Automorphism Groups of Some Designs of Steiner Triple Systems and the Automorphism Groups of their Block Intersection Graphs.

by
Sunday Vodah

a thesis submitted in fulfillment of the requirements for the degree of Master of Science
in the
Department of Mathematics and Applied Mathematics,
University of the Western Cape

Supervisor: **Prof Eric Mwambene**

June 2014

Declaration of Authorship

I declare that *Automorphism Groups of Some Designs of Steiner Triple Systems and the Automorphism Groups of their Block Intersection Graphs* is my own work, that it has not been submitted for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged by complete references.

Sunday Vodah June 2014

Signed:..

Abstract

A Steiner triple system of order v is a collection of subsets of size three from a set of $v-$elements such that every pair of the elements of the set is contained in exactly one 3-subset. In this study, we discuss some known Steiner triple systems and their automorphism groups. We also construct block intersection graphs of the Steiner triple systems of our consideration and compare their automorphism groups to the automorphism groups of the Steiner triple systems.

June 2014.

For her irreplaceable and endless love, this thesis is dedicated to my late mother.

Acknowledgment

"One man may hit the mark, another blunder; but heed not these distinctions. Only from the alliance of the one, working with and through the other, are great things born." —Antoine de Saint-Exupéry

Respectfully to a very special advisor without whose motivation, support, and guidance, this vision would not have been a reality. Your tremendous patience and resilient encouragement has made this dream come true. I appreciate your efforts in introducing me into the intriguing world of algebraic combinatorics.

I would like to specially appreciate Prof. David Holgate, Prof. Witbooi, Dr. Cloud Makasu and all other staff members of the department. Sincerely, I am grateful for your support.

I would also like to extend my appreciation to the University of the Western Cape for the teaching assistant position in the Department of Mathematics.

To those that have shown to me that there is more to life than work and because I am the sum of my life experiences, I would like to appreciate Dr Albert Amosu, Dr Oluwakemi Tovide, Mrs Emilia Marshall and family, Dr Aderibigbe Anjorin, Dr Kehinde Agbele, Dr Raji Odutayo, Dr Badmus Jelili, Dr Oluwafemi Alamu, Dr Christopher Sunday, Mr Gbenga Abiodun and Mr Gbenga Popoola.

Finally, my heartfelt appreciation to all my family members for their care, support, encouragement and prayers in actualizing this dream.

Publication arising from this thesis

Eric Mwambene and Sunday Vodah. **On the automorphism groups of Steiner triple system obtained by the Skolem method** .
Submitted 2014.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction and background

Combinatorial design theory constitutes the arrangement of elements of a set into patterns according to defined rules. Its history can be traced as far back as Euler's work on Latin squares. Design theory is now a rapidly developing area of mathematics with applications in several other areas including finite geometry, software testing, cryptography, engineering, algebraic geometry, graph theory and coding theory, just to name a few.

A Steiner system is an important type of block design. Many variations of the block designs have been studied, but the most intensely studied are the balanced incomplete block designs (BIBDs or 2-designs) which historically are related to statistical issues in the design of experiments.

Steiner systems were defined through a posed problem for the first time by W.S.B. Woolhouse in 1844 [26]. The posed problem on Steiner triple systems was solved by Thomas Kirkman in 1847 [22]. In 1850 Kirkman introduced a variation of the problem now known as Kirkman's schoolgirl problem, which added additional property called resolvability to triple systems. Oblivious of Kirkman's work, Jakob Steiner (1853) re-established triple systems. His extensive study on this subject matter made it more popular and it is not surprising that they are named after him.

Kirkman [22] established the fact that a Steiner triple system of order v exists if and only if $v \equiv 1$ or $3 \pmod 6$ in 1847. Bose [18] constructed such systems in 1939 for $v \equiv 3 \pmod 6$. Two decades later, Skolem [24] constructed triple systems for which $v \equiv 1 \pmod 6$.

Several studies have shown that Steiner triple systems exist in affine and projective geometries and their automorphisms are well known ([11], [6], [14], [4]).

Recently, Lovegrove [8] determined the automorphism group of the Steiner triple systems obtained by Bose construction.

J. Šiftar and H. Zeitler [12] investigated automorphisms of some special type of 2-generated quasigroups of different orders of which at first sight would appear to be similar to the quasigroups used in the construction of Steiner triple systems by Skolem constructions. Their search for automorphism was based on commuting pairs.

The quasigroups used in Skolem construction are commutative and half-idempotent. All elements in the quasigroups commute. We therefore develop a different approach in the search for automorphisms of these quasigroups. Further we explore the symmetry of the quasigroups; proving that the automorphism group of the quasigroup is $\{1\}$, the trivial group. We also determine the full automorphism group of the design of Steiner triple system by the Skolem construction.

We further explore the block intersection graphs of the designs of our consideration and investigate the properties of the graphs.

Finally, we investigate the automorphism groups of the block intersection graphs of the designs and compare them with the automorphism groups of the designs.

1.2 Overview of the thesis

In this study, after giving the necessary preliminaries, we examine the existence question of Steiner triple systems; and in the course present the Bose and Skolem constructions of Steiner triple systems. We also discuss the constructions of Steiner triple systems from the projective and affine geometries. In Chapter 4 we examine the automorphism groups of the designs of Steiner triple systems from Bose and Skolem constructions as well as the projective and affine geometries. In Chapter 5, we present the block intersection graphs of the designs presented in Chapter 4. We further investigate the properties of the graphs. Finally, in Chapter 6, we examine the automorphism groups of the block intersection graphs of the designs.

Chapter 2

Preliminaries and notations

In this chapter we introduce the notation which we use throughout this study. We also state some fundamental results that we will use in the course of this study as well as some basic definitions.

In Chapter 3, we construct Steiner triple systems from odd order abelian groups using the Bose construction. The Bose construction of Steiner triple systems is capable of different modifications and generalizations. We consider abelian groups because of their richness in symmetry. A permutation is defined on the abelian group in order to make it idempotent. This is discussed in detail in Chapter 3.

In discussing the automorphism group of Steiner triple systems by Bose construction in Chapter 4, we also consider the automorphism group of abelian groups used in their constructions. Hence, we briefly discuss the automorphism of abelian groups.

The following result is fundamental in characterizing abelian groups.

2.1 Theorem [20] *Let G be a finite abelian group. Then G is isomorphic to a direct product of groups of the form $H_p = \mathbb{Z}/p^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{e_n}\mathbb{Z}$ in which p is a prime number and $1 < e_1 < \cdots < e_n$ are positive integers.*

In discussing the automorphism group of abelian groups, it is essential to begin with the following.

Let G and H be finite groups with relatively prime orders. It is well known that Aut $(G \times H) =$ Aut $G \times$ Aut H (see [5], Lemma 2.1).

We now describe the automorphism group of an Abelian group.

The inner automorphism group of the group $\mathbb{Z}_p^n$ is trivial. The outer automorphism group of $\mathbb{Z}_p^n$ is $\mathrm{GL}(n,p)$.

Now, if $G = \mathbb{Z}_{p_1}^{n_1} \times \mathbb{Z}_{p_2}^{n_2} \times \cdots \times \mathbb{Z}_{p_k}^{n_k}$, where $\mathbb{Z}_{p_1}^{n_1} \ncong \mathbb{Z}_{p_2}^{n_2} \ncong, \cdots, \ncong \mathbb{Z}_{p_k}^{n_k}$. Then Aut G is the direct product of the groups $\mathrm{GL}(n_i,p_i), i = 1,\ldots,k$.

In other words,

$$\text{Aut } G = \bigoplus_{i=1}^{k} \mathrm{GL}(n_i, m_i).$$

In Chapter 4 of this study, one of the concepts employed in discussing the automorphism groups of Steiner triple systems by the Bose construction is the holomorph of a group.

We now define the concept.

Let G and H be groups. Suppose there is a homomorphism $\phi : H \to \text{Aut } G$. Then define a binary operation $*$ on $G \times_\phi H$ by

$$(g_1, h_1) * (g_2, h_2) = (g_1\phi(h_1)(g_2), h_1h_2).$$

It is well known that $G \times_\phi H$ is a group. Such groups are semi-direct products in the form $G \rtimes_\phi H$. If H coincides with Aut G and ϕ is the identity map, then $G \rtimes_\phi H$ is the holomorph of G (see [21], p. 461). The holomorph of a group denoted $\mathrm{Hol}(G)$ is therefore the semi-direct product of a group and its automorphism group.

For more details on the automorphism group of finite Abelian groups, see [5].

In Chapter 3 of this study, we construct Steiner triple systems from the projective and affine planes and discuss their automorphism groups in Chapter 4. This construction of Steiner triple systems and their automorphism groups are ultimately linked to the general linear groups. Hence, we introduce general linear groups.

2.1 Definition *Let $\mathbb{F}$ be a field. Then the general linear group* $\mathrm{GL}(n,\mathbb{F})$ *is the group of invertible $n \times n$ matrices with entries in $\mathbb{F}$ under matrix multiplication.*

If $\mathbb{F}$ is a finite field of order q, then it is written $\mathrm{GL}(n,q)$ instead of $\mathrm{GL}(n,\mathbb{F})$.

It is a well known fact [2] that

$$|\mathrm{GL}(n,q)| = \prod_{m=0}^{n-1} (q^n - q^m). \tag{2.1}$$

We now discuss the projective and affine linear groups.

The quotient of $\mathrm{GL}(n,\mathbb{F})$ by its center $Z(\mathrm{GL}(n,\mathbb{F}))$ is called the projective linear group.

The affine group $\mathrm{AG}(n,\mathbb{F})$ is an extension of $\mathrm{GL}(n,\mathbb{F})$ by the group of translations in $\mathbb{F}^n$. It is aptly written as a semidirect product:

$$\mathrm{AG}(n,\mathbb{F}) = \mathrm{GL}(n,\mathbb{F}) \rtimes \mathbb{F}^n$$

where $\mathrm{GL}(n,\mathbb{F})$ acts on $\mathbb{F}^n$ naturally. The affine group can be considered as the group of all affine transformations of the affine space underlying the vector space $\mathbb{F}^n$.

A Galois group is a group of field automorphisms under composition. It is denoted $\mathrm{Gal}(\mathbb{F})$. The Galois group acts on $\mathrm{GL}(n,\mathbb{F})$ by the Galois action on its entries.

A semilinear transformation is a transformation which is linear up to a field automorphism under scalar multiplication. The general semilinear group $\Gamma\mathrm{L}(n,\mathbb{F})$ is the group of all invertible semilinear transformations. The general semilinear group contains $\mathrm{GL}(n,\mathbb{F})$. It is conveniently written as a semidirect product:

$$\Gamma\mathrm{L}(n,\mathbb{F}) = \mathrm{Gal}(\mathbb{F}) \rtimes \mathrm{GL}(n,\mathbb{F})$$

where $\mathrm{Gal}(\mathbb{F})$ is the Galois group over its prime field $\mathbb{F}$.

The general semilinear group $\Gamma\mathrm{L}(n,\mathbb{F})$ is of important interest in this study because the associated projective semilinear group $\mathrm{P}\Gamma\mathrm{L}(n,\mathbb{F})$, which contains $\mathrm{PGL}(n,\mathbb{F})$ is the collineation group of projective space, for $n > 2$.

For more details on linear groups, see [9].

Another interesting algebraic structure considered in this study is the quasigroups. Quasigroups continue to play important roles in constructing Steiner triple systems. In this respect, for instance, the constructions of Steiner triple systems by both Bose and Skolem are based on quasigroups.

2.2 Definition A quasigroup $(\mathrm{Q}, *)$ is a set Q together with a binary operation $*$ such that :

(i) The set Q is closed under $*$. That is $x * y \in \mathrm{Q}$, for all $x, y \in \mathrm{Q}$.

(ii) Given $a, b \in \mathrm{Q}$, such that $a * x = b$, and $y * a = b$, there exist unique solutions $x, y \in \mathrm{Q}$.

Conditions (i) and (ii) above ensures that each element of Q occurs exactly once in each row and exactly once in each column of the quasigroup's multiplication table. In other words, Q is endowed with left and right division.

Quasigroups are in general non-commutative and non-associative algebraic structures. They differ from groups mainly because the binary operation $*$ need not be associative.

Another related concept of the quasigroups is the latin square.

2.3 Definition Let Q be a finite set of order n. An $n \times n$ array M with entries from Q is a latin square of order n provided every row of M is a permutation of Q and every column of M is a permutation of Q.

In other words, a latin square is an $n \times n$ square matrix M whose entries consist of n symbols such that each symbol appears exactly once in each row and each column.

The operation table of a binary operation $*$ defined on Q is the $|\mathrm{Q}| \times |\mathrm{Q}|$ array $\mathrm{M} = (a_{x,y})$, where $a_{x,y} = x * y$. This property ensures that the Cayley table of a finite quasigroup is a latin square. The following result relates quasigroups to latin squares.

2.2 Theorem [7] *Let $*$ be a binary operation defined on a finite set* Q *of cardinality n. Then* $(\mathrm{Q}, *)$ *is a quasigroup if and only its operation table is a latin square of order n.*

For the constructions of Steiner triple systems, we need an idempotent and commutative quasigroup for Bose constructions and a half-idempotent and commutative quasigroup for Skolem constructions. Here, we define these two special properties of quasigroups.

2.4 Definition (a) A quasigroup $(\mathrm{Q}, *)$ is *idempotent* if for all $x \in \mathrm{Q}$, $x * x = x$.

(b) A quasigroup $(\mathrm{Q}, *)$ is *commutative* if for all $x, y \in \mathrm{Q}$, $x * y = y * x$.

2.5 Definition A latin square L of order $2n$ is *half-idempotent* if the cells (i, i) and $(n+i, n+i)$ contain the symbol i, for every $1 \leq i \leq n$.

A quasigroup $(\mathrm{Q}, *)$ of order $2n$ is half-idempotent if its Cayley table is half-idempotent.

Commutative and half-idempotent quasigroups $(\mathrm{Q}, *)$ exist only for even orders of Q. On the other hand,

Remark [7] *Let* $(\mathrm{Q}, *)$ *be a commutative and idempotent quasigroup of order* n. *Then* n *is odd.*

Now, we discuss some essentials of design theory.

2.1 Basics of design theory

2.6 Definition Let V be a set of elements called points. A design is a pair $\mathcal{D} = (V, \mathcal{B})$ such that $\mathcal{B}$ is a collection of nonempty subsets of V called blocks.

A block design in which all the blocks have the same size is called $uniform$. Two identical blocks in a design are said to be repeated blocks. A design is said to be *simple* if it does not contain repeated blocks. A design is *regular* if every point occurs equally often in the design. In this study, we consider simple, regular and uniform designs.

2.7 Definition An incidence system (v, k, λ, b, r) in which a set V of v points and a family $\mathcal{B}$ of b subsets (blocks) containing k points each in such a way that any two points determine λ blocks, and each point is contained in r different blocks is a block design.

In view of Definition 2.7, the following hold:

(i) If $k < v$, then the block design is said to be an *incomplete block design*.

(ii) If every pair of distinct points in a design is contained in exactly λ blocks, then the design is called a balanced design.

(iii) A block design which is incomplete and balanced is called a balanced incomplete block design, or simply a BIBD.

1 Example Let $V = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and

$\mathcal{B} = \{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{1, 4, 7\}, \{2, 5, 8\}, \{3, 6, 9\}, \{1, 5, 9\}, \{2, 6, 7\},$

$\{3, 4, 8\}, \{1, 6, 8\}, \{2, 4, 9\}, \{3, 5, 7\}\}$. Then $(V, \mathcal{B})$ is a $(9, 3, 1, 12, 4)$-BIBD.

Definition 2.7 can also be re-formulated as a *t-design* in the following way.

Let V be a set with cardinality v and $\mathcal{B}$ is a collection of subsets (blocks) of size k selected from V. Let t, v and λ be positive integers such that $1 < k < v$, and any set of t points appears as a subset of exactly λ blocks. Then $(V, \mathcal{B})$ is called a t-design with parameters (v, k, λ).

It is also generally required that $k < v$ and in such case, the design is said to be incomplete. Should $k = 3, t = 2, \lambda = 1$, then a t-design is said to be a $2-$design with parameters $(v, 3, 1)$ denoted $S(2, 3, v)$. These designs are at the center of our study.

We now give the definition of the fundamental object of our study.

2.8 Definition Let V be a finite nonempty set with v elements and $\mathcal{B}$ be a collection of 3-element subsets of V called *blocks* or *triples*. A Steiner triple system of order(v), briefly STS(v) is the pair $(V, \mathcal{B})$ such that every pair of elements of V appear together in a unique block of $\mathcal{B}$.

2.9 Definition Let $(V, \mathcal{B})$ and $(V', \mathcal{B}')$ be any two designs. An isomorphism is a map $\phi : V \to V'$ such that

(a) ϕ is a bijection;

(b) $\phi(B) \in \mathcal{B}'$ for every $B \in \mathcal{B}$.

If two designs $(V, \mathcal{B})$ and $(V', \mathcal{B}')$ are isomorphic, it is denoted $(V, \mathcal{B}) \cong (V', \mathcal{B}')$. Steiner triple systems of orders 3, 7 and 9 are unique (see [16], [17]). Should $(V, \mathcal{B})$ and $(V', \mathcal{B}')$ coincide then ϕ is said to be an automorphism.

An automorphism of a design is an isomorphism of the design with itself. Composing two automorphisms produces an automorphism. The identity is always an automorphism and the inverse of an automorphism is also an automorphism. Hence the set of all automorphisms forms a permutation group under composition, which is called the automorphism group of the design.

The automorphism group of a design is always a subgroup of the symmetric group on v letters where v is the number of points of the design. For a design $\mathcal{D}$, the automorphism group is denoted Aut $\mathcal{D}$.

For design theory terms not defined, we follow [7].

Graphs are the content of Chapter 5 and their automorphism groups are the contents of Chapter 6.

We now turn our attention to some fundamentals of graph theory.

2.2 Graph theoretic definitions

Let V be a set and R a relation defined on V. Then $D = (V, R)$ is called a *digraph* if R is irreflexive, i.e., $(v, v) \notin R$ for all $v \in V$. The elements of V are called *vertices* and the elements of R are called *arcs*. The out-degree of a vertex x is the size of the set $\{y \in V : (x, y) \in R\}$. The in-degree of x is similarly defined as the size of the set $\{y \in V : (y, x) \in R\}$.

A *graph* $\Gamma = (V, E)$ is a digraph with the additional property that E is symmetric. In other words, a graph $\Gamma = (V, E)$ consists of a set of vertices V and a relation E which is irreflexive and symmetric. If it is not clear from the context, we will denote V by $V(\Gamma)$ and E by $E(\Gamma)$.

The arcs (x, y) and (y, x) are identified into a single *edge* and denoted $[x, y]$. Let V be a set and denote $V^{\{2\}}$ the family of all 2-subsets of V. Edges of the graph $\Gamma = (V, E)$ can be identified as the subset of $V^{\{2\}}$. In this sequel, we consider only finite graphs, i.e., a graph Γ for which both $V(\Gamma)$ and $E(\Gamma)$ are finite sets.

Two vertices x and y of a graph Γ are *adjacent* if there is an edge $e = [x, y]$ joining them. The vertices x and y are said to be *incident* with e. If x and y are adjacent, it is said that they are *neighbours*. Similarly, two distinct edges e and e' are *adjacent* if they have a vertex in common.

Let Γ be a graph. The *neighbourhood* of a vertex $x \in$ V(Γ) is the set of vertices that are adjacent to x, and it is denoted by $N_\Gamma(x)$. The *degree* $\deg(v)$ of a vertex $v \in \mathrm{V}(\Gamma)$ is the number edges incident on v. That is, the size of its neighbourhood, $|N_\Gamma(v)|$.

One of the interesting foundational results commonly used in graph theory is the hand shaking lemma [13], which is in the following:

Let $\Gamma = (V, E)$ be a graph. Then

$$\sum_{v \in V} \deg(v) = 2|E|.$$

A graph in which each vertex has the same degree is said to be *regular*. If each vertex has degree r, the graph is *regular of degree* r or r*-regular*. A *complete graph* is the one in which every two distinct vertices are adjacent. The complete graph on n vertices is denoted K_n.

A sequence $x_0, x_1, \ldots, x_k$ of vertices of a graph Γ is a path if $[x_i, x_{i+1}] \in E(\Gamma)$ for all $i = 0, \ldots, k-1$. A graph Γ is said to be connected if for every pair of vertices, there is a path joining them.

A graph $\Gamma' = (V', E')$ is called a *subgraph* of $\Gamma = (V, E)$ if $V' \subset V$ and $E' \subset E$. Let $\Gamma = (V, E)$ be a graph and Γ' be a subgraph of Γ. Then Γ' is an *induced subgraph* on V' if $E' = E \cap V'^{\{2\}}$.

2.10 Definition *Let $\Gamma = (V, E)$ be a graph and $V' \subseteq V$. Then the induced subgraph $\Gamma[V']$ is a clique (independent set) if it is a complete graph (null graph).*

The size of a clique is the number of vertices in the clique. A *maximal clique* (*maximal independent set*) is a clique (independent set) that cannot be extended by an additional vertex. That is, a maximal clique (maximal independent set) is the one which is not contained in a larger clique (independent set). A *maximum clique* (*maximum independent set*) is the clique (independent set) of the largest possible size in a given graph Γ. The *clique number* $\omega(\Gamma)$ (*independence number* $\omega'(\Gamma)$) of a graph Γ is the number of vertices in the maximum clique (maximum independent set) of Γ.

It will be shown that block intersection graphs of Steiner triple systems are strongly regular graphs. We now define the concept.

2.11 Definition A strongly regular graph Γ with parameters (n, k, λ, μ) is a graph on n vertices which is regular with degree k and has the following properties:

(i) any two adjacent vertices have exactly λ common neighbors;

(ii) any two non-adjacent vertices have exactly μ common neighbors.

We now discuss the automorphism groups of graphs.

2.12 Definition (a) Let Γ_1, Γ_2 be graphs. A *homomorphism* from Γ_1 to Γ_2 is a map $\alpha : V(\Gamma_1) \to V(\Gamma_2)$ that preserves adjacency, i.e.,

$$[\alpha(x), \alpha(y)] \in V(\Gamma_2) \text{ for any } [x, y] \in V(\Gamma_1).$$

(b) A homomorphism $\alpha : V(\Gamma_1) \to V(\Gamma_2)$ is an *isomorphism* if

(i) α is a bijection;

(ii) α^{-1} is also a homomorphism.

In this case, it is said that Γ_1 is isomorphic to Γ_2 and written $\Gamma_1 \cong \Gamma_2$.

(c) A homomorphism $\alpha : \mathrm{V}(\Gamma_1) \to \mathrm{V}(\Gamma_2)$ for which Γ_1 and Γ_2 coincide is called an *endomorphism*. If in addition, α is a permutation, then it is an *automorphism*.

In other words, an *automorphism* α of a graph Γ is a permutation of the vertex set with the property that $\alpha(x)$ and $\alpha(y)$ are adjacent if and only if x and y are.

The set of all automorphisms forms a permutation group under composition and is denoted by Aut Γ.

For graph theory terms not defined, we follow [19].

Having given the necessary preliminaries, we now focus on the fundamental object of our study, Steiner triple systems.

Chapter 3

Steiner triple systems

In this chapter we discuss the admissibility, as well as the necessity and the sufficiency conditions of the existence of Steiner triple systems.

There are several ways of constructing Steiner triple systems of an admissible order v. We consider archetypal constructions of Steiner triple systems. We are interested in the Bose construction, Skolem construction, and the constructions from the projective and affine geometries.

For brevity, we shall also call the Steiner triple systems from the Bose's constructions, the *Bose Steiner triple systems* and the ones from the Skolem's constructions, the *Skolem Steiner triple systems*.

We now consider the construction of Steiner triple systems in the sequel.

As mentioned in the introduction of this study, Kirkman [22] proved that a Steiner triple system of order v exists if and only if $v \equiv 1$ or $3 \pmod 6$. Such values of v are called *admissible*.

We now explore the necessary conditions for the existence of Steiner triple systems.

3.1 Lemma *Let $(V, \mathcal{B})$ be a Steiner triple system of order v. Then $v \equiv 1$ or 3* $\pmod 6$.

Proof. The number of 2-element subsets of V is clearly $\binom{v}{2}$. By the definition of Steiner triple systems, every pair of elements in V appears in a unique triple, and any triple $\{x, y, z\} \in \mathcal{B}$ contains 3 2-element subsets. Then it follows that the total 2-element subsets of V is $\frac{v(v-1)}{2} = 3 \times |\mathcal{B}|$. This implies that $|\mathcal{B}| = \frac{v(v-1)}{6}$.

For a fixed point $p \in V$, let $\mathcal{B}_p$ be a collection of triples containing p. Let $\mathrm{B_p}, \mathrm{B'_p} \in \mathcal{B}_p$. $(\mathrm{B_p} \backslash p) \cap (\mathrm{B'_p} \backslash p) = \{\}$, since the intersection of any two triples in V can either be $\{\}$ or 1. Hence, $\mathcal{B}_p$ partitions $(V \setminus \{p\})$ into pairs. Therefore $(v-1)$ must be even, so v is odd. This implies that $v \equiv 1, 3$ or 5 (mod 6).

If $v = 6n+5$, then $|\mathcal{B}| = (6n+5)(6n+4)/6 = (36n^2 + 54n + 20)/6$. This is not an integer, hence this case does not arise.

□

3.2 Corollary *Let* $(V, \mathcal{B})$ *be a Steiner triple system of order* v. *A point* $x \in V$ *is in exactly* $\frac{v-1}{2}$ *blocks.*

Proof. The total 2-element subsets of V is $\frac{v(v-1)}{2}$ and there are v points. For a point $x \in V$, there are $\left(\left(\frac{v(v-1)}{2}\right)/v\right)$ points and the result follows.

□

The next theorem is a sufficiency condition for the existence of Steiner triple systems.

3.3 Theorem [22]*If* $v \equiv 1$ *or* 3 (mod 6), *then there exists a Steiner triple system* $(V, \mathcal{B})$ *of order* v.

The sufficiency conditions of Steiner triple systems involve the constructions of Steiner triple systems. We must show that there exist Steiner triple system for any given admissible order $v \equiv 1$ or 3 (mod 6).

In order to prove Theorem 3.3 above, we consider the Bose's and Skolem's constructions of Steiner triple systems. Theorem 3.3 can be broken down as follows:

3.4 Lemma *If* $v \equiv 3$ (mod 6), *then there exists a Steiner triple system* $(V, \mathcal{B})$ *of order* v.

3.5 Lemma *If* $v \equiv 1 \pmod 6$, *then there exists a Steiner triple system* $(V, \mathcal{B})$ *of order* v.

The proof of Lemma 3.4 is the content of Section 3.1 and that of Lemma 3.5 is Section 3.2.

We now present Bose Steiner triple systems.

3.1 Bose Steiner triple system

In 1939, Bose gave a construction of Steiner triple systems $(V, \mathcal{B})$. The concepts of latin squares and quasigroups discussed in Chapter 2 of this study play important roles in the construction of Steiner triple systems by Bose.

In this section, we present Bose Steiner triple systems $\mathbb{B} = (V, \mathcal{B})$ from the construction involving odd order abelian groups G, which we shall always write additively. We consider abelian groups in this construction because they are very rich in symmetry.

The construction of Bose Steiner triple systems using an abelian group G holds because given any two of the elements $x, y, z \in G$, the equation $x + y = 2z$ uniquely establishes the third.

A permutation is defined on the abelian group $(G, +)$ in order to make its multiplication table (latin square) idempotent.

We now describe the required quasigroup (latin square).

Let $(G, +)$ be an abelian group of order $(2n+1), n > 0$. Define a permutation $\pi : G \to G$ by

$$\pi(x) = (2^{-1}(x)) \pmod{2n+1}.$$

With π, a binary operation on the set of elements of G is defined by

$$x * y = \pi(x + y),$$

for all $x, y \in G$. The operation $*$ on G defines a commutative and idempotent quasigroup of order $(2n+1)$. We will call such an algebraic structure a Bose abelian quasigroup $(\mathrm{Q}, *)$ and denote it as Q_{2n+1} for brevity.

With such a Bose abelian quasigroup, it is now appropriate to define the Bose design.

Let $V := \mathrm{Q}_{2n+1} \times \mathbb{Z}_3$ and $\mathcal{B}$ be a family of 3-subsets of V defined as follows:

$$\{(x,0),(x,1),(x,2) : x \in \mathrm{Q}_{2n+1}\}; \tag{3.1}$$

$$\{(x,i),(y,i),(x*y,i+1)\} : x \neq y, i \in \mathbb{Z}_3, \text{ and } x,y \in \mathrm{Q}_{2n+1}\}. \tag{3.2}$$

We refer to blocks of the first kind, **type 1 blocks**, the second kind, **type 2 blocks**.

