point-wise) sum

$$\gamma = \alpha + \beta = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0+3 & 3+2 & 1+1 & 4+0 & 2+4 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 0 & 2 & 4 & 1 \end{pmatrix}$$

is itself a permutation that encodes a transversal of $L^{(\mathbb{Z}_5,+)}$; this is equivalent to the green transversal

$$\{(3,0,3),(4,1,0),(0,2,2),(1,3,4),(2,4,1)\}$$

marked in Table 2.9.

**Remark 2.56.** It is known that counting the pairs of permutations over a finite group $(\mathcal{G},\oplus)$ whose point-wise sum is also a permutation is equivalent to counting the number of transversals in the latin square $L^{(\mathcal{G},\oplus)}$.

### 2.6.1 Delta Lemma

In the last several years, significant progress in latin square transversal research has been achieved; much of this progress has resulted from the discovery of a new tool called the "Delta Lemma" [6], which is now being used to confirm and explain numerous classical and modern results regarding transversals. As it turns out, the idea behind the Delta Lemma [6] is a deceptively simple, yet enormously powerful tool for investigating latin square transversals. It simultaneously occurred to two independent research teams in 2005, which eventually led to the publications [92, 93]. In [94, 95, 96, 97, 98, 99, 100] other researchers have used variants of the Delta Lemma to achieve results.

In order apply the Delta Lemma (which is the upcoming Lemma 2.58), it is useful to think of a latin square as being a set of entries, where each entry is an ordered 3-tuple of the form (row, column, symbol) [6]; for this we first recall the ordered 3-tuple latin square notation $(x, y, z) \in \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$ of Definition 2.5 and Example 2.6 of Section 2.2, and then consider the following.

**Definition 2.57.** [**Delta Function**] Let $L^{(\mathbb{Z}_n,+)} \in \mathcal{L}^n$ encode $\mathbb{Z}_n = (\mathbb{Z}_n, +)$. Then the mapping $\Delta : \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ is called the *Delta Function* if $\Delta(x, y, z) = z - x - y \mod n$.

Therefore, using Definition 2.57 and given any row $x$ of $L^{(\mathbb{Z}_n,+)}$, one can iterate over each entry $(x, y_j, z_j)$ of $x$ for $0 \leq j \leq n-1$ to sum $x$'s $\Delta$ values (mod $n$) as [100]

$$\sum_{j=0}^{n-1} \Delta(x, y_j, z_j) = \sum_{j=0}^{n-1} (z_j - x - y_j) = \sum_{j=0}^{n-1} z_j - \sum_{j=0}^{n-1} x - \sum_{j=0}^{n-1} y_j = nx = 0 \mod n,$$

and similarly, given any column $y$ of $L^{(\mathbb{Z}_n,+)}$, one can iterate over each entry $(x_i, y, z_i)$ of $y$ for $0 \leq i \leq n-1$ to sum $x$'s $\Delta$ values as

$$\sum_{i=0}^{n-1} \Delta(x_i, y, z_i) = \sum_{i=0}^{n-1} (z_i - x_i - y_i) = \sum_{i=0}^{n-1} z_i - \sum_{i=0}^{n-1} x_i - \sum_{i=0}^{n-1} y_i = ny = 0 \mod n.$$

Thus, from [6, 100] we obtain the following.

**Lemma 2.58** (**Delta Lemma**). *Let $L^{(\mathbb{Z}_n,+)} \in \mathcal{L}^n$ and let $T \in \mathcal{T}(L^{(\mathbb{Z}_n,+)})$ be a transversal of $L^{(\mathbb{Z}_n,+)}$. Then*

$$\sum_{(x_i,y_i,z_i)\in T} \Delta(x_i, y_i, z_i) = \begin{cases} 0 \mod n & \text{if } n \text{ is odd} \\ \frac{1}{2}n \mod n & \text{if } n \text{ is even.} \end{cases}$$

***Proof.*** Let $L^{(\mathbb{Z}_n,+)} \in \mathcal{L}^n$ possess a transversal $T \in \mathcal{T}(L^{(\mathbb{Z}_n,+)})$. Let $\sum_{t\in T} \Delta(t)$ be the sum of all the $\Delta$-values over each entry of $T$. Then

$$\begin{aligned}
\sum_{t\in T}\Delta(t) &= \sum_{(x_i,y_i,z_i)\in T}\Delta(x_i,y_i,z_i)\\
&= \sum_{i=0}^{n-1}\Delta(x_i,y_i,z_i) \mod n\\
&= \sum_{i=0}^{n-1}(z_i-x_i-y_i) \mod n\\
&= \sum_{i=0}^{n-1}z_i \;-\; \sum_{i=0}^{n-1}x_i \;-\; \sum_{i=0}^{n-1}y_i \quad \mod n.
\end{aligned}$$

Now since

$$\sum_{i=0}^{n-1}z_i=\sum_{i=0}^{n-1}x_i=\sum_{i=0}^{n-1}y_i,$$

then

$$\begin{aligned}
\sum_{i=0}^{n-1}z_i-\sum_{i=0}^{n-1}x_i-\sum_{i=0}^{n-1}y_i \mod n &= \sum_{i=0}^{n-1}z_i-\sum_{i=0}^{n-1}z_i-\sum_{i=0}^{n-1}z_i \mod n\\
&= \sum_{i=0}^{n-1}z_i-2\sum_{i=0}^{n-1}z_i \mod n\\
&= \tfrac{n(n-1)}{2}-2\left(\tfrac{n(n-1)}{2}\right) \mod n\\
&= \tfrac{n(n-1)}{2}-n(n-1) \mod n\\
&= n(n-1)\left(\tfrac{1}{2}-1\right) \mod n\\
&= -\tfrac{1}{2}n(n-1) \mod n.
\end{aligned}$$

At this point, there are two cases to consider.

***Case 1:*** *n is even.* Then $n=2k$ for some $k\in\mathbb{Z}$. So

$$\begin{aligned}
\sum_{t\in T}\Delta(t) &= -\tfrac{1}{2}n(n-1) \mod n\\
&= -\tfrac{1}{2}(2k)(n-1) \mod n\\
&= -k(n-1) \mod n\\
&= (-kn+k) \mod n\\
&= -kn \mod n+k \mod n\\
&= k \mod n\\
&= \tfrac{1}{2}n \mod n. \;☑
\end{aligned}$$

***Case 2:*** *n is odd.* Then $n=2k+1$ for some $k\in\mathbb{Z}$. So

$$\begin{aligned}
\sum_{t\in T}\Delta(t) &= -\tfrac{1}{2}n(n-1) \mod n\\
&= -\tfrac{1}{2}(2k+1)((2k+1)-1) \mod n\\
&= \left(-\tfrac{1}{2}(2k)-\tfrac{1}{2}\right)(2k) \mod n\\
&= \left(-k-\tfrac{1}{2}\right)(2k) \mod n\\
&= \left(-2k^2-\tfrac{1}{2}(2k)\right) \mod n\\
&= (-2k^2-k) \mod n\\
&= -k(2k+1) \mod n\\
&= -kn \mod n\\
&= 0 \mod n. \text{ ☑}
\end{aligned}$$

■

**Example 2.59.** Let $L^{(\mathbb{Z}_5,+)}$ be the latin square that encodes the finite group $(\mathbb{Z}_5,+)$. Let $\{(3,0,3),(4,1,0),(0,2,2),(1,3,4),(2,4,1)\}$ be a transversal of $L^{(\mathbb{Z}_5,+)}$ (the green transversal marked in Table 2.9). We apply the Delta Function $\Delta(x,y,z)$ to each entry $\Delta(x_i,y_i,z_i)$ of this transversal to obtain

$$\begin{aligned}
\Delta(3,0,3) &= 3-3-0 \mod 5 \equiv 0 \mod 5\\
\Delta(4,1,0) &= 0-4-1 \mod 5 \equiv 0 \mod 5\\
\Delta(0,2,2) &= 2-0-2 \mod 5 \equiv 0 \mod 5\\
\Delta(1,3,4) &= 4-1-3 \mod 5 \equiv 0 \mod 5\\
\Delta(2,4,1) &= 1-2-4 \mod 5 \equiv 0 \mod 5
\end{aligned}$$

where

$$\Delta(3,0,3)+\Delta(4,1,0)+\Delta(0,2,2)+\Delta(1,3,4)+\Delta(2,4,1) \equiv 0 \mod 5,$$

which is predicted by the Delta Lemma since 5 is odd.

**Theorem 2.60.** *Let $L^{(\mathbb{Z}_n,+)} \in \mathcal{L}^n$ encode $(\mathbb{Z}_n,+)$. If $n$ is even, then $L^{(\mathbb{Z}_n,+)}$ has no transversals.*

***Proof***. Suppose $L^{(\mathbb{Z}_n,+)} \in \mathcal{L}^n$ encodes $\mathbb{Z}_n = (\mathbb{Z}_n,+)$ where $n$ is even. Since $z = x+y \mod n$ for all $(x,y,z) \in {}^{\{\}}L^{(\mathbb{Z}_n,+)}$, then

$$\begin{aligned}\sum_{z=0}^{n-1} z &= \sum_{x=0}^{n-1} (x+y) \mod n\\ &= \sum_{x=0}^{n-1} x \mod n + \sum_{y=0}^{n-1} y \mod n.\end{aligned}$$

Now by the well-known Faulhaber's formula [101] we know that

$$\sum_{x=0}^{n-1} x = 0+1+2+...+(n-1) = \frac{n(n-1)}{2},$$

which gives

$$\begin{aligned}\sum_{x=0}^{n-1} x \mod n + \sum_{y=0}^{n-1} y \mod n &= \sum_{x=0}^{n-1} x \mod n + \sum_{y=0}^{n-1} y \mod n\\ &= \tfrac{n(n-1)}{2} \mod n + \tfrac{n(n-1)}{2} \mod n\\ &= \left(\tfrac{n(n-1)}{2} + \tfrac{n(n-1)}{2}\right) \mod n\\ &= n(n-1) \mod n.\end{aligned}$$

Therefore,

$$\begin{aligned}\tfrac{n(n-1)}{2} &\equiv n(n-1) \mod n\\ \tfrac{n(n-1)}{2} &\equiv 0 \mod n\\ n\left(\tfrac{n-1}{2}\right) &\equiv 0 \mod n.\end{aligned}$$

Now since $n$ is even, then $n-1$ is odd. So $\frac{n-1}{2}$ is not an integer, implying that $n\left(\frac{n-1}{2}\right)$ is not an integer. As a consequence, $L^{(\mathbb{Z}_n,+)}$ has no transversals; so $\mathcal{T}(L^{(\mathbb{Z}_n,+)}) = \emptyset$ when $n$ is even. ■

The original proof of Theorem 2.60 (with $n$ even) was achieved by Euler and delivered to the St. Petersburg Academy on October 17, 1776 [10]. Thereafter, it was published in Euler's 1849 paper titled *De quadratis magicis* [9, 10]. In fact, Theorem 2.60 was one of the first theorems regarding transversals that was ever proved [6]. Thereafter, the $n$ odd case of Theorem 2.60 was proved after the discovery of the Delta Lemma [6].

The following generalization was proved in [100] by Wanless and Webb.

**Theorem 2.61.** *For any $n \in \mathbb{N}$ with $n \notin \{1,3\}$, there exists some $L \in \mathcal{L}^n$ that contains an entry through which no transversal passes.*

***Proof***. Let $L^{(\mathbb{Z}_n,+)} \in \mathcal{L}^n$ encode $\mathbb{Z}_n = (\mathbb{Z}_n,+)$. If $n$ is even, then Theorem 2.60 implies that $L^{(\mathbb{Z}_n,+)}$ has no transversals. Thus, we may assume that $n$ is odd, and therefore we will consider the two cases of $n \equiv 1 \mod 4$ and $n \equiv 3 \mod 4$.

***Case 1:*** $n \equiv 1 \mod 4$. Then $n \geq 5$ and so we define $L^{(\mathbb{Z}_n,+)}$ as follows; that is, $(x, y, x+y \mod n)$ for each entry of $L^{(\mathbb{Z}_n,+)}$ with the following exceptions:

1. $(0,0,1)$ so $\Delta((0,0,1)) = 1$,
2. $(0,1,0)$ so $\Delta((0,1,0)) = -1$,
3. $(x,0,x+2)$ so $\Delta((x,0,x+2)) = 2$ for all $x = 1,3,\ldots,\frac{n-7}{2}$,
4. $(x,2,x)$ so $\Delta((x,2,x)) = -2$ for all $x = 1,3,\ldots,\frac{n-7}{2}$,
5. $\left(\frac{n-3}{2},0,0\right)$ so $\Delta\left(\left(\frac{n-3}{2},0,0\right)\right) = -\frac{n-3}{2}$,
6. $\left(\frac{n-3}{2},2,\frac{n-3}{2}\right)$ so $\Delta\left(\left(\frac{n-3}{2},2,\frac{n-3}{2}\right)\right) = -2$,
7. $\left(\frac{n-3}{2},\frac{n+3}{2},\frac{n+1}{2}\right)$ so $\Delta\left(\left(\frac{n-3}{2},\frac{n+3}{2},\frac{n+1}{2}\right)\right) = -\frac{n-1}{2}$,
8. $(n-1,1,1)$ so $\Delta((n-1,1,1)) = 1$,
9. $\left(n-1,2,\frac{n+1}{2}\right)$ so $\Delta\left(\left(n-1,2,\frac{n+1}{2}\right)\right) = \frac{n-1}{2}$, and
10. $\left(n-1,\frac{n+3}{2},0\right)$ so $\Delta\left(\left(n-1,\frac{n+3}{2},0\right)\right) = \frac{n-1}{2}$.

Then define the set of "unamended entries" of $L^{(\mathbb{Z}_n,+)}$ as

$$\Omega = \bigcup_{0 \leq x,y \leq n-1} \{(x,y,x+y \mod n)\},$$

where $\Delta(t) = 0$ for all $t \in \Omega$, and the set of "amended entries" of $L^{(\mathbb{Z}_n,+)}$ as

$$\begin{aligned} \Omega' \ = \ & \Big\{(0,0,1),(0,1,0),\left(\tfrac{n-3}{2},0,0\right),\left(\tfrac{n-3}{2},2,\tfrac{n-3}{2}\right),\left(\tfrac{n-3}{2},\tfrac{n+3}{2},\tfrac{n+1}{2}\right), \\ & (n-1,1,1),\left(n-1,2,\tfrac{n+1}{2}\right),\left(n-1,\tfrac{n+3}{2},0\right)\Big\} \\ & \cup \left(\bigcup_{x=1,3,\ldots,\frac{n-7}{2}} \Big\{(x,0,x+2) \cup (x,2,x)\Big\}\right), \end{aligned}$$

where $\Delta(t) \neq 0$ for all $t \in \Omega'$.

Suppose, towards contradiction, that $T \in \mathcal{T}(L^{(\mathbb{Z}_n,+)})$ is a transversal of $L^{(\mathbb{Z}_n,+)}$ such that $T$ passes through the element $t_0 = (x_0, y_0, z_0) = (0, 0, 1)$. Then $\Delta(t_0) = 1 \neq 0$. Now since $t_0 \in T$ with $x_0 = 0$, $y_0 = 0$, and $z_0 = 1$, then for $t_1 \in T$ it must be that $x_1 \neq 0$, $y_1 \neq 0$, and $z_1 \neq 1$. So

$$t_1 \neq t_0, (0,1,0), \left(\frac{n-3}{2}, 0, 0\right), (n-1, 1, 1)$$

and

$$t_1 \neq (x, 0, x+2), \quad \text{for} \quad x = 1, 3, \ldots, \frac{n-7}{2}.$$

Thus, for the candidate choices of $t_1$ it must be that

$$t_1 \in \left(\Omega' \setminus \left\{t_0, (0,1,0), \left(\frac{n-3}{2}, 0, 0\right), (n-1,1,1), (x, 0, x+2\right\}\right) \cup \Omega$$

implies

$$\begin{aligned} t_1 \quad \in \quad & \Big\{(x,2,x), \left(\tfrac{n-3}{2}, 2, \tfrac{n-3}{2}\right), \left(\tfrac{n-3}{2}, \tfrac{n+3}{2}, \tfrac{n+1}{2}\right), \left(n-1, 2, \tfrac{n+1}{2}\right), \\ & \left(n-1, \tfrac{n+3}{2}, 0\right)\Big\} \cup \Omega, \end{aligned}$$

recalling that $(x, 2, x)$ for $x = 1, 3, \ldots, \frac{n-7}{2}$. Since we have that $n \geq 5$ and $n \equiv 1 \mod 4$, then there are four possible choices to consider.

***Case: 1.1*** *Choose* $t_1 = (x_1, y_1, z_1) = \left(\frac{n-3}{2}, 2, \frac{n-3}{2}\right)$. Then

$$\Delta(t_1) = \frac{n-3}{2} - \frac{n-3}{2} - 2 = -2 \neq 0 \implies \Delta(t_0) + \Delta(t_1) = 1 - 2 = -1 \neq 0.$$

Now since $t_1 \in T$ with $x_1 = \frac{n-3}{2}$, $y_1 = 2$, and $z_1 = \frac{n-3}{2}$, then for $t_2 = (x_2, y_2, z_2) \in T$ it follows that $x_2 \neq \frac{n-3}{2}$, $y_2 \neq 2$, and $z_2 \neq \frac{n-3}{2}$ with $t_2 \neq t_0, t_1$. Thus, it must be that $t_2 \in \left\{ \left(n-1, \frac{n+3}{2}, 0\right) \right\} \cup \Omega$. Therefore, we may choose $t_2 = \left(n-1, \frac{n+3}{2}, 0\right)$. Then

$$\Delta(t_2) = 0 - (n-1) - \left(\frac{n+3}{2}\right) = \frac{-3n-1}{2}$$

implies

$$\Delta(t_0) + \Delta(t_1) + \Delta(t_2) = 1 - 2 + \frac{-3n-1}{2} \neq 0.$$

Consequently, for any $t_3 = (x_3, y_3, z_3) \in T$ it must be that $t_3 \in \Omega$. But since

$\Delta(t_0)+\Delta(t_1)+\Delta(t_2)\neq 0$ and $\Delta(t)=0$ for all $t\in\Omega$, then there is no such $t_3\in T,\Omega$ where $\Delta(t_0)+\Delta(t_1)+\Delta(t_2)+\Delta(t_3)=0$. Hence,

$$t_3\in\Omega,T \text{ and } \Delta(t_0)+\Delta(t_1)+\Delta(t_2)+\Delta(t_3)\neq 0 \implies T\notin\mathcal{T}(L^{(\mathbb{Z}_n,+)}),$$

implying that $T$ is not a transversal of $L^{(\mathbb{Z}_n,+)}$—a contradiction. ☑

***Case 1.2:*** *Choose* $t_1=(x_1,y_1,z_1)=\left(\frac{n-3}{2},\frac{n+3}{2},\frac{n+1}{2}\right)$. Then

$$\Delta(t_1)=\frac{n+1}{2}-\frac{n-3}{2}-\frac{n+3}{2}=\frac{-n+1}{2}\neq 0 \implies \Delta(t_0)+\Delta(t_1)=1+\frac{-n+1}{2}\neq 0.$$

Now since $t_1\in T$ with $x_1=\frac{n-3}{2}$, $y_1=\frac{n+3}{2}$, and $z_1=\frac{n+1}{2}$, then for $t_2=(x_2,y_2,z_2)\in T$ it follows that $x_2\neq\frac{n-3}{2}$, $y_2\neq\frac{n+3}{2}$, and $z_2\neq\frac{n+1}{2}$ with $t_2\neq t_0,t_1$. Thus, it must be that $t_2\in\Omega$. But since $\Delta(t_0)+\Delta(t_1)\neq 0$ and $\Delta(t)=0$ for all $t\in\Omega$, then there is no such $t_2\in T,\Omega$ where $\Delta(t_0)+\Delta(t_1)+\Delta(t_2)=0$. Hence,

$$t_2\in\Omega,T \text{ and } \Delta(t_0)+\Delta(t_1)+\Delta(t_2)\neq 0 \implies T\notin\mathcal{T}(L^{(\mathbb{Z}_n,+)}),$$

implying that $T$ is not a transversal of $L^{(\mathbb{Z}_n,+)}$—a contradiction. ☑

***Case 2.3:*** *Choose* $t_1=\left(n-1,2,\frac{n+1}{2}\right)$. Then

$$\begin{aligned}\Delta(t_1) &= \tfrac{n+1}{2}-(n-1)-2=\tfrac{-n-1}{2}\neq 0\\ &\implies \Delta(t_0)+\Delta(t_1)=1+\tfrac{-n-1}{2}\neq 0.\end{aligned}$$

Now since $t_1\in T$ with $x_1=n-1$, $y_1=2$, and $z_1=\frac{n+1}{2}$, then for $t_2=(x_2,y_2,z_2)\in T$ it follows that $x_2\neq n-1$, $y_2\neq 2$, and $z_2\neq\frac{n+1}{2}$ with $t_2\neq t_0,t_1$. Thus, it must be that $t_2\in\Omega$. But since $\Delta(t_0)+\Delta(t_1)+\Delta(t_2)\neq 0$ and $\Delta(t)=0$ for all $t\in\Omega$, then there is no such $t_2\in T,\Omega$ where $\Delta(t_0)+\Delta(t_1)+\Delta(t_2)=0$. So

$$t_2\in\Omega,T \text{ and } \Delta(t_0)+\Delta(t_1)+\Delta(t_2)\neq 0 \implies T\notin\mathcal{T}(L^{(\mathbb{Z}_n,+)}),$$

implying that $T$ is not a transversal of $L^{(\mathbb{Z}_n,+)}$—a contradiction. ☑

***Case 1.4:*** *Choose* $t_1=(x_1,y_1,z_1)=\left(n-1,\frac{n+3}{2},0\right)$. Then

$$\begin{aligned}\Delta(t_1) &= 0-(n-1)-\left(\tfrac{n+3}{2}\right)=\tfrac{-3n-1}{2}\neq 0\\ &\implies \Delta(t_0)+\Delta(t_1)=1+\tfrac{-3n-1}{2}\neq 0.\end{aligned}$$

Now since $t_1 \in T$ with $x_1 = n-1$, $y_1 = \frac{n+3}{2}$, and $z_1 = 0$, then for $t_2 = (x_2, y_2, z_2) \in T$ it follows that $x_2 \neq n-1$, $y_2 \neq \frac{n+3}{2}$, and $z_2 \neq 0$ with $t_2 \neq t_0, t_1$. Thus, it must be that $t_2 \in \left\{ \left(\frac{n-3}{2}, 2, \frac{n-3}{2}\right) \right\} \cup \Omega$. Therefore, we may let $t_2 = \left(\frac{n-3}{2}, 2, \frac{n-3}{2}\right)$. Then

$$\begin{aligned} \Delta(t_2) &= \tfrac{n-3}{2} - \tfrac{n-3}{2} - 2 = -2 \neq 0 \\ &\implies \Delta(t_0) + \Delta(t_1) + \Delta(t_2) = 1 + \tfrac{-3n-1}{2} - 2 \neq 0. \end{aligned}$$

Consequently, for any $t_3 = (x_3, y_3, z_3) \in T$ it must be that $t_3 \in \Omega$. But since $\Delta(t_0) + \Delta(t_1) + \Delta(t_2) \neq 0$ and $\Delta(t) = 0$ for all $t \in \Omega$, then there is no such $t_3 \in T, \Omega$ where $\Delta(t_0) + \Delta(t_1) + \Delta(t_2) + \Delta(t_3) = 0$. Hence,

$$t_3 \in \Omega, T \;\text{ and }\; \Delta(t_0) + \Delta(t_1) + \Delta(t_2) + \Delta(t_3) \neq 0 \implies T \notin \mathcal{T}(L^{(\mathbb{Z}_n,+)}),$$

implying that $T$ is not a transversal of $L^{(\mathbb{Z}_n,+)}$—a contradiction. ☑

***Case 2:*** $n \equiv 3 \mod 4$. Then $n \geq 5$ and so we define $L^{(\mathbb{Z}_n,+)}$ as follows; that is, $(x, y, x+y \mod n)$ for each entry of $L^{(\mathbb{Z}_n,+)}$ with the following exceptions:

1. $(0,0,1)$ so $\Delta((0,0,1)) = 1$,

2. $(0,1,0)$ so $\Delta((0,1,0)) = -1$,

3. $(x,0,x+2)$ so $\Delta((x,0,x+2)) = 2$ for all $x = 1, 3, \ldots, \frac{n-5}{2}$,

4. $(x,2,x)$ so $\Delta((x,2,x)) = -2$ for all $x = 1, 3, \ldots, \frac{n-5}{2}$,

5. $\left(\frac{n-1}{2}, 0, 0\right)$ so $\Delta\left(\left(\frac{n-1}{2}, 0, 0\right)\right) = -\frac{n-1}{2}$,

6. $\left(\frac{n-1}{2}, \frac{n+1}{2}, \frac{n-1}{2}\right)$ so $\Delta\left(\left(\frac{n-1}{2}, \frac{n+1}{2}, \frac{n-1}{2}\right)\right) = \frac{n-1}{2}$,

7. $(n-1,1,1)$ so $\Delta\left((n-1,1,1)\right) = 1$,

8. $\left(n-1, 2, \frac{n-1}{2}\right)$ so $\Delta\left(\left(n-1, 2, \frac{n-1}{2}\right)\right) = \frac{n-3}{2}$, and

9. $\left(n-1, \frac{n+1}{2}, 0\right)$ so $\Delta\left(\left(n-1, \frac{n+1}{2}, 0\right)\right) = -\frac{n-1}{2}$.

Then define the set of "unamended entries" of $L^{(\mathbb{Z}_n,+)}$ as

$$\Omega = \bigcup_{0\le x,y\le n-1} \{(x,y,x+y \mod n)\},$$

where $\Delta(t)=0$ for all $t\in\Omega$, and the set of "amended entries" of $L^{(\mathbb{Z}_n,+)}$ as

$$\begin{aligned}\Omega' \ &= \ \Big\{(0,0,1),(0,1,0),\left(\tfrac{n-1}{2},0,0\right),\left(\tfrac{n-1}{2},\tfrac{n+1}{2},\tfrac{n-1}{2}\right),\\ &\quad (n-1,1,1),\left(n-1,2,\tfrac{n-1}{2}\right),\left(n-1,\tfrac{n+1}{2},0\right)\Big\}\\ &\quad \cup\left(\bigcup_{x=1,3,\ldots,\frac{n-5}{2}}\Big\{(x,0,x+2)\cup(x,2,x)\Big\}\right),\end{aligned}$$

where $\Delta(t)\neq 0$ for all $t\in\Omega'$.

Suppose, towards contradiction, that $T\in\mathcal{T}(L^{(\mathbb{Z}_n,+)})$ is a transversal of $L^{(\mathbb{Z}_n,+)}$ such that $T$ passes through the element $t_0=(x_0,y_0,z_0)=(0,0,1)$. Then $\Delta(t_0)=1\neq 0$. Now since $t_0\in T$ with $x_0=0$, $y_0=0$, and $z_0=1$, then for $t_1\in T$ it must be that $x_1\neq 0$, $y_1\neq 0$, and $z_1\neq 1$. So

$$t_1\neq t_0,(0,1,0),\left(\frac{n-1}{2},0,0\right),(n-1,1,1)$$

and

$$t_1\neq (x,0,x+2),\quad \text{for}\quad x=1,3,\ldots,\frac{n-5}{2}.$$

Thus, for the candidate choices of $t_1$ it must be that

$$\begin{aligned} t_1 \quad &\in \quad \left(\Omega'\setminus\Big\{t_0,(0,1,0),\left(\tfrac{n-1}{2},0,0\right),(n-1,1,1),(x,0,x+2)\Big\}\right)\cup\Omega\\ &\Longrightarrow\\ t_1 \quad &\in \quad \Big\{(x,2,x),\left(\tfrac{n-1}{2},\tfrac{n+1}{2},\tfrac{n-1}{2}\right),\left(n-1,2,\tfrac{n-1}{2}\right),\\ &\quad \left(n-1,\tfrac{n+1}{2},0\right)\Big\}\cup\Omega,\end{aligned}$$

recalling that $(x,2,x)$ for $x=1,3,\ldots,\frac{n-5}{2}$. Since we have that $n\geq 5$ and $n\equiv 1 \mod 4$, then there are four possible choices to consider.

***Case 2.1:*** *Choose* $t_1=(x_1,y_1,z_1)=\left(\frac{n-1}{2},\frac{n+1}{2},\frac{n-1}{2}\right)$. Then

$$\begin{aligned}\Delta(t_1) \quad &= \quad \tfrac{n-1}{2}-\tfrac{n-1}{2}-\tfrac{n+1}{2}=\tfrac{-n-1}{2}\neq 0\\ &\Longrightarrow \quad \Delta(t_0)+\Delta(t_1)=1-\tfrac{-n-1}{2}\neq 0.\end{aligned}$$

Now since $t_1\in T$ with $x_1=\frac{n-1}{2}$, $y_1=\frac{n+1}{2}$, and $z_1=\frac{n-1}{2}$, then for $t_2=(x_2,y_2,z_2)\in T$ it follows that $x_2\neq\frac{n-1}{2}$, $y_2\neq\frac{n+1}{2}$, and $z_2\neq\frac{n-1}{2}$ with $t_2\neq t_0,t_1$. Thus, it must be that

$t_2 \in \Big\{ \Big(n-1, 2, \frac{n-1}{2}\Big), (x,2,x) \Big\} \cup \Omega$. Therefore, we may choose $t_2 = \Big(n-1, 2, \frac{n-1}{2}\Big)$. Then

$$\begin{aligned} \Delta(t_2) \quad &= \quad \frac{n-1}{2} - (n-1) - 2 = \frac{-n+1}{2} - 2 \\ &\implies \Delta(t_0) + \Delta(t_1) + \Delta(t_2) = 1 - 2 + \Big(\frac{-n+1}{2} - 2\Big) \neq 0. \end{aligned}$$

Consequently, for any $t_3 = (x_3, y_3, z_3) \in T$ it must be that $t_3 \in \Omega$ because $y_3 \neq y_2 = 2$ implies that $t_3 \neq (x, 2, x)$. But since $\Delta(t_0) + \Delta(t_1) + \Delta(t_2) \neq 0$ and $\Delta(t) = 0$ for all $t \in \Omega$, then there is no such $t_3 \in T, \Omega$ where $\Delta(t_0) + \Delta(t_1) + \Delta(t_2) + \Delta(t_3) = 0$. Hence,

$$t_3 \in \Omega, T \ \text{ and } \ \Delta(t_0) + \Delta(t_1) + \Delta(t_2) + \Delta(t_3) \neq 0 \implies T \notin \mathcal{T}(L^{(\mathbb{Z}_n,+)}),$$

implying that $T$ is not a transversal of $L^{(\mathbb{Z}_n,+)}$—a contradiction. ☑

***Case 2.2:*** *Choose* $t_1 = (x_1, y_1, z_1) = \Big(n-1, 2, \frac{n-1}{2}\Big)$. Then

$$\begin{aligned} \Delta(t_1) \quad &= \quad (n-1) - 2 - \frac{n-1}{2} = \frac{n-5}{2} \neq 0 \\ &\implies \quad \Delta(t_0) + \Delta(t_1) = 1 + \frac{n-5}{2} \neq 0. \end{aligned}$$

Now since $t_1 \in T$ with $x_1 = n-1$, $y_1 = 2$, and $z_1 = \frac{n-1}{2}$, then for $t_2 = (x_2, y_2, z_2) \in T$ it follows that $x_2 \neq n-1$, $y_2 \neq 2$, and $z_2 \neq \frac{n-1}{2}$ with $t_2 \neq t_0, t_1$. Thus, it must be that $t_2 \in \Omega$. But since $\Delta(t_0) + \Delta(t_1) \neq 0$ and $\Delta(t) = 0$ for all $t \in \Omega$, then there is no such $t_2 \in T, \Omega$ where $\Delta(t_0) + \Delta(t_1) + \Delta(t_2) = 0$. Hence,

$$t_2 \in \Omega, T \ \text{ and } \ \Delta(t_0) + \Delta(t_1) + \Delta(t_2) \neq 0 \implies T \notin \mathcal{T}(L^{(\mathbb{Z}_n,+)}),$$

implying that $T$ is not a transversal of $L^{(\mathbb{Z}_n,+)}$—a contradiction. ☑

***Case 2.3:*** *Choose* $t_1 = (x, 2, x)$. Then

$$\begin{aligned} \Delta(t_1) \quad &= \quad x - x - 2 = -2 \neq 0 \\ &\implies \quad \Delta(t_0) + \Delta(t_1) = 1 + -2 \neq 0. \end{aligned}$$

Now since $t_1 \in T$ with $x_1 = x$, $y_1 = 2$, and $z_1 = x$, then for $t_2 = (x_2, y_2, z_2) \in T$ it follows that $x_2 \neq x$, $y_2 \neq 2$, and $z_2 \neq x$ with $t_2 \neq t_0, t_1$. Thus, it must be that $t_2 \in \Big\{ \Big(\frac{n-1}{2}, \frac{n+1}{2}, \frac{n-1}{2}\Big) \Big\} \cup \Omega$. Therefore, we may choose $t_2 = \Big(\frac{n-1}{2}, \frac{n+1}{2}, \frac{n-1}{2}\Big)$. Then

$$\begin{aligned}\Delta(t_2) \quad &= \quad \tfrac{n-1}{2} - \tfrac{n-1}{2} - \tfrac{n+1}{2} = -\tfrac{n+1}{2} \\ &\Longrightarrow \; \Delta(t_0) + \Delta(t_1) + \Delta(t_2) = 1 - 2 - \tfrac{n+1}{2} \neq 0.\end{aligned}$$

Consequently, for any $t_3 = (x_3, y_3, z_3) \in T$ it must be that $t_3 \in \Omega$. But since $\Delta(t_0) + \Delta(t_1) + \Delta(t_2) \neq 0$ and $\Delta(t) = 0$ for all $t \in \Omega$, then there is no such $t_3 \in T, \Omega$ where $\Delta(t_0) + \Delta(t_1) + \Delta(t_2) + \Delta(t_3) = 0$. Hence,

$$t_3 \in \Omega, T \;\text{ and }\; \Delta(t_0) + \Delta(t_1) + \Delta(t_2) + \Delta(t_3) \neq 0 \implies T \notin \mathcal{T}(L^{(\mathbb{Z}_n,+)}),$$

implying that $T$ is not a transversal of $L^{(\mathbb{Z}_n,+)}$—a contradiction. ☑

Therefore, in the cases of $n \equiv 1 \mod 4$, $n \equiv 3 \mod 4$, and $n \equiv 0 \mod 2$ when $n \geq 4$, we can always find such an $L^{(\mathbb{Z}_n,+)}$ with amended entries where there exists an entry of $L^{(\mathbb{Z}_n,+)}$ for which no transversal passes. Consequently, for every $n > 3$, there exists order-$n$ latin square which contains an entry that is not included in any transversal. ■

The $n \equiv 1 \mod 4$ case of Theorem 2.61 was proved by Mann [102], but the $n \equiv 1 \mod 4$ of Theorem 2.61 was an open problem until the discovery of the Delta Lemma 2.58 [6, 100].

The following result was proved in [103] by Balasubramanian.

**Theorem 2.62.** *If $n \in \mathbb{N}$ is even, then any $L \in \mathcal{L}^n$ possesses an even number of transversals.*

**Remark 2.63.** Let $n \in \mathbb{N}$ be even and consider a latin square $L^{(\mathcal{G},\oplus)} \in \mathcal{L}^n$ that encodes an order-$n$ group $(\mathcal{G}, \oplus)$. If $(\mathcal{G}, \oplus)$ is a cyclic group, then Theorem 2.60 tells us that $L^{(\mathcal{G},\oplus)}$ has zero transversals and equivalently that $(\mathcal{G}, \oplus)$ has zero additive permutations (i.e. see Table 2.18 in Section 2.8)—if we're building a cryptographic system that operates with additive permutations, then we surely wish to avoid using $(\mathcal{G}, \oplus)$ in its construction! On the other hand, if $(\mathcal{G}, \oplus)$ is not a cyclic group, then

Theorem 2.62 tells us that $L^{(\mathcal{G},\oplus)}$ has an even number of transversals and equivalently that $(\mathcal{G},\oplus)$ has an even number of additive permutations—many cryptographic systems for digital computers operate over Galois fields with orders that are powers of 2, which means that the addition groups of such fields will have an even number of additive permutations.

If a latin square's order is odd, then we consider the following conjecture by Ryser [104].

**Conjecture 2.64.** *If $n \in \mathbb{N}$ is odd, then any $L \in \mathcal{L}^n$ possesses an even number of transversals. Each latin square of odd order has at least one transversal.*

Today Conjecture 2.64 remains unproven in general, but relatively recent computational evidence obtained by McKay, McLeod, and Wanless [8] proves that Conjecture 2.64 is true given the following condition:

**Theorem 2.65.** *If $n \in \mathbb{N}$ is odd and $n \leq 9$, then any $L \in \mathcal{L}^n$ possesses at least one transversal.*

### 2.6.2 Hall-Paige Conjecture and Finite Solvable Groups

As it turns out, numerous studies and results regarding latin square transversals have been stated in terms of the following two equivalent concepts for quasi-groups [6].

**Definition 2.66.** Let $\mathcal{G} = (\mathcal{G},\star)$ be a finite quasi-group. A permutation (and biunique mapping) $\theta : \mathcal{G} \to \mathcal{G}$ is said to be a *complete mapping* if the biunique mapping $\eta : \mathcal{G} \to \mathcal{G}$ defined by $\eta(g_x) = g_x \star \theta(g_x)$ for all $g_x \in \mathcal{G}$ is also a permutation. In this case, $\eta$ is said to be an *orthomorphism.*

In [102] Mann originally introduced the notion of complete mappings for groups, yet Definition 2.66 works just as well for quasi-groups [6].

The following fact from [6] implies that all of the latin square transversal results (ex. of this thesis or any literature result pertaining to latin square transversals) can be restated in terms of results pertaining to complete mappings and orthomorphisms of quasi-groups.

**Theorem 2.67.** *Let $\mathcal{G} = (\mathcal{G}, \bullet)$ be a finite quasi-group of order-$n$ and let $L^{\mathcal{G}} \in \mathcal{L}^n$ encode $\mathcal{G}$. Then $\mathcal{G}$ has:*

1. *A complete mapping $\theta : \mathcal{G} \to \mathcal{G}$ if and only if $L^{\mathcal{G}}$ has a transversal (that is, we can locate a transversal by selecting, in each row $L^{\mathcal{G}}_{g_x,*}$, the entry $L^{\mathcal{G}}_{g_x,\theta(g_x)}$ in column $L^{\mathcal{G}}_{*,\theta(g_x)}$).*
2. *An orthomorphism $\eta : \mathcal{G} \to \mathcal{G}$ if and only if $L^{\mathcal{G}}$ has a transversal (that is, we can locate a transversal by selecting, in each row $L^{\mathcal{G}}_{g_x,*}$, the entry $L^{\mathcal{G}}_{g_x,\eta(g_x)}$ in column $L^{\mathcal{G}}_{*,\eta(g_x)}$).*

**Remark 2.68.** Counting the number of complete mappings in a finite group $(\mathcal{G}, \oplus)$ is equivalent to:

- Counting the number of additive permutations over $(\mathcal{G}, \oplus)$.
- Counting the number of transversals in the latin square $L^{(\mathcal{G},\oplus)}$.

**Definition 2.69.** Let $\mathcal{G} = (\mathcal{G}, \bullet)$ be a finite quasi-group of order-$n$. Then $\mathcal{G}$ is said to be an *admissible quasi-group* if $\mathcal{G}$ possesses a complete mapping (or equivalently an orthomorphism). Similarly, if $\mathcal{G}$ is a group, then $\mathcal{G}$ is said to be an *admissible group*. In other words, $\mathcal{G}$ is admissible if and only if $\mathcal{G}$'s representative $L^{\mathcal{G}} \in \mathcal{L}^n$ possesses a transversal.

The “Hall-Paige Conjecture” aims to identify conditions in which a finite group $\mathcal{G}$ will possess a complete mapping, or equivalently conditions in which the latin square $L^{\mathcal{G}}$ that encodes $\mathcal{G}$ will possess a transversal [105]. In this section, we systematically survey existing literature results that are related to the Hall-Paige Conjecture (identified as the upcoming Conjecture 2.87).

In [106] Paige first proved the following result.

**Lemma 2.70.** *Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite group of order-n and let $L^{\mathcal{G}} \in \mathcal{L}^n$ encode $\mathcal{G}$. If $L^{\mathcal{G}}$ has a transversal, then there exists some ordering of the elements of $\mathcal{G}$, say $g_1, g_2, \dots, g_i, \dots, g_n$, which yields the trivial product $g_1 \oplus g_2 \oplus \cdots \oplus g_i \oplus \dots g_n = e$.*

***Proof.*** Suppose that $L^{\mathcal{G}}$ has a transversal $T$ (or equivalently assume that $\mathcal{G}$ is admissible). Then Theorem 2.67 implies that there is a complete mapping $g_i \to \theta_T(g_i)$ of $\mathcal{G}$. Without loss of generality we may assume $\theta_T(e) = \eta_T(e) = e$ as the identity. First, consider $g_1 \oplus \theta_T(g_1)$ with $g_1 \neq e$. Then

$$\begin{aligned} g_1 \oplus \theta_T(g_1) \neq e \quad &\Longrightarrow \quad g_1^{-1} \neq \theta_T(g_1) \;\text{ and }\; \theta_T(g_1)^{-1} \neq g_1 \\ &\Longrightarrow \quad \theta_T(g_1)^{-1} \in \mathcal{G} \setminus \{e, g_1\}. \end{aligned}$$

Next we choose $g_2 = \theta_T(g_1)^{-1}$ to form the product

$$g_1 \oplus \theta_T(g_1) \oplus g_2 \oplus \theta_T(g_2),$$

where $\theta_T(g_1) \oplus g_2 = e$. Thereafter, we repeat this step to subsequently obtain

$$\begin{aligned} g_2 \oplus \theta_T(g_2) \neq e \quad &\Longrightarrow \quad g_2^{-1} \neq \theta_T(g_2) \;\text{ and }\; \theta_T(g_2)^{-1} \neq g_2 \\ &\Longrightarrow \quad \theta_T(g_2)^{-1} \in \mathcal{G} \setminus \{e, g_1, \theta_T(g_1), g_2\}. \end{aligned}$$

Next we choose $g_3 = \theta_T(g_2)^{-1}$ to form the product

$$g_1 \oplus \theta_T(g_1) \oplus g_2 \oplus \theta_T(g_2) \oplus g_3 \oplus \theta_T(g_3),$$

where $\theta_T(g_1) \oplus g_2 \oplus \theta_T(g_2) \oplus g_3 = e$. We inductively repeat this step to eventually achieve the trivial product

$$g_1 \oplus \theta_T(g_1) \oplus g_2 \oplus \theta_T(g_2) \oplus g_3 \oplus \theta_T(g_3) \oplus ... \oplus g_k \oplus \theta_T(g_k) = e, \tag{2.6}$$

where $g_i^{-1}(i = 2, 3, ..., k) = \theta_T(g_{i-1})^{-1}$ and $g_1^{-1} = \theta_T(g_k)$. Now in the case that $k < n$, then we choose $g_{k+1}$ for $g_{k+1} \oplus \theta_T(g_{k+1})$ and inductively repeat the procedure until we ultimately achieve a product similar to (2.6). Therefore, since $g_i \to \theta_T(g_i)$ with $g_i \oplus \theta_T(g_i) \equiv \eta_T(g_i)$ we obtain

$$\begin{aligned} g_1 \oplus \theta_T(g_1) \oplus g_2 \oplus \theta_T(g_2) \oplus g_3 \oplus \theta_T(g_3) \oplus ... \oplus z_n \oplus \theta_T(z_n) &= e \\ \eta_T(g_1) \oplus \eta_T(g_2) \oplus \eta_T(g_3) \oplus ... \oplus \eta_T(z_n) &= e, \end{aligned}$$

where each $\eta_T(g_i) = g_i \oplus \theta_T(g_i)$ is distinct (because if they were not distinct then the equality of two such products would imply that $\theta_T(g_i) = \theta_T(g_j)$ or $i = j$). ■

Before we move on to the next main result (of the upcoming Lemma 2.79), we must introduce some preliminary definitions and results from [107].

**Definition 2.71.** Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a group. Then $\mathcal{G}$ is said to be a *solvable group* if there exist subgroups $\mathcal{G}_0, \mathcal{G}_1, \mathcal{G}_2, \dots, \mathcal{G}_k \subset \mathcal{G}$ such that

$$\{e\} = \mathcal{G}_0 < \mathcal{G}_1 < \mathcal{G}_2 < \cdots < \mathcal{G}_k = \mathcal{G},$$

where $\mathcal{G}_{i-1}$ is normal in $\mathcal{G}$ and $\mathcal{G}_i/\mathcal{G}_{i-1}$ is an abelian group for $i = 1, 2, \dots, k$.

**Definition 2.72.** Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite group and let $p$ be a prime number. Then $\mathcal{G}$ is said to be a *p-group* if, for all $g \in \mathcal{G}$, there exists an integer $m \geq 0$ such that $|g| = p^m$.

**Definition 2.73.** Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite group and let $\mathcal{H}$ be a subgroup of $\mathcal{G}$. Let $p$ be a prime number and furthermore suppose that $\mathcal{H}$ is a $p$-group (a $p$-subgroup of $\mathcal{G}$). Then $\mathcal{H}$ is said to be a *Sylow p-subgroup* of $\mathcal{G}$ if $\mathcal{H}$ is not a proper subgroup of any other $p$-subgroup of $\mathcal{G}$; that is, $\mathcal{H}$ is a *maximal* $p$-subgroup of $\mathcal{G}$.

In [108] the following result was achieved by Lagrange.

**Theorem 2.74** (***Lagrange***)**.** *If $\mathcal{G} = (\mathcal{G}, \oplus)$ is a finite group with a subgroup $\mathcal{H} \leq \mathcal{G}$, then $|\mathcal{H}|$ divides $|\mathcal{G}|$.*

In [109] the following result was achieved by Sylow.

**Theorem 2.75** (***Sylow***)**.** *Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite group. Let $p$ be a prime with multiplicity $n$. If $p$ divides $|\mathcal{G}|$, then there exists a Sylow $p$-subgroup $\mathcal{P} \leq \mathcal{G}$ where $|\mathcal{P}| = p^n$.*

**Definition 2.76.** Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite group with subgroups $\mathcal{H}, \mathcal{K} \leq \mathcal{G}$. Then $\mathcal{K}$ is said to be the *complement* of $\mathcal{H}$ in $\mathcal{G}$ if

$$\mathcal{G} = \mathcal{H} \oplus \mathcal{K} = \{h \oplus k : h \in \mathcal{H}, k \in \mathcal{K}\} \text{ and } \mathcal{H} \cap \mathcal{K} = \{e\}.$$

Furthermore, if $\mathcal{H}$ is a Sylow $p$-subgroup, then $\mathcal{K}$ is said to be a *$p$-complement subgroup* of $\mathcal{G}$ (or equivalently if $|\mathcal{K}|$ is relatively prime to $p$ and $[\mathcal{G} : \mathcal{K}] = p^m$ for some $m \in \mathbb{N}$).

**Definition 2.77.** Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a group. An element $t \in \mathcal{G}$ is said to be an *involution* if $t^2 = e$; that is, $t$ has order $|t| = 2$. An element $g \in \mathcal{G}$ is said to be an *strongly real* if there is an involution $t$ with $g^t = t^{-1} \oplus g \oplus t$; by definition, every involution is strongly real.

A standard group theory result (i.e. Proposition 10.20 in Section 10 of [110]) is the following.

**Lemma 2.78.** *If $\mathcal{P}$ is a non-trivial $p$-group, then the center $Z(\mathcal{P})$ of $\mathcal{P}$ is a non-trivial subgroup.*

The following result includes the first direct, elementary proof by Vaughan-Lee and Wanless [105], which builds on the results originally proved by Hall and Paige [107].

**Lemma 2.79.** *Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite group of order-$n$. Then the following conditions are equivalent:*

*(i) There exists some ordering of the elements of $\mathcal{G}$, say $g_1, g_2, \ldots, g_i, \ldots, g_n$, which yields the trivial product $g_1 \oplus g_2 \oplus \cdots \oplus g_i \oplus \cdots \oplus g_n = e$.*

*(ii) Any Sylow 2-subgroup $\mathcal{P}$ of $\mathcal{G}$ is trivial or non-cyclic.*

***Proof***. Let $\mathcal{P}$ be a Sylow 2-subgroup of $\mathcal{G}$. The objectives of this proof strategy are as follows:

For $(ii) \implies (i)$, we first wish to show that if $\mathcal{P}$ is trivial or non-cyclic, then we can list the elements $\{g_1, g_2, \ldots, g_i, \ldots, g_n\}$ of $\mathcal{G}$ to obtain the trivial product

$$g_1 \oplus g_2 \oplus \cdots \oplus g_i \oplus \cdots \oplus g_n = e. \tag{2.7}$$

For $(i) \implies (ii)$, we wish to show, via proof-by-contrapositive, that if $\mathcal{P}$ is non-trivial and cyclic, and if $t$ is the unique involution element in $\mathcal{P}$, then we can list the elements $\{g_1, g_2, \ldots, g_i, \ldots, g_n\}$ of $\mathcal{G}$ to obtain the involution product

$$g_1 \oplus g_2 \oplus \cdots \oplus g_i \oplus \cdots \oplus g_n = t. \tag{2.8}$$

***Case 1:*** *Suppose that $\mathcal{P} = \{e\}$ is trivial.* First, we wish to show that $\mathcal{G}$ has no involutions. If we suppose, for a moment, that 2 is a divisor of $|\mathcal{G}|$, then Sylow's Theorem 2.75 implies that $\mathcal{G}$ has a non-trivial Sylow 2-subgroup $\mathcal{P}$. Therefore, since $\mathcal{P}$ is trivial by hypothesis, then $|\mathcal{G}|$ is not divisible by 2; so $|\mathcal{G}|$ is odd. Hence, since no non-trivial element of $\mathcal{G}$ is its own inverse, then $\mathcal{G}$ has an even number of non-trivial elements. Thus, we can list the elements of $\mathcal{G}$ so that each $g_i \in \mathcal{G} \setminus \mathcal{P}$ is "adjacently paired" with its inverse $g_i^{-1}$ in the list; in other words, we can write $\mathcal{G}$ as the union of a list of disjoint inverse pairs as

$$\mathcal{G} = \{e, e^{-1}\} \cup \{g_1, g_1^{-1}\} \cup \{g_2, g_2^{-1}\} \cup \cdots \cup \{g_n, g_n^{-1}\}$$

to obtain the trivial product

$$g_1 \oplus g_1^{-1} \oplus g_2 \oplus g_2^{-1} \oplus \cdots \oplus g_n \oplus g_n^{-1} = e.$$

So we are done for the $\mathcal{P} = \{e\}$ case of $(ii) \Longrightarrow (i)$. ☑

***Case 2:*** *Suppose that $\mathcal{P}$ is non-trivial.* Since $\mathcal{P}$ is a 2-group, then the order of each element in $\mathcal{P}$ is a power of 2 and therefore Lagrange's Theorem 2.74 implies that every subgroup of $\mathcal{P}$ is a 2-subgroup. Let

$$Z(\mathcal{P}) = \{z \in \mathcal{P} : \forall g_i \in \mathcal{P},\ z \oplus g = g \oplus z\}$$

be the center of $\mathcal{P}$; $Z(\mathcal{P})$ is the set of elements that commute with every element of $\mathcal{P}$. Now since $\mathcal{P}$ is non-trivial, it follows that $Z(\mathcal{P})$ is non-trivial by Lemma 2.78. Moreover, since $|\mathcal{P}|$ is a power of 2, then 2 is a prime factor of $|\mathcal{P}|$ so Theorem 2.75 guarantees the existence of an order-2 subgroup of $\mathcal{P}$, which is also a subgroup of $Z(\mathcal{P})$; so there exists an involution $t \in Z(\mathcal{P})$. By definition we have that $|t| = 2$, so let

$$C_{\mathcal{G}}(t) = \{g_i \in \mathcal{G} : g_i \oplus t = t \oplus g_i\} \tag{2.9}$$

be the centralizer of $t \in \mathcal{G}$; $C_{\mathcal{G}}(t)$ is the set of all elements in $\mathcal{G}$ that commute with $t$. Therefore, since $\mathcal{P}$ is a non-trivial 2-group and $t \in Z(\mathcal{P})$, it follows that

$$\forall g_i \in \mathcal{P},\ t \oplus g_i = g_i \oplus t \implies \mathcal{P} \subseteq C_{\mathcal{G}}(t) \implies \mathcal{P} \leq C_{\mathcal{G}}(t),$$

so $\{e\} \leq Z(P) \leq P \leq C_{\mathcal{G}}(t) \leq \mathcal{G}$. From this point forward, we will break the remainder of the proof up into the following two "sub-cases" (namely Case 2.1 and Case 2.2), which depend on whether or not $\mathcal{C}_{\mathcal{G}}(t)$ is a proper subgroup of $\mathcal{G}$.