For clarity, some further terminology are introduced.

The *label* of an element $v \in V$ is the corresponding $\mathbb{Z}_3$ component. The *signature* of a block $B \in \mathcal{B}$ is the sum of the values of the labels of the block modulo 3.

Clearly, the signature of a type 1 block is 0 and a type 2 block is of signature 1. No block has signature 2.

We shall say that a block B is valid if it is of the form of Equations 3.1 and 3.2, and *invalid* if otherwise.

These terminology are employed in Chapter 5 in discussing the automorphism groups of Bose Steiner triple systems.

We now show that $\mathbb{B} = (V, \mathcal{B})$ is a Steiner triple system.

3.6 Lemma *Let $V = \mathrm{Q}_{2n+1} \times \mathbb{Z}_3$ and $\mathcal{B}$ be a family of 3-subsets of V as defined in* (3.1) *and* (3.2)*. Then* $|\mathcal{B}| = \dfrac{v(v-1)}{6}$.

Proof. From (3.1) above, let $x \in \mathrm{Q}$. It is clear that the total number of such blocks depends on the order of the quasigroup. Hence, the number of type 1 triples is exactly $(2n+1)$.

Similarly, from (3.2), there are $\binom{2n+1}{2} = (2n+1)n$ choices for x and y in type 2 blocks, since x must be different from y. Each choice of x and y produces 3-type 2 triples. Hence we have $3(2n+1)n$ type 2 triples.

Therefore, the total number of blocks $|\mathcal{B}|$ is then equal to

$$\begin{aligned}(2n+1) + 3(2n+1)n &= (2n+1)(3n+1)\\ &= (\frac{v}{3})(\frac{v-1}{2})\\ &= \frac{v(v-1)}{6}.\end{aligned}$$

□

We now show that each pair of distinct elements of V occurs together in at exactly one block of $\mathcal{B}$.

3.7 Lemma *Let $V = \mathrm{Q}_{2n+1} \times \mathbb{Z}_3$ and $\mathcal{B}$ be a family of 3-subsets of V as defined in (3.1) and (3.2). Then every pair of distinct elements of V appears in exactly one block of $\mathcal{B}$.*

Proof. Let (x, i) and (y, j) be any pair of distinct elements of V. Then consider the following possibilities:

Case 1: Suppose $x = y$, then the pair (x, i) and (y, j) appears exactly in the form $\{(x, i), (x, j), (x, k)\}$, which is a type 1 triple.

Case 2: Suppose $i = j$, then $x \neq y$ and we have $\{(x, i), (y, i), (x * y, i + 1)\}$. Hence, we have a type 2 triple containing (x, i) and (y, j).

Case 3: Suppose $x \neq y$ and $i \neq j$, then there exist a solution $x * a = y$ for some $a \in \mathrm{Q}_{2n+1}$, since Q_{2n+1} is a commutative quasigroup. The fact that Q_{2n+1} is idempotent and $x \neq y$, implies that $a \neq x$. Without loss of generality, if $j = (i + 1) \in \mathbb{Z}_3$ then the triple $\{(x, i), (a, i), (x * a = y, i + 1)\}$ is clearly a type 2 triple containing (x, i) and (y, j). □

In view of Lemmas 3.6 and 3.7, we have:

3.8 Theorem *Let $V = \mathrm{Q}_{2n+1} \times \mathbb{Z}_3$ and $\mathcal{B}$ be a family of 3-subsets of V as defined in (3.1) and (3.2). Then $\mathbb{B} = (V, \mathcal{B})$ is a Steiner triple system.*

The triple system defined in Theorem 3.8 above is called the Bose Steiner triple system.

We further illustrate the Bose Steiner triple systems with an example.

2 Example Let G be an Abelian group of order 7. Define a permutation $\pi : G \to G$ by

$$\pi(x) = 4x \,(\mathrm{mod}\ 7),$$

for all $x \in G$.

Now, let $* : G \times G \to G$ be defined by

$$x * y = \pi(x + y),$$

for all $x, y \in G$.

The multiplication table below is the Bose abelian quasigroup $(\mathrm{Q}, *)$ of order 7.

Table 3.1: A Latin square of order 7

$*$	0	1	2	3	4	5	6
0	**0**	4	1	5	2	6	3
1	4	**1**	5	2	6	3	0
2	1	5	**2**	6	3	0	4
3	5	2	6	**3**	0	4	1
4	2	6	3	0	**4**	1	3
5	6	3	0	4	1	**3**	2
6	3	0	4	1	3	2	**6**

Let $V = \mathrm{Q}_7 \times \mathbb{Z}_3$ and let $\mathcal{B}$ be a family of 3-subsets of V as defined in (3.1) and (3.2). This is shown below:

Type 1 :

$$\{\{(0,0),(0,1),(0,2)\},\{(1,0),(1,1),(1,2)\},\{(2,0),(2,1),(2,2)\},$$
$$\{(3,0),(3,1),(3,2)\},\{(4,0),(4,1),(4,2)\},\{(5,0),(5,1),(5,2)\},$$
$$\{(6,0),(6,1),(6,2)\}\}.$$

Type 2 :

$$\{\{(0,0),(1,0),(0*1=4,1)\},\{(0,1),(1,1),(4,2)\},\{(0,2),(1,2),(4,0)\}$$
$$\{(0,0),(2,0),(0*2=1,1)\},\{(0,1),(2,1),(1,2)\},\{(0,2),(2,2),(1,0)\}$$
$$\{(0,0),(3,0),(0*3=5,1)\},\{(0,1),(3,1),(5,2)\},\{(0,2),(3,2),(5,0)\}$$
$$\{(0,0),(4,0),(0*4=2,1)\},\{(0,1),(4,1),(2,2)\},\{(0,2),(4,2),(2,0)\}$$
$$\{(0,0),(5,0),(0*5=6,1)\},\{(0,1),(5,1),(6,2)\},\{(0,2),(5,2),(6,0)\}$$
$$\{(0,0),(6,0),(0*6=3,1)\},\{(0,1),(6,1),(3,2)\},\{(0,2),(6,2),(3,0)\}$$
$$\{(1,0),(2,0),(1*2=5,1)\},\{(1,1),(2,1),(5,2)\},\{(1,2),(2,2),(5,0)\}$$
$$\{(1,0),(3,0),(1*3=2,1)\},\{(1,1),(3,1),(2,2)\},\{(1,2),(3,2),(2,0)\}$$

$$\{(1,0),(4,0),(1*4=6,1)\},\{(1,1),(4,1),(6,2)\},\{(1,2),(4,2),(6,0)\}$$
$$\{(1,0),(5,0),(1*5=3,1)\},\{(1,1),(5,1),(3,2)\},\{(1,2),(5,2),(3,0)\}$$
$$\{(1,0),(6,0),(1*6=0,1)\},\{(1,1),(6,1),(0,2)\},\{(1,2),(6,2),(0,0)\}$$
$$\{(2,0),(3,0),(2*3=6,1)\},\{(2,1),(3,1),(6,2)\},\{(2,2),(3,2),(6,0)\}$$
$$\{(2,0),(4,0),(2*4=3,1)\},\{(2,1),(4,1),(3,2)\},\{(2,2),(4,2),(3,0)\}$$
$$\{(2,0),(5,0),(2*5=0,1)\},\{(2,1),(5,1),(0,2)\},\{(2,2),(5,2),(0,0)\}$$
$$\{(2,0),(6,0),(2*6=4,1)\},\{(2,1),(6,1),(4,2)\},\{(2,2),(6,2),(4,0)\}$$
$$\{(3,0),(4,0),(3*4=0,1)\},\{(3,1),(4,1),(0,2)\},\{(3,2),(4,2),(0,0)\}$$
$$\{(3,0),(5,0),(3*5=4,1)\},\{(3,1),(5,1),(4,2)\},\{(3,2),(5,2),(4,0)\}$$
$$\{(3,0),(6,0),(3*6=1,1)\},\{(3,1),(6,1),(1,2)\},\{(3,2),(6,2),(1,0)\}$$
$$\{(4,0),(5,0),(4*5=1,1)\},\{(4,1),(5,1),(1,2)\},\{(4,2),(5,2),(1,0)\}$$
$$\{(4,0),(6,0),(4*6=5,1)\},\{(4,1),(6,1),(5,2)\},\{(4,2),(6,2),(5,0)\}$$
$$\{(5,0),(6,0),(5*6=0,1)\},\{(5,1),(6,1),(0,2)\},\{(5,2),(6,2),(0,0)\}\}.$$

Clearly, every pair of distinct elements of V occurs together in exactly one block of $\mathcal{B}$. There are 7 type 1 triples and 63 type 2 triples. Therefore $(V, \mathcal{B})$ is a Steiner triple system of order 21.

In general, for a Bose Steiner triple system of order v there are $\dfrac{v}{3}$ type 1 blocks and $\dfrac{v(v-3)}{6}$ type 2 blocks.

We now discuss the Skolem's construction.

3.2 Skolem Steiner triple system

Skolem Steiner triple system differs from Bose Steiner triple system in the sense that it uses a half-idempotent quasigroup of even order and an additional point. Moreover, $v \equiv 1 \pmod 6$.

The first stage of the Skolem's construction considers the set $\mathrm{Q} = \{0, 1, \cdots 2n-1\}$ on which he defines a binary operation which is intimately linked to the binary operation in the group $\mathbb{Z}_{2n}$.

The elements of Q together with the binary operation $*$ form a commutative and half-idempotent quasigroup $(\mathrm{Q}, *)$. For brevity, we will call such an algebraic structure a Skolem quasigroup and denote it as Q_{2n}.

The second stage of the Skolem's construction involves defining triples on $\mathrm{Q}_{2n} \times \mathbb{Z}_3$ together with the additional point which we denote $(p, q), p \notin \mathrm{Q}_{2n}$, and $q \notin \mathbb{Z}_3$.

We will call these systems Skolem designs or Skolem Steiner triple systems for brevity.

We now present Skolem quasigroups and their corresponding Skolem Steiner triple systems.

For $n \in \mathbb{N}$, $n \geq 2$, consider the set $\mathrm{Q} = \{0, 1, 2, \cdots, (2n-1)\}$. Define a permutation $\rho : \mathrm{Q} \to \mathrm{Q}$ by

$$\rho(x) = \begin{cases} \dfrac{2n + x - 1}{2} & \text{if } x \equiv 1 \pmod 2; \\ \dfrac{x}{2} & \text{if } x \equiv 0 \pmod 2. \end{cases}$$

With ρ, a binary operation on the set of elements of Q is defined by

$$x * y = \rho((x + y) \pmod{2n}),$$

for any $x, y \in \mathrm{Q}$. It is easy to see that $(\mathrm{Q}, *)$ defines an even order, commutative and half-idempotent quasigroup.

With such a Skolem quasigroup, the following hold.

3.9 Lemma *Let $x, y \in \mathrm{Q}$. Then*

(i) *if $0 \leq x, y \leq (n-1)$, then $x + y \pmod{2n}$ is the ordinary sum $x + y$;*

(ii) *$x * x = x$ for any $0 \leq x \leq (n-1)$;*

(iii) *$x * x = x - n$ for any $n \leq x < 2n$.*

Proof. (i) $0 \leq x + y < 2n$.

(ii) and (iii) follow by direct calculation. ☐

Equipped with these Skolem quasigroups, it is now apt to define its corresponding designs. The points set of the Skolem design comprises the set

$$V := \mathrm{Q}_{2n} \times \mathbb{Z}_3 \cup \{(p, q)\}.$$

Blocks of the designs are now defined as follows.

Let $\mathcal{B}$ be a collection of 3-element subsets of V of the form:

$$\{(x, 0), (x, 1), (x, 2)\} : 0 \leq x \leq (n-1); \tag{3.3}$$
$$\{(p, q), (x+n, i), (x, (i+1) \pmod 3)) : 0 \leq x \leq (n-1), i \in \mathbb{Z}_3\}; \tag{3.4}$$
$$\{(x, i), (y, i), (x * y, (i+1) \pmod 3)) : x < y, i \in \mathbb{Z}_3, x, y \in \mathrm{Q}\}. \tag{3.5}$$

We refer to blocks of the first kind, **type 1 blocks**, the second kind, **type 2 blocks** and the third kind **type 3 blocks**. We shall say that a block B is valid if B $\in \mathcal{B}$ and invalid if otherwise. It is easy to see that the type 3 blocks in this design coincide with the type 2 blocks of the Bose Steiner triple systems.

We now show that this construction produces Steiner triple systems.

First, we count the number of triples in this construction.

3.10 Lemma *Let $V = \mathrm{Q}_{2n} \times \mathbb{Z}_3 \cup \{(p, q)\}$ and $\mathcal{B}$ be a family of 3-subsets of V as defined in* (3.3), (3.4) *and* (3.5). *Then* $|\mathcal{B}| = \dfrac{v(v-1)}{6}$.

Proof. From type 1 and type 2 triples above, we have that $0 \leq x \leq n-1$. Hence there are n possibilities in the case of type 1 blocks and $3n$ choices for type 2.

The number of triples in type 3 is $3\dbinom{2n}{2} = \dfrac{3(2n)(2n-1)}{2} = 6n^2 - 3n$.

Therefore the total number of triples altogether is $(6n^2 - 3n) + 3n + n = \dfrac{(6n+1)(6n)}{6} = \dfrac{v(v-1)}{6}$. □

We now show that every pair of distinct elements of V occurs in exactly one block.

3.11 Lemma *Let $V = \mathrm{Q}_{2n} \times \mathbb{Z}_3 \cup \{(p,q)\}$ and $\mathcal{B}$ be a family of 3-subsets of V as defined in (3.3), (3.4) and (3.5). Then every pair of distinct elements of V appears in exactly one block of $\mathcal{B}$.*

Proof. Let $(x,i),(y,j)$ be a pair of elements of V.

If $x = y \leq n-1$, then this pair is clearly a type 1 block and occurs in no other block type.

Suppose $x = y \geq n$. Then $i \neq j$, so without loss of generality we have $j = (i+1) \mod 3$. The equation $x * a = x$ has a unique solution $a = z$.

If $z > x$, then the pair occurs in the type 3 blocks. Similarly if $z < x$, then, since the operation $*$ is symmetric, the pair $(x,i),(y,j)$ is also in type 3 and is contained in no other block type.

We now consider the case $x \neq y$.

Without loss of generality, suppose $x < y$, then there are three cases in this regard.

Case 1: If $i = j$, then the pairs appear in the block of the form $\{(x,i),(y,i),(x*y,i+1)\}$ which is clearly of type 3 and appears in no other block, hence it is unique.

Case 2: If $j = (i+1) \mod 3$, then the equation $a * x = y$ has a unique solution $a = z$. Note that for any $x \in \mathrm{Q}$, $x * x \leq x$ and hence $x < y$, $z \neq x$. If $z < x$, then the pair $(x,i),(y,j)$ clearly appears in type 3 blocks. Thus it appears in no other block type. If $z > x$, then, since $*$ is symmetric, the pair $(x,i),(y,j)$ appears in type 3 blocks, and hence appears in no other block type.

Case 3: When $i = j+1 \pmod 3$, we have a similar argument as in case 2.

Next, we consider pairs of the form $(p,q),(x,i)$.

If $x \leq n-1$, then this pair occurs clearly in type 2 block, and in no other block type. If $x \geq n$, then this pair occurs clearly in type 2 block, and in no other block type. $\square$

In view of Lemmas 3.10 and 3.11, we have:

3.12 Theorem *Let $V = \mathrm{Q}_{2n} \times \mathbb{Z}_3 \cup \{(p,q)\}$ and $\mathcal{B}$ be a family of 3-subsets of V as defined in (3.3), (3.4) and (3.5). Then $\mathbb{B} = (V, \mathcal{B})$ is a Steiner triple* *system.*

The triple system defined in Theorem 3.12 above is called the Skolem Steiner triple system.

We now illustrate the Skolem Steiner triple system with an example.

3 Example Let Q $= \{0, 1, \cdots 7\}$. Define a permutation $\rho : \mathrm{Q} \to \mathrm{Q}$ by

$$\rho(x) = \begin{cases} \dfrac{8 + x - 1}{2} & \text{if } x \equiv 1 \pmod 2; \\ \dfrac{x}{2} & \text{if } x \equiv 0 \pmod 2). \end{cases}$$

With ρ, let $* : \mathrm{Q} \times \mathrm{Q} \to \mathrm{Q}$ be defined by

$$x * y = \rho((x + y) \pmod 8),$$

for any $x, y \in \mathrm{Q}$.

The table below describes the Skolem quasigroup $(\mathrm{Q}, *)$ of order 8.

Table 3.2: Skolem quasigroup of order 8

$*$	0	1	2	3	4	5	6	7
0	**0**	4	1	5	2	6	3	7
1	4	**1**	5	2	6	3	7	0
2	1	5	**2**	6	3	7	0	4
3	5	2	6	**3**	7	0	4	1
4	2	6	3	7	**0**	4	1	5
5	6	3	7	0	4	**1**	5	2
6	3	7	0	4	1	5	**2**	6
7	7	0	4	1	5	2	6	**3**

Now, let $V = \mathrm{Q}_8 \times \mathbb{Z}_3 \cup \{(p, q)\}$, and let $\mathcal{B}$ be a family of 3-subsets of V as defined in (3.3), (3.4) and (3.5). This is shown below:

Type 1 :

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

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

Type 2 :

$$\{\{(p,q),(4,0),(0,1)\},\{(p,q),(4,1),(0,2)\},\{(p,q),(4,2),(0,0)\}$$
$$\{(p,q),(5,0),(1,1)\},\{(p,q),(5,1),(1,2)\},\{(p,q),(5,2),(1,0)\}$$
$$\{(p,q),(6,0),(2,1)\},\{(p,q),(6,1),(2,2)\},\{(p,q),(6,2),(2,0)\}$$
$$\{(p,q),(7,0),(3,1)\},\{(p,q),(7,1),(3,2)\},\{(p,q),(7,2),(3,0)\}\}$$

Type 3 :

$$\{\{(0,0),(1,0),(0*1=4,1)\},\{(0,1),(1,1),(4,2)\},\{(0,2),(1,2),(4,0)\}$$
$$\{(0,0),(2,0),(0*2=1,1)\},\{(0,1),(2,1),(1,2)\},\{(0,2),(2,2),(1,0)\}$$
$$\{(0,0),(3,0),(0*3=5,1)\},\{(0,1),(3,1),(5,2)\},\{(0,2),(3,2),(5,0)\}$$
$$\{(0,0),(4,0),(0*4=2,1)\},\{(0,1),(4,1),(2,2)\},\{(0,2),(4,2),(2,0)\}$$
$$\{(0,0),(5,0),(0*5=6,1)\},\{(0,1),(5,1),(6,2)\},\{(0,2),(5,2),(6,0)\}$$
$$\{(0,0),(6,0),(0*6=3,1)\},\{(0,1),(6,1),(3,2)\},\{(0,2),(6,2),(3,0)\}$$
$$\{(0,0),(7,0),(0*7=7,1)\},\{(0,1),(7,1),(7,2)\},\{(0,2),(7,2),(7,0)\}$$
$$\{(1,0),(2,0),(1*2=5,1)\},\{(1,1),(2,1),(5,2)\},\{(1,2),(2,2),(5,0)\}$$
$$\{(1,0),(3,0),(1*3=2,1)\},\{(1,1),(3,1),(2,2)\},\{(1,2),(3,2),(2,0)\}$$
$$\{(1,0),(4,0),(1*4=6,1)\},\{(1,1),(4,1),(6,2)\},\{(1,2),(4,2),(6,0)\}$$
$$\{(1,0),(5,0),(1*5=3,1)\},\{(1,1),(5,1),(3,2)\},\{(1,2),(5,2),(3,0)\}$$
$$\{(1,0),(6,0),(1*6=7,1)\},\{(1,1),(6,1),(7,2)\},\{(1,2),(6,2),(7,0)\}$$
$$\{(1,0),(7,0),(1*7=0,1)\},\{(1,1),(7,1),(0,2)\},\{(1,2),(7,2),(0,0)\}$$
$$\{(2,0),(3,0),(2*3=6,1)\},\{(2,1),(3,1),(6,2)\},\{(2,2),(3,2),(6,0)\}$$
$$\{(2,0),(4,0),(2*4=3,1)\},\{(2,1),(4,1),(3,2)\},\{(2,2),(4,2),(3,0)\}$$
$$\{(2,0),(5,0),(2*5=7,1)\},\{(2,1),(5,1),(7,2)\},\{(2,2),(5,2),(7,0)\}$$
$$\{(2,0),(6,0),(2*6=0,1)\},\{(2,1),(6,1),(0,2)\},\{(2,2),(6,2),(0,0)\}$$
$$\{(2,0),(7,0),(2*7=4,1)\},\{(2,1),(7,1),(4,2)\},\{(2,2),(7,2),(4,0)\}$$
$$\{(3,0),(4,0),(3*4=7,1)\},\{(3,1),(4,1),(7,2)\},\{(3,2),(4,2),(7,0)\}$$

$\{(3,0),(5,0),(3*5=0,1)\},\{(3,1),(5,1),(0,2)\},\{(3,2),(5,2),(0,0)\}$
$\{(3,0),(6,0),(3*6=4,1)\},\{(3,1),(6,1),(4,2)\},\{(3,2),(6,2),(4,0)\}$
$\{(3,0),(7,0),(3*7=1,1)\},\{(3,1),(7,1),(1,2)\},\{(3,2),(7,2),(1,0)\}$
$\{(4,0),(5,0),(4*5=4,1)\},\{(4,1),(5,1),(4,2)\},\{(4,2),(5,2),(4,0)\}$
$\{(4,0),(6,0),(4*6=1,1)\},\{(4,1),(6,1),(1,2)\},\{(4,2),(6,2),(1,0)\}$
$\{(4,0),(7,0),(4*7=5,1)\},\{(4,1),(7,1),(5,2)\},\{(4,2),(7,2),(5,0)\}$
$\{(5,0),(6,0),(5*6=5,1)\},\{(5,1),(6,1),(5,2)\},\{(5,2),(6,2),(5,0)\}$
$\{(5,0),(7,0),(5*7=2,1)\},\{(5,1),(7,1),(2,2)\},\{(5,2),(7,2),(2,0)\}$
$\{(6,0),(7,0),(6*7=6,1)\},\{(6,1),(7,1),(6,2)\},\{(6,2),(7,2),(6,0)\}\}.$

Clearly, every pair of distinct elements of V occurs together in exactly one block of $\mathcal{B}$. There are 4 type 1 triples, 12 type 2 triples and 84 type 3 triples. Hence $(V,\mathcal{B})$ is a Steiner triple system of order 25.

In general, there are $\dfrac{(v-1)}{6}$ type 1 triples, $\dfrac{(v-1)}{2}$ type 2 triples and $\dfrac{(v-1)(v-4)}{6}$ type 3 triples in any Skolem Steiner triple system of order v.

In view of Lemmas 3.1, 3.7 and 3.11, we have proved Theorem 3.3.

Next, we consider Steiner triple systems from projective and affine spaces.

3.3 Steiner triple systems from the projective and affine planes

In this section, we are interested in Steiner triple systems from vector spaces constructed over a field.

3.1 Definition Let $\mathbb{F}_q^{n+1}$ be a vector space of rank $(n+1)$ over GF(q). The projective space PG(n,q) is the geometry whose points, lines, planes, $\ldots$, hyperplanes are the subspaces of $\mathbb{F}_q^{n+1}$ of rank $1,2,3,\cdots,n$ respectively.

The dimension of a subspace of PG(n,q) is one less than the rank of a subspace of $\mathbb{F}_2^{n+1}$.

3.2 Definition Let $\mathbb{F}_q^n$ be a vector space of rank n over GF(q). The affine space AG(n, q) is the geometry whose points, lines, planes, $\ldots$, hyperplanes are the cosets of the subspaces of a vector space $\mathbb{F}_q^n$ of rank $1, 2, 3, \cdots, n$ respectively.

The projective plane is an extension of an affine plane. An affine plane of order n can be obtained from a projective plane of the same order by removing one line and all of the points on it from a projective plane.

For brevity, we shall call the Steiner triple systems from the projective and affine planes the *projective triple systems* and *affine triple systems* respectively.

We now consider the construction of projective Steiner triple systems.

3.3.1 Projective triple systems

Let $\mathbb{F}_2$ be a field of order 2. Let $\mathbb{F}_2^{n+1}$ be a vector space of dimension $(n+1)$ over a finite field of order 2. Then $\mathbb{F}_2^{n+1}$ can be realized concretely as the set of all $(n+1)$-tuples of elements of $\mathbb{F}_2$, so that $|\mathbb{F}_2^{n+1}| = 2^{n+1}$. Consider the set $V = \mathbb{F}_2^{n+1} \setminus \{\mathbf{0}\}$.

The set $V = \mathbb{F}_2^{n+1} \setminus \{\mathbf{0}\}$ is considered as a set of points of Steiner triple systems.

3.13 Proposition [14] *Let V be the set of all non-zero vectors in $\mathbb{F}_2^{n+1}$, and let $\mathcal{B} = \{\{v_1, v_2, v_3\} : \{v_1, v_2, v_3\}$ is distinct, $v_1 + v_2 + v_3 = 0\}$. Then $(V, \mathcal{B})$ is a Steiner triple system of order $2^{(n+1)} - 1$.*

Proof. It is clear that, if $v_1 + v_2 + v_3 = 0$, then any two of v_1, v_2, v_3 determine the third. We have to show that, if v_1 and v_2 are distinct and non-zero, then v_3 is distinct from both and non-zero. So suppose that $0 \neq v_1 \neq v_2 \neq 0$, then $v_3 = -(v_1 + v_2) = v_1 + v_2$.

Since $v_2 \neq 0$, then $v_3 \neq v_1$. Similarly, since $v_3 \neq 0$, we must have $v_3 \neq v_2$.

Now, since $v_1 \neq v_2$, it follows that $v_3 = v_1 + v_2 = v_1 - v_2 \neq 0$.

In consideration of $v_1 + v_2 + v_3 = 0$ and $v_1 \neq v_2 \neq v_3 \neq 0$, it follows that each pair of elements of V appears in a unique triple and hence the result. $\square$

This system is called a projective Steiner triple system of order $2^{(n+1)} - 1$ or a projective plane of dimension n and of order 2. It is denoted $\mathrm{PG}(n, 2)$.

As seen above, they are realized from a vector space $V = \mathbb{F}_2^{n+1}$ of a dimension higher than the projective plane. The projective plane $\mathrm{PG}(n, 2)$ is of dimension n and not $(n+1)$. This is because in projective geometry, lines through the origin consist of just two points of which the origin is one. We can thus identify the lines through the origin with this point and we can identify any point of $\mathrm{PG}(n, 2)$ with the non-zero vector spanning the corresponding line.

We illustrate this with an example.

4 Example Let $\mathbb{F}_2^4$ be a vector space of dimension 4 over $\mathbb{F}_2$. Then $\mathbb{F}_2^4$ consists of the 16 vectors:

$$(0,0,0,0),(0,0,0,1),(0,0,1,0),(0,0,1,1),(0,1,0,0),(0,1,0,1),(0,1,1,0),$$

$$(0,1,1,1),(1,0,0,0),(1,0,0,1),(1,0,1,0),(1,0,1,1),(1,1,0,0),(1,1,0,1),$$

$(1,1,1,0)$ and $(1,1,1,1)$.

Now, consider the set $V = \mathbb{F}_2^4 \setminus \{(0,0,0,0)\}$. That is,

$V = \{(0,0,0,1),(0,0,1,0),(0,0,1,1),(0,1,0,0),(0,1,0,1),(0,1,1,0),$

$(0,1,1,1),(1,0,0,0),(1,0,0,1),(1,0,1,0),(1,0,1,1),(1,1,0,0),(1,1,0,1),$

$(1,1,1,0),(1,1,1,1)\}$.

Then consider the family $\mathcal{B}$ of 3-element subsets of the set V such that for all $v_1, v_2, v_3 \in V$, $\{v_1, v_2, v_3\}$ is distinct and $v_1 + v_2 + v_3 = 0$. This is shown below:

$\mathcal{B} = \{\{(0,0,0,1),(0,0,1,0),(0,0,1,1)\},\{(0,0,0,1),(0,1,0,0),(0,1,0,1)\},$

$\{(0,0,0,1),(0,1,1,0),(0,1,1,1)\},\{(0,0,0,1),(1,0,0,0),(1,0,0,0)\},$

$\{(0,0,0,1),(1,0,1,0),(1,0,1,1)\},\{(0,0,0,1),(1,1,0,0),(1,1,0,1)\},$

$\{(0,0,0,1),(1,1,1,0),(1,1,1,1)\},\{(0,0,1,0),(0,1,0,0),(0,1,1,0)\},$

$\{(0,0,1,0),(0,1,0,1),(0,1,1,1)\},\{(0,0,1,0),(1,0,0,0),(1,0,1,0)\},$

$\{(0,0,1,0),(1,0,0,1),(1,0,1,1)\},\{(0,0,1,0),(1,1,0,0),(1,1,1,0)\},$

$\{(0,0,1,0),(1,1,0,1),(1,1,1,1)\},\{(0,0,1,1),(0,1,0,0),(0,1,1,1)\},$

$\{(0,0,1,1),(0,1,0,1),(0,1,1,0)\},\{(0,0,1,1),(1,0,0,0),(1,0,1,1)\},$

$\{(0,0,1,1),(1,0,0,1),(1,0,1,0)\},\{(0,0,1,1),(1,1,0,0),(1,1,1,1)\},$

$\{(0,1,0,0),(1,0,0,0),(1,1,0,0)\},\{(0,1,0,0),(1,0,0,1),(1,1,0,1)\},$

$\{(0,1,0,0),(1,0,1,0),(1,1,1,0)\},\{(0,1,0,0),(1,0,1,1),(1,1,1,1)\},$

$\{(0,1,0,1),(1,0,0,0),(1,1,0,1)\},\{(0,1,0,1),(1,0,0,1),(1,1,0,0)\},$

$\{(0,1,0,1),(1,0,1,0),(1,1,1,1)\},\{(0,1,0,1),(1,0,1,1),(1,1,1,0)\},$

$\{(0,1,1,0),(1,0,0,0),(1,1,1,0)\},\{(0,1,1,0),(1,0,0,1),(1,1,1,1)\},$

$\{(0,1,1,0),(1,0,1,0),(1,1,0,0)\},\{(0,1,1,0),(1,0,1,1),(1,1,0,1)\},$

$\{(0,1,1,1),(1,0,0,0),(1,1,1,1)\},\{(1,0,0,1),(0,1,1,1),(1,1,1,0)\},$

$\{(1,0,1,0),(0,1,1,1),(1,1,0,1)\},\{(1,0,1,1),(0,1,1,1),(1,1,0,0)\},$

$\{(1,1,0,1),(0,0,1,1),(1,1,1,0)\}\}$.

Clearly, every pair of elements of the set V appears together in a unique triple. Hence, in view of Proposition 3.13, $(V,\mathcal{B})$ is a Steiner triple system of order 15.

We now turn to affine triple systems.

3.3.2 Affine triple systems

Here, we consider the construction involving the field $\mathbb{F}_3$.

Let $\mathbb{F}_3$ be a field of order 3 and let $\mathbb{F}_3^n$ be a vector space of dimension n over $\mathbb{F}_3$. Then $\mathbb{F}_3^n$ can be realized concretely as the set of all $n-$tuples of elements of $\mathbb{F}_3$, so that $|\mathbb{F}_3^n| = 3^n$.

We now show the vector space described above together with certain subspaces is a Steiner triple system.

3.14 Proposition [14] *Let $\mathbb{F}_3^n$ be a vector space of dimension n over a finite field of order 3. Let V be the set of all vectors in $\mathbb{F}_3^n$, and let $\mathcal{B} = \{\{v_1,v_2,v_3\} \subseteq V : \{v_1,v_2,v_3\}$ is distinct, $v_1+v_2+v_3 = 0\}$. Then $(V,\mathcal{B})$ form a Steiner triple system.*

Proof. If $v_1 + v_2 + v_3 = 0$, then any two of v_1, v_2, v_3 determine the third. Suppose that $v_1 \neq v_2$, then $v_3 \neq v_1$. If $v_1 = v_3 = -(v_1 + v_2)$ then $v_2 = -2v_1 = v_1$. Similarly $v_3 \neq v_2$, so all the three points are distinct.

In consideration of $v_1 + v_2 + v_3 = 0$ and $v_1 \neq v_2 \neq v_3 \neq 0$, it follows that each pair of elements of V appears in a unique triple and hence the result.

□

This system is called an affine triple system or affine plane of dimension n over $\mathbb{F}_3$, denoted $\mathrm{AG}(n, 3)$. The affine plane is of order 3 and it is a Steiner triple system of 3^n.

We illustrate with an example.

5 Example Let $\mathbb{F}_3^2$ be a vector space of dimension 2 over the field $\mathbb{F}_3$. Then $\mathbb{F}_3^2$ consists of the 9 vectors

$$(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,1) \text{ and } (2,2).$$

Now, let V be the set of all vectors of $\mathbb{F}_3^2$. That is,

$$V = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,1), (2,2)\}.$$

Consider the family $\mathcal{B}$ of all 3-element subsets of V such that for all $v_1, v_2, v_3 \in V$, $\{v_1, v_2, v_3\}$ is distinct and $v_1 + v_2 + v_3 = 0$ as shown below.

$$\begin{aligned}\mathcal{B} = \{&\{(0,0), (0,1), (0,2)\}, \{(0,0), (1,0), (2,0)\}, \{(0,0), (1,1), (2,2)\},\\ &\{(0,0), (1,2), (2,1)\}, \{(1,0), (1,1), (1,2)\}, \{(0,1), (1,1), (2,1)\},\\ &\{(0,1), (1,2), (2,0)\}, \{(0,1), (1,0), (2,2)\}, \{(2,0), (2,1), (2,2)\},\\ &\{(0,2), (1,2), (2,2)\}, \{(0,2), (1,0), (2,1)\}, \{(0,2), (1,1), (2,0)\}\}.\end{aligned}$$

Clearly, every pair of elements of the set V appears together in a unique triple. Hence, in view of Proposition 3.14, $(V, \mathcal{B})$ is a Steiner triple system of order 9.

Having presented the fundamental structures of this study, we proceed to discuss their automorphism groups.

Chapter 4

Automorphism groups of Steiner triple systems

In this chapter we investigate the automorphism groups of the designs of Steiner triple systems of our consideration in Chapter 4. Our interest is to determine which permutations lead to identical forms of the designs.

The essence of investigating the automorphisms of these designs discussed in this course of study is to look at their symmetry and compare these automorphism groups to that of their graphs.

We begin with the Bose Steiner triple systems.

4.1 Automorphism groups of Bose Steiner triple systems

In this section, we present the full automorphism groups of Bose Steiner triple systems $\mathbb{B} = (V, \mathcal{B})$ from the construction involving an odd order abelian group G as discussed in Section 3.1, following Lovegrove [8].

Two crucial classes of automorphisms of the Bose Steiner triple systems are the translations by the points of the design, and an action of the automorphism of the group used in constructing the design.

We now explore the full automorphism groups of the Bose Steiner triple systems. We begin by giving the appropriate structures of the translations and the automorphism of the group used in the construction of Bose Steiner triple systems $\mathbb{B} = (V, \mathcal{B})$.

4.1 Lemma *Let G be an abelian group, $V = G \times \mathbb{Z}_3$ and $\mathbb{B} = (V, \mathcal{B})$ be a Bose Steiner triple system of order v. For each $(x, i) \in V$ and an $a \in G$, define a map $\sigma_a : V \to V$ by*

$$\sigma_a(x, i) = (x + a, i).$$

Then σ_a is an automorphism of $\mathbb{B}$.

Proof. For $(x, i), (y, j) \in V$, suppose $\sigma_a(x, i) = \sigma_a(y, j)$. Then

$$\begin{aligned}
&(x + a, i) = (y + a, j), \\
&\implies x + a = y + a \text{ and } i = j, \\
&\implies x = y.
\end{aligned}$$

Hence σ_a is injective. By the pigeonhole principle, σ_a is surjective since we are considering finite sets.

It therefore follows that σ_a is a bijection.

Now, let $\mathrm{B} = \{(x, 0), (x, 1), (x, 2)\}$ be a type 1 block of $\mathcal{B}$. Then

$$\sigma_a(\mathrm{B}) = \{(x + a, 0), (x + a, 1), (x + a, 2)\}.$$

Clearly, $\sigma_a(\mathrm{B})$ is a type 1 block of $\mathcal{B}$.

Let $\mathrm{B}' = \{(x, i), (y, i), (x * y, i + 1)\}$ be a type 2 block of $\mathcal{B}$. Then

$$\begin{aligned}
\sigma_a(\mathrm{B}') &= \{(x + a, i), (y + a, i), ((x * y) + a), i + 1)\} \\
&= \{(x + a, i), (y + a, i), (\left(\frac{x + y}{2}\right) + a, i + 1)\} \\
&= \{(x + a, i), (y + a, i), (\left(\frac{x + y}{2} + \frac{2a}{2}\right), i + 1)\} \\
&= \{(x + a, i), (y + a, i), (\left(\frac{(x + a) + (y + a)}{2}\right), i + 1)\} \\
&= \{(x + a, i), (y + a, i), ((x + a) * (y + a), i + 1)\}.
\end{aligned}$$

Clearly, $\sigma_a(\mathrm{B}')$ is a type 2 block of $\mathcal{B}$. Therefore, we conclude that σ_a preserves the block of $\mathbb{B}$ and the result follows.

$\square$

4.2 Lemma *Let $V = G \times \mathbb{Z}_3$ and $\mathbb{B} = (V, \mathcal{B})$ be a Bose Steiner triple system of order v. For each $(x, i) \in V$ and $j \in \mathbb{Z}_3$, define a map $\sigma_j : V \to V$ by*

$$\sigma_j(x, i) = (x, i + j).$$

Then σ_j is an automorphism of $\mathbb{B}$.

Proof. Let $(x, i), (y, i') \in V$. Suppose $\sigma_j(x, i) = \sigma_j(y, i')$. Then

$$\begin{aligned}(x, i + j) &= (y, i' + j),\\ &\Longrightarrow x = y \text{ and } i + j = i' + j,\\ &\Longrightarrow i = i'.\end{aligned}$$

Hence σ_j is injective. By the pigeonhole principle, σ_j is surjective since we are considering $\mathbb{Z}_3$.

It therefore follows that σ_j is a bijection.

Let $\mathrm{B} = \{(x, 0), (x, 1), (x, 2)\}$ be a type 1 block of $\mathcal{B}$. Then

$$\sigma_j(\mathrm{B}) = \{(x, 0 + j), (x, 1 + j), (x, 2 + j)\}.$$

Clearly, $\sigma_j(\mathrm{B})$ is a type 1 block of $\mathcal{B}$.

Let $\mathrm{B}' = \{(x, i), (y, i), (x * y, i + 1)\}$ be a type 2 block of $\mathcal{B}$. Then

$$\sigma_j(\mathrm{B}') = \{(x, i + j), (y, i + j), (x * y, i + 1 + j)\}.$$

Clearly, $\sigma_j(\mathrm{B}')$ is a type 2 block of $\mathcal{B}$. Therefore, we conclude that σ_j preserves the block of $\mathbb{B}$ and the result follows.

$\square$

4.3 Lemma *Let G be an abelian group, $V = G \times \mathbb{Z}_3$, $\alpha \in$ Aut G and $\mathbb{B} = (V, \mathcal{B})$ be a Bose Steiner triple system of order v. For each $(x, i) \in V$, define a map $\sigma_\alpha : V \to V$ by*

$$\sigma_\alpha(x, i) = (\alpha(x), i).$$

Then σ_α is an automorphism of $\mathbb{B}$.

Proof. For $(x,i),(y,j) \in V$, suppose $\sigma_\alpha(x,j) = \sigma_\alpha(y,i)$. Then

$$\begin{aligned}
(\alpha(x), i) &= (\alpha(y), j), \\
\Longrightarrow \alpha(x) &= \alpha(y) \text{ and } i = j, \\
\Longrightarrow x = y &\text{ and } i = j.
\end{aligned}$$

Hence σ_α is injective. By the pigeonhole principle, σ_α is surjective since we are considering finite sets.

It therefore follows that σ_α is a bijection.

Let $\mathrm{B} = \{(x,0),(x,1),(x,2)\}$ be a type 1 block of $\mathcal{B}$. Then

$$\sigma_\alpha(\mathrm{B}) = \{(\alpha(x),0),(\alpha(x),1),(\alpha(x),2)\}.$$

Clearly, $\sigma_\alpha(\mathrm{B})$ is a type 1 block of $\mathcal{B}$.

Let $\mathrm{B}' = \{(x,i),(y,i),(x*y,i+1)\}$ be a type 2 block of $\mathcal{B}$. Then

$$\sigma_a(\mathrm{B}') = \{(\alpha(x),i),(\alpha(y),i),(\alpha(x)*\alpha(y),i+1)\}$$

Clearly, $\sigma_\alpha(\mathrm{B}')$ is a type 2 block of $\mathcal{B}$. Therefore, we conclude that σ_a preserves the blocks of $\mathbb{B}$ and the result follows.

□

Lemmas 4.1, 4.2 and 4.3 above can be rewritten as:

4.4 Proposition *Let* $\mathbb{B} = (V,\mathcal{B})$ *be a Bose Steiner triple system,* $\alpha \in \mathrm{Aut}\ G$, $i' \in \mathbb{Z}_3$ *and* $a \in G$. *Let* $\mathrm{B} \in \mathcal{B}$. *Define a map* $\sigma_{\alpha,a,i'} : V \to V$ *by*

$$\sigma_{\alpha,a,i'}(\mathrm{B}) = \{(a+\alpha(x), i'+i),(a+\alpha(x), i'+j),(a+\alpha(x), i'+k)\}.$$

Then $\sigma_{\alpha,a,i'} \in \mathrm{Aut}\ \mathbb{B}$.

Clearly, $\sigma_{\alpha,a,i'}$ preserves the blocks of Bose Steiner triple systems. It takes a block type to the same block type. It will be evident that the sets of automorphisms describe above generates the automorphisms of the design.

Having identified some of the automorphisms of the design, we now explore the symmetry of the Bose Steiner triple systems. We consider the actions of automorphisms on the blocks of this design. First, we consider the simplest possibility of having the two block types of the design together.

4.5 Lemma *Let $x_m, y_m, z_m \in G$ and $i_r, j_r, k_r \in \mathbb{Z}_3$ where $m = r = \{0,1,2\}$. Consider the 3×3 matrix M with the usual matrix notation and entries from $G \times \mathbb{Z}_3$. That is, M is of the form:*

$$\mathrm{M} = \begin{pmatrix} (x_0, i_0) & (x_1, j_0) & (x_2, k_0) \\ (y_0, i_1) & (y_1, j_1) & (y_2, k_1) \\ (z_0, i_2) & (z_1, j_2) & (z_2, k_2) \end{pmatrix} \tag{4.1}$$

If the rows and columns of M are distinct triples of a Bose Steiner triple system $\mathbb{B}$. Then all the rows of M are of the same block type and the columns are of the other block type.

Proof. There must be at least two rows or two columns of the same block type, since M is a 3×3 matrix and that every Bose Steiner triple system consists of 2 block types. Without loss of generality, suppose the first two rows are of type 1. Then it follows that $x_0 = x_1 = x_2$ and $y_0 = y_1 = y_2$.

Suppose without loss of generality that $i_0 = i_1$, since $i_0, i_1, i_2, j_0, j_1, j_2, k_1, k_2$ and k_3 are all elements of $\mathbb{Z}_3$, and that $y_0 = y_1 = y_2$. Then it follows that z_0 must be equal to $\frac{(x_0 + y_0)}{2}$, since $x_0 \neq y_0$.

Now, since $i_0 = i_1$, $x_0 = x_1 = x_2$, $y_0 = y_1 = y_2$, $i_1 \neq j_1 \neq k_1$ and $i_0 \neq j_0 \neq k_0$. It follows without loss of generality that $j_0 = j_1$ and $k_0 = k_1$. Hence, $j_2 = j_0 + 1 = j_1 + 1$, and $k_2 = k_0 + 1 = k_1 + 1$.

We must have that $j_2 = j_0 + 1 = j_1 + 1$ and $z_1 = \frac{(x_1 + y_1)}{2}$, since $j_0 = j_1$. Similarly, since $k_0 = k_1$, we must have that $k_2 = k_0 + 1 = k_1 + 1$ and $z_2 = \frac{(x_2 + y_2)}{2}$.

Finally, since $i_1 \neq j_1 \neq k_1$ and $i_2 \neq j_2 \neq k_2$, it follows that $z_0 = z_1 = z_2 = \frac{(x_0 + y_0)}{2} = \frac{(x_1 + y_1)}{2} = \frac{(x_2 + y_2)}{2}$. $\square$

Lemma 4.5 above can be generalized as follows:

Consider M of the form:

$$\begin{pmatrix} (x, i) & (x, j) & (x, k) \\ (y, i) & (y, j) & (y, k) \\ (\frac{(x+y)}{2}, i+1) & (\frac{(x+y)}{2}, j+1) & (\frac{(x+y)}{2}, k+1) \end{pmatrix} \tag{4.2}$$

where $x, y \in G$, and $i, j, k \in \mathbb{Z}_3$ such that

$$i + j + k = (i + 1) + (j + 1) + (k + 1) \equiv 0 \pmod 3, \text{ and}$$

$$i + i + (i + 1) = j + j + (j + 1) = k + k + (k + 1) \equiv 1 \pmod 3.$$

In order words, all the rows of M are type 1 blocks while the columns are type 2 or vice versa.

A consequence of the Lemma 4.5 above is the following:

4.6 Corollary [8] *Let* M *be a* 3×3 *matrix with entries from* $G \times \mathbb{Z}_3$, *such that rows and columns are distinct triples of a Bose Steiner triple system* $\mathbb{B} = (V, \mathcal{B})$. *Then*

(i) *all the rows of* M *have the same signature;*

(ii) *all the columns of* M *have the same signature;*

(iii) *if all rows* (columns) *have signature* 0, *then all columns* (rows) *have signature* 1.

A peculiar case of the matrix M described in (4.1) above is the unique Steiner triple system of order 9.

4.7 Lemma *Let* $x_0 \neq y_0 \neq z_0$, *such that* $x_m, y_m, z_m \in G$ *and* $i_r, j_r, k_r \in \mathbb{Z}_3$ *where* $m = r = \{0, 1, 2\}$. *Consider the* 3×3 *matrix* M *with the usual matrix notation and entries from* $G \times \mathbb{Z}_3$. *That is,* M *is of the form:*

$$\mathrm{M} = \begin{pmatrix} (x_0, i_0) & (x_1, j_0) & (x_2, k_0) \\ (y_0, i_1) & (y_1, j_1) & (y_2, k_1) \\ (z_0, i_2) & (z_1, j_2) & (z_2, k_2) \end{pmatrix} \tag{4.3}$$

If the rows and columns of M *are distinct triples of a Bose Steiner triple system* $\mathbb{B}$, *then all rows and columns of* M *are all type* 2 *blocks.*

Proof. Suppose the first two rows of the matrix M above are of type 2 blocks. We have that $x_0 \neq x_1, y_0 \neq y_1, x_2 = \dfrac{x_0 + x_1}{2}, y_2 = \dfrac{y_0 + y_1}{2}$, and $k_0 = i_0 + 1 = j_0 + 1$ since i_0 must be equal to j_0 and $k_1 = i_1 + 1 = j_1 + 1$ since i_1 must be equal to j_1. Since $x_0 \neq y_0 \neq z_0$, then $x_2 \neq y_2$. This implies $z_2 = \dfrac{(x_2 + y_2)}{2}$ and therefore $k_0 = k_1$. It then follows that $i_0 = i_1$ and $j_0 = j_1$.

Now, since $x_0 \neq y_0 \neq z_0$ and $x_2 \neq y_2 \neq z_2$ it follows that the last row must be a type 2 block. $\square$

Lemma 4.7 above generalizes to matrices of the form:

$$\begin{pmatrix} (x_0, i_0) & (x_1, i_0) & (\frac{x_0 + x_1}{2}, i_0 + 1) \\ (y_0, j_0) & (y_1, j_0) & (\frac{y_0 + y_1}{2}, j_0 + 1) \\ (\frac{(x_0 + y_0)}{2}, i_0 + 1) & (\frac{(x_1 + y_1)}{2}, i_0 + 1) & (\frac{(x_0 + y_0) + (x_1 + y_1)}{2}, i_0 + 1) \end{pmatrix}$$

Here, all rows and columns of M are all type 2 blocks and

$$\frac{(x_0 + y_0) + (x_1 + y_1)}{2} = \frac{(x_0 + x_1) + (y_0 + y_1)}{2}. \tag{4.4}$$

Remark *The condition* $\dfrac{(x_0 + y_0) + (x_1 + y_1)}{2} = \dfrac{(x_0 + x_1) + (y_0 + y_1)}{2}$ *in* (4.4) *above is only a possibility if the distinct rows and columns of the matrix* M *are from a Bose Steiner triple system of order 9.*

Equipped with the results so far, we now begin to classify automorphisms which exist on Bose Steiner triple systems.

4.8 Lemma [8] *Let* $\mathbb{B} = (V, \mathcal{B})$ *be a Bose Steiner triple system and* $\sigma \in \operatorname{Aut} \mathbb{B}$. *Then* σ *maps the type* 1 *blocks of* $\mathbb{B}$ *either all to type* 1 *blocks or all to type* 2 *blocks.*

Proof. Let $x, y \in G$ such that $x \neq y$. Consider the matrix

$$\mathrm{M} = \begin{pmatrix} (x, 0) & (x, 1) & (x, 2) \\ (y, 0) & (y, 1) & (y, 2) \\ (\frac{(x + y)}{2}, 1) & (\frac{(x + y)}{2}, 2) & (\frac{(x + y)}{2}, 0) \end{pmatrix}$$

By Corollary 4.6, suppose σ maps a particular row or column to a type 1 block. Then other rows or columns are mapped in the same way. $\square$

To this end, automorphisms of the Bose Steiner triple system are classified as type 1 or type 2 according to whether it maps type 1 blocks to type 1 blocks or to type 2 blocks.

Automorphisms are also classified according to the permutation of their labels.

4.1 Definition Let $\mathbb{B} = (V, \mathcal{B})$ be a Bose Steiner triple system. An automorphism $\sigma \in \text{Aut } \mathbb{B}$ is said to be *even type* 1 or *odd type* 1, if σ maps type 1 blocks to type 1 blocks, and permutes the labels evenly or oddly, respectively.

4.9 Lemma [8] *Let* $\mathbb{B} = (V, \mathcal{B})$ *be a Bose Steiner triple system and* $\sigma \in \text{Aut } \mathbb{B}$ *be a type* 1 *automorphism. Then* σ *maps the type 1 blocks of* $\mathbb{B}$ *either all as even type* 1 *or all as odd type* 1.

Proof. Consider the image $\sigma(\text{M})$ of the matrix M of Lemma 4.8. Suppose that a particular row is mapped as even type 1 and another as odd type 1. Then the values of the labels of the individual points of the even type 1 block can be written as $(i,\ i+1,\ i+2,)$, and that of the odd type 1 block as $(j,\ j+2,\ j+1)$.

By Corollary 4.6, all columns of $\sigma(\text{M})$ must have signature 1. Hence the label values of the third row must be $1 - i - j$. Clearly this is not a valid block of $\mathcal{B}$. □

From the results so far, automorphisms of the Bose Steiner triple systems will be classified in the following:

(i) An automorphism $\sigma \in \text{Aut } \mathbb{B}$ is type 1 if $\sigma(\text{B})$ is a type 1 block for all type 1 block $\text{B} \in \mathcal{B}$.

(ii) An automorphism $\sigma \in \text{Aut } \mathbb{B}$ is type 2, if σ maps the type 1 blocks of $\mathcal{B}$ to type 2.

Similarly, $\sigma \in \text{Aut } \mathbb{B}$ is classified as even type 1 or odd type 1 according to Definition 4.1. We illustrate these classifications of automorphisms in the diagram below.

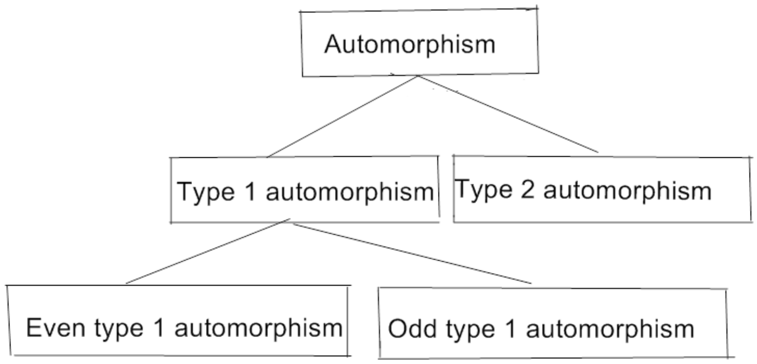


Figure 4.1: Types of automorphisms on Bose Steiner triple systems

The next result shows that the automorphism groups of the Bose Steiner triple systems are all even type 1 except in some special cases where they are odd type 1 or type 2.

4.10 Theorem [8] *Let* $\mathbb{B} = (V, \mathcal{B})$ *be a Bose Steiner triple system and* $\sigma \in \operatorname{Aut} \mathbb{B}$. *If* σ *is either odd type* 1 *or type* 2, *then* $G \cong \mathbb{Z}_3$, *and* $\mathbb{B}$ *is the unique* STS(9).

Proof. First, we consider the odd type 1 automorphisms. Suppose to the contrary that $G \ncong \mathbb{Z}_3$. Then, let x, y be any two non-zero elements of G such that $x \neq y$ and $x \neq 2y$. Let B be the type 1 block $\{(0,0),(0,1),(0,2)\}$. Without loss of generality, let $i, i+2, i+1$ be the label values of σ(B). Now, consider the matrix

$$\mathrm{M} = \begin{pmatrix} (2y-x,0) & (x,0) & (y,1) \\ (x-2y,0) & (-x,0) & (-y,1) \\ (0,1) & (0,1) & (0,2) \end{pmatrix}.$$

All columns and the first two rows of M are type 2 blocks. By Lemma 4.8 they go to type 2 blocks. The signatures of the columns sum to zero. The signature of the top two rows are both 1. The signature of the bottom row is $(i+2)+(i+2)+(i+1) = 2$ which contradicts the fact that no block has signature 2.

We now consider the type 2 automorphism.

Suppose σ is type 2. This implies that each type 1 block is the image of a type 2 block. Clearly, the composition of a type 2 automorphism with a translation is still type 2. So, suppose $\mathrm{B} = \{(x,0),(-x,0),(0,1)\}$ is mapped to $\{(0,0),(0,1),(0,2)\}$, for some non-zero $x \in G$ without changing the type 2 property of σ. Let

$$\mathrm{M} = \begin{pmatrix} (x,2) & (-x,2) & (0,0) \\ (x,1) & (-x,1) & (0,2) \\ (x,0) & (-x,0) & (0,1) \end{pmatrix}.$$

Then by Corollary 4.6, $\sigma(\mathrm{M})$ has type 1 blocks as rows and type 2 blocks as columns. Now, suppose $G \ncong \mathbb{Z}_3$. Consider the matrix

$$\mathrm{M} = \begin{pmatrix} (2x,0) & (0,0) & (x,1) \\ (-2x,0) & (0,0) & (-x,1) \\ (0,1) & (0,0) & (0,2) \end{pmatrix}.$$

Any triple $\mathrm{B} \in \mathcal{B}$ containing $(0,0)$ can only be mapped to one type 1 block, that is, the image of $\{(x,2),(-x,2),(0,0)\}$. Therefore, the last column maps to a type 1 block, and the signature of the image of the second column is 0. The first column also maps to a type 1 block. Now, since $(0,1) \mapsto (0,2)$, it follows that $(2x,0)$ maps to either $(0,0)$ or $(0,1)$. However, $(0,0)$ and $(0,1)$ are the images of $(\pm x,0)$, so $3x = 0$, since x is non-zero.

Suppose now that G has another non-zero element $y \neq x$ or $2x$, and consider the matrix:

$$\begin{pmatrix} (-\frac{1}{2}y,0) & (0,2) & (y,2) \\ (\frac{1}{2}y,0) & (0,2) & (-y,2) \\ (0,1) & (0,2) & (0,0) \end{pmatrix}.$$

Then all the rows are mapped to type 2 blocks because the image of $(0,2)$ is only included in one type 1 block; namely, the image of $\{(x,1),(-x,1),(0,2)\}$. In the same way, the first and the last column map to type 2 blocks. This is because the only type 1 block containing the image of the point $(0,1)$ is the image of the block $\{(x,0),(-x,0),(0,1)\}$. This is clearly not

$$\{(\frac{1}{2}y,0),(-\frac{1}{2}y,0),(0,1)\}$$

by the assumption on y.