***Case 2.1:*** *Suppose that $\mathcal{C}_{\mathcal{G}}(t)$ is a proper subgroup of $\mathcal{G}$.* Then we consider the following two "sub-sub-cases" (namely Case 2.1.1 and Case 2.1.2), which depend on whether or not $\mathcal{P}$ is cyclic.

***Case 2.1.1:*** *Suppose that $\mathcal{P}$ is non-cyclic.* Since $\mathcal{C}_{\mathcal{G}}(t)$ from (2.9) is a group, then for all $c_i \in \mathcal{C}_{\mathcal{G}}(t)$ there exists a unique $c_i^{-1}$. So we start by applying induction to the elements of $\mathcal{C}_{\mathcal{G}}(t)$ to partition it into the pairwise disjoint sets of inverse pairs

$$\mathcal{C}_{\mathcal{G}}(t) = \{c_1, c_1^{-1}\} \cup \{c_2, c_2^{-1}\} \cup \cdots \cup \{c_i, c_i^{-1}\} \cup \cdots \cup \{c_l, c_l^{-1}\}$$

to obtain the trivial product

$$\prod_{i=1}^{l}(c_i \oplus c_i^{-1}) = (c_1 \oplus c_1^{-1}) \oplus \cdots \oplus (c_i \oplus c_i^{-1}) \oplus \cdots \oplus (c_l \oplus c_l^{-1}) = e,$$

where we let $\mathscr{L}_{\mathcal{C}_{\mathcal{G}}(t)}$ denote the list of the elements in the product $\prod_{i=1}^{l}(c_i \oplus c_i^{-1}) = e$ as

$$\mathscr{L}_{\mathcal{C}_{\mathcal{G}}(t)} : c_1, c_1^{-1}, c_2, c_2^{-1}, \ldots, c_i, c_i^{-1}, \ldots, c_l, c_l^{-1}. \tag{2.10}$$

Next, in order to similarly apply induction to the elements of $\mathcal{G} \setminus \mathcal{C}_{\mathcal{G}}(t)$ to obtain desired products, we first partition $\mathcal{G} \setminus \mathcal{C}_{\mathcal{G}}(t)$ into the two disjoint sets

$$\mathcal{U} = \{g_i \in \mathcal{G} \setminus \mathcal{C}_{\mathcal{G}}(t) : g_i^2 \neq e\} \;\text{ and }\; \mathcal{V} = \{g_i \in \mathcal{G} \setminus \mathcal{C}_{\mathcal{G}}(t) : g_i^2 = e\}.$$

First, we consider the (non-involution) elements of $\mathcal{U} \subset \mathcal{G} \setminus \mathcal{C}_{\mathcal{G}}(t)$. For each $u_i \in \mathcal{U}$ (all with $|u_i| \neq 2$ and $u_i \neq u_i^{-1}$) we have

$$e = e^{|u_i|} = (u_i \oplus u_i^{-1})^{|u_i|} = u_i^{|u_i|} \oplus (u_i^{-1})^{|u_i|} = e \oplus (u_i^{-1})^{|u_i|} = (u_i^{-1})^{|u_i|}$$

which implies that $|u_i| = |u_i^{-1}|$ and $u_i^{-1} \in \mathcal{U}$. So for all $u_i \in \mathcal{U}$ there exists a unique $u_i^{-1} \in \mathcal{U}$ where $u_i \neq u_i^{-1}$; this result allows us partition $\mathcal{U}$ into pairwise disjoint sets of inverse pairs

$$\mathcal{U} = \{u_1, u_1^{-1}\} \cup \{u_2, u_2^{-1}\} \cup \cdots \cup \{u_i, u_i^{-1}\} \cup \cdots \cup \{u_k, u_k^{-1}\}$$

to obtain the trivial product as

$$\prod_{i=1}^{k}(u_i \oplus u_i^{-1}) = (u_1 \oplus u_1^{-1}) \oplus \cdots \oplus (u_i \oplus u_i^{-1}) \oplus \cdots \oplus (u_k \oplus u_k^{-1}) = e,$$

where we let $\mathscr{L}_{\mathcal{U}}$ denote the list of the elements in the product $\prod_{i=1}^{k}(u_i \oplus u_i^{-1}) = e$ as

$$\mathscr{L}_{\mathcal{U}} : u_1, u_1^{-1}, u_2, u_2^{-1}, \ldots, u_i, u_i^{-1}, \ldots, u_l, u_l^{-1}. \tag{2.11}$$

Second, we consider the (involution) elements of $\mathcal{V} \subset \mathcal{G} \setminus \mathcal{C}_{\mathcal{G}}(t)$. For each $v_i \in \mathcal{V}$ (all with $|v_i| = 2$ and $v_i = v_i^{-1}$) we know that

$$\begin{aligned} v_i &= v_i \\ &= e^{-1} \oplus v_i \oplus e \\ &= (t^2)^{-1} \oplus v_i \oplus t^2 && // \text{ since } e = t^2 \\ &= t^{-2} \oplus v_i \oplus t^2 \\ &= (t^{-1} \oplus t^{-1}) \oplus v_i \oplus (t \oplus t) \\ &= t^{-1} \oplus (t^{-1} \oplus v_i \oplus t) \oplus t \\ &= t^{-1} \oplus (v_i^t) \oplus t && // \text{ by Definition 2.77} \\ &= (v_i^t)^t \end{aligned}$$

which implies

$$v_i \in \mathcal{V} \implies v_i = v_i^{-1} = (v_i^t)^t \in \mathcal{V}.$$

Next, since $v_i \in \mathcal{V} \subset G \setminus C_{\mathcal{G}}(t)$ implies $v_i \notin C_{\mathcal{G}}(t)$, we have that

$$\begin{aligned} v_i \oplus t &\neq t \oplus v_i \\ t^{-1} \oplus v_i \oplus t &\neq v_i \\ v_i^t &\neq v_i. \end{aligned}$$

Moreover

$$\begin{aligned} (v_i^t)^2 &= v_i^t \oplus v_i^t \\ &= (t^{-1} \oplus v_i \oplus t) \oplus (t^{-1} \oplus v_i \oplus t) \\ &= t^{-1} \oplus v_i \oplus (t \oplus t^{-1}) \oplus v_i \oplus t \\ &= t^{-1} \oplus v_i \oplus e \oplus v_i \oplus t \\ &= t^{-1} \oplus (v_i \oplus v_i) \oplus t \\ &= t^{-1} \oplus e \oplus t \\ &= t^{-1} \oplus t \\ &= e, \end{aligned}$$

which implies

$$v_i \in \mathcal{V} \implies v_i^t \in \mathcal{V}.$$

Therefore, for all $v_i \in \mathcal{V}$ there exists a unique $v_i^t \in \mathcal{V}$ with $v_i^t \neq v_i$; this result allows us to partition $\mathcal{V}$ into the disjoint sets of pairs

$$\mathcal{V} = \{v_1, v_1^t\} \cup \{v_2, v_2^t\} \cup \cdots \cup \{v_i, v_i^t\} \cup \cdots \cup \{v_m, v_m^t\}.$$

Next, for each $v_i \in \mathcal{V}$ we have

$$\begin{aligned} v_i^t &= t^{-1} \oplus v_i \oplus t \\ t \oplus v_i^t &= v_i \oplus t \\ v_i^{-1} \oplus t \oplus v_i^t &= t \\ v_i \oplus t \oplus v_i^t &= t \qquad\qquad // \text{ since } v_i = v_i^{-1} \end{aligned}$$

which permits us to obtain the involution product

$$\begin{aligned} v_1 \oplus t \oplus v_1^t &= t \\ v_1 \oplus (v_2 \oplus t \oplus v_2^t) \oplus v_1 &= t \\ \vdots &= \vdots \\ v_1 \oplus (v_2 \oplus (\dots (v_m \oplus t \oplus v_m^t) \dots) \oplus v_2^t) \oplus v_1^t &= t, \end{aligned} \tag{2.12}$$

where we let $\mathscr{L}_\mathcal{V}$ denote the list of the elements in the product of (2.12) as

$$\mathscr{L}_\mathcal{V} : v_1, v_2, \dots, v_m, t, v_m^t, \dots, v_2^t, v_1^t. \tag{2.13}$$

Next, we will combine the lists $\mathscr{L}_{C_\mathcal{G}(t)}$ of eq. (2.10), $\mathscr{L}_\mathcal{U}$ of eq. (2.11), and $\mathscr{L}_\mathcal{V}$ of eq. (2.13), in a specific way in order to obtain the desired trivial product. For this we insert $v_1, v_2, \dots, v_m$ of $\mathscr{L}_\mathcal{V}$ into $\mathscr{L}_{C_\mathcal{G}(t)}$ immediately before $t$, and we insert $v_m^t, \dots, v_2^t, v_1^t$ of $\mathscr{L}_\mathcal{V}$ into $\mathscr{L}_{C_\mathcal{G}(t)}$ immediately after $t$ to obtain the product

$$\overbrace{c_1 \oplus c_2 \oplus \dots}^{\mathscr{L}_{C_\mathcal{G}(t)}} \oplus \overbrace{v_1 \oplus v_2 \oplus \cdots \oplus v_m}^{\mathscr{L}_\mathcal{V}} \oplus \overbrace{\ t\ }^{\mathscr{L}_{C_\mathcal{G}(t)}} \oplus \overbrace{v_m^t \oplus \cdots \oplus v_2^t \oplus v_1^t}^{\mathscr{L}_\mathcal{V}} \oplus \overbrace{\cdots \oplus c_l}^{\mathscr{L}_{C_\mathcal{G}(t)}} = e, \tag{2.14}$$

which remains trivial, where we let $\mathscr{L}_{\mathcal{V},C_\mathcal{G}(t)}$ denote the list of the elements in the product of (2.14) as

$$\mathscr{L}_{\mathcal{V},C_\mathcal{G}(t)} : c_1, \dots, v_1, \dots v_m, t, v_m^t, \dots, v_1^t, \dots c_l. \tag{2.15}$$

Then we append the elements of $\mathscr{L}_\mathcal{U}$ to the right-hand side of $\mathscr{L}_{\mathcal{V},C_\mathcal{G}(t)}$ from (2.14) to obtain the desired trivial product

$$\overbrace{c_1 \oplus \cdots \oplus v_1 \oplus \cdots \oplus v_m \oplus t \oplus v_m^t \oplus \cdots \oplus v_1^t \oplus \cdots \oplus c_l}^{\mathscr{L}_{\mathcal{V},C_\mathcal{G}}(t)} \oplus \overbrace{u_1 \oplus u_1^{-1} \oplus \cdots \oplus u_k \oplus u_k^{-1}}^{\mathscr{L}_\mathcal{U}} = e.$$

So we've shown that when $\mathcal{C}_G(t) < \mathcal{G}$ and $\mathcal{P}$ is non-trivial and non-cyclic, there exists an ordering of the elements of $\mathcal{G}$ that yields the desired trivial product of (2.7). ☑

***Case 2.1.2:*** *Suppose that $\mathcal{P}$ is cyclic.* This proof is similar to the previous case but with one exception: we list the elements of $\mathscr{L}_{C_{\mathcal{G}}(t)}$ of eq. (2.10), $\mathscr{L}_{\mathcal{U}}$ of eq. (2.11), and $\mathscr{L}_{\mathcal{V}}$ of eq. (2.13) so for $\mathcal{G}$ they give the unique involution product $t$ (instead of the trivial product $e$). So we've shown that when $\mathcal{C}_G(t) < \mathcal{G}$ and $\mathcal{P}$ is a non-trivial and cyclic, there exists an ordering of the elements of $\mathcal{G}$ that yields the desired involution product of (2.8). ☑

***Case 2.2:*** *Suppose that $\mathcal{C}_{\mathcal{G}}(t) = \mathcal{G}$.* Take any $g_i \in \mathcal{G}$ and take $g_j \in \mathcal{G}$ such that

$$\begin{aligned} g_j &= g_i^{-1} \oplus t \oplus g_i \\ g_j \oplus g_i^{-1} &= g_i^{-1} \oplus t \\ g_i \oplus g_j \oplus g_i^{-1} &= t. \end{aligned}$$

Then $t^2 = e$ and $g_j = g_i^{-1} \oplus t \oplus g_i = t$ imply

$$g_j^2 = (g_i^{-1} \oplus t \oplus g_i)^2 = t^2 = e \in Z(\mathcal{G}) \text{ and } g_j = g_i^{-1} \oplus t \oplus g_i = t \in Z(\mathcal{G}).$$

So we let $\langle t\rangle = (\langle t\rangle, \oplus) = \{e, t\}$ be the order-2 group generated by $t$. Since $\mathcal{P}$ is a non-trivial 2-subgroup of $\mathcal{G}$ where $|\mathcal{P}|$ divides $|\mathcal{G}|$, then $|\mathcal{G}|$ is even. So $|\langle t\rangle| = 2$ divides both $|\mathcal{P}|$ and $|\mathcal{G}|$. Thus, by Sylow's Theorem 2.75 it follows that $\langle t\rangle$ is a normal 2-subgroup of both $\mathcal{P}$ and $\mathcal{G}$. Therefore, we have the two quotient 2-groups

$$\mathcal{G}/\langle t\rangle = \{g_i \oplus \langle t\rangle : g_i \in \mathcal{G}\} \text{ and } \mathcal{P}/\langle t\rangle = \{g_i \oplus \langle t\rangle : g_i \in \mathcal{P}\}.$$

Now $P < G$ implies $P/\langle t\rangle < \mathcal{G}/\langle t\rangle$, where Sylow's Theorem 2.75 implies that $\mathcal{P}/\langle t\rangle$ is in fact a Sylow 2-subgroup of $\mathcal{G}/\langle t\rangle$. (Note: at this point it is still possible that $\mathcal{P}/\langle t\rangle$ is a Sylow 2-subgroup with $|\mathcal{P}/\langle t\rangle| = 2^0 = 1$.) So we will consider the following two sub-cases for $\mathcal{P}/\langle t\rangle$, which depend on the following properties.

***Case 2.2.1:*** *Suppose that $\mathcal{P}/\langle t\rangle$ is trivial or non-cyclic.* Now since $|\langle t\rangle| = 2$, then by Lagrange's Theorem 2.74 we have $|\mathcal{G}| = |\langle t\rangle| \cdot |\mathcal{G}/\langle t\rangle| = 2k$ for some $k \in \mathbb{N}$. Hence, by induction there exist $k$ elements of $\mathcal{G}$, denoted by $h_1, h_2, \ldots, h_k \in \mathcal{G}$, such that we can choose either

$$h_1 = g_1,\ h_2 = g_1^{-1},\ h_3 = g_2,\ h_4 = g_2^{-1},\ \ldots,\ h_{k-1} = g_{k/2},\ h_k = g_{k/2}^{-1} \tag{2.16}$$

to obtain one version of $\mathcal{G}/\langle t\rangle$'s trivial product

$$h_1 \oplus h_2 \oplus \cdots \oplus h_{k-1} \oplus h_k = e \in \langle t\rangle \implies e \oplus \langle t\rangle = \langle t\rangle, \tag{2.17}$$

or alternatively we choose all of the same values as above in (2.16) except for the final $h_k = g_{k/2}^{-1} \oplus t$, which, instead of (2.17), gives us another instance of $\mathcal{G}/\langle t\rangle$'s trivial product

$$h_1 \oplus h_2 \oplus \cdots \oplus h_{k-1} \oplus h_k = t \in \langle t\rangle \implies t \oplus \langle t\rangle = \langle t\rangle \tag{2.18}$$

for

$$e \oplus \langle t\rangle = t \oplus \langle t\rangle = \langle t\rangle \in \mathcal{G}/\langle t\rangle.$$

Henceforth, for either selection (2.17) or (2.18) of $h_1, h_2, \ldots, h_k \in \mathcal{G}$, we can list the elements of $\mathcal{G}/\langle t\rangle$ to obtain the trivial product

$$h_1 \oplus \langle t\rangle \oplus h_2 \oplus \langle t\rangle \oplus \cdots \oplus h_k \oplus \langle t\rangle = (h_1 \oplus h_2 \oplus \cdots \oplus h_k) \oplus \langle t\rangle = \langle t\rangle,$$

which gives

$$\mathcal{G}/\langle t\rangle = \{h_1 \oplus \langle t\rangle,\ h_2 \oplus \langle t\rangle,\ \ldots,\ h_k \oplus \langle t\rangle\} \tag{2.19}$$

such that

$$h_1 \oplus h_2 \oplus \cdots \oplus h_k \in \langle t\rangle.$$

Consequently, for any $h_i \in \{h_1, h_2, \ldots, h_k\} \subset \mathcal{G}$ we have $h_i \oplus \langle t\rangle = \{h_i \oplus e, h_i \oplus t\}$. Then we can write all the elements of $\mathcal{G}$ as

$$\begin{aligned} \mathcal{G} &= \{h_1 \oplus e, h_2 \oplus e, \ldots, h_k \oplus e, h_1 \oplus t, h_2 \oplus t, \ldots, h_k \oplus t\} \\ &= \{h_1, h_2, \ldots, h_k, h_1 \oplus t, h_2 \oplus t, \ldots, h_k \oplus t\}, \end{aligned}$$

where $t \in Z(\mathcal{G})$ is central and $h_1 \oplus h_2 \oplus \cdots \oplus h_k \in \langle t\rangle$ implies

$$\begin{aligned} & h_1 \oplus h_2 \oplus \cdots \oplus h_k \oplus (h_1 \oplus t) \\ & \quad \oplus (h_2 \oplus t) \oplus \cdots \oplus (h_k \oplus t) &= (h_1 \oplus h_1) \oplus (h_2 \oplus h_2) \oplus \ldots (h_k \oplus h_k) \oplus t^k \\ & &= h_1^2 \oplus h_2^2 \oplus \cdots \oplus h_k^2 \oplus t^k \\ & &= (h_1 \oplus h_2 \oplus \cdots \oplus h_k)^2 \oplus t^k \\ & &= (h_1 \oplus h_2 \oplus \cdots \oplus h_k)^2 \oplus t^k \\ & &= e \oplus t^k \\ & &= t^k. \end{aligned}$$

Now recall that $\mathcal{P}$ is non-trivial by hypothesis. Therefore, we must consider two additional cases, which depend on whether $\mathcal{P}/\langle t\rangle$ is trivial or not.

- ***Case 2.2.1.A:*** *Suppose that $\mathcal{P}/\langle t\rangle$ is trivial.* Then Theorem 2.74 implies $|\mathcal{P}| = |\mathcal{P}/\langle t\rangle| \bullet |\langle t\rangle| = 1 \bullet 2 = 2$, so $\mathcal{P}$ is cyclic. Now since $\mathcal{P}/\langle t\rangle$ is a trivial Sylow 2-subgroup of $\mathcal{G}/\langle t\rangle$, then 2 does not divide $|\mathcal{G}/\langle t\rangle|$ because $\mathcal{P}/\langle t\rangle$ is a maximal 2-subgroup of $\mathcal{G}/\langle t\rangle$; so it follows that $|\mathcal{G}/\langle t\rangle| = k = 2l + 1$ is odd for some $l \in \mathbb{N}$. Hence, we obtain

  $$(h_1 \oplus h_2 \oplus \cdots \oplus h_{2l+1})^2 \oplus t^{2l+1} = e \oplus t^{2l} \oplus t = e \oplus (t^2)^l \oplus t = e \oplus e^l \oplus t = t,$$

  which is the involution product since $\mathcal{P}$ is non-trivial and cyclic. So we've shown that when $\mathcal{C}_G(t) = \mathcal{G}$ and $\mathcal{P}$ is a non-trivial and cyclic, there exists an ordering of the elements of $\mathcal{G}$ that yields the desired involution product of (2.8). ☑

- ***Case 2.2.1.B:*** *Suppose that $\mathcal{P}/\langle t\rangle$ is non-trivial.* Then $\mathcal{P}/\langle t\rangle$ is a non-cyclic. Therefore, the fact that $\langle t\rangle$ is cyclic implies that $\mathcal{P}$ is non-cyclic. Furthermore, $\mathcal{P}/\langle t\rangle$ being a non-trivial Sylow 2-subgroup of $\mathcal{G}/\langle t\rangle$ implies that $|\mathcal{G}/\langle t\rangle| = k = 2l$ is even for some $l \in \mathbb{N}$ by Theorem 2.74. So we obtain

  $$(h_1 \oplus h_2 \oplus \cdots \oplus h_{2l})^2 \oplus t^{2l} = e \oplus (t^2)^l = e \oplus e^l = e,$$

  which is the trivial product since $\mathcal{P}$ is non-cyclic. So we've shown that when $\mathcal{C}_G(t) = \mathcal{G}$ and $\mathcal{P}$ is a non-trivial and non-cyclic, there exists an ordering of the elements of $\mathcal{G}$ that yields the desired trivial product of (2.7). ☑

***Case 2.2.2:*** *Suppose that $\mathcal{P}/\langle t\rangle$ is non-trivial and cyclic.* Let $h \oplus \langle t\rangle$ be the generator of $\mathcal{P}/\langle t\rangle$. Since $|\mathcal{P}|$ and $|\langle t\rangle|$ are both even, and $\langle t\rangle < \mathcal{P}$ is normal in $\mathcal{P}$, then $|\mathcal{P}/\langle t\rangle| = |h \oplus \langle t\rangle| = m \in \mathbb{N}$ is also even by Theorem 2.74. Therefore, by induction we can choose $g_1, g_2, \ldots, g_k \in \mathcal{G}$ with

$$|\mathcal{G}/\langle t\rangle| = \frac{|\mathcal{G}|}{|\langle t\rangle|} = \frac{2k}{2} = k$$

for some $k \in \mathbb{N}$ such that

$$\mathcal{G}/\langle t\rangle = \{g_1 \oplus \langle t\rangle, g_2 \oplus \langle t\rangle, \ldots, g_k \oplus \langle t\rangle\}$$

and

$$\begin{aligned}(g_1 \oplus \langle t\rangle) \oplus (g_2 \oplus \langle t\rangle) \oplus \cdots \oplus (g_k \oplus \langle t\rangle) &= (g_1 \oplus g_2 \oplus \cdots \oplus g_k) \oplus \langle t\rangle \\ &= h^{\frac{m}{2}} \oplus \langle t\rangle,\end{aligned}$$

where $h^{\frac{m}{2}} \oplus \langle t\rangle$ is the unique involution in $\mathcal{P}/\langle t\rangle$ because

$$(h^{\frac{m}{2}} \oplus \langle t\rangle)^2 = (h^{\frac{m}{2}} \oplus \langle t\rangle^{\frac{m}{2}})^2 = ((h \oplus \langle t\rangle)^{\frac{m}{2}})^2 = (h \oplus \langle t\rangle)^m = \langle t\rangle.$$

Now since $\mathcal{P}/\langle t\rangle$ is a non-trivial Sylow 2-subgroup of $\mathcal{G}/\langle t\rangle$ it follows that $|\mathcal{G}/\langle t\rangle| = k = 2l$ is even for some $l \in \mathbb{N}$. Then we can write all of the $2k$ elements of $\mathcal{G}$ as

$$\begin{aligned}\mathcal{G} &= \{g_1 \oplus e, g_2 \oplus e, \ldots, g_k \oplus e, g_1 \oplus t, g_2 \oplus t, \ldots, g_k \oplus t\} \\ &= \{g_1 \oplus e, g_2 \oplus e, \ldots, g_{2l} \oplus e, g_1 \oplus t, g_2 \oplus t, \ldots, g_{2l} \oplus t\} \\ &= \{g_1, g_2, \ldots, g_{2l}, g_1 \oplus t, g_2 \oplus t, \ldots, g_{2l} \oplus t\},\end{aligned}$$

where we obtain the product

$$\begin{aligned}&g_1 \oplus g_2 \oplus \cdots \oplus g_{2l} \oplus (g_1 \oplus t) \oplus \\ &\quad (g_2 \oplus t) \oplus \cdots \oplus (g_{2l} \oplus t) = (g_1 \oplus g_1) \oplus (g_2 \oplus g_2) \oplus \cdots \oplus (g_{2l} \oplus g_{2l}) \oplus t^{2l} \\ &\quad = g_1^2 \oplus g_2^2 \oplus \cdots \oplus g_{2l}^2 \oplus t^{2l} \\ &\quad = (g_1 \oplus g_2 \oplus \cdots \oplus g_{2l})^2 \oplus (t^2)^l \\ &\quad = (g_1 \oplus g_2 \oplus \cdots \oplus g_{2l})^2 \oplus (e)^l \\ &\quad = (g_1 \oplus g_2 \oplus \cdots \oplus g_{2l})^2 \\ &\quad = (h^{\frac{m}{2}})^2 \\ &\quad = h^m\end{aligned} \tag{2.20}$$

because either

$$g_1 \oplus g_2 \oplus \cdots \oplus g_{2l} = h^{\frac{m}{2}} \oplus e = h^{\frac{m}{2}}$$

or

$$g_1 \oplus g_2 \oplus \cdots \oplus g_{2l} = h^{\frac{m}{2}} \oplus t,$$

since $(g_1 \oplus g_2 \oplus \cdots \oplus g_k) \oplus \langle t\rangle = h^{\frac{m}{2}} \oplus \langle t\rangle$ and $\langle t\rangle = \{e, t\}$. Now since $h \oplus \langle t\rangle$ is the generator of $\mathcal{P}/\langle t\rangle$, then $h^m \oplus \langle t\rangle = \langle t\rangle$, so $\langle t\rangle = \{e, t\}$ implies that either

$$h^m = e \quad \text{or} \quad h^m = t;$$

we will consider both of these cases as follows.

- ***Case 2.2.2.A:*** *Suppose that $h^m = e$.* Then $\mathcal{P}$ is non-cyclic because $\mathcal{P} = \langle h, t \rangle$, where we have that (2.20) gives the trivial product when. So we've shown that when $\mathcal{C}_G(t) = \mathcal{G}$ and $\mathcal{P}$ is a non-trivial and non-cyclic, there exists an ordering of the elements of $\mathcal{G}$ that yields the desired trivial product of (2.7). ☑

- ***Case 2.2.2.B:*** *Suppose that $h^m = t$.* Then the fact that $h^m$ is an involution gives
$$(h^m)^2 = t^2 = e \implies h^{2m} = e \implies |h| = 2m.$$
Now $|h \oplus \langle t \rangle| = |\mathcal{P}/\langle t \rangle| = m$ and $\langle t \rangle = 2$ gives $|\mathcal{P}| = |\mathcal{P}/\langle t \rangle| \bullet |\langle t \rangle| = 2m$ by hypothesis; so $|h| = 2m = |\mathcal{P}|$ implies that $\mathcal{P}$ is cyclic. So in the case that $h^m = t$, we have that (2.20) gives the involution product when $\mathcal{P}$ is cyclic. So we've shown that when $\mathcal{C}_G(t) = \mathcal{G}$ and $\mathcal{P}$ is a non-trivial and cyclic, there exists an ordering of the elements of $\mathcal{G}$ that yields the desired involution product of (2.8). ☑

Finally, this completes the proof that there exists some ordering of the elements of $\mathcal{G}$ that yields the trivial product if and only any Sylow 2-subgroup $\mathcal{P}$ of $\mathcal{G}$ is trivial or non-cyclic. ■

Before we move on to the next main result (of the upcoming Lemma 2.84), we must introduce some preliminary definitions and results.

**Lemma 2.80.** *Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite group and let $\mathcal{H}$ be a subgroup with index $[\mathcal{G} : \mathcal{H}] = k$. Let $\{g_0, g_1, g_2, \ldots, g_{k-1}\} \subset \mathcal{G}$ be a set of representatives for both the left and right coset expansions of $\mathcal{G}$ by $\mathcal{H}$. Let*
$$\alpha = \begin{pmatrix} 0 & 1 & 2 & \ldots & k-1 \\ \alpha(0) & \alpha(1) & \alpha(2) & \ldots & \alpha(k-1) \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 0 & 1 & 2 & \ldots & k-1 \\ \beta(0) & \beta(1) & \beta(2) & \ldots & \beta(k-1) \end{pmatrix}$$

*be permutations of $\mathbb{Z}_k = \{0, 1, 2, \ldots, k-1\}$ such that*

$$g_i \oplus (g_{\alpha(i)} \oplus \mathcal{H}) = g_{\beta(i)} \oplus \mathcal{H},\ \forall i = 0, 1, 2, \ldots, k-1.$$

*Then, if there exists a complete mapping for $\mathcal{H}$, then there exists a complete mapping for $\mathcal{G}$.*

**Lemma 2.81.** *Let $\mathcal{G} = (\mathcal{G}, \oplus) = \mathcal{A} \bullet \mathcal{B} = \{a \oplus b \mid a \in \mathcal{A}, b \in \mathcal{B}\}$, where $\mathcal{A}, \mathcal{B} \leq \mathcal{G}$ and $\mathcal{A} \cap \mathcal{B} = \{e\}$. If a complete mapping exists for $\mathcal{A}$, then there exists a complete mapping for $\mathcal{B}$.*

**Lemma 2.82.** *If $\mathcal{G} = (\mathcal{G}, \oplus)$ is a finite non-cyclic 2-group, then there exists a complete mapping for $\mathcal{G}$.*

M. Hall and Paige also used the following result by P. Hall [111].

**Lemma 2.83.** *Let $\mathcal{G}$ be a solvable finite group. Then for every prime $p$ where $p$ divides $|\mathcal{G}|$, there exists a $p$-complement subgroup $\mathcal{H}$ of $\mathcal{G}$.*

From [105, 107] we obtain the following three results for any finite *solvable* group.

**Lemma 2.84.** *Let $\mathcal{G}$ be a finite solvable group of order-$n$ and let $L^{\mathcal{G}} \subset \mathcal{L}^n$ encode $\mathcal{G}$. If $\mathcal{P}$ is a Sylow 2-subgroup of $\mathcal{G}$ that is trivial or non-cyclic, then $L^{\mathcal{G}}$ has a transversal.*

***Proof***. Suppose that $\mathcal{G}$ is a finite solvable group and let $\mathcal{P}$ be a non-cyclic Sylow 2-subgroup of $\mathcal{G}$. Since $\mathcal{P} < \mathcal{G}$ and $|\mathcal{P}| = 2^m$ for some integer $m > 0$, then 2 is a prime that divides $|\mathcal{G}|$. Therefore, Lemma 2.83 implies that $\mathcal{G}$ has a 2-complement; lets use $\mathcal{P}'$ to denote this 2-complement of $\mathcal{P}$ in $\mathcal{G}$. Then by definition of $\mathcal{P}'$ we have that $\mathcal{G} = \mathcal{P} \oplus \mathcal{P}'$ and $\mathcal{P} \cap \mathcal{P}' = \{e\}$, where $|\mathcal{P}'|$ is odd (since $|\mathcal{P}'|$ is relatively prime to 2). Now by definition of $\mathcal{P}$, Lemma 2.82 implies the existence of a complete mapping for $\mathcal{P}$. Henceforth, since $\mathcal{G} = \mathcal{P} \oplus \mathcal{P}'$ and $\mathcal{P} \cap \mathcal{P}' = \{e\}$ it follows from Lemma 2.81

that there also exists a complete mapping for $\mathcal{P}'$. Consequently, Lemma 2.80 implies the existence of a complete mapping for $\mathcal{G}$. Therefore, Theorem 2.67 implies $L^{\mathcal{G}}$ has a transversal. ■

**Corollary 2.85.** *Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite solvable group of order-$n$ and let $L^{\mathcal{G}} \in \mathcal{L}^n$ encode $\mathcal{G}$. If there exists some ordering of the elements of $\mathcal{G}$, say $g_1, g_2, \ldots, g_i, \ldots, g_n$, which yields the trivial product $g_1 \oplus g_2 \oplus \cdots \oplus g_i \oplus \ldots g_n = e$, then $L^{\mathcal{G}}$ has a transversal.*

***Proof.*** Suppose that $\mathcal{G} = (\mathcal{G}, \oplus)$ is a finite solvable group of order-$n$ and let $L^{\mathcal{G}} \in \mathcal{L}^n$ encode $\mathcal{G}$. Suppose there exists some ordering of the elements of $\mathcal{G}$, say $g_1, g_2, \ldots, g_i, \ldots, g_n$, which yields the trivial product $g_1 \oplus g_2 \oplus \cdots \oplus g_i \oplus \ldots g_n = e$. Then Lemma 2.79 implies that the Sylow 2-subgroups of $\mathcal{G}$ are trivial or non-cyclic. Consequently, Lemma 2.84 implies that $L^{\mathcal{G}}$ has a transversal. ■

**Corollary 2.86.** *Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite solvable group of order-$n$ and let $L^{\mathcal{G}} \in \mathcal{L}^n$ encode $\mathcal{G}$. Then the following three conditions are equivalent:*

*(i) $L^{\mathcal{G}}$ has a transversal (or equivalently $\mathcal{G}$ is admissible).*

*(ii) The Sylow 2-subgroups of $\mathcal{G}$ are trivial or non-cyclic.*

*(iii) There exists some ordering of the elements of $\mathcal{G}$, say $g_1, g_2, \ldots, g_i, \ldots, g_n$, which yields the trivial product $g_1 \oplus g_2 \oplus \cdots \oplus g_i \oplus \cdots \oplus g_n = e$.*

***Proof.*** Suppose that $\mathcal{G} = (\mathcal{G}, \oplus)$ is a finite solvable group of order-$n$ and let $L^{\mathcal{G}}$ be the unbordered Cayley table of $\mathcal{G}$. Suppose that $L^{\mathcal{G}}$ has a transversal. Then Lemma 2.70 implies that there exists some ordering of the elements of $\mathcal{G}$, say $g_1, g_2, \ldots, g_i, \ldots, g_n$, which yields the trivial product $g_1 \oplus g_2 \oplus \cdots \oplus g_i \oplus \cdots \oplus g_n = e$. Then Lemma 2.79 implies that the Sylow 2-subgroups of $\mathcal{G}$ are trivial or non-cyclic. Then Lemma 2.84 implies that $L^{\mathcal{G}}$ has a transversal. ■

At this point, we state the Hall-Paige Conjecture [107] as follows.

**Conjecture 2.87.** *Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite group of order-$n$ and let $L^{\mathcal{G}} \in \mathcal{L}^n$ be a latin square that encodes $\mathcal{G}$. Then the following three conditions are equivalent:*

*(i) $L^{\mathcal{G}}$ has a transversal (or equivalently $\mathcal{G}$ is admissible).*

*(ii) The Sylow 2-subgroups of $\mathcal{G}$ are trivial or non-cyclic.*

*(iii) There exists some ordering of the elements of $\mathcal{G}$, say $g_1, g_2, \ldots, g_i, \ldots, g_n$, which yields the trivial product $g_1 \oplus g_2 \oplus \cdots \oplus g_i \oplus \cdots \oplus g_n = e$.*

Thus, we observe that Corollaries 2.85 and 2.86 prove that *the Hall-Paige Conjecture 2.87 is true for the specific case of solvable groups.* Today *Conjecture 2.87 remains unproven for all groups* in general (to obtain such a result one would need to prove that Conjecture 2.87 also holds for non-solvable groups). Henceforth, we move on to consider some additional conditions that will further extend the results of Corollaries 2.85 and 2.86.

**Definition 2.88.** Let $L \in \mathcal{L}^n$ be a latin square. We say that $L$ can be *decomposed into disjoint transversals* if there exist $n$ disjoint transversals across $L$.

**Table 2.10: An example of five disjoint transversals that decompose the latin square $L^{(\mathbb{Z}_5,+)}$ that encodes the Cayley table of the group $\mathbb{Z}_5 = (\mathbb{Z}_5, +)$. Each transversal is marked with a distinct color and set of brackets.**

| + | **0** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|---|
| **0** | [0] | (1) | {2} | <3> | ⟨4⟩ |
| **1** | ⟨1⟩ | [2] | (3) | {4} | <0> |
| **2** | <2> | ⟨3⟩ | [4] | (0) | {1} |
| **3** | {3} | <4> | ⟨0⟩ | [1] | (2) |
| **4** | (4) | {0} | <1> | ⟨2⟩ | [3] |

The following fact is well-established in the literature [6, 105]; we rewrite the proofs for such additional conditional equivalences as follows.

**Lemma 2.89.** *Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite group of order-$n$ and let $L^{\mathcal{G}} \in \mathcal{L}^n$ encode $\mathcal{G}$. Then the following three conditions are equivalent:*

*(i) $L^{\mathcal{G}}$ has a transversal.*

*(ii) $L^{\mathcal{G}}$ can be decomposed into disjoint transversals.*

*(iii) There exists a latin square $L^{\mathcal{G}'} \in \mathcal{L}^n$ that is orthogonal to $L^{\mathcal{G}}$.*

***Proof.*** Suppose that $\mathcal{G} = (\mathcal{G}, \oplus)$ is a finite group of order-$n$ and let $L^{\mathcal{G}} \in \mathcal{L}^n$ encode $\mathcal{G}$.

***Claim 1:*** $(i) \implies (ii)$. Suppose that $T_i^{L^{\mathcal{G}}} \subset {}^{\{\}}L^{\mathcal{G}}$ is a transversal of $L^{\mathcal{G}}$ written as

$$T_i^{L^{\mathcal{G}}} = \{(x_{i,0}, y_{i,0}, z_{i,0}), (x_{i,1}, y_{i,1}, z_{i,1}), (x_{i,2}, y_{i,2}, z_{i,2}), ..., (x_{i,n-1}, y_{i,n-1}, z_{i,n-1})\},$$

where each $(x_{i,k}, y_{i,k}, z_{i,k}) \in T_i^{L^{\mathcal{G}}}$ is the choice from the $k$th row of $L^{\mathcal{G}}$ for the symbol $z_{i,k} \in \mathcal{G}$. Now take any fixed element $g \in \mathcal{G}$. Then, for each row $k = 0, 1, 2, ..., n-1$ choose $g \oplus z_{i,k}$; this gives a new transversal $T^{L^{\mathcal{G}}}_{i+k \mod n}$ for row $k$ with respect to $g$. Therefore, by fixing each $g \in G$ and repeating this process for $n-1$ additional iterations we obtain a set of $n$ transversals

$$\mathcal{T}(L^{\mathcal{G}}) = \{T^{L^{\mathcal{G}}}_{i+0 \mod n}, T^{L^{\mathcal{G}}}_{i+1 \mod n}, T^{L^{\mathcal{G}}}_{i+2 \mod n}, ..., T^{L^{\mathcal{G}}}_{i+(n-1) \mod n}\}$$

such that

$${}^{\{\}}L^{\mathcal{G}} = \bigcup_{T_i \in \mathcal{T}(L^{\mathcal{G}})} T_i^{L^{\mathcal{G}}} \text{ and } i \not\equiv j \mod n \implies T_i^{L^{\mathcal{G}}} \cap T_j^{L^{\mathcal{G}}} = \emptyset.$$

So $\mathcal{T}(L^{\mathcal{G}})$ is a set of $n$ disjoint transversals that partitions ${}^{\{\}}L^{\mathcal{G}}$. Consequently, $L^{\mathcal{G}}$ can be decomposed into disjoint transversals. ☑

***Claim 2:*** $(ii) \implies (i)$. Suppose that $L^{\mathcal{G}}$ can be composed into a set $\mathcal{T}(L^{\mathcal{G}})$ of disjoint transversals. Then clearly $L^{\mathcal{G}}$ has a transversal. ☑

***Claim 3:*** $(ii) \Longrightarrow (iii)$. Suppose that $L^{\mathcal{G}}$ can be composed into a set $\mathcal{T}(L^{\mathcal{G}})$ of disjoint transversals, which we write as

$$\mathcal{T}(L^{\mathcal{G}}) = \{T^{L^{\mathcal{G}}}_{i+0 \mod n}, \; T^{L^{\mathcal{G}}}_{i+1 \mod n}, \; T^{L^{\mathcal{G}}}_{i+2 \mod n}, \; ..., \; T^{L^{\mathcal{G}}}_{i+(n-1) \mod n}\}.$$

Then construct an $n \times n$ array of symbols from $\mathcal{G}$, denoted $L^{\mathcal{G}'}$, where

$$\forall T^{L^{\mathcal{G}}}_i \in \mathcal{T}(L^{\mathcal{G}}), \;\; \forall (x_{i,k}, y_{i,k}, z_{i,k}) \in T^{L^{\mathcal{G}}}_i, \;\; \text{set} \;\; L^{\mathcal{G}'}[x_{i,k}][y_{i,k}] \leftarrow i.$$

Now since each $T^{L^{\mathcal{G}}}_i \in \mathcal{T}(L^{\mathcal{G}})$ is a disjoint transversal of $L^{\mathcal{G}}$ and each $L^{\mathcal{G}'}[x_{i,k}][y_{i,k}]$ contains the same symbol $i \in \mathcal{G}$ for $k = 0, 1, 2, ..., n-1$, then $L^{\mathcal{G}'}$ is a latin square. Moreover, for any fixed $T^{L^{\mathcal{G}}}_i \in \mathcal{T}(L^{\mathcal{G}})$, since each $(x_{i,k}, y_{i,k}, z_{i,k}) \in T^{L^{\mathcal{G}}}_i$ contains a distinct symbol $z_{i,k} \in \mathcal{G}$ that corresponds to the fixed $i$, then it follows that each of the $n^2$ ordered pair entries of the graeco-latin square superimposition

$$\begin{aligned} L^{\mathcal{G}} \otimes L^{\mathcal{G}'} &= \begin{bmatrix} z_{0,0} & z_{0,1} & \cdots & z_{0,n-1} \\ z_{1,0} & z_{1,1} & \cdots & z_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ z_{n-1,0} & z_{n-1,1} & \cdots & z_{n-1,n-1} \end{bmatrix} \otimes \begin{bmatrix} z'_{0,0} & z'_{0,1} & \cdots & z'_{0,n-1} \\ z'_{1,0} & z'_{1,1} & \cdots & z'_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ z'_{n-1,0} & z'_{n-1,1} & \cdots & z'_{n-1,n-1} \end{bmatrix} \\ &= \begin{bmatrix} (z_{0,0}, z'_{0,0}) & (z_{0,1}, z'_{0,1}) & \cdots & (z_{0,n-1}, z'_{0,n-1}) \\ (z_{1,0}, z'_{1,0}) & (z_{1,1}, z'_{1,1}) & \cdots & (z_{1,n-1}, z'_{1,n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ (z_{n-1,0}, z'_{n-1,0}) & (z_{n-1,1}, z'_{n-1,1}) & \cdots & (z_{n-1,n-1}, z'_{n-1,n-1}) \end{bmatrix} \end{aligned} \tag{2.21}$$

are distinct. Consequently, it follows that since $L^{\mathcal{G}}$ has a decomposition into disjoint transversals, then there exists $L^{\mathcal{G}'}$ such that $L^{\mathcal{G}}$ and $L^{\mathcal{G}'}$ are orthogonal mates. ☑

***Claim 4:*** $(iii) \Longrightarrow (ii)$. Suppose that $L^{\mathcal{G}}$ has an orthogonal mate $L^{\mathcal{G}'}$. Then the $n^2$ ordered pair entries of the graeco-latin square superimposition of $L^{\mathcal{G}} \otimes L^{\mathcal{G}'}$ of (2.21) are distinct. So there are two cases to consider.

***Case 4.1:*** *Fix any symbol $z \in \mathcal{G}$ of $L^{\mathcal{G}}$.* Then there are $n$ distinct ordered pairs of the form $(z, z')$ in the graeco-latin square $L^{\mathcal{G}} \otimes L^{\mathcal{G}'}$ for $z' = 0, 1, 2, ..., n-1$. Now since $L^{\mathcal{G}}$ is a latin square, then each entry of $L^{\mathcal{G}}$ with the symbol $z$ is in a distinct row and a distinct column of $L^{\mathcal{G}}$. Thus, since each of the $n$ ordered pairs $(z, z')$ of $L^{\mathcal{G}} \otimes L^{\mathcal{G}'}$ are distinct, then (with $z$ fixed) the set of positions of each $(z, z')$ in $L^{\mathcal{G}} \otimes L^{\mathcal{G}'}$ correspond to a distinct disjoint transversal $T_z^{L^{\mathcal{G}}}$ in $L^{\mathcal{G}'}$; there exists a set of $n$ disjoint transversals $\mathcal{T}(L^{\mathcal{G}})$ of $L^{\mathcal{G}'}$. So $L^{\mathcal{G}'}$ has a decomposition into disjoint transversals. ☑

***Case 4.2:*** *Fix any symbol $z' \in \mathcal{G}$ of $L^{\mathcal{G}'}$.* Then by a similar argument to the previous case, it follows that $L^{\mathcal{G}}$ has a decomposition into disjoint transversals. ☑

Consequently, if a latin square has an orthogonal mate, then it has a decomposition into disjoint transversals. ☑

This completes the proof that $L^{\mathcal{G}}$ has a transversal if and only if $L^{\mathcal{G}}$ can be decomposed into disjoint transversals if and only if there exists a latin square $L^{\mathcal{G}'}$ that is orthogonal to $L^{\mathcal{G}}$. ■

Finally, we obtain the main result of this section.

**Theorem 2.90.** *Let $\mathcal{G} = (\mathcal{G}, \oplus)$ be a finite solvable group of order-$n$ and let $L^{\mathcal{G}} \in \mathcal{L}^n$ encode $\mathcal{G}$. Then the following six conditions are equivalent:*

*(i) $L^{\mathcal{G}}$ has a transversal.*

*(ii) The Sylow 2-subgroups of $\mathcal{G}$ are trivial or non-cyclic.*

*(iii) There exists some ordering of the elements of $\mathcal{G}$, say $g_1, g_2, \ldots, g_i, \ldots, g_n$, which yields the trivial product $g_1 \oplus g_2 \oplus \cdots \oplus g_i \oplus \cdots \oplus g_n = e$.*

*(iv) $L^{\mathcal{G}}$ can be decomposed into disjoint transversals.*

*(v) There exists a latin square $L^{\mathcal{G}'}$ that is orthogonal to $L^{\mathcal{G}}$.*

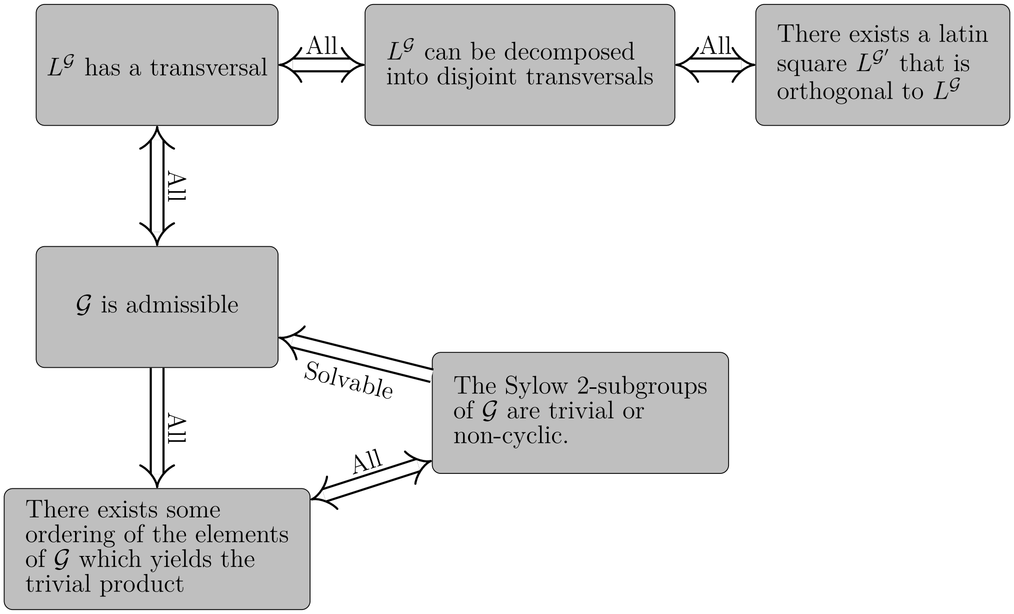
*(vi) $\mathcal{G}$ is admissible.*

***Proof*.** Suppose that $\mathcal{G} = (\mathcal{G}, \oplus)$ is a finite solvable group of order-$n$ and let $L^{\mathcal{G}} \in \mathcal{L}^n$ encode $\mathcal{G}$. Then Lemma 2.86 implies that conditions $(i)$, $(ii)$, and $(iii)$ are equivalent.

Since Lemma 2.89 implies that conditions (*i*), (*iv*) and (*v*) are equivalent, then conditions (*i*), (*ii*), (*iii*), (*iv*) and (*v*) are equivalent. Consequently, since Theorem 2.67 implies that conditions (*vi*) and (*i*) are equivalent, then conditions (*i*), (*ii*), (*iii*), (*iv*), (*v*), and (*vi*) are equivalent. ■

Here we observe that the main result of this section, namely Theorem 2.90, goes beyond Corollaries 2.85 and 2.86 by providing additional equivalent conditions for determining the existence of transversals in a latin square that encodes a finite *solvable* group; see Figure 2.4. In the future, it will be interesting to see if Theorem 2.90 can be further generalized to include all finite groups.