Similarly, the only type 1 block containing the image of the point $(0,0)$ is the image of the block $\{(x,2),(-x,2),(0,0)\}$, which is not equal to

$$\{(y,2),(-y,2),(0,0)\}.$$

The image of the middle column has signature zero. Hence, the sum of the row signatures does not equal that of the columns. This implies that our initial assumption must be false. $\square$

Having seen that automorphisms of the Bose Steiner triple systems are even type 1 except when $G \cong \mathbb{Z}_3$, we focus on even type 1 automorphisms.

4.2 Definition Let $\mathbb{B} = (V, \mathcal{B})$ be a Bose Steiner triple system and $\sigma \in \text{Aut } \mathbb{B}$ be an even type 1 automorphism. Then σ is *standard* on an element x of G, if σ permutes the labels of $\{(x,0),(x,1),(x,2)\}$ in the same way as those of $\{(0,0),(0,1),(0,2)\}$.

A group of even type 1 automorphism is *non- standard* if it is not standard. Automorphisms of the Bose Steiner triple systems are further classified as standard and non-standard based on their actions on the labels of the blocks. This consideration is important because it will be observed that the full automorphism group of most Bose Steiner triple systems $\mathbb{B}$ consists of standard automorphisms. We now discus the standard automorphisms.

4.1.1 Standard automorphisms

The main interest in this section is on the actions of automorphisms on the labels of type 1 blocks of a Bose Steiner triple systems $\mathbb{B} = (V, \mathcal{B})$. It will be evident that the groups $G \ncong \mathbb{Z}_3$ for which the automorphisms of the Bose Steiner triple systems are non-standard are products of powers of $\mathbb{Z}_3$ and $\mathbb{Z}_9$ or products of powers of $\mathbb{Z}_3$ or $\mathbb{Z}_9$.

We now describe the standard automorphism on a Bose design in the sequel.

4.11 Theorem [8] *Let $\mathbb{B} = (G \times \mathbb{Z}_3, \mathcal{B})$ be a Bose Steiner triple system and $\sigma \in$ Aut $\mathbb{B}$. If σ is non-standard, then all elements of G are of order either* 3 *or* 9, *and so G is isomorphic to a direct sum of copies of $\mathbb{Z}_3$ or $\mathbb{Z}_9$.*

Proof. It is enough to show the case $|G| \geq 3$.

Let $|G| \geq 3$, and σ acts non-standardly on an element $a \in G$. Consider the matrix below:

$$\mathrm{M} = \begin{pmatrix} (0,0) & (0,1) & (0,2)) \\ (a,2) & (a,0) & (a,1) \\ (-a,2) & (-a,0) & (-a,1) \end{pmatrix}.$$

The composition of σ with a translation will also act non-standardly on a. Hence, suppose the top row in M above is mapped to $\{(x,0),(x,1),(x,2)\}$ for some $x \in G$. Without loss of generality, since a and $-a$ can replace each other, then we have the following possibilities for the second and third row. It is either the second row maps to $\{(y,0),(y,1),(y,2)\}$ and the third row to $\{(z,1),(z,2),(z,0)\}$ or the second row maps to $\{(y,1),(y,2),(y,0)\}$ and the third row now to $\{(z,0),(z,1),(z,2)\}$, for some $y,z \in G$. This is shown below as the matrices M_1 and M_2 respectively.

$$\mathrm{M}_1 = \begin{pmatrix} (x,0) & (x,1) & (x,2) \\ (y,0) & (y,1) & (y,2) \\ (z,1) & (z,2) & (z,0) \end{pmatrix} \qquad \mathrm{M}_2 = \begin{pmatrix} (x,0) & (x,1) & (x,2) \\ (y,1) & (y,2) & (y,0) \\ (z,0) & (z,1) & (z,2) \end{pmatrix}.$$

In either case, the result is the same since the second and third rows can easily be swapped. So, suppose the matrix M above maps to M_1, then it follows that $x + y = 2z$. Now, suppose $3a \neq 0$, and consider the blocks $\{(-3a,0),(a,0),(-a,1)\}$ and $\{(3a,1),(-a,1),(a,2)\}$. It follows that $(-3a,0)$ maps to $(2z-y,0)$ and $(3a,1)$ maps to $(\dfrac{y+z}{2},1)$.

Now, consider the block $\{(9a,0),(-3a,0),(3a,1)\}$, then $(9a,0)$ maps to $(2y-z,0) = (x,0)$. We therefore conclude that $9x = 0$. This implies that all elements of G which are non-standard under σ are of order either 3 or 9.

To complete the proof, we need to show that if $a,b,c \in G$ and $a+b = 2c$, then for any even type 1 automorphism $\sigma \in \mathrm{Aut}\,\mathbb{B}$, σ acts standardly on either on all three a,b,c, or on exactly one of them. Even type 1 automorphisms preserve signatures hence, it follows that σ either moves all the labels of any type 2 block containing a,b,c by the same value, or all by different values. Now, assume that σ acts non-standardly on a and standardly on b which is different from 0. From the block $\{(a,0),(b,0),(\dfrac{a+b}{2},1)\}$, σ acts non-standardly on $\dfrac{a+b}{2}$. Hence $9(\dfrac{a+b}{2}) = 0$, which implies that $9b = 0$.

It follows that all elements other than the identity are of order either 3 or 9. $\square$

The next theorem discusses the structure of all standard automorphisms of the Bose Steiner triple systems. The concept of the holomorph of a group discussed in Chapter 2 plays a role in describing these structures. First, we describe the standard map.

4.3 Definition *Let $\mathbb{B} = (G \times \mathbb{Z}_3, \mathcal{B})$ be a Bose Steiner triple system, and let $a \in G, \alpha \in \mathrm{Aut}\ G$ and $i \in \mathbb{Z}_3$. For an $(x, j) \in V = G \times \mathbb{Z}_3$, define a map $[a, \alpha, i] : V \to V$ by*

$$[a, \alpha, i](x, j) = (a + \alpha(x), j + i).$$

Then the map $[a, \alpha, i]$ is said to be standard.

4.12 Theorem [8] *Let $\mathbb{B} = (V, \mathcal{B})$ be a Bose Steiner triple system. The group of standard automorphisms of $\mathbb{B}$ is isomorphic to $\mathrm{Hol}(G) \times \mathbb{Z}_3$.*

Proof. Let $a \in G$, $\alpha \in \mathrm{Aut}\ G$, and $i \in \mathbb{Z}_3$. Consider the map $\sigma_{[a,\alpha,i]} : [a, \alpha, i] \mapsto (a, \alpha, i)$ of elements of $\mathbb{B}$ defined by

$$\sigma_{[a,\alpha,i]}(x, j) = (a + \alpha(x), j + i).$$

In view of Proposition 4.4, it is enough to show that $\sigma_{[a,\alpha,i]}$ is a surjection to the subgroup comprising the standard automorphisms of $\mathbb{B}$. That is, we need to show that given any element $(a, \alpha, i) \in \mathrm{Hol}(G) \times \mathbb{Z}_3$, there exists a corresponding triple of the standard automorphism $[a, \alpha, i] \in \mathrm{Aut}\ \mathbb{B}$.

First, we consider the restriction map on the elements of $\mathbb{Z}_3$. Clearly, $\sigma|_{\mathbb{Z}_3}$ maps the $\mathbb{Z}_3$ components in the same way for every element $x \in G$. Hence, $i \in \mathbb{Z}_3$ can be easily implied. We also say that the map $\sigma_{[a,\alpha,i]}$ uniquely defines a restriction map $\sigma|_G : G \to G$. This map is a set isomorphism of G.

Now, we shall produce the elements of the triple. $\sigma_G(0)$ gives the first element of the triple. For the second element, it is essential we present an automorphism of G.

Claim: The map $\rho : x \mapsto \sigma|_G(x) - \sigma|_G(0)$ is an automorphism of G.

Proof. $\rho(\{(x, 0), (y, 0), (z, 1)\}) = \{(\sigma|_G(x), i), (\sigma|_G(y), i), (\sigma|_G(z), i + 1)$.

Now, for the action of the map ρ on type 2 blocks, consider the type 2 blocks below:

$$\begin{array}{ccc} \{(x,0) & (-x,0) & (0,1)\}; \\ \{(y,0) & (0,0) & (\frac{y}{2},1)\}; \\ \{(x+y,0) & (-x,0) & (\frac{y}{2},1)\}. \end{array}$$

It follows that

$$\sigma|_G(x) + \sigma|_G(-x) = 2\sigma|_G(0), \tag{4.5}$$

$$\sigma|_G(y) + \sigma|_G(0) = 2\sigma|_G(\frac{y}{2}), \tag{4.6}$$

and combining (4.5) and (4.6), we have:

$$\sigma|_G(x+y) + \sigma|_G(-x) = 2\sigma|_G(\frac{y}{2}). \tag{4.7}$$

It follows from (4.6) and (4.7) that

$$\sigma|_G(x+y) + \sigma|_G(-x) = \sigma|_G(y) + \sigma|_G(0).$$

Coupling with (4.5), we have:

$$\sigma|_G(x+y) = \sigma|_G(x) + \sigma|_G(y) - \sigma|_G(0),$$

and by taking $\sigma|_G(0)$ from both sides, we have:

$$\sigma|_G(x+y) - \sigma|_G(0) = \sigma|_G(x) - \sigma|_G(0) + \sigma|_G(y) - \sigma|_G(0).$$

This implies

$$\rho(x+y) = \rho(x) + \rho(y).$$

Hence we conclude that ρ is an automorphism of G, and $[\sigma_G(0), \rho, i]$ is the required triple of standard automorphisms and hence, we have the required isomorphism. $\square$

4.1.2 Non- standard automorphisms

Lovegrove [8] has shown that the non-standard automorphisms are only applicable on Bose Steiner triple systems constructed from groups G of the form: $\mathbb{Z}_3^n \times \mathbb{Z}_9^m, n+m \neq 0$. He has also shown that the non-standard and standard automorphisms of a Bose Steiner triple systems together also form a subgroup of the automorphism group which is the whole automorphism group unless $G \cong \mathbb{Z}_3$.

We now discuss the structure of the groups of a Bose Steiner triple system that produces non-standard automorphisms in the sequel.

We begin with the following pertinent observation.

4.13 Lemma [8] *If $i, j \in \mathbb{Z}_3$, then*

$$(-2)^i + (-2)^j \equiv (-2)^{i+j} + 1 \pmod 9.$$

Proof. Since $i, j \in \mathbb{Z}_3$, there are only nine possibilities. This is shown below:

i	j	$(-2)^i$	$(-2)^j$	$(-2)^i + (-2)^j$	$(-2)^{i+j} + 1$
0	0	1	1	2	2
0	1	1	7	8	8
0	2	1	4	5	5
1	0	7	1	8	8
1	1	7	7	5	5
1	2	7	4	2	2
2	0	4	1	5	5
2	1	4	7	2	2
2	2	4	4	8	8

The result therefore follows. □

The following lemma proves the identities necessary for the characterization of the group of all even type 1 automorphisms of the Bose Steiner triple systems.

4.14 Lemma [8] *Let $\mathbb{B} = (G \times \mathbb{Z}_3, \mathcal{B})$ be a Bose Steiner triple system, and let (α, β) be a pair of even type 1 automorphism $\sigma \in \mathrm{Aut}\,\mathbb{B}$, such that $\alpha : G \to G, \quad \beta : G \to \mathbb{Z}_3$, where α is an automorphism of G. Then for any point $(x, i) \in \mathbb{B}, \sigma$ can be written as*

$$\sigma : (x, i) \mapsto (\alpha(x), i + \beta(x)).$$

If G is of the form $\mathbb{Z}_3^n \times \mathbb{Z}_9^m$, and $\sigma = (\alpha, \beta)$ is any even type 1 automorphism of $\mathbb{B}$, then

(i) *if $x, y, z \in G$, such that $x + y = 2z$, then $\beta(x) + \beta(y) + \beta(z) \equiv 0 \pmod 3$;*

(ii) *the map $G \to \mathbb{Z}_3$ defined by $x \mapsto \beta(x) - \beta(0)$ is a homomorphism.*

Proof. (i) σ preserves block signatures, since it is an even type 1 automorphism. A type 2 block $\{(x, 0), (y, 0), (z, 1)\}$ will be mapped to a type 2 block with the label values $\beta(x), \beta(y)$, and $(\beta(z) + 1)$ respectively. Hence we have that $\beta(x) + \beta(y) + (\beta(z) + 1) \equiv 1 \pmod 3$. Similarly, if $x = y = z$, the signature of the type 1 block $\{(x, 0), (x, 1), (x, 2)\}$ is also preserved since σ is a type 1 automorphism. Hence we have

$$\beta(x) + \beta(x) + 1 + (\beta(x) + 2) = 3\beta(x) + 3 \equiv 0 \pmod 3.$$

Therefore we have that $\beta(x) = \beta(y) = \beta(z)$, or $\beta(x) \neq \beta(y) \neq \beta(z)$, since $\beta(x), \beta(y)$ and $\beta(z)$ are all elements of $\mathbb{Z}_3$.

(ii) Here, we need to show that for any $x, y \in G$, $\beta(x + y) - \beta(0) = \beta(x) - \beta(0) + \beta(y) - \beta(0)$. This implies that $\beta(x + y) + \beta(0) = \beta(x) + \beta(y)$. From case (i) above, we have that $x + y = 2z = (x + y) + 0$ and that

$$\beta(x) + \beta(y) + \beta(z) = 0 = \beta(x + y) + \beta(0) + \beta(z).$$

Hence the result follows.

□

4.15 Lemma [8] *Let G be of the form $\mathbb{Z}_3^n \times \mathbb{Z}_9^m$, and let $\mathbb{B} = (G \times \mathbb{Z}_3, \mathcal{B})$ be a Bose Steiner triple system. Let (α, β) be a pair of even type 1 automorphism $\sigma \in \operatorname{Aut} \mathbb{B}$, such that $\alpha : G \to G$, $\quad \beta : G \to \mathbb{Z}_3$, where α is an automorphism of G. Then for any point (x, i) in $\mathbb{B}$, σ can be written as*

$$\sigma : (x, i) \mapsto (\alpha(x), \beta(x) + i).$$

(i) *If $x, y, z \in G$, such that $x + y = 2z$, then*

$$(-2)^{\beta(x)}\alpha(x) + (-2)^{\beta(y)}\alpha(y) + (-2)^{1+\beta(z)}\alpha(z) = 0.$$

(ii) *If $x, y, z \in G$, such that $x + y = 2z$, then*

$$(-2)^{\beta(x)} + (-2)^{\beta(y)} + (-2)^{1+\beta(z)} \equiv 0 \pmod 9.$$

Proof. (i) From case (i) of Lemma 4.14 above, we have that $\beta(x) + \beta(y) + (\beta(z) + 1) \equiv 1 \pmod 3$ for all $x, y, z \in G$. Suppose (α, β) maps the block $\{(x, i), (y, i), (z, i + 1)\}$ to

$$\{(\alpha(x), i + \beta(x)), (\alpha(y), i + \beta(y)), (\alpha(z), i + 1 + \beta(z))\}$$

and $\beta(x) = \beta(y) = \beta(z)$. It follows that $\alpha(x) + \alpha(y) = 2\alpha(z)$. Therefore $\alpha(x) + \alpha(y) + (-2)\alpha(z) = 0$. Suppose $\beta(x) \neq \beta(y) \neq \beta(z)$. Then without loss of generality, we have $\beta(x) = 1 + \beta(z)$, and $\beta(y) = 2 + \beta(z)$. Hence the image of the block $\{(x, i), (y, i), (z, i + 1)\}$ becomes

$$\{(\alpha(x), i + 1 + \beta(z)), ((\alpha(y), i + 2 + \beta(z)), ((\alpha(z), i + 1 + \beta(z))\}.$$

It follows that $\alpha(x) + \alpha(z) = 2\alpha(y)$, or $\alpha(x) + (-2)\alpha(y) + \alpha(z) = 0$. We then have:

$$(-2)^{1+\beta(z)}\alpha(x) + (-2)^{2+\beta(z)}\alpha(y) + (-2)^{1+\beta(z)}\alpha(z) = 0.$$

Hence

$$(-2)^{\beta(x)}\alpha(x) + (-2)^{\beta(y)}\alpha(y) + (-2)^{1+\beta(z)}\alpha(z) = 0.$$

(ii) This proof is very similar to the last one. We only need the result in case (i) of Lemma 4.14 above to check the cases where :

(i) $\beta(x), \beta(y),$ and $\beta(z)$, are all the same,

(ii) $\beta(x), \beta(y),$ and $\beta(z)$, is an even permutation of $\mathbb{Z}_3$,

(iii) $\beta(x), \beta(y),$ and $\beta(z)$, is an odd permutation of $\mathbb{Z}_3$.

$\square$

4.16 Theorem [8] *Let $\mathbb{B} = (G \times \mathbb{Z}_3, \mathcal{B})$ be a Bose Steiner triple system and let $G \cong \mathbb{Z}_3^n \times \mathbb{Z}_9^m$. If $\sigma = (\alpha, \beta)$ is an even type 1 automorphism of $\mathbb{B}$, then*

(i) *the map*

$$x \mapsto (-2)^{\beta(x)}(\alpha(x) - \alpha(0))$$

is an automorphism of G;

(ii) *the group of even type* 1 *automorphisms of* $\mathbb{B}$ *is isomorphic to a group on the set* $\mathbb{Z}_3 \times G \times \mathrm{Hom}(G, \mathbb{Z}_3) \times \mathrm{Aut}\ G$, *by the map:*

$$(\alpha, \beta)(x) \to (\beta(0), \alpha(0), \beta(x) - \beta(0), (-2)^{\beta(x)}(\alpha(x) - \alpha(0))).$$

Hence, all even type 1 *automorphisms* $\sigma = (\alpha, \beta)$ *of* $\mathbb{B}$ *can be expressed in the form:*

$$\alpha(x) = x + (-2)^{-\beta(x)}\phi(x), \quad \beta(x) = i + \pi(x),$$
$$i \in \mathbb{Z}_3, \pi \in \mathrm{Hom}(G, \mathbb{Z}_3), x \in G, \text{ and } \phi \in \mathrm{Aut}\ G.$$

Proof. First, we need show that the map $x \mapsto (-2)^{\beta(x)}(\alpha(x) - \alpha(0))$ is a group homomorphism. Suppose $\beta(x) \neq \beta(y) \neq \beta(z)$, and $x + y = 2z$. Then setting $\phi(x) = (-2)^{\beta(x)}(\alpha(x) - \alpha(0))$, we have from cases (i) and (ii) of Lemma 4.15 that

$$\begin{aligned}\phi(x) + \phi(y) - 2\phi(z) &= (-2)^{\beta(x)}\alpha(x) + (-2)^{\beta(y)}\alpha(y) + (-2)^{1+\beta(z)}\alpha(z) \\ &\quad - \alpha(0)((-2)^{\beta(x)} + (-2)^{\beta(y)} + (-2)^{1+\beta(z)}) \\ &= 0.\end{aligned}$$

The result is the same for $x = y = z$. Thus in the same manner as Theorem 4.12, we have

$$\begin{aligned}\phi(2x) + \phi(2y) &= 2\phi(x + y); \\ 2\phi(x) &= \phi(2x) + \phi(0); \\ 2\phi(y) &= \phi(2y) + \phi(0).\end{aligned}$$

Hence it follows that $2\phi(x) + 2\phi(y) = \phi(2x) + \phi(2y) + 2\phi(0)$. This implies $\phi(x) + \phi(y) = \phi(x + y)$, for all $x, y \in G$, since $\phi(0) = 0$. Therefore ϕ is a group homomorphism on G.

Clearly, the map

$$\mathrm{Aut}\ \mathbb{B} \to \mathbb{Z}_3 \times G \times \mathrm{Hom}(G, \mathbb{Z}_3) \times \mathrm{Aut}\ G$$

is well-defined.

This map is injective because $\alpha(0)$ and β can be realised by the first three components of the image. Then α can be sufficiently established by these components and Aut G.

In order to show that ϕ is injective, it is sufficient to show that $\alpha(x) = 0$ if and only if $x = 0$. By definition, $\phi(x) = 0$ if and only if $\alpha(x) = \alpha(0)$. Hence we say that $x = 0$ since α is a set homomorphism on G.

Next, we show that the map ϕ is surjective. From the image of the map, we need to show that if $i \in \mathbb{Z}_3, \pi \in \mathrm{Hom}(G, \mathbb{Z}_3), a \in G,$ and $\phi \in \mathrm{Aut}\ G$, such that

$$\beta : G \to \mathbb{Z}_3, \text{ defined as } \beta(x) = i + \pi(x),$$

and

$$\alpha : G \to G, \text{ defined as } \alpha(x) = a + (-2)^{-\beta(x)}\phi(x),$$

then (α, β) is an automorphism of $\mathbb{B}$. To see this, we first consider the actions of (α, β) on blocks.

Clearly (α, β) maps type 1 blocks to type 1 blocks. Hence we only need to examine type 2 blocks. It is clear that if $x, y, z \in G$ such that $x + y = 2z$, then $\beta(x) + \beta(y) + \beta(z) = 0$. By definition $\beta(x) = i + \pi(x)$. Therefore we have:

$$\begin{aligned}
\beta(x) + \beta(y) + \beta(z) &= 3i + \pi(x) + \pi(y) + \pi(z) \\
&= \pi(x + y) - 2\pi(z) \qquad (\pi \in \mathrm{Hom}(G, \mathbb{Z}_3)) \\
&= \pi(x + y - 2z) \\
&= 0.
\end{aligned}$$

Again by definition, $\alpha(x) = a + (-2)^{-\beta(x)}\phi(x)$. Now suppose $x \neq y \neq z$, and $x + y = 2z$, then $\phi(x) + \phi(y) - 2\phi(z) = 0$. This implies that

$$\begin{aligned}
\phi(x) + \phi(y) - 2\phi(z) = (-2)^{\beta(x)}\alpha(x) + (-2)^{\beta(y)}\alpha(y) + (-2)^{1+\beta(z)}\alpha(z) \\
- a((-2)^{\beta(x)} + (-2)^{\beta(y)} + (-2)^{\beta(z)}). \qquad (4.8)
\end{aligned}$$

By case (i) of Lemma 4.15, (4.8) becomes

$$= 0 + a(1 + (-2)^{\beta(x)+\beta(y)} + (-2)^{1+\beta(z)}).$$

By Lemma 4.13, we have

$$= a(2 + (-2)^{\beta(x)+\beta(y)+1+\beta(z)}),$$

and by the definition of β, we have

$$= a(2 + (-2)^{3i+3\beta(z)+1}) = 0.$$

From the equation $\beta(x) + \beta(y) + \beta(z) = 0$, there are two possibilities. These in turn affect $\sigma = (\alpha, \beta)$.

Case 1 : If $\beta(x) = \beta(y) = \beta(z)$, then by the argument above, $\alpha(x) + \alpha(y) = 2\alpha(z)$. Thus, the block

$$\{(\alpha(x), i + \beta x), (\alpha(y), i + \beta y), (\alpha(z), i + 1 + \beta x)\}$$

is the image of the block $\{(x, i), (y, i), (z, i + 1)\}$ under (α, β).

Case 2 : If $\beta(x) \neq \beta(y) \neq \beta(z)$, then we have that $1 + \beta(z)$ must be $\beta(x)$ or $\beta(y)$, since $\beta : G \to \mathbb{Z}_3$. Without loss of generality, suppose $1 + \beta(z) = \beta(x)$. It follows from (4.8) that

$$(-2)^{\beta(x)}\alpha(x) + (-2)^{1+\beta(x)}\alpha(y) + (-2)^{\beta(x)}\alpha(z) = 0.$$

Therefore $\phi(x) + \phi(z) - 2\phi(y) = 0$ since $(-2)^{\beta(x)} \neq 0$, so $\phi(x) + \phi(z) = 2\phi(y)$. It follows that $\{(\alpha(x), i + \beta x), (\alpha(z), i + \beta x), (\alpha(y), i + 1 + \beta x)\}$ is the image of the block $\{(x, i), (y, i), (z, i + 1)\}$ under the composition (α, β).

So far, it has been shown that the composition (α, β) maps blocks to blocks. We now need to show that $\sigma = (\alpha, \beta)$ is injective to complete our proof. To achieve this, we need to show that giving any two points (x, i) and (y, i), such that $(\alpha, \beta)(x, i) = (\alpha, \beta)(y, i')$, then $x = y$, and $i = i'$.

By definition, $(\alpha, \beta)(x, i) = a + (-2)^{-\beta(x)}\phi(x)$. Similarly, $(\alpha, \beta)(y, i') = a + (-2)^{-\beta(y)}\phi(y)$. If $(\alpha, \beta)(x, i) = (\alpha, \beta)(y, i')$, then we have

$$a + (-2)^{-\beta(x)}\phi(x) = a + (-2)^{-\beta(y)}\phi(y).$$

Observe that (-2) commutes with ϕ, hence we have $\phi((-2)^{\beta(x)}x) = \phi((-2)^{\beta(y)}y)$. Therefore, since ϕ is injective, $(-2)^{-\beta(x)+\beta(y)}x - y = (-2)^{\pi(x-y)}x - y = 0$. Observe that $\pi(x - y) = \pi((-2)^{-\pi(x-y)}x - y) = \pi(0) = 0$. This is because for any $i \in \mathbb{Z}_3$, $\pi((-2)^i x) = (-2)^i \pi(x) = \pi(x)$. Hence we conclude that $\sigma = (\alpha, \beta)$ is an automorphism of $\mathbb{B}$, since (α, β) is injective, and $x = y$, and $i = i'$. $\square$

To this end, we have seen the full non-standard automorphism groups of a Bose design $\mathbb{B}$. It has been shown that the full automorphism group for $G \cong \mathbb{Z}_3^n \times \mathbb{Z}_9^m$ is the group on the set $G \times \mathbb{Z}_3 \times \mathrm{Hom}(G, \mathbb{Z}_3) \times \mathrm{Aut}\ G$. Its order is $3^{2n+3m+1}|\mathrm{Aut}\ G|$.

The case involving direct copies of $\mathbb{Z}_3$ is a special case where the Bose Steiner triple system coincides with the affine Steiner triple systems.

4.17 Theorem *Let $G \cong (\mathbb{Z}_3)^n$ consisting of the direct product of n copies of $\mathbb{Z}_3$, where the blocks are all triples $\{x, y, z\}$ such that $x, y, z \in \mathbb{Z}_3^n$, and $x \neq y \neq z$. Then the Bose Steiner triple system is isomorphic to* $\mathrm{AG}(n, 3)$.

Proof. The group G is considered as a vector space over the field $\mathbb{F}_3 \cong \mathbb{Z}_3$. In this case, every automorphism is an invertible linear transformation of the vector space and conversely. $\square$

We further illustrate with an example. We present 5 examples of a Bose Steiner triple system of the same order.

6 Example We consider 5 Steiner triple systems of order 243 and compute the order of their automorphism groups.

If $G_1 = \mathbb{Z}_{81}$, $G_2 = \mathbb{Z}_3 \times \mathbb{Z}_{27}$, $G_3 = \mathbb{Z}_9 \times \mathbb{Z}_9$, $G_4 = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, and $G_5 = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Then $G_1, G_2, G_3,$ and G_4, are Bose constructions of STS(243). The affine geometry $\mathrm{AG}(5,3)$ on G_5 is also a Steiner triple system of order 243. It will be evident that its order is 115562653240320.

By Theorem 4.12, the automorphism group of G_1 and G_2 are standard since the groups have elements of order 81 and 27 respectively. Hence the automorphism of the design on G_1 is then

$$3|\mathbb{Z}_{81}||\mathrm{Aut}(\mathbb{Z}_{81})| = 3 \times 81 \times 54 = 13122,$$

while that of the design G_2 is

$$3|\mathbb{Z}_3 \times \mathbb{Z}_{27}||\mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_{27})| = 3 \times 81 \times 324 = 78732.$$

The designs on G_3 and G_4 have non-standard automorphism groups. Hence by Theorem 4.16, the order of the automorphism groups are:

$$3^7|\mathrm{Aut}(G_3)| = 3^7 \times 3888 = 8503056,$$

and

$$3^9|\mathrm{Aut}(G_4)| = 3^9(3^4-1) \times (3^4-3) \times (3^4-9) \times (3^4-27) = 477531624960$$

respectively.

We now come to the automorphism groups of Skolem Steiner triple systems.