**Figure 2.4: A visual depiction of the implications of main result of Corollary 2.90, which extends the Hall-Paige Conjecture 2.87 for solvable groups. All six conditions are equivalent for solvable groups. However, the Hall-Paige Conjecture 2.87 remains unresolved for non-solvable groups.**


$L^{\mathcal{G}}$ has a transversal
All
$L^{\mathcal{G}}$ can be decomposed into disjoint transversals
All
There exists a latin square $L^{\mathcal{G}'}$ that is orthogonal to $L^{\mathcal{G}}$
All
$\mathcal{G}$ is admissible
Solvable
The Sylow 2-subgroups of $\mathcal{G}$ are trivial or non-cyclic.
All
All
There exists some ordering of the elements of $\mathcal{G}$ which yields the trivial product

## 2.7 Computational Enumeration of Transversals

In the previous Section 2.6 we mathematically examined latin square transversals and some key conditions for their existence. Thus, in order to make further use of such results for cryptographic application, one needs the ability to efficiently count the number transversals of a latin square $L \in \mathcal{L}^n$, namely $|\mathcal{T}(L)|$. In Section 2.7.1 we survey some existing pertinent transversal enumeration results in the literature [5, 6, 8]. Subsequently, in Section 2.7.2 we introduce our algorithms for enumerating transversals.

### 2.7.1 Survey of Transversal Enumeration Results

The challenges of counting and predicting the number of transversals in latin squares tend to become greater as the order increases. Over the course of recent decades, numerous mathematicians and scientists have put forth a significant effort in their attack on such challenges. For this, some of major open questions are:

- Which latin squares have the maximum number of transversals? Which have the minimum number of transversals?
- Which groups have the maximum number of good permutations? Which have the minimum number of good permutations?

Here we report some of the pertinent latin square transversal counting results from the literature which aim to address such inquiries. For the reader who is further interested in the details of such endeavors, we recommend the literature [5, 6, 8] and the plethora of important references therein.

In [112] the authors evaluate the complexity of counting the $|\mathcal{T}(L)|$ in a given $L$. More specifically, they show that [112]:

- For closed structures the counting problem is $\#\mathscr{P}$-complete.
- For closed structures with a left-identity and a left-cancellation law the counting problem is $\#\mathscr{P}$-complete.
- For an abelian groups the counting problem is beyond the $\#\mathscr{P}$-class.
- The famous counting problems of $n$-queens and toroidal $n$-queens are both beyond the $\#\mathscr{P}$-class.

In the transversal counting case of [112] the transversal counting problems are not in $\mathscr{N}\mathscr{P}$ because the machine's job is not to just determine if a given latin square has a transversal, but rather to count *all* of the transversals across the latin square (hence the class $\#\mathscr{P}$).

However, in [6] the author remarks on the analysis of [112], where he proposes that their conclusions would be much different if the input would be a Cayley table that encodes the group (instead of using a single integer to specify the order of the group). So far as we can tell, there appears to be relatively few results in the literature pertaining to the counting complexity.

In any case, there are numerous literature results with computational data obtained by counting latin square transversals directly. For instance, in Table 2.11 we list the number of transversals for the latin squares that encode general finite groups from order-3 to order-23 as reported in [5, 6]; this transversal count list corresponds to the group list in the catalog of Thomas and Wood [7]. To the best of our knowledge, order-23 is the highest order for which it is computationally feasible to count all of the transversals across a given single latin square.

**Table 2.11: The number of transversals across latin squares that encode groups from order-3 to order-23 [5, 6]; the transversal count list corresponds to the group list in the catalog of [7].**

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

Let $\mathbb{t}(n)$ and $\mathbb{T}(n)$ denote the minimum and maximum number of transversals, respectively, for any latin square in $\mathcal{L}^n$. In Table 2.12 we list $\mathbb{t}(n)$ and $\mathbb{T}(n)$ for all latin squares from order-2 to order-9 as reported in [5, 6]. To date of writing, order-9 is the highest order for which it is computationally feasible to count all of the transversals for the set of all latin squares of a given order.

For $n \geq 10$, the values of $\mathbb{T}(n)$ are not yet known due to current computational limitations—there are only estimates. Let $\lfloor \mathbb{T}(n) \rfloor_{MMW}$ and $\lceil \mathbb{T}(n) \rceil_{MMW}$ denote the estimated lower and upper bounds on $\mathbb{T}(n)$, respectively, as proposed by McKay, McLeod, and Wanless [8]:

**Theorem 2.91.** *If $n \geq 5$ then*

$$15^{n/5} = \lfloor \mathbb{T}(n) \rfloor_{MMW} \leq \mathbb{T}(n) \leq c^n \sqrt{n} n! = \lceil \mathbb{T}(n) \rceil_{MMW}$$

*where* $c = \sqrt{\frac{3-\sqrt{3}}{6}} e^{\sqrt{3}/6} \approx 0.61354.$

In Table 2.13 we report the estimates of $\lfloor \mathbb{T}(n) \rfloor_{MMW}$ and $\lceil \mathbb{T}(n) \rceil_{MMW}$ from [5, 6, 8], which we denote as $\lfloor \mathbb{T}(n) \rfloor_{MMW}$ and $\lceil \mathbb{T}(n) \rceil_{MMW}$ (for McKay-McLeod-Wanless [8]), respectively, from order-10 to order-21. Table 2.13 exemplifies a crucial effort to extend the results of Table 2.12.

**Table 2.12: The *confirmed* minimum $\mathtt{t}(n)$ and maximum $\mathbb{T}(n)$ number of transversals across latin squares from order-2 to order-9 [5, 6, 8].**

| **Order-$n$** | $\mathtt{t}(n)$ | **Mean** | **Standard Deviation** | $\mathbb{T}(n)$ |
|---|---|---|---|---|
| 2 | 0 | 0 | 0 | 0 |
| 3 | 3 | 3 | 0 | 3 |
| 4 | 0 | 2 | 3.46 | 8 |
| 5 | 3 | 4.29 | 3.71 | 15 |
| 6 | 0 | 6.86 | 5.19 | 32 |
| 7 | 3 | 20.41 | 6.00 | 133 |
| 8 | 0 | 61.05 | 8.66 | 384 |
| 9 | 68 | 214.11 | 15.79 | 2 241 |

In the upcoming Section 2.8 we refer to the results of Tables 2.11, 2.12, and 2.13 during our search for $\mathbb{T}(n)$.

**Table 2.13: Estimates for the lower bound $\lfloor \mathbb{T}(n) \rfloor_{MMW}$ and the upper bound $\lceil \mathbb{T}(n) \rceil_{MMW}$ on the maximum number of transversals $\mathbb{T}(n)$ across latin squares from order-10 to order-21 as given by Theorem 2.91 [5, 6, 8].**

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

### 2.7.2 Creation of Transversal Enumeration Algorithms

In the previous section we surveyed some of the existing data and results in the literature that pertain to counting latin square transversals. In order to obtain our own data and results for this research, we create a set of software tools for computing counting latin square transversals. Here we introduce these algorithms, which aim to address the following questions:

- How fast can we count $|\mathcal{T}(L)|$ for a given $L \in \mathcal{L}^n$?
- What is the highest order-$n$ for which it is computationally feasible to count $|\mathcal{T}(L)|$ for a given $L \in \mathcal{L}^n$?
- What is the highest order-$n$ for which it is computationally feasible to count $|\mathcal{T}(L)|$ for all $L \in \mathcal{L}^n$? How fast?

Thus, given some $L \in \mathcal{L}^n$ and currently available computational power, the objective is to develop our own algorithms to efficiently count $|\mathcal{T}(L)|$ for the highest order-$n$

that we can reach. We work to continually improve the efficiency, capability, and overall performance of our algorithm implementations in order to obtain counts for a progressively increasing $n$. We design, implement, and experiment with the three main versions of our algorithms for enumerating latin square transversals, namely the:

- *Brute-Force Latin Square Transversal Counting Algorithm* (BF-LS-TCAv1).
- *Subsquare Sequence Latin Square Transversal Counting Algorithm* (SS-LS-TCAv2).
- *Boolean Matrix Latin Square Transversal Counting Algorithm* (BM-LS-TCAv3).

Note: the BF-LS-TCAv1, the SS-LS-TCAv2, and the BM-LS-TCAv3 are given in Appendix B.2.1.

The BF-LS-TCAv1 of Algorithm 2.4 (in Appendix B.2.1) is our first and most rudimentary approach to counting transversals. We say that the BF-LS-TCAv1 is rudimentary because, given an order-$n$ latin square $L$ as input, it determines $|\mathcal{T}(L)|$ by using iterative brute force to exhaustively evaluate every possible order-$n$ diagonal to determine if it is a transversal. We implement the BF-LS-TCAv1 in the C programming language. We find this implementation to be sufficient for counting transversals on single latin squares up to order-10, where it serves as an important tool for the preliminary phase of our research on latin square transversals (where the need to quickly evaluate latin squares of order-($n \geq 10$) has not yet come into play).

As our research progresses, we eventually develop the ability to generate latin squares beyond order-10 (recall Section 2.5); thus, we need to (attempt to) obtain transversal counts for those orders. A major computational bottleneck of the BF-LS-TCAv1 is that it's implementation requires that the set of all order-$n$ diagonals be loaded into RAM for exhaustive evaluation (this was $n!$ diagonals); this significant limitation revealed itself when we attempted to process relatively large data sets (ex. 100,000) of order-10 latin squares. As a result, we invest more effort into designing a completely new transversal counting algorithm to obtain such counts for order-($n \geq$ 10), which motivates us to create Version 2: the SS-LS-TCAv2 of 2.5 (in Appendix B.2.1). The SS-LS-TCAv2 is a non-brute force algorithm that, when given $L \in \mathcal{L}^n$ as input, determines $|\mathcal{T}(L)|$ by recursively calling itself, where it makes a new sub-square state of descending order if a state symbol is found inside its current sub-square state. In terms of computational resource consumption, a major advantage that the SS-LS-TCAv2 has over the BF-LS-TCAv1 is that it doesn't on the loading of $n!$ diagonals into RAM. Thus, the SS-LS-TCAv2 Java implementation serves as an important tool for counting transversals on relatively large latin square data sets up to order-13 (ex. 100,000 latin squares) and on single latin squares up to order-16. For counting the number of transversals of order-10 latin squares, we find that SS-LS-TCAv2 is approximately 25.5 times faster than BF-LS-TCAv1 implementation, and that the SS-LS-TCAv2 implementation only consumes approximately 18.6% of the RAM that the BF-LS-TCAv1 implementation consumes; in Appendix B.2.3 see the performance benchmark results of the SS-LS-TCAv2 versus the BF-LS-TCAv1.

A major computational limitation of the SS-LS-TCAv2 is the repeated allocation (and deallocation) of sub-square objects in RAM. Thus, upon further evaluations of the SS-LS-TCAv2, we discover that such repeated constructions of sub-squares are not necessary because instead we can just use a Boolean matrix (stored in globally) to keep track of the transversal states; this leads to the successive development of Version 3: the BM-LS-TCAv3 of Algorithm 2.6 (in Appendix B.2.1). To summarize, the BM-LS-TCAv3 counts transversals by recursively calling itself, where it accepts a row as input and looks at global data to see which entries in the row are valid to generate a partial transversal that could become a transversal. For counting the number of transversals of order-16 latin squares, we find that the BM-LS-TCAv3 Java implementation is approximately 1.3 times faster than the SS-LS-TCAv2 implementation; in Appendix B.2.3 see the performance benchmark results of the BM-LS-TCAv3 versus the SS-LS-TCAv2. Thus, by using the BM-LS-TCAv3 we are able to process larger data sets with order-16 latin squares at a faster rate.

In Table 2.14 we report the *minimum and maximum* transversal counts that we observe by using the BM-LS-TCAv3 to process our data sets of order-$n$ latin squares for $3 \leq n \leq 9$; our resulting transversal counts fall within the confirmed $[\mathbb{t}(n), \mathbb{T}(n)]$ range reported in [5, 6, 8]. Thereafter, in Table 2.15 we report the *maximum* transversal counts that we observe by using the BM-LS-TCAv3 on (subsets of) our data sets of order-$n$ latin squares for $9 < n \leq 16$; our resulting transversal counts are bounded above by the estimated lower and upper bounds on the maximum transversal counts that were reported in [5, 6, 8].

**Table 2.14: The minimum and maximum transversal counts that we observed by using the BM-LS-TCAv3 Java implementation on our order-3 to order-9 latin square data sets fall within the confirmed $[\mathbb{t}(n), \mathbb{T}(n)]$ range [5, 6, 8]. The matching counts are marked in (blue) bold.**

| **Order-$n$** | **Data Set Size: # Latin Squares** | **Data Set Observed # Transversals Range: [Min, Max]** | **Confirmed # Transversals Range: $[\mathbb{t}(n), \mathbb{T}(n)]$** | **Is Observed Within Confirmed Range?** |
|---|---:|---|---|---|
| 3 | 12 | [**3**, **3**] | [**3**, **3**] | Yes |
| 4 | 576 | [**0**, **8**] | [**0**, **8**] | Yes |
| 5 | 161 280 | [**3**, **15**] | [**3**, **15**] | Yes |
| 6 | 4 000 000 | [**0**, **32**] | [**0**, **32**] | Yes |
| 7 | 3 000 000 | [**3**, 63] | [**3**, 133] | Yes |
| 8 | 2 750 000 | [**0**, **384**] | [**0**, **384**] | Yes |
| 9 | 2 500 000 | [84, 444] | [68, 2 241] | Yes |

**Table 2.15: The maximum transversal counts that we observed by using the BM-LS-TCAv3 implementation on subsets of our latin square data sets from order-10 to order-16; our maximum observed counts are less than or equal to the estimated $\lfloor \mathbb{T}(n) \rfloor_{\mathrm{MMW}}$ [5, 6, 8].**

| **Order-$n$** | **Data Set Size: # Latin Squares** | **Data Set Observed # Transversals Max** | **Estimated $\lfloor \mathbb{T}(n) \rfloor_{\mathrm{MMW}}$** | **Estimated $\lceil \mathbb{T}(n) \rceil_{\mathrm{MMW}}$** | **Is Observed Max $\leq$ Estimated?** |
|---|---|---|---|---|---|
| 10 | 1 000 000 | 1 664 | 5 504 | 75 000 | Yes |
| 11 | 500 000 | 3 896 | 37 851 | 528 647 | Yes |
| 12 | 300 341 | 132 096 | 198 144 | 3 965 268 | Yes |
| 13 | 176 516 | 82 628 | 1 030 367 | 32 837 805 | Yes |
| 14 | 15 000 | 557 440 | 3 477 504 | 300 019 037 | Yes |
| 15 | 1 000 | 3 316 847 | 36 362 925 | 2 762 962 210 | Yes |
| 16 | 358 | 183 558 144 | 244 744 192 | 28 218 998 328 | Yes |

Next, we give proof that the BM-LS-TCAv3 of Algorithm 2.6 correctly counts the number of transversals in a latin square.

**Theorem 2.92.** *Let $L \in \mathcal{L}^n$ be a latin square of order $n \geq 3$ and let $T \in \mathcal{T}(L)$ be a transversal of $L$. Let $\mathcal{T}'(L)$ be the set of transversals of $L$ that are counted by the BM-LS-TCAv3. Then $T \in \mathcal{T}'(L)$.*

***Proof***. Let $L \in \mathcal{L}^n$ be a latin square of order $n \geq 3$ and let $T \in \mathcal{T}(L)$ be a transversal of $L$ written as

$$T = \{(x_0, y_0, z_0), (x_1, y_1, z_1), \ \ldots, (x_{n-1}, y_{n-1}, z_{n-1})\},$$

where $(x_i, y_i, z_i) \in T$ is the $i$th row of $L$ and the $i$th element of $T$. Let $\mathcal{T}'(L)$ be the set of transversals of $L$ that are counted by the BM-LS-TCAv3. We wish to show that $T \in \mathcal{T}'(L)$.

By definition, the BM-LS-TCAv3 begins at row 0 and chooses the first available entry $(0, y, z)$ of row 0 to see if $(0, y, z)$ is passed through by a transversal. Since the BM-LS-TCAv3 has made no selection, then we may assume that the BM-LS-TCAv3 chooses $(x_0, y_0, z_0) \in T$ of row 0. So $\bar{x}_0 = \bar{y}_0 = \bar{z}_0 = 0$. Next, the BM-LS-TCAv3 considers row 1. Since $T$ is a transversal of $L$, then there exists an available entry $(x_1, y_1, z_1) \in T$ of row 1, where $x_0 \neq x_1$, $y_0 \neq y_1$, and $z_0 \neq z_1$. By definition, the BM-LS-TCAv3 considers each available entry of row 1. Thus, we may assume that the BM-LS-TCAv3 chooses $(x_1, y_1, z_1) \in T$ of row 1. So $\bar{x}_1 = \bar{y}_1 = \bar{z}_1 = 0$.

Thereafter, since $n \geq 3$ it follows that the BM-LS-TCAv3 considers row $i$ where $3 \leq i + 1 < n$ because the BM-LS-TCAv3 considers each of the $n$ rows of $L$. Since $T$ is a transversal of $L$, then there exists an available entry $(x_i, y_i, z_i) \in T$ of row $i$ where $x_i \neq x_0, x_1$ and $y_i \neq y_0, y_1$ and $z_i \neq z_0, z_1$. So we may assume that the BM-LS-TCAv3 chooses $(x_i, y_i, z_i) \in T$.

***Case:*** $n = 3$. Then the BM-LS-TCAv3 counts $T$ as a transversal. ☑

***Case:*** $n > 3$. Then the BM-LS-TCAv3 continues to the next row, so BM-LS-TCAv3 considers row $i + 1$. Since $i + 1 < n$ and $T$ is a transversal of $L$, then there exists an available entry $(x_{i+1}, y_{i+1}, z_{i+1}) \in T$ of row $i + 1$, where $x_{i+1} \neq x_0, x_1, x_i$ and $y_{i+1} \neq y_0, y_1, y_i$ and $z_{i+1} \neq z_0, z_1, z_i$ for $i = 2, 3, \ \ldots, n - 2$. So we may assume that the BM-LS-TCAv3 chooses $(x_{i+1}, y_{i+1}, z_{i+1}) \in T$. By inductively repeating this process, it follows that the BM-LS-TCAv3 chooses each $(x_i, y_i, z_i) \in T$ and will count $T$ as a transversal when $i + 1 = n$. ☑

Therefore, $T \in \mathcal{T}'(L)$ for $n \geq 3$. ■

## 2.8 Searching for Maximum Transversal Counts

Before we proceed to the main content of this section, let us briefly recapitulate the main prerequisite content of the preceding three sections.

- In Sections 2.5 and 2.7 we created software tools for generating latin square data sets and counting transversals.
- In Section 2.6 we surveyed some recent results and conjectures related to transversals, which included some key equivalent conditions for the existence of transversals in latin squares that encode groups.

Therefore, now that we've obtained some knowledge of latin square transversals and are equipped with the appropriate software tools to evaluate latin squares up to order-17, we begin our attack on the following questions:

- For order-$n$ with $3 \leq n \leq 9$, can we accurately predict which finite groups will possess the *confirmed* $\mathbb{T}(n)$? How about the confirmed $\mathbb{t}(n)$?
- For order-$n$ with $9 < n \leq 17$, can we accurately predict which finite groups will possess the *estimated* $\lfloor \mathbb{T}(n) \rfloor_{\mathbf{MMW}}$? How about the estimated $\lceil \mathbb{T}(n) \rceil_{\mathbf{MMW}}$?

### 2.8.1 Evaluating Cyclic Latin Squares

**Definition 2.93.** A latin square is said to be *cyclic* if its rows are generated by cyclically permuting the first row (it follows that the columns have the same property). In other words, a cyclic latin square of order-$n$ is, up to relabeling the symbols, just the addition Cayley table (or the subtraction table) for the finite cyclic groups of the integers modulo $n$; such groups are denoted by $\mathbb{Z}_n = (\mathbb{Z}_n, +)$ and the corresponding latin squares are denoted by $L^{(\mathbb{Z}_n,+)} \in \mathcal{L}^n$.

**Definition 2.94.** Let $\mathbb{Z}_n = (\mathbb{Z}_n, +)$ be a finite group encoded by the latin square $L^{(\mathbb{Z}_n,+)} \in \mathcal{L}^n$. If $n = p \in \mathbb{N}$ is prime, then we say that $L^{(\mathbb{Z}_p,+)}$ is a latin square with *prime order*. More generally, if $n = p^d \in \mathbb{N}$ is a prime power for some $d \in \mathbb{N}$, then we say that $L^{(\mathbb{Z}_{p^d},+)}$ is a latin square with *prime power order*.

Here we consider the cyclic latin squares that encode cyclic groups from order-3 to order-9 that are listed in Table 2.16. We use the BM-LS-TCAv3 Java implementation to process these cyclic latin squares and report the results in Table 2.17; the observed counts for each order are compared next to the counts of the confirmed range $[\mathbb{t}(n), \mathbb{T}(n)]$ from [5, 6, 8].

**Table 2.16: Cyclic order-$n$ latin squares that encode cyclic groups from $(\mathbb{Z}_3, +)$ to $(\mathbb{Z}_9, +)$.**

$L^{(\mathbb{Z}_3,+)}$

| | | |
|---|---|---|
| 0 | 1 | 2 |
| 1 | 2 | 0 |
| 2 | 0 | 1 |

$L^{(\mathbb{Z}_4,+)}$

| | | | |
|---|---|---|---|
| 0 | 1 | 2 | 3 |
| 1 | 2 | 3 | 0 |
| 2 | 3 | 0 | 1 |
| 3 | 0 | 1 | 2 |

$L^{(\mathbb{Z}_5,+)}$

| | | | | |
|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 |
| 1 | 2 | 3 | 4 | 0 |
| 2 | 3 | 4 | 0 | 1 |
| 3 | 4 | 0 | 1 | 2 |
| 4 | 0 | 1 | 2 | 3 |

$L^{(\mathbb{Z}_6,+)}$

| | | | | | |
|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 0 | 1 | 2 | 3 | 4 |

$L^{(\mathbb{Z}_7,+)}$

| | | | | | | |
|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 0 | 1 | 2 | 3 | 4 | 5 |

$L^{(\mathbb{Z}_8,+)}$

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 |
| 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 |
| 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 |
| 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 |
| 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |

$L^{(\mathbb{Z}_9,+)}$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 0 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 |
| 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 | 3 |
| 5 | 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 |
| 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 8 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

First, in Table 2.17 we observe that the *even order* cyclic latin squares $L^{(\mathbb{Z}_4,+)}$, $L^{(\mathbb{Z}_6,+)}$, and $L^{(\mathbb{Z}_8,+)}$ have the *confirmed minimum* (zero) counts of $\mathbb{T}(4)$, $\mathbb{T}(6)$, and $\mathbb{T}(8)$, respectively. Thus, to obtain more data on this even order phenomena we use the BM-LS-TCAv3 to count the number of transversals in even order cyclic latin squares from order-2 to order-14 and report the results in Table 2.18. Here we observe that all of the transversal counts are zero from $L^{(\mathbb{Z}_2,+)}$ to $L^{(\mathbb{Z}_{14},+)}$; we recall that this phenomena is predicted by Theorem 2.60 from Section 2.6.1, which is a result that one can prove with the Delta Lemma 2.58.

Second, in Table 2.17 we observe that the *odd prime order* cyclic latin squares

**Table 2.17: The observed transversal counts for cyclic order-$n$ latin squares from order-3 to order-9 that encode cyclic groups from $(\mathbb{Z}_3,+)$ to $(\mathbb{Z}_9,+)$ are compared to the confirmed $[\mathtt{t}(n),\mathbb{T}(n)]$ range. The $\mathbb{T}(n)$ counts possessed by the prime order latin squares $L^{(\mathbb{Z}_3,+)}$, $L^{(\mathbb{Z}_5,+)}$, and $L^{(\mathbb{Z}_7,+)}$ are marked in (blue) bold.**

| **Order-$n$** | **Cyclic Latin Square** | **Cyclic Group** | **Observed # Transversals** | **Confirmed # Transversal Range: $[\mathtt{t}(n),\mathbb{T}(n)]$** |
|---|---|---|---|---|
| 3 | $L^{(\mathbb{Z}_3,+)}$ | $(\mathbb{Z}_3,+)$ | **3** | $[3,\mathbf{3}]$ |
| 4 | $L^{(\mathbb{Z}_4,+)}$ | $(\mathbb{Z}_4,+)$ | 0 | $[0,8]$ |
| 5 | $L^{(\mathbb{Z}_5,+)}$ | $(\mathbb{Z}_5,+)$ | **15** | $[3,\mathbf{15}]$ |
| 6 | $L^{(\mathbb{Z}_6,+)}$ | $(\mathbb{Z}_6,+)$ | 0 | $[0,32]$ |
| 7 | $L^{(\mathbb{Z}_7,+)}$ | $(\mathbb{Z}_7,+)$ | **133** | $[3,\mathbf{133}]$ |
| 8 | $L^{(\mathbb{Z}_8,+)}$ | $(\mathbb{Z}_8,+)$ | 0 | $[0,384]$ |
| 9 | $L^{(\mathbb{Z}_9,+)}$ | $(\mathbb{Z}_9,+)$ | 2 050 | $[68,2\ 241]$ |

$L^{(\mathbb{Z}_3,+)}$, $L^{(\mathbb{Z}_5,+)}$, and $L^{(\mathbb{Z}_7,+)}$ have the *confirmed maximum* counts of $\mathbb{T}(3)$, $\mathbb{T}(5)$, and $\mathbb{T}(7)$, respectively. We also observe that the *odd non-prime order* cyclic latin square $L^{(\mathbb{Z}_9,+)}$ has a transversal count of 2,050 that is much closer to $\mathbb{T}(9) = 2{,}241$ than it is to $\mathtt{t}(9) = 68$; the fact that $L^{(\mathbb{Z}_9,+)}$ has odd order influences its transversal count as predicted by Theorem 2.60.

Based on the results of Tables 2.17 and 2.18 we observe the following:

1. All even order cyclic latin squares from order-2 to order-14 that encode the corresponding cyclic groups of the integers modulo $n$ under addition from $(\mathbb{Z}_2,+)$ to $(\mathbb{Z}_{14},+)$ have zero transversals.

2. All of our cyclic latin square transversal counts fall within the bounds of $\mathtt{t}(n)$ and $\mathbb{T}(n)$ as reported by [5, 6, 8].

3. The cyclic latin squares with *odd prime order*—namely $L^{(\mathbb{Z}_3,+)}$, $L^{(\mathbb{Z}_5,+)}$, and $L^{(\mathbb{Z}_7,+)}$—have transversal counts that match $\mathbb{T}(3)$, $\mathbb{T}(5)$, and $\mathbb{T}(7)$, respectively.

**Table 2.18: The observed transversal counts are zero for all even order cyclic latin squares from $L^{(\mathbb{Z}_2,+)}$ to $L^{(\mathbb{Z}_{14},+)}$.**

| **Order-$n$** | **Cyclic Latin Square** | **Cyclic Group** | **Observed # Transversals** |
|---|---|---|---|
| 2 | $L^{(\mathbb{Z}_2,+)}$ | $(\mathbb{Z}_4,+)$ | 0 |
| 4 | $L^{(\mathbb{Z}_4,+)}$ | $(\mathbb{Z}_4,+)$ | 0 |
| 6 | $L^{(\mathbb{Z}_6,+)}$ | $(\mathbb{Z}_6,+)$ | 0 |
| 8 | $L^{(\mathbb{Z}_8,+)}$ | $(\mathbb{Z}_8,+)$ | 0 |
| 10 | $L^{(\mathbb{Z}_{10},+)}$ | $(\mathbb{Z}_{10},+)$ | 0 |
| 12 | $L^{(\mathbb{Z}_{12},+)}$ | $(\mathbb{Z}_{12},+)$ | 0 |
| 14 | $L^{(\mathbb{Z}_{14},+)}$ | $(\mathbb{Z}_{14},+)$ | 0 |

4. The cyclic latin squares with *non-prime order*—namely $L^{(\mathbb{Z}_4,+)}$, $L^{(\mathbb{Z}_6,+)}$, $L^{(\mathbb{Z}_8,+)}$, and $L^{(\mathbb{Z}_9,+)}$—have transversal counts below $\mathbb{T}(4)$, $\mathbb{T}(6)$, $\mathbb{T}(8)$, and $\mathbb{T}(9)$, respectively. In fact, the even non-prime order latin squares $L^{(\mathbb{Z}_4,+)}$, $L^{(\mathbb{Z}_6,+)}$, and $L^{(\mathbb{Z}_8,+)}$ have transversal counts that match $\mathbb{t}(4)$, $\mathbb{t}(6)$, and $\mathbb{t}(8)$, respectively. Meanwhile, the odd non-prime order latin square $L^{\mathbb{Z}_9}$ has a transversal count that is relatively close to $\mathbb{T}(9)$ in contrast to the even non-prime order latin squares.

**Remark 2.95.** We note that if $p$ is prime, then $\mathbb{Z}_p = (\mathbb{Z}_p,+)$ is also a Galois field of order-$p$.

Hence, based on the results of Tables 2.17 and 2.18, we decide to investigate the following transversal prediction questions:

- Given that $L^{(\mathbb{Z}_3,+)}$, $L^{(\mathbb{Z}_5,+)}$, and $L^{(\mathbb{Z}_7,+)}$ have maximum transversal counts, can we use such *prime order* cyclic latin squares as "latin sub-square building blocks" to construct larger latin squares with *prime power orders* that also have maximum transversal counts?

- Given that $L^{(\mathbb{Z}_4,+)=(\mathbb{Z}_{2^2},+)}$, $L^{(\mathbb{Z}_8,+)=(\mathbb{Z}_{2^3},+)}$, and $L^{(\mathbb{Z}_9,+)=(\mathbb{Z}_{3^2},+)}$ are prime power order cyclic latin squares (which do *not* have maximum transversal counts), is it possible to use prime order cyclic latin squares such as $L^{(\mathbb{Z}_2,+)}$ and $L^{(\mathbb{Z}_3,+)}$ (which do have maximum transversal counts for those orders—even though $\mathbb{T}(2) = \mathtt{t}(2) = 0$ for $L^{(\mathbb{Z}_2},+)$) as "latin sub-square building blocks" to construct larger latin squares with prime power orders that also have maximum transversal counts?
- Can we use the above results to predict which types of prime power order latin squares will possess the maximum number of transversals?

The said questions motivate our investigation in the next sections.

### 2.8.2 Building Super-Symmetric Latin Squares

Based on the observed maximum transversal results for latin squares that encode cyclic groups, we decide to investigate the question: *can we use this to design and implement a new algorithm to generate specific types of prime power order latin squares that possess the maximum number of transversals?* Our hypothesis is: *yes.*

Upon considering this question, we design and implement a new algorithm (discussed in more detail below and listed as Algorithm 2.3 in Appendix B.1.1) that generates a specific type of latin square with prime power order-$p^d$, which is based on the concept of *self-similarity* (an object that is exactly or approximately similar to a part of itself). The design of our proposed algorithm is based on the fact that: each cyclic latin square of prime order-$p$ with $p \in \{2, 3, 5, 7\}$ has the desired $\mathbb{T}(2)$, $\mathbb{T}(3)$, $\mathbb{T}(5)$, and $\mathbb{T}(7)$, respectively. For the sake of notational simplicity, we will use $\mathbb{L}^{(\mathbb{F}_{p^d},+)} \in \mathcal{L}^{p^d}$ to denote such an order-$p^d$ self-similar latin square, even though we are not yet claiming that $\mathbb{L}^{(\mathbb{F}_{p^d},+)}$ encodes the group $(\mathbb{F}_{p^d},+)$ of Galois field addition. So we make the conjecture: *for any $p^d$ with $d > 1$, there exists a prime power order-$p^d$ "self-similar latin square $\mathbb{L}^{(\mathbb{F}_{p^d},+)}$ of $p \times p$ adjacent order-$p^{d-1}$ latin sub-squares" each possessing $\mathbb{T}(p^{d-1})$ transversals so that $\mathbb{L}^{(\mathbb{F}_{p^d},+)}$ possesses $\mathbb{T}(p^d)$ transversals.*

To give a general summary: given $p$ and $d > 1$ as input, our proposed algorithm generates an order-$p^d$ latin square $\mathbb{L}^{(\mathbb{F}_{p^d},+)} \in \mathcal{L}^{p^d}$ that is recursively built from $p \times p$ adjacent latin sub-squares of order-$p^{d-1}$, where each order-$p^{d-1}$ latin sub-square that is equivalent to $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)} \in \mathcal{L}^{p^{d-1}}$ (up to order-preserving symbol relabeling) is recursively built from $p \times p$ adjacent latin sub-squares of order-$p^{d-2}$, where each order-$p^{d-2}$ latin sub-square is equivalent to $\mathbb{L}^{(\mathbb{F}_{p_{d-2}},+)} \in \mathcal{L}^{p^{d-2}}$, etc., where the smallest latin sub-square "building blocks" are cyclic latin squares of prime order-$p$ that are equivalent to $L^{(\mathbb{Z}_p,+)}$. During the generation process, for each "grid level" of $p \times p$ latin sub-squares, the same permutation $\pi$ that cyclically generates the rows (or columns) of $L^{(\mathbb{Z}_p,+)}$ is recursively applied to cyclically permute the $p \times p$ latin sub-squares to construct a latin square $\mathbb{L}^{(\mathbb{F}_{p^d},+)}$ that exhibits a *self-similar structure.* Upon creating our algorithm for generating such self-similar order-$p^d$ latin squares, we then discover that it is an apparent generalization of the algorithm proposed in [60] which generates the so-called "super-symmetric" latin squares of order-$2^d$. Thus, we define the following:

**Definition 2.96.** Let $\mathbb{Z}_p = (\mathbb{Z}_p,+)$ be the cyclic group of integers modulo $p$ under addition where $p \in \mathbb{N}$ is prime. Let $L^{(\mathbb{Z}_p,+)} \in \mathcal{L}^p$ be the cyclic latin square of prime order-$p$ that encodes $(\mathbb{Z}_p,+)$ with symbols from $\{0,1,2,\ldots,p-1\}$, where each row (or column) of $L^{(\mathbb{Z}_p,+)}$ is cyclically generated by the permutation $\pi$. Let $L^{(\mathbb{Z}_p,+)+kp} \in \mathcal{L}^p$ be a cyclic latin square of prime order-$p$ that encodes $(\mathbb{Z}_p,+)$ with symbols from $\{0+kp, 1+kp, 2+kp, \ldots, (p-1)+kp\}$, where each row (or column) of $L^{(\mathbb{Z}_p,+)+kp}$

is cyclically generated by the permutation $\pi$, so that each $L^{(\mathbb{Z}_p,+)+kp}$ is equivalent to $L^{(\mathbb{Z}_p,+)}$ (up to order-preserving symbol relabeling) for $k = 0, 1, 2, \ldots, (p-1)$. Then, we say that a latin square $\mathbb{L}^{(\mathbb{F}_{p^2},+)} \in \mathcal{L}^{p^2}$ of prime power order-$p^2$ is *order-$p^2$ super-symmetric* if $\mathbb{L}^{(\mathbb{F}_{p^2},+)}$ can be written as the $p \times p$ latin sub-square grid

| | | | | |
|---|---|---|---|---|
| $L^{(\mathbb{Z}_p,+)}$ | $L^{(\mathbb{Z}_p,+)+p}$ | $L^{(\mathbb{Z}_p,+)+2p}$ | $\ldots$ | $L^{(\mathbb{Z}_p,+)+(p-1)p}$ |
| $L^{(\mathbb{Z}_p,+)+p}$ | $L^{(\mathbb{Z}_p,+)+2p}$ | $\ldots$ | $L^{(\mathbb{Z}_p,+)+(p-1)p}$ | $L^{(\mathbb{Z}_p,+)}$ |
| $L^{(\mathbb{Z}_p,+)+2p}$ | $\ldots$ | $L^{(\mathbb{Z}_p,+)+(p-1)p}$ | $L^{(\mathbb{Z}_p,+)}$ | $L^{(\mathbb{Z}_p,+)+p}$ |
| $\ldots$ | $L^{(\mathbb{Z}_p,+)+(p-1)p}$ | $L^{(\mathbb{Z}_p,+)}$ | $L^{(\mathbb{Z}_p,+)+p}$ | $L^{(\mathbb{Z}_p,+)+2p}$ |
| $L^{(\mathbb{Z}_p,+)+(p-1)p}$ | $L^{(\mathbb{Z}_p,+)}$ | $L^{(\mathbb{Z}_p,+)+p}$ | $L^{(\mathbb{Z}_p,+)+2p}$ | $\ldots$ |

where each row (or column) of $\mathbb{L}^{(\mathbb{F}_{p^2},+)}$ is cyclically generated by $\pi$ and consists of the set

$$\left\{L^{(\mathbb{Z}_p,+)}, L^{(\mathbb{Z}_p,+)+p}, L^{(\mathbb{Z}_p,+)+2p}, \ldots, L^{(\mathbb{Z}_p,+)+kp}, \ldots, L^{(\mathbb{Z}_p,+)+(p-1)p}\right\}$$

of prime order-$p$ cyclic latin sub-squares (each with rows that are cyclically generated by $\pi$) that are each equivalent to the latin square $L^{(\mathbb{Z}_p,+)}$ (up to order-preserving symbol relabeling) that encodes $(\mathbb{Z}_p, +)$. More generally, we say that a latin square $\mathbb{L}^{(\mathbb{F}_{p^d},+)} \in \mathcal{L}^{p^d}$ of prime power order-$p^d$ is *order-$p^d$ super-symmetric* if $\mathbb{L}^{(\mathbb{F}_{p^d},+)}$ can be written as the $p \times p$ latin sub-square grid

| | | | | |
|---|---|---|---|---|
| $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)}$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+p}$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+2p}$ | $\ldots$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+(p-1)p}$ |
| $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+p}$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+2p}$ | $\ldots$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+(p-1)p}$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)}$ |
| $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+2p}$ | $\ldots$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+(p-1)p}$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)}$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+p}$ |
| $\ldots$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+(p-1)p}$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)}$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+p}$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+2p}$ |
| $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+(p-1)p}$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)}$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+p}$ | $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+2p}$ | $\ldots$ |

where each row (or column) of $\mathbb{L}^{(\mathbb{F}_{p^2},+)}$ is cyclically generated by $\pi$ and consists of the set

$$\left\{\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)}, \mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+p}, \mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+2p}, \ldots, \mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+kp}, \ldots, \mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)+(p-1)p}\right\}$$

of prime power order-$p^{d-1}$ latin sub-squares (each with rows that are cyclically generated by $\pi$) that are each equivalent to the latin square $\mathbb{L}^{(\mathbb{F}_{p^{d-1}},+)}$.

Our proposed *Super-Symmetric Latin Square Generation Algorithm* (SS-LS-GA) for constructing a latin square that satisfies Definition 2.96 is Algorithm 2.3 in Appendix B.1.1. If $p = 2$, then the SS-LS-GA Java implementation starts with the cyclic latin square $L^{(\mathbb{Z}_2,+)}$ for $(\mathbb{Z}_2, +)$ and follows a procedure that is similar to the one proposed in [60]. Otherwise, if $p > 2$, then the SS-LS-GA starts with the cyclic latin square $L^{(\mathbb{Z}_p,+)}$ for $(\mathbb{Z}_p, +)$ and follows a procedure that is a generalization of the specific $p = 3$ case in Example 2.97. Note: in the $d = 1$ "base case", the SS-LS-GA will simply generate a prime order-$p$ cyclic latin square $L^{(\mathbb{Z}_p,+)}$. Thus, for any prime power order-$p^d$ super-symmetric latin square $\mathbb{L}^{(\mathbb{F}_{p^d},+)}$ we may assume that $d > 1$.

**Example 2.97.** Let $\mathbb{Z}_3 = (\mathbb{Z}_3, +)$ be the cyclic group of integers modulo 3 under addition. Let $L^{(\mathbb{Z}_3,+)}$ be the cyclic latin square of prime order-3 that encodes $(\mathbb{Z}_3, +)$ with symbols from $\{0, 1, 2\}$ and the maximum $\mathbb{T}(3)$, where each row (or column) of $L^{(\mathbb{Z}_3,+)}$ is cyclically generated by the permutation

$$\pi = \begin{pmatrix} 0 & 1 & 2 \\ \pi(0) & \pi(1) & \pi(2) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$$

to obtain

$$L^{(\mathbb{Z}_3,+)} = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \in \mathcal{L}^3 \subset \mathbb{Z}_3^{3\times 3}.$$

Then for $k = 0, 1, 2$ (with the order-preserving symbol relabeling) we obtain

$$L^{(\mathbb{Z}_3,+)} = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}, \quad L^{(\mathbb{Z}_3,+)+3} = \begin{bmatrix} 3 & 4 & 5 \\ 4 & 5 & 3 \\ 5 & 3 & 5 \end{bmatrix}, \quad \text{and} \quad L^{(\mathbb{Z}_3,+)+6} = \begin{bmatrix} 6 & 7 & 8 \\ 7 & 8 & 6 \\ 8 & 6 & 7 \end{bmatrix}$$

so the first order-3 latin sub-square row of the order-$3^2$ super-symmetric latin square $\mathbb{L}^{(\mathbb{F}_{3^2},+)}$ is the partial latin square

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |

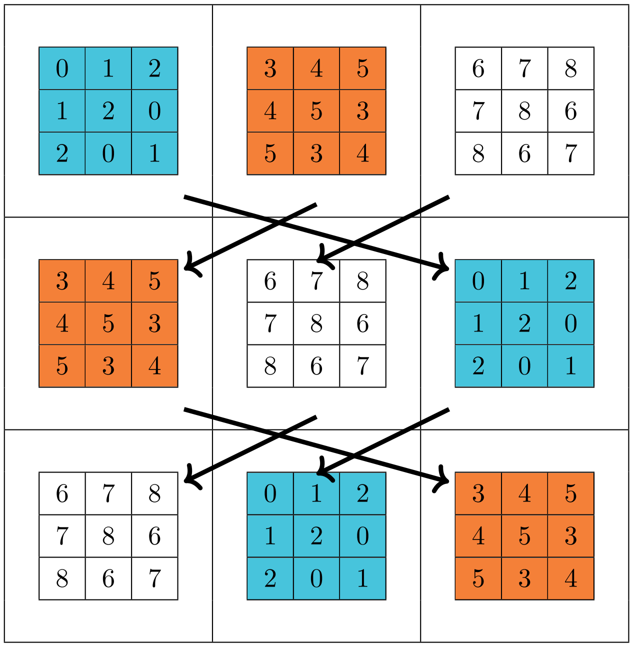
.

Then to cyclically generate the second and third rows (in order to complete $\mathbb{L}^{(\mathbb{F}_{3^2},+)}$) we reapply $\pi$ to the set $\{L^{(\mathbb{Z}_3,+)}, L^{(\mathbb{Z}_3,+)+3}, L^{(\mathbb{Z}_3,+)+6}\}$ comprising the first row, which we write as

$$\pi = \begin{pmatrix} L^{(\mathbb{Z}_3,+)} & L^{(\mathbb{Z}_3,+)+3} & L^{(\mathbb{Z}_3,+)+6} \\ \pi(L^{(\mathbb{Z}_3,+)}) & \pi(L^{(\mathbb{Z}_3,+)+3}) & \pi(L^{(\mathbb{Z}_3,+)+6}) \end{pmatrix} = \begin{pmatrix} L^{(\mathbb{Z}_3,+)} & L^{(\mathbb{Z}_3,+)+3} & L^{(\mathbb{Z}_3,+)+6} \\ L^{(\mathbb{Z}_3,+)+3} & L^{(\mathbb{Z}_3,+)+6} & L^{(\mathbb{Z}_3,+)} \end{pmatrix},$$

to construct the complete prime power order-$3^2$ super-symmetric latin square $\mathbb{L}^{(\mathbb{F}_{3^2},+)}$ given in Table 2.19. Thereafter, if we wish to further construct the prime power order-$3^3$ super-symmetric $\mathbb{L}^{(\mathbb{F}_{3^3},+)}$ given in Table 2.20, we simply iterate this procedure one more time.

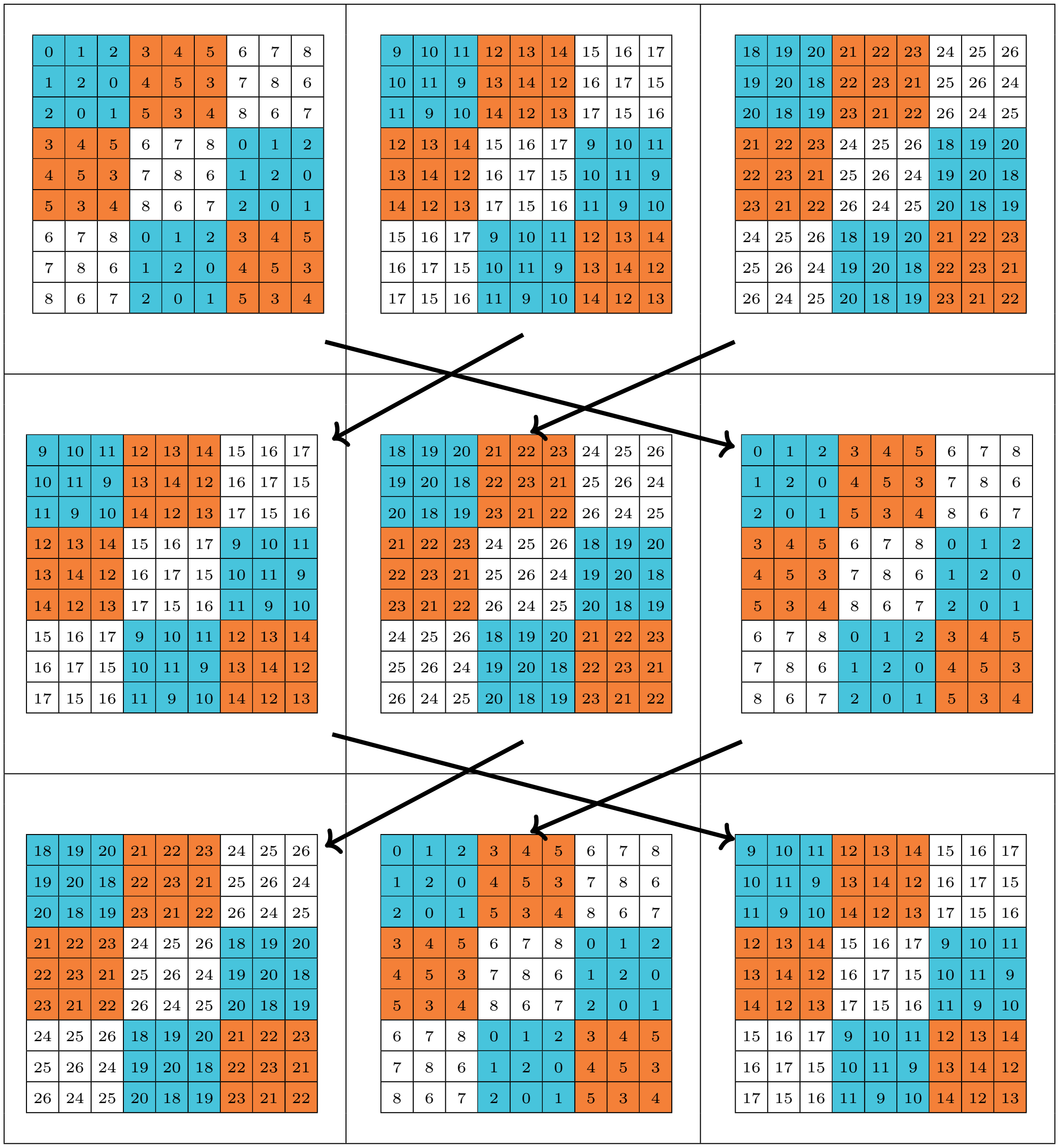
**Table 2.19: The self-similar prime power order-$3^2$ super-symmetric latin square $\mathbb{L}^{(\mathbb{F}_{3^2},+)}$ constructed using the SS-LS-GA. The permutation $\pi$ is the cyclic generator for the prime order-3 cyclic latin sub-squares. Thereafter, the prime order-3 cyclic latin sub-squares in the $3 \times 3$ grid are permuted with $\pi$.**



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |
| 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 |
| 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 |
| 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 |
| 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 |

.

**Table 2.20: The self-similar prime power order-$3^3$ super-symmetric latin square $\mathbb{L}^{(\mathbb{F}_{3^3},+)}$ constructed using the SS-LS-GA. The permutation $\pi$ is the cyclic generator for the prime order-3 cyclic latin sub-squares and also the prime power order-$3^2$ super-symmetric latin sub-squares.**



| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 | 10 | 11 | 9 | 13 | 14 | 12 | 16 | 17 | 15 | 19 | 20 | 18 | 22 | 23 | 21 | 25 | 26 | 24 |
| 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 | 11 | 9 | 10 | 14 | 12 | 13 | 17 | 15 | 16 | 20 | 18 | 19 | 23 | 21 | 22 | 26 | 24 | 25 |
| 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 | 12 | 13 | 14 | 15 | 16 | 17 | 9 | 10 | 11 | 21 | 22 | 23 | 24 | 25 | 26 | 18 | 19 | 20 |
| 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 | 13 | 14 | 12 | 16 | 17 | 15 | 10 | 11 | 9 | 22 | 23 | 21 | 25 | 26 | 24 | 19 | 20 | 18 |
| 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 | 14 | 12 | 13 | 17 | 15 | 16 | 11 | 9 | 10 | 23 | 21 | 22 | 26 | 24 | 25 | 20 | 18 | 19 |
| 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 | 15 | 16 | 17 | 9 | 10 | 11 | 12 | 13 | 14 | 24 | 25 | 26 | 18 | 19 | 20 | 21 | 22 | 23 |
| 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 | 16 | 17 | 15 | 10 | 11 | 9 | 13 | 14 | 12 | 25 | 26 | 24 | 19 | 20 | 18 | 22 | 23 | 21 |
| 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 | 17 | 15 | 16 | 11 | 9 | 10 | 14 | 12 | 13 | 26 | 24 | 25 | 20 | 18 | 19 | 23 | 21 | 22 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10 | 11 | 9 | 13 | 14 | 12 | 16 | 17 | 15 | 19 | 20 | 18 | 22 | 23 | 21 | 25 | 26 | 24 | 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| 11 | 9 | 10 | 14 | 12 | 13 | 17 | 15 | 16 | 20 | 18 | 19 | 23 | 21 | 22 | 26 | 24 | 25 | 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |
| 12 | 13 | 14 | 15 | 16 | 17 | 9 | 10 | 11 | 21 | 22 | 23 | 24 | 25 | 26 | 18 | 19 | 20 | 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| 13 | 14 | 12 | 16 | 17 | 15 | 10 | 11 | 9 | 22 | 23 | 21 | 25 | 26 | 24 | 19 | 20 | 18 | 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 |
| 14 | 12 | 13 | 17 | 15 | 16 | 11 | 9 | 10 | 23 | 21 | 22 | 26 | 24 | 25 | 20 | 18 | 19 | 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 |
| 15 | 16 | 17 | 9 | 10 | 11 | 12 | 13 | 14 | 24 | 25 | 26 | 18 | 19 | 20 | 21 | 22 | 23 | 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 16 | 17 | 15 | 10 | 11 | 9 | 13 | 14 | 12 | 25 | 26 | 24 | 19 | 20 | 18 | 22 | 23 | 21 | 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 |
| 17 | 15 | 16 | 11 | 9 | 10 | 14 | 12 | 13 | 26 | 24 | 25 | 20 | 18 | 19 | 23 | 21 | 22 | 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| 19 | 20 | 18 | 22 | 23 | 21 | 25 | 26 | 24 | 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 | 10 | 11 | 9 | 13 | 14 | 12 | 16 | 17 | 15 |
| 20 | 18 | 19 | 23 | 21 | 22 | 26 | 24 | 25 | 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 | 11 | 9 | 10 | 14 | 12 | 13 | 17 | 15 | 16 |
| 21 | 22 | 23 | 24 | 25 | 26 | 18 | 19 | 20 | 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 | 12 | 13 | 14 | 15 | 16 | 17 | 9 | 10 | 11 |
| 22 | 23 | 21 | 25 | 26 | 24 | 19 | 20 | 18 | 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 | 13 | 14 | 12 | 16 | 17 | 15 | 10 | 11 | 9 |
| 23 | 21 | 22 | 26 | 24 | 25 | 20 | 18 | 19 | 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 | 14 | 12 | 13 | 17 | 15 | 16 | 11 | 9 | 10 |
| 24 | 25 | 26 | 18 | 19 | 20 | 21 | 22 | 23 | 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 | 15 | 16 | 17 | 9 | 10 | 11 | 12 | 13 | 14 |
| 25 | 26 | 24 | 19 | 20 | 18 | 22 | 23 | 21 | 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 | 16 | 17 | 15 | 10 | 11 | 9 | 13 | 14 | 12 |
| 26 | 24 | 25 | 20 | 18 | 19 | 23 | 21 | 22 | 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 | 17 | 15 | 16 | 11 | 9 | 10 | 14 | 12 | 13 |

### 2.8.3 Connecting Super-Symmetric Latin Squares, Galois Field Addition Groups, and Maximum Transversal Count Predictions

So we use our SS-LS-GA implementation to generate the super-symmetric latin squares $\mathbb{L}^{(\mathbb{F}_{2^2},+)} \in \boldsymbol{\mathcal{L}}^{2^2}$, $\mathbb{L}^{(\mathbb{F}_{2^3},+)} \in \boldsymbol{\mathcal{L}}^{2^3}$, and $\mathbb{L}^{(\mathbb{F}_{3^2},+)} \in \boldsymbol{\mathcal{L}}^{3^2}$. A further "visual" examination of these squares leads to the realization that these self-similar latin squares (with prime power order-$p^d$ for $4 \leq n = p^d \leq 9$ with $d > 1$) are in fact the corresponding addition group Cayley tables of the Galois fields $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^3}$, and $\mathbb{F}_{3^2}$!

Thus, let us further illustrate this connection between super-symmetric latin squares and Galois field addition groups.

First, we choose the degree 2 irreducible polynomial $x^2 + 1 \in \mathbb{Z}_2[x]$ to construct the Galois field $\mathbb{F}_{2^2}[x] = \mathbb{Z}_2[x]/\langle x^2 + 1\rangle \cong \mathbb{F}_{2^2}$ to obtain the corresponding addition group $(\mathbb{F}_{2^2}[x], +) \cong (\mathbb{F}_{2^2}, +)$ with the super-symmetric Cayley table

| $+$ | $\mathbf{0}$ | $\mathbf{1}$ | $\boldsymbol{x}$ | $\boldsymbol{x+1}$ |
|---|---|---|---|---|
| $\mathbf{0}$ | $0$ | $1$ | $x$ | $x+1$ |
| $\mathbf{1}$ | $1$ | $0$ | $x+1$ | $x$ |
| $\boldsymbol{x}$ | $x$ | $x+1$ | $0$ | $1$ |
| $\boldsymbol{x+1}$ | $x+1$ | $x$ | $1$ | $0$ |

$L^{(\mathbb{F}_{2^2}[x],+)}$ **Polynomial Form**

$\cong$

| $+$ | $\mathbf{0}$ | $\mathbf{1}$ | $\mathbf{2}$ | $\mathbf{3}$ |
|---|---|---|---|---|
| $\mathbf{0}$ | 0 | 1 | 2 | 3 |
| $\mathbf{1}$ | 1 | 0 | 3 | 2 |
| $\mathbf{2}$ | 2 | 3 | 0 | 1 |
| $\mathbf{3}$ | 3 | 2 | 1 | 0 |

$L^{(\mathbb{F}_{2^2},+)}$ **Symbol Form**

,

where we let $x = 2$ to obtain the equivalent symbol form. We observe that $L^{(\mathbb{F}_{2^2},+)}$ contains 4 adjacent latin sub-square "building blocks" that are each a prime order-2 cyclic latin square that is equivalent to $L^{(\mathbb{Z}_2,+)}$ and possesses $\mathbb{T}(2) = \mathbb{t}(2) = 0$ transversals (the confirmed maximum and minimum).

Second, we choose the degree 3 irreducible polynomial $x^3 + x + 1 \in \mathbb{Z}_2[x]$ to construct the Galois field $\mathbb{F}_{2^3}[x] = \mathbb{Z}_2[x]/\langle x^3+x+1\rangle \cong \mathbb{F}_{2^3}$ to obtain the corresponding addition group $(\mathbb{F}_{2^3}[x], +) \cong (\mathbb{F}_{2^3}, +)$ with the super-symmetric Cayley table

| $+$ | $\mathbf{0}$ | $\mathbf{1}$ | $\mathbf{2}$ | $\mathbf{2{+}1}$ | $\mathbf{2^2}$ | $\mathbf{2^2{+}1}$ | $\mathbf{2^2{+}2}$ | $\mathbf{2^2{+}2{+}1}$ |
|---|---|---|---|---|---|---|---|---|
| $\mathbf{0}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| $\mathbf{1}$ | 1 | 0 | 3 | 2 | 5 | 4 | 7 | 6 |
| $\mathbf{2}$ | 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 |
| $\mathbf{2{+}1}$ | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 |
| $\mathbf{2^2}$ | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| $\mathbf{2^2{+}1}$ | 5 | 4 | 7 | 6 | 1 | 0 | 3 | 2 |
| $\mathbf{2^2{+}2}$ | 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 |
| $\mathbf{2^2{+}2{+}1}$ | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

,

where we let $x = 2$ to obtain the equivalent symbol form. We observe that $L^{(\mathbb{F}_{2^3},+)}$ contains 4 adjacent latin sub-squares in a $2 \times 2$ that are each a prime power order-$2^2$ latin square that is equivalent to $L^{(\mathbb{F}_{2^2},+)}$. Moreover, we observe that each latin square that is equivalent to $L^{(\mathbb{F}_{2^2},+)}$ contains 4 adjacent latin sub-squares in a $2 \times 2$ grid that are each a prime order-2 cyclic latin square that is equivalent to $L^{(\mathbb{Z}_2,+)}$ and possesses $\mathbb{T}(2) = \mathfrak{t}(2) = 0$ transversals.

Third, we choose the degree 2 irreducible polynomial $x^2 + 1 \in \mathbb{Z}_3[x]$ to construct the Galois field $\mathbb{F}_{3^2}[x] = \mathbb{Z}_3[x]/\langle x^2 + 1\rangle \cong \mathbb{F}_{3^2}$ to obtain the corresponding addition group $(\mathbb{F}_{3^2}[x], +) \cong (\mathbb{F}_{3^2}, +)$ with the super-symmetric Cayley table

| $+$ | $\mathbf{0}$ | $\mathbf{1}$ | $\mathbf{2}$ | $\mathbf{3}$ | $\mathbf{3{+}1}$ | $\mathbf{3{+}2}$ | $\mathbf{2{\cdot}3}$ | $\mathbf{2{\cdot}3{+}1}$ | $\mathbf{2{\cdot}3{+}2}$ |
|---|---|---|---|---|---|---|---|---|---|
| $\mathbf{0}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| $\mathbf{1}$ | 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| $\mathbf{2}$ | 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |
| $\mathbf{3}$ | 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| $\mathbf{3{+}1}$ | 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 |
| $\mathbf{3{+}2}$ | 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 |
| $\mathbf{2{\cdot}3}$ | 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| $\mathbf{2{\cdot}3{+}1}$ | 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 |
| $\mathbf{2{\cdot}3{+}2}$ | 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 |

,

where we let $x = 3$ to obtain the equivalent symbol form. We observe that $L^{(\mathbb{F}_{3^2},+)}$ contains 9 adjacent latin sub-squares in a $3 \times 3$ grid that are each a prime order-3 cyclic latin square that is equivalent to $L^{(\mathbb{Z}_3,+)}$ and possesses $\mathbb{T}(3) = 3$ transversals.

At this point, our hypothesis becomes: $L^{(\mathbb{F}_{2^2},+)}$*,* $L^{(\mathbb{F}_{2^3},+)}$*, and* $L^{(\mathbb{F}_{3^2},+)}$ *may have the maximum confirmed* $\mathbb{T}(4)$*,* $\mathbb{T}(8)$*, and* $\mathbb{T}(9)$*, respectively.* Since the $\mathbb{T}(n)$ for $4 \leq p^d \leq 9$ have been confirmed in [5, 6, 8], then we know it is possible to determine if our prediction is correct or incorrect.

Thus, we use our BM-LS-TCAv3 implementation to count the number of transversals in the super-symmetric latin squares $L^{(\mathbb{F}_{2^2},+)}$, $L^{(\mathbb{F}_{2^3},+)}$, and $L^{(\mathbb{F}_{3^2},+)}$ and report the results in Table 2.21; the respective $\mathbb{T}(4)$, $\mathbb{T}(8)$, and $\mathbb{T}(9)$ [5, 6, 8] are re-listed next to our super-symmetric latin squares transversal counts in Table 2.21.

**Table 2.21: The transversal counts for the super-symmetric latin squares $L^{(\mathbb{F}_{2^2},+)}$, $L^{(\mathbb{F}_{2^3},+)}$, and $L^{(\mathbb{F}_{3^2},+)}$ that encode the addition groups of Galois fields are equal to the respectively confirmed maximum transversal counts $\mathbb{T}(4)$, $\mathbb{T}(8)$, and $\mathbb{T}(9)$. Our prediction is correct!**

| **Order-$n$** | **Galois Field Latin Square** | **Galois Field Addition Group** | **Observed # Transversals** | **Confirmed # Transversals Range:** $[\mathtt{t}(n), \mathbb{T}(n)]$ |
|---|---|---|---|---|
| $2^2 = 4$ | $L^{(\mathbb{F}_{2^2},+)}$ | $(\mathbb{F}_{2^2},+)$ | **8** | $[0, \mathbf{8}]$ |
| $2^3 = 8$ | $L^{(\mathbb{F}_{2^3},+)}$ | $(\mathbb{F}_{2^3},+)$ | **384** | $[0, \mathbf{384}]$ |
| $3^2 = 9$ | $L^{(\mathbb{F}_{3^2},+)}$ | $(\mathbb{F}_{3^2},+)$ | **2 241** | $[68, \mathbf{2\ 241}]$ |

In Table 2.21 we observe an exciting result: *our prediction is correct!* More specifically, we observe that the super-symmetric latin squares of prime power order-$p^d$ (with $4 \leq p^d \leq 9$) that encode the Galois field addition Cayley tables—namely $L^{(\mathbb{F}_{2^2},+)}$, $L^{(\mathbb{F}_{2^3},+)}$, and $L^{(\mathbb{F}_{3^2},+)}$—have *maximum* transversal counts that match $\mathbb{T}(4)$, $\mathbb{T}(8)$, and $\mathbb{T}(9)$, respectively; a significant improvement over the respective zero transversal counts of the cyclic Cayley tables $L^{(\mathbb{Z}_4,+)}$, $L^{(\mathbb{Z}_8,+)}$, and $L^{(\mathbb{Z}_9,+)}$ that we reported in Tables 2.17 and 2.18.

To us, these prediction results suggest that perhaps the maximum transversal counts of prime order cyclic latin squares may be directly related to the maximum transversal counts of self-similar prime power order super-symmetric latin squares that are built from appropriately arranged cyclic latin sub-squares; such evidence seems to support the idea that it may be possible to predict which types of prime power order-$p^d$ latin squares will possess the maximum number of transversals!

### 2.8.4 Results and Conjectures

Here, based on the results of the preceding sections, we further examine the transversal counts of prime power order-$p^d$ cyclic and super-symmetric latin squares for $3 \leq n = p^d \leq 17$ with $d > 0$.

First, for latin squares with prime power orders $3 \leq p^d \leq 17$, we report the comparison between the maximum transversal counts of our NPS-LS-GA generated data sets with the maximum transversal counts of the cyclic and super-symmetric latin squares generated by our SS-LS-GA in Table 2.22; these cyclic and super-symmetric latin squares are listed in Appendix C. Note: due to current limitations on computational resources, we are only able to count the number of transversals for subsets of our data sets with latin squares up to order-16 and a single order-17 latin square.

In Table 2.22 we observe that:

1. For prime power orders $3 \leq p^d \leq 16$, the cyclic and super-symmetric latin square transversal counts are always greater than or equal to the latin squares in the NPS-LS-GA generated data sets.
2. For prime power orders $3 \leq p^d \leq 9$, the cyclic and super-symmetric latin square transversal counts are all equal to the confirmed maximum transversal counts $\mathbb{T}(p^d)$ that are reported in [5, 6, 8].

**Table 2.22: For latin squares with prime power orders $3 \leq p^d \leq 16$ with $d > 0$, we compare the observed maximum transversal counts of our NPS-LS-GA generated data sets with the observed maximum transversal counts of the cyclic and super-symmetric latin squares generated by our SS-LS-GA, which are then compared with either the confirmed $\mathbb{T}(p^d)$ or the estimated bounds $[\lfloor \mathbb{T}(p^d) \rfloor_{\mathbf{MMW}}, \lceil \mathbb{T}(p^d) \rceil_{\mathbf{MMW}}]$.**

| **Prime Power Order-$p^d$** | **Data Set Size: # Latin Squares (NPS-LS-GA)** | **Observed Max # Transversals: Data Set (NPS-LS-GA)** | **Observed # Transversals: Cyclic or Super-Symmetric (SS-LS-GA)** | **Max # Transversals: Confirmed $\mathbb{T}(p^d)$ or Estimated Bounds $[\lfloor \mathbb{T}(p^d) \rfloor_{\mathbf{MMW}}, \lceil \mathbb{T}(p^d) \rceil_{\mathbf{MMW}}]$** |
|---|---:|---:|---:|---:|
| $3^1 = 3$ | 12 | **3** | **3** | **3** |
| $2^2 = 4$ | 576 | **8** | **8** | **8** |
| $5^1 = 5$ | 161 280 | **15** | **15** | **15** |
| $7^1 = 7$ | 3 000 000 | 63 | **133** | **133** |
| $2^3 = 8$ | 2 750 000 | **384** | **384** | **384** |
| $3^2 = 9$ | 2 500 000 | 444 | **2 241** | **2 241** |
| $11^1 = 11$ | 500 000 | 3 896 | **37 851** | [**37 851**, 528 647] |
| $13^1 = 13$ | 176 516 | 82 628 | **1 030 367** | [**1 030 367**, 32 837 805] |
| $2^4 = 16$ | 358 | 183 558 144 | **244 744 192** | [**244 744 192**, 28 218 998 328] |

3. For prime power orders $9 < p^d \leq 16$, the cyclic and super-symmetric latin square transversal counts are all equal to the estimated lower bounds on the maximum transversal counts $\lfloor \mathbb{T}(p^d) \rfloor_{\mathbf{MMW}}$ that are reported in [5, 6, 8].

Next, we wish to investigate a possible relationship between transversal counts and the following:

**Definition 2.98.** Let $L^{\mathcal{G}}$ be a latin square that encodes the quasi-group $\mathcal{G} = (\mathcal{G}, \star)$. For any $g_x, g_y \in \mathcal{G}$ let $L^{\mathcal{G}}_{g_x,g_y}$ be the entry of $L^{\mathcal{G}}$ at row $g_x$ and column $g_y$. Then we say that:

- The number of times that a transversal of $L^{\mathcal{G}}$ passes through $L^{\mathcal{G}}_{g_x,g_y}$ is the *heat value of entry* $L^{\mathcal{G}}_{g_x,g_y}$, which we denote by $h(L^{\mathcal{G}}_{g_x,g_y})$.
- The $n \times n$ matrix $\mathbb{H}(L^{\mathcal{G}})$ is the *heat map* of $L^{\mathcal{G}}$ if each entry $\mathbb{H}(L^{\mathcal{G}}_{g_x,g_y})$ of $\mathbb{H}(L^{\mathcal{G}})$ at row $g_x$ and column $g_y$ contains $h(L^{\mathcal{G}}_{g_x,g_y})$ for all $g_x, g_y \in \mathcal{G}$.

- $h(L^{\mathcal{G}})$ is the *(uniform entry) heat value* of $L^{\mathcal{G}}$ if $h(L^{\mathcal{G}}_{g_{x_1},g_{y_1}}) = h(L^{\mathcal{G}}_{g_{x_2},g_{y_2}})$ for all $g_{x_1}, g_{y_1}, g_{x_2}, g_{y_2} \in \mathcal{G}$.

**Example 2.99.** Suppose that we have the following order-9 latin squares

$L^{(\mathcal{G},\star)}$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 0 | 3 | 2 | 5 | 4 | 7 | 8 | 6 |
| 2 | 3 | 0 | 1 | 6 | 7 | 8 | 4 | 5 |
| 3 | 2 | 1 | 0 | 7 | 8 | 5 | 6 | 4 |
| 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 | 3 |
| 5 | 4 | 7 | 8 | 0 | 6 | 2 | 3 | 1 |
| 6 | 7 | 8 | 4 | 1 | 2 | 3 | 5 | 0 |
| 7 | 8 | 5 | 6 | 3 | 1 | 4 | 0 | 2 |
| 8 | 6 | 4 | 5 | 2 | 3 | 0 | 1 | 7 |

$L^{(\mathbb{Z}_9,+)}$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 0 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 |
| 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 | 3 |
| 5 | 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 |
| 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 8 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

$L^{(\mathbb{F}_{3^2},+)}$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |
| 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 |
| 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 |
| 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 |
| 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 |

that encode some order-9 quasi-group $\mathcal{G} = (\mathcal{G}, \star)$, the order-9 cyclic group $\mathbb{Z}_9 = (\mathbb{Z}_9, +)$, and the order-9 group $\mathbb{F}_{3^2} = (\mathbb{F}_{3^2}, +)$ of Galois field addition. Then we compute the number of transversals for $L^{(\mathcal{G},\star)}$, $L^{(\mathbb{Z}_9,+)}$, and $L^{(\mathbb{F}_{3^2},+)}$ using the BM-LS-TCAv3 implementation and simply record the number of times that each entry appears in a transversal in a $9 \times 9$ heat map matrix; we obtain the respective transversal counts $|\mathcal{T}(L^{(\mathcal{G},\star)})| = 150$, $|\mathcal{T}(L^{(\mathbb{Z}_9,+)})| = 2{,}025$, and $|\mathcal{T}(L^{(\mathbb{F}_{3^2},+)})| = 2{,}241$, along with the corresponding heat maps

$\mathbb{H}(L^{(\mathcal{G},\star)})$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 22 | 27 | 20 | 14 | 12 | 13 | 21 | 12 | 9 |
| 19 | 15 | 24 | 19 | 10 | 18 | 10 | 15 | 20 |
| 26 | 24 | 25 | 20 | 18 | 15 | 7 | 11 | 4 |
| 23 | 15 | 12 | 23 | 21 | 12 | 20 | 10 | 14 |
| 12 | 10 | 15 | 13 | 42 | 16 | 15 | 10 | 17 |
| 10 | 17 | 16 | 15 | 11 | 33 | 18 | 9 | 21 |
| 9 | 10 | 11 | 20 | 12 | 14 | 11 | 57 | 6 |
| 11 | 21 | 13 | 13 | 13 | 14 | 32 | 16 | 17 |
| 18 | 11 | 14 | 13 | 11 | 15 | 16 | 10 | 42 |

,

$\mathbb{H}(L^{(\mathbb{Z}_9,+)})$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 |
| 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 |
| 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 |
| 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 |
| 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 |
| 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 |
| 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 |
| 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 |
| 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 | 225 |

$\mathbb{H}(L^{(\mathbb{F}_{3^2},+)})$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |

.

We observe that $\mathbb{H}(L^{\mathcal{G}})$ has *non-uniform* entry heat values, while $\mathbb{H}(L^{(\mathbb{Z}_9,+)})$ and $\mathbb{H}(L^{(\mathbb{F}_{3^2},+)})$ have *uniform* entry heat values of $h(L^{(\mathbb{Z}_9,+)}) = 225$ and $h(L^{(\mathbb{F}_{3^2},+)}) = 249$, respectively. Moreover, for the uniform cases, we observe that

$$\begin{aligned} |\mathcal{T}(L^{(\mathbb{Z}_9,+)})| &= h(L^{(\mathbb{Z}_9,+)}) \bullet 9 = 225 \bullet 9 = 2{,}025 \text{ and} \\ |\mathcal{T}(L^{(\mathbb{F}_{3^2},+)})| &= h(L^{(\mathbb{F}_{3^2},+)}) \bullet 9 = 249 \bullet 9 = 2{,}241, \end{aligned}$$

where $|\mathcal{T}(L^{(\mathbb{F}_{3^2},+)})| = 2{,}241 = \mathbb{T}(9)$.

Using the approach described in Example 2.99, we compute the heat maps for the cyclic and super-symmetric latin squares of prime power orders $3 \leq p^d \leq 17$; the heat maps are listed in Appendix C. Interestingly enough, we observe that *each of these cyclic and super-symmetric latin squares have a uniform heat value*! Hence, in Table 2.23 we report the apparent relationship between the transversal counts, the uniform heat values, and the prime power order of each cyclic or super-symmetric latin square. Note: we are finally able to process the single cyclic latin square of prime order-17, so we also include that result in Table 2.23.

**Table 2.23: For cyclic and super-symmetric latin squares with prime power orders $3 \leq p^d \leq 17$ generated by our SS-LS-GA, we report the apparent relationship between the transversal counts, the uniform heat values, and the order. For prime power orders $3 \leq p^d \leq 9$ the transversal counts are all equal to the confirmed maximum transversal counts $\mathbb{T}(p^d)$, whereas for prime power orders $9 < p^d \leq 17$ the transversal counts are equal to the estimated lower bounds on the maximum transversal counts $\lfloor \mathbb{T}(p^d) \rfloor_{\text{MMW}}$; these are marked in (blue) bold.**

| Prime Power Order-$p^d$ | Type | Observed Uniform Heat Value | Observed # Transversals: Cyclic or Super-Symmetric | Max # Transversals: Confirmed $\mathbb{T}(p^d)$ or Estimated Bounds $[\lfloor \mathbb{T}(p^d) \rfloor_{\text{MMW}}, \lceil \mathbb{T}(p^d) \rceil_{\text{MMW}}]$ |
|---|---|---|---|---|
| $3^1 = 3$ | Cyclic | 1 | $3^1 \cdot 1 =$ **3** | **3** |
| $2^2 = 4$ | Super-Symm. | 2 | $2^2 \cdot 2 =$ **8** | **8** |
| $5^1 = 5$ | Cyclic | 3 | $5^1 \cdot 3 =$ **15** | **15** |
| $7^1 = 7$ | Cyclic | 19 | $7^1 \cdot 19 =$ **133** | **133** |
| $2^3 = 8$ | Super-Symm. | 48 | $2^3 \cdot 48 =$ **384** | **384** |
| $3^2 = 9$ | Super-Symm. | 249 | $3^2 \cdot 249 =$ **2 241** | **2 241** |
| $11^1 = 11$ | Cyclic | 3 441 | $11^1 \cdot 3\,441 =$ **37 851** | [**37 851**, 528 647] |
| $13^1 = 13$ | Cyclic | 79 259 | $13^1 \cdot 79\,259 =$ **1 030 367** | [**1 030 367**, 32 837 805] |
| $2^4 = 16$ | Super-Symm. | 15 296 512 | $2^4 \cdot 15\,296\,512 =$ **244 744 192** | [**244 744 192**, 28 218 998 328] |
| $17^1 = 17$ | Cyclic | 94 471 089 | $17^1 \cdot 94\,471\,089 =$ **1 606 008 513** | [**1 606 008 513**, 300 502 249 052] |

In Table 2.23 we observe that some interesting related sequences are:

1. The transversal counts for cyclic and super-symmetric latin squares of prime power orders $3 \leq p^d \leq 17$:

$$3, 8, 15, 133, 384, 2241, 37851, 1030367, 244744192, 1606008513.$$

2. The uniform heat values of entries for cyclic and super-symmetric latin squares of prime power orders $3 \leq p^d \leq 17$:

$$1, 2, 3, 19, 48, 249, 3441, 79259, 15296512, 94471089.$$

Moreover, based on the preliminary evidence of Table 2.23, we propose the following:

**Conjecture 2.100.** *Let $L \in \mathcal{L}^{p^d}$ be a cyclic or super-symmetric latin square of prime power order-$p^d$ with $d > 0$. Then:*

*(i) $L$ possesses the maximum number of transversals $\mathbb{T}(p^d)$ for any order-$p^d$ latin square.*

*(ii) $L$ possesses a uniform heat value uniform heat value $h(L)$, where the number of transversals is $\mathbb{T}(p^d) = |\mathcal{T}(L)| = h(L) \bullet p^d$.*

**Remark 2.101.** Our conjecture predicts that for prime power order-$p^d$ with $d > 0$:

- The estimated lower bound $\lfloor \mathbb{T}(p^d) \rfloor$ in [5, 6, 8] may be the correct $\mathbb{T}(p^d)$.
- The estimated upper bound $\lceil \mathbb{T}(p^d) \rceil$ in [5, 6, 8] may be too high.

**Remark 2.102.** At this point we briefly recall the latin square equivalence classes of Section 2.4: isotopy classes, conjugacy classes, and main classes. More specifically, in Definition 2.48 it is said that two latin squares $L^{\mathcal{G}}, L^{\mathcal{H}} \in \mathcal{L}^n$ are main class equivalent if one of them is isotopic equivalent to some $L^{\mathcal{K}} \in \mathcal{L}^n$ that is conjugate equivalent to the other. In other words, all of the latin squares in the same main class have essentially the same structure [6]. This implies that all of the latin squares in the same main class have the same number of transversals. Thus, if Conjecture 2.100 is correct, then it follows that: if $L^{\mathcal{G}} \in \mathcal{L}^{p^d}$ is a latin square of prime power order-$p^d$

with $d > 0$ that is main class equivalent to a cyclic or super-symmetric latin square $L^{\mathcal{H}} \in \mathcal{L}^{p^d}$ (i.e. generated by the SS-LS-GA), then $L^{\mathcal{G}}$ possesses the maximum number of transversals $\mathbb{T}(p^d)$.

It would be very interesting to test Conjecture 2.100 by generating cyclic and super-symmetric latin squares of larger prime power orders (such as $5^2$ and $3^3$, etc.) and counting their transversals to see if Conjecture 2.100 holds. Unfortunately, we only have the practical capability to count all of the transversals of latin squares up to order-17 due to the hardware restrictions of our current computing resources. Perhaps in the near future it will be possible to determine if Conjecture 2.100 is correct for any order-$p^d$ via the methods of science and mathematics.

In the meantime, let's use the largest super-symmetric latin square that we know has the confirmed maximum number of transversals, namely $L^{(\mathbb{F}_{3^2},+)}$, to design and implement a new cryptographic system in the next chapter!

# CHAPTER 3

# CRYPTOGRAPHIC APPLICATION

## 3.1 Introduction to Cryptographic Hash Functions

A critical sector of cryptographic research, development, and application is that of *cryptographic hash functions* (CHF). A CHF is a mathematical algorithm defined as a function $\mathcal{F} : \mathfrak{M} \to \mathfrak{H}$ that maps an input *message* $\mathcal{M} \in \mathfrak{M}$ of an arbitrary size to an output hash $\mathcal{H} \in \mathfrak{H}$ of a fixed size.

The ideal computationally secure CHF has three main properties:

1. *Preimage resistance*: Given a hash $\mathcal{H}_i \in \mathfrak{H}$, it is computationally infeasible for an attacker to find a message $\mathcal{M}_i \in \mathfrak{M}$ with the same hash, such that $\mathcal{H}_i = \mathcal{F}(\mathcal{M}_i)$.

2. *Second preimage resistance*: Given a message $\mathcal{M}_i \in \mathfrak{M}$, it is computationally infeasible for an attacker to find a second message $\mathcal{M}_j \in \mathfrak{M}$ such that $\mathcal{M}_i \neq \mathcal{M}_j$ but $\mathcal{F}(\mathcal{M}_i) = \mathcal{F}(\mathcal{M}_j) \in \mathfrak{H}$.

3. *Collision resistance*: It is computationally infeasible for the attacker to choose any two messages $\mathcal{M}_i, \mathcal{M}_j \in \mathfrak{M}$ with $\mathcal{M}_i \neq \mathcal{M}_j$ and $\mathcal{F}(\mathcal{M}_i) = \mathcal{F}(\mathcal{M}_j) \in \mathfrak{H}$.

Table 3.1 includes examples of six distinct messages and their corresponding hashes, which are generated using the MD5 CHF created by Rivest in 1992 [113].

We observe that a small (single character) change to the input message yields a dramatically different output hash; this desirable property of cryptographic algorithms is known as the *avalanche effect* [114].

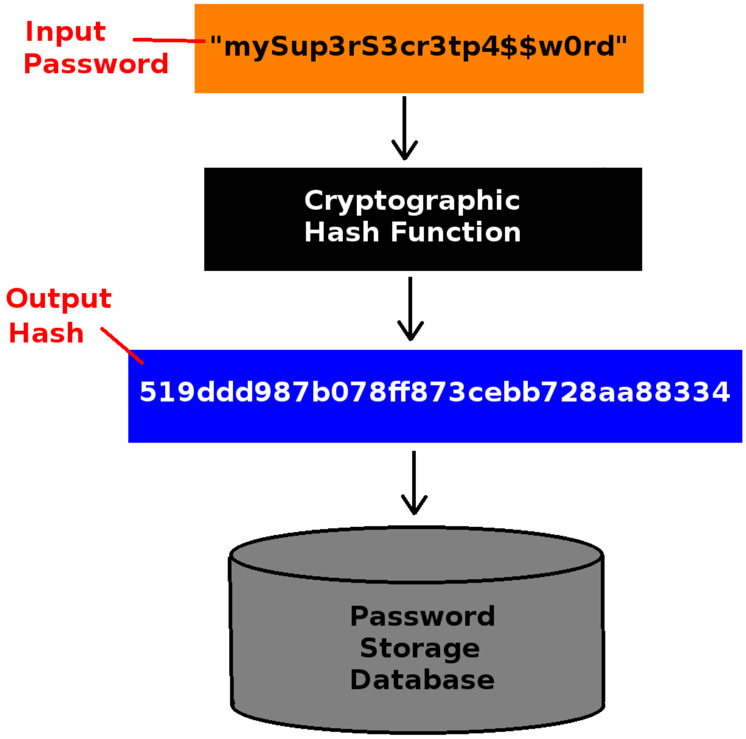
**Table 3.1: Examples of arbitrarily sized input messages and their corresponding 128-bit output hashes.**

| Input Message (Arbitrary Size) | Output Hash (128-Bit Size) |
|---|---|
| $\mathcal{M}_0 =$ “`mySup3rS3cr3tp4$$w0rd`” | $\mathcal{F}(\mathcal{M}_0) =$ `519ddd987b078ff873cebb728aa88334` |
| $\mathcal{M}_1 =$ “`MySup3rS3cr3tp4$$w0rd`” | $\mathcal{F}(\mathcal{M}_1) =$ `438e74075616dd238dfd0989c372626d` |
| $\mathcal{M}_2 =$ “`'In the middle of difficulty lies opportunity.' -A. Einstein`” | $\mathcal{F}(\mathcal{M}_2) =$ `f6d25cb72eae4cf5c4dcb65580e548d2` |
| $\mathcal{M}_3 =$ “`'In the middle of difficulty l1es opportunity.' -A. Einstein`” | $\mathcal{F}(\mathcal{M}_3) =$ `6c91069711f3ee39af23e05e99e76995` |
| $\mathcal{M}_4 =$ “`'Never trust a computer you can’t throw out a window.' -S. Wozniak`” | $\mathcal{F}(\mathcal{M}_4) =$ `cf237059c1acc17db94290ffe0c887c3` |
| $\mathcal{M}_5 =$ “`'Nev3r trust a computer you can’t throw out a window.' -S. Wozniak`” | $\mathcal{F}(\mathcal{M}_5) =$ `b15b56ab21de119480413cd4a0ed2884` |

CHFs have been nicknamed the “workhorses of modern cryptography” [115] because they have numerous crucial applications in the territory of cyber security. For instance, a major notable area of application is that of *authentication*: the process of determining whether someone or something is, in fact, who or what they declare to be. For example, CHFs are deployed for password verification, digital signatures, digital fingerprinting, and message authentication codes [116, 117, 118, 119]; see Figures 3.1 and 3.2 for an example depiction of password hashing and authentication. Furthermore, CHFs are also utilized to generate and evaluate checksums for *integrity verification* [116, 120]; accidental or malicious data corruption of messages, passwords, files, or hard drives can be detected by computing the checksum for such data and then comparing it to the target checksum.

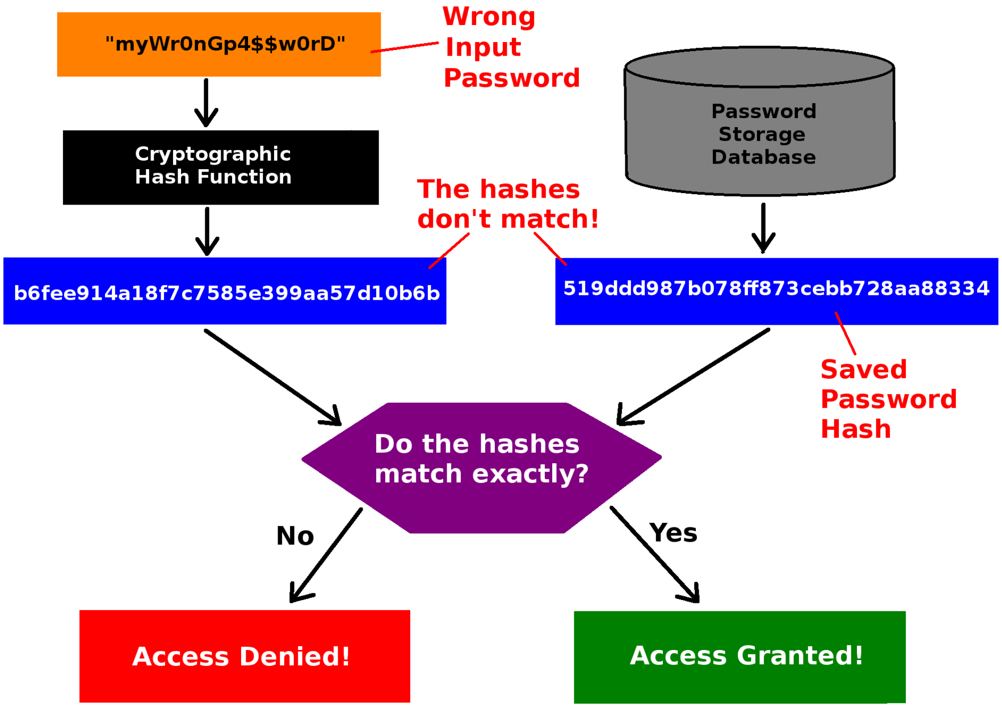
Thus, in order to assess of the degree of protection, strength, and reliability that a given CHF offers, it is paramount to rigorously evaluate the CHF’s preimage

**Figure 3.1: A simple depiction of the account password hashing and storing process. First, user Bob's password (message) is fed into the CHF as input. Then the CHF computes and outputs the hash, which is then stored in a database. Now user Bob has an account on the system.**


Input Password
"mySup3rS3cr3tp4$$w0rd"
Cryptographic Hash Function
Output Hash
519ddd987b078ff873cebb728aa88334
Password Storage Database

resistance, second preimage resistance, and collision resistance both computationally and mathematically. Hence, these three important CHF resistance properties imply that a malicious adversary cannot modify or replace the original message without altering the corresponding hash. If a CHF lacks one or more of the said resistance properties, then it exhibits a weakness and thus is vulnerable to attack in practice; this implies that the CHF can potentially be "hacked", exploited, and/or circumvented in the "real world". In such a case that a CHF exhibits a weakness, then it is imperative for the analysts to hunt down and identify the weakness mechanism so appropriate fixes and security measures can be immediately implemented. Hence, the need and

**Figure 3.2: A simple depiction of the user authentication process. Evil Eve is trying to guess user Bob's password. Evil Eve submits a password. The CHF computes and outputs Evil Eve's proposed hash, which is then compared to user Bob's hash that is stored in the database. In this case, since Evil Eve submits the wrong password, then the hashes don't match. So Evil Eve will be denied access.**


"myWr0nGp4$$w0rD"
Wrong Input Password
Cryptographic Hash Function
Password Storage Database
The hashes don't match!
b6fee914a18f7c7585e399aa57d10b6b
519ddd987b078ff873cebb728aa88334
Saved Password Hash
Do the hashes match exactly?
No
Yes
Access Denied!
Access Granted!

motivation to examine the underlying algebraic and algorithmic characteristics of CHFs arise.

Thus, order to assess the computational security of a crypto-system such as a CHF, one must mathematically and computationally evaluate the algebraic structures upon which it operates. A great strategy for assessing a CHF is through publicly open international competitions, where scientists, mathematicians, programmers, and hackers from around the globe have the opportunity to design, implement, evaluate, and discuss various CHF candidates. One example of such an event was the 2007-2012 NIST Hash Function Competition held by the U.S. National Institute of Standards and Technology (NIST) [121], where the objective was to openly develop a new CHF called Secure Hash Algorithm 3 (SHA-3) for standardization that is more computationally secure that its SHA-1 and SHA-2 predecessors. NIST selected 51 entries for round 1 [122], where 14 of those teams advanced to round 2 [123, 124], from which the 5 finalists were selected for round 3 [125]:

1. *BLAKE* by Aumasson, Henzen, Meier, and Phan [126].
2. *Grøstl* by Gauravaram, Knudsen, Matusiewicz, Mendel, Rechberger, Schläffer, and Thomsen [61].
3. *JH* by Wu [127].
4. *Keccak* by Bertoni, Daemen, Peeters, and Van Assche [128].
5. *Skein* by Schneier, Ferguson, Lucks, Whiting, Bellare, Kohno, Callas, and Walker [129].

In October of 2012 NIST selected Keccak as the winner [125] which was subsequently released as the SHA-3 standard in August of 2015 [130].

We selected Grøstl [61] for the cryptographic application component of this thesis. In our opinion, Grøstl is an excellent CHF for study and application. A key design goal for the creators Grøstl was *transparency*—a goal based on principles that differ from those shared by many other members in the SHA family [61].

## 3.2 Grøstl and Related "AES-Like" Constructions

Here we briefly introduce Grøstl and how such CHFs are frequently connected to *symmetric-key algorithms*, which is another fundamental area of cryptography.

In a symmetric-key crypto-system the communicating parties share the same cryptographic secret keys for both the encryption of plaintext and the decryption of ciphertext. Symmetric-key encryption can use either stream ciphers or block ciphers [131]:

- Stream ciphers encrypt the bytes of a message one at a time.
- Block ciphers break the message into $l$-bit blocks and encrypt each block as a single unit, where the plaintext is padded so that it is a multiple of the block size.

Note: for a stronger discussion of symmetric-key cryptography we recommend [131] and the references therein.

Although the application domain of symmetric-key encryption systems is generally different than that of CHF systems, it turns out that there is a great overlap between them: not only are they used together to build security protocols (ex. key agreement, symmetric encryption, and message authentication), but in fact CHFs are frequently based on symmetric ciphers, so many of the algorithms and underlying algebraic structures are similar. In fact there are numerous methods for which a symmetric cipher can be used to construct a CHF [61, 132, 133, 134, 135, 136]. A prime example of this is Grøstl [61], which is based on the block cipher of the Rijndael Advanced Encryption Standard (AES) [137].

Grøstl, AES, and many other block cipher algorithms are members of a "family" in which they are related via the notion of a substitution-permutation network [138]. In short, a substitution-permutation network takes a block of the message (plaintext) and the key as inputs, and applies several alternating "rounds" or "layers" of substitution operations and permutation operations to output the ciphertext (or hash) block. In this case, a CHF such as Grøstl [61] (which does not accept a key as input) is often referred to as being "AES-like" because its algorithm and the underlying algebraic structures are roughly similar to AES [137]. Like numerous CHFs in this family, Grøstl "borrows" some essential components from AES such as the S-box and the method for which the diffusion layers are constructed [61]. Moreover, since the *wide-pipe* construction of Grøstl gives it an internal state size that is much larger than the output size, the resistance against all known, generic attacks is strengthened [61]. In general, many features of Grøstl are well-understood in terms of similar work regarding AES. Therefore, the mathematical and computational strategies for assessing the security of Grøstl are roughly similar to the strategies that are used to assess numerous CHFs and other AES-like crypto-systems.

Both Grøstl and AES-like algorithms utilize a Galois field $\mathbb{F}_{p^d} \cong \mathbb{F}_{p^d}[x] = \mathbb{Z}_p[x]/\langle P(x)\rangle$ (with additive permutations), which is built from a commutative polynomial ring (with an identity) comprising a finite number of polynomial elements, where the operations are modular addition and multiplication with respect to an irreducible polynomial $P(x) \in \mathbb{Z}_p[x]$ of degree $d = 8$ whose modulo coefficients are in $\mathbb{Z}_p$ with $p = 2$. In the case of AES, each polynomial $b(x) \in \mathbb{F}_{2^8}[x] = \mathbb{Z}_2[x]/\langle P_{AES}(x)\rangle$ encodes a byte which is a binary string of 8 coefficients that is written as

$$b(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0 \in \mathbb{F}_{2^8}[x]$$

with $b_i \in \mathbb{Z}_2 = \{0, 1\}$ for $i = 0, 1, 2, \ldots, 7$, while the degree $d = 8$ irreducible polynomial $P_{AES}(x) \in \mathbb{Z}_2[x]$ is written as

$$P_{AES}(x) = x^8 + x^4 + x^3 + x + 1 = 1\ 0001\ 1011 \in \mathbb{Z}_2[x],$$

where the binary number 1 0001 1011 (11b in hexadecimal) encodes $P_{AES}(x)$. One can obtain a more comprehensive explanation regarding the structure of AES (as used by Grøstl [61]) in [139, 140, 141, 142].

Grøstl is an example of a block-based CHF that is *iterated.* This means that in order to compute the hash $\mathcal{F}(\mathcal{M}) = \mathcal{H} \in \mathfrak{H}$ of a given message $\mathcal{M} \in \mathfrak{M}$ of arbitrary length, a certain sequence of computations, which comprise a *round*, is repeatedly executed a specific number of times. Since Grøstl is block-based, it first pads and partitions $\mathcal{M}$ into a sequence of $l$-bit blocks

$$\mathcal{M} : m_1, \ldots, m_k, \ldots, m_\nu \quad \text{with} \quad m_k \in \mathbb{F}_{2^l} \quad \text{for} \quad k = 1, 2, \ldots, \nu.$$

Grøstl can process $l$-bit block sizes of 512 or 1024 [61]. Thus, for $p = 2$ and $d = 8$ with a given common block size of $l = 512$, each element

$$m_k \in \mathbb{F}_{2^l} = \mathbb{F}_{2^{d \cdot 8 \cdot 8}} = \mathbb{F}_{2^{8 \cdot 8 \cdot 8}} = \mathbb{F}_{2^{512}}, \quad \text{for} \quad k = 1, 2, \ldots, \nu,$$

of $\mathcal{M}$ is a 512-bit (64-byte) *message block* given by the length-64 sequence of bytes

$$m_k : m_k[0], m_k[1], \ldots, m_k[\eta], \ldots, m_k[63] \quad \text{with} \quad m_k[\eta] \in \mathbb{F}_{2^8} \quad \text{for} \quad \eta = 0, 1, \ldots, 63,$$

such that each $m_k \in \mathbb{F}_{2^l}$ is defined as a corresponding *initial state* matrix $\mathcal{S}_k^0 \in M_{8,8}(\mathbb{F}_{2^8})$ via the mapping

$$\xi : \mathbb{F}_{2^{512}} \to M_{8,8}(\mathbb{F}_{2^8}),$$

where $\xi(m_k) = \mathcal{S}_k^0$ is given by $S_{k:i,j} = m_k[8i + j]$ for $0 \leq i < 8$ and $0 \leq j < 8$, such that $M_{8,8}(\mathbb{F}_{2^8})$ denotes the set of all $8 \times 8$ matrices over $\mathbb{F}_{2^8}$. Therefore, Grøstl then maps each 512-bit block $m_k$ to the $8 \times 8$ initial state matrix

$$\xi(m_k) = \mathcal{S}_k^0 = \begin{bmatrix} m_k[0] & m_k[8] & m_k[16] & m_k[24] & m_k[32] & m_k[40] & m_k[48] & m_k[56] \\ m_k[1] & m_k[9] & m_k[17] & m_k[25] & m_k[33] & m_k[41] & m_k[49] & m_k[57] \\ m_k[2] & m_k[10] & m_k[18] & m_k[26] & m_k[34] & m_k[42] & m_k[50] & m_k[58] \\ m_k[3] & m_k[11] & m_k[19] & m_k[27] & m_k[35] & m_k[43] & m_k[51] & m_k[59] \\ m_k[4] & m_k[12] & m_k[20] & m_k[28] & m_k[36] & m_k[44] & m_k[52] & m_k[60] \\ m_k[5] & m_k[13] & m_k[21] & m_k[29] & m_k[37] & m_k[45] & m_k[53] & m_k[61] \\ m_k[6] & m_k[14] & m_k[22] & m_k[30] & m_k[38] & m_k[46] & m_k[54] & m_k[62] \\ m_k[7] & m_k[15] & m_k[23] & m_k[31] & m_k[39] & m_k[47] & m_k[55] & m_k[63] \end{bmatrix} \in M_{8,8}(\mathbb{F}_{2^8})$$

of $m_k$, where each byte $m_k[\eta] \in \mathbb{F}_{2^8}$ for $\eta = 0, 1, 2, \ldots, 63$ is an encoded polynomial with coefficients from $\mathbb{Z}_2$.

The (512-bit) *compression function* $f_{Grøstl}$ is based on two underlying 512-bit permutations $P_{Grøstl}$ and $Q_{Grøstl}$ (each is a round-dependent composition of four distinct transformations), which is defined as [61]

$$f_{Grøstl}(h, \xi(m)) = P_{Grøstl}(h \oplus_2 \xi(m)) \oplus_2 Q_{Grøstl}(\xi(m)) \oplus_2 h, \tag{3.1}$$

where $\oplus_2$ is the bitwise addition in $\mathbb{Z}_2$ and $m$ is a 512-bit message block. During the hashing process, Grøstl iteratively applies $f_{Grøstl}$ to each block $m_k$ of $\mathcal{M}$ during the execution of each round, where each $m_k$ undergoes a length-$q$ sequence of transitions denoted by

$$m_k \to \mathcal{S}_k^0 \to \mathcal{S}_k^1 \to \mathcal{S}_k^2 \to \cdots \to \mathcal{S}_k^t \to \mathcal{S}_k^{t+1} \to \cdots \to \mathcal{S}_k^q,$$

where we let $q$ denote the number of transitions which depends on the number of rounds and the $l$-bit block size, etc., and we let $t$ denote the $t$th state. For this, the underlying transformations of $f_{Grøstl}$ are sequentially applied to each entry $m_k[\eta] \in \mathbb{F}_{2^8}$ and are encoded as operations in $\mathbb{F}_{2^8}[x]$ as Grøstl iteratively applies $f_{Grøstl}$ as follows: an initial $l$-bit value $h_0 = iv$ is defined and then each $m_k$ is processed as

$$h_k \leftarrow f_{Grøstl}(h_{k-1}, \xi(m_k)) \quad \text{for} \quad k = 1, 2, \ldots, \nu,$$

where $f_{Grøstl}$ maps each pair of 512-bit inputs to a single 512-bit output, such that the first 512-bit input $h_{k-1}$ of $f_{Grøstl}$ is called the *chaining input.* After the final message block $m_\nu$ has been processed, the final hashed output $\mathcal{H}$ of Grøstl is computed as

$$\mathcal{H} \leftarrow \mathcal{F}_{Grøstl}(\mathcal{M}) = \Omega_{Grøstl}(h_\nu),$$

where $\Omega_{Grøstl}$ is the final output transformation (which truncates the final state and maps it to the final hash string format).

## 3.3 Simplified Grøstl: Specification and Construction

The algebraic structure of the original Grøstl CHF [61] over the Galois field $\mathbb{F}_{2^8} \cong \mathbb{F}_{2^8}[x]$ is complex (by design) and thus one faces an immense challenge if one aims to evaluate Grøstl over such a gigantic order. Therefore, we design and implement a new, generalized version of the Grøstl CHF over $\mathbb{F}_{p^d} \cong \mathbb{F}_{p^d}[x]$, where we fix $p = 3$ and $d = 2$ to create a "Simplified Grøstl" CHF over a smaller Galois field $\mathbb{F}_{3^2} \cong \mathbb{F}_{3^2}[x]$: namely *S-Grøstl*. Thus, our objective is to study and evaluate the S-Grøstl CHF over $\mathbb{F}_{3^2}$ in order to learn more about the original Grøstl CHF over $\mathbb{F}_{2^8}$ [61].

### 3.3.1 Algebraic Structure

Our S-Grøstl CHF is similar to the original Grøstl CHF [61]: the only major difference is that S-Grøstl operates over $\mathbb{F}_{3^2}$ while Grøstl operates over $\mathbb{F}_{2^8}$. We select $\mathbb{F}_{3^2}$ for the construction of S-Grøstl based on the following transversal results of Chapter 2:

- The order-$3^2$ super-symmetric latin square $L^{(\mathbb{F}_{3^2},+)} \in \mathcal{L}^9$ that encodes $(\mathbb{F}_{3^2}, +)$ possesses the confirmed maximum number of transversals $\mathbb{T}(9) = 2{,}241$, which is the largest confirmed $\mathbb{T}(n)$ reported by [5, 6, 8];
- The number of "good" additive permutations over $(\mathbb{F}_{3^2}, +)$ is equal to the number of transversals $\mathbb{T}(9) = 2{,}241$ of $L^{(\mathbb{F}_{3^2},+)}$.
- The six conditions of Theorem 2.90 are equivalent since $(\mathbb{F}_{3^2}, +)$ is a solvable group, where we note that:
  (i) $L^{(\mathbb{F}_{3^2},+)}$ has a transversal.
  (ii) The Sylow 2-subgroups of $(\mathbb{F}_{3^2}, +)$ are trivial or non-cyclic.

(iii) There exists some ordering of the elements of $(\mathbb{F}_{3^2}, +)$ which yields the trivial product 0.

(iv) $L^{(\mathbb{F}_{3^2},+)}$ can be decomposed into disjoint transversals.

(v) There exists a latin square $L^{(\mathbb{F}_{3^2},+)'}$ that is orthogonal to $L^{(\mathbb{F}_{3^2},+)}$.