4.2 Automorphism groups of Skolem Steiner triple systems

The essence of this section, just like the previous one is to determine the full automorphism group of Skolem Steiner triple systems $\mathcal{D} = (V, \mathcal{B})$. We also explore the symmetry of the Skolem quasigroups.

Here, we exclude the special cases of $\mathrm{Q} = \{0, 1\}$ and $\mathrm{Q} = \{0, 1, 2, 3\}$. In the case $\mathrm{Q} = \{0, 1\}$, there is no unique third element of Q such that given any two elements, the third can be uniquely determined. The case $\mathrm{Q} = \{0, 1\}$ yields the well-known Fano plane, while the case $\mathrm{Q} = \{0, 1, 2, 3\}$ has an extra line of symmetry with $\mathrm{Q} = \{0, 1\}$.

As will be seen later, Skolem designs are almost asymmetrical as compared to the triple systems constructed by Bose. Unlike the automorphism groups of Bose Steiner triple systems with automorphisms intimately linked to the automorphisms of the group they are defined on, Skolem designs are constrained by the rigidity of the quasigroups from which they are derived.

Before proceeding, some relevant notation, terminology and definitions are essential in order to fully discuss this section.

Let $V = \mathrm{Q}_{2n} \times \mathbb{Z}_3 \cup \{(p, q)\}$. We denote the set $\mathrm{Q}_{2n} \cup \{p\}$ by R and the set $\mathbb{Z}_3 \cup \{q\}$ by S. By $\Pi_1 : V \to R$ ($\Pi_2 : V \to S$) we mean the usual natural projections. To facilitate our discussion, we partition Q into two disjoint subsets $\mathrm{Q}^{\mathrm{i}}, \mathrm{i} = 1, 2$ as follows:

$$\mathrm{Q}^1 = \{0, 1, \cdots, (n-1)\} \text{ and} \tag{4.9}$$

$$\mathrm{Q}^2 = \{n, n+1, \cdots, (2n-1)\}. \tag{4.10}$$

First, we observe some additional pertinent relations in Q_{2n}.

4.18 Lemma *Let* Q^1 *be as defined in* (4.9) *and let* $x, y \in \mathrm{Q}^1$ *such that* $x < y$. *Then*

(i) $(n + x) * y = z$ *has no solution if and only if* $z = \rho(n-1)$;

(ii) $x * y = 2n - 1$ *has no solution;*

(iii) $x * y = 0$ *has no solution;*

(iv) $x * y = n-1$ *has no solution;*

(v) *if* $x \equiv y \pmod 2$ *and* $x+1 < y$, *then* $x < x*y < y$.

(vi) *if* $x \not\equiv y \pmod 2$ *and* $x+1 < y$, *then* $n+x < x*y < n+y$.;

(vii) $x*(x+1) = n+x$.

Proof. (i) $(n+x)*y = \rho(n-1) \Longrightarrow \rho(((n+x)+y) \pmod{2n}) = \rho(n-1) \Longrightarrow ((n+x+y) \pmod{2n}) = (n-1) \Longrightarrow x+y = 2n-1$ or $x+y=-1$. In either case, no such x and y exist.

On the other hand,

$$\{x*2n-1-y : x, y \in \mathrm{Q}^1, x-y = 0, \pm1, \pm2, \ldots, \pm(n-1)\} = \mathrm{Q}_{2n} \setminus \{\rho(n-1)\}.$$

Hence the result follows.

(ii) $x*y = 2n-1 \Longleftrightarrow \rho(x+y) = 0*(2n-1) \Longleftrightarrow \rho(x+y) = \rho(2n-1) \Longleftrightarrow x+y = 2n-1$ which is false since $x+y < 2n-2$.

(iii) $x*y = 0 \Longleftrightarrow \rho(x+y) = 0*0 \Longleftrightarrow \rho(x+y) = \rho(0) \Longleftrightarrow x+y = 0$ which is false since $0 < (x+y) < (2n-2)$.

(iv) $x*y = n-1 \Longleftrightarrow \rho(x+y) = (n-1)*(n-1) \Longleftrightarrow \rho(x+y) = \rho(2n-2) \Longleftrightarrow x+y = 2n-2$ which is false since $x+y = 2n-2 \Longleftrightarrow x = y = n-1$.

(v), (vi) and (vii) hold by direct calculation. □

In other to determine automorphisms of the Skolem designs, we explore structures which are preserved by automorphisms. The structures have conveniently been examined as matrices.

4.19 Lemma *Let* $\mathcal{D} = (V, \mathcal{B})$ *be a Skolem design,* $\sigma \in \mathrm{Aut}\ \mathcal{D}$ *and let* M *be a* 3×3 *matrix with elements from* V *such that its rows and columns are valid blocks of* $\mathcal{B}$. *If each block type* i, $i = 1, 2, 3$ *is in exactly one row and one column, then* M *is symmetric and* $\sigma(M)$ *is also symmetric.*

Proof. Since M contains a unique row and column containing a type 2 block, there exist a unique row r and a unique column c such that $M_{rc} = (p, q)$. By definition of blocks and without loss of generality, $M_{rc'} = (x, i+1), x \in \mathrm{Q}^1, i \in \mathbb{Z}_3$ and $M_{rc''} = (n+x, i)$ for fixed columns c', c'', $c \neq c' \neq c''$.

Again, by definition of blocks, we have that column c' contains a type 1 block, since $\Pi_1(M_{rc'}) = x \in \mathrm{Q}^1$. Similarly column c'' contains a type 3 block, since $\Pi_1(M_{rc''}) = n + x \notin \mathrm{Q}^1$.

By similar argument, we have that $M_{r'c} = (y, j+1), y \in \mathrm{Q}^1, j \in \mathbb{Z}_3$ and $M_{r''c} = (n+y, j)$ for fixed rows $r', r'', r \neq r' \neq r''$. This implies that row r' contains a type 1 block, hence $\Pi_1(M_{r'c}) = y \in \mathrm{Q}^1$ and row r'' contains a type 3 block, because $\Pi_1(M_{r''c}) = n + y \notin \mathrm{Q}^1$.

Now, without loss of generality, suppose $\Pi_2(M_{r'c}) = i+1$. It follows that row r' and column c' must contain type 1 blocks. Hence $\Pi_1(M_{r'c'}) = x = y$, and $\Pi_2(M_{r'c'}) = i+2$ or i.

We now consider both cases of $\Pi_2(M_{r'c'})$.

Case 1: $\Pi_2(M_{r'c'}) = i$. Suppose $M_{r''c''} = (z, k), z \in \mathrm{Q}$, $k \in \mathbb{Z}_3$. This implies $\Pi_2(M_{r'c''}) = \Pi_2(M_{r''c'}) = i+2$, and we have the following possibilities:

(i) $k = i$ and $z * (n+x) = x$. Clearly, this is not a valid type 3 block of $\mathcal{D}$, since $\Pi_2(M_{r'c''}) = \Pi_2(M_{r''c'}) = i+2$.

(ii) $k = i+2$ and $z * x = n + x$.
$z * x = n + x$ implies $\rho((z+x) \pmod{2n}) = n + x$ and this also implies $\rho(z+x) = n+x$ or $\rho((z+x) - 2n) = n + x$.

First, we consider the case $\rho(z+x) = n+x$.

$\rho(z+x) = n + x$ implies $\dfrac{z+x}{2} = n + x$ if $z + x \equiv 0 \pmod 2$ or $\dfrac{2n+z+x-1}{2} = n + x$ if $z + x \equiv 1 \pmod 2$.

Now, suppose $\dfrac{z+x}{2} = n + x$. It follows that $z = 2n + x \notin \mathrm{Q}$ and hence this case is not possible.
If $\dfrac{2n+z+x-1}{2} = n + x$, then $z = x + 1 \in \mathrm{Q}$ since $x \in \mathrm{Q}^1$.
Next, we consider the case $\rho((z+x) - 2n) = n + x$.

$\rho((z+x) - 2n) = n + x$ implies $\dfrac{z+x-2n}{2} = n + x$ if $z + x - 2n \equiv 0 \pmod 2$ or $\dfrac{2n+z+x-2n-1}{2} = n + x$ if $z + x - 2n \equiv 1 \pmod 2$.

Now, suppose $\dfrac{z+x-2n}{2} = n + x$. It follows that $z = 4n + x \notin \mathrm{Q}$ and hence this case is not possible.

If $\dfrac{2n+z+x-2n-1}{2} = n+x$, then $z = 2n+x+1 \notin Q$ for any $x \in Q^1$. Hence this case is not also possible.

Case 2: $\Pi_2(M_{r'c'}) = i+2$. This implies $\Pi_2(M_{r'c''}) = \Pi_2(M_{r''c'}) = i$, $\Pi_1(M_{r''c''}) = (n+x) * x$ and $\Pi_2(M_{r''c''}) = i+1$ and the result follows.

Hence in either case, M is symmetric. $\sigma(M)$ is also symmetric since M must be preserved by automorphisms.

□

We will call the matrices of Lemma 4.19 *Skolem symmetric matrices.* For instance, if the entry in the first row and first column is (p,q), then we have exactly 2 possibilities of Skolem symmetric matrices. They are of the form:

(a)

$$M = \begin{pmatrix} (p,q) & (x,i+1) & (n+x,i) \\ (x,i+1) & (x,i+2) & (x,i) \\ (n+x,i) & (x,i) & ((n+x)*x,i+1) \end{pmatrix} \tag{4.11}$$

(b)

$$M = \begin{pmatrix} (p,q) & (x,i+1) & (n+x,i) \\ (x,i+1) & (x,i) & (x,i+2) \\ (n+x,i) & (x,i+2) & (x+1,i+2) \end{pmatrix} \tag{4.12}$$

for some $i \in \mathbb{Z}_3$.

4.20 Corollary *Let* $0 \leq x \leq (n-1)$ *and* $\sigma \in \operatorname{Aut} \mathcal{D}$, *then*

(i) $\sigma((p,q)) = (p,q)$;

(ii) σ *preserves type* 2 *blocks.*

Proof. Since σ must preserve Skolem symmetric matrices of (4.11) and (4.12) above, (i) follows immediately.

(ii) That σ preserves type 2 blocks follows immediately from (i). □

4.21 Lemma *Let $\mathcal{D} = (V, \mathcal{B})$ be a Skolem design, $\sigma \in \mathrm{Aut}\ \mathcal{D}$ and let M be a 3×3 matrix with elements from V such that its rows and columns are valid blocks of $\mathcal{B}$. If two rows of M are distinct blocks of type 2, then the third row and the third column contain type 3 blocks and $\sigma(M)$ is of the same form as that of M.*

Proof. Suppose $M_{rc} = M_{r'c'} = (p, q)$. Then $r \neq r'$ and $c \neq c'$. Since the blocks in rows r and r' are distinct, it follows that $\Pi_1(M_{r''c}) \neq \Pi_1(M_{r''c'})$ where r'' is the third row. This implies that row r'' cannot contain a type 1 block. The same argument holds for the third column c'', where $c \neq c' \neq c''$. Hence we have that row r'' cannot contain type 2 blocks, since there exist two distinct rows of type 2 blocks already. This implies $M_{r''c''} \neq (p, q)$ and hence column c'' cannot contain a type 2 block. Hence row r'' and column c'' contains type 3 blocks.

It immediately follows that $\sigma(M)$ is of the same form of M since M must be preserved by automorphisms. $\square$

For instance if $M_{11} = M_{22} = (p, q)$, then we have the following possibilities:

$$M_1 = \begin{pmatrix} (p,q) & (x, i+1) & (n+x, i) \\ (y, j+1) & (p,q) & (n+y, j) \\ (n+y, j) & (n+x, i) & (z, k) \end{pmatrix} \tag{4.13}$$

$$M_2 = \begin{pmatrix} (p,q) & (n+x, i) & (x, i+1) \\ (n+y, j) & (p,q) & (y, j+1) \\ (y, j+1) & (x, i) & (z, k) \end{pmatrix} \tag{4.14}$$

$$M_3 = \begin{pmatrix} (p,q) & (x, i+1) & (n+x, i) \\ (y+n, j) & (p,q) & (y, j+1) \\ (y, j+1) & (n+x, i) & (z, k) \end{pmatrix} \tag{4.15}$$

where $x, y \in \mathrm{Q}^1$.

In each of the matrices above, there are 3 possibilities of the element (z, k).

In M_1 above, we have: (i) $(z, k) = (x*y, i+1)$, and $i = j$; (ii) $z*(n+x) = n+y$, $k = i$ and $j = i+1$; (iii) $z*(n+y) = n+x$, $k = j$ and $i = j+1$.

In M_2, we have: (i) $(z, k) = (x*y, i+1)$, where $i = j$; (ii) $z*x = y$ and $k = j = i+1$; (iii) $z*y = x$ and $k = i = j+1$.

In M_3, we have: (i) $(z,k) = ((n+x)*y, i = j+1)$; (ii) $z*(n+x) = y$ and $k = j = i$; (iii) $z*y = n+x$, $k = j+1$ and $i = j$.

4.22 Corollary *Let* $0 \leq x \leq (n-1)$, $i, j \in \mathbb{Z}_3$ *and* $\sigma \in \text{Aut } \mathcal{D}$, *then*

(i) σ *preserves block types.*

(ii) $\Pi_1(\sigma(x,i)) \in \mathrm{Q}^1$, *for all* $x \in \mathrm{Q}^1$;

Proof. (i) Suppose $M_{rc} = M_{r'c'} = (p,q)$, for fixed rows r, r' and columns c, c'. Then by Corollary 4.20(ii), σ maps blocks of rows r and r', columns c and c' to type 2 blocks. Hence, it follows that σ preserves type 3 blocks since σ must preserve the matrices of Lemma 4.21 and the result follows.

(ii) The result follows immediately from (i) because type 1 blocks must also be preserved. $\square$

4.23 Lemma *Let* $0 \leq x \leq (n-1)$, $i, j \in \mathbb{Z}_3$ *and* $\sigma \in \text{Aut } \mathcal{D}$, *then*

(i) $\Pi_1(\sigma(n+x,i)) = n + \Pi_1(\sigma(x,i))$;

(ii) $\Pi_1(\sigma(x+1,i)) = 1 + \Pi_1(\sigma(x,i))$;

(iii) $\Pi_1(\sigma(x,i)) = x \Longleftrightarrow \Pi_1(\sigma(n+x,i)) = n+x$;

(iv) $\Pi_1(\sigma(x,i)) = x \Longleftrightarrow \Pi_1(\sigma(x+1,i)) = x+1$;

(v) $\Pi_2(\sigma(x,i)) = j \Longleftrightarrow \Pi_2(\sigma((n+x)*x, i+1)) = j+1$.

(vi) $\Pi_1(\sigma(\rho(n-1),i)) = \rho(n-1)$, *for any* $i \in \mathbb{Z}_3$;

Proof. Since σ preserves Skolem symmetric matrices, $\Pi_1(\sigma(x,i)) = y \Longleftrightarrow \Pi_1(\sigma(n+x,i)) = n+y$. Hence (i) and (ii) follow.

(iii) and (iv) follow immediately from (i) and (ii) respectively.

(v) The result follows immediately from Corollary 4.22(i) and 4.22(ii).

(vi) By Lemma 6.2(i), the equation $(n+x)*x = z$ has a solution if $z \neq \rho(n-1)$ and has no solution if $z = \rho(n-1)$. Hence, the result follows since any $\sigma \in \text{Aut } \mathcal{D}$ preserves Skolem symmetric matrices of Lemma 4.19. $\square$

4.24 Lemma *Let $\mathcal{D} = (V, \mathcal{B})$ be a Skolem design, $\sigma \in \mathrm{Aut}\ \mathcal{D}$ and let M be a 3×3 matrix with elements from V such that its rows and columns are valid blocks of $\mathcal{B}$. If any two distinct rows $B_x = \{(x,i),(x,i+1),(x,i+2)\}$ and $B_y = \{(y,j),(y,j+1),(y,j+2)\}$ where $x \neq y$ and $0 \leq x,y \leq (n-1)$ are of type 1 blocks, then the third row contains a type 1 block, $x \equiv y \pmod 2$, every column contains a type 3 block and $\sigma(M)$ is of the same form of M.*

Proof. Without loss of generality, let the first row and the second row be $B_x = \{(x,i),(x,i+1),(x,i+2)\}$ and $B_y = \{(y,j),(y,j+1),(y,j+2)\}$ respectively, where $x \neq y$ and $0 \leq x,y \leq (n-1)$. It follows that no column contains type 1 block since $x \neq y$. In addition, no column also contain type 2 block, since $0 \leq x,y \leq (n-1)$.

Now, if $i = j$, then we have that $\Pi_1(M_{3c}) = x * y$ for all columns.

On the other hand, if $i \neq j$ then there are three possibilities.

Case 1: $\Pi_1(M_{3c}) = z = x * y$

Case 2: $\Pi_1(M_{3c}) = z, z * x = y$

Case 3: $\Pi_1(M_{3c}) = z, z * y = x$

In all these three cases, the result is similar to the case $i = j$. Hence the proof follows since M must be preserved by automorphisms. $\square$

For instance, if $\Pi_1(M_{3c}) = x * y$ for all columns, then M is of the form:

$$\begin{pmatrix} (x,i) & (x,i+1) & (x,i+2) \\ (y,i) & (y,i+1) & (y,i+2) \\ (x*y,i+1) & (x*y,i+2) & (x*y,i) \end{pmatrix}.$$

4.25 Proposition *Let $\sigma \in \mathrm{Aut}\ \mathcal{D}$, then $\Pi_1(\sigma(x,i)) = x$, for all $x \in \mathrm{Q}$ and $i \in \mathbb{Z}_3$.*

Proof. By Lemma 6.2(iii), $x * y = 0$ has no solution and by Lemma 6.2(iv), $x * y = n-1$ also has no solution. By considering the matrices of Lemma 4.24, it follows that $\Pi_1(\sigma(x,i)) \in \{0, n-1\}$ when $x \in \{0, n-1\}$.

Now, suppose $n = 2k+1$. Then $\rho(n-1) = k \in \mathrm{Q}^1$. Consider the matrices of Lemma 4.19. By Lemma 4.23(vi), $\Pi_1(\sigma(\rho(n-1),i)) = \Pi_1(\sigma(k,i)) = k$.

By Lemma 4.23(iii), $\Pi_1(\sigma(3k+1, i)) = 3k+1$ and by Corollary 4.22(i), $\Pi_1(\sigma((k*(3k+1)), i+1)) = 4k+1 \in \mathrm{Q}^2$.

Again by Lemma 4.23(iii), $\Pi_1(\sigma(4k+1-n, i)) = \Pi_1(\sigma(n-1, i)) = n-1$. Therefore $\Pi_1(\sigma(0, i)) = 0$ and $\Pi_1(\sigma(n-1, i)) = n-1$.

Suppose $n = 2k$. Then $\rho(n-1) = \rho(2k-1) = 3k-1 \in \mathrm{Q}^2$. Again, consider the matrices of Lemma 4.19. By Lemma 4.23(vi), $\Pi_1(\sigma(\rho(n-1), i)) = \Pi_1(\sigma(3k-1, i)) = 3k-1$.

By Lemma 4.23(iii), $\Pi_1(\sigma(k-1, i)) = k-1$ and by Corollary 4.22(i), $\Pi_1(\sigma((k-1*(3k-1)), i+1)) = \Pi_1(\sigma(\rho((4k-2) \pmod{4k}), i+1))) = \Pi_1(\sigma(\rho(4k-2, i+1))) = 2k-1 = n-1 \in \mathrm{Q}^1$.

Again, $\Pi_1(\sigma(0, i)) = 0$ and $\Pi_1(\sigma(n-1, i)) = n-1$.

Now, to complete the proof, it is enough to show that $\Pi_1(\sigma(x, i)) = x$ for all $x \in \mathrm{Q}^1$ by Lemma 4.23(iii).

Let $x = 0$. Then by Lemma 4.23(iii), $\Pi_1(\sigma(n, i)) = n$ and so by Lemma 4.23(iv), $\Pi_1(\sigma(1, i+2)) = 1$ from the matrices in (4.12). Hence, by induction $\Pi_1(x, i+1) = x$ for all $x \in \mathrm{Q}^1$. $\square$

Now, on the other hand, we have that translations $\sigma_i : \mathcal{D} \longrightarrow \mathcal{D}$ defined by

$$\sigma_i(x, j) = (x, i+j),$$

for $i \in \mathbb{Z}_3$ are clearly automorphisms of the designs. We therefore have the following:

4.26 Theorem *Let $n \in \mathbb{N}, n \geq 3$ and let $\mathcal{D} = (V, \mathcal{B})$ be a Skolem design. Then* Aut $\mathcal{D}$ *is isomorphic to* $\mathbb{Z}_3$.

Proof. By Proposition 4.25 and Lemma 4.23(v), the result follows. $\square$

4.2.1 Automorphism group of Skolem quasigroups

In this section we explore the symmetry of the quasigroups; proving that there exist no non-trivial automorphism of the quasigroup. We will contrast the behaviour of automorphism of the designs and those of the quasigroup.

Recall that if $(\mathrm{P}, *)$ and $(\mathrm{Q}, \circ)$ are quasigroups, a function

$$\alpha : \mathrm{P} \to \mathrm{Q}$$

is a *quasigroup homomorphism* if $\alpha(x) \circ \alpha(y) = \alpha(x*y)$ holds for all $x, y \in \mathrm{P}$. Should $(\mathrm{P}, *)$ and $(\mathrm{Q}, \circ)$ coincide and α be a bijection, then α is said to be an automorphism. The set of automorphisms of a quasigroup Q forms a group under composition and is denoted by Aut Q.

4.27 Lemma *Let* $\mathrm{Q}^1, \mathrm{Q}^2$ *be as defined in* (4.9) *and* (4.10) *respectively and let* $x, y, x', y' \in \mathrm{Q}^1$, $w \in \mathrm{Q}^2$ *and* $\alpha \in$ Aut Q. *Then*

(i) $\alpha(x) \in \mathrm{Q}^1$ *and* $\alpha(w) \in \mathrm{Q}^2$;

(ii) $\alpha(n + x) = n + \alpha(x)$;

(iii) *if* $x + y = x' + y'$, *then* $\alpha(x) + \alpha(y) = \alpha(x') + \alpha(y')$.

Proof. (i) Since idempotents are mapped to themselves, the result follows from Lemma 3.9(ii).

(ii) By (i), given $x \in \mathrm{Q}^1$, $\alpha(n + x) = n + y$ for some $y \in \mathrm{Q}^1$. Then

$$\begin{aligned}
\alpha(x) &= \alpha((n + x) * (n + x)) \\
&= \alpha(n + x) * \alpha(n + x) \\
&= (n + y) * (n + y) \\
&= y.
\end{aligned}$$

Hence $\alpha(n + x) = n + y = n + \alpha(x)$.

(iii) By (i), we have that $\alpha(x), \alpha(y) \in \mathrm{Q}^1$.

Now,

$$\begin{aligned}
& x * y = \rho(x + y) = \rho(x' + y') = x' * y'; \\
& \Longrightarrow \alpha(x * y) = \alpha(x' * y'); \\
& \Longrightarrow \alpha(x) * \alpha(y) = \alpha(x') * \alpha(y'); \\
& \Longrightarrow \rho(\alpha(x) + \alpha(y)) = \rho(\alpha(x') + \alpha(y')); \\
& \Longrightarrow \alpha(x) + \alpha(y)) = \alpha(x') + \alpha(y'). \qquad (\rho \text{ is one-one})
\end{aligned}$$

□

4.28 Theorem *For all n, there exist no non-trivial automorphism of* Q.

Proof. By Lemma 4.27(ii), the cycle structure of α on Q^2 is the same as on Q^1. Hence it is enough to determine the cycle structure of α on Q^1.

By Lemma 4.27(iii), we have

$$\alpha(x+1) = \alpha(x) + \alpha(1) - \alpha(0). \tag{4.16}$$

By induction on y, if $x, y \in \mathrm{Q}^1$, we have from (4.16) that

$$\alpha(x+y) = \alpha(x) + y(\alpha(1) - \alpha(0)) \tag{4.17}$$

provided $(x+y) \in \mathrm{Q}^1$.

Now, letting $x = 0$ in (4.17), then for any $y \in \mathrm{Q}^1$,

$$\alpha(y) = y(\alpha(1) - \alpha(0)) + \alpha(0). \tag{4.18}$$

We now see that $\alpha(y)$ depends on $\alpha(1) - \alpha(0)$.

Case 1: $\alpha(1) - \alpha(0) = 0$. This is impossible since α is one-one.

Case 2: $\alpha(1) - \alpha(0) < 0$. That is, $\alpha(1) - \alpha(0) \leq -1$. Let $\alpha(0) = u$. Clearly,

$$u > 0 \text{ and } \alpha(1) - u + 1 \leq 0. \tag{4.19}$$

From (4.18) and (4.19), we have

$$\alpha(u) = u(\alpha(1) - u) + u = u(\alpha(1) - u + 1) \leq 0.$$

This implies $\alpha(1) - u + 1 = 0$, because otherwise $\alpha(u) < 0$ which is impossible. Therefore $\alpha(1) = u - 1$ and (4.18) then reads

$$\alpha(y) = y((u-1) - u) + u = u - y \in \mathrm{Q}^1 \text{ for any } y \in \mathrm{Q}^1. \tag{4.20}$$

In other words, α is the product of the (disjoint) transpositions $(0\ u)(1\ u-1)(2\ u-2)\ldots$

It follows that

$$u = \alpha(0) = n - 1 \tag{4.21}$$

because for $y = n-1$, (4.20) gives $\alpha(n-1) = u - (u-1) \in \mathrm{Q}^1$ and $u-(u-1) \geq 0$, $u \geq n-1$. On the other hand, $u = \alpha(0) \in \mathrm{Q}^1$ implies $u \leq n-1$, hence equality. Therefore $\alpha = (0\ u)(1\ u-1)(2\ u-2)\ldots$ and in particular,

$$\alpha(1) = n-2. \tag{4.22}$$

Now,

$$0 * 1 = \rho(1) = n. \tag{4.23}$$

Hence by Lemma 4.27(i) and (4.22),

$$\alpha(0*1) = \alpha(n) = n + \alpha(0) = n + (n-1) = 2n-1. \tag{4.24}$$

From (4.21) and (4.22),

$$\alpha(0) * \alpha(1) = (n-1) * (n-2) = \rho(2n-3) = n + \frac{(2n-4)}{2} = 2n-2.$$

Therefore, $\alpha(0)*\alpha(1) \neq \alpha(0*1)$, contrary to α being an automorphism.

This contradiction implies that the case $\alpha(1) - \alpha(0) < 0$ cannot arise.

Case 3: $\alpha(1) - \alpha(0) > 0$. This implies $\alpha(1) - \alpha(0) \geq 1$.

Suppose $\alpha(1) - \alpha(0) \geq 2$, since we are dealing with integers which also include the case $\alpha(0) = 0$, then (4.18) implies $\alpha(y) \geq 2y + \alpha(0) \geq 2y$.

Now, let $y \geq \left[\frac{n}{2}\right]$, then $\alpha(y) \geq n$. Thus we have that $\alpha(y) \notin \mathrm{Q}^1$ for $y = \left[\frac{n}{2}\right] \in \mathrm{Q}^1$, a contradiction to (i).

Consequently, $\alpha(1) - \alpha(0) = 1$. Hence (4.18) becomes

$$\alpha(y) = y + \alpha(0) \text{ for any } y \in \mathrm{Q}^1. \tag{4.25}$$

If $\alpha(0) > 0$, then $n - \alpha(0) \in \mathrm{Q}^1$ and by (4.25), $\alpha(n - \alpha(0)) = n \notin \mathrm{Q}^1$. This again is a contradiction to (i).

Hence $\alpha(0) = 0$ and the result follows. $\square$

We now consider automorphism groups of Steiner triple systems from the projective and affine geometries.

4.3 Automorphism groups of projective and affine triple systems

It will be evident that the automorphism group of the projective and affine triple systems are linked to the general linear group $\mathrm{GL}(n, \mathbb{F})$.

4.4 Definition Let $\mathrm{PG}(n, \mathbb{F})$ and $\mathrm{PG}(n', \mathbb{F}')$ be projective spaces. The map $\sigma : \mathbb{F}_q^{n+1} \to \mathbb{F}_{q'}^{n'+1}$ such that:

(i) σ is a bijection;

(ii) the images of collinear points are also collinear.

is called a *collineation*.

By Definition 4.4, it is clear that a collineation is an isomorphism. Should $\mathrm{PG}(n, \mathbb{F}) = \mathrm{PG}(n', \mathbb{F}')$, then a collineation is called an automorphism. The set of all collineations of a space to itself form a group under composition of functions.