(vi) $(\mathbb{F}_{3^2}, +)$ is admissible.

In order to construct a polynomial Galois field over $\mathbb{F}_{3^2}$ for usage in S-Grøstl, we first select an irreducible polynomial $P(x) \in \mathbb{Z}_3[x]$ of degree 2 with coefficients $p_0, p_1, p_2 \in \mathbb{Z}_3$. Thus, we choose

$$P(x) = x^2 + 1 = 1 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0 = 101 \in \mathbb{Z}_3[x],$$

where $p_2 = 1, p_1 = 0, p_0 = 1 \in \mathbb{Z}_3$, such that $P(x)$ is irreducible in $\mathbb{Z}_3[x]$. Therefore, we obtain the Galois field $\mathbb{F}_{3^2}[x] = \mathbb{Z}_3[x]/\langle P(x) \rangle$ where the 9 distinct polynomial elements of $\mathbb{F}_{3^2}[x]$ are encoded as *ternary strings* written as

$$\begin{array}{rcrcl rcrcl}
a_0(x) & = & 0 & = & 00 \in \mathbb{F}_{3^2}[x] & a_5(x) & = & x+2 & = & 12 \in \mathbb{F}_{3^2}[x] \\
a_1(x) & = & 1 & = & 01 \in \mathbb{F}_{3^2}[x] & a_6(x) & = & 2x+0 & = & 20 \in \mathbb{F}_{3^2}[x] \\
a_2(x) & = & 2 & = & 02 \in \mathbb{F}_{3^2}[x] & a_7(x) & = & 2x+1 & = & 21 \in \mathbb{F}_{3^2}[x] \\
a_3(x) & = & x+0 & = & 10 \in \mathbb{F}_{3^2}[x] & a_8(x) & = & 2x+2 & = & 22. \in \mathbb{F}_{3^2}[x] \\
a_4(x) & = & x+1 & = & 11 \in \mathbb{F}_{3^2}[x] & & & & &
\end{array} . \qquad (3.2)$$

The super-symmetric Cayley table that encodes the addition group $(\mathbb{F}_{3^2}[x], +)$ of $\mathbb{F}_{3^2}[x]$ with respect to $P(x) = x^2 + 1 \in \mathbb{Z}_3[x]$ is displayed in Table 3.2.

Since S-Grøstl encodes data with polynomials and operates in $\mathbb{F}_{3^2}[x]$, then any polynomial $a(x) \in \mathbb{F}_{3^2}[x]$ will have coefficients in $\mathbb{Z}_3 = \{0, 1, 2\}$. Therefore, since our polynomial coefficients are not restricted to $\mathbb{Z}_2 = \{0, 1\}$ due to the changed characteristic, the "bit" and "binary" terminology is no longer applicable. Thus, for the sake of clarity, we'll refer to any such polynomial coefficient in $\mathbb{Z}_3$ as a *trit* and use *ternary* numbering for the rest of this thesis. Therefore, when we say that an operation as *tritwise*, we're indicating that the operation is performed on each

**Table 3.2: S-Grøstl operates over the Galois field $\mathbb{F}_{3^2} \cong \mathbb{F}_{3^2}[x] = \mathbb{Z}_3[x]/\langle P(x)\rangle$ with respect to the irreducible polynomial $P(x) = x^2+1 = 101 \in \mathbb{Z}_3[x]$ with coefficients in $\mathbb{Z}_3 = \{0,1,2\}$. This is the super-symmetric latin square $L^{(\mathbb{F}_{3^2}[x],+)}$ (generated by the SS-LS-GA) that encodes the addition group $(\mathbb{F}_{3^2}[x],+)$, which has the confirmed maximum number of transversals $\mathbb{T}(9)$ = 2,241.**

| $+$ | $\mathbf{0}$ | $\mathbf{1}$ | $\mathbf{2}$ | $\boldsymbol{x}$ | $\boldsymbol{x+1}$ | $\boldsymbol{x+2}$ | $\boldsymbol{2x}$ | $\boldsymbol{2x}+1$ | $\boldsymbol{2x+2}$ |
|---|---|---|---|---|---|---|---|---|---|
| $\mathbf{0}$ | $0$ | $1$ | $2$ | $x$ | $x+1$ | $x+2$ | $2x$ | $2x+1$ | $2x+2$ |
| $\mathbf{1}$ | $1$ | $2$ | $0$ | $x+1$ | $x+2$ | $x$ | $2x+1$ | $2x+2$ | $2x$ |
| $\mathbf{2}$ | $2$ | $0$ | $1$ | $x+2$ | $x$ | $x+1$ | $2x+2$ | $2x$ | $2x+1$ |
| $\boldsymbol{x}$ | $x$ | $x+1$ | $x+2$ | $2x$ | $2x+1$ | $2x+2$ | $0$ | $1$ | $2$ |
| $\boldsymbol{x+1}$ | $x+1$ | $x+2$ | $x$ | $2x+1$ | $2x+2$ | $2x$ | $1$ | $2$ | $0$ |
| $\boldsymbol{x+2}$ | $x+2$ | $x$ | $x+1$ | $2x+2$ | $2x$ | $2x+1$ | $2$ | $0$ | $1$ |
| $\boldsymbol{2x}$ | $2x$ | $2x+1$ | $2x+2$ | $0$ | $1$ | $2$ | $x$ | $x+1$ | $x+2$ |
| $\boldsymbol{2x}+1$ | $2x+1$ | $2x+2$ | $2x$ | $1$ | $2$ | $0$ | $x+1$ | $x+2$ | $x$ |
| $\boldsymbol{2x+2}$ | $2x+2$ | $2x$ | $2x+1$ | $2$ | $0$ | $1$ | $x+2$ | $x$ | $x+1$ |

individual trit in a ternary string modulo 3. For example, given a 2-trit string 12 and executing a *tritwise multiplication* by 2, the result would be 21 because $4 \equiv 1 \pmod 3$ and $2 \equiv 2 \pmod 3$; the same process applies for *tritwise addition.* For this, we denote tritwise addition and multiplication by the operators $\oplus_3$ and $\otimes_3$, respectively.

For S-Grøstl we have $p = 3$ and $d = 2$, and we fix the length of our message $\mathcal{M} \in \mathfrak{M}$ to be 32-trits and set the $l$-trit block size to be $l = 32$. So each element

$$m_k \in \mathbb{F}_{3^l} = \mathbb{F}_{3^{d\cdot 4\cdot 4}} = \mathbb{F}_{3^{2\cdot 4\cdot 4}} = \mathbb{F}_{3^{32}}, \quad \text{for} \quad k = 1,2,\ldots,\nu,$$

of $\mathcal{M}$ is a 32-trit block given by the length-16 sequence of length-2 ternary strings

$$m_k : m_k[0], m_k[1], \ldots, m_k[\eta], \ldots, m_k[15] \quad \text{with} \quad m_k[\eta] \in \mathbb{F}_{3^2} \quad \text{for} \quad \eta = 0,1,\ldots,15,$$

such that each $m_k \in \mathbb{F}_{3^l}$ is defined as a corresponding matrix $\mathcal{S}_k^0 \in M_{4,4}(\mathbb{F}_{3^2})$ via the mapping

$$\xi : \mathbb{F}_{3^{32}} \to M_{4,4}(\mathbb{F}_{3^2}),$$

where $\xi(m_k) = \mathcal{S}_k^0$ is given by $\mathcal{S}_{k:i,j}^0 = m_k[4i+j]$ for $0 \leq i < 4$ and $0 \leq j < 4$, such that $M_{4,4}(\mathbb{F}_{3^2})$ denotes the set of all $4 \times 4$ matrices over $\mathbb{F}_{3^2}$. Therefore, S-Grøstl then maps each 32-trit block $m_k$ to its $4 \times 4$ initial state matrix

$$\xi(m_k) = \mathcal{S}_k^0 = \begin{bmatrix} m_k[0] & m_k[4] & m_k[8] & m_k[12] \\ m_k[1] & m_k[5] & m_k[9] & m_k[13] \\ m_k[2] & m_k[6] & m_k[10] & m_k[14] \\ m_k[3] & m_k[7] & m_k[11] & m_k[15] \end{bmatrix} = \begin{bmatrix} \mathcal{S}^0_{k:0,0} & \mathcal{S}^0_{k:0,1} & \mathcal{S}^0_{k:0,2} & \mathcal{S}^0_{k:0,3} \\ \mathcal{S}^0_{k:1,0} & \mathcal{S}^0_{k:1,1} & \mathcal{S}^0_{k:1,2} & \mathcal{S}^0_{k:1,3} \\ \mathcal{S}^0_{k:2,0} & \mathcal{S}^0_{k:2,1} & \mathcal{S}^0_{k:2,2} & \mathcal{S}^0_{k:2,3} \\ \mathcal{S}^0_{k:3,0} & \mathcal{S}^0_{k:3,1} & \mathcal{S}^0_{k:3,2} & \mathcal{S}^0_{k:3,3}, \end{bmatrix} \in M_{4,4}(\mathbb{F}_{3^2}),$$

where each $m_k[\eta] \in \mathbb{F}_{3^2}$ for $\eta = 0, 1, \ldots, 15$ is an encoded polynomial with coefficients from $\mathbb{Z}_3$, such that (in the rightmost matrix representation) each $\mathcal{S}_{k:i,j}$ is the entry in the $i$th row and $j$th column of the matrix of message block $m_k$.

Therefore, since S-Grøstl operates over $\mathbb{F}_{3^2}$, the compression function $f_{S-Grøstl}$ is similarly based on two underlying 32-trit permutations $P_{S-Grøstl}$ and $Q_{S-Grøstl}$ such that

$$f_{S-Grøstl}(h, \xi(m)) = P_{S-Grøstl}(h \oplus_3 \xi(m)) \oplus_3 Q_{S-Grøstl}(\xi(m)) \oplus_3 h, \tag{3.3}$$

recalling that $\oplus_3$ is the bitwise addition in $\mathbb{Z}_3$, where $m$ is an arbitrary 32-bit message block. For the purpose of this thesis, we need only to consider a single 32-trit $m_1 = \mathcal{M}$. Therefore, S-Grøstl initializes the single 32-trit value $h_0 = iv$ and processes the single $m_1$ by applying the compression function $f_{S-Grøstl}$ as

$$h_1 \leftarrow f_{S-Grøstl}(h_0, \xi(m_1))$$

since $k = 1$ for a single iteration, where $f_{S-Grøstl}$ maps the two 32-trit inputs to a single 32-trit output.

Thus, after the last (and single) $m_1 = \mathcal{M} \in \mathfrak{M}$ has been processed, the final hashed output $\mathcal{H} \in \mathfrak{H}$ of S-Grøstl is computed as

$$\mathcal{H} \leftarrow \mathcal{F}_{S-Grøstl}(\mathcal{M}) = \Omega_{S-Grøstl}(h_1),$$

where we omit the S-Grøstl truncation of $\Omega_{S-Grøstl}$ because it isn't necessary for the purposes of this thesis.

From this point forward, for the sake of simple description, we let $\mathcal{S}_k^t = \mathcal{S}^t \in M_{4,4}(\mathbb{F}_{3^2})$ denote the $t$th state of $m_k = m_1 = \mathcal{M}$ (we drop the "$k$" subscript since we need only to consider one message block), where the initial state is $\xi(m_k) = \xi(m_1) = \xi(\mathcal{M}) = \mathcal{S}_k^0 = \mathcal{S}^0$.

### 3.3.2 Compression Function and Round Transformations

In the original Grøstl [61] over $\mathbb{F}_{2^8}$, the (512-bit) compression function $f_{Grøstl}$ of (3.1) is based on 512-bit permutations $P_{Grøstl}$ and $Q_{Grøstl}$, where the design of $P_{Grøstl}$ and $Q_{Grøstl}$ was motivated by the Rijndael AES block cipher algorithm [139, 140, 141, 142]. This implies that the AES-like design of $P_{Grøstl}$ and $Q_{Grøstl}$ comprises a certain number of *rounds* $R$, where each round comprises a certain number of *round transformations*. Hence, in the specific case of Grøstl, both $P_{Grøstl}$ and $Q_{Grøstl}$ are composed of the following four round transformations:

1. *AddRoundConstant*,
2. *SubBytes*,
3. *ShiftBytes* (or "ShiftRows"), and
4. *MixBytes* (or "MixColumns").

Each of these round transformations operates on the 8 × 8 (matrix) state for 512-bit blocks.

Our S-Grøstl has exactly four similar such round transformations for both $P_{S-Grøstl}$ and $Q_{S-Grøstl}$:

1. *AddRoundConstant* ($\sigma$),
2. *SubTrits* ($\lambda$),
3. *ShiftRows* ($\pi$), and

4. *MixColumns* ($\rho$).

Hence, a round permutation $P_{S-Grøstl}$ (or $Q_{S-Grøstl}$) is composed of the said round transformations in the following order:

$$P_{S-Grøstl} = \rho \circ \pi \circ \lambda \circ \sigma.$$

Each of these round transformations operates on the $4 \times 4$ (matrix) state for 32-trit blocks.

### AddRoundConstant ($\sigma$)

The original Grøstl [61] uses *bitwise* addition to add a round-dependent constant matrix to the input state matrix. The purpose of adding round constants is to make each round distinct and also to ensure that $P_{Grøstl}$ and $Q_{Grøstl}$ are independent from one another [61]; this is the general design criteria for the AddRoundConstant transformation.

In S-Grøstl we have a similar such transformation:

**Definition 3.1.** Let $\sigma[A^r] : M_{4,4}(\mathbb{F}_{3^2}) \to M_{4,4}(\mathbb{F}_{3^2})$ denote the mapping defined by $\sigma[A^r](S^t) = \mathcal{S}^{t+1}$ if and only if $\mathcal{S}_{ij}^{t+1} = \mathcal{S}_{ij}^{t} \oplus A^r \in M_{4,4}(\mathbb{F}_{3^2})$ for all $0 \leq i, j < 4$. We say that $\sigma[A^r]$ is the *AddRoundConstant transformation of round-r*.

For round $r$ of S-Grøstl, the AddRoundConstant transformation $\sigma$ uses *tritwise* addition to add a round-dependent constant matrix $A^r \in M_{4,4}(\mathbb{F}_{3^2})$ to the input state matrix $\mathcal{S}^t \in M_{4,4}(\mathbb{F}_{3^2})$ to output the resulting state matrix $\mathcal{S}^{t+1} \in M_{4,4}(\mathbb{F}_{3^2})$.

So $\sigma$ updates the state of $\mathcal{S}^t$ via

$$\mathcal{S}^{t+1} \leftarrow \mathcal{S}^t \oplus A^r,$$

where the round constant $A^r$ depends on the round $r$, such that $0 \leq r < R$ and $R$ is the total number of rounds. $P_{S-Grøstl}$ and $Q_{S-Grøstl}$ have distinct round constants, which are

$$P_{S-Grøstl}: \; A^r = \begin{bmatrix} 00 \oplus r & 01 \oplus r & 02 \oplus r & 10 \oplus r \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{bmatrix} \in M_{4,4}(\mathbb{F}_{3^2})$$

and

$$Q_{S-Grøstl}: \; A^r = \begin{bmatrix} 22 & 22 & 22 & 22 \\ 22 & 22 & 22 & 22 \\ 22 & 22 & 22 & 22 \\ 22 \oplus r & 21 \oplus r & 20 \oplus r & 12 \oplus r \end{bmatrix} \in M_{4,4}(\mathbb{F}_{3^2}),$$

respectively, where $r \in \mathbb{F}_{3^2}$ is the round number that corresponds to an enumeration of 2-trit element of $\mathbb{F}_{3^2}[x]$ as listed in (3.2). For example, $r = 2$ corresponds to $a_2(x) \in \mathbb{F}_{3^2}[x]$ of (3.2), and $r = 7$ corresponds $a_7(x) \in \mathbb{F}_{3^2}[x]$ of (3.2), etc.

The $\sigma$ transformation of S-Grøstl is similar to that of the original Grøstl [61] with one minor exception: on the first row of $A^r$ for $P_{S-Grøstl}$ and on the last row of $A^r$ for $Q_{S-Grøstl}$ S-Grøstl increments (decrements) starting at the *least significant trit*, whereas on the first row of $A^r$ for $P_{Grøstl}$ and on the last row of $A^r$ for $Q_{Grøstl}$ Grøstl increments (decrements) the *most significant nibble.*

### SubTrits ($\lambda$)

In Grøstl [61] the SubBytes transformation is an *element-wise* operation that substitutes each byte in the state matrix by another value from the S-box. The Grøstl S-box is identical to the one used in Rijandael AES [139, 140, 141, 142]. SubBytes is the only non-linear transformation in Grøstl, where its values are generated from the multiplicative inverse of a Galois field with an affine transform. It has been well-studied and is specifically designed to be resistant to linear and differential cryptanalysis attacks.

In S-Grøstl we have a similar such transformation:

**Definition 3.2.** Let $\lambda : M_{4,4}(\mathbb{F}_{3^2}) \to M_{4,4}(\mathbb{F}_{3^2})$ denote the mapping given as a parallel application of $4^2$ bijective S-box-mappings $\lambda_{i,j} : \mathbb{F}_{3^2} \to \mathbb{F}_{3^2}$ and defined by $\lambda(\mathcal{S}^t) = \mathcal{S}^{t+1}$ if and only if $\mathcal{S}^{t+1}_{i,j} = \lambda_{i,j}(\mathcal{S}^t_{i,j})$ for all $0 \leq i, j < 4$. We say that $\lambda$ is the *SubTrits transformation*.

The SubTrits transformation $\lambda$ is an element-wise operation that does a substitution that is similar to that of Grøstl (and AES): the multiplicative inverse of each 2-trit element $\mathcal{S}^t_{i,j} \in \mathbb{F}_{3^2}[x]$ in an entry of the state matrix $\mathcal{S}^t \in M_{4,4}(\mathbb{F}_{3^2})$ is computed and then multiplied by a fixed element $B$, and then the result is added to a second fixed element $C$.

Now since each $\mathcal{S}^t_{i,j} \in \mathbb{F}_{3^2}[x]$ is in fact a polynomial with coefficients that can be written as a column-vector, then $B$ must be an invertible square matrix $B$ and $C$ must a column-vector $C$, where both must have dimensions that correspond to the size of the possible size of the ciphertext of $\mathcal{S}^t$. Consequently, in this case of $d = 2$, $B \in M_{2,2}(\mathbb{Z}_3)$ is required to be an invertible $2 \times 2$ matrix with elements modulo 3, while $C \in M_{2,1}(\mathbb{Z}_3)$ is required to be a length-2 column-vector with elements modulo 3.

For convenience, we define $\lambda$ on all of $\mathbb{F}_{3^2}[x]$ so that it maps 0 to $C$ and any nonzero $x = S^t_{i,j}$ to

$$\mathcal{S}^{t+1}_{i,j} = B \cdot x^{-1} + C. \tag{3.4}$$

Thus, for our implementation, we select *two* fixed elements $b_0(x), b_1(x) \in \mathbb{F}_{3^2}[x]$ to fix the invertible $2 \times 2$ matrix

$$B = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{bmatrix}, \;\; b_{i,j} \in \mathbb{Z}_3, \;\; b_0(x) = b_{0,0}x + b_{0,1}, b_1(x) = b_{1,0}x + b_{1,1} \in \mathbb{F}_{3^2}[x],$$

and select the fixed (zero) column-vector

$$C = \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}, \;\; c_i \in \mathbb{Z}_3, \;\; c(x) = c_0 x + c_1 \in \mathbb{F}_{3^2}[x]$$

for (3.4).

**ShiftRows ($\pi$)**

In Grøstl [61] the design criteria for the ShiftBytes transformation requires that $P_{Grøstl}$ and $Q_{Grøstl}$ are independent and achieve optimal diffusion. In short, diffusion means that if one changes a single bit of the input message (i.e. plaintext), then (statistically) half of the bits in the output hash (i.e. ciphertext) should change (and conversely) [143]; in other words, diffusion refers to "scattering" the statistical structure of the input over "the bulk" of the output.

In S-Grøstl we have a similar such transformation:

**Definition 3.3.** Let $\pi : M_{4,4}(\mathbb{F}_{3^2}) \to M_{4,4}(\mathbb{F}_{3^2})$ denote the mapping for which there is a mapping $\varsigma : \{0, 1, ..., 3\} \to \{0, 1, ..., 3\}$ such that $\pi(\mathcal{S}^t) = \mathcal{S}^{t+1}$ if and only if $\mathcal{S}^{t+1}_{i,j} = \mathcal{S}^t_{i,j-\varsigma(i) \bmod 4}$ for all $0 \leq i, j < 4$. We say that $\pi$ is the *ShiftRows transformation.*

In S-Grøstl the ShiftRows transformation $\pi$ remains unchanged from the original Grøstl [61] except for the size of the state matrix $\mathcal{S}^t$ for which it acts on. For each row, $\pi$ cyclically shifts each element within a row to the left by a certain number of positions.

Thus, let $\varsigma = [\varsigma(0), \varsigma(1), \varsigma(2), \varsigma(3)]$ be a list of integers in the range from 0 to 3. Then $\pi$ cyclically shifts all elements in row $i$ of the state matrix $\mathcal{S}^t$ by $\varsigma(i)$ positions to the left (wrapping around as necessary). For $P_{S-Grøstl}$ and $Q_{S-Grøstl}$ the operation is identical and only the order of the values of $\varsigma$ change:

$$\begin{aligned} P_{S-Grøstl} : \ \varsigma &= [0,1,2,3] \\ Q_{S-Grøstl} : \ \varsigma &= [1,3,0,2]. \end{aligned}$$

Therefore, $\pi$ may be illustrated as follows:

$$P_{S-Grøstl} : \quad \mathcal{S}^t = \begin{bmatrix} \mathcal{S}^t_{0,0} & \mathcal{S}^t_{0,1} & \mathcal{S}_{0,2} & \mathcal{S}^t_{0,3} \\ \mathcal{S}^t_{1,0} & \mathcal{S}^t_{1,1} & \mathcal{S}^t_{1,2} & \mathcal{S}^t_{1,3} \\ \mathcal{S}^t_{2,0} & \mathcal{S}^t_{2,1} & \mathcal{S}^t_{2,2} & \mathcal{S}^t_{2,3} \\ \mathcal{S}^t_{3,0} & \mathcal{S}^t_{3,1} & \mathcal{S}^t_{3,2} & \mathcal{S}^t_{3,3} \end{bmatrix} \longrightarrow \begin{bmatrix} \mathcal{S}^t_{0,0} & \mathcal{S}^t_{0,1} & \mathcal{S}^t_{0,2} & \mathcal{S}^t_{0,3} \\ \mathcal{S}^t_{1,1} & \mathcal{S}^t_{1,2} & \mathcal{S}^t_{1,3} & \mathcal{S}^t_{1,0} \\ \mathcal{S}^t_{2,2} & \mathcal{S}^t_{2,3} & \mathcal{S}^t_{2,0} & \mathcal{S}^t_{2,1} \\ \mathcal{S}^t_{3,3} & \mathcal{S}^t_{3,0} & \mathcal{S}^t_{3,1} & \mathcal{S}^t_{3,2} \end{bmatrix} = \pi(\mathcal{S}^t) = \mathcal{S}^{t+1}$$

$$Q_{S-Grøstl} : \quad \mathcal{S}^t = \begin{bmatrix} \mathcal{S}^t_{0,0} & \mathcal{S}^t_{0,1} & \mathcal{S}^t_{0,2} & \mathcal{S}^t_{0,3} \\ \mathcal{S}^t_{1,0} & \mathcal{S}^t_{1,1} & \mathcal{S}^t_{1,2} & \mathcal{S}^t_{1,3} \\ \mathcal{S}^t_{2,0} & \mathcal{S}^t_{2,1} & \mathcal{S}^t_{2,2} & \mathcal{S}^t_{2,3} \\ \mathcal{S}^t_{3,0} & \mathcal{S}^t_{3,1} & \mathcal{S}^t_{3,2} & \mathcal{S}^t_{3,3} \end{bmatrix} \longrightarrow \begin{bmatrix} \mathcal{S}^t_{0,1} & \mathcal{S}^t_{0,2} & \mathcal{S}^t_{0,3} & \mathcal{S}^t_{0,0} \\ \mathcal{S}^t_{1,3} & \mathcal{S}^t_{1,0} & \mathcal{S}^t_{1,1} & \mathcal{S}^t_{1,2} \\ \mathcal{S}^t_{2,0} & \mathcal{S}^t_{2,1} & \mathcal{S}^t_{2,2} & \mathcal{S}^t_{2,3} \\ \mathcal{S}^t_{3,2} & \mathcal{S}^t_{3,3} & \mathcal{S}^t_{3,0} & \mathcal{S}^t_{3,1} \end{bmatrix} = \pi(\mathcal{S}^t) = \mathcal{S}^{t+1}.$$

### MixColumns ($\rho$)

In Grøstl [61] the main design criteria for the MixBytes transformation is that it must utilize the wide trail strategy. This strategy is a design approach that aims to combine efficiency and resistance against differential and linear cryptanalysis attacks [144].

**Definition 3.4.** We say that an $n \times n$ matrix $D \in M_{n,n}$ is a *circulant* matrix if $D$ is composed of cyclically shifted versions of an $n$-length list.

**Definition 3.5.** We say that an $m \times n$ matrix $D \in M_{m,n}$ over a Galois field $\mathbb{F}$ is a *maximum distance separable* (MDS) matrix if all possible square sub-matrices of $D$ obtained by discarding rows and colums are non-singular.

The following transformation of S-Grøstl is similar to that of the original Grøstl [61], where each column of the state matrix $\mathcal{S}^t$ is transformed independently.

**Definition 3.6.** Let $\rho : M_{4,4}(\mathbb{F}_{3^2}) \to M_{4,4}(\mathbb{F}_{3^2})$ denote the mapping given as the parallel application of 4 "column" mappings $\rho_j : M_{4,1}(\mathbb{F}_{3^2}) \to M_{4,1}(\mathbb{F}_{3^2})$ defined by $\rho(\mathcal{S}^t) = \mathcal{S}^{t+1}$ if and only if $\mathcal{S}_j^{t+1} = \rho_j(S_j^t)$ for all $0 \leq j < 4$, where each $\rho_j$ is given by $\rho_j(x) = D \cdot x$ for all $x \in M_{4,1}(\mathbb{F}_{3^2})$, such that $D \in M_{4,4}(\mathbb{F}_{3^2})$ is an invertible diffusion matrix.

In S-Grøstl the MixColumns transformation $\rho$ multiplies each column of $\mathcal{S}^t$ by a constant, invertible, circulant, MDS matrix $D$, such that $\mathcal{S}^t$ and $D$ have the same dimensions, and where both have elements from $\mathbb{F}_{3^2}[x]$. Thus, the application of $\rho$ on the entire $\mathcal{S}^t$ can be written as the matrix multiplication

$$\mathcal{S}^{t+1} \leftarrow D \times \mathcal{S}^t,$$

where each column of $\mathcal{S}^t$ is multiplied tritwise with $D$ to produce a single column of output. For S-Grøstl we select the constant, invertible, circulant, MDS $4 \times 4$ matrix

$$D = \begin{bmatrix} 00 & 01 & 01 & 10 \\ 10 & 00 & 01 & 01 \\ 01 & 10 & 00 & 01 \\ 01 & 01 & 10 & 00 \end{bmatrix} \in M_{4,4}(\mathbb{F}_{3^2}),$$

where each entry of $D$ stores an element of $\mathbb{F}_{3^2}[x]$.

## 3.4 Simplified Grøstl: Example Execution

Here we give a step-by-step demonstration of 1-round S-Grøstl over $\mathbb{F}_{3^2}$.

### 3.4.1 Setup

Suppose that we wish to use S-Grøstl to hash the message

$$\mathcal{M} = 01221020111002211210020102011201$$

which is a ternary string of 32-trits; here, we need only to consider a single 32-trit block $m_1 = \mathcal{M} \in \mathfrak{M}$. Therefore, $m_1$ is split into the 16 sub-strings

$$01, 22, 10, 20, 11, 10, 02, 21, 12, 10, 02, 01, 02, 01, 12, 01$$

where each length-2 sub-string stores 2 trits. Then the sub-strings of $m_1$ are arranged in the $4 \times 4$ matrix

$$\xi(m_1) = \begin{bmatrix} 01 & 11 & 12 & 02 \\ 22 & 10 & 10 & 01 \\ 10 & 02 & 02 & 12 \\ 20 & 21 & 01 & 01 \end{bmatrix} = \begin{bmatrix} 1 & x+1 & x+2 & 2 \\ 2x+2 & x & x & 1 \\ x & 2 & 2 & x+2 \\ 2x & 2x+1 & 1 & 1 \end{bmatrix} \in M_{4,4}(\mathbb{F}_{3^2}),$$

which is the initial input for $Q_{S-Gr\o stl}$ of $f_{S-Gr\o stl}$ in (3.3). Now since $\mathcal{M}$ is 32 trits in size, we do the decimal (base-10) to ternary (base-3) conversion

$$32_{10} = 1 \cdot 3^3 + 0 \cdot 3^2 + 1 \cdot 3^1 + 2 \cdot 3^0 = 1012_3$$

to construct the initial value

$$h_0 = \begin{bmatrix} 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 10 \\ 00 & 00 & 00 & 12 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x \\ 0 & 0 & 0 & x+2 \end{bmatrix}.$$

Therefore, the initial input for $P_{S-Gr\o stl}$ of $f_{S-Gr\o stl}$ in (3.3) is

$$h_0 \oplus_3 \xi(m_1) = \begin{bmatrix} 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 10 \\ 00 & 00 & 00 & 12 \end{bmatrix} \oplus_3 \begin{bmatrix} 01 & 11 & 12 & 02 \\ 22 & 10 & 10 & 01 \\ 10 & 02 & 02 & 12 \\ 20 & 21 & 01 & 01 \end{bmatrix} = \begin{bmatrix} 01 & 11 & 12 & 02 \\ 22 & 10 & 10 & 01 \\ 10 & 02 & 02 & 22 \\ 20 & 21 & 01 & 10 \end{bmatrix} \in M_{4,4}(\mathbb{F}_{3^2}).$$

Consequently, for this example demonstration of $f_{S-Gr\o stl}$ (3.3) we will execute

$$f_{S-Gr\o stl}(h_0, \xi(m_1)) = P_{S-Gr\o stl}(h_0 \oplus_3 \xi(m_1)) \oplus_3 Q_{S-Gr\o stl}(\xi(m_1)) \oplus_3 h_0$$

for 1-round S-Grøstl.

### 3.4.2 Permutation $P$

For the sake of description, we start with the input $\mathcal{S}^{0|P} = h_0 \oplus_3 \xi(m_1)$, which we refer to as *state 0* of the permutation $P_{S-Gr\o stl}$.

**AddRoundConstant** ($\sigma$)

First, we apply the round-dependent $\sigma$ transformation. Since this is round $r = 0$ for the permutation $P_{S-Gr\o stl}$, the round constant for $\sigma$ is

$$A^0 = \begin{bmatrix} 00 & 01 & 02 & 10 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 2 & x \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

So *state 1* of the permutation $P_{S-Gr\o stl}$ is

$$\begin{aligned} \mathcal{S}^{1|P} = \sigma(\mathcal{S}^{0|P}) &= \begin{bmatrix} 01 \oplus_3 00 & 11 \oplus_3 01 & 12 \oplus_3 02 & 02 \oplus_3 10 \\ 22 \oplus_3 00 & 10 \oplus_3 00 & 10 \oplus_3 00 & 01 \oplus_3 00 \\ 10 \oplus_3 00 & 02 \oplus_3 00 & 02 \oplus_3 00 & 22 \oplus_3 00 \\ 20 \oplus_3 00 & 21 \oplus_3 00 & 01 \oplus_3 00 & 10 \oplus_3 00 \end{bmatrix} = \begin{bmatrix} 01 & 12 & 11 & 12 \\ 22 & 10 & 10 & 01 \\ 10 & 02 & 02 & 22 \\ 20 & 21 & 01 & 10 \end{bmatrix} \\ &= \begin{bmatrix} 1 & x+2 & x+1 & x+2 \\ 2x+2 & x & x & 1 \\ x & 2 & 2 & 2x+2 \\ 2x & 2x+1 & 1 & x \end{bmatrix}. \end{aligned}$$

**SubTrits** ($\lambda$)

Second, we apply the $\lambda$ transformation, which is sequentially applied to each element of $\mathcal{S}^{1|P}$. Our first element $\mathcal{S}^{1|P}_{0,0} = 01$ is equivalent to the polynomial 1. So our first step for $\lambda$ is to find the multiplicative inverse of this polynomial in $\mathbb{F}_{3^2}[x]$ with respect to the irreducible polynomial $x^2+1$, which can be done with a modified Extended Euclidean algorithm, and results in $(\mathcal{S}^{1|P}_{0,0})^{-1} = 01$ for the polynomial 1 (which happens to be a trivial case). This polynomial 1 is then written in column-vector form, from top to bottom, and then multiplied by the matrix $B$ modulo 3; this yields the vector output

$$\lambda(01) = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \pmod 3 = \begin{bmatrix} 1 \\ 1 \end{bmatrix},$$

which is the vector encoding of the polynomial $x + 1$ whose coefficients are concatenated into the 2-trit string form 11. This gives us the new first element $\mathcal{S}^{2|P}_{0,0} = 11$ of $\mathcal{S}^{2|P}$.

The second element $\mathcal{S}^{1|P}_{0,1} = 12$ is equivalent to the polynomial $x+2$, which has the corresponding multiplicative inverse $(\mathcal{S}^{1|P}_{0,1})^{-1} = 11$ for the polynomial $x + 1$. Again, $x + 1$ is written in column-vector form, from top to bottom, and then multiplied by the matrix $B$ modulo 3; this yields the vector output

$$\lambda(11) = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \pmod 3 = \begin{bmatrix} 0 \\ 2 \end{bmatrix},$$

which is the vector encoding of the polynomial 2 whose coefficients are concatenated into the 2-trit string form 02, which gives us the new second element $\mathcal{S}^{2|P}_{0,1} = 02$ of $\mathcal{S}^{2|P}$.

Thus, $\lambda$ is repeatedly applied to all sixteen entries of $\mathcal{S}^{1|P}$ to obtain

$$\mathcal{S}^{2|P} = \begin{bmatrix} 11 & 02 & 10 & 02 \\ 20 & 12 & 12 & 11 \\ 12 & 22 & 22 & 20 \\ 21 & 01 & 11 & 12 \end{bmatrix} = \begin{bmatrix} x+1 & 2 & x & 2 \\ 2x & x+2 & x+2 & x+1 \\ x+2 & 2x+2 & 2x+2 & 2x \\ 2x+1 & 1 & x+1 & x+2 \end{bmatrix},$$

which is *state 2* of the permutation $P_{S-Grøstl}$.

### ShiftRows ($\pi$)

Third, we apply the $\pi$ transformation to each row of the state matrix $\mathcal{S}^{2|P}$. Since we're currently applying the permutation $P_{S-Gr\o stl}$, then the values $\varsigma$ for which $\pi$ will cyclically left shift all elements in rows 0, 1, 2, and 3 of $\mathcal{S}^{2|P}$ respectively correspond to

$$\varsigma = [\varsigma(0) = 0, \varsigma(1) = 1, \varsigma(2) = 2, \varsigma(3) = 3].$$

Therefore, by applying $\pi$ to cyclically left shift each $i$th row of $\mathcal{S}^{2|P}$ by $\varsigma(i)$ we obtain

$$\mathcal{S}^{2|P} = \begin{bmatrix} 11 & 02 & 10 & 02 \\ 20 & 12 & 12 & 11 \\ 12 & 22 & 22 & 20 \\ 21 & 01 & 11 & 12 \end{bmatrix} \longrightarrow \begin{bmatrix} 11 & 02 & 10 & 02 \\ 12 & 12 & 11 & 20 \\ 22 & 20 & 12 & 22 \\ 12 & 21 & 01 & 11 \end{bmatrix} = \begin{bmatrix} x+1 & 2 & x & 2 \\ x+2 & x+2 & x+1 & 2x \\ 2x+2 & 2x & x+2 & 2x+2 \\ x+2 & 2x+1 & 1 & x+1 \end{bmatrix}$$

$$= \pi(\mathcal{S}^{2|P}) = \mathcal{S}^{3|P},$$

which is *state 3* of the permutation $P_{S-Gr\o stl}$.

### MixColumns ($\rho$)

Fourth, we apply the $\rho$ transformation to each column of the state matrix $\mathcal{S}^{3|P}$, which is given by the matrix multiplication $\mathcal{S}^{4|P} \leftarrow D \times \mathcal{S}^{3|P}$, such that $\mathcal{S}^{4|P}$ is *state 4* of the permutation $P_{S-Gr\o stl}$.

To obtain the *first* column of $\mathcal{S}^{4|P}$ we compute

$$\rho\left(\begin{bmatrix} 11 \\ 12 \\ 22 \\ 12 \end{bmatrix}\right) = \begin{bmatrix} 00 & 01 & 01 & 10 \\ 10 & 00 & 01 & 01 \\ 01 & 10 & 00 & 01 \\ 01 & 01 & 10 & 00 \end{bmatrix} \cdot \begin{bmatrix} 11 \\ 12 \\ 22 \\ 12 \end{bmatrix} = \begin{bmatrix} 20 \\ 10 \\ 12 \\ 11 \end{bmatrix} = \begin{bmatrix} 2x \\ x \\ x+2 \\ x+1 \end{bmatrix}$$

which was obtained via

$$\left.\begin{array}{lcl}
\mathcal{S}_{0,0}^{4|P} : (00 \otimes_3 11) \oplus_3 (01 \otimes_3 12) \oplus_3 (01 \otimes_3 22) \oplus_3 (01 \otimes_3 12) & = & 00 \oplus_3 12 \oplus_3 22 \oplus_3 22 = 20 = 2x \\
\mathcal{S}_{1,0}^{4|P} : (10 \otimes_3 11) \oplus_3 (00 \otimes_3 12) \oplus_3 (01 \otimes_3 22) \oplus_3 (01 \otimes_3 12) & = & 12 \oplus_3 00 \oplus_3 22 \oplus_3 12 = 10 = x \\
\mathcal{S}_{2,0}^{4|P} : (01 \otimes_3 11) \oplus_3 (10 \otimes_3 12) \oplus_3 (00 \otimes_3 22) \oplus_3 (01 \otimes_3 12) & = & 11 \oplus_3 22 \oplus_3 00 \oplus_3 12 = 12 = x + 2 \\
\mathcal{S}_{3,0}^{4|P} : (01 \otimes_3 11) \oplus_3 (01 \otimes_3 12) \oplus_3 (10 \otimes_3 22) \oplus_3 (00 \otimes_3 12) & = & 11 \oplus_3 12 \oplus_3 21 \oplus_3 00 = 11 = x + 1
\end{array}\right. .$$

To obtain the *second* column of $\mathcal{S}^{4|P}$ we compute

$$\rho\left(\begin{bmatrix} 02 \\ 12 \\ 20 \\ 21 \end{bmatrix}\right) = \begin{bmatrix} 00 & 01 & 01 & 10 \\ 10 & 00 & 01 & 01 \\ 01 & 10 & 00 & 01 \\ 01 & 01 & 10 & 00 \end{bmatrix} \cdot \begin{bmatrix} 02 \\ 12 \\ 20 \\ 21 \end{bmatrix} = \begin{bmatrix} 10 \\ 01 \\ 12 \\ 12 \end{bmatrix} = \begin{bmatrix} x \\ 1 \\ x+2 \\ x+2 \end{bmatrix}$$

which was obtained via

$$\left.\begin{array}{lcl}
\mathcal{S}_{0,1}^{4|P} : (00 \otimes_3 02) \oplus_3 (01 \otimes_3 12) \oplus_3 (01 \otimes_3 20) \oplus_3 (10 \otimes_3 21) & = & 00 \oplus_3 12 \oplus_3 20 \oplus_3 11 = 10 = x \\
\mathcal{S}_{1,1}^{4|P} : (10 \otimes_3 02) \oplus_3 (00 \otimes_3 12) \oplus_3 (01 \otimes_3 20) \oplus_3 (01 \otimes_3 21) & = & 20 \oplus_3 00 \oplus_3 20 \oplus_3 21 = 01 = 1 \\
\mathcal{S}_{2,1}^{4|P} : (01 \otimes_3 02) \oplus_3 (10 \otimes_3 12) \oplus_3 (00 \otimes_3 20) \oplus_3 (01 \otimes_3 21) & = & 02 \oplus_3 22 \oplus_3 00 \oplus_3 21 = 12 = x + 2 \\
\mathcal{S}_{3,1}^{4|P} : (01 \otimes_3 02) \oplus_3 (01 \otimes_3 12) \oplus_3 (10 \otimes_3 20) \oplus_3 (00 \otimes_3 21) & = & 02 \oplus_3 12 \oplus_3 01 \oplus_3 00 = 12 = x + 2
\end{array}\right. .$$

To obtain the *third* column of $\mathcal{S}^{4|P}$ we compute

$$\rho\left(\begin{bmatrix} 10 \\ 11 \\ 12 \\ 01 \end{bmatrix}\right) = \begin{bmatrix} 00 & 01 & 01 & 10 \\ 10 & 00 & 01 & 01 \\ 01 & 10 & 00 & 01 \\ 01 & 01 & 10 & 00 \end{bmatrix} \cdot \begin{bmatrix} 10 \\ 11 \\ 12 \\ 01 \end{bmatrix} = \begin{bmatrix} 00 \\ 12 \\ 20 \\ 10 \end{bmatrix} = \begin{bmatrix} 0 \\ x+2 \\ 2x \\ x \end{bmatrix}$$

which was obtained via

$$\left.\begin{array}{lcl}
\mathcal{S}_{0,2}^{4|P} : (00 \otimes_3 10) \oplus_3 (01 \otimes_3 11) \oplus_3 (01 \otimes_3 12) \oplus_3 (10 \otimes_3 01) & = & 00 \oplus_3 11 \oplus_3 12 \oplus_3 10 = 00 = 0 \\
\mathcal{S}_{1,2}^{4|P} : (10 \otimes_3 10) \oplus_3 (00 \otimes_3 11) \oplus_3 (01 \otimes_3 12) \oplus_3 (01 \otimes_3 01) & = & 02 \oplus_3 00 \oplus_3 12 \oplus_3 01 = 12 = x + 2 \\
\mathcal{S}_{2,2}^{4|P} : (01 \otimes_3 10) \oplus_3 (10 \otimes_3 11) \oplus_3 (00 \otimes_3 12) \oplus_3 (01 \otimes_3 01) & = & 10 \oplus_3 12 \oplus_3 00 \oplus_3 01 = 20 = 2x \\
\mathcal{S}_{3,2}^{4|P} : (01 \otimes_3 10) \oplus_3 (01 \otimes_3 11) \oplus_3 (10 \otimes_3 12) \oplus_3 (00 \otimes_3 01) & = & 10 \oplus_3 11 \oplus_3 22 \oplus_3 00 = 10 = x
\end{array}\right. .$$

To obtain the *fourth* column of $\mathcal{S}^{4|P}$ we compute

$$\rho\left(\begin{bmatrix} 02 \\ 20 \\ 22 \\ 11 \end{bmatrix}\right) = \begin{bmatrix} 00 & 01 & 01 & 10 \\ 10 & 00 & 01 & 01 \\ 01 & 10 & 00 & 01 \\ 01 & 01 & 10 & 00 \end{bmatrix} \cdot \begin{bmatrix} 02 \\ 20 \\ 22 \\ 11 \end{bmatrix} = \begin{bmatrix} 21 \\ 20 \\ 11 \\ 10 \end{bmatrix} = \begin{bmatrix} 2x+1 \\ 2x \\ x+1 \\ x \end{bmatrix}$$

which was obtained via

$$\begin{array}{lcl}
\mathcal{S}^{4|P}_{0,3} : (00 \otimes_3 02) \oplus_3 (01 \otimes_3 20) \oplus_3 (01 \otimes_3 22) \oplus_3 (10 \otimes_3 11) & = & 00 \oplus_3 20 \oplus_3 22 \oplus_3 12 = 21 = 2x+1 \\
\mathcal{S}^{4|P}_{1,3} : (10 \otimes_3 02) \oplus_3 (00 \otimes_3 20) \oplus_3 (01 \otimes_3 22) \oplus_3 (01 \otimes_3 11) & = & 20 \oplus_3 00 \oplus_3 22 \oplus_3 11 = 20 = 2x \\
\mathcal{S}^{4|P}_{2,3} : (01 \otimes_3 02) \oplus_3 (10 \otimes_3 20) \oplus_3 (00 \otimes_3 22) \oplus_3 (01 \otimes_3 11) & = & 02 \oplus_3 01 \oplus_3 00 \oplus_3 11 = 11 = x+1 \\
\mathcal{S}^{4|P}_{3,3} : (01 \otimes_3 02) \oplus_3 (01 \otimes_3 20) \oplus_3 (10 \otimes_3 22) \oplus_3 (00 \otimes_3 11) & = & 02 \oplus_3 20 \oplus_3 21 \oplus_3 00 = 10 = x
\end{array}.$$

Consequently, the result is

$$\mathcal{S}^{4|P} = \begin{bmatrix} 20 & 10 & 00 & 21 \\ 10 & 01 & 12 & 20 \\ 12 & 12 & 20 & 11 \\ 11 & 12 & 10 & 10 \end{bmatrix} = \begin{bmatrix} 2x & x & 0 & 2x+1 \\ x & 1 & x+2 & 2x \\ x+2 & x+2 & 2x & x+1 \\ x+1 & x+2 & x & x \end{bmatrix},$$

which is *state 4* of the permutation $P_{S-Gr\o stl}$.

### 3.4.3 Permutation $Q$

Here we start with the input

$$\mathcal{S}^{0|Q} = \xi(m_1) = \begin{bmatrix} 01 & 11 & 12 & 02 \\ 22 & 10 & 10 & 01 \\ 10 & 02 & 02 & 12 \\ 20 & 21 & 01 & 01 \end{bmatrix},$$

which is state 0 of the permutation $Q_{S-Gr\o stl}$.

**AddRoundConstant** ($\sigma$)

First, we apply the $\sigma$ transformation. Since this is round $r = 0$ for the permutation $Q_{S-Gr\o stl}$, the round constant for $\sigma$ is

$$A^r = \begin{bmatrix} 22 & 22 & 22 & 22 \\ 22 & 22 & 22 & 22 \\ 22 & 22 & 22 & 22 \\ 22 & 21 & 20 & 12 \end{bmatrix} = \begin{bmatrix} 2x+2 & 2x+2 & 2x+2 & 2x+2 \\ 2x+2 & 2x+2 & 2x+2 & 2x+2 \\ 2x+2 & 2x+2 & 2x+2 & 2x+2 \\ 2x+2 & 2x+1 & 2x & x+2 \end{bmatrix}.$$

So state 1 of the permutation $Q_{S-Gr\o stl}$ is

$$\begin{aligned}\mathcal{S}^{1|Q} = \sigma(\mathcal{S}^{0|Q}) &= \begin{bmatrix} 22 \oplus_3 01 & 22 \oplus_3 11 & 22 \oplus_3 12 & 22 \oplus_3 02 \\ 22 \oplus_3 22 & 22 \oplus_3 10 & 22 \oplus_3 10 & 22 \oplus_3 01 \\ 22 \oplus_3 10 & 22 \oplus_3 02 & 22 \oplus_3 02 & 22 \oplus_3 12 \\ 22 \oplus_3 20 & 21 \oplus_3 21 & 20 \oplus_3 01 & 12 \oplus_3 01 \end{bmatrix} = \begin{bmatrix} 20 & 00 & 01 & 21 \\ 11 & 02 & 02 & 20 \\ 02 & 21 & 21 & 01 \\ 12 & 12 & 21 & 10 \end{bmatrix} \\ &= \begin{bmatrix} 2x & 0 & 1 & 2x+1 \\ x+1 & 2 & 2 & 2x \\ 2 & 2x+1 & 2x+1 & 1 \\ x+2 & x+2 & 2x+1 & x \end{bmatrix}.\end{aligned}$$

**SubTrits ($\lambda$)**

Second, we apply the $\lambda$ transformation, which is sequentially applied to each element of $\mathcal{S}^{1|Q}$. Our first element $\mathcal{S}^{1|Q}_{0,0} = 20$ is equivalent to the polynomial $2x$, so the multiplicative inverse is $(\mathcal{S}^{1|Q}_{0,0})^{-1} = 10$ for the polynomial $x$. This polynomial $x$ is then written in column-vector form, from top to bottom, and then multiplied by the matrix $B$ modulo 3; this yields the vector output

$$\lambda(10) = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \pmod 3 = \begin{bmatrix} 2 \\ 1 \end{bmatrix},$$

which is the vector encoding of the polynomial $2x+1$ whose coefficients are concatenated into the 2-trit string form 21. This gives us the new first element $\mathcal{S}^{2|Q}_{0,0} = 21$ of $\mathcal{S}^{Q}_{2}$.

Thus, $\lambda$ is repeatedly applied to all sixteen entries of $\mathcal{S}^{1|Q}$ to obtain

$$\lambda(\mathcal{S}^{1|Q}) = \mathcal{S}^{2|Q} = \begin{bmatrix} 21 & 00 & 11 & 01 \\ 10 & 22 & 22 & 21 \\ 22 & 01 & 01 & 11 \\ 02 & 02 & 01 & 12 \end{bmatrix} = \begin{bmatrix} 2x+1 & 0 & x+1 & 1 \\ x & 2x+2 & 2x+2 & 2x+1 \\ 2x+2 & 1 & 1 & x+1 \\ 2 & 2 & 1 & x+2 \end{bmatrix},$$

which is state 2 of the permutation $Q_{S-Grøstl}$.

### ShiftRows ($\pi$)

Third, we apply the $\pi$ transformation to each row of the state matrix $\mathcal{S}^{2|Q}$. Since we're currently applying the permutation $Q_{S-Grøstl}$, then the values $\varsigma$ for which $\pi$ will cyclically left shift all elements in rows 0, 1, 2, and 3 of $\mathcal{S}^{2|Q}$ respectively correspond to

$$\varsigma = [\varsigma(0) = 1, \varsigma(1) = 3, \varsigma(2) = 0, \varsigma(3) = 2].$$

Therefore, by applying $\pi$ to cyclically left shift each $i$th row of $\mathcal{S}^{2|Q}$ by $\sigma(i)$ we obtain

$$\begin{aligned}\mathcal{S}^{2|Q} = \begin{bmatrix} 21 & 00 & 11 & 01 \\ 10 & 22 & 22 & 21 \\ 22 & 01 & 01 & 11 \\ 02 & 02 & 01 & 12 \end{bmatrix} \longrightarrow \begin{bmatrix} 00 & 11 & 01 & 21 \\ 21 & 10 & 22 & 22 \\ 22 & 01 & 01 & 11 \\ 01 & 12 & 02 & 02 \end{bmatrix} &= \begin{bmatrix} 0 & x+1 & 1 & 2x+1 \\ 2x+1 & x & 2x+2 & 2x+2 \\ 2x+2 & 1 & 1 & x+1 \\ 1 & x+2 & 2 & 2 \end{bmatrix} \\ &= \pi(\mathcal{S}^{2|Q}) = \mathcal{S}_3^Q,\end{aligned}$$

which is state 3 of the permutation $Q_{S-Grøstl}$.

### MixColumns ($\rho$)

Fourth, we apply the $\rho$ transformation to each column of the state matrix $\mathcal{S}^{3|Q}$, which is given by the matrix multiplication $\mathcal{S}^{4|Q} \leftarrow D \times \mathcal{S}^{3|Q}$, such that $\mathcal{S}^{4|Q}$ is state 4 of the permutation $Q_{S-Grøstl}$.

To obtain the *first* column of $\mathcal{S}^{4|Q}$ we compute

$$\rho\left(\begin{bmatrix} 00 \\ 21 \\ 22 \\ 01 \end{bmatrix}\right) = \begin{bmatrix} 00 & 01 & 01 & 10 \\ 10 & 00 & 01 & 01 \\ 01 & 10 & 00 & 01 \\ 01 & 01 & 10 & 00 \end{bmatrix} \cdot \begin{bmatrix} 00 \\ 21 \\ 22 \\ 01 \end{bmatrix} = \begin{bmatrix} 20 \\ 20 \\ 12 \\ 12 \end{bmatrix} = \begin{bmatrix} 2x \\ 2x \\ x+2 \\ x+2 \end{bmatrix}.$$

To obtain the *second* column of $\mathcal{S}^{4|Q}$ we compute

$$\rho\left(\begin{bmatrix}11\\10\\01\\12\end{bmatrix}\right)=\begin{bmatrix}00&01&01&10\\10&00&01&01\\01&10&00&01\\01&01&10&00\end{bmatrix}\cdot\begin{bmatrix}11\\10\\01\\12\end{bmatrix}=\begin{bmatrix}00\\22\\22\\01\end{bmatrix}=\begin{bmatrix}0\\2x+2\\2x+2\\1\end{bmatrix}.$$

To obtain the *third* column of $\mathcal{S}^{4|Q}$ we compute

$$\rho\left(\begin{bmatrix}01\\22\\01\\02\end{bmatrix}\right)=\begin{bmatrix}00&01&01&10\\10&00&01&01\\01&10&00&01\\01&01&10&00\end{bmatrix}\cdot\begin{bmatrix}01\\22\\01\\02\end{bmatrix}=\begin{bmatrix}10\\10\\21\\00\end{bmatrix}=\begin{bmatrix}x\\x\\2x+1\\0\end{bmatrix}.$$

To obtain the *fourth* column of $\mathcal{S}^{4|Q}$ we compute

$$\rho\left(\begin{bmatrix}21\\22\\11\\02\end{bmatrix}\right)=\begin{bmatrix}00&01&01&10\\10&00&01&01\\01&10&00&01\\01&01&10&00\end{bmatrix}\cdot\begin{bmatrix}21\\22\\11\\02\end{bmatrix}=\begin{bmatrix}20\\21\\11\\22\end{bmatrix}=\begin{bmatrix}2x\\2x+1\\x+1\\2x+2\end{bmatrix}.$$

Consequently, the result is

$$\rho(\mathcal{S}^{3|Q})=\mathcal{S}^{4|Q}=\begin{bmatrix}20&00&10&20\\20&22&10&21\\12&22&21&11\\12&01&00&22\end{bmatrix}=\begin{bmatrix}2x&0&x&2x\\2x&2x+2&x&2x+1\\x+2&2x+2&2x+1&x+1\\x+2&1&0&2x+2\end{bmatrix},$$

which is *state 4* of the permutation $Q_{S-Grøstl}$.

### 3.4.4 Completing the Round

Finally, to complete the round, we add the results of $P_{S-Grøstl}$ and $Q_{S-Grøstl}$ together with $h_0$ to obtain

$$\begin{aligned}
\mathcal{S}^5 &= \mathcal{S}^{4|P} \oplus_3 \mathcal{S}^{4|Q} \oplus_3 h_0 \\
&= \begin{bmatrix} 20 & 10 & 00 & 21 \\ 10 & 01 & 12 & 20 \\ 12 & 12 & 20 & 11 \\ 11 & 12 & 10 & 10 \end{bmatrix} \oplus_3 \begin{bmatrix} 20 & 00 & 10 & 20 \\ 20 & 22 & 10 & 21 \\ 12 & 22 & 21 & 11 \\ 12 & 01 & 00 & 22 \end{bmatrix} \oplus_3 \begin{bmatrix} 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 10 \\ 00 & 00 & 00 & 12 \end{bmatrix} \\
&= \begin{bmatrix} 20 \oplus_3 20 \oplus_3 00 & 10 \oplus_3 00 \oplus_3 00 & 00 \oplus_3 10 \oplus_3 00 & 21 \oplus_3 20 \oplus_3 00 \\ 10 \oplus_3 20 \oplus_3 00 & 01 \oplus_3 22 \oplus_3 00 & 12 \oplus_3 10 \oplus_3 00 & 20 \oplus_3 21 \oplus_3 00 \\ 12 \oplus_3 12 \oplus_3 00 & 12 \oplus_3 22 \oplus_3 00 & 20 \oplus_3 21 \oplus_3 00 & 11 \oplus_3 11 \oplus_3 10 \\ 11 \oplus_3 12 \oplus_3 00 & 12 \oplus_3 01 \oplus_3 00 & 10 \oplus_3 00 \oplus_3 00 & 10 \oplus_3 22 \oplus_3 12 \end{bmatrix} \\
&= \begin{bmatrix} 10 & 10 & 10 & 11 \\ 00 & 20 & 22 & 11 \\ 21 & 01 & 11 & 02 \\ 20 & 10 & 10 & 11 \end{bmatrix} = \begin{bmatrix} x & x & x & x+1 \\ 0 & 2x & 2x+2 & x+1 \\ 2x+1 & 1 & x+1 & 2 \\ 2 & x & x & x+1 \end{bmatrix},
\end{aligned}$$

which is the final state of round 0. Since we're only doing 1 round for this example, then $\mathcal{S}^5$ is the final state in total, which contains the hash $\mathcal{H}$ of the original message $m_1 = \mathcal{M}$.

This concludes our example application of how the super-symmetric latin square $L^{(\mathbb{F}_{3^2},+)} \in \mathcal{L}^9$—that was generated by the SS-LS-GA, encodes the Galois field addition group $(\mathbb{F}_{3^2}, +)$, and possesses the confirmed maximum number of transversals $\mathbb{T}(9) = 2{,}241$—can be used to construct a cryptographic system.

# CHAPTER 4

# CONCLUSION

In this thesis we investigated the following questions:

- How can we efficiently generate latin squares? How can we efficiently count the number of transversals in a latin square?
- Which conditions indicate the existence of transversals in a latin square that encodes a group (or quasi-group)?
- Which latin squares possess the maximum (or minimum) transversal counts for a given order-$n$?
- Can we accurately predict which latin squares have the maximum (or minimum) transversal counts for a given order-$n$?
- Can we generate latin squares with maximum transversal counts?
- By investigating the above questions, can we obtain practical results that can be applied cryptography?

## 4.1 Main Results

Through our survey of pertinent results in the existing literature, we examined conditions in which latin squares possess transversals; for this we considered quasi-groups and groups (including Galois field addition). We examined the Delta Lemma

2.58 [6, 92, 93, 100], along with the Hall-Paige Conjecture 2.87 [106, 107] and its generalization, Theorem 2.90, which identifies six equivalent conditions that hold for solvable groups [6, 105]. To help guide our mathematical investigation, we created software tools to efficiently generate latin squares (up to at least order-31) and count their transversals up to order-17. By mathematically and computationally evaluating latin squares in terms of transversals, we were able to:

1. Generate latin square data sets and obtain transversal count results that match the existing results for minimum and maximum transversal counts [5, 6, 8].

2. Verify that the even order-$n$ cyclic latin squares that encode cyclic groups possess the confirmed minimum transversal counts $\mathbb{t}(n)$ for $2 \leq n \leq 9$ [5, 6, 8].

3. Verify that the prime order-$p$ cyclic latin squares that encode cyclic groups possess the confirmed maximum transversal counts $\mathbb{T}(p)$ for $2 \leq p \leq 9$ [5, 6, 8].

4. Create the new SS-LS-GA of Algorithm 2.3 for constructing super-symmetric latin squares of prime power order-$p^d$ that generalizes the order-$2^d$ algorithm proposed in [60].

5. Correctly predict that the prime power order-$p^d$ cyclic and super-symmetric latin squares possess the confirmed maximum transversal counts $\mathbb{T}(p^d)$ for $3 \leq p^d \leq 9$ [5, 6, 8] and the estimated lower bound $\lfloor \mathbb{T}(p^d) \rfloor$ for $9 < p^d \leq 17$ [5, 6, 8].

6. Discover that the Cayley tables which encode the addition groups of Galois fields are prime power order-$p^d$ super-symmetric latin squares (at least for $3 \leq p^d \leq 17$).

7. Propose Conjecture 2.100, which predicts that for prime power order-$p^d$ with $d > 0$:

- A cyclic or super-symmetric latin square $L$ (and every latin square in the same main equivalence class) may possess the maximum number of transversals $\mathbb{T}(p^d) = |\mathcal{T}(L)| = h(L) \cdot p^d$ with a uniform heat value $h(L)$.
- The estimated lower bound $\lfloor \mathbb{T}(p^d) \rfloor$ from [5, 6, 8] may be the correct $\mathbb{T}(p^d)$ and the estimated upper bound $\lceil \mathbb{T}(p^d) \rceil$ from [5, 6, 8] may be too high.

8. Apply the super-symmetric latin square $L^{(\mathbb{F}_{3^2},+)}$, which encodes the Galois field addition group $(\mathbb{F}_{3^2}, +)$, to create a new generalized and simplified version of the Grøstl CHF [61].

## 4.2 Outlook: Past and Future

The origin of Latin squares and the origin of magic squares are not known for certain. Some surviving historical evidence indicates that magic squares were known to numerous ancient civilizations [14, 15, 16]. Other evidence suggests that the latin square concept might be a relatively recent development [9, 10, 11, 17, 18]. In the author's opinion, the fact that such squares have practical applications in modern cryptography is fascinating and important! Moreover, it may be advantageous to conduct a thorough examination of historical literature and archaeological records pertaining to latin squares, graeco-latin squares, and magic squares; could one find additional square-based properties or methods known by the ancients that would have additional modern applications to disciplines such as cryptography?

To the best of our knowledge, it was Euler [9, 10, 11] who initiated a systematic mathematical examination of latin squares and their practical applications. After Cayley realized that his tables of finite groups are latin squares, the subject began to attract the serious interest of numerous mathematicians from around the world.

As a result, a “latin square bridge” was constructed between disciplines such as combinatorics and algebra. Such developments have built the foundation for a legion of historical and modern applications throughout the 20th and 21st centuries.

Since World War I and World War II, the methods of cryptography have become increasingly complex. The digital infrastructure of the modern world relies on our ability to maintain and increase the privacy, integrity, and security of computing systems with the methods of cryptography. Thus, it is critical to rigorously evaluate the computational security of cryptographic systems with new approaches via the methods of science and mathematics. Looking forward, in the author’s opinion, it may be advantageous to conduct a thorough investigation of inquiries such as the following:

- Can anybody prove Conjecture 2.100?
- If we thoroughly examine the proof of the estimated bounds $[\lfloor \mathbb{T}(n) \rfloor, \lceil \mathbb{T}(n) \rceil]$ from [5, 6, 8] for order-$n$, could this help us prove Conjecture 2.100 for order-$p^d$?
- How might super-symmetric latin square applications impact cryptography and cyber security?
- Can super-symmetric latin squares be generalized to $n$-dimensional super-symmetric latin hyper-cubes (ex. applied to [145, 146])? If so, would super-symmetric latin hyper-cubes be applicable to cryptography?
- Can ternary arithmetic, order-$3^d$ super-symmetric latin squares, and order-$3^d$ Galois fields be applied to developments in ternary computation and cryptographic systems (ex. applied to [147, 148, 149])? Moreover, will future computers and cryptographic systems be based on generalized order-$p^d$ Galois fields?

- What future applications will Musto's new quantum latin squares [150, 151] have? Is it possible to construct super-symmetric quantum latin squares? Could super-symmetric quantum latin squares be applied to quantum computing and post-quantum cryptography (ex. applied to [152])?

Perhaps in the future, if hard work, collaboration, and creativity are combined with the methods of science and mathematics, then it might be possible to answer such questions!

# REFERENCES

[1] L. Comtet, Dénes J., A. D. Keedwell, R. A. Fisher, and et. al. Sequence #A000315: Number of reduced latin squares of order n; also number of labeled loops with a fixed identity element. *The On-Line Encyclopedia of Integer Sequences.*

[2] C. A. Pickover, H. J. Ryser, J. A. A Sloane, and et. al. Sequence #A002860: Number of latin squares of order n; or labeled quasigroups. *The On-Line Encyclopedia of Integer Sequences.*

[3] J. W. Brown, R. A. Fisher, F. Yates, and et. al. Sequence #A040082: Number of inequivalent latin squares (or isotopy classes of latin squares) of order n. *The On-Line Encyclopedia of Integer Sequences.*

[4] F. Harary, Palmer E. M., N. J. A. Sloane, and et. al. Sequence #A003090: Number of species (or "main classes" or "paratopy classes") of latin squares of order n. *The On-Line Encyclopedia of Integer Sequences.*

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

[6] I. M. Wanless. Transversals in latin squares: a survey. *Surveys in Combinatorics 2011, London Mathematical Society*, Lecture Note Series 392:403–437, 2011.

[7] A. D. Thomas and G. V. Wood. *Group tables, Shiva Mathematics Series*, volume 2. Shiva Publishing Ltd., Cambridge, Mass, 1980.

[8] B. D. McKay, J. C. McLeod, and I. M. Wanless. The number of transversals in a latin square. *Designs, Codes and Cryptography*, 40(3):269–284, 2006.

[9] L. Euler. De quadratis magicis. *Commentationes arithmeticae*, 2:593–602, 1849.

[10] L. Euler. On magic squares. *arXiv preprint math/0408230*, (Translated by Jordan Bell in 2004).

[11] L. Euler. *Recherches sur une nouvelle espece de quarres magiques.* Zeeuwsch Genootschao, 1782.

[12] A. D. Keedwell and J. Dénes. *Latin squares and their applications.* Elsevier, 2015.

[13] N. Rapanos. Latin squares and their partial transversals. *The Harvard College Mathematics Review*, 2:4–12, 2008.

[14] S. S. Block and S. A. Tavares. *Before Sudoku.* Oxford University Press, Oxford, 2009.

[15] S. Cammann. The evolution of magic squares in China. *Journal of the American Oriental Society*, 80(2):116–124, 1960.

[16] T. Hayashi. Magic squares in Indian mathematics. In *Encyclopaedia of the History of Science, Technology, and Medicine in Non-Western Cultures*, pages 1252–1259. Springer, 2008.

[17] M. Petković. *Mathematics and Chess: 110 Entertaining Problems and Solutions.* Dover Publications, 1997.

[18] R. B. Bapat. Exploring mathematical ideas with a deck of cards. *Resonance: Journal of Science Education*, 12(3), 2007.

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

[20] A. Cayley. Desiderata and suggestions: No. 1. the theory of groups. *American journal of Mathematics*, 1(1):50–52, 1878.

[21] A. Cayley. Desiderata and suggestions: No. 2. the theory of groups: graphical representation. *American Journal of Mathematics*, 1(2):174–176, 1878.

[22] A. Cayley. On latin squares. *Messenger of Math*, 19:135–137, 1890.

[23] S. G. Ibragimov. On forgotten works of Ernst Schröder lying between algebra and logic (Russian). *Istor.-Mat. Issled.*, (17):247–258, 1966.

[24] R. Moufang. Zur struktur von alternativkörpern. *Mathematische Annalen*, 110(1):416–430, 1935.

[25] J. Dénes. On a problem of L. Fuchs. *Acta Sci. Math. (Szeged)*, 23:237–241, 1962.

[26] J. Dénes and E. Pásztor. Akvázicsoportok néhány problémájárol. *Magyar Tud. Akad. Mat. Fiz. Oszt. Közl.*, 13:109–118, 1963.

[27] J. R. Barra. A propos d'un théorème de r. c. rose. *C. R. Acad. Sci. Paris*, 256:5502–5504, 1963.

[28] R. Guérin. Aspects algébraiques du probldme de yamamoto. *C. R. Acad. Sci. Paris*, 256:583–586, 1963.

[29] D. Fog. Gruppentafeln and abstrakte gruppentheorie. *Skand. Mat. Kongr. Stockholm.*, pages 376–384, 1934.

[30] E. Schöhardt. Über lateinische quadrate und unionen. *J. Reine Angew. Math.*, 163:183–229, 1930.

[31] H. Wielandt and B. Huppert. Arithmetical and normal structure. *1960 Institute on Finite Groups: Held at California Institute of Technology, Pasadena, California, August 1-August 28, 1960:[Report]*, 6:17, 1962.

[32] R. G. U. Stell and J. H. Torrie. *Principles and procedures of statistics.* McGraw-Hill Book Company, Inc., New York, Toronto, London, 1960.

[33] R. Mandl. Orthogonal latin squares: an application of experiment design to compiler testing. *Communications of the ACM*, 28(10):1054–1058, 1985.

[34] R. Datta and N. A. Touba. Generating burst-error correcting codes from orthogonal latin square codes–a graph theoretic approach. In *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2011 IEEE International Symposium on*, pages 367–373. IEEE, 2011.

[35] L. Janczewski. *Cyber warfare and cyber terrorism.* IGI Global, 2007.

[36] R. R. Dipert. The ethics of cyberwarfare. *Journal of Military Ethics*, 9(4):384–410, 2010.

[37] J. Andress and S. Winterfeld. *Cyber warfare: techniques, tactics and tools for security practitioners.* Elsevier, 2013.

[38] E. Byres and J. Lowe. The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress*, volume 116, pages 213–218, 2004.

[39] United States Coast Guard. *Cyber Strategy*, 2015. Available at `http://www.uscg.mil/seniorleadership/DOCS/cyber.pdf`; accessed on 2016-11.

[40] United States Department of Energy. *Cybersecurity*, 2016. Available at `http://www.energy.gov/oe/services/cybersecurity`; accessed on 2016-11.

[41] K. Zetter. *The Biggest Security Threats We'll Face in 2016*, 2016. Available at `http://www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016/`; accessed on 2016-01.

[42] McAfee Labs. *2016 Threats Predictions Report*, 2015. Available at `http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf`; accessed on 2016-05.

[43] M. Krancer. *The Biggest Cybersecurity Threat: The Energy Sector*, 2015. Available at `http://www.forbes.com/sites/michaelkrancer/2015/11/04/the-biggest-cybersecurity-threat-the-energy-sector/`; accessed on 2015-11.

[44] A. M. Turing. Mathematical theory of enigma machine. *Public Record Office, London*, 3, 1940.

[45] S. Singh. *The code book: the science of secrecy from ancient Egypt to quantum cryptography.* Anchor, 2011.

[46] W. Kozaczuk. *Enigma: how the German machine cipher was broken, and how it was read by the Allies in World War Two.* Univ Pubns of Amer, 1984.

[47] B. J. Copeland. Colossus: its origins and originators. *IEEE Annals of the History of Computing*, (4):38–45, 2004.

[48] F. L. Carter. *Codebreaking with the Colossus Computer*. Bletchley Park Trust, 2008.

[49] É. Galois and P. M. Neumann. *The mathematical writings of Évariste Galois*, volume 6. European mathematical society, 2011.

[50] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications.* Cambridge university press, 1994.

[51] J. Bewersdorff. Galois theory for beginners. *American Mathematical Society, Providence, Rhode Island*, 2006.

[52] D. P. Mehendale. Finite projective planes. *arXiv preprint math/0611492*, 2006.

[53] J. Dénes and A. D. Keedwell. *Latin squares: New developments in the theory and applications*, volume 46. Elsevier, 1991.

[54] C. F. Laywine and G. L. Mullen. *Discrete mathematics using Latin squares*, volume 49. John Wiley & Sons, 1998.

[55] C. J. Colbourn and J. H. Dinitz. *Handbook of combinatorial designs.* CRC press, 2006.

[56] S. Dasgupta, G. Károlyi, O. Serra, and B. Szegedy. Transversals of additive latin squares. *Israel Journal of Mathematics*, 126(1):17–28, 2001.

[57] N. Alon. Additive latin transversals. *Israel Journal of Mathematics*, 117(1):125–130, 2000.

[58] C. Cooper, R. Gilchrist, I. N. Kovalenko, and D. Novakovic. Estimation of the number of "good" permutation with applications to cryptography. *Cybernetics and Systems Analysis*, 35(5):688–693, 1999.

[59] C. Cooper. A lower bound for the number of good permutations. *Data Recording, Storage and Processing (Nat. Acad. Sci. Ukraine)*, 213:15–25, 2000.

[60] M. A. P. Chamikara, S. R. Kodituwakku, A. A. C. A. Jayathilake, and A. A. I. Perera. An algorithm to construct super-symmetric latin squares of order $2^n$. *IJRIT International Journal of Research in Information Technology*, 1(4):38–50, 2013.

[61] P. Gauravaram, L. R. Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schläffer, and S. S. Thomsen. Grøstl - a SHA-3 candidate. In *Dagstuhl Seminar Proceedings.* Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2009.

[62] M. Frolov. Sur les permutations carrés. *J. de Math. spéc*, 4:8–11, 1890.

[63] M. G. Tarry. *Le probleme des 36 officiers.* Association Française, 1900.

[64] P. A. MacMahon. Combinatorial analysis, vols. 1 and 2, 1915.

[65] H. W. Norton. The 7 × 7 squares. *Annals of Eugenics*, 9(3):269–307, 1939.

[66] A. Sade. Enumeration des carrés latins. *Application au 7e ordre. Conjecture pour les ordres supérieurs, Marseille*, 1948.

[67] P. N. Saxena. A simplified method of enumerating latin squares by MacMahon's differential operators; ii. the 7 × 7 latin squares. *J. Indian Soc. Agric. Statistics*, 3:24–79, 1951.

[68] M. B. Wells. The number of latin squares of order eight. *Journal of Combinatorial Theory*, 3(1):98–99, 1967.

[69] S. E. Bammel and J. Rothstein. The number of 9 × 9 latin squares. *Discrete Mathematics*, 11(1):93–95, 1975.

[70] B. D. McKay and E. Rogoyski. Latin squares of order 10. *Electron. J. Combin*, 2:N3, 1995.

[71] B. D. McKay and I. M. Wanless. On the number of latin squares. *Annals of combinatorics*, 9(3):335–344, 2005.

[72] J. H. van Lint and R. M. Wilson. *A course in combinatorics*. Cambridge University Press, 2001.

[73] J. Shao and W. Wei. A formula for the number of latin squares. *Discrete mathematics*, 110(1):293–296, 1992.

[74] D. S. Stones. The many formulae for the number of latin rectangles. *Electronic Journal of Combinatorics*, 17(1), 2010.

[75] R. J. Stones, S. Lin, X. Liu, and G. Wang. On computing the number of latin rectangles. *Graphs and Combinatorics*, pages 1–16, 2015.

[76] A. Cayley. *The collected mathematical papers of Arthur Cayley*, volume 7. The University Press, 1894.

[77] R. Baer. Nets and groups. *Transactions of the American Mathematical Society*, 46(1):110–141, 1939.

[78] R. Baer. Nets and groups. ii. *Transactions of the American Mathematical Society*, 47(3):435–439, 1940.

[79] A. A. Albert. Quasigroups. i. *Transactions of the American Mathematical Society*, 54(3):507–519, 1943.

[80] A. A. Albert. Quasigroups. ii. *Transactions of the American Mathematical Society*, 55(3):401–419, 1944.

[81] K. Yamamoto. Generation principles of latin squares. *Bull. Inst. Internat. Statist*, 38:73–76, 1961.

[82] M. J. Strube. A basic program for the generation of latin squares. *Behavior Research Methods*, 20(5):508–509, 1988.

[83] B. G. Kim and H. H. Stein. A spreadsheet program for making a balanced latin square design. *Revista Colombiana de Ciencias Pecuarias*, 22(4):591–596, 2009.

[84] R. Fontana. Random latin squares and sudoku designs generation. *Electronic Journal of Statistics*, 8(1):883–893, 2014.

[85] I. Gallego Sagastume. Generation of random latin squares step by step and graphically. In *XX Congreso Argentino de Ciencias de la Computación (Buenos Aires, 2014)*, 2014.

[86] C. J. Colbourn. The complexity of completing partial latin squares. *Discrete Applied Mathematics*, 8(1):25–30, 1984.

[87] T. Easton and R. G. Parker. On completing latin squares. *Discrete Applied Mathematics*, 113(2):167–181, 2001.

[88] H. R. Lewis and C. H. Papadimitriou. *Elements of the Theory of Computation.* Prentice Hall PTR, 1997.

[89] J. Van Leeuwen. *Handbook of theoretical computer science (vol. A): algorithms and complexity.* Mit Press, 1991.

[90] J. J. Watkins. *Across the board: the mathematics of chessboard problems.* Princeton University Press, 2004.

[91] H. S. Snevily. The Cayley addition table of $\mathbb{Z}_n$. *The American Mathematical Monthly*, 106(6):584–585, 1999.

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

[93] A. B. Evans. Latin squares without orthogonal mates. *Designs, Codes and Cryptography*, 40(1):121–130, 2006.

[94] D. Bryant, J. Egan, B. Maenhaut, and I. M. Wanless. Indivisible plexes in latin squares. *Designs, Codes and Cryptography*, 52(1):93–105, 2009.

[95] P. Danziger, I. M. Wanless, and B. S. Webb. Monogamous latin squares. *Journal of Combinatorial Theory, Series A*, 118(3):796–807, 2011.

[96] J. Egan. Bachelor latin squares with large indivisible plexes. *Journal of Combinatorial Designs*, 19(4):304–312, 2011.

[97] J. Egan and I. M. Wanless. Indivisible partitions of latin squares. *Journal of Statistical Planning and Inference*, 141(1):402–417, 2011.

[98] J. Egan and I. M. Wanless. Latin squares with restricted transversals. *Journal of Combinatorial Designs*, 20(2):124–141, 2012.

[99] K. Pula. A generalization of plexes of latin squares. *Discrete Mathematics*, 311(8):577–581, 2011.

[100] I. M. Wanless and B. S. Webb. The existence of latin squares without orthogonal mates. *Designs, Codes and Cryptography*, 40(1):131–135, 2006.

[101] J. Faulhaber. *Academia Algebrae: darinnen dir miraculosische Guvontiones zu den höchsten Costen weiters continuirt u. profitiert werden.* Remmelin, 1631.

[102] H. B. Mann. The construction of orthogonal latin squares. *The Annals of Mathematical Statistics*, 13(4):418–423, 1942.

[103] K. Balasubramanian. On transversals in latin squares. *Linear Algebra and Its Applications*, 131:125–129, 1990.

[104] H. J. Ryser. Neuere probleme der kombinatorik. *Vorträge über Kombinatorik, Oberwolfach*, pages 69–91, 1967.

[105] M. Vaughan-Lee and I. M. Wanless. Latin squares and the hall–paige conjecture. *Bulletin of the London Mathematical Society*, 35(2):191–195, 2003.

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

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

[108] J. Louis. Lagrange. *Suite des réflexions sur la résolution algébrique des équations.* CF Voss, 1773.

[109] M. L. Sylow. Théoremes sur les groupes de substitutions. *Mathematische Annalen*, 5(4):584–594, 1872.

[110] J. F. Humphreys. *A course in group theory*, volume 6. Oxford University Press on Demand, 1996.

[111] P. Hall. A note on soluble groups. *Journal of the London Mathematical Society*, 1(2):98–105, 1928.

[112] J. Hsiang, D. F. Hsu, and Y. Shieh. On the hardness of counting problems of complete mappings. *Discrete mathematics*, 277(1):87–100, 2004.

[113] R. Rivest. The md5 message-digest algorithm, 1992. *RFC1321, Internet Activities Board, Internet Engineering Task Force*, 2004.

[114] H. Feistel. Cryptography and computer privacy. *Scientific American*, 228:15–23, 1973.

[115] B. Schneier. Cryptanalysis of MD5 and SHA: Time for a new standard. *Computer World*, 2004.

[116] M. Bellare, R. Canetti, and H. Krawczyk. Keying hash functions for message authentication. In *Advances in Cryptology (CRYPTO'96)*, pages 1–15. Springer, 1996.

[117] J. A. Halderman, B. Waters, and E. W. Felten. A convenient method for securely managing passwords. In *Proceedings of the 14th International Conference on World Wide Web*, WWW '05, pages 471–479, New York, NY, USA, 2005. ACM.

[118] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell. Stronger password authentication using browser extensions. In *Usenix security*, pages 17–32. Baltimore, MD, USA, 2005.

[119] C. Lee, L. Li, and M. Hwang. A remote user authentication scheme using hash functions. *ACM SIGOPS Operating Systems Review*, 36(4):23–29, 2002.

[120] J. Fridrich and M. Goljan. Robust hash functions for digital watermarking. In *Information Technology: Coding and Computing, 2000. Proceedings. International Conference on*, pages 178–183. IEEE, 2000.

[121] United States National Institute of Standards and Technology. *SHA-3 Competition (2007-2012)*, 2005. Available at `http://csrc.nist.gov/groups/ST/hash/sha-3/`; accessed on 2016-11.

[122] United States National Institute of Standards and Technology. *SHA-3 Competition First Round Candidates*, 2008. Available at `http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions_rnd1.html`; accessed on 2016-11.

[123] United States National Institute of Standards and Technology. *SHA-3 Competition Second Round Candidates*, 2009. Available at `http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/submissions_rnd2.html`; accessed on 2016-11.

[124] A. Regenscheid, R. Perlner, S. Chang, J. Kelsey, M. Nandi, and S. Paul. Status report on the first round of the SHA-3 cryptographic hash algorithm competition. *Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD*, pages 20899–8930, 2009.

[125] United States National Institute of Standards and Technology. *NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition*, 2012. Available at `http://www.nist.gov/itl/csd/sha-100212.cfm`; accessed on 2016-11.

[126] J. Aumasson, L. Henzen, W. Meier, and R. C. Phan. SHA-3 proposal BLAKE. *Submission to NIST*, 2008.

[127] H. Wu. The hash function JH. *Submission to NIST (round 3)*, page 6, 2011.

[128] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. The Keccak SHA-3 submission. *Submission to NIST (Round 3)*, 6(7):16, 2011.

[129] N. Ferguson, S. Lucks, B. Schneier, D. Whiting, M. Bellare, T. Kohno, J. Callas, and J. Walker. The skein hash function family. *Submission to NIST (round 3)*, 7(7.5):3, 2010.

[130] United States National Institute of Standards and Technology. *NIST Releases SHA-3 Cryptographic Hash Standard*, 2015. Available at `http://www.nist.gov/itl/csd/201508_sha3.cfm`; accessed on 2016-11.

[131] C. Paar and J. Pelzl. *Understanding cryptography: a textbook for students and practitioners.* 2009.

[132] B. Preneel, R. Govaerts, and J. Vandewalle. Hash functions based on block ciphers: A synthetic approach. In *Advances in Cryptology (CRYPTO'93)*, pages 368–378. Springer, 1993.

[133] T. Bartkewitz. Building hash functions from block ciphers, their security and implementation properties. *Ruhr-University Bochum*, 2009.

[134] R. L. Rivest and J. C. N. Schuldt. Spritz-a spongy rc4-like stream cipher and hash function. *Proceedings of the Charles River Crypto Day, Palo Alto, CA, USA*, 24, 2014.

[135] A. Bogdanov, F. Mendel, F. Regazzoni, V. Rijmen, and E. Tischhauser. Ale: Aes-based lightweight authenticated encryption. In *Fast Software Encryption*, pages 447–466. Springer, 2013.

[136] S. Gueron and M. E. Kounavis. Vortex: A new family of one-way hash functions based on aes rounds and carry-less multiplication. In *Information Security*, pages 331–340. Springer, 2008.

[137] J. Daemen and V. Rijmen. *The design of Rijndael: AES-the advanced encryption standard.* Springer Science & Business Media, 2013.

[138] B. Preneel, V. Rijmen, and A. Bosselaers. Principles and performance of cryptographic algorithms. *Dr. Dobb's journal*, 23(12):126–131, 1998.

[139] J. Daemen and V. Rijmen. AES proposal: Rijndael. 1999.

[140] J. Daemen and V. Rijmen. The design of Rijndael. information security and cryptography. *Text and Monographs, Springer Verlag*, 2002.

[141] United States National Institute of Standards and Technology. *Commerce Department Announces Winner of Global Information Security Competition*, 2000. Available at `https://www.nist.gov/news-events/news/2000/10/commerce-department-announces-winner-global-information-security`; accessed on 2016-11.

[142] C. Cid, S. Murphy, and M. Robshaw. *Algebraic aspects of the advanced encryption standard*. Springer Science & Business Media, 2006.

[143] W. Stallings. Electronic mail security. *Cryptography and Network Security Principles and Practice. 6th Edition, Pearson Education, Upper Saddle River*, pages 67–68, 2014.

[144] J. Daemen and V. Rijmen. The wide trail design strategy. In *IMA International Conference on Cryptography and Coding*, pages 222–238. Springer, 2001.

[145] B. Tang. Orthogonal array-based latin hypercubes. *Journal of the American statistical association*, 88(424):1392–1397, 1993.

[146] K. Q. Ye. Orthogonal column latin hypercubes and their application in computer experiments. *Journal of the American Statistical Association*, 93(444):1430–1439, 1998.

[147] G. Frieder. Ternary computers: Part i: Motivation for ternary computers. In *Conference Record of the 5th Annual Workshop on Microprogramming*, MICRO 5, pages 83–86, New York, NY, USA, 1972. ACM.

[148] M. Glusker, D. M. Hogan, and P. Vass. The ternary calculating machine of thomas fowler. *IEEE Annals of the History of Computing*, 27(3):4–22, 2005.

[149] J. Yi, H. Huacan, and L. Yangtian. Ternary optical computer architecture. *Physica Scripta*, 2005(T118):98, 2005.

[150] B. Musto and J. Vicary. Quantum latin squares and unitary error bases. *arXiv preprint arXiv:1504.02715*, 2015.

[151] B. Musto. Constructing mutually unbiased bases from quantum latin squares. *arXiv preprint arXiv:1605.08919*, 2016.

[152] P. Gaborit. *Post-Quantum Cryptography*. Springer, 2013.

[153] S. Warner. *Modern algebra*. Courier Corporation, 1990.

[154] T. W. Judson. Abstract algebra. 2010.

[155] J. Gallian. *Contemporary abstract algebra.* Cengage Learning, 2016.

[156] D. S. Dummit and R. M. Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

# APPENDIX A

# ARITHMETIC AND GALOIS FIELDS

Here we introduce Galois fields in terms of elementary and modular arithmetic. All of the definitions and results provided here in known facts that can be obtained from textbooks on abstract algebra or number theory. Most of this content is obtained from [50, 153, 154, 155, 156].

To the best of our knowledge, the oldest and most elementary branch of mathematics is *arithmetic*: the study of numbers and the properties of the traditional operations between them: addition, subtraction, multiplication, and division. Anybody who has studied any form of mathematics probably knows this. Many of us use arithmetic on a routine basis and take crucial notions such as division, factorization, and commutativity for granted. However, one fact that many people may not know is that there exists a multitude of mathematical objects and structures for which the commonly assumed division, factorization, and commutativity "don't work" or "behave in a bizarre way".

For example, one might say that a structure such as the integers ($\mathbb{Z}$) is not as "well-behaved" as structures such as the rationals ($\mathbb{Q}$) or the reals ($\mathbb{R}$); if one is restricted to working in $\mathbb{Z}$, then a division operation such as $\frac{3}{2}$ "doesn't work" because $\frac{3}{2} \notin \mathbb{Z}$, etc. Thus, there are important branches of modern mathematics such as number theory and abstract algebra which aim to study, evaluate, and classify the fundamental properties and capabilities of such objects and structures. Number theory and abstract algebra have enormous applications in disciplines such as cryptography and cyber security.

Now let's consider the importance of arithmetic in the discipline of cryptography, where the objective may be to build computationally secure systems for applications such as encryption or password authentication; a crypto-system upon which the security of an modern infastructure (ex. the Internet) greatly depends on. For the designers of such crypto-systems, it is imperative to know the fundamental properties and capabilities of the underlying algebraic structures upon which those systems operate. For example, in the case of symmetric-key encryption, the sender must be able to apply a sequence of transformations that converts a plaintext message to ciphertext; it is likely that such transformations require arithmetic operations. Thereafter, the receiver must be able to apply a sequence of "reverse" or inverse transformations that converts the ciphertext back to the original plaintext. Thus, in order to decrypt the message that was encrypted using arthimetic operations such as addition and multiplication, the underlying algebraic structures of the crypto-system must have "built-in" inverse operations such as subtraction and division. Now in the case of CHFs it is clear that such decryption doesn't apply (even though we recall that many CHFs are based on such symmetric-key ciphers to begin with) because they are one-way functions. However, in order for us to build any such workable crypto-system in the first place, we must also have the ability to apply the various elementary arithmetic operations and their inverse counterparts.

With this notion of arithmetic in mind, let's first consider the following elementary algebraic structure:

**Definition A.1.** A *monoid* $\mathcal{M} = (\mathcal{M}, \oplus)$ is a set equipped with a binary operation

$\oplus$ such that the following monoid axioms hold:

(i) $\oplus$ is *closed*: $a \oplus b \in \mathcal{M}, \quad \forall a, b \in \mathcal{M}$.

(ii) $\oplus$ is *associative*: $a \oplus (b \oplus c) = (a \oplus b) \oplus c, \quad \forall a, b, c \in \mathcal{M}$.

(iii) There exists an *identity element* (denoted by $e \in \mathcal{M}$) such that: $a \oplus e = a = e \oplus a, \quad \forall a \in \mathcal{M}$.

We see that a monoid $\mathcal{M} = (\mathcal{M}, \oplus)$ let's us "add" two elements together with the operation $\oplus$; but $\oplus$ is *not* the same as the traditional arithmetic operation $+$ because $\oplus$ lacks numerous arithmetic properties. For example, if we're restricted to working in $\mathcal{M}$, then there is no well-defined method to compute the inverse of an element to establish any form of "subtraction", nor is $\oplus$ commutative, etc. Therefore, let's consider the following structures, which enable us to introduce notions such as inverse elements, commutativity, and so forth.

**Definition A.2.** A monoid $\mathcal{G} = (\mathcal{G}, \oplus)$ is said to be a *group* if, for each element, there exists an *inverse element*: $\forall a \in \mathcal{G},\ \exists b \in \mathcal{G},\ a \oplus b = e = b \oplus a$.

**Definition A.3.** A group $\mathcal{G} = (\mathcal{G}, \oplus)$ is said to be an *abelian group* if $\oplus$ is *commutative*: $a \oplus b = b \oplus a, \quad \forall a, b \in \mathcal{G}$.

Next, let's use the above definitions to define an additional structure which is slightly more "sophisticated".

**Definition A.4.** A *ring* $\mathcal{R} = (\mathcal{R}, \oplus, \otimes)$ is a set equipped with the binary operations of addition $\oplus$ and multiplication $\otimes$ such that the following ring axioms hold:

(i) $(\mathcal{R}, \oplus)$ is an abelian group.

(ii) $(\mathcal{R}, \otimes)$ is a monoid.

(iii) $\otimes$ is left and right *distributive* over $\oplus$:

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c) \ \text{ and } \ (a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c), \ \ \forall a, b, c \in \mathcal{R}.$$

In other words, one can build a ring $\mathcal{R} = (\mathcal{R}, \oplus, \otimes)$ by "combining" an abelian group $\mathcal{G} = (\mathcal{G}, \oplus)$ with a monoid $\mathcal{M} = (\mathcal{M}, \oplus)$ in compliance with the above axioms, where $\mathcal{G}$ and $\mathcal{M}$ "interact" via the distributive property. In terms of our cryptographic goals, an algebraic structure such as $\mathcal{R}$ gives us more of the desired "arithmetic behavior" to work with. In fact $\mathcal{R}$ can be equipped with additional properties such as the following:

**Definition A.5.** Let $\mathcal{R} = (\mathcal{R}, \oplus, \otimes)$ be a ring.

(i) $\mathcal{R}$ is said to be a *commutative ring* if: the multiplication $\otimes$ is commutative.

(ii) $\mathcal{R}$ is said to be a *ring with identity* if: there is a unique identity element, denoted by $1 \in \mathcal{R}$, such that $1 \neq 0$, where $1 \otimes a = a \otimes 1, \ \ \forall a \in \mathcal{R}$.

(iii) If $\mathcal{R}$ is a commutative ring with identity ($1 \neq 0$), then $\mathcal{R}$ is said to be an *integral domain* if: $a \otimes b = 0 \implies a = 0 \ \text{ or } \ b = 0$.

(iv) If $\mathcal{R}$ is a ring with identity, then $\mathcal{R}$ is said to be a *division ring* if:
$$\forall a \in \mathcal{R}, \ a \neq 0 \implies \exists b \in \mathcal{R}, \ a \otimes b = 1.$$

**Example A.6.** Consider the set of integers $\mathbb{Z}$. As it turns out, $\mathbb{Z}$ is a classic example of an integral domain so we may write it in ring notation as $\mathbb{Z} = (\mathbb{Z}, +, \bullet)$. In this case, $\mathbb{Z}$ is a ring with identity such that its two binary operations $+$ and $\bullet$ are both commutative and associative, and where $\bullet$ distributes over $+$; so these are useful arithmetic properties to have at our disposal! Furthermore $\mathbb{Z}$'s $+$ operation has an additive inverse so each element of $\mathbb{Z}$ has a corresponding inverse and can be related to the additive identity; this is also a very useful property. But what about $\mathbb{Z}$'s $\bullet$ operation? Does $\bullet$ have the same useful properties as $+$? For this let's consider an example: take $5 \in \mathbb{Z}$. Does 5 have a multiplicative inverse in $\mathbb{Z}$ that would enable us to "reverse" 5 to obtain the multiplicative identity 1? No. This is because the multiplicative inverse of 5 is $\frac{1}{5}$, and we're working strictly in $\mathbb{Z}$ so $\frac{1}{5} \notin \mathbb{Z}$. This means that $\mathbb{Z}$ is not a division ring because in general division "doesn't work". Therefore, if we were to try to build a crypto-system based entirely on $\mathbb{Z}$ it wouldn't be very applicable because we can't perform the elementary arithmetic operation of division to undo such transformations.

Therefore, the above example motivates us to consider an algebraic structure equipped with division that fully supports elementary arithmetic.

**Definition A.7.** A ring $\mathbb{F} = (\mathbb{F}, +, \bullet)$ is said to be a *field* if $\mathbb{F}$ is a commutative division ring.

The division capability of $\mathbb{F}$ makes it a powerful structure indeed! But are all such fields applicable to crypto-systems that operate on modern digital computers?

**Example A.8.** Some classic examples of fields are $\mathbb{Q} = (\mathbb{Q}, +, \bullet)$ and $\mathbb{R} = (\mathbb{R}, +, \bullet)$. If we're working in either of these structures, then we have every property of $\mathbb{Z}$ plus the additional operation of division. However, in terms of cryptographic applicability there is still a major issue: assuming that we have modern digital computers that encode only finite states, how can we build a working crypto-system that is based on the totality of either $\mathbb{Q}$ or $\mathbb{R}$ when they both require us to encode an infinite number of states? We can't, as such an exact infinite representation on a finite digital system is impossible.

Therefore, the above example motivates us to consider a specific type of field that can be fully represented with a finite number of states on a digital computer.

**Definition A.9.** A field $\mathbb{F}_n = (\mathbb{F}, +, \bullet)$ is said to be a *finite field* if it contains a finite number of elements $n$; that is, if its *order*, denoted by $|\mathbb{F}| = n$, is finite. Equivalently, a finite field $\mathbb{F}_n$ is often called a *Galois field.*

**Remark A.10.** For the sake of conciseness, from this point forward we will write $\mathbb{F}$ to declare a field and omit the full notation of $\mathbb{F} = (\mathbb{F}, +, \bullet)$ unless a clear distinction is required. If such a field is necessarily Galois with a $n$ elements, then we will write $\mathbb{F}_n$; Galois field is the term that we use throughout this thesis for Évariste Galois [49, 51].

Next we show how to use the properties of an integral domain (like $\mathbb{Z}$) to construct a Galois field with arithmetic that we can use in crypto-systems.

**Definition A.11.** Let $\mathcal{R} = (\mathcal{R}, +, \bullet)$ be a ring and let $\mathcal{R}^* = \mathcal{R} \setminus \{0\}$.

- An element $a \in \mathcal{R}$ is said to be a *zero divisor* in $\mathcal{R}$ if there exists some $b \in \mathcal{R}^*$ such that $a \bullet b = 0$ or $b \bullet a = 0$.
- An element $a \in \mathcal{R}^*$ is said to be a *proper zero divisor* in $\mathcal{R}$ if there exists some $b \in \mathcal{R}^*$ such that $a \bullet b = 0$ or $b \bullet a = 0$.

**Definition A.12.** Let $\mathcal{R} = (\mathcal{R}, +, \bullet)$ be a ring. Then an element $r \in \mathcal{R}$ is said to be *cancellable* if and only if for all $a, b \in \mathcal{R}$

$$\begin{array}{rclcrcl} r \bullet a & = & r \bullet b & \Longrightarrow & a & = & b \\ a \bullet r & = & b \bullet r & \Longrightarrow & a & = & b. \end{array}$$

**Theorem A.13.** *Let $\mathcal{R} = (\mathcal{R}, +, \bullet)$ be a ring such that $\mathcal{R} \neq \emptyset$ and let $\mathcal{R}^* = \mathcal{R} \setminus \{0\}$. If $r \in \mathcal{R}^*$, then $r$ is a zero divisor if and only if $r$ is not cancellable for $\bullet$.*

***Proof.*** Let $\mathcal{R} = (\mathcal{R}, +, \bullet)$ be a ring such that $\mathcal{R} \neq 0$ and let $\mathcal{R}^* = \mathcal{R} \setminus \{0\}$. Take any $r \in \mathcal{R}^*$.

($\Longrightarrow$) Suppose that $r$ is a zero divisor. Then by Definition A.11 there exists some $a \in \mathcal{R}^*$ such that $r \bullet a = 0$ or $a \bullet r = 0$. Then $r$ is not cancellable for $\bullet$ because $r \bullet 0 = 0 = 0 \bullet r$. ☑

($\Longleftarrow$) Suppose that $r$ is cancellable. Then by Definition A.12 there exists some $a, b \in \mathcal{R}^*$ such that $r \bullet a = r \bullet b$ where $a \neq b$ for left $\bullet$ by $r$. Then

$$r \bullet a = r \bullet b \implies r \bullet a - r \bullet b = 0 \implies r \bullet (a - b) = 0 \implies a - b \neq 0.$$

So $r$ is a zero divisor. By similar argument, we may also suppose that $a \bullet r = b \bullet r$ where $a \neq b$ for right $\bullet$ by $r$; then it similarly follows that $r$ is a zero divisor. ☑

Consequently $r$ is a zero divisor if and only if $r$ is not cancellable for $\bullet$. ■

**Theorem A.14.** *If the ring $\mathcal{R} = (\mathcal{R}, +, \bullet)$ is a finite integral domain, then $\mathcal{R}$ is a Galois field.*

***Proof***. Suppose that $\mathcal{R} = (\mathcal{R}, +, \bullet)$ is a finite integral domain. Since $\mathcal{R}$ is finite, then we may list the elements of $\mathcal{R}$ as $x_0, x_1, x_2, x_3, \ldots, x_n$ where we let $x_0 = 0$ and $x_1 = 1$ be the identities for $+$ and $\bullet$, respectively. Now let $\mathcal{R}^* = \mathcal{R} \setminus \{0\}$. Fix any $r \in \mathcal{R}^*$ and consider the set of products

$$\mathcal{R}' = \{r \bullet x_1,\ r \bullet x_2,\ r \bullet x_3,\ \ldots,\ r \bullet x_n\},$$

where each $r \bullet x_i \in \mathcal{R}$ for $i = 1, 2, 3, \ldots, n$ because $\mathcal{R}$ is closed under $+$ and $\bullet$. So $\mathcal{R}' \subset \mathcal{R}$. Now by Definition A.5, since $\mathcal{R}$ is an integral domain, it follows that

$$r \bullet x_i \neq 0 \implies r \bullet x_i \in \mathcal{R}^*, \quad \text{for } i = 1, 2, 3, \ldots, n.$$

Hence, by Theorem A.13 it follows that each $r \in \mathcal{R}^*$ is cancellable for $\bullet$; so

$$r \bullet x_i = r \bullet x_j \implies x_i = x_j, \quad \text{for } i, j = 1, 2, 3, \ldots, n.$$

Therefore each $r \bullet x_i \in \mathcal{R}'$ is distinct and cancellable with $|\mathcal{R}'| = n = |\mathcal{R}^*|$, so $\mathcal{R}' = \mathcal{R}^*$. Therefore, since $1 \in \mathcal{R}^*$ there exists some $r^{-1} \in \mathcal{R}^*$ such that $r \bullet r^{-1} = 1$; so this holds for any nonzero $r \in \mathcal{R}$. Consequently by Definitions A.7 and A.9 it follows that $\mathcal{R}$ is a Galois field of order-$(n+1)$. ■

**Definition A.15.** Let $\mathcal{R} = (\mathcal{R}, +, \bullet)$ be a ring.

- A subset $\mathcal{A}$ of a ring $\mathcal{R}$ is a *subring* of $\mathcal{R}$ if the $+$ and $\bullet$ of $\mathcal{A}$ are closed; that is

$$a + b \in \mathcal{A} \text{ and } a \bullet b \in \mathcal{A}, \quad \forall a, b \in \mathcal{A}.$$

- A subring $\mathcal{I}$ of a ring $\mathcal{R}$ is an *ideal* if:

$$a \bullet r \in \mathcal{I} \text{ and } r \bullet a \in \mathcal{I},\ \forall a \in \mathcal{I} \text{ and } \forall r \in \mathcal{R}.$$

**Definition A.16.** Let $\mathcal{I}$ be an ideal of the ring $\mathcal{R} = (\mathcal{R}, +, \bullet)$.

- Then a binary relation $\sim$ of $\mathcal{R}$ is said to be an *equivalence relation* if $\sim$ is:
  (i) *Reflexive*: $\forall a \in \mathcal{R}, \quad a \sim a$.
  (ii) *Symmetric*: $\forall a, b \in \mathcal{R}, \quad a \sim b \implies b \sim a$.
  (iii) *Transitive*: $\forall a, b, c \in \mathcal{R}, \quad a \sim b \text{ and } b \sim c \implies a \sim c$.

- For $a, b \in \mathcal{R}$ it is said that *$a$ is congruent to $b$ modulo $\mathcal{I}$* if $a - b \in \mathcal{I}$. In this case we write $a \equiv b \mod \mathcal{I}$ if and only if $a - b \in \mathcal{I}$.

**Theorem A.17.** *If $\mathcal{I}$ is an ideal of the ring $\mathcal{R} = (\mathcal{R}, +, \bullet)$, then congruence modulo $\mathcal{I}$ is an equivalence relation.*

***Proof***. Suppose that $\mathcal{I}$ is an ideal of the ring $\mathcal{R} = (\mathcal{R}, +, \bullet)$. We wish to show that $\equiv$ is an equivalence relation.