We now discuss the automorphism groups of the projective and affine geometries.

4.3.1 The Fundamental Theorem of Projective Geometry

Any element of the general linear group $\mathrm{GL}(n + 1, \mathbb{F})$ maps subspaces of V into subspaces of the same dimension, and preserves inclusion; so it induces a collineation on $\mathrm{PG}(n, \mathbb{F})$. The group $\mathrm{Aut}\ \mathbb{F}$ of automorphisms of $\mathbb{F}$ has a coordinate-wise action on V^{n+1}; these transformations also induce collineations. The group generated by $\mathrm{GL}(n + 1, \mathbb{F})$ and $\mathrm{Aut}\ \mathbb{F}$, that is, the semi-direct product of $\mathrm{GL}(n+1, \mathbb{F})$ and $\mathrm{Aut}\ \mathbb{F}$, is denoted by $\Gamma\mathrm{L}(n+1, \mathbb{F})$. Its elements are called semi-linear transformations. The groups of collineation of $\mathrm{PG}(n, \mathbb{F})$ induced by $\mathrm{GL}(n + 1, \mathbb{F})$ and $\Gamma\mathrm{L}(n + 1, \mathbb{F})$, are denoted by $\mathrm{PGL}(n + 1, \mathbb{F})$ and $\mathrm{P}\Gamma\mathrm{L}(n + 1, \mathbb{F})$, respectively.

By and large, a semi-linear transformation from one vector space to another is the composition of a linear transformation and a coordinate-wise field automorphism of the target space.

In linear algebra, a semi-linear transformation between two vector spaces V and W over a field $\mathbb{F}$ is a function that is a linear transformation up to a field automorphism of the vector space. That is, $T : V \to W$ and

(i) T is linear with respect to vector addition: $T(V+V^{'}) = T(V)+T(V^{'})$;

(ii) T is semi-linear with respect to scalar multiplication: $T(\lambda v) = \lambda^{\sigma} T(v)$, where σ is a field automorphism of $\mathbb{F}$, and λ^{σ} is the image of the scalar λ under the automorphism.

4.29 Lemma [15] *In a projective space* $\mathrm{PG}(n, \mathbb{F})$*, two semi-linear transformations which induce the same collineation differ only by a scalar factor.*

Proof. We have to show that a semi-linear transformation which fixes every point of $\mathrm{PG}(n, \mathbb{F})$ is a scalar multiplication.

Now, let $v \to v^{\sigma} A$ fix every point of $\mathrm{PG}(n, \mathbb{F})$, where $\sigma \in \mathrm{Aut}\ \mathbb{F}$ and $A \in \mathrm{GL}(n+1, \mathbb{F})$. Then every vector is mapped to a scalar multiple of itself. Let $e_0, \cdots, e_n$ be the standard basis for V. Then $e_i A = \lambda_i e_i$, for $i = 0, \cdots, n$, and

$$(e_0 + \cdots + e_n)A = \lambda_0 e_0 + \cdots + \lambda_n e_n = \lambda(e_0 + \cdots + e_n),$$

so $\lambda_0 = \cdots = \lambda_n = \lambda$, since σ fixes the standard basis vectors. Now, for any $\alpha \in F$, the vector $(1, \alpha, 0, \cdots, 0)$ is mapped to the vector $(\lambda, \alpha^{\sigma}\lambda, 0, \cdots, 0)$; so we have $\lambda\alpha = \alpha^{\sigma}\lambda$. Thus $v^{\sigma} A = v^{\sigma}\lambda = \lambda v$ for any vector v, as required. $\square$

Note that the field automorphism σ is a conjugation by the element λ. That is, $\alpha^{\sigma} = \lambda\alpha\lambda^{-1}$; in other words, an inner automorphism.

We now consider the semi-linearity of such isomorphisms.

4.5 Definition Let $\mathrm{PG}(n, \mathbb{F})$ be a projective space. An $(n+2)-$tuple of points is called special if no $(n+1)$ of them are linearly dependent.

There is a linear map carrying any special tuple to another in the same space, or another space of the same dimension over the same field. For, given a special tuple in the first space, spanning vectors for the first $(n+1)$ points form a basis $e_0, \cdots, e_n$, and the last point is spanned by a vector with all coordinates non-zero relative to the basis. Considering the action of the basis vector by scalar factors, we may assume that the last point is spanned by $e_0 + \cdots + e_n$. Similarly, the points of a special tuple in the second space are spanned by the vectors of a basis $b_0, \cdots, b_n$, and $b_0 + \cdots + b_n$. The unique linear transformation carrying the first basis to the second also carries the first special tuple to the second.

Let ϕ be any isomorphism, then there is a linear map $\bar{\phi}$ which acts in the same manner as ϕ on a special $(n+2)-$tuple. Composing ϕ with the inverse of $\bar{\phi}$ we obtain an automorphism of PG$(n, \mathbb{F})$ which fixes the $(n+2)-$tuple point-wise.

4.30 Lemma [15]*Let ϕ be any isomorphism of the projective space $PG(n, \mathbb{F})$, and $\bar{\phi}$ be a linear map which acts in the same manner as ϕ on a special $(n+2)-$tuple. The automorphism obtained from composing ϕ with the inverse of $\bar{\phi}$, which fixes the $(n+2)-$tuple point-wise is the product of a scalar and a field automorphism.*

Proof. As shown above, left and right multiplications by λ differ by an inner automorphism. Let ζ be a collineation fixing the spans of $e_0, e_1, \cdots, e_n$ and $e_0 + e_1, + \cdots + e_n$. This can be written as $(1, 0, \cdots, 0), (0, 1, \cdots, 0), (0, 0, 1, \cdots, 0), \cdots, (1, 1, \cdots, 1)$ by collineation and its general point is denoted $(x_1, \cdots, x_n)$.

The points on the line $(x_0, 0, \cdots, x_n)$, apart from $(1, 0, \cdots, 0)$, have the form $(x, 0, \cdots, 1)$ for $x \in \mathbb{F}$, and so can be identified with elements of $\mathbb{F}$.

Now, the bijection between this set and the set of points on $(0, x_2, \cdots, 1)$ on the line $(0, x_1, \cdots, x_n)$, given by $(x, 0, \cdots, 1) \longmapsto (0, x, \cdots, 1)$, can be geometrically defined in a way which is invariant under collineations fixing the $n-$tuple. Doing this, the coordinates of all points in the plane are determined. Also the operations of addition and multiplication in $\mathbb{F}$ can be defined geometrically in the same sense. It follows that any collineation fixing any finite points induces an automorphism of the field $\mathbb{F}$, and its actions on the coordinates agree. $\square$

4.31 Theorem [15]*[The fundamental theorem of projective geometry] Any isomorphism between projective spaces of dimension at least 2 is induced by a semi-linear transformation between the underlying vector spaces, unique up to scalar multiplication.*

Proof. The proof follows directly from lemmas 4.29 and 4.30 above. $\square$

4.32 Corollary *Isomorphic projective spaces of dimension at least* 2 *have the same dimension and are coordinatised by isomorphic fields.*

4.33 Corollary (a) *For* $n > 1$, *the collineation group of* $\mathrm{PG}(n, \mathbb{F})$ *is the group* $\mathrm{P\Gamma L}(n, \mathbb{F})$.

(b) *The kernel of the action of* $\Gamma\mathrm{L}(n+1, \mathbb{F})$ *on* $\mathrm{PG}(n, \mathbb{F})$ *is the group of non-zero scalars* (*acting by left multiplication*).

The theorem is called the Fundamental Theorem of Projective Geometry because the algebraic structure of the underlying vector space can be recovered from the incidence geometry of the projective space. It is assumed that $n > 1$ because the only proper subspaces of a projective line are its points, and so any bijection is an isomorphism, and the collineation group is the full symmetric group.

In view Proposition 3.13, Theorem 4.31 and Corollary 4.33, we have that the automorphism group of $\mathrm{PG}(n, 2)$ is $\mathrm{GL}(n+1, 2)$.

We recall that the affine plane can be realized from the projective plane and vice versa. Hence, by similar argument of Theorem 4.31 and Corollary 4.33, coupled with Proposition 3.14, we have that the automorphism group of $\mathrm{AG}(n, q)$ is $(3^n) \times \mathrm{GL}(n, 3)$.

In connection to the Bose Steiner triple system, we have:

4.34 Theorem [8] *Let* $G \cong (\mathbb{Z}_3)^n$ *consisting of the direct product of* n *copies of* $\mathbb{Z}_3$, *where the blocks are all triples* $\{x, y, z\}$ *such that* $x, y, z \in \mathbb{Z}_3$, *and* $x \neq y \neq z$. *Let* $\mathbb{B}_n$ *be the Steiner triple system of order* 3^n *formed on the elements of* G. *The full automorphism group of* $\mathbb{B}_n$ *is isomorphic to* $\mathrm{Hol}(G)$.

By Theorem 4.34, the full automorphism group of the design on G_5 in Example 6 which is the affine geometry AG(5, 3) is isomorphic to $\mathrm{Hol}(G_5)$.

As discussed in Chapter 3,

$$|\mathrm{Aut}\ G| = |\mathrm{GL}(5, \mathbb{Z}_3)| = \prod_{j=0}^{4} (3^5 - 3^j).$$

Hence $\mathrm{AG}(5, 3)$ is of order $|G_5||\mathrm{Aut}(G_5)| = 3^5(3^5 - 1) \times (3^5 - 3) \times (3^5 - 9) \times (3^5 - 27) \times (3^5 - 81) = 115562653240320$.

We now discuss the block intersection graphs of the fundamental object of our study.

Chapter 5

Block intersection graphs and their properties

There are different ways of constructing graphs from Steiner triple systems. One of such considerations is a complete graph on v vertices, K_v. The decomposition of K_v into edge disjoint triangles K_3 is equivalent to a Steiner triple system. We consider the block intersection graphs of Steiner triple systems and we intend to study their automorphism groups in the next chapter.

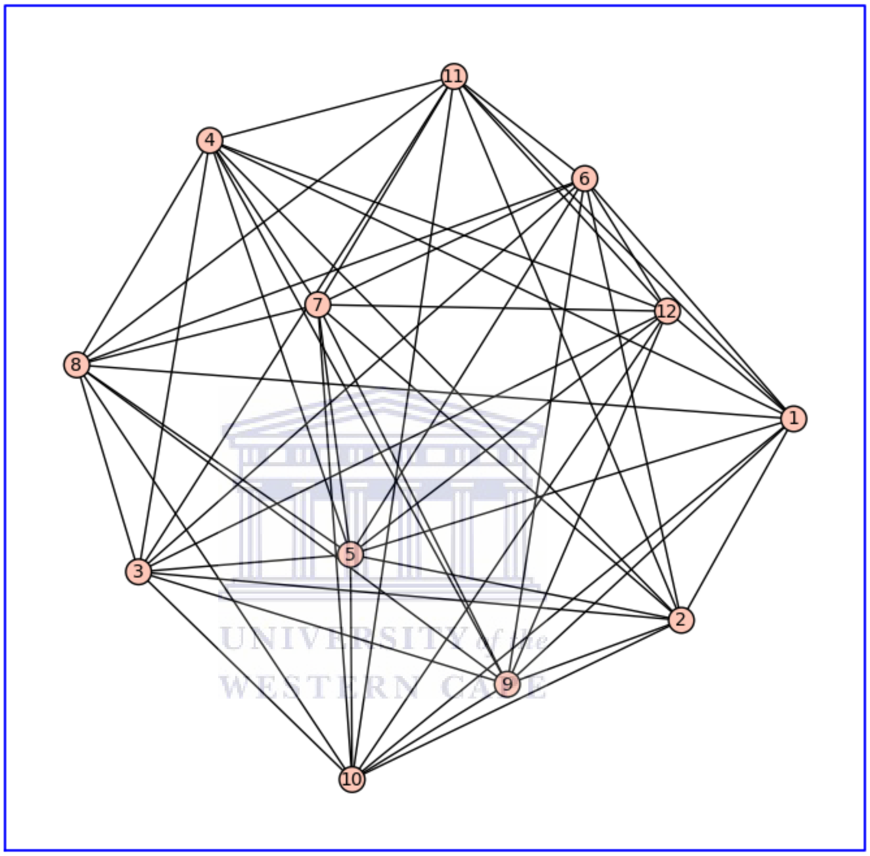
5.1 Definition Let $\mathbb{D} = (V, \mathcal{B})$ be a Steiner triple system. The block intersection graph $\Gamma = (\mathcal{B}, E)$ of $\mathbb{D}$ is the graph with vertices, the set of blocks $\mathrm{B} \in \mathcal{B}$ and for any $\mathrm{B}, \mathrm{B}' \in \mathcal{B}$ such that $\mathrm{B} \cap \mathrm{B}' \neq \varnothing$, $[\mathrm{B}, \mathrm{B}'] \in E(\Gamma)$.

7 Example Let $V = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0),$ $(2,1), (2,2)\}$, and

$$\begin{aligned}\mathcal{B} = \{&\{(0,0),(0,1),(0,2)\}, \{(0,0),(1,0),(2,0)\}, \{(1,0),(1,1),(1,2)\},\\ &\{(0,0),(1,2),(2,1)\}, \{(0,0),(1,1),(2,2)\}, \{(0,1),(1,0),(2,2)\},\\ &\{(2,0),(2,1),(2,2)\}, \{(0,1),(1,1),(2,1)\}, \{(0,1),(1,2),(2,0)\},\\ &\{(0,2),(1,1),(2,0)\}, \{(0,2),(1,0),(2,1)\}, \{(0,2),(1,2),(2,2)\}\}\end{aligned}$$

as in Example 5. The figure below is a block intersection graph of the design AG(2,3). For convenience, we denote the elements of the set of vertices above as the elements of the set $\{1, 2, \ldots, 12\}$ respectively.

Figure 5.1: A block intersection graph of AG(2,3)



Vertices	Blocks
1	{ (0,0), (0,1), (0,2)}
2	{ (0,0), (1,0), (2,0)}
3	{ (1,0), (1,1), (1,2)}
4	{ (0,0), (1,2), (2,1)}
5	{ (0,0), (1,1), (2,2)}
6	{ (0,1), (1,0), (2,2)}
7	{ (2,0), (2,1), (2,2)}
8	{ (0,1), (1,1), (2,1)}
9	{ (0,1), (1,2), (2,0)}
10	{ (0,2), (1,1), (2,0)}
11	{ (0,2), (1,0), (2,1)}
12	{ (0,2), (1,2), (2,2)}

We now explore the properties of block intersection graphs.

5.1 Elementary properties of block intersection graphs

The vertices of the block intersection graphs are defined by the blocks of the designs of Steiner triple systems. Thus, for all block intersection graphs of an admissible order v, the number of vertices is the same as the number of blocks of the design. Hence, there are $\dfrac{v(v-1)}{6}$ vertices in a block intersection graph of Steiner triple systems. We now discuss the degree of a vertex in block intersection graphs and their regularity.

5.1 Lemma *Let* $(V, \mathcal{B})$ *be a Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Then the degree* $\deg(\mathrm{B})$ *of a vertex* $\mathrm{B} \in \mathrm{V}(\Gamma)$ *is exactly* $3\left(\dfrac{v-3}{2}\right)$.

Proof. The degree of a vertex of a graph is the number of edges incident on the vertex. By Corollary 3.2, an arbitrary point $x \in V$ is in exactly $(\dfrac{v-1}{2} - 1) = \dfrac{v-3}{2}$ other vertices. Hence, the degree of a vertex is exactly $3\left(\dfrac{v-3}{2}\right)$, since each vertex is made up of 3 points. □

Clearly, every vertex has equal degree. Therefore the block intersection graphs are regular graphs with degree $\dfrac{3(v-3)}{2}$.

The total number of edges $|\mathrm{E}|$ is easily computed by the hand shaking lemma, since the block intersection graphs are regular graphs. Hence, $2|\mathrm{E}| = \sum_{\mathrm{B} \in \mathcal{B}} \deg(\mathrm{B})$ and the total number of edges

$$|\mathrm{E}| = \frac{\frac{v(v-1)}{6} \times \frac{3(v-3)}{2}}{2} = \frac{v(v-1)(v-3)}{8}.$$

Block intersection graphs are rich in symmetry. It is shown below that they are strongly regular graphs.

One of the important parameters of the definition of a strongly regular graph is adjacency parameters (See Definition 2.11). In block intersection graphs, it is obvious that any two adjacent vertices must be adjacent to some other vertices. It is also clear that a point $x \in V$ is in exactly $\frac{v-1}{2}$ vertices which implies that vertices containing the point $x \in V$ must be adjacent to each other. Hence, there is need to critically examine the adjacency of block intersection graphs.

Let $(V, \mathcal{B})$ be a Steiner triple system of order v. Given any three vertices $\mathrm{B}_1, \mathrm{B}_2, \mathrm{B}_3 \in \mathcal{B}$ of a block intersection graph $\Gamma = (\mathcal{B}, \mathrm{E})$, there are two possibilities if any two of the vertices must be adjacent. We use this distinction to classify adjacency.

Case 1: ($[\mathrm{B}_1, \mathrm{B}_2] \cap [\mathrm{B}_1, \mathrm{B}_3] \cap [\mathrm{B}_2, \mathrm{B}_3] = x$, for some $x \in V$). There exists a common point in $\mathrm{B}_1, \mathrm{B}_2$ and B_3 deciding edges between any two of the three vertices.

Case 2: ($[\mathrm{B}_1, \mathrm{B}_2], [\mathrm{B}_1, \mathrm{B}_3], [\mathrm{B}_2, \mathrm{B}_3] \in \mathrm{E}(\Gamma)$ and $\mathrm{B}_1 \cap \mathrm{B}_2 \cap \mathrm{B}_3 = \varnothing$). The point deciding an edge between a first vertex and a second differs from the point determining an edge between the first and a third.

In view of the two possibilities above, we shall classify adjacency in this study in the following:

5.2 Definition (i) An adjacency defined by **Case 1** above is called **type I adjacency**.

(ii) An adjacency defined by **Case 2** above is called **type II adjacency**.

We now discuss the type I adjacency of the block intersection graphs of Steiner triple systems.

5.2 Lemma *Let $(V, \mathcal{B})$ be a Steiner triple system of order v and $\Gamma = (\mathcal{B}, \mathrm{E})$ be a block intersection graph. Then any two adjacent vertices have $\frac{v-5}{2}$ common neighbours of type* I *adjacency .*

Proof. Let B_1 and B_2 be adjacent vertices. Then there exists an $x \in V$: $x \in \mathrm{B}_1 \cap \mathrm{B}_2$. It follows from Corollary 3.2 that B_1 and B_2 are incident to $\frac{v-1}{2} - 2$ other vertices. □

We now discuss the type II adjacency of the block intersection graphs of Steiner triple systems.

5.3 Lemma *Let* $(V, \mathcal{B})$ *be a Steiner triple system of order* $v > 7$ *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Then two adjacent vertices are commonly adjacent to four vertices of type* (II) *adjacency of which form a* $4-$*cycle.*

Proof. We will prove this by building other vertices from any two given set of adjacent vertices.

Suppose $[\mathrm{B}_1, \mathrm{B}_2] \in \mathrm{E}(\Gamma)$, then $\mathrm{B}_1 \cap \mathrm{B}_2 \neq \varnothing$. So, without loss of generality $\mathrm{B}_1 = \{x_1, x_2, x_3\}$ and $\mathrm{B}_2 = \{x_1, x_4, x_5\}$. Hence, each pair $(x_2, x_4), (x_2, x_5)$, (x_3, x_4) and (x_3, x_5) are without loss of generality contained in distinct blocks $\mathrm{B}_3 = \{x_2, x_4, x_6\}$, $\mathrm{B}_4 = \{x_2, x_5, x_7\}$, $\mathrm{B}_5 = \{x_3, x_4, x_8\}$, and $\mathrm{B}_6 = \{x_3, x_5, x_9\}$. Clearly, $\mathrm{B}_3, \cdots, \mathrm{B}_6$ form a $4-$cycle and each one of them is incident to B_1 and B_2. $\square$

The next lemma discusses the total number of common neighbours of any two adjacent vertices of the block intersection graphs.

5.4 Lemma *Let* $(V, \mathcal{B})$ *be a Steiner triple system of order* $v > 7$ *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Then, the total number of all common neighbours of any two adjacent vertices, that is of type* I *and type* II *adjacency is* $\left(\dfrac{v+3}{2}\right)$.

Proof. The proof follows immediately from Lemmas 5.2 and 5.3. $\square$

We now discuss the total number of common neighbours of any two non-adjacent vertices.

5.5 Lemma *Let* $(V, \mathcal{B})$ *be a Steiner triple system of order* $v > 7$, $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph, and let* $\mathrm{B}, \mathrm{B}' \in \mathrm{V}(\Gamma)$ *be non-adjacent vertices. Then* B *and* B′ *have 9 common adjacent vertices.*

Proof. Without loss of generality, suppose $\mathrm{B} = \{x_1, x_2, x_3\}$ and $\mathrm{B}' = \{x_4, x_5, x_6\}$, and $\mathrm{B} \cap \mathrm{B}' \neq \varnothing$. For $x_i, i = 1, 2, 3$, and $x_j, j = 4, 5, 6$, each pair (x_i, x_j), is contained in a unique block B''. So B and B′ have a common vertex B''. Now between B and B′, there are 9 distinct pairs. The result therefore follows. $\square$

Note that in the smallest case of $v = 9$, B and B$'$ occupy 6 non common points in V. Hence, each of the 3 remaining points can then go through 3 pairs each of the nine pairs (x_i, x_j), $x_i \in$ B, $x_j \in$ B$'$.

Note that because of symmetry, block intersection graphs are strongly regular graphs, of which we show below.

5.6 Proposition *Let $(V, \mathcal{B})$ be a Steiner triple system of order $v > 7$. Then the block intersection graph $\Gamma = (\mathcal{B}, \mathrm{E})$ is strongly regular with parameters*

$$\left(\frac{v(v-1)}{6}, \frac{3(v-3)}{2}, \frac{v+3}{2}, 9\right).$$

Proof. The proof follows immediately from Lemmas 5.4 and 5.5 in addition to the fact that the degree of every vertex is $\dfrac{3(v-3)}{2}$ and the total number of vertices in $\Gamma = (\mathcal{B}, \mathrm{E})$ is $\left(\dfrac{v(v-1)}{6}\right)$. $\square$

Strongly regular graphs have been well characterized. Hence, they demonstrate the highly structured nature of the block intersection graphs of Steiner triple systems. We are particularly interested in the connectivity of strongly regular graphs.

It is an established fact that in a strongly regular graph Γ, the connectivity $\kappa(\Gamma)$ is the same as its degree [1].

We now explore more properties of our specific designs in Chapter 3.

5.2 Vertex types and neighbourhoods in block intersection graphs of Steiner triple systems

In this section, we discuss symmetry of the block intersection graphs that are defined by differences in block types of Steiner triple systems of our consideration. We pay particular attention to the Bose and Skolem Steiner triple systems.

We also study the neighbourhoods of the Bose and Skolem Steiner triple systems because they help in describing cliques and independent sets that are used later in this study.

We begin with the Bose Steiner triple systems.

Recall that the Bose Steiner triple system consists of 2 block types. For brevity, we shall call the type 1 blocks of the Bose Steiner triple systems *type* 1 *vertices* and the type 2 blocks are called *type* 2 *vertices*. Hence, there are $\frac{v}{3}$ type 1 vertices and $\frac{v(v-3)}{6}$ type 2 vertices of the block intersection graphs of Bose Steiner triple systems.

5.7 Lemma *Let* $(V, \mathcal{B})$ *be a Bose Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Let* $\mathrm{B}, \mathrm{B}' \in \mathrm{V}(\Gamma)$ *be type* 1 *vertices in* Γ. *Then,* $[\mathrm{B}, \mathrm{B}'] \notin \mathrm{E}(\Gamma)$ *and* B *and* B′ *has exactly* $\frac{3(v-3)}{2}$ *type* 2 *neighbours each.*

Proof. Clearly type 1 blocks have no common points. Hence all the neighbours of any type 1 block are clearly type 2 vertices. □

5.8 Lemma *Let* $(V, \mathcal{B})$ *be a Bose Steiner triple system of order* $v > 9$ *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Let* $\mathrm{B} = \{(x, i), (y, i), (x * y, i+1)\}$ *be a type* 2 *vertex in* Γ. *Then,* B *has exactly* 3 *type* 1 *neighbours.*

Proof. We recall that $x * y = \pi(x + y) = \left(\frac{n+1}{2}\right)(x + y) \mod (2n + 1)$. Hence, $x * y \neq x \neq y$. Therefore, each of the three points of B has a corresponding type 1 vertex of the form: $\mathrm{B}_1 = \{(x, i), (x, i + 1), (x, i + 2)\}, \mathrm{B}_2 = \{(y, i), (y, i+1), (y, i+2)\}$ and $\mathrm{B}_3 = \{(x*y, i+1), (x*y, i+2), (x*y, i)\}$. □

We now discuss neighbourhoods in Skolem Steiner triple systems

By the remark of Example 3, Skolem Steiner triple systems consist of $\left(\frac{(v-1)}{6}\right)$ type 1 blocks, $\left(\frac{(v-1)}{2}\right)$ type 2 blocks and $\left(\frac{(v-1)(v-4)}{6}\right)$ type 3 blocks. The type 1, type 2 and type 3 blocks are hereinafter called type 1, type 2 and type 3 vertices respectively.

5.9 Lemma *Let* $\mathbb{D} = (V, \mathcal{B})$ *be a Skolem Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph of* $\mathbb{D}$*. Let* B *and* $\mathrm{B}' \in \mathrm{V}(\Gamma)$ *be type* 1 *vertices in* Γ*. Then,* $[\mathrm{B}, \mathrm{B}'] \notin \mathrm{E}(\Gamma)$ *and each type* 1 *vertex has exactly* 3 *type* 2 *neighbours and* $\left(\dfrac{3v-15}{2}\right)$ *type* 3 *neighbours.*

Proof. Clearly, type 1 vertices are not neighbours of themselves. (See the definition of blocks of the Skolem Steiner triple systems)

The next task is to show that each of B and B′ are connected to 3 type 2 neighbours.

So, let $\mathrm{B} = \{(x,i),(x,i+1),(x,i+2)\}$, and $\mathrm{B}' = \{(x',i),(x',i+1),(x',i+2)\}$ Clearly, $(p,q),(x+n,i) \notin \mathrm{B}$ and $(p,q),(x+n,i) \notin \mathrm{B}'$ since (p,q) is a unique type 2 point and $(x+n) \pmod{2n} > x$ if $0 \leq x \leq (n-1)$, where n is half the order of the group. Thus, without loss of generality, the points $(x,0),(x,1)$ and $(x,2)$ are in exactly 3 type 2 neighbours of the form: $\mathrm{B}_1 = \{(p,q),(x+n,i),(x,i+1)\}$, $\mathrm{B}_2 = \{(p,q),(x+n,i),(x,i+2)\}$ and $\mathrm{B}_3 = \{(p,q),(x+n,i),(x,i)\}$. The same argument holds for B′.

We now finally show that there are $\left(\dfrac{3v-15}{2}\right)$ type 3 neighbours of each B and B′.

By Proposition 5.1, $\deg(\mathrm{B}) = \deg(\mathrm{B}') = \dfrac{3(v-2)}{2}$. By the previous argument, each point in B is in exactly 3 neighbours of type 2 vertices. Therefore, the remaining $\dfrac{3(v-2)}{2} - 3 = \dfrac{(3v-15)}{2}$ vertices are of type 3. The same argument holds for B′. $\square$

5.10 Corollary *Let* $(V, \mathcal{B})$ *be a Skolem Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Let* $\mathrm{B} \in \mathrm{V}(\Gamma)$ *be type* 2 *vertex in* Γ*. Then* B *has exactly one type* 1 *neighbour.*

We finally consider type 2 to type 2 neighbours and type 2 to type 3 neighbours.

5.11 Lemma *Let* $(V, \mathcal{B})$ *be a Skolem Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Let* $\mathrm{B} \in \mathrm{V}(\Gamma)$ *be type* 2 *vertex in* Γ*. Then,* B *has exactly* $\left(\dfrac{v-3}{2}\right)$ *type* 2 *to type* 2 *neighbours and* $(2v-7)$ *type*

3 *neighbours.*

Proof. There are exactly $\binom{\frac{v-1}{2}}{}$ type 2 vertices of Γ. The unique point (p,q) is common to all type 2 vertices. Therefore, B has a type (I) adjacency with all type 2 vertices. Hence B has $\frac{v-1}{2} - 1 = \frac{v-3}{2}$ type 2 to type 2 neighbours.