***Claim:*** *$\equiv$ is reflexive.* Take any $a \in \mathcal{R}$. Since $\mathcal{I}$ is a subring then $a - a = 0 \in \mathcal{I}$ implies that $a \equiv a \mod \mathcal{I}$. So $\equiv$ is reflexive. ☑

***Claim:*** *$\equiv$ is symmetric.* Take $a, b \in \mathcal{R}$ such that $a \equiv b \mod \mathcal{I}$. Then $a - b \in \mathcal{I}$. Since $\mathcal{I}$ is a subring of $\mathcal{R}$, then the additive inverse of $a-b$ is $b-a$ since $(a-b)+(b-a) = 0$. Therefore $b - a \in \mathcal{I}$ implies $b \equiv a \mod \mathcal{I}$. So $\equiv$ is symmetric. ☑

***Claim:*** $\equiv$ *is transitive.* Take $a, b, c \in \mathcal{R}$ such that $a \equiv b \mod \mathcal{I}$ and $b \equiv c \mod \mathcal{I}$. Then

$$\begin{aligned} a - b \in \mathcal{I} \text{ and } b - c \in \mathcal{I} &\implies (a-b) + (b-c) \in \mathcal{I} \\ &\implies a - b + b - c \in \mathcal{I} \\ &\implies a - c \in \mathcal{I} \\ &\implies a \equiv c \mod \mathcal{I}. \end{aligned}$$

So $\equiv$ is transitive. ☑

Consequently $\equiv$ is an equivalence relation. ■

**Theorem A.18.** *Let $\mathcal{I}$ be an ideal of the ring $\mathcal{R} = (\mathcal{R}, +, \bullet)$. If $a \equiv b \mod \mathcal{I}$ and $c \equiv d \mod \mathcal{I}$, then*

*(i)* $a + c \equiv b + d \mod \mathcal{I}$, *and*

*(ii)* $a \bullet c \equiv b \bullet d \mod \mathcal{I}$.

***Proof*.** Suppose that $\mathcal{I}$ is an ideal of the ring $\mathcal{R} = (\mathcal{R}, +, \bullet)$, and that $a \equiv b \mod \mathcal{I}$ and $c \equiv d \mod \mathcal{I}$.

***Claim:*** $a + c \equiv b + d \mod \mathcal{I}$. By hypothesis we obtain

$$\begin{aligned} a - b \in \mathcal{I} \text{ and } c - d \in \mathcal{I} &\implies (a-b) + (c-d) \in \mathcal{I} \\ &\implies a - b + c - d \in \mathcal{I} \\ &\implies a + c - b - d \in \mathcal{I} \\ &\implies (a+c) - (b+d) \in \mathcal{I} \\ &\implies a + c \equiv b + d \mod \mathcal{I}. \text{ ☑} \end{aligned}$$

***Claim:*** $a \bullet c \equiv b \bullet d \mod \mathcal{I}$. By hypothesis we have $a - b \in \mathcal{I}$ and $c - d \in \mathcal{I}$ so we let $x = a - b \in \mathcal{I}$ and $y = c - d \in \mathcal{I}$. Then

$$\begin{aligned} a \bullet c \in \mathcal{I} &\implies (x + b) \bullet (y + d) \in \mathcal{I} \\ &\implies x \bullet y + x \bullet d + b \bullet y + b \bullet d \in \mathcal{I} \\ &\implies b \bullet d \in \mathcal{I} \\ &\implies a \bullet c \equiv b \bullet d \mod \mathcal{I}. \text{ ☑} \end{aligned}$$

So (i) and (ii) are satisfied. ■

**Definition A.19.** Let $\mathcal{I}$ be an ideal of the ring $\mathcal{R} = (\mathcal{R}, +, \bullet)$ The set $[a] = \{x \in \mathcal{R} : a \equiv x\} = a + \mathcal{I}$ is said to be the *equivalence class* of an element $a \in \mathcal{R}$ if $\equiv$ of $\mathcal{R}$ is a congruence relation. If $a \equiv b \mod \mathcal{I}$ we say that $a$ and $b$ are *congruent*, which may equivalently be denoted by $a + \mathcal{I} = b + \mathcal{I}$ or $[a] = [b]$. We write $\mathcal{R}/\mathcal{I}$ to denote the set of all such equivalence classes.

**Theorem A.20.** *If $\mathcal{I}$ is an ideal of the ring $\mathcal{R} = (\mathcal{R}, +, \bullet)$, then $\mathcal{R}/\mathcal{I}$ becomes a ring (called the quotient ring of $\mathcal{R}$ modulo $\mathcal{I}$) under the operations*

$$\begin{aligned}(a + \mathcal{I}) + (b + \mathcal{I}) &= (a + b) + \mathcal{I}\\ (a + \mathcal{I}) \bullet (b + \mathcal{I}) &= (a \bullet b) + \mathcal{I}.\end{aligned}$$

***Proof***. Suppose that $\mathcal{I}$ is an ideal of the ring $\mathcal{R} = (\mathcal{R}, +, \bullet)$. We wish to show that $\mathcal{R}/\mathcal{I}$ is a quotient ring under the said operations.

***Claim:*** *addition is commutative.* Take any $a + \mathcal{I}, b + \mathcal{I} \in \mathcal{R}/\mathcal{I}$. Then

$$(a + \mathcal{I}) + (b + \mathcal{I}) = (a + b) + \mathcal{I} = (b + a) + \mathcal{I} = (b + \mathcal{I}) + (a + \mathcal{I}),$$

so addition is commutative for all $a + \mathcal{I}, b + \mathcal{I} \in \mathcal{R}/\mathcal{I}$. ☑

***Claim:*** *addition is associative.* Take any $a + \mathcal{I}, b + \mathcal{I}, c + \mathcal{I} \in \mathcal{R}/\mathcal{I}$. Then

$$\begin{aligned}((a + \mathcal{I}) + (b + \mathcal{I})) + (c + \mathcal{I}) &= ((a + b) + \mathcal{I}) + (c + \mathcal{I})\\ &= (a + b + \mathcal{I}) + (c + \mathcal{I})\\ &= a + b + c + \mathcal{I}\\ &= (a + \mathcal{I}) + (b + c + \mathcal{I})\\ &= (a + \mathcal{I}) + ((b + c) + \mathcal{I})\\ &= (a + \mathcal{I}) + ((b + \mathcal{I}) + (c + \mathcal{I}),\end{aligned}$$

so for all $a + \mathcal{I}, b + \mathcal{I}, c + \mathcal{I} \in \mathcal{R}/\mathcal{I}$ addition is associative. ☑

***Claim:*** *there exists a unique additive identity $0 + \mathcal{I} \in \mathcal{R}/\mathcal{I}$.* Take any $a + \mathcal{I} \in \mathcal{R}/\mathcal{I}$. Then

$$(a + \mathcal{I}) + (0 + \mathcal{I}) = (a + 0) + \mathcal{I} = a + \mathcal{I},$$

so $0 + \mathcal{I}$ is the additive identity of $\mathcal{R}/\mathcal{I}$ for all $a + \mathcal{I} \in \mathcal{R}/\mathcal{I}$. ☑

***Claim:*** *there exists a unique multiplicative identity* $1+\mathcal{I} \in \mathcal{R}/\mathcal{I}$*.* Take any $a+\mathcal{I} \in \mathcal{R}/\mathcal{I}$. Then

$$(a+\mathcal{I}) \bullet (1+\mathcal{I}) = (a \bullet 1) + \mathcal{I} = a + \mathcal{I} = (1 \bullet a) + \mathcal{I} = (1+\mathcal{I}) \bullet (a+\mathcal{I}),$$

so $1+\mathcal{I}$ is the multiplicative identity of $\mathcal{R}/\mathcal{I}$ for all $a+\mathcal{I} \in \mathcal{R}/\mathcal{I}$.

***Claim:*** *for each element, there exists an additive inverse.* Let $a+\mathcal{I} \in \mathcal{R}/\mathcal{I}$. Then

$$(a+\mathcal{I}) + (-a+\mathcal{I}) = (a+(-a)) + \mathcal{I} = 0 + \mathcal{I},$$

so for all $a+\mathcal{I} \in \mathcal{R}/\mathcal{I}$ there exists an additive inverse $-a+\mathcal{I}$. ☑

Consequently $\mathcal{R}/\mathcal{I}$ is a quotient ring. ■

**Definition A.21.** An ideal $\mathcal{I}$ of the commutative ring $\mathcal{R} = (\mathcal{R}, +, \bullet)$ is said to be a *principal ideal* if there exists $n \in \mathcal{R}$ such that $\mathcal{I} = \langle n \rangle$; in this case, we say that $\mathcal{I}$ is *generated* by $n$.

**Example A.22.** Let $\mathbb{Z} = (\mathbb{Z}, +, \bullet)$ be the integers and let $\langle n \rangle$ be a principal ideal generated by $n \in \mathbb{Z}$. Then the elements of the quotient ring $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$ are

$$[0] = 0 + \langle n \rangle,\ [1] = 1 + \langle n \rangle,\ [2] = 2 + \langle n \rangle,\ \ldots,\ [n-1] = n-1+\langle n \rangle.$$

**Theorem A.23.** *If* $\langle p \rangle$ *is the principal ideal generated by the prime* $p \in \mathbb{Z}$*, then the quotient ring* $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$ *is a Galois field.*

***Proof***. Suppose $\langle p \rangle$ is the principal ideal generated by the prime $p \in \mathbb{Z}$ for the quotient ring $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$. So we have that $[0] \in \mathbb{Z}_p$ and $[1] \in \mathbb{Z}_p$ are the additive and multiplicative identities of $\mathbb{Z}_p$, respectively. Take any $[a], [b] \in \mathbb{Z}_p$ and consider $[a] \bullet [b] = [a \bullet b]$. Now since $\langle p \rangle$ is the principal ideal generated by $p$, then

$$[0] = [k \bullet p], \quad \text{for } k = 1, 2, 3,\ \ldots\ .$$

Therefore

$$[a \bullet b] = [0] \iff \exists k \in \mathbb{Z},\ a \bullet b = k \bullet p.$$

But since $p$ is prime, then $p$ divides $a \bullet b$ if and only if $p$ divides $a$ or $p$ divides $b$. So either $[a] = [kp]$ or $[b] = [kp]$ for some $k \in \mathcal{Z}$. Hence, $\mathbb{Z}_p$ contains no zero divisor and is thus an integral domain. Consequently since $\mathbb{Z}_p$ is finite, Theorem A.14 implies that the quotient ring $\mathbb{Z}_p = \mathbb{F}_p$ is a Galois field. ■

**Example A.24.** Let $\mathbb{Z} = (\mathbb{Z}, +, \bullet)$ be the integers and let $\langle 3 \rangle$ be a principal ideal generated by the prime $3 \in \mathbb{Z}$. Then the elements of the Galois field $\mathbb{Z}_3 = \mathbb{Z}/\langle 3 \rangle = \mathbb{F}_3$ are

$$\begin{array}{ccccl} [0] & = & 0 + \langle 3 \rangle & = & \{0,\ 3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ \ldots\} \\ [1] & = & 1 + \langle 3 \rangle & = & \{1,\ 4,\ 7,\ 10,\ 13,\ 16,\ 19,\ 22,\ \ldots\} \\ [2] & = & 2 + \langle 3 \rangle & = & \{2,\ 5,\ 8,\ 11,\ 14,\ 17,\ 20,\ 23,\ \ldots\}, \end{array}$$

where $|\mathbb{Z}/\langle 3 \rangle| = 3$. Here, the addition and multiplication operations of $\mathbb{F}_3$ can be expressed by the following respective operation tables.

| + | **[0]** | **[1]** | **[2]** |
|---|---|---|---|
| **[0]** | [0] | [1] | [2] |
| **[1]** | [1] | [2] | [0] |
| **[2]** | [2] | [0] | [1] |

| • | **[0]** | **[1]** | **[2]** |
|---|---|---|---|
| **[0]** | [0] | [0] | [0] |
| **[1]** | [0] | [1] | [2] |
| **[2]** | [0] | [2] | [1] |

**Definition A.25.** Let $\mathcal{R} = (\mathcal{R}, +, \bullet)$ be a ring. If there exists some $n \in \mathbb{Z}$ with $n > 0$ such that $n \bullet r = 0$ for each $r \in \mathcal{R}$, then the least such $n$ is said to be the *characteristic* of $\mathcal{R}$. In this case, $\mathcal{R}$ is said to have (positive) characteristic $n$. If $n$ is a prime power, then $\mathcal{R}$ is said to have *prime characteristic*. Otherwise, if no such $n > 0$ exists, then $\mathcal{R}$ is said to have characteristic O.

**Theorem A.26.** *If $\mathcal{R} = (\mathcal{R}, +, \bullet) \neq \emptyset$ is an integral domain with characteristic $p \in \mathbb{Z}$, then $p$ must be prime.*

***Proof.*** Suppose that $\mathcal{R} = (\mathcal{R}, +, \bullet) \neq \emptyset$ is an integral domain with characteristic $p \in \mathbb{Z}$. Then we have the identities $0, 1 \in \mathcal{R}$ so $p \geq 2$, where $p \bullet r = 0$ for all $r \in \mathcal{R}$. Now suppose, towards contradiction, that $p$ is not prime. Then there exists some $a, b \in \mathbb{Z}$ where $1 < a, b < p$ such that for all $r \in \mathcal{R}$ we have

$$\begin{aligned} p = a \bullet b \implies \quad p \bullet r &= (a \bullet b) \bullet r = 0 \\ \implies \quad p \bullet 1 &= (a \bullet b) \bullet 1 = a \bullet 1 \bullet b \bullet 1 = (a \bullet 1) \bullet (b \bullet 1) = 0. \end{aligned} \tag{A.1}$$

Now since $\mathcal{R}$ is an integral domain, then it has no zero divisors. Therefore (A.1) implies that either

$$a \bullet r = 0 \implies a \bullet r = (a \bullet 1) \bullet r = 0 \text{ or } b \bullet r = 0 \implies b \bullet r = (b \bullet 1) \bullet r = 0, \ \forall r \in \mathcal{R}.$$

But $1 < a, b < p$ and (by definition of the characteristic) $p$ is the least such integer such that $p \bullet r = 0$ for all $r \in \mathcal{R}$—a contradiction. Consequently $p$ must be prime. ■

**Theorem A.27.** *If $\mathbb{F}_n$ is a Galois field, then $\mathbb{F}_n$ has prime characteristic $p$.*

***Proof.*** Let $\mathbb{F}_n$ be a Galois field. Consider the multiples of the identity

$$1, \ 1 \bullet (1+1) = 1 \bullet 2, \ 1 \bullet (1+1+1) = 1 \bullet 3, \ 1 \bullet (1+1+1+1) = 1 \bullet 4, \ \ldots \ .$$

Now since $\mathbb{F}_n$ contains only a finite number of distinct elements then there exist $a, b \in \mathcal{Z}$ such that $1 \leq a < b$ where

$$a \bullet 1 = b \bullet 1 \implies a \bullet 1 - b \bullet 1 = 0 \implies (a - b) \bullet 1 = 0 \implies (a - b) \bullet c = 0, \ \forall c \in \mathbb{F}_n.$$

So $\mathbb{F}_n$ has a positive characteristic which we denote as $p$. Now since $\mathbb{F}_n$ is an integral domain with characteristic $p > 0$, then $p$ must be prime by Theorem A.26; so $\mathbb{F}_n$ has prime characteristic $p$. ■

**Definition A.28.** Let $\mathbb{F}$ be a field. A *vector space* $\mathcal{K} = (\mathcal{K}, +, \bullet)$ is an abelian group equipped with *scalar multiplication*, denoted by $a \bullet \vec{u}$ for all $a \in \mathbb{F}$ and for all $\vec{u} \in \mathcal{K}$, where the following axioms hold for all $a, b \in \mathbb{F}$ and for all $\vec{u}, \vec{v} \in \mathcal{K}$:

(i) $a \bullet (b \bullet \vec{u}) = (a \bullet b) \bullet \vec{u}$,

(ii) $(a+b) \bullet \vec{u} = a \bullet \vec{u} + b \bullet \vec{u}$,

(iii) $a \bullet (\vec{u} + \vec{v}) = a \bullet \vec{u} + a \bullet \vec{v}$, and

(iv) $1 \bullet \vec{u} = \vec{u}$,

In this case, $\mathcal{K}$ is said to be a vector space over $\mathbb{F}$.

**Definition A.29.** Let $\mathbb{F}$ and $\mathbb{K}$ be fields. If $\mathbb{F} \subset \mathbb{K}$, then $\mathbb{F}$ is said to be a *subfield* of $\mathbb{K}$ and (equivalently) $\mathbb{K}$ is said to be an *extension field* of $\mathbb{F}$. If $\mathbb{F} \neq \mathbb{K}$, then $\mathbb{F}$ is said to be a *proper* subfield of $\mathbb{K}$.

**Theorem A.30.** *Let* $\mathbb{F}$ *and* $\mathbb{K}$ *be fields where* $\mathbb{F} \subset \mathbb{K}$. *If we define the scalar multiplication as*

$$\mathbb{F} \times \mathbb{K} \to \mathbb{K} \ : \ (a, \vec{u}) \mapsto a \bullet \vec{u}, \quad \forall a \in \mathbb{F}, \quad \forall \vec{u} \in \mathbb{K}, \tag{A.2}$$

*then* $\mathbb{K}$ *is a vector space over* $\mathbb{F}$.

***Proof***. Suppose that $\mathbb{F}$ and $\mathbb{K}$ are fields where $\mathbb{F} \subset \mathbb{K}$. Define the scalar multiplication as given by (A.2). We wish to show that vector space properties of Definition A.28 are satisfied.

***Claim:*** $\mathbb{K} = (\mathbb{K}, +, \bullet)$ *is an abelian group.* Since $\mathbb{K}$ is a field, then the elements of $\mathbb{K}$ form an abelian group under $+$. Next, take any "vector" $\vec{u} \in \mathbb{K}$ and any "scalar" $a \in \mathbb{F}$. Now since $\mathbb{F} \subset \mathbb{K}$, then any scalar multiplication $(a, \vec{u}) \mapsto a \bullet \vec{u} \in \mathbb{K}$ is just multiplication in $\mathbb{K}$. ☑

***Claim:*** *the vector space axioms (i)—(iv) of Definition A.28 hold for all* $a, b \in \mathbb{F}$ *and for all* $\vec{u}, \vec{v} \in \mathbb{K}$. Since $\mathbb{K}$ is an extension field of $\mathbb{F}$, then by the field axioms it immediately follows that for all $a, b \in \mathbb{F}$ and for all $\vec{u}, \vec{v} \in \mathbb{K}$:

(i) $a \bullet (b \bullet \vec{u}) = (a \bullet b) \bullet \vec{u}$.

(ii) $(a+b) \bullet \vec{u} = a \bullet \vec{u} + b \bullet \vec{u}$.

(iii) $a \bullet (\vec{u} + \vec{v}) = a \bullet \vec{u} + a \bullet \vec{v}$.

(iv) $1 \bullet \vec{u} = \vec{u}$. ☑

Consequently, $\mathbb{K}$ is a vector space over $\mathbb{F}$. ■

**Definition A.31.** Let $\mathbb{K}$ be a vector space over a field $\mathbb{F}$. Let $\mathcal{B}_{\mathbb{K}} = \{\vec{v}_0,\ \vec{v}_1,\ \vec{v}_2,\ \ldots, \vec{v}_{d-1}\}$ be a finite subset of $\mathbb{K}$. Then $\mathcal{B}_{\mathbb{K}}$ is said to be a *basis* if the following conditions hold:

(i) The *linear independence* property:

$$\forall a_i \in \mathbb{F},\ a_0 \bullet \vec{v}_0 + a_1 \bullet \vec{v}_1 + \cdots + a_{d-1} \bullet \vec{v}_{d-1} \implies a_0 = a_1 = \cdots = a_{d-1} = 0.$$

(ii) The *spanning* property:

$$\forall \vec{u} \in \mathbb{K},\ \exists! a_0, a_1, \ldots, a_{d-1} \in \mathbb{F},\ \vec{u} = a_0 \bullet \vec{v}_0 + a_1 \bullet \vec{v}_1 + \cdots + a_{d-1} \bullet \vec{v}_{d-1}.$$

The numbers $a_i \in \mathbb{F}$ for $i = 0,\ 1,\ \ldots,\ d-1$ are said to be the *coordinates* of the vector $\vec{u}$ with respect to the basis $\mathcal{B}_{\mathbb{K}}$, which we may write in coordinate form as $(a_0, a_1, \ldots, a_{d-1}) \in \mathbb{F}^d$, where $d = [\mathbb{K} : \mathbb{F}]$ is said to be the *dimension* of $\mathbb{K}$ over $\mathbb{F}$ and (equivalently) the *degree* of extension. If $d$ is a finite, then $\mathbb{K}$ is said to be *finite dimensional* vector space over $\mathbb{F}$ and $d$ is said to be a *finite extension.*

**Lemma A.32.** *Let $\mathbb{F}_q$ be a Galois field (with $|\mathbb{F}_q| = q$ elements) and let the Galois field $\mathbb{K}$ be a vector space over $\mathbb{F}_q$. Then $\mathbb{K} = \mathbb{K}_{q^d}$ (with $|\mathbb{K}_{q^d}| = q^d$ elements) where $d = [\mathbb{K}_{q^d} : \mathbb{F}_q]$.*

***Proof.*** Suppose that the Galois field $\mathbb{K}$ is a vector space over $\mathbb{F}_q$. Then there exists a basis $\mathcal{B}_{\mathbb{K}}$ of $\mathbb{K}$. Since $\mathbb{F}_q$ has a finite number of elements, then $\mathbb{K}$ is a finite dimensional vector space over $\mathbb{F}_q$; let's denote this by $d = [\mathbb{K} : \mathbb{F}_q]$. Then $\mathcal{B}_{\mathbb{K}}$ has $d$ elements which we denote as $\mathcal{B}_{\mathbb{K}} = \{\vec{v}_0, \vec{v}_1, \vec{v}_2, \ldots, \vec{v}_{n-1}\}$. Next, take any $\vec{u} \in \mathbb{K}$. Then by the spanning property of Definition A.31 it follows that there exists a coordinate $(a_0, a_1, \ldots, a_{d-1}) \in \mathbb{F}_q^d$ such that

$$\vec{u} = a_0 \bullet \vec{v}_0 + a_1 \bullet \vec{v}_1 + a_2 \bullet \vec{v}_2 + \cdots + a_{d-1} \bullet \vec{v}_{d-1}, \ \forall \vec{u} \in \mathbb{K},$$

is unique. Therefore, since each $a_i \in \mathbb{F}_q$ for $i = 0,\ 1,\ 2,\ \ldots,\ d-1$ can be any one of the $q$ possible values of $\mathbb{F}_q$, then $|\mathbb{K}| = d$ so $\mathbb{K} = \mathbb{K}_{q^d}$. ■

**Remark A.33.** Now that we've established that a Galois field $\mathbb{K}$ is a vector space over its subfield $\mathbb{F}$, from this point forward we will omit the finite field vector notation (ex. $\vec{v}_i \in \mathbb{K}$) for the sake of consistency and conciseness.

**Definition A.34.** Let $\mathcal{F} = (\mathcal{F}, +, \bullet)$ and $\mathcal{K} = (\mathcal{K}, \oplus, \otimes)$ be rings with multiplicative identities denoted by $1_{\mathcal{F}} \in \mathcal{F}$ and $1_{\mathcal{K}} \in \mathcal{K}$, respectively. Then a function $\alpha : \mathcal{F} \to \mathcal{K}$ is said to be a *ring homomorphism* if the following operator morphism properties hold under $\alpha$:

(i) *Addition*: $\alpha(a + b) = \alpha(a) \oplus \alpha(b), \quad \forall a, b \in \mathcal{F}$.

(ii) *Multiplication*: $\alpha(a \bullet b) = \alpha(a) \otimes \alpha(b), \quad \forall a, b \in \mathcal{F}$.

(iii) *Multiplicative Identity*: $\alpha(1_{\mathcal{F}}) = 1_{\mathcal{K}}$.

If $\mathcal{F} = \mathbb{F}$ and $\mathcal{K} = \mathbb{K}$ are both fields, then $\alpha$ is said to be a *field homomorphism.*

**Definition A.35.** Let $\mathcal{F}$ and $\mathcal{K}$ be sets. The function $\alpha : \mathcal{F} \to \mathcal{K}$ is a *bijective* function if and only if $\alpha$ is:

(i) *Injective*: $\alpha(a) = \alpha(b) \implies a = b$.

(ii) *Surjective*: $\forall b \in \mathcal{K}, \quad \exists a \in \mathcal{F}, \quad \alpha(a) = b$.

In this case $\alpha$ is said to be a *bijection.*

**Definition A.36.** Let $\mathcal{F}$ and $\mathcal{K}$ be rings. Then a ring homomorphism $\alpha : \mathcal{F} \to \mathcal{K}$ is said to be a *ring isomorphism* if and only if it is bijective. In this case $\mathcal{F}$ and $\mathcal{K}$ are said to be *isomorphic*, which is denoted by $\mathcal{F} \cong \mathcal{K}$. If $\mathcal{F} = \mathbb{F}$ and $\mathcal{K} = \mathbb{K}$ are both fields, then $\alpha$ is said to be a *field isomorphism*.

**Definition A.37.** A field $\mathbb{F}$ is said to be a *prime field* if it does not contain any proper subfields.

**Theorem A.38.** *If $\mathbb{K}$ is a field and $\mathbb{F}$ is the prime subfield of $\mathbb{K}$, then:*

*(i)* $\mathbb{F} \cong \mathbb{Q}$ *if $\mathbb{K}$ has characteristic 0.*

*(ii)* $\mathbb{F} \cong \mathbb{F}_p$ *if $\mathbb{K}$ has prime characteristic $p$.*

***Proof***. Suppose that $\mathbb{K}$ is a field and $\mathbb{F}$ is the prime subfield of $\mathbb{K}$. Denote $0_{\mathbb{K}}, 1_{\mathbb{K}} \in \mathbb{K}$ as the additive and multiplicative identities of $\mathbb{K}$, respectively. We will consider the following two cases.

***Case 1:*** *$\mathbb{K}$ has characteristic 0.* First, consider the distinct list of elements

$$0 \bullet 1_{\mathbb{K}},\ 1 \bullet 1_{\mathbb{K}},\ 2 \bullet 1_{\mathbb{K}},\ \ldots,\ n \bullet 1_{\mathbb{K}},\ \ldots,\ \forall n \in \mathbb{Z},$$

for which we define the subring

$$\mathcal{S} = \{n \bullet 1_{\mathbb{K}} : n \in \mathbb{Z}\}$$

of $\mathbb{K}$. Then we define the ring homomorphism $\alpha : \mathcal{S} \to \mathbb{Z}$ and see that

$$\alpha(a +_{\mathcal{S}} b) = \alpha(a) +_{\mathbb{Z}} \alpha(b) \ \text{ and } \ \alpha(a \bullet_{\mathcal{S}} b) = \alpha(a) \bullet_{\mathbb{Z}} \alpha(b),\ \forall a, b \in \mathcal{S},$$

immediately follows; so $\alpha$ is an isomorphism and $\mathcal{S} \cong \mathbb{Z}$. Second, consider the distinct list of elements

$$0 \bullet 1_{\mathbb{K}},\ \frac{1 \bullet 1_{\mathbb{K}}}{1 \bullet 1_{\mathbb{K}}},\ \frac{1 \bullet 1_{\mathbb{K}}}{2 \bullet 1_{\mathbb{K}}},\ \ldots,\ \frac{2 \bullet 1_{\mathbb{K}}}{1 \bullet 1_{\mathbb{K}}},\ \frac{3 \bullet 1_{\mathbb{K}}}{1 \bullet 1_{\mathbb{K}}},\ \ldots,\ \frac{m \bullet 1_{\mathbb{K}}}{n \bullet 1_{\mathbb{K}}},\ \ldots,\ \forall m, n \in \mathbb{Z},\ n \neq 0,$$

for which we define the subfield

$$\mathbb{T} = \left\{ \frac{m \bullet 1_{\mathbb{K}}}{n \bullet 1_{\mathbb{K}}} : m, n \in \mathbb{Z},\ n \neq 0 \right\} \tag{A.3}$$

of $\mathbb{K}$. Then we define the field homomorphism $\beta : \mathbb{T} \to \mathbb{Q}$ and see that

$$\beta(a +_{\mathbb{T}} b) = \beta(a) +_{\mathbb{Q}} \beta(b) \ \text{ and } \ \beta(a \bullet_{\mathbb{T}} b) = \beta(a) \bullet_{\mathbb{Q}} \beta(b), \ \forall a, b \in \mathbb{T},$$

immediately follows; so $\beta$ is an isomorphism and $\mathbb{T} \cong \mathbb{Q}$. Now since any subfield of $\mathbb{K}$ must contain the identities $0_{\mathbb{K}}, 1_{\mathbb{K}} \in \mathbb{K}$, then $0_{\mathbb{K}}, 1_{\mathbb{K}} \in \mathbb{T}$. So

$$\mathbb{T} \subset \mathbb{F} \ \text{ and } \ \mathbb{T} \subset \mathbb{K} \implies \mathbb{T} = \mathbb{F},$$

where $\mathbb{T} = \mathbb{F}$ is the prime subfield of $\mathbb{K}$. Consequently $\mathbb{T} = \mathbb{F} \cong \mathbb{Q}$. ☑

***Case 2:*** *$\mathbb{K}$ has prime characteristic $p$.* Then we apply a similar argument to the previous case where instead of (A.3) we define the subfield

$$\mathbb{T} = \{0 \bullet 1_{\mathbb{K}}, \ 1 \bullet 1_{\mathbb{K}}, \ 2 \bullet 1_{\mathbb{K}}, \ \ldots, \ (p-1) \bullet 1_{\mathbb{K}}\}$$

to obtain $\mathbb{T} \cong \mathbb{F}_p$, where $\mathbb{F}_p$ is the prime subfield of $\mathbb{K}$ which both have prime characteristic $p$. ☑

■

**Theorem A.39.** *If $\mathbb{F}_n$ is a Galois field and $\mathbb{F}_q$ is the prime subfield of $\mathbb{F}_n$, then $n = p^d$ where $p$ is the characteristic of $\mathbb{F}_n$ and $d = [\mathbb{F}_n : \mathbb{F}_q]$.*

***Proof*.** Suppose that $\mathbb{F}_n$ is a Galois field with the prime subfield $\mathbb{F}_q$. Since the order of $\mathbb{F}_n$ is finite with $n = q^m$ for some $m > 0$, then $\mathbb{F}_n$ must have prime characteristic $p$ by Theorem A.27. Therefore, $\mathbb{F}_q \cong \mathbb{F}_p$ by Theorem A.38, so $|\mathbb{F}_q| = p$. Hence, $n = q^m = p^d$ with $m = d = [\mathbb{F}_n : \mathbb{F}_q]$ by Lemma A.32. ■

**Remark A.40.** Let $\mathcal{R} = (\mathcal{R}, +, \bullet)$ be a ring. For the sake of conciseness, from this point forward we may denote the multiplication $a \bullet b$ as $ab$ for any $a, b \in \mathbb{R}$.

**Definition A.41.** Let $\mathcal{R} = (\mathcal{R}, +, \bullet)$ be ring. Then any expression of the form

$$f(x) = \sum_{i=0}^{n} f_i x^i = f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n,$$

where $f_i \in \mathcal{R}$ and $f_n \neq 0$, is said to be a *polynomial* over $\mathcal{R}$ with *indeterminant* $x$. For this we say:

(i) The elements $f_0, f_1, f_2, \ldots, f_n$ are the *coefficients* of $f(x)$.

(ii) The coefficient $a_n$ is the *leading coefficient* of $f(x)$.

(iii) $f(x)$ is *monic* if $f_n = 1$.

(iv) The *degree* of $f(x)$ is $n$ and write $\deg f(x) = n$ if $n$ is the largest nonnegative number for which $f_n \neq 0$. If no such $n$ exists, then we have $f(x) = 0$, which is the *zero polynomial.*

(v) $f(x)$ is a *constant polynomial* if $f(x) = a_0$ for all $x \in \mathbb{R}$ with constant $f_0 \in \mathcal{R}$.

**Definition A.42.** Let $\mathcal{R} = (\mathcal{R}, +, \bullet)$ be a ring. Then the ring formed by all of the polynomials over $\mathcal{R}$ is denoted by $\mathcal{R}[x] = (\mathcal{R}[x], +, \bullet)$ and is said to be the *polynomial ring* over $\mathcal{R}$. From this point forward, we'll just write $\mathcal{R}$ or $\mathcal{R}[x]$ to declare such rings unless it is necessary to distinguish between the operations.

As it turns out, certain useful properties of $\mathcal{R}$ can be inherited by $\mathcal{R}[x]$.

**Theorem A.43.** *Let $\mathcal{R}$ be a ring. Then:*

*(i) $\mathcal{R}[x]$ is commutative if and only if $\mathcal{R}$ is commutative.*

*(ii) $\mathcal{R}[x]$ has an identity if and only if $\mathcal{R}$ is has an identity.*

*(iii) $\mathcal{R}[x]$ is an integral domain if and only if $\mathcal{R}$ is an integral domain.*

**Theorem A.44 (Division Algorithm).** *Let $\mathbb{F}$ be a field and let $f(x), g(x) \in \mathbb{F}[x]$ with $f(x), g(x) \neq 0$ where $g(x)$ is nonconstant polynomials. Then there exist the unique polynomials $q(x), r(x) \in \mathbb{F}[x]$ such that*

$$f(x) = g(x)q(x) + r(x),$$

*where either $\deg r(x) < \deg g(x)$ or $r(x) = 0$.*

The division algorithm formalizes the long division of polynomials.

**Definition A.45.** Let $\mathbb{F}$ be a field and take $f(x) \in \mathbb{F}[x]$. $a \in \mathbb{F}$ is said to be a *root* of $f(x)$ if $f(a) = 0$.

**Theorem A.46.** *Let $\mathbb{F}$ be a field. An element $a \in \mathbb{F}$ is a root of $f(x) \in \mathbb{F}[x]$ if and only if $x - a$ is a factor of $f(x)$ in $\mathbb{F}[x]$*

***Proof***. Let $\mathbb{F}$ be a field and take any $f(x) \in \mathbb{F}[x]$.

($\Longrightarrow$) Take $a \in \mathbb{F}$ and suppose that $a$ is a root of $f(x)$. Then $f(a) = 0$ and by the division algorithm of Theorem A.44 there exist $g(x), r(x) \in \mathbb{F}[x]$ such that

$$f(x) = (x - a) \bullet g(x) + r(x),$$

where $\deg r(x) < \deg(x - a) = 1$. Therefore $r(x)$ is a constant polynomial, so let $r(x) = b \in \mathbb{F}$. Then $f(x) = (x - a) \bullet g(x) + b$ and $f(a) = 0$ gives

$$\begin{array}{rcl} f(a) & = & (a-a) \bullet g(a) + b \\ & = & 0 \bullet g(a) + b \\ & = & b \\ & = & 0 \end{array} \qquad \Longrightarrow \quad f(x) = (x - a) \bullet g(x).$$

So $x - a$ is a linear factor of $f(x)$.

($\Longleftarrow$) Suppose $(x-a) \in \mathbb{F}[x]$ is a factor of $f(x)$. Then there exists some $g(x) \in \mathbb{F}[x]$ such that

$$f(x) = (x - a) \bullet g(x) \implies 0 = (x - a) \bullet g(x) \implies 0 = x - a.$$

So $f(a) = 0$ and $a \in \mathbb{F}$ is a root of $f(x)$. ■

**Definition A.47.** Let $\mathcal{R}[x]$ be a polynomial ring. Then a polynomial $f(x) \in \mathcal{R}[x]$ is said to be *irreducible over* $\mathcal{R}$ (or equivalently *irreducible in* $\mathcal{R}[x]$) if $\deg f(x) > 0$ and $f(x) = g(x) \bullet h(x)$ with $g(x), h(x) \in \mathcal{R}[x]$ implies that either $g(x)$ or $h(x)$ is constant. Otherwise, if $\deg f(x) > 0$ and $f(x)$ is not irreducible over $\mathcal{R}$, then $f(x)$ is said to be *reducible over* $\mathcal{R}$.

Roughly speaking, irreducible polynomials are the “prime numbers” of polynomial rings. Irreducible polynomials allow us to construct the finite fields of non prime order. The irreducibility or reducibility of a given polynomial largely depends on the ring over which it is defined.

**Theorem A.48.** *Let $\mathbb{F}$ be a field and take $f(x) \in \mathbb{F}[x]$. Then the quotient ring $\mathbb{F}[x]/\langle f(x)\rangle$ is a Galois field if and only if $f(x)$ is irreducible over $\mathbb{F}$.*

**Theorem A.49.** *For any Galois field $\mathbb{F}_{p^d}$ with $p \in \mathbb{Z}$ prime and $d \in \mathbb{Z}$ such that $d > 0$, there exists an irreducible polynomial $f(x) \in \mathbb{F}_{p^d}[x]$ of degree $d$ where $\mathbb{F}_{p^d}/\langle f(x)\rangle$ is a field of order $|\mathbb{F}_{p^d}/\langle f(x)\rangle| = p^d$.*

**Definition A.50.** Let $\mathbb{F}$ be a field and let $f(x) = f_0 + f_1x + \cdots + f_nx^n \in \mathbb{F}[x]$ be a nonconstant polynomial. A vector space $\mathbb{K}$ over $\mathbb{F}$ is said to be a *splitting field* of $f(x)$ if there exist $u_1, u_2, \ldots, u_n \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(u_1, u_2, \ldots, u_n)$ and

$$f(x) = (x - u_1)(x - u_2)\cdots(x - u_n).$$

In this case $f(x) \in \mathbb{F}[x]$ is said to *split* in $\mathbb{K}$ if it is the product of $n$ distinct linear factors in $\mathbb{K}[x]$. In this case, $f(x)$ is said to be *separable* and $\mathbb{K}$ is said to be a *separable extension* of $\mathbb{F}$ if every element in $\mathbb{K}$ is the root of a separable polynomial in $\mathbb{F}[x]$.

**Lemma A.51.** *If $\mathbb{F}_n$ is a Galois field, then $a^n = a$ for any $a \in \mathbb{F}_n$.*

***Proof.*** Let $\mathbb{F}_n$ be a Galois field. Then we consider the following two cases.

- *Case:* $a = 0$. Then we obtain the trivial result $0^n = 0$. ☑
- *Case:* $a \neq 0$. Since $\mathbb{F}_n$ is a field, then $(\mathbb{F}_n \setminus \{0\}, \bullet)$ is a group of order $n - 1$. Therefore, we obtain

$$a^{n-1} = 1 \implies a \bullet a^{n-1} = a \implies a^n = a, \ \forall a \in \mathbb{F}_n \setminus \{0\}. ☑$$

So $a^n = a$ for any $a \in \mathbb{F}_n$. ■

**Lemma A.52.** *If the Galois field $\mathbb{K}_n$ is a vector space over the subfield $\mathbb{F} \subset \mathbb{K}_n$, then the polynomial $f(x) = x^n - x \in \mathbb{F}[x]$ factors in $\mathbb{K}_n[x]$ as*

$$f(x) = x^n - x = \prod_{u_i \in \mathbb{K}} (x - u_i)$$

*and $\mathbb{K}_n$ is a splitting field of $f(x)$ over $\mathbb{F}$.*

***Proof.*** Suppose that the Galois field $\mathbb{K}_n$ is a vector space over the subfield $\mathbb{F} \subset \mathbb{K}_n$. Let $f(x) = x^n - x \in \mathbb{F}[x]$. Since $\deg f(x) = n$, then $f(x)$ has at most $n$ roots in $\mathbb{K}_n$. Now since $|\mathbb{K}_n| = n$, and that Lemma A.51 gives $u^n = u$ for all $u \in \mathbb{K}_n$, then we have $n$ such roots $\{u_0, u_1, \dots, u_{n-1}\} \subset \mathbb{K}_n$ for $f(x)$; that is, $f(u_i) = 0$ for all $u_i \in \mathbb{K}_n$. Therefore, $f(x)$ splits in $\mathbb{K}_n$ and there is no proper subfield of $\mathbb{K}_n$ for which $f(x)$ splits. ■

**Theorem A.53.** *Let $\mathbb{F}_{p^d}$ be a Galois field. Then every subfield $\mathbb{F}_{p^m}$ of $\mathbb{F}_{p^d}$ has $p^m$ elements, where $m \mid d$. Conversely, if $m \mid d$ for $m > 0$, then there exists a unique subfield of $\mathbb{F}_{p^d}$ that is isomorphic to $\mathbb{F}_{p^m}$.*

***Proof.*** Suppose that $\mathbb{F}_{p^d}$ is a Galois field.

($\Longrightarrow$) Let $\mathbb{K}$ be a subfield of $\mathbb{F}_{p^d}$ and let $\mathbb{L}_p$ be isomorphic to $\mathbb{Z}_p$. Then $\mathbb{K} = \mathbb{K}_{p^m}$ must be an $m$-dimensional vector space over $\mathbb{L}_p$ where $m = [\mathbb{K}_{p^m} : \mathbb{L}_p]$ and $|\mathbb{K}_{p^m}| = p^m$. Moreover, $\mathbb{F}_{p^d}$ must be a $d$-dimensional vector space over $\mathbb{L}_p$ where $d = [\mathbb{F}_{p^d} : \mathbb{L}_p]$ and $|\mathbb{K}_{p^d}| = p^d$. Therefore,

$$[\mathbb{F}_{p^d} : \mathbb{L}_p] = [\mathbb{F}_{p^d} : \mathbb{K}_{p^m}] \cdot [\mathbb{K}_{p^m} : \mathbb{L}_p] \implies m \mid d.$$

($\Longleftarrow$) Suppose there exists some $m \in \mathbb{N}$ such that $m \mid d$ and there exists the Galois field $\mathbb{F}_{p^m}$. Then $p^m - 1 \mid p^d - 1$. Hence, there exists $f(x) = x^{p^m - 1} - 1, g(x) = x^{p^d - 1} - 1 \in \mathbb{F}_{p^d}$, where $f(x) \mid g(x)$. So $x \cdot f(x) \mid x \cdot g(x)$, where every root of $x \cdot f(x)$ is a root of $x \cdot g(x)$. Thus, there is a splitting field $\mathbb{K}_{p^m} \subset \mathbb{F}_{p^d}$ of $x \cdot f(x)$, where $\mathbb{K}_{p^m} \cong \mathbb{F}_{p^m}$.

■

**Lemma A.54.** *Let $\mathbb{F}$ be a field and take any $f(x) \in \mathbb{F}[x]$. Then there exists a splitting field $\mathbb{K}$ of $f(x)$ that is unique up to isomorphism.*

**Definition A.55.** Let $\mathbb{F}$ be a field and let $f(x) = f_0 + f_1x + f_2x^2 + \cdots + f_nx^n \in \mathbb{F}[x]$ be a polynomial. Then the polynomial $f'(x)$ is said to be the *derivative* of $f(x)$ if

$$f'(x) = f_1 + f_2x + \cdots + nf_nx^{n-1} \in \mathbb{F}[x].$$

**Lemma A.56.** *Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$ be a polynomial with the derivative $f'(x) \in \mathbb{F}[x]$. Then $a \in \mathbb{F}$ is a multiple root of $f(x) \in \mathbb{F}[x]$ if and only if $a$ is a root of both $f(x)$ and $f'(x)$.*

**Lemma A.57.** *Let $\mathcal{R}$ be a commutative ring with prime characteristic $p$. Then*

$$(a+b)^{p^d} = a^{p^d} + b^{p^d} \quad \text{and} \quad (a-b)^{p^d} = a^{p^d} - b^{p^d},\ \forall a, b \in \mathcal{R},\ \forall d \in \mathbb{Z},\ d > 0.$$

**Theorem A.58.** *If $p^d \in \mathbb{Z}$ is a prime power, then there exists a Galois field $\mathbb{F}_{p^d}$. Any Galois field $\mathbb{F}_{p^d}$ is isomorphic to the splitting field of $f(x) = x^{p^d} - x$ over $\mathbb{F}_p$, where $\mathbb{F}_{p^d}$ that is a vector space over its prime subfield $\mathbb{F}_p$.*

***Proof***. Suppose that $p^d \in \mathbb{Z}$ is a prime power.

***Claim:*** *The Galois field $\mathbb{F}_{p^d}$ exists.* Let $\mathbb{F}_p$ be a Galois field. By Lemma A.51 we let $f(x) = x^{p^d} - x \in \mathbb{F}_p[x]$. By Lemma A.52 we let $\mathbb{K}$ be the splitting field of $f(x)$ over $\mathbb{F}_p$. Now the derivative of $f(x)$ is $f'(x) = p^dx^{p^d-1} - 1 = -1 \in \mathbb{F}_p[x]$, so $f(x)$ has $p^d$ distinct roots $\{u_0, u_1, \ldots, u_{p^d-1}\} \subset \mathbb{K}$. Therefore, by Lemma A.56 $f(x)$ and $f'(x)$ have no roots in common. Now we define $\mathbb{L} = \{u_i \in \mathbb{K} : u_i^{p^d} - u_i = 0\}$, which is a subfield of $\mathbb{K}$ because $0, 1 \in \mathbb{L}, \mathbb{K}$, and by Lemma A.57 we obtain

$$a, b \in \mathbb{L} \implies (a-b)^{p^d} = a^{p^d} - b^{p^d} = a - b \implies a - b \in \mathbb{L},$$

and

$$a, b \in \mathbb{L},\ b \neq 0 \implies (ab^{-1})^{p^d} = a^{p^d} b^{-p^d} = ab^{-1} \implies ab^{-1} \in \mathbb{L}.$$

Thus, for each of $f(x)$'s distinct roots we have $\{u_0, u_1, \ldots, u_{p^d-1}\} \subset \mathbb{L} \subset \mathbb{K}$, which implies that $f(x)$ splits in $\mathbb{L}$. So $|\mathbb{L}| = p^n$ implies that $\mathbb{K} = \mathbb{L}$. Consequently, $\mathbb{L} = \mathbb{F}_{p^d}$ is a Galois field.

***Claim:*** *The Galois field* $\mathbb{F}_{p^d}$ *is unique.* Let $\mathbb{F}_{p^d}$ be a Galois field. Then $\mathbb{F}_{p^d}$ has prime characteristic $p$ by Theorem A.27. So let $\mathbb{F}_p$ be the prime subfield of $\mathbb{F}_{p^d}$. Then $\mathbb{F}_{p^d}$ is a $d$-dimensional vector space over $\mathbb{F}_p$ where $d = [\mathbb{F}_{p^d} : \mathbb{F}_p]$. By Lemma A.51 we let $f(x) = x^{p^d} - x \in \mathbb{F}_p[x]$. Moreover, it follows that $\mathbb{F}_{p^d}$ is a splitting field of $f(x)$ over $\mathbb{F}_p$. Consequently, $\mathbb{F}_{p^d}$ is unique (up to isomorphisms) as given by Lemma A.54. ■

From Theorem A.58 we obtain the following result.

**Corollary A.59.** *If* $\mathbb{F}_{p^d}$ *and* $\mathbb{K}_{p^d}$ *are both Galois fields of order* $|\mathbb{F}_{p^d}| = |\mathbb{K}_{p^d}| = p^d$*, then there exists some isomorphism* $\alpha : \mathbb{F}_{p^d} \to \mathbb{K}_{p^d}$ *such that* $\mathbb{F}_{p^d} \cong \mathbb{K}_{p^d}$*.*

# APPENDIX B

# SOFTWARE

## B.1 Computational Construction of Latin Squares

### B.1.1 Algorithms

The first two algorithms that we present are our latest (and personal best) algorithms for generating subsets of $\mathcal{L}^n$: the NPS-LS-GA of Algorithm 2.1 and the PS-LS-GA of Algorithm 2.2. In terms of algorithmic structure, the PS-LS-GA is nearly identical to the NPS-LS-GA with the exception of a few statements (that are marked with $*$ in Algorithm 2.2). Thereafter, the third Algorithm 2.3 that we present is our SS-LS-GA for generating prime power order-$p^d$ super-symmetric latin squares (and also prime order-$p$ cyclic latin squares if $d = 1$).

**Algorithm 2.1** Non-Preloading Selection-Based Latin Square Generation Algorithm

```
input:
   $n$                                            ▷ Latin square order (integer)
   $limit$                                        ▷ Number of latin squares to generate (integer)
global data:
   $count$                                        ▷ Counter (integer)
   $row$, $col$                                   ▷ Row usage and column usage ($n \times n$ boolean arrays)
   $rowId$, $colId$                               ▷ Row index and column index (integers)
output:
   $L$                                            ▷ Latin square buffer ($n \times n \times n$ integer array)

procedure GENERATESQUARESNONPRELOAD($n$, $limit$)
    ▷ Initialize default values
    $count \leftarrow 0$                          ▷ Set generation counter to zero
    for $i \leftarrow 0, i < n, i \leftarrow (i + 1)$ do     ▷ Set rows and columns to empty
        for $j \leftarrow 0, j < n, j \leftarrow (j + 1)$ do
            $row[i][j] \leftarrow true$
            $col[i][j] \leftarrow true$
        end for
    end for
    ▷ Generate $limit$ latin squares of order-$n$
    GENERATESQUARESNONPRELOADRECURSE($0, 0$)      ▷ Initiate recursion
end procedure

procedure GENERATESQUARESNONPRELOADRECURSE($rowId$, $colId$)
    for $i \leftarrow 0, i < n, i \leftarrow (i + 1)$ do
        ▷ If both row and column not used, then attempt to add next cell
        if $(row[rowId][i] == true)$ and $(col[colId][i] == true)$ then
            $row[rowId][i] \leftarrow false$      ▷ Set current row flag to used
            $col[colId][i] \leftarrow false$      ▷ Set current column flag to used
            $L[rowId][colId] \leftarrow i$        ▷ Set cell's symbol as $i$
            if $(rowId == colId)$ and $(colId == (n - 1))$ then     ▷ If adding the final cell to square
                if CHECKLATINSQUAREPROPERTY($L$) $== true$ then     ▷ If the latin square property holds
                    PRINT($L$)                    ▷ Output to command terminal
                    $count \leftarrow (count + 1)$    ▷ Increment counter
                    if $(limit \neq 0)$ and $(count == limit)$ then     ▷ If $limit$ number of latin squares are generated
                        terminateProcess          ▷ Terminate system generation process
                    end if
                end if
            else if $colId == (n - 1)$ then       ▷ If finished generating current row and still more to do
                GENERATESQUARESNONPRELOADRECURSE($rowId + 1, 0$)     ▷ Begin generating next row
            else                                  ▷ If still generating current row
                GENERATESQUARESNONPRELOADRECURSE($rowId, colId + 1$)     ▷ Go to next column
            end if
            $row[colId][i] \leftarrow true$       ▷ Reset row flag to unused
            $col[colId][i] \leftarrow true$       ▷ Reset column flag to unused
        end if
    end for
end procedure
```

**Algorithm 2.2** Preloading Selection-Based Latin Square Generation Algorithm

```
input:
  $n$                                          ▷ Latin square order (integer)
  $limit$                                      ▷ Number of latin squares to generate (integer)
global data:
  $count$                                      ▷ Counter (integer)
  $row$, $col$                                 ▷ Row usage and column usage ($n \times n$ boolean arrays)
  $rowId$, $colId$                             ▷ Row index and column index (integers)
  $preLoad$                                    ▷ *Preload switch (boolean)*
output:
  $L$                                          ▷ Latin square buffer ($n \times n \times n$ integer array)

procedure GENERATESQUARESPRELOAD($n$, $limit$)
    ▷ Initialize default values
    $count \leftarrow 0$                       ▷ Set generation counter to zero
    for $i \leftarrow 0, i < n, i \leftarrow (i + 1)$ do     ▷ Set rows and columns to empty
        for $j \leftarrow 0, j < n, j \leftarrow (j + 1)$ do
            $row[i][j] \leftarrow true$
            $col[i][j] \leftarrow true$
        end for
    end for
    $preLoad \leftarrow true$                  ▷ *Set preloading mode*
    ▷ Generate $limit$ latin squares of order-$n$
    GENERATESQUARESPRELOADRECURSE$(0, 0)$      ▷ Initiate recursion
end procedure

procedure GENERATESQUARESPRELOADRECURSE($rowId$, $colId$)
    for $i \leftarrow 0, i < n, i \leftarrow (i + 1)$ do
        if $preLoad == true$ then              ▷ If in preloading mode
            $i \leftarrow ((rowId + colId)\%n)$     ▷ *Preload symbol*
        end if
        ▷ If both row and column not used, then attempt to add next cell
        if $(row[rowId][i] == true)$ and $(col[colId][i] == true)$ then
            $row[rowId][i] \leftarrow false$    ▷ Set current row flag to used
            $col[colId][i] \leftarrow false$    ▷ Set current column flag to used
            $L[rowId][colId] \leftarrow i$      ▷ Set cell's symbol as $i$
            if $(rowId == colId)$ and $(colId == (n - 1))$ then     ▷ If adding the final cell to square
                if CHECKLATINSQUAREPROPERTY$(L) == true$ then       ▷ If the latin square property holds
                    if $preLoad == true$ then   ▷ If already preloaded
                        $preLoad \leftarrow false$     ▷ *Clear preloading mode for this instance*
                    end if
                    PRINT$(L)$                  ▷ Output to command terminal
                    $count \leftarrow (count + 1)$     ▷ Increment counter
                    if $(limit \neq 0)$ and $(count == limit)$ then     ▷ If $limit$ number of latin squares are generated
                        terminateProcess        ▷ Terminate system generation process
                    end if
                end if
            else if $colId == (n - 1)$ then     ▷ If finished generating current row and still more to do
                GENERATESQUARESPRELOADRECURSE$(rowId + 1, 0)$     ▷ Begin generating next row
            else                                ▷ If still generating current row
                GENERATESQUARESPRELOADRECURSE$(rowId, colId + 1)$     ▷ Go to next column
            end if
            $row[colId][i] \leftarrow true$     ▷ Reset row flag to unused
            $col[colId][i] \leftarrow true$     ▷ Reset column flag to unused
        end if
    end for
end procedure
```

**Algorithm 2.3** Super-Symmetric Latin Square Generation Algorithm

```
input:
    $p$                                                    ▷ Prime base
    $d$                                                    ▷ Exponent
output:
    $superL$                                               ▷ Latin square buffer ($p^d \times p^d \times p^d$ integer array)

▷ Generates and returns a super-symmetric latin square given a prime power order
procedure generateSuperSymmetricSquare($p$, $d$)
    if $d < 1$ then                                        ▷ If invalid prime power
        return null                                        ▷ Then return null
    end if
    $superL \leftarrow$ generateCyclicBaseSquare($p$)      ▷ Latin square buffer ($p^d \times p^d \times p^d$ integer array)
    if $d == 1$ then                                       ▷ If prime power is just one
        return $superL$                                    ▷ Then return prime order-$p$ cyclic latin square
    end if
    ▷ Generate by lifting the super-symmetric square for each power
    $order \leftarrow p$
    for $i \leftarrow 1, i < d, i \leftarrow (i + 1)$ do   ▷ Set rows and columns to empty
        $order \leftarrow (order \times p)$
        $superL \leftarrow$ liftSquare($superL, order, p$)
    end for
    return $superL$                                        ▷ Return prime power order-$p^d$ super-symmetric latin square
end procedure

▷ Generates and returns an order-$p$ cyclic latin square in reduced form
procedure generateCyclicBaseSquare($p$)
    ▷ Set the symbols of the prime order-$p$ cyclic latin square
    for $i \leftarrow 0, i < p, i \leftarrow (i + 1)$ do
        for $j \leftarrow 0, j < p, i \leftarrow (j + 1)$ do
            $B[i][j] \leftarrow (i + j) \mod p$
        end for
    end for
    return $B$                                             ▷ Return prime order-$p$ cyclic latin square
end procedure

▷ Generates and returns a lifted super-symmetric square built with a $p \times p$ latin sub-square grid
procedure liftSquare($L, orderL, p$)
    ▷ Set each latin sub-square in the $p \times p$ grid
    for $i \leftarrow 0, i < p, i \leftarrow (i + 1)$ do
        for $j \leftarrow 0, j < p, i \leftarrow (j + 1)$ do
            $liftedL \leftarrow$ insertSubsquare($i, j, (i + j) \mod p, L, orderL$)
        end for
    end for
    return $liftedL$                                       ▷ Return the lifted super-symmetric square
end procedure

▷ Inserts a latin sub-square into a super-symmetric latin square
procedure insertSubSquare($row, col, offSym, L, orderL$)
    $i \leftarrow row \times orderL$                       ▷ Set starting row for sub-square insertion
    $j \leftarrow col \times orderL$                       ▷ Set starting column for sub-square insertion
    ▷ Insert the latin sub-square into the grid of the lifted square
    for $i \leftarrow 0, i < ((row + 1) \times orderL), i \leftarrow (i + 1)$ do
        for $j \leftarrow 0, j < ((col + 1) \times orderL), j \leftarrow (j + 1)$ do
            $liftedL[i][j] \leftarrow (L[i \mod orderL][j \mod orderL] + (offSym \times orderL))$
        end for
    end for
    return $liftedL$                                       ▷ Return the super-symmetric square with inserted sub-square
end procedure
```

### B.1.2 Implementation and Usage

#### NPS-LS-GA

We implemented the NPS-LS-GA of Algorithm 2.1 in the Java programming language, which is available at https://sourceforge.net/projects/latin-square-toolbox/. Some of the NPS-LS-GA implementation's key features are:

- Theoretically capable of generating the complete $\mathcal{L}^n$ without skipping any latin squares.
- Practically capable of generating subsets of $\mathcal{L}^n$ up to order-21 on a laptop computer (with an Intel® Core™ M-5Y71 1.2 GHz Processor and 8 GB DDR3L SD-RAM).
- Practically capable of generating approximately 607 order-21 latin squares per second on a laptop computer.
- Practically capable of generating the complete $\mathcal{L}^n$ up to order-5 on a laptop computer.

**Example B.1.** One can generate a data set of 100,000 order-5 latin squares via the Unix command-line as follows:

```
[nathan@icebox ~]$ java LS_Generator_Selection 5 100000
(0,0,0)(0,1,1)(0,2,2)(0,3,3)(0,4,4)
(1,0,1)(1,1,0)(1,2,3)(1,3,4)(1,4,2)
(2,0,2)(2,1,3)(2,2,4)(2,3,0)(2,4,1)
(3,0,3)(3,1,4)(3,2,1)(3,3,2)(3,4,0)
(4,0,4)(4,1,2)(4,2,0)(4,3,1)(4,4,3)
...
[outputs order-5 latin squares until the job is complete or the user presses control-c]
```

If the user does not specify the size of the data set, then the NPS-LS-GA implementation will begin to generate the complete $\mathcal{L}^n$.

### PS-LS-GA

We implemented the PS-LS-GA of Algorithm 2.2 in the Java programming language. Some of the PS-LS-GA implementation's key features are:

- Theoretically capable of generating proper subsets of $\mathcal{L}^n$ because it skips some latin squares.

- Practically capable of generating proper subsets of $\mathcal{L}^n$ up to at least order-30 on a laptop computer (with an Intel® Core™ M-5Y71 1.2 GHz Processor and 8 GB DDR3L SD-RAM).

- Practically capable of generating approximately 2,801 order-21 latin squares per second on a laptop computer (approximately 4.6 times faster than the NPS-LS-GA).

**Example B.2.** One can generate a data set of 100,000 order-5 latin squares via the Unix command-line as follows:

```
[nathan@icebox ~]$ java LS_Generator_Selection_Preload 5 100000
(0,0,0)(0,1,1)(0,2,2)(0,3,3)(0,4,4)
(1,0,1)(1,1,0)(1,2,3)(1,3,4)(1,4,2)
(2,0,2)(2,1,3)(2,2,4)(2,3,0)(2,4,1)
(3,0,3)(3,1,4)(3,2,1)(3,3,2)(3,4,0)
(4,0,4)(4,1,2)(4,2,0)(4,3,1)(4,4,3)
...
[outputs order-5 latin squares until the job is complete or the user presses control-c]
```

### SS-LS-GA

We implemented the SS-LS-GA of Algorithm 2.3 in the Java programming language, which is available at https://sourceforge.net/projects/latin-square-toolbox/. Some of the SS-LS-GA implementation's key features are:

- Capable of generating a prime order-$p$ cyclic latin square.
- Capable of generating a prime power order-$p^d$ super-symmetric latin square.
- Displays the latin square in a "human readable" format.
- Automatically counts and displays the number of transversals.

**Example B.3.** One can generate the prime order-5 cyclic latin square (that encodes the cyclic group $(\mathbb{Z}_5, +)$) via the Unix command-line as follows:

```
[nathan@icebox ~]$ java LS_Generator_Super_Symmetric 5 1
The super symmetric square of 5^1 is
(0,0,0)(0,1,1)(0,2,2)(0,3,3)(0,4,4)
(1,0,1)(1,1,2)(1,2,3)(1,3,4)(1,4,0)
(2,0,2)(2,1,3)(2,2,4)(2,3,0)(2,4,1)
(3,0,3)(3,1,4)(3,2,0)(3,3,1)(3,4,2)
(4,0,4)(4,1,0)(4,2,1)(4,3,2)(4,4,3)
With human readable form of
 0 1 2 3 4
 1 2 3 4 0
 2 3 4 0 1
 3 4 0 1 2
 4 0 1 2 3
The square has 15 transversals
```

**Example B.4.** One can generate the prime power order-$3^2$ cyclic latin square (that encodes the Galois field addition group $(\mathbb{F}_{3^2}, +)$) via the Unix command-line as follows:

```
[nathan@icebox ~]$ java LS_Generator_Super_Symmetric 3 2
The super symmetric square of 3^2 is
(0,0,0)(0,1,1)(0,2,2)(0,3,3)(0,4,4)(0,5,5)(0,6,6)(0,7,7)(0,8,8)
(1,0,1)(1,1,2)(1,2,0)(1,3,4)(1,4,5)(1,5,3)(1,6,7)(1,7,8)(1,8,6)
(2,0,2)(2,1,0)(2,2,1)(2,3,5)(2,4,3)(2,5,4)(2,6,8)(2,7,6)(2,8,7)
(3,0,3)(3,1,4)(3,2,5)(3,3,6)(3,4,7)(3,5,8)(3,6,0)(3,7,1)(3,8,2)
(4,0,4)(4,1,5)(4,2,3)(4,3,7)(4,4,8)(4,5,6)(4,6,1)(4,7,2)(4,8,0)
(5,0,5)(5,1,3)(5,2,4)(5,3,8)(5,4,6)(5,5,7)(5,6,2)(5,7,0)(5,8,1)
(6,0,6)(6,1,7)(6,2,8)(6,3,0)(6,4,1)(6,5,2)(6,6,3)(6,7,4)(6,8,5)
(7,0,7)(7,1,8)(7,2,6)(7,3,1)(7,4,2)(7,5,0)(7,6,4)(7,7,5)(7,8,3)
(8,0,8)(8,1,6)(8,2,7)(8,3,2)(8,4,0)(8,5,1)(8,6,5)(8,7,3)(8,8,4)
With human readable form of
0 1 2 3 4 5 6 7 8
1 2 0 4 5 3 7 8 6
2 0 1 5 3 4 8 6 7
3 4 5 6 7 8 0 1 2
4 5 3 7 8 6 1 2 0
5 3 4 8 6 7 2 0 1
6 7 8 0 1 2 3 4 5
7 8 6 1 2 0 4 5 3
8 6 7 2 0 1 5 3 4
The square has 2241 transversals
```

### B.1.3 Performance Benchmarks

Here we present the performance benchmark comparison results for: the NPS-LS-GA of Algorithm 2.1 versus the PS-LS-GA of Algorithm 2.2.

We conducted two distinct system run-time performance comparison benchmarks for our software implementations of the NPS-LS-GA of the Algorithm 2.1 and the

PS-LS-GA of Algorithm 2.2 for generating sample data sets of latin squares. NPS-LS-GA and PS-LS-GA were both implemented in the Java programming language. The benchmarks were executed on a laptop computer with an Intel® Core™ M-5Y71 1.2 GHz Processor and 8 GB DDR3L SD-RAM equipped with a Linux operating system. Note: as they were generated, all of the latin squares were printed to standard output on the Linux terminal so this would impact overall performance.

For each data set processed, the timing result was obtained via the user-mode of the Linux *time* command and is the average of three runs. For instance, if $k$ is the number of latin squares in a given data set and $t_0, t_1$, and $t_2$ are the number of seconds for the three runs, then the time quantity $t_{avg} = \frac{t_0+t_1+t_2}{3}$ is the average of the three runs and the rate quantity $\frac{k}{t_{avg}}$ is the number of latin squares (whose transversals were counted) per second.

First, we benchmarked the algorithms on generating data sets comprising 100,000 latin squares from order-5 to order-22—see the results in Table B.1.

Consequently, to summarize our generation results of Table B.1, we observed that

1. First, NPS-LS-GA outperforms PS-LS-GA from order-5 to order-14 by a relatively small margin.

2. Second, PS-LS-GA begins to outperform NPS-LS-GA by a relatively small margin (in all but one case) up to order-19.

3. Third, PS-LS-GA begins to outperform NPS-LS-GA by a factor of 2.4 at order-20 and a factor of 4.6 at order-21.

4. Finally, at order-22, NPS-LS-GA appears to hit an “extreme slow down” and was evidently unable to generate the data set in the observed time frame, whereas PS-LS-GA continued to perform up to order-33 and beyond.

**Table B.1: A software performance benchmark comparison for implementations of the NPS-LS-GA and the PS-LS-GA for generating data sets of 100,000 latin squares from order-5 to order-22.**

| # Latin Squares Generated / Second | | | |
|---|---|---|---|
| **Order-$n$** | **NPS-LS-GA** | **PS-LS-GA** | **Winner** |
| 5 | 83 333 | 94 340 | PS-LS-GA |
| 6 | 76 923 | 74 074 | NPS-LS-GA |
| 7 | 62 500 | 64 102 | PS-LS-GA |
| 8 | 52 632 | 47 170 | NPS-LS-GA |
| 9 | 39 215 | 36 765 | NPS-LS-GA |
| 10 | 32 258 | 29 940 | NPS-LS-GA |
| 11 | 23 641 | 23 474 | NPS-LS-GA |
| 12 | 20 284 | 17 986 | NPS-LS-GA |
| 13 | 13 495 | 15 314 | PS-LS-GA |
| 14 | 11 947 | 11 338 | NPS-LS-GA |
| 15 | 8 651 | 9 174 | PS-LS-GA |
| 16 | 7 746 | 7 353 | NPS-LS-GA |
| 17 | 5 241 | 6 211 | PS-LS-GA |
| 18 | 3 559 | 4 975 | PS-LS-GA |
| 19 | 3 725 | 4 132 | PS-LS-GA |
| 20 | 1 390 | 3 367 | PS-LS-GA |
| 21 | 607 | 2 801 | PS-LS-GA |
| 22 | – | 2 351 | PS-LS-GA |

Second, we benchmarked the algorithms on generating data sets comprising of only a *single* latin square from order-5 to order-10—see the results in Table B.2.

Consequently, to summarize our transversal counting results of Table B.2, we observed that

1. First, from order-5 to order-8, NPS-LS-GA and PS-LS-GA are within 0.001 seconds so we call this a “tie”.

2. Second, from order-9 to order-13, PS-LS-GA wins slightly but they are within a relatively small margin (within 0.01 seconds).

3. Third, from order-14 to order-19, PS-LS-GA wins by a larger margin (within 0.1 seconds).
4. Fourth, from order-20 to order-22, PS-LS-GA wins by a relatively significant margin.
5. Finally, at order-23 we stop benchmarking NPS-LS-GA because it takes too long, meanwhile PS-LS-GA continues to generate larger order latin squares with a relatively small increase in time.

**Table B.2: A software performance benchmark comparison for implementations of the NPS-LS-GA and the PS-LS-GA for generating a single latin square from order-5 to order-30.**

| **Single Latin Square Generation Time (# Seconds / Square)** | | | |
|---|---|---|---|
| **Order-$n$** | **NPS-LS-GA** | **PS-LS-GA** | **Winner** |
| 5 | 0.056 | 0.056 | Tie |
| 6 | 0.056 | 0.057 | Tie (within 0.001) |
| 7 | 0.056 | 0.057 | Tie (within 0.001) |
| 8 | 0.056 | 0.057 | Tie (within 0.001) |
| 9 | 0.058 | 0.054 | PS-LS-GA |
| 10 | 0.059 | 0.055 | PS-LS-GA |
| 11 | 0.063 | 0.062 | PS-LS-GA |
| 12 | 0.065 | 0.058 | PS-LS-GA |
| 13 | 0.087 | 0.059 | PS-LS-GA |
| 14 | 0.177 | 0.060 | PS-LS-GA |
| 15 | 1.122 | 0.062 | PS-LS-GA |
| 16 | 0.066 | 0.063 | PS-LS-GA |
| 17 | 0.101 | 0.063 | PS-LS-GA |
| 18 | 0.264 | 0.064 | PS-LS-GA |
| 19 | 0.974 | 0.064 | PS-LS-GA |
| 20 | 34.551 | 0.063 | PS-LS-GA |
| 21 | 114.509 | 0.064 | PS-LS-GA |
| 22 | 3 510.148 | 0.068 | PS-LS-GA |
| 23 | – | 0.069 | PS-LS-GA |
| 24 | – | 0.069 | PS-LS-GA |
| 25 | – | 0.070 | PS-LS-GA |
| 26 | – | 0.067 | PS-LS-GA |
| 27 | – | 0.068 | PS-LS-GA |
| 28 | – | 0.075 | PS-LS-GA |
| 29 | – | 0.069 | PS-LS-GA |
| 30 | – | 0.071 | PS-LS-GA |

# B.2 Computational Enumeration of Latin Square Transversals

## B.2.1 Algorithms

Here we present the three versions of our algorithms for counting the number of transversals in a given latin square.

**Algorithm 2.4** Brute Force Latin Square Transversal Counting Algorithm (Version 1)

```
input:
    $n$                          ▷ Latin square order (integer)
    $L$                          ▷ Latin square buffer ($n \times n \times n$ integer array)
    $d$                          ▷ Number of all possible order-$n$ latin square diagonals: $n$ factorial (integer)
    $D$                          ▷ Set of all possible order-$n$ latin square diagonals ($d \times n$ ordered pair $(row, col)$ array)

global data:
    $count$                      ▷ Counter (integer)
    $symCount$                   ▷ Observed symbol counts ($n$ integer array)
    $n, L, d, D$                 ▷ Note: input set as global

output:
    $count$

▷ Accepts an order-$n$ latin square as input and counts the number of transversals by using brute force to
exhaustively evaluate every possible order-$n$ diagonal to determine if it is a transversal.
procedure countTransversalsV1($n$, $L$, $d$, $D$)
    for $i \leftarrow 0, i < d, i \leftarrow (i+1)$ do              ▷ For every order-$n$ diagonal
        ▷ Reset/clear counter values
        $count \leftarrow 0$                                        ▷ Set transversal counter to zero
        for $j \leftarrow 0, j < n, j \leftarrow (j+1)$ do
            $symCounts[j] \leftarrow 0$                             ▷ Set all symbol counts to zero
        end for
        for $j \leftarrow 0, j < n, j \leftarrow (j+1)$ do          ▷ For every cell in current diagonal
            $rowId \leftarrow D[i][j][0]$                           ▷ Identify current cell's row in ordered pair
            $colId \leftarrow D[i][j][1]$                           ▷ Identify current cell's column in ordered pair
            $symCount[L[rowId][colId]] \leftarrow (symCount[L[rowId][colId]] + 1)$    ▷ Increment symbol count
        end for
        $isTransversal \leftarrow true$                             ▷ Assume current diagonal is a transversal, then look for contradiction
        for $j \leftarrow 0, j < n, j \leftarrow (j+1)$ do          ▷ For every symbol count of current diagonal
            if $symCount[j] \neq 1$ then                            ▷ If current symbol's count is not 1
                $isTransversal \leftarrow false$                    ▷ Then current diagonal is not a transversal
                break                                               ▷ Terminate symbol counting because contradiction found
            end if
        end for
        if $isTransversal == true$ then                             ▷ If current diagonal is a transversal
            $count \leftarrow (count + 1)$                          ▷ Increment transversal count
        end if
    end for
    return $count$                                                  ▷ Return resulting transversal count as output
end procedure
```

**Algorithm 2.5** Subsquare Sequence Latin Square Transversal Counting Algorithm (Version 2)

```
input:
    $n$                                          ▷ Latin square order (integer)
    $L$                                          ▷ Latin square buffer ($n \times n \times n$ integer array)

global data:
    $count$                                      ▷ Counter (integer)
    $states$                                     ▷ Subsquare states ($n \times n \times n \times n$ integer array)
    $statesN$                                    ▷ Subsquare order ($n$ integer array)
    $n, L$                                       ▷ Note: input set as global

output:
    $count$

▷ Accepts an order-$n$ latin square as input and recursively counts the number of transversals.
procedure countTransversalsV2($n$, $L$)
    ▷ Initialize default values
    $count \leftarrow 0$                         ▷ Set transversal counter to zero
    $states[0] \leftarrow L$                     ▷ Set initial subsquare state to be the input latin square
    for $i \leftarrow 0, i < n, i \leftarrow (i + 1)$ do
        $statesN[i] \leftarrow (n - i)$          ▷ Set the descending orders of the subsquare states
    end for
    countTransversalsRecurseV2(0)                ▷ Initiate recursion on subsquare state 0
    return $count$                               ▷ Return resulting transversal count as output
end procedure

▷ Counts transversals by recursively calling itself, where it makes a new subsquare state of descending order if a
  state symbol is found inside its current subsquare state.
procedure countTransversalsRecurseV2($stateId$)
    if $statesN[stateId]\ == 1$ then             ▷ If at final subsquare state with single cell (base case)
        if $state == states[stateId][0][0]$ then ▷ If this final symbol completes a transversal
            $count \leftarrow (count + 1)$       ▷ Then transversal found, so increment count
        end if
        return
    end if
    ▷ Determine if the current subsquare state contains the symbol we're searching for
    for $i \leftarrow 0, i < statesN[stateId], i \leftarrow (i + 1)$ do
        for $j \leftarrow 0, j < statesN[stateId], j \leftarrow (j + 1)$ do
            if $states[stateId][i][j] == stateId$ then            ▷ If symbol is found
                makeSubsquare($i$, $j$, $stateId$)                ▷ Build next (smaller) subsquare state
                countTransversalsRecurseV2($stateId + 1$)         ▷ Recurse on next subsquare state
            end if
        end for
    end for
end procedure

▷ Accepts a row, column, and state (symbol) as input and creates a new subsquare state that does not include
  the row and column in the next state's memory location.
procedure makeSubsquare($rowId$, $colId$, $stateId$)
    ▷ Evaluate every cell in the current subsquare state to see if it's symbol belongs in the next subsquare state
    for $i \leftarrow 0, i < statesN[stateId], i \leftarrow (i + 1)$ do
        for $j \leftarrow 0, j < statesN[stateId], j \leftarrow (j + 1)$ do
            ▷ If the current cell is not in an excluded row or column
            if $((i == rowId)$ or $(j == colId)) == false$ then
                $xTemp \leftarrow i$
                $yTemp \leftarrow j$
                if $i > rowId$ then                               ▷ Enforce row boundary condition
                    $xTemp \leftarrow (xTemp - 1)$
                end if
                if $j > colId$ then                               ▷ Enforce column boundary condition
                    $yTemp \leftarrow (yTemp - 1)$
                end if
                ▷ Then insert the current cell's symbol into the next subsquare state
                $states[stateId + 1][xTemp][yTemp] \leftarrow states[stateId][i][j]$
            end if
        end for
    end for
end procedure
```

**Algorithm 2.6** Boolean Matrix Latin Square Transversal Counting Algorithm (Version 3)

```
input:
    $n$                                                    ▷ Latin square order (integer)
    $L$                                    ▷ Latin square buffer ($n \times n \times n$ integer array)

global data:
    $count$                                                          ▷ Counter (integer)
    $sym$                                   ▷ Symbol observed flags ($n \times n$ boolean array)
    $col$                                   ▷ Column observed flags ($n \times n$ boolean array)
    $n, L$                                                   ▷ Note: input set as global

output:
    $count$

▷ Accepts an order-$n$ latin square as input and recursively counts the number of transversals.
procedure countTransversalsV3($n$, $L$)
    ▷ Initialize default values
    $count \leftarrow 0$                                      ▷ Set transversal counter to zero
    for $i \leftarrow 0, i < n, i \leftarrow (i + 1)$ do
        $sym[i] \leftarrow true$                                ▷ Set all symbols as unobserved
        $col[i] \leftarrow true$                                ▷ Set all columns as unobserved
    end for
    countTransversalsRecurseV3(0)                              ▷ Initiate recursion on row 0
    return $count$                              ▷ Return resulting transversal count as output
end procedure

▷ Counts transversals by recursively calling itself, where it accepts a row as input and looks at global data to see
  which cells in the row are valid to generate a partial transversal that could become a transversal.
procedure countTransversalsRecurseV3($rowId$)
    ▷ For every column in current row, evaluate the cell's symbol
    for $i \leftarrow 0, i < n, i \leftarrow (i + 1)$ do
        ▷ If adding the cell's symbol would create a partial transversal
        if $(sym[L[row][i]] == true)$ and $(col[i] == true)$ then
            $sym[L[row][i]] \leftarrow false$                          ▷ Set symbol as observed
            $col[i] \leftarrow false$                                  ▷ Set column as observed
            if $row == (n - 1)$ then                ▷ If this final symbol completes a transversal
                $count \leftarrow (count + 1)$       ▷ Then transversal found, so increment count
            else
                countTransversalsRecurseV3($rowId + 1$)          ▷ Otherwise, recurse on next row
            end if
            $sym[L[row][i]] \leftarrow true$                     ▷ Reset symbol as unobserved
            $col[i] \leftarrow true$                             ▷ Reset column as unobserved
        end if
    end for
end procedure
```

### B.2.2 Implementation and Usage

**BF-LS-TCAv1**

We implemented the BF-LS-TCAv1 of Algorithm 2.4 in the C programming language. Some of the BF-LS-TCAv1 implementation's key features are:

- Practically capable of counting the number of transversals across latin squares up to order-10 on a laptop computer (with an Intel® Core™ M-5Y71 1.2 GHz Processor and 8 GB DDR3L SD-RAM).
- Uses an iterative brute force approach to exhaustively evaluate every possible order-$n$ diagonal to determine if it is a transversal.
- Requires a file that contains a list of all possible diagonals as input.
- Displays the number of latin squares that have specific counts.
- Displays the minimum, maximum, and average transversal counts.

**Example B.5.** One can count all of the transversals for a data set with 1001 order-5 latin squares via the Unix command-line as follows:

```
[nathan@icebox ~]$ ./LS_Transversal_Counter_v1 ls_order05_1001.txt ls_diag_order05.txt
Computing some stats for 1001 latin squares...
# of latin squares with transversal counts of:
    891 squares with a transversal count of 3
    110 squares with a transversal count of 15
Transversals/square stats:
    Minimum: 3
    Maximum: 15
    Average: 4.3
```

### SS-LS-TCAv2

We implemented the SS-LS-TCAv2 of Algorithm 2.5 in the Java programming language. Some of the SS-LS-TCAv2 implementation's key features are:

- Practically capable of counting the number of transversals across latin squares up to order-17 on a laptop computer (with an Intel® Core™ M-5Y71 1.2 GHz Processor and 8 GB DDR3L SD-RAM).
- Uses a recursive "sub-square" algorithm to count transversals.
- Does not require a file that contains a list of all possible diagonals as input.
- Displays the number of latin squares that have specific counts.
- Displays the heat maps for each latin square.
- Counts the transversals of 63 order-10 latin squares per second (approximately 25.5 faster than the BF-LS-TCAv1 implementation).
- Consumes approximately 18.6% of the RAM that the BF-LS-TCAv1 implementation at counting order-10 latin squares.

**Example B.6.** One can count all of the transversals for a data set with 1001 order-5 latin squares via the Unix command-line as follows:

```
[nathan@icebox ~]$ java LS_Transversal_Counter_v2 ls_order05_1001.txt
1  3  2  0  4
2  4  0  3  1
0  1  3  4  2
3  2  4  1  0
4  0  1  2  3
Heat Map:
3   3   3   3   3
3   3   3   3   3
```

```
3   3   3   3   3
3   3   3   3   3
3   3   3   3   3
Transversal count: 15
...
For a transversal count of 15 there were 110 squares
For a transversal count of 3 there were 891 squares
```

### BM-LS-TCAv3

We implemented the BM-LS-TCAv3 of Algorithm 2.6 in the Java programming language, which is available at https://sourceforge.net/projects/latin-square-toolbox/. Some of the BM-LS-TCAv3 implementation's key features are:

- Practically capable of counting the number of transversals across latin squares up to order-17 on a laptop computer (with an Intel® Core™ M-5Y71 1.2 GHz Processor and 8 GB DDR3L SD-RAM).
- Uses a recursive "boolean matrix" algorithm to count transversals.
- Does not require a file that contains a list of all possible diagonals as input.
- Displays the number of latin squares that have specific counts.
- Displays the heat maps for each latin square.
- Approximately 1.3 times faster than the SS-LS-TCAv2 implementation at counting the transversals of order-16 latin squares.
- Consumes approximately the same amount of the RAM as the SS-LS-TCAv2 implementation (but requires much less memory allocations and deallocations).

The usage of the BM-LS-TCAv3 implementation is identical to the SS-LS-TCAv2 implementation.

### B.2.3 Performance Benchmarks

Here we present the performance benchmark results for the software implementations of the three versions of our latin square transversal enumeration algorithms.

We conducted two distinct system run-time performance comparison benchmarks for our software implementations of the BF-LS-TCAv1 of Algorithm 2.4, the SS-LS-TCAv2 of Algorithm 2.5, and the BM-LS-TCAv3 of Algorithm 2.6 for counting the number of transversals in latin square data sets. BF-LS-TCAv1 was implemented in the C programming language, while SS-LS-TCAv2 and BM-LS-TCAv3 were implemented in the Java programming language. The benchmarks were executed on a laptop computer with an Intel® Core™ M-5Y71 1.2 GHz Processor and 8 GB DDR3L SD-RAM equipped with a Linux operating system.

For each data set processed, the timing result was obtained via the user-mode of the Linux *time* command and is the average of three runs. For instance, if $k$ is the number of latin squares in a given data set and $t_0, t_1$, and $t_2$ are the number of seconds for the three runs, then the time quantity $t_{avg} = \frac{t_0+t_1+t_2}{3}$ is the average of the three runs and the rate quantity $\frac{k}{t_{avg}}$ is the number of latin squares (whose transversals were counted) per second.

First, we benchmarked the algorithms on data sets comprising 100,000 latin squares from order-5 to order-10—see the results in Table B.3. To summarize our transversal counting results of Table B.3, we observed that

1. First, at order-5 BF-LS-TCAv1 outperforms SS-LS-TCAv2 and BM-LS-TCAv3 by a relatively large margin.
2. Second, at order-6 BM-LS-TCAv3 outperforms BF-LS-TCAv1 and SS-LS-TCAv2 but all are within a relatively small margin.

3. Third, from order-7 to order-9 BM-LS-TCAv3 outperforms SS-LS-TCAv2 by a relatively small margin and BF-LS-TCAv1 by a relatively large margin.
4. Finally, at order-10 BF-LS-TCAv1 appears to "hit a wall" and exhibit an extreme slowdown (possibly due to thephysical limitations of the computer such as 8 GB SD-RAM, etc.), meanwhile BM-LS-TCAv3 continued to outperform the others.

**Table B.3: A software performance benchmark comparison for implementations of the BF-LS-TCAv1, the SS-LS-TCAv2, and the BM-LS-TCAv3 for counting the number of transversals of 100,000 latin squares from order-**5 **to order-10.**

| **# Latin Squares (With Transversals Counted) Per Second** | | | | |
|---|---|---|---|---|
| **Order-*n*** | **BF-LS-TCAv1** | **SS-LS-TCAv2** | **BM-LS-TCAv3** | **Winner** |
| 5 | 99 900 | 31 250 | 32 258 | BF-LS-TCAv1 |
| 6 | 19 608 | 22 727 | 23 810 | BM-LS-TCAv3 |
| 7 | 2 061 | 7 463 | 9 217 | BM-LS-TCAv3 |
| 8 | 220 | 1 845 | 2 331 | BM-LS-TCAv3 |
| 9 | 22 | 338 | 419 | BM-LS-TCAv3 |
| 10 | – | 63 | 78 | BM-LS-TCAv3 |

Second, we benchmarked the algorithms on data sets comprising of only a *single* latin square from order-5 to order-16—see the results in Table B.4.

**Table B.4: A software performance benchmark comparison for implementations of the BF-LS-TCAv1, the SS-LS-TCAv2, and the BM-LS-TCAv3 for counting the number of transversals in a single latin square from order-5 to order-16.**

| **Single Latin Square Transversal Counting Time (# Seconds / Square)** | | | | |
|---|---|---|---|---|
| **Order-$n$** | **BF-LS-TCAv1** | **SS-LS-TCAv2** | **BM-LS-TCAv3** | **Winner** |
| 5 | 0.001 | 0.087 | 0.083 | BF-LS-TCAv1 |
| 6 | 0.001 | 0.088 | 0.084 | BF-LS-TCAv1 |
| 7 | 0.005 | 0.090 | 0.088 | BF-LS-TCAv1 |
| 8 | 0.039 | 0.102 | 0.095 | BF-LS-TCAv1 |
| 9 | 0.341 | 0.115 | 0.097 | BM-LS-TCAv3 |
| 10 | 3.749 | 0.147 | 0.107 | BM-LS-TCAv3 |
| 11 | – | 0.208 | 0.158 | BM-LS-TCAv3 |
| 12 | – | 0.612 | 0.453 | BM-LS-TCAv3 |
| 13 | – | 3.238 | 2.393 | BM-LS-TCAv3 |
| 14 | – | 25.914 | 15.658 | BM-LS-TCAv3 |
| 15 | – | 214.123 | 155.719 | BM-LS-TCAv3 |
| 16 | – | 1 744.701 | 1 294.353 | BM-LS-TCAv3 |

# APPENDIX C

# PRIME POWER ORDER CYCLIC AND SUPER-SYMMETRIC LATIN SQUARES

Here we list the cyclic and super-symmetric latin squares of prime power order-$p^d$ for $3 \leq p^d \leq 17$ with $d > 0$ that were generated by our SS-LS-GA of Algorithm 2.3. We also report the corresponding transversal counts and heat maps obtained by our BM-LS-TCAv3 of Algorithm 2.6.

**Table C.1: The prime order-3 cyclic latin square $L^{(\mathbb{Z}_3,+)}$ that encodes the cyclic group $(\mathbb{Z}_3, +)$ (and also the Galois field addition group $(\mathbb{F}_{3^1}, +)$) with a confirmed maximum (and minimum) transversal count $|\mathcal{T}^{L^{(\mathbb{Z}_3,+)}}| = 3 = \mathbb{T}(3) = \mathbb{t}(3)$ [left] and its transversal heat map $\mathbb{H}(L^{(\mathbb{Z}_3,+)})$ with a uniform heat value $h(L^{(\mathbb{Z}_3,+)}) = 1$ [right].**

$L^{(\mathbb{Z}_3,+)}$

| | | |
|---|---|---|
| 0 | 1 | 2 |
| 1 | 2 | 0 |
| 2 | 0 | 1 |

$\mathbb{H}(L^{(\mathbb{Z}_3,+)})$

| | | |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 1 | 1 |
| 1 | 1 | 1 |

**Table C.2: The prime power order-4 super-symmetric latin square $L^{(\mathbb{F}_{2^2},+)}$ that encodes the Galois field addition group $(\mathbb{F}_{2^2},+)$ with a confirmed maximum transversal count $|\mathcal{T}^{L^{(\mathbb{F}_{2^2},+)}}| = 8 = \mathbb{T}(4)$ [left] and its transversal heat map $\mathbb{H}(L^{(\mathbb{F}_{2^2},+)})$ with a uniform heat value $h(L^{(\mathbb{F}_{2^2},+)}) = 2$ [right].**

$L^{(\mathbb{F}_{2^2},+)}$

| | | | |
|---|---|---|---|
| 0 | 1 | 2 | 3 |
| 1 | 0 | 3 | 2 |
| 2 | 3 | 0 | 1 |
| 3 | 2 | 1 | 0 |

$\mathbb{H}(L^{(\mathbb{F}_{2^2},+)})$

| | | | |
|---|---|---|---|
| 2 | 2 | 2 | 2 |
| 2 | 2 | 2 | 2 |
| 2 | 2 | 2 | 2 |
| 2 | 2 | 2 | 2 |

**Table C.3: The prime order-5 cyclic latin square $L^{(\mathbb{Z}_5,+)}$ that encodes the cyclic group $(\mathbb{Z}_5,+)$ (and also the Galois field addition group $(\mathbb{F}_{5^1},+)$) with a confirmed maximum transversal count $|\mathcal{T}^{L^{(\mathbb{Z}_5,+)}}| = 15 = \mathbb{T}(5)$ [left] and its transversal heat map $\mathbb{H}(L^{(\mathbb{Z}_5,+)})$ with a uniform heat value $h(L^{(\mathbb{Z}_5,+)}) = 3$ [right].**

$L^{(\mathbb{Z}_5,+)}$

| | | | | |
|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 |
| 1 | 2 | 3 | 4 | 0 |
| 2 | 3 | 4 | 0 | 1 |
| 3 | 4 | 0 | 1 | 2 |
| 4 | 0 | 1 | 2 | 3 |

$\mathbb{H}(L^{(\mathbb{Z}_5,+)})$

| | | | | |
|---|---|---|---|---|
| 3 | 3 | 3 | 3 | 3 |
| 3 | 3 | 3 | 3 | 3 |
| 3 | 3 | 3 | 3 | 3 |
| 3 | 3 | 3 | 3 | 3 |
| 3 | 3 | 3 | 3 | 3 |

**Table C.4: The prime order-7 cyclic latin square $L^{(\mathbb{Z}_7,+)}$ that encodes the cyclic group $(\mathbb{Z}_7,+)$ (and also the Galois field addition group $(\mathbb{F}_{7^1},+)$) with a confirmed maximum transversal count $|\mathcal{T}^{L^{(\mathbb{Z}_7,+)}}| = 133 = \mathbb{T}(7)$ [left] and its transversal heat map $\mathbb{H}(L^{(\mathbb{Z}_7,+)})$ with a uniform heat value $h(L^{(\mathbb{Z}_7,+)}) = 19$ [right].**

$L^{(\mathbb{Z}_7,+)}$

| | | | | | | |
|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 0 | 1 | 2 | 3 | 4 | 5 |

$\mathbb{H}(L^{(\mathbb{Z}_7,+)})$

| | | | | | | |
|---|---|---|---|---|---|---|
| 19 | 19 | 19 | 19 | 19 | 19 | 19 |
| 19 | 19 | 19 | 19 | 19 | 19 | 19 |
| 19 | 19 | 19 | 19 | 19 | 19 | 19 |
| 19 | 19 | 19 | 19 | 19 | 19 | 19 |
| 19 | 19 | 19 | 19 | 19 | 19 | 19 |
| 19 | 19 | 19 | 19 | 19 | 19 | 19 |
| 19 | 19 | 19 | 19 | 19 | 19 | 19 |

**Table C.5: The prime power order-8 super-symmetric latin square $L^{(\mathbb{F}_{2^3},+)}$ that encodes the Galois field addition group $(\mathbb{F}_{2^3},+)$ with a confirmed maximum transversal count $|\mathcal{T}^{L^{(\mathbb{F}_{2^3},+)}}| = 384 = \mathbb{T}(8)$ [left] and its transversal heat map $\mathbb{H}(L^{(\mathbb{F}_{2^3},+)})$ with a uniform heat value $h(L^{(\mathbb{F}_{2^3},+)}) = 48$ [right].**

$L^{(\mathbb{F}_{2^3},+)}$

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 0 | 3 | 2 | 5 | 4 | 7 | 6 |
| 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 |
| 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 |
| 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| 5 | 4 | 7 | 6 | 1 | 0 | 3 | 2 |
| 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 |
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

$\mathbb{H}(L^{(\mathbb{F}_{2^3},+)})$

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 48 | 48 | 48 | 48 | 48 | 48 | 48 | 48 |
| 48 | 48 | 48 | 48 | 48 | 48 | 48 | 48 |
| 48 | 48 | 48 | 48 | 48 | 48 | 48 | 48 |
| 48 | 48 | 48 | 48 | 48 | 48 | 48 | 48 |
| 48 | 48 | 48 | 48 | 48 | 48 | 48 | 48 |
| 48 | 48 | 48 | 48 | 48 | 48 | 48 | 48 |
| 48 | 48 | 48 | 48 | 48 | 48 | 48 | 48 |
| 48 | 48 | 48 | 48 | 48 | 48 | 48 | 48 |

**Table C.6: The prime power order-9 super-symmetric latin square $L^{(\mathbb{F}_{3^2},+)}$ that encodes the Galois field addition group $(\mathbb{F}_{3^2},+)$ with a confirmed maximum transversal count $|\mathcal{T}^{L^{(\mathbb{F}_{3^2},+)}}| =$ 2,241 $= \mathbb{T}(9)$ [left] and its transversal heat map $\mathbb{H}(L^{(\mathbb{F}_{3^2},+)})$ with a uniform heat value $h(L^{(\mathbb{F}_{3^2},+)}) = 249$ [right].**

$L^{(\mathbb{F}_{3^2},+)}$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 |
| 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 |
| 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 |
| 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 |
| 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 |
| 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 |
| 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 |

$\mathbb{H}(L^{(\mathbb{F}_{3^2},+)})$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |

**Table C.7: The prime order-11 cyclic latin square $L^{(\mathbb{Z}_{11},+)}$ that encodes the cyclic group $(\mathbb{Z}_{11},+)$ (and also the Galois field addition group $(\mathbb{F}_{11^1},+)$) with a conjectured maximum transversal count $|\mathcal{T}^{L^{(\mathbb{Z}_{11},+)}}| = \mathbf{37{,}851} = \lfloor \mathbb{T}(11)\rfloor_{\mathbf{MMW}}$ [left] and its transversal heat map $\mathbb{H}(L^{(\mathbb{Z}_{11},+)})$ with a uniform heat value $h(L^{(\mathbb{Z}_{11},+)}) =$ 3,441 [right].**

$L^{(\mathbb{Z}_{11},+)}$

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 0 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 0 | 1 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 0 | 1 | 2 |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 | 0 | 1 | 2 | 3 |
| 5 | 6 | 7 | 8 | 9 | 10 | 0 | 1 | 2 | 3 | 4 |
| 6 | 7 | 8 | 9 | 10 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 8 | 9 | 10 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 8 | 9 | 10 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 9 | 10 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

$\mathbb{H}(L^{(\mathbb{Z}_{11},+)})$

| | | | | | | |
|---|---|---|---|---|---|---|
| 3 441 | 3 441 | 3 441 | 3 441 | 3 441 | ... | 3 441 |
| 3 441 | 3 441 | 3 441 | 3 441 | 3 441 | ... | 3 441 |
| 3 441 | 3 441 | 3 441 | 3 441 | 3 441 | ... | 3 441 |
| 3 441 | 3 441 | 3 441 | 3 441 | 3 441 | ... | 3 441 |
| 3 441 | 3 441 | 3 441 | 3 441 | 3 441 | ... | 3 441 |
| 3 441 | 3 441 | 3 441 | 3 441 | 3 441 | ... | 3 441 |
| 3 441 | 3 441 | 3 441 | 3 441 | 3 441 | ... | 3 441 |
| 3 441 | 3 441 | 3 441 | 3 441 | 3 441 | ... | 3 441 |
| 3 441 | 3 441 | 3 441 | 3 441 | 3 441 | ... | 3 441 |
| 3 441 | 3 441 | 3 441 | 3 441 | 3 441 | ... | 3 441 |
| 3 441 | 3 441 | 3 441 | 3 441 | 3 441 | ... | 3 441 |

**Table C.8: The prime order-13 cyclic latin square $L^{(\mathbb{Z}_{13},+)}$ that encodes the cyclic group $(\mathbb{Z}_{13},+)$ (and also the Galois field addition group $(\mathbb{F}_{13^1},+)$) with a conjectured maximum transversal count $|\mathcal{T}^{L^{(\mathbb{Z}_{13},+)}}| = \mathbf{1{,}030{,}367} = \lfloor \mathbb{T}(13)\rfloor_{\mathbf{MMW}}$ [left] and its transversal heat map $\mathbb{H}(L^{(\mathbb{Z}_{13},+)})$ with a uniform heat value $h(L^{(\mathbb{Z}_{13},+)}) =$ 79,259 [right].**

$L^{(\mathbb{Z}_{13},+)}$

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 0 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 0 | 1 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 0 | 1 | 2 |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 0 | 1 | 2 | 3 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 0 | 1 | 2 | 3 | 4 |
| 6 | 7 | 8 | 9 | 10 | 11 | 12 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 8 | 9 | 10 | 11 | 12 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 8 | 9 | 10 | 11 | 12 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 9 | 10 | 11 | 12 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10 | 11 | 12 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 11 | 12 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 12 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |

$\mathbb{H}(L^{(\mathbb{Z}_{13},+)})$

| | | | | | |
|---|---|---|---|---|---|
| 79 259 | 79 259 | 79 259 | 79 259 | ... | 79 259 |
| 79 259 | 79 259 | 79 259 | 79 259 | ... | 79 259 |
| 79 259 | 79 259 | 79 259 | 79 259 | ... | 79 259 |
| 79 259 | 79 259 | 79 259 | 79 259 | ... | 79 259 |
| 79 259 | 79 259 | 79 259 | 79 259 | ... | 79 259 |
| 79 259 | 79 259 | 79 259 | 79 259 | ... | 79 259 |
| 79 259 | 79 259 | 79 259 | 79 259 | ... | 79 259 |
| 79 259 | 79 259 | 79 259 | 79 259 | ... | 79 259 |
| 79 259 | 79 259 | 79 259 | 79 259 | ... | 79 259 |
| 79 259 | 79 259 | 79 259 | 79 259 | ... | 79 259 |
| 79 259 | 79 259 | 79 259 | 79 259 | ... | 79 259 |
| 79 259 | 79 259 | 79 259 | 79 259 | ... | 79 259 |
| 79 259 | 79 259 | 79 259 | 79 259 | ... | 79 259 |

**Table C.9: The prime power order-16 super-symmetric latin square $L^{(\mathbb{F}_{2^4},+)}$ that encodes the Galois field addition group $(\mathbb{F}_{2^4},+)$ with a conjectured maximum transversal count $|\mathcal{T}^{L^{(\mathbb{F}_{2^4},+)}}| =$ 244,744,192 $= \lfloor \mathbb{T}(16) \rfloor_{\text{MMW}}$ [left] and its transversal heat map $\mathbb{H}(L^{(\mathbb{F}_{2^4},+)})$ with a uniform heat value $h(L^{(\mathbb{F}_{2^4},+)}) =$ 15,296,512 [right].**

$L^{(\mathbb{F}_{2^4},+)}$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 1 | 0 | 3 | 2 | 5 | 4 | 7 | 6 | 9 | 8 | 11 | 10 | 13 | 12 | 15 | 14 |
| 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 | 10 | 11 | 8 | 9 | 14 | 15 | 12 | 13 |
| 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 11 | 10 | 9 | 8 | 15 | 14 | 13 | 12 |
| 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 12 | 13 | 14 | 15 | 8 | 9 | 10 | 11 |
| 5 | 4 | 7 | 6 | 1 | 0 | 3 | 2 | 13 | 12 | 15 | 14 | 9 | 8 | 11 | 10 |
| 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 | 14 | 15 | 12 | 13 | 10 | 11 | 8 | 9 |
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 9 | 8 | 11 | 10 | 13 | 12 | 15 | 14 | 1 | 0 | 3 | 2 | 5 | 4 | 7 | 6 |
| 10 | 11 | 8 | 9 | 14 | 15 | 12 | 13 | 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 |
| 11 | 10 | 9 | 8 | 15 | 14 | 13 | 12 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 |
| 12 | 13 | 14 | 15 | 8 | 9 | 10 | 11 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| 13 | 12 | 15 | 14 | 9 | 8 | 11 | 10 | 5 | 4 | 7 | 6 | 1 | 0 | 3 | 2 |
| 14 | 15 | 12 | 13 | 10 | 11 | 8 | 9 | 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 |
| 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

$\mathbb{H}(L^{(\mathbb{F}_{2^4},+)})$

| | | | |
|---|---|---|---|
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |
| 15 296 512 | 15 296 512 | ... | 15 296 512 |

**Table C.10: The prime order-17 cyclic latin square $L^{(\mathbb{Z}_{17},+)}$ that encodes the cyclic group $(\mathbb{Z}_{17},+)$ (and also the Galois field addition group $(\mathbb{F}_{17^1},+)$) with a conjectured maximum transversal count $|\mathcal{T}^{L^{(\mathbb{Z}_{17},+)}}| =$ 1,606,008,513 $= \lfloor \mathbb{T}(17) \rfloor_{\text{MMW}}$ [left] and its transversal heat map $\mathbb{H}(L^{(\mathbb{Z}_{17},+)})$ with a uniform heat value $h(L^{(\mathbb{Z}_{17},+)}) =$ 94,471,089 [right].**

$L^{(\mathbb{Z}_{17},+)}$

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 0 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 0 | 1 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 0 | 1 | 2 |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 0 | 1 | 2 | 3 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 0 | 1 | 2 | 3 | 4 |
| 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 11 | 12 | 13 | 14 | 15 | 16 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 12 | 13 | 14 | 15 | 16 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 13 | 14 | 15 | 16 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 14 | 15 | 16 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 15 | 16 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 16 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |

$\mathbb{H}(L^{(\mathbb{Z}_{17},+)})$

| | | | |
|---|---|---|---|
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |
| 94 471 089 | 94 471 089 | ... | 94 471 089 |