We now consider the type 3 neighbours.

By Proposition 5.1, $\deg(\mathrm{B}) = \frac{3(v-2)}{2}$. Therefore, B has $\frac{3(v-3)}{2} - \left(\frac{v-3}{2}\right) - 1 = (2v-7)$ neighbours of type 3 vertices, since each type 2 vertex has exactly one edge with type 1 vertices. $\square$

Having discussed the neighbourhoods of block intersection graphs that are defined by differences in block types of Steiner triple systems of our consideration, we can now describe cliques and independent sets of their block intersection graphs.

5.3 Cliques and independent sets in block intersection graphs of Steiner triple systems

The concepts of cliques and independent sets play important roles in graph theory and in this study, they are the basis of our discussion in Chapter 6.

In this subsection, we focus on cliques and independent sets to elaborate on the structure of the block intersection graphs.

First, we discuss the clique number as well as the least possible maximal cliques of block intersection graphs of Steiner triple systems.

5.12 Lemma *Let* $(V,\mathcal{B})$ *be a Steiner triple system of order* $v > 9$ *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Let* $\mathcal{B}' \subseteq \mathcal{B}$, *and* $\Gamma' = (\mathcal{B}', \mathrm{E}')$ *be a maximum clique of* Γ *such that* $\mathrm{E}'(\Gamma') \subseteq \mathrm{E}(\Gamma)$. *Then* $|\Gamma'| = \frac{(v-1)}{2}$.

Proof. Let $x_1, x_2, x_3 \in V$ such that $\{x_1, x_2, x_3\} \in \Gamma'$. By Corollary 3.2, each of the points x_1, x_2 and x_3 is in exactly $\dfrac{(v-1)}{2}$ vertices of Γ. Hence, by the type I adjacency which clearly has more vertices than the type II adjacency, there exist at least v cliques of size $\dfrac{(v-1)}{2}$.

Suppose to the contrary that Γ' can be extended by an additional adjacent vertex $\mathrm{B}'' \in \mathcal{B}$ then, it follows without loss of generality that $x_1 \in \mathrm{B}''$ which contradicts the fact that x_1 is in exactly $\dfrac{(v-1)}{2}$ vertices.

Hence, the clique number equals $\dfrac{(v-1)}{2}$. □

5.13 Corollary *Let $(V, \mathcal{B})$ be a Steiner triple system of order $v > 9$ and $\Gamma = (\mathcal{B}, \mathrm{E})$ be a block intersection graph. Let $\mathcal{B}' \subseteq \mathcal{B}$, and $\Gamma' = (\mathcal{B}', \mathrm{E}')$ be a maximum clique of Γ such that $\mathrm{E}'(\Gamma') \subseteq \mathrm{E}(\Gamma)$. Then the total number of maximum cliques is v.*

We now discuss the minimum maximal cliques in a block intersection graph.

5.14 Lemma *Let $(V, \mathcal{B})$ be a Steiner triple system of order $v > 7$ and $\Gamma = (\mathcal{B}, \mathrm{E})$ be a block intersection graph. Then there exist no maximal clique whose size is less than 4.*

Proof. By Lemma 5.3, any two adjacent vertices are commonly adjacent to four vertices of type (II) adjacency of which form a 4−cycle. Hence, the result follows. □

Next, we specifically discuss the cliques and the independent sets of the Bose and Skolem Steiner triple systems.

The block intersection graphs from the Bose Steiner triple systems are rich in symmetry. They have well structured cliques and independent set sizes, except in some special cases.

In addition to Lemmas 5.12 and 5.14, the following also hold for the block intersection graphs from Bose Steiner triple systems.

5.15 Lemma *Let $(V, \mathcal{B})$ be a Bose Steiner triple system of order v, $\Gamma = (\mathcal{B}, \mathrm{E})$ be a block intersection graph. Let B and B' be any two type 1 vertices* *in* Γ. *Then each clique of* Γ *containing a type* 1 *vertex has at most one vertex of type* 1.

Proof. By Lemma 5.7, $[\mathrm{B}, \mathrm{B}'] \notin \mathrm{E}(\Gamma)$. Hence, every clique containing a type 1 vertex has exactly one type 1 vertex. $\square$

5.16 Lemma *Let* $(V, \mathcal{B})$ *be a Bose Steiner triple system of order* $v > 9$ *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Let* $\mathcal{B}' \subseteq \mathcal{B}$, *and* $\Gamma' = (\mathcal{B}', \mathrm{E}')$ *be a maximum clique of* Γ *such that* $\mathrm{E}'(\Gamma') \subseteq \mathrm{E}(\Gamma)$. *Then* Γ' *contains type* 1 *and type* 2 *vertices.*

Proof. We prove this by showing that Γ' contains a type 1 vertex. We consider this in three cases.

Case 1: (Γ' is of all type 1 vertices) This clearly contradicts Lemma 5.15, since type 1 vertices do not form edges.

Case 2: (Γ' is of all type 2 vertices) By Lemma 5.12, $|\Gamma'| = \dfrac{(v-1)}{2}$. This order is determined by the type I adjacency. By Lemma 5.8, any type 2 vertex has exactly 3 type 1 neighbours containing each of the points of the type 2 vertex. Hence, Γ' can be extended by a common edge, thereby contradicting the hypothesis that Γ' is a maximum clique.

Case 3: (Γ' is of both types of vertices) By Lemma 5.15, there is exactly one type 1 vertex in a clique containing it.

$\square$

5.17 Corollary *Let* $(V, \mathcal{B})$ *be a Bose Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Let* $\mathcal{B}' \subseteq \mathcal{B}$, *and* $\Gamma' = (\mathcal{B}', \mathrm{E}')$ *be a maximum clique of* Γ *such that* $\mathrm{E}'(\Gamma') \subseteq \mathrm{E}(\Gamma)$. *Then* Γ' *contains at most* 1 *type* 1 *vertex.*

We present few examples of the cliques of Bose Steiner triple systems.

Table 5.1: Cliques of some Bose Steiner triple systems

$V = (\mathrm{Q}_{2n+1} \times \mathbb{Z}_3)$	Clique number	Number of maximum cliques	Size 4 cliques	Size 5 cliques	Total number of cliques
$(\mathrm{Q}_3 \times \mathbb{Z}_3)$	4	81	maximum	-	81
$(\mathrm{Q}_5 \times \mathbb{Z}_3)$	7	15	420	-	435
$(\mathrm{Q}_7 \times \mathbb{Z}_3)$	10	21	756	126	903
$(\mathrm{Q}_9 \times \mathbb{Z}_3)$	13	27	2808	-	2835
$(\mathrm{Q}_{11} \times \mathbb{Z}_3)$	16	33	5280	-	5313
$(\mathrm{Q}_{13} \times \mathbb{Z}_3)$	19	39	8892	-	8931

The case $(\mathrm{Q}_7 \times \mathbb{Z}_3)$ is a special one arising from a type I adjacency due to the symmetry of design.

We now describe the structure of size 4 cliques. This cliques constitute the bulk of the cliques in Bose Steiner triple systems.

5.18 Proposition *Let* Q_{2n+1} *be a Bose quasigroup obtained from an odd order abelian group* G. *Let* $(\mathrm{Q}_{2n+1} \times \mathbb{Z}_3, \mathcal{B})$ *be a Bose Steiner triple system of order* $v > 9$, *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Let* $\mathcal{B}' \subseteq \mathcal{B}$, *and* $\Gamma' = (\mathcal{B}', \mathrm{E}')$ *be a maximal clique of order* 4 *such that* $\mathrm{E}'(\Gamma') \subseteq \mathrm{E}(\Gamma)$. *Then*

(i) Γ' *contains* 1 *type* 1 *and* 3 *type* 2 *vertices or*

(ii) Γ' *contains type* 2 *vertices only.*

Proof. Let $\mathrm{B}, \mathrm{B}', \mathrm{B}'' \in \mathcal{B}'(\Gamma') \subseteq \mathrm{V}(\Gamma)$ be type 1 vertices, and let $\mathrm{B}_1, \mathrm{B}_2, \dots, \mathrm{B}_\mathrm{n} \in \mathcal{B}'(\Gamma') \subseteq \mathrm{V}(\Gamma)$ be type 2 vertices Γ. By Lemma 5.15, $\mathrm{B} \cap \mathrm{B}' = \mathrm{B} \cap \mathrm{B}'' = \mathrm{B}' \cap \mathrm{B}'' = \varnothing$. Hence, Γ' does not contain 2 type 1 and 2 type 2 vertices.

Now, the first task is to show that there exists a size 4 clique containing exactly one type 1 vertex.

Case 1: (Γ' contains 1 type 1 and 3 type 2 vertices.) Let $x_1 = 0, x_2 = 1, \cdots, x_n =$

$n-1, x_{n+1} = n, \ldots, x_{2n+1} = 2n \in \mathrm{G}$ and consider:

$$\begin{aligned}
\mathrm{B} &= \{(x_1, 0), (x_1, 1), (x_1, 2)\};\\
\mathrm{B}_1 &= \{(x_1, 1), (x_3, 1), (x_1 * x_3, 2)\};\\
\mathrm{B}_2 &= \{(x_1, 2), (x_1 * x_3, 2), (x_1 * (x_1 * x_3), 0)\};\\
\mathrm{B}_3 &= \{((x_1 * (x_1 * x_3), 0), (x_{n+1}, 0), (x_1, 1)\}.
\end{aligned}$$

Clearly, for all $x_1, x_2, x_3, x_{n+1}, x_{n+2} \in \mathrm{G}$,

$$\begin{aligned}
x_1 * x_3 &= x_1 \pmod{(2n+1)};\\
x_1 * x_2 &= x_{n+2} \pmod{(2n+1)};\\
x_{n+2} * x_{n+1} &= x_1 \pmod{(2n+1)}.
\end{aligned}$$

Hence $[\mathrm{B}, \mathrm{B}_1], [\mathrm{B}, \mathrm{B}_2], [\mathrm{B}, \mathrm{B}_3], [\mathrm{B}_1, \mathrm{B}_2], [\mathrm{B}_1, \mathrm{B}_3], [\mathrm{B}_2, \mathrm{B}_3] \in \mathrm{E}'(\Gamma')$ and $\mathrm{B}, \mathrm{B}_1, \mathrm{B}_2$ and B_3 form a maximal clique, since there exists no common point in $\mathrm{B}, \mathrm{B}_1, \mathrm{B}_2$ and B_3 to form a type I adjacency.

Therefore, it is enough to show that there exists a clique of size 4 consisting of type 2 vertices only.

Case 2: (Γ' contains type 2 vertices only.) Let $x, y, z \in \mathrm{G} : x \neq y \neq z$. Then consider the vertices

$$\begin{aligned}
\mathrm{B}_1 &= \{(x, 0), (y, 0), (x * y, 1)\};\\
\mathrm{B}_2 &= \{(y, 0), (z, 0), (x, 1)\};\\
\mathrm{B}_3 &= \{(x * y, 2), (z, 2), (y, 0)\};\\
\mathrm{B}_4 &= \{(y * z, 1), (x * y, 1), (z, 2)\}.
\end{aligned}$$

It is clear that there exists no point common to the four vertices $\mathrm{B}_1, \mathrm{B}_2, \mathrm{B}_3$ and B_4 to form a type I adjacency. Hence, they form a maximal clique.

□

Remark Let $(V, \mathcal{B})$ be a Bose Steiner triple system of order v and $\Gamma = (\mathcal{B}, \mathrm{E})$ a block intersection graph. Then, there exist no independent set of size 4 containing type 2 vertices only.

We now present examples of size 4 cliques of the graphs of $(\mathrm{Q}_3 \times \mathbb{Z}_3)$ and $(\mathrm{Q}_5 \times \mathbb{Z}_3)$ Bose Steiner triple systems.

Table 5.2: Bose cliques of size 4

Design	Type 1 vertex	Type 2 vertex	Total number cliques
$(\mathrm{Q}_3 \times \mathbb{Z}_3)$	1	3	81
$(\mathrm{Q}_5 \times \mathbb{Z}_3)$	1	3	236
$(\mathrm{Q}_5 \times \mathbb{Z}_3)$	0	4	184

In the special case of the graph of the $(\mathrm{Q}_3 \times \mathbb{Z}_3)$ design, there are no cliques of size 4 containing type 2 vertices only. The maximum clique size is 4. We present 3 special maximum cliques of size 4 from the graphs of Bose Steiner triple system $(\mathrm{Q}_3 \times \mathbb{Z}_3)$. These cliques are special because they appear in all size 4 cliques of the graphs of any Bose Steiner triple system $(\mathrm{Q}_{2n+1} \times \mathbb{Z}_3)$. They are shown below:

$$\left\{\begin{array}{c} \{(0,0),(1,0),(2,1)\} \\ \{(0,0),(2,0),(1,1)\} \\ \{(1,0),(2,1),(0,1)\} \\ \{(0,0),(0,1),(0,2)\} \end{array}\right\} \left\{\begin{array}{c} \{(0,1),(1,1),(2,2)\} \\ \{(0,1),(2,1),(1,2)\} \\ \{(1,1),(2,1),(0,2)\} \\ \{(1,0),(1,1),(1,2)\} \end{array}\right\} \left\{\begin{array}{c} \{(0,2),(1,2),(2,0)\} \\ \{(0,2),(2,2),(1,0)\} \\ \{(1,2),(2,2),(0,0)\} \\ \{(2,0),(2,1),(2,2)\} \end{array}\right\}$$

In order to fully discuss the automorphism groups of the block intersection graphs of Bose Steiner triple systems in the next chapter, we further observe the structures of the maximum cliques of the block intersection graphs of Bose Steiner triple systems.

We denote by C_x cliques of the block intersection graph defined by the type I adjacency. That is, C_x is such that a point $x \in V$ is common to all vertices $B \in C_x$.

5.19 Lemma *Let $(V, \mathcal{B})$ be a Bose Steiner triple system of order $v > 9$, $\Gamma = (\mathcal{B}, \mathrm{E})$ be a block intersection graph and Γ' be a maximum clique of Γ. Let C_x such that $x \in V$ be a clique of Γ. Then $C_x = \Gamma'$.*

Proof. By Corollary 3.2, the point $x \in V$ is in exactly $\dfrac{(v-1)}{2}$ vertices of Γ.

By the type I adjacency, $|C_x| = \dfrac{(v-1)}{2}$. Hence, by the proof of Lemma 5.12, C_x is a maximum clique. $\square$

5.20 Lemma *Let $(V, \mathcal{B})$ be a Bose Steiner triple system of order $v > 9$, $\Gamma = (\mathcal{B}, \mathrm{E})$ be a block intersection graph and Γ' be a maximum clique of Γ. Let C_x such that $x \in V$ be a clique of Γ. Then $\Gamma' = C_x$.*

Proof. By Lemma 5.12, $|\Gamma'| = \dfrac{(v-1)}{2}$. Hence, if $v > 9$, then $|\Gamma'| > 4$. Clearly, since each vertex $\mathrm{B} \in \mathcal{B}$ is made up of 3 points of the points set V, it follows that Γ' is of the type I adjacency. $\square$

In view of Lemmas 5.19 and 5.20, we have:

5.21 Theorem *Let $(V, \mathcal{B})$ be a Bose Steiner triple system of order $v > 9$, $\Gamma = (\mathcal{B}, \mathrm{E})$ be a block intersection graph and Γ' be a maximum clique of Γ. Let C_x such that $x \in V$ be a clique of Γ. Then Γ' is a maximum clique of Γ if and only if $\Gamma' = C_x$.*

Now, we turn our attention to independent sets and an independent numbers of the block intersection graphs of Bose Steiner triple systems.

First, we consider a general case of all maximum independent sets of any block intersection graph of a Steiner triple system.

5.22 Proposition *Let $(V, \mathcal{B})$ be a Steiner triple system of order v and $\Gamma = (\mathcal{B}, \mathrm{E})$ be a block intersection graph. Then the order of the maximum independent sets of Γ is atmost $\dfrac{v}{3}$.*

Proof. Let I be an independent set. For any $B, B' \in I$, $B \cap B' = \varnothing$. So vertices contained in I partition the set $X = \bigcup_{B \in I} B$. Now, $|X| \leq V$. Therefore $I \leq \dfrac{v}{3}$. $\square$

5.23 Corollary *Let $(V, \mathcal{B})$ be a Bose Steiner triple system of order v and $\Gamma = (\mathcal{B}, \mathrm{E})$ be a block intersection graph. Then the set of all type 1 vertices form a maximum independent set.*

Proof. Clearly, the set of all type 1 vertices are not connected. They also contain all the points of V since there are $\dfrac{v}{3}$ vertices. $\square$

Next, we discuss maximum independent sets on type 2 vertices.

5.24 Lemma *Let* Q_{2n+1} *be a Bose quasigroup obtained from an odd order abelian group* G*. Let* $(\mathrm{Q}_{2n+1} \times \mathbb{Z}_3, \mathcal{B})$ *be a Bose Steiner triple system of order* $v = 9, 27$ *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Then there exist maximum independent sets containing type 2 vertices only.*

Proof. First, we consider the case $v = 9$.

(a) Clearly, $v = 9$ implies $\mathrm{G} \cong \mathbb{Z}_3$. There are 9 type 2 vertices and 3 type 1 vertices. We list all the independent sets of the $(\mathrm{Q}_3 \times \mathbb{Z}_3)$ design containing type 2 vertices only.

$$\left\{ \begin{array}{c} \{(0,0),(2,0),(1,1)\} \\ \{(0,1),(2,1),(1,2)\} \\ \{(0,2),(2,2),(1,0)\} \end{array} \right\} \quad \left\{ \begin{array}{c} \{(0,0),(1,0),(2,1)\} \\ \{(0,1),(1,1),(2,2)\} \\ \{(0,2),(1,2),(2,0)\} \end{array} \right\}$$

$$\left\{ \begin{array}{c} \{(1,0),(2,0),(0,1)\} \\ \{(1,1),(2,1),(0,2)\} \\ \{(1,2),(2,2),(0,0)\} \end{array} \right\}$$

(b) $v = 27$ implies $\mathrm{G} \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ or $\mathrm{G} \cong \mathbb{Z}_9$. There are 108 type 2 vertices and 9 type 1 vertices. The diagonal subgroup of $\mathbb{Z}_3 \times \mathbb{Z}_3 \cong \mathbb{Z}_3$. Hence, the argument above clearly completes the case $\mathrm{G} \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. Therefore, it is enough to show that there exist maximum independent set of all type 2 vertices if $\mathrm{G} \cong \mathbb{Z}_9$.

Consider a maximum independent set of 9 type 1 vertices. Now, consider a partition of these 9 vertices into a subset of 3 type 1 vertices each such that for each $x, y, z \in \mathrm{G}$, $x \neq y \neq z$ and $x * y = z$. Hence, the 9 type 1 vertices can be resolved into 3 unique subsets containing 3 type 1 vertices each.

Now, consider the transpose of each of the 3 subsets of 3 type 1 vertices as shown below:

$$\left\{\begin{array}{c}\{(x,0),(x,1),(x,2)\}\\ \{(y,0),(y,1),(y,2)\}\\ \{(z,0),(z,1),(z,2)\}\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\{(x,0),(y,0),(z,1)\}\\ \{(x,1),(y,1),(z,2)\}\\ \{(x,2),(y,2),(z,0)\}\end{array}\right\}$$

Clearly, each transpose of the 3 subsets of 3 type 1 vertices gives a maximum independent set of type 2 vertices.

□

We present a maximum independent set of containing type 2 vertices only from the Bose Steiner triple system of order $v = 27$, $\mathrm{G} \cong \mathbb{Z}_9$.

$$\left\{\begin{array}{c}\{(0,0),(5,0),(7,1)\}\\ \{(0,1),(5,1),(7,2)\}\\ \{(0,2),(5,2),(7,0)\}\\ \{(1,0),(2,0),(6,1)\}\\ \{(1,1),(2,1),(6,2)\}\\ \{(1,2),(2,2),(6,0)\}\\ \{(3,0),(4,0),(8,1)\}\\ \{(3,1),(4,1),(8,2)\}\\ \{(3,2),(4,2),(8,0)\}\end{array}\right\}$$

There are several of such maximum independent sets discussed above. Table 5.3 provides the orders of the maximum independent sets for some Bose Steiner triple systems.

In the next 2 lemmas, we discuss the possibilities of maximum independent sets containing type 2 vertices only in Bose Steiner triple systems.

5.25 Lemma *Let* Q_{2n+1} *be a Bose quasigroup obtained from an odd order abelian group* G. *Let* $(\mathrm{Q}_{2n+1} \times \mathbb{Z}_3, \mathcal{B})$ *be a Bose Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Then there exists a maximum independent set containing type* 2 *vertices only if* $G \cong (\mathbb{Z}_3)^n \times (\mathbb{Z}_9)^m$, *where* $n + m \neq 0$.

Proof. $G \cong (\mathbb{Z}_3)^n \times (\mathbb{Z}_9)^m$, where $n + m \neq 0$ implies:

(i) G is isomorphic to $\mathbb{Z}_3$ or multiples of $\mathbb{Z}_3$

(ii) G is isomorphic to $\mathbb{Z}_9$ or multiples of $\mathbb{Z}_9$

(iii) G is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_9$ or multiples of $\mathbb{Z}_3 \times \mathbb{Z}_9$.

Cases (i) and (ii) above are similar. Hence the proof to the two cases readily follow from Lemma 5.24, since $(\mathbb{Z}_3)^n$ contains $\mathbb{Z}_3$ and $(\mathbb{Z}_9)^m$ contains $\mathbb{Z}_9$. Therefore, it is enough to show that there exist independent sets containing type 2 vertices only if G is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_9$ since $\mathbb{Z}_3 \times \mathbb{Z}_9$ is also contained in multiples of $\mathbb{Z}_3 \times \mathbb{Z}_9$. By similar argument of the Case (b) of Lemma 5.24, $\mathbb{Z}_3 \times \mathbb{Z}_9$ can be resolved into 9 unique sets containing 3 type 1 vertices such that $x \neq y \neq z$ is contained in any 3 type 1 vertices where $x * y = z$, for $x, y, z \in (\mathbb{Z}_3 \times \mathbb{Z}_9)$. The total number of type 1 vertices is a multiple of 3. Hence, the transpose of the sets of 3 type 1 vertices each to the type 2 vertices gives a maximum independent set of the order of G. $\square$

5.26 Lemma *Let* Q_{2n+1} *be a Bose quasigroup obtained from an odd order abelian group* G*. Let* $(\mathrm{Q}_{2n+1} \times \mathbb{Z}_3, \mathcal{B})$ *be a Bose Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Then there exists no maximum independent set of all type* 2 *vertices if* $G \ncong (\mathbb{Z}_3)^n \times (\mathbb{Z}_9)^m$*, where* $n + m \neq 0$.

Proof. Clearly, if $G \ncong (\mathbb{Z}_3)^n \times (\mathbb{Z}_9)^m$, where $n + m \neq 0$. Then considering the arguments of case (b) in Lemma 5.24, $|G|$ is not resolvable into multiples of 3. Hence we do not have a partition of the type 1 vertices into subsets of 3 type 1 vertices such that for each $x, y, z \in G$, $x \neq y \neq z$ and $x * y = z$. $\square$

5.27 Theorem *Let* Q_{2n+1} *be a Bose quasigroup obtained from an odd order abelian group* G*. Let* $(\mathrm{Q}_{2n+1} \times \mathbb{Z}_3, \mathcal{B})$ *be a Bose Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Then there exists a maximum independent set containing type* 2 *vertices only if and only if* $G \cong (\mathbb{Z}_3)^n \times (\mathbb{Z}_9)^m$*, where* $n + m \neq 0$.

Proof. The proof follows from Lemmas 5.25 and 5.26. $\square$

We present few examples of the independent sets of Bose Steiner triple systems.

Table 5.3: Some independent sets in Bose Steiner triple system

$Q_{2n+1} \times \mathbb{Z}_3$	Maximum independent sets	Independent sets of size 3	Independent sets of size 4	Independent sets of size 5	Total
$Q_3 \times \mathbb{Z}_3$	4	4	-	-	4
$Q_5 \times \mathbb{Z}_3$	11	120	120	-	251
		Independent sets of size 4	Independent sets of size 5	Independent sets of size 6	
$Q_7 \times \mathbb{Z}_3$	64	42	5859	3948	9913
		Independent sets of size 6	Independent sets of size 7	Independent sets of size 8	
$Q_9 \times \mathbb{Z}_3$	8191	10368	744066	57186	819811
$(Q_3 \times Q_3) \times \mathbb{Z}_3$	7921	40824	678456	71928	799129

We now discuss the structures of the cliques and the independent sets of the Skolem Steiner triple systems.

The cliques in the block intersection graphs of the Skolem Steiner triple systems differ from that of the Bose Steiner triple systems especially in terms of clique number and maximal cliques. This is due to the additional vertex type in the design.

In addition to Lemmas 5.12 and 5.14, the following also hold for the block intersection graphs of the Skolem Steiner triple systems.

5.28 Lemma *Let* $(V, \mathcal{B})$ *be a Skolem Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Let* $\mathcal{B}' \subseteq \mathcal{B}$, *and* $\Gamma' = (\mathcal{B}', \mathrm{E}')$ *be a maximum clique of* Γ *such that* $\mathrm{E}'(\Gamma') \subseteq \mathrm{E}(\Gamma)$. *Then the total number of* Γ' *is* $|V|$.

Proof. This is similar to Corollary 5.13 □

5.29 Lemma *Let* $(V, \mathcal{B})$ *be a Skolem Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Then any clique of* Γ *containing a type* 1 *vertex has at most that vertex.*

Proof. This is similar to the proof of Lemma 5.15. □

5.30 Lemma *Let* $(V, \mathcal{B})$ *be a Skolem Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Then there exists a maximum clique of the total type* 2 *vertices.*

Proof. Every type 2 vertex has the unique point (p, q). Hence, the set of type 2 vertices form a clique. By Corollary 3.2, (p, q) is in exactly $\dfrac{v-1}{2}$ vertices, which by Lemma 5.12 equals the clique number. $\square$

5.31 Corollary *Let* $(V, \mathcal{B})$ *be a Skolem Steiner triple system of order* v*,* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Let* $\mathcal{B}' \subseteq \mathcal{B}$*, and* $\Gamma' = (\mathcal{B}', \mathrm{E}')$ *be a maximum clique of* Γ *such that* $\mathrm{E}'(\Gamma') \subseteq \mathrm{E}(\Gamma)$*. Then there exists no* Γ' *containing* 2 *or more but less than* $|\Gamma'|$ *type* 2 *vertices.*

Proof. This is as a result of the type I adjacency. $\square$

The next proposition gives the general structure of maximum cliques in Skolem Steiner triple systems.

5.32 Proposition *Let* $(V, \mathcal{B})$ *be a Skolem Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Let* $\mathcal{B}' \subseteq \mathcal{B}$*, and* $\Gamma' = (\mathcal{B}', \mathrm{E}')$ *be a maximum clique of* Γ *such that* $\mathrm{E}'(\Gamma') \subseteq \mathrm{E}(\Gamma)$*. Then* Γ' *is of the* 3 *types below:*

(i) Γ' *has exactly* 1 *of* $(\dfrac{v-1}{2})$ *type* 2 *and no other vertex type.*

(ii) Γ' *has exactly* $(\dfrac{v-1}{2})$ *of* 1 *type* 1*,* 1 *type* 2 *and* $(\dfrac{v-5}{2})$ *type* 3 *vertices.*

(iii) Γ' *has exactly* $(\dfrac{v-1}{2})$ *of no type* 1*,* 1 *type* 2 *and* $(\dfrac{v-3}{2})$ *type* 3 *vertices.*

Proof. Case (i) above readily comes from Lemma 5.30. By Lemma 5.29, it is clear that Γ' contains at most 1 type 1 vertex. Similarly by Corollary 5.31, it is also easy to see that such Γ' contains at most one type 2 vertex. Hence by the type I adjacency, type 3 vertices make up the rest of the clique in case (ii).

The result in Case (iii) above also comes from Lemma 5.29 and Corollary 5.31. Hence, if Γ' does not contain a type 1 vertex, then it can only contain at most since it also contain type 3 vertices.

By Lemma 5.9, every type 1 vertex is a neighbour of 3 type 2 vertices. Hence, the case where Γ' contains 1 type 1 vertex and 0 type 2 vertex is impossible. $\square$

The table below is an example of the maximum cliques of the block intersection graph of Skolem Steiner triple system $(\mathrm{Q}_6 \times \mathbb{Z}_3 \cup (p, q))$.

Table 5.4: Three types of maximum cliques on Skolem Steiner triple systems

Design	No. of type 1 vertices	No. of type 2 vertices	No. of type 3 vertices	Total
$(\mathrm{Q}_6 \times \mathbb{Z}_3 \cup (p, q))$	0	9	0	1
$(\mathrm{Q}_6 \times \mathbb{Z}_3 \cup (p, q))$	1	1	7	9
$(\mathrm{Q}_6 \times \mathbb{Z}_3 \cup (p, q))$	0	1	8	9

In order to discuss the full automorphism groups of the block intersection graphs of Skolem Steiner triple systems in the next chapter, we further observe the structures of the maximum cliques of the block intersection graphs of the Skolem Steiner triple systems.

We denote by C_x, cliques of the block intersection graph defined by the type I adjacency. That is, C_x is such that a point $x \in V$ is common to all vertices $\mathrm{B} \in C_x$.

5.33 Lemma *Let $(V, \mathcal{B})$ be a Skolem Steiner triple system of order $v > 13$, $\Gamma = (\mathcal{B}, \mathrm{E})$ be a block intersection graph and Γ' be a maximum clique of Γ. Let C_x such that $x \in V$ be a clique of Γ. Then $C_x = \Gamma'$.*

Proof. This is similar to the proof of Lemma 5.19 $\square$

5.34 Lemma *Let $(V, \mathcal{B})$ be a Skolem Steiner triple system of order $v > 9$, $\Gamma = (\mathcal{B}, \mathrm{E})$ be a block intersection graph and Γ' be a maximum clique of Γ. Let C_x such that $x \in V$ be a clique of Γ. Then $\Gamma' = C_x$.*

Proof. This is similar to the proof of Lemma 5.20 □

In view of Lemmas 5.33 and 5.34, we have:

5.35 Theorem *Let $(V, \mathcal{B})$ be a Skolem Steiner triple system of order $v > 13$, $\Gamma = (\mathcal{B}, \mathrm{E})$ be a block intersection graph and Γ' be a maximum clique of Γ. Let C_x such that $x \in V$ be a clique of Γ. Then Γ' is a maximum clique of Γ if and only if $\Gamma' = C_x$.*

We present a few examples of the general cliques of some Skolem Steiner triple systems.

Table 5.5: Cliques in Skolem Steiner triple system

$(\mathrm{Q}_{2n} \times \mathbb{Z}_3 \cup (p, q))$	No. of maximum clique	Size 4 cliques	Size 5 cliques	Size 6 cliques	Total cliques
$(\mathrm{Q}_4 \times \mathrm{Q}_3 \cup (p, q))$	13	104	39	13	156
$(\mathrm{Q}_6 \times \mathrm{Q}_3 \cup (p, q))$	19	648	57	3	727
$(\mathrm{Q}_8 \times \mathrm{Q}_3 \cup (p, q))$	25	1792	102	-	1919
$(\mathrm{Q}_{10} \times \mathrm{Q}_3 \cup (p, q))$	31	3824	129	-	3984
$(\mathrm{Q}_{12} \times \mathrm{Q}_3 \cup (p, q))$	37	6744	201	-	6982
$(\mathrm{Q}_{14} \times \mathrm{Q}_3 \cup (p, q))$	43	11092	237	-	11372
$(\mathrm{Q}_{16} \times \mathrm{Q}_3 \cup (p, q))$	49	16868	291	-	17208

We now describe the independence number and the independent sets of Skolem Steiner triple systems.

5.36 Corollary *Let Q_{2n} be a Skolem quasigroup, $(V, \mathcal{B})$ be a Skolem Steiner triple system of order v and $\Gamma = (\mathcal{B}, \mathrm{E})$ be a block intersection graph. Then the independence number of Γ is $2n$.* $\mathrm{Q}_{2n} \times \mathbb{Z}_3 \cup \{(p, q)\}$

Proof. Let I be an independent set. By Proposition 5.22, $I \leq \dfrac{v}{3}$. By Lemma 5.30 every block containing the point (p, q) forms a clique. Hence we have $I = \dfrac{v-1}{3} = 2n$. □

5.37 Lemma *Let $(V, \mathcal{B})$ be a Skolem Steiner triple system of order v and $\Gamma = (\mathcal{B}, \mathrm{E})$ be a block intersection graph. Then there exists no maximum independent set of all type 1 or all type 2 vertices.*

Proof. Clearly, the set of all type 1 vertices are not connected but they do not contain all points in V. Hence they do not form maximum independent sets.

By Lemma 5.30, there exists a maximum clique of total type 2 vertices. Hence, any independent set containing a type 2 vertex has at most the type 2 vertex.

Now, consider the sets $\{(x, i), (y, i), (x * y, i + 1)\}$ and $\{(x + 1, i + 1), (y + 1, i + 1), ((x + 1) * (y + 1), i + 2)\}$ for distinct $x, y \in \mathrm{Q}$. These sets clearly form independent sets of the order of Q.

Suppose to the contrary that the sets can be extended by any other vertex of Γ. Without loss of generality, consider the 3 types of vertices $\{(x, 0), (x, 1), (x, 2)\}$, $\{(p, q), (x + n, i), (x, i + 1)\}$ and $\{(x, i), (y, i), (x * y, i + 1)\}$. Clearly each of these 3 sets of vertices intersects $\{(x, i), (y, i), (x * y, i + 1)\}$ and $\{(x + 1, i + 1), (y + 1, i + 1), ((x + 1) * (y + 1), i + 2)\}$.

$\square$

We present some independent sets of Skolem Steiner triple systems.

Table 5.6: Independent sets from Skolem Steiner triple system

$(\mathrm{Q}_{2n} \times \mathbb{Z}_3 \cup (p, q))$	No. of maximum independent sets	Independent sets of size 3	-	-	Total
$(\mathrm{Q}_4 \times \mathbb{Z}_3) \cup (p, q)$	13	78	-	-	91
		Independent sets of size 4	Independent sets of size 5	-	
$(\mathrm{Q}_6 \times \mathbb{Z}_3 \cup (p, q))$	68	339	2585	-	2992
		Independent sets of size 5	Independent sets of size 6	Independent sets of size 7	
$(\mathrm{Q}_8 \times \mathbb{Z}_3 \cup (p, q))$	1991	48	70277	87280	159596

We hope to examine cliques and independent sets of Steiner triple systems, especially the projective and affine designs in further studies.

Having described the structures of the cliques and independent sets of the designs of our consideration in this study, we now discuss the automorphism groups of the graphs.

Chapter 6

Automorphism groups of the block intersection graphs of Steiner triple systems

The essence of this chapter is to investigate the automorphism groups of the block intersection graphs of the constructions of Steiner triple systems in Chapter 4. We study the automorphism of the graphs of the designs of our consideration in order to study their symmetry and compare their automorphism groups to that of their designs.

First, we discuss the automorphism groups of the block intersection graphs of Bose Steiner triple systems.

6.1 Automorphism groups of the block intersection graphs obtained from Bose Steiner triple systems

In this section, we are interested in studying the full automorphism groups of the graphs of Bose Steiner triple systems. Cliques and independent sets will play important roles in describing the actions of the full automorphism groups on the block intersection graphs of the Bose Steiner triple systems.

We begin by describing the actions of automorphism on the vertices of the block intersection graphs $\Gamma = (\mathcal{B}, \mathrm{E})$ of the Bose Steiner triple system constructed from odd order Abelian groups.

Our aim is to discuss how automorphisms permute the vertices of the graph. We recall that the vertices of the Bose Steiner triple systems are of two types. Therefore we intend to see the action of automorphisms on the vertex set of Γ from this point of view.

Let $V = \mathrm{Q}_{2n+1} \times \mathbb{Z}_3$ and $\mathbb{B} = (V, \mathcal{B})$ be a Bose Steiner triple system of order v. Let $p \in V$ be a point of the set V, and $\beta \in \mathrm{Aut\ G}$ be an automorphism of G. Let $x, y, z, a \in \mathrm{G}$, and $i, j, k, b \in \mathbb{Z}_3$ such that $p = (a, b)$, and $\mathrm{B} = \{(x, i), (y, j), (z, k)\} \in \mathcal{B}$. Define a map $\beta : V \to V$ by

$$\beta(\mathrm{B}) = \{(\beta(x), i), (\beta(y), j), (\beta(z), k)\} \tag{6.1}$$

and the map $\alpha : V \to V$ by

$$\alpha(\mathrm{B}) = \{p + (x, i), p + (y, j), p + (z, k)\} \tag{6.2}$$

for any $p \in V$.

By Theorem 4.12, we have that the pair of maps (α, β) defined by

$$(\alpha, \beta)(\mathrm{B}) = \{(p + ((\beta(x), i)), (p + ((\beta(y), j)), (p + ((\beta(z), k))\} \tag{6.3}$$

is clearly an automorphism of $\mathbb{B}$.

We now show that the automorphisms described above induce automorphisms of the graph Γ.

6.1 Lemma *Let* Q_{2n+1} *be a Bose quasigroup obtained from an odd order abelian group G. Let* $V = \mathrm{Q}_{2n+1} \times \mathbb{Z}_3$ *and* $\mathbb{B} = (V, \mathcal{B})$ *be a Bose Steiner triple system of order* v*, and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Let* $x, y, z, a \in \mathrm{G}$*, and* $i, j, k, b \in \mathbb{Z}_3$ *such that* $p = (a, b) \in V$*, and* $\mathrm{B} = \{(x, i), (y, j), (z, k)\} \in \mathcal{B}$*. Let* $\beta \in \mathrm{Aut\ G}$ *and* α *be the map defined in* (6.2) *above.*

We define a pair of maps

$$(\bar{\alpha}, \bar{\beta}) : \mathrm{V}(\Gamma) \to \mathrm{V}(\Gamma) \text{ by}$$

$$(\bar{\alpha}, \bar{\beta})(\mathrm{B}) = \{(p + ((\beta(x), i)), (p + ((\beta(y), j)), (p + ((\beta(z), k))\}$$

where

$$\begin{aligned}\bar{\alpha}(\mathrm{B}) &= \{p+(x,i), p+(y,j), p+(z,k)\}\\ \bar{\beta}(\mathrm{B}) &= \{(\beta(x),i), (\beta(y),j), (\beta(z),k)\}.\end{aligned}$$

Then the pair of maps $(\bar{\alpha},\bar{\beta})$ *defined above is an automorphism of* Γ.

Proof. Let $\mathrm{B} = \{(x,i),(x,i+1),(x,i+2)\} \in \mathrm{V}(\Gamma)$ be a type 1 vertex, and $\mathrm{B}' = \{(x,i),(y,i),(\frac{(x+y)}{2}, i{+}1)\}, \mathrm{B}'' = \{(x,i),(z,i),(\frac{(x+y)}{2}, i{+}1)\, i{+}1)\} \in \mathrm{V}(\Gamma)$ be type 2 vertices of Γ.

$$\begin{aligned}(\bar{\alpha},\bar{\beta})(\mathrm{B}) &= \{(a+\beta(x), b+i), (a+\beta(x), b+i+1), (a+\beta(x), b+i+2)\},\\ (\bar{\alpha},\bar{\beta})(\mathrm{B}') &= \{(a+\beta(x), b+i), (a+\beta(y), b+i)\\ &\quad \left(\frac{(2a+\beta(x)+\beta(y))}{2}, b+i+1\right)\},\\ (\bar{\alpha},\bar{\beta})(\mathrm{B}'') &= \{(a+\beta(x), b+i), (a+\beta(z), b+i),\\ &\quad \left(\frac{(2a+\beta(x)+\beta(z))}{2}, b+i+1\right)\}.\end{aligned}$$

Clearly, $(\bar{\alpha},\bar{\beta})(\mathrm{B}), (\bar{\alpha},\bar{\beta})(\mathrm{B}'), (\bar{\alpha},\bar{\beta})(\mathrm{B}'') \in \mathrm{V}(\Gamma)$ for any $p \in V$. $(\bar{\alpha},\bar{\beta})$ takes a vertex type to the same vertex type. Hence, it is enough to show that $(\bar{\alpha},\bar{\beta})$ preserves the edges of Γ. By Lemma 5.7, type 1 vertices do not form edges in Γ. Clearly, $[\mathrm{B},\mathrm{B}'], [\mathrm{B}',\mathrm{B}''] \in \mathrm{E}(\Gamma)$ and similarly,

$$[(\bar{\alpha},\bar{\beta})(\mathrm{B}), (\bar{\alpha},\bar{\beta})(\mathrm{B}')], [(\bar{\alpha},\bar{\beta})(\mathrm{B}'), (\bar{\alpha},\bar{\beta})(\mathrm{B}'')] \in \mathrm{E}(\Gamma).$$

□

By Theorem 4.12, the pair of maps (α,β) in (6.3) describes the standard automorphisms of the Bose Steiner triple systems.

In view of the Theorem 4.12 and the Lemma 6.1 above, we have:

6.2 Theorem *Let* $\mathbb{B} = (V,\mathcal{B})$ *be a Bose Steiner triple system of order* v *and* $\Gamma = (\mathcal{B},\mathrm{E})$ *be a block intersection graph. Then automorphisms of* $\mathbb{B}$ *induce automorphisms of* Γ.

In view of Theorem 6.2, we have:

6.3 Proposition *Let* $\mathbb{B} = (V, \mathcal{B})$ *be a Bose Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Then* Aut $\mathbb{B} \leq$ Aut Γ.

Now, we consider the action of automorphisms on the cliques of the block intersection graphs of Bose Steiner triple systems.

In view of Theorem 5.21, we denote $V_C := \{C_x : x \in V\}$, the set of cliques of the form C_x. Clearly, V_C is a collection of all maximum cliques of the block intersection graph of Bose Steiner triple systems. By Lemma 5.12 and Corollary 5.13, except the trivial case $\mathrm{G} = \mathbb{Z}_3$, every Bose Steiner triple system $(V, \mathcal{B})$ of order v has v maximum cliques of order $\left(\dfrac{v-1}{2}\right)$. Hence, there exists a 1–1 correspondence between the sets V and V_C.

In the case $v = 9$, there exist maximum cliques of the type II adjacency. Hence, there exists no 1–1 correspondence between the points set V and the collection of all maximum cliques of the block intersection graph Γ.

We now describe the full automorphism group of the block intersection graphs of Bose Steiner triple systems.

For an automorphism $\bar{\sigma} \in$ Aut Γ, we define $\bar{\sigma} : V_C \to V_C$ by

$$\bar{\sigma}(C_x) = \sigma(\mathrm{C}_x). \tag{6.4}$$

$\bar{\sigma}$ is an induced map on V, since there exists a $1-1$ correspondence between V and the set V_C. Hence, we need to show that $\bar{\sigma}$ preserves the blocks of $(V, \mathcal{B})$.

6.4 Lemma *Let* $(V, \mathcal{B})$ *be a Bose Steiner triple system of order* $v > 9$, $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph and* $V_C := \{C_x : x \in V\}$, *the set of cliques of the form* C_x. *Let* $\bar{\sigma}$ *be as described* (6.4) *above. Then* $\bar{\sigma}$ *preserves the blocks of* $(V, \mathcal{B})$.

Proof. Let $x_0, x_1, x_2, \cdots, x_n \in V$. With $\sigma \in$ Aut Γ as in Theorem 6.2, consider $\sigma(\mathrm{C}_{x_i}), i = 0, 1, 2, \ldots, n$. Clearly, $\bar{\sigma}(\mathrm{C}_x) \in \mathcal{B}$ and $\bar{\sigma}$ preserves the blocks of Γ. $\square$

In view of Lemma 6.4, we have:

6.5 Proposition *Let* $\mathbb{B} = (V, \mathcal{B})$ *be a Bose Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Then* Aut $\Gamma \leq$ Aut $\mathbb{B}$.

In view of Propositions 6.3 and 6.5, we have:

6.6 Theorem *Let* $\mathbb{B} = (V, \mathcal{B})$ *be a Bose Steiner triple system of order* $v > 9$ *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Then* $\mathrm{Aut}\ \Gamma \cong \mathrm{Aut}\ \mathbb{B}$.

6.2 Automorphism groups of the block intersection graphs obtained from Skolem designs

In this section we are interested in studying the full automorphism groups of the block intersection graphs of Skolem Steiner triple systems. The approach here is similar to that we employed in discussing the automorphism groups of the block intersection graphs of the Bose Steiner triple systems.

We begin by describing the actions of automorphism on the vertices of the block intersection graphs $\Gamma = (\mathcal{B}, \mathrm{E})$ from the Skolem Steiner triple system.

We recall that the vertices of a Skolem Steiner triple system $\mathcal{D}= (V, \mathcal{B})$ is of three types. Hence we intend to see the action of automorphism on the vertex set of Γ from this point of view.

For any $\mathrm{B} = \{(x, i), (y, j), (z, k)\} \in \mathcal{B}$, and $\sigma \in \mathrm{Aut}\ \mathcal{D}$, we have by Proposition 4.25 that $\Pi_1(\sigma(\mathrm{B}))$ is an identity map. Similarly by Lemma 4.23(v), we have that translations $\sigma_i : \mathcal{D} \longrightarrow \mathcal{D}$ defined by

$$\sigma_i(x, j) = (x, i + j),$$

for $i \in \mathbb{Z}_3$ are clearly automorphisms of the designs.

We now show that the automorphisms describe above induce automorphisms of the block intersection graph Γ.

6.7 Lemma *Let* Q_{2n} *be a Skolem quasigroup,* $V = \mathrm{Q}_{2n} \times \mathbb{Z}_3$, $\mathbb{B} = (V, \mathcal{B})$ *be a Skolem Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Let* $\sigma \in \mathrm{Aut}\ \mathbb{B}$, $\bar{\sigma}$ *be an induced map on* Γ *such that* $\bar{\Pi}_i\sigma, i = 1, 2$ *be the usual natural projections of the map* $(\bar{\Pi}_1\sigma, \bar{\Pi}_2\sigma) : \mathrm{V}(\Gamma) \to \mathrm{V}(\Gamma)$ *defined by*

$$(\bar{\Pi}_1\sigma, \bar{\Pi}_2\sigma)(\mathrm{B}) = \{(\bar{\Pi}_1\sigma(x), \bar{\Pi}_2\sigma(i)), (\bar{\Pi}_1\sigma(y), \bar{\Pi}_2\sigma(j)), (\bar{\Pi}_1\sigma(z), \bar{\Pi}_2\sigma(k))\} \quad (6.5)$$

for any $\mathrm{B} = \{(x,i),(y,j),(z,k)\} \in \mathcal{B}$*. Then the pair of maps* $(\bar{\Pi}_1\sigma, \bar{\Pi}_2\sigma)$ *defined above is an automorphism of* Γ.

Proof. The result follows easily by Proposition 4.25, Lemma 4.23(v) and Corollary 4.22, since $\sigma \in \mathrm{Aut}\ \mathcal{D}$. □

In view of Lemma 4.23(v), and Lemma 6.7 above, we have:

6.8 Lemma *Let* $(V,\mathcal{B})$ *be a Skolem Steiner triple system of order* v *and* $\Gamma = (\mathcal{B},\mathrm{E})$ *be a block intersection graph. Then automorphisms of* $(V,\mathcal{B})$ *induce automorphisms of* Γ.

In view of Lemma 6.8, we have:

6.9 Proposition *Let* $\mathbb{B} = (V,\mathcal{B})$ *be a Skolem Steiner triple system of order* v *and* $\Gamma = (\mathcal{B},\mathrm{E})$ *be a block intersection graph. Then* $\mathrm{Aut}\ \mathbb{B} \leq \mathrm{Aut}\ \Gamma$.

Now, we consider the action of automorphisms on the cliques of the block intersection graphs of Skolem Steiner triple systems.

In view of Theorem 5.35, we denote $V_C := \{C_x : x \in V\}$, the set of cliques of the form C_x. Clearly, V_C is a collection of all maximum cliques of the block intersection graph of a Skolem Steiner triple system. By Lemma 5.12 and Corollary 5.13, except the trivial case $\mathrm{Q} = \mathbb{Z}_3$, every Skolem Steiner triple system $(V,\mathcal{B})$ of order v has v maximum cliques of order $\left(\dfrac{v-1}{2}\right)$. Hence, there exists a 1–1 correspondence between V and V_C.

The case $v = 7$ is an exception. This is the familiar fano plane so we do not consider it in this study.

We now describe the full automorphism group of the block intersection graphs of Skolem Steiner triple systems.

For an automorphism $\bar{\sigma} \in \mathrm{Aut}\ \Gamma$, we define $\bar{\sigma} : V_C \to V_C$ by

$$\bar{\sigma}(C_x) = \sigma(\mathrm{C}_x). \tag{6.6}$$

$\bar{\sigma}$ is an induced map on V, since there exist a 1–1 correspondence between V and the set V_C. Hence, we need to show that $\bar{\sigma}$ preserves the blocks of $(V,\mathcal{B})$.

6.10 Lemma *Let* $(\mathrm{Q} \times \mathbb{Z}_3,\mathcal{B})$ *be a Skolem Steiner triple system of order* $v > 13$, $\Gamma = (\mathcal{B},\mathrm{E})$ *be a block intersection graph and* $V_C := \{C_x : x \in V\}$, *the set of cliques of the form* C_x. *Let* $\bar{\sigma}$ *be as described* (6.6) *above. Then* $\bar{\sigma}$ *preserves the blocks of* $(V, \mathcal{B})$.

Proof. This is similar to the proof of Lemma 6.4 $\square$

In view of Lemma 6.10, we have:

6.11 Proposition *Let* $\mathbb{B} = (V, \mathcal{B})$ *be a Skolem Steiner triple system of order* v *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Then* $\mathrm{Aut}\ \Gamma \leq \mathrm{Aut}\ \mathbb{B}$.

In view of Propositions 6.9 and 6.11, we have:

6.12 Theorem *Let* $\mathbb{B} = (V, \mathcal{B})$ *be a Skolem Steiner triple system of order* $v \geq 13$ *and* $\Gamma = (\mathcal{B}, \mathrm{E})$ *be a block intersection graph. Then* $\mathrm{Aut}\ \Gamma \cong \mathrm{Aut}\ \mathbb{B}$.

Appendix A

Code for Bose Steiner triple systems

$q := \{((2*p)+1) : p \text{ in } [1..n]\};$
for m in q do
$z3 := [i : i \text{ in } \{0..2 \text{ mod } 3\ \}];$
$g := [j : j \text{ in } \{0..(m-1) \text{ mod } 3\ \}];$
$pts := [< j, i >: i \text{ in } z3, j \text{ in } g];$
$po := SetToIndexedSet(\{1..\#pts\});$
$vb1 := func < pts|[a : a \text{ in } [1..\#pts]|pts[a][2]eq0] >;$
$vb2 := func < pts|[b : b \text{ in } [1..\#pts]|pts[b][2]eq1] >;$
$vb3 := func < pts|[c : c \text{ in } [1..\#pts]|pts[c][2]eq2] >;$
$b1 := vb1(pts);$
$b2 := vb2(pts);$
$b3 := vb3(pts);$
$rb1 := Seqset(b1);$
$rb2 := Seqset(b2);$
$rb3 := Seqset(b3);$
$b4 := Seqset(b1)diff\{(b1[1])\};$
$b5 := Seqset(b1)diff\{(b1[\#b1])\};$
$b6 := Seqset(b2)diff\{(b2[1])\};$
$b7 := Seqset(b2)diff\{(b2[\#b2])\};$
$b8 := Seqset(b3)diff\{(b3[1])\};$
$b9 := Seqset(b3)diff\{(b3[\#b3])\};$
$rvb := func < pts|\{\{a, b, c\} : a \text{ in } b1, b \text{ in } b2, c \text{ in } b3|pts[a][1] \text{ eq pts } [b][1]$

and pts $[b][1]$ eq pts $[c][1]\} >$;
$vb := rvb(pts)$;
$f1 := func < pts|\{\{a, b, c\} : a$ in $b5, b$ in $b4, c$ in $rb2|pts[c][1]eq((pts[a][1] + pts[b][1])div2)$
mod m and IsEven $(pts[a][1] + pts[b][1])$ and pts $[a][1]$
ne pts $[b][1]\} >$;
$fnvb1 := f1(pts)$;
$f2 := func < pts|\{\{a, b, c\} : a$ in $b5, binb4, c$ in $rb2|pts[c][1]eq(((m+1)div2)* (pts[a][1] + pts[b][1]))$
mod m and IsOdd $(pts[a][1] + pts[b][1])$ and pts $[a][1]$
ne pts $[b][1]\} >$;
$fnvb2 := f2(pts)$;
$nvb1 := fnvb1$ join $fnvb2$;
$f3 := func < pts|\{\{a, b, c\} : a$ in $b7, b$ in $b6, c$ in $rb3|pts[c][1]eq((pts[a][1] + pts[b][1])div2)$
mod m and IsEven $(pts[a][1] + pts[b][1])$ and pts $[a][1]$
ne pts $[b][1]\} >$;
$fnvb3 := f3(pts)$;
$f4 := func < pts|\{\{a, b, c\} : a$ in $b7, b$ in $b6, c$ in $rb3|pts[c][1]eq(((m+1)div2)* (pts[a][1] + pts[b][1]))$
mod m and IsOdd $(pts[a][1] + pts[b][1])$ and pts $[a][1]$
ne pts $[b][1]\} >$;
$fnvb4 := f4(pts)$;
$nvb2 := fnvb3$ join $fnvb4$;
$f5 := func < pts|\{\{a, b, c\} : a$ in $b9, b$ in $b8, c$ in $rb1|pts[c][1]eq((pts[a][1] + pts[b][1])div2)$
mod m and IsEven $(pts[a][1] + pts[b][1])$ and pts $[a][1]$
ne pts $[b][1]\} >$;
$fnvb5 := f5(pts)$;
$f6 := func < pts|\{\{a, b, c\} : a$ in $b9, b$ in $b8, c$ in $rb1|pts[c][1]eq(((m+1)div2)* (pts[a][1] + pts[b][1]))$
mod m and IsOdd $(pts[a][1] + pts[b][1])$ and pts $[a][1]$
ne pts $[b][1]\} >$;
$fnvb6 := f6(pts)$;
$nvb3 := fnvb5$ join $fnvb6$;
$rbb := vb$ join $nvb1$ join $nvb2$ join $nvb3$;
$bb := Setseq(rbb)$;
$bdes := Design < 2, \#pts|bb >$;

end for ;

Appendix B

Code for Skolem Steiner triple systems


```
q := {((2 * p)) : p in [1..n]};
for m in q do
convert := function(x);
if IsOdd (x) then
 return ((m + x) - 1) div 2;
 elif x eq (m - 1) then  return (m - 1);
 elif x eq 0 then  return 0;
else return (x div 2);
 end if;
 end function;
z3 := [i : i in {0..2 mod 3}];
g := [j : j in {0..(m - 1) mod m}];
pt1 := {< m + 1, 3 >};
pt2 := {< j, i >: i in z3, j in g};
po := pt1 join pt2;
pts := Setseq(po);
f1 := func < pts|[a : a in [1..#pts]|pts[a][2] eq 0] >;
f2 := func < pts|[b : b in [1..#pts]|pts[b][2] eq 1] >;
f3 := func < pts|[c : c in [1..#pts]|pts[c][2] eq 2] >;
f4 := func < pts|[d : d in [1..#pts]|pts[d][2] eq 3] >;
b1 := f1(pts);
b2 := f2(pts);
```

$b3 := f3(pts);$
$b4 := f4(pts);$
$f8 := func < pts|\{\{a, b, c\} : a \text{ in } b1, b \text{ in } b2, c \text{ in } b3|pts[a][1] \text{ eq } pts[b][1]$
$\text{ and pts } [b][1] \text{ eq } pts[c][1] \text{ and pts } \ [a][1]lt(mdiv2)\} >;$
$bb1 := f8(pts);$
$vbb1 := Setseq(bb1);$
$f9 := func < pts|[d : d \text{ in } b1|pts[d][1]lt(\#b1div2)] >;$
$b9 := f9(pts);$
$f10 := func < pts|[d : d \text{ in } b1|pts[d][1]ge(\#b1div2)] >;$
$b10 := f10(pts);$
$f11 := func < pts|[d : d \text{ in } b2|pts[d][1]lt(\#b2div2)] >;$
$b11 := f11(pts);$
$f12 := func < pts|[d : d \text{ in } b2|pts[d][1]ge(\#b2div2)] >;$
$b12 := f12(pts);$
$f13 := func < pts|[d : d \text{ in } b3|pts[d][1]lt(\#b3div2)] >;$
$b13 := f13(pts);$
$f14 := func < pts|[d : d \text{ in } b3|pts[d][1]ge(\#b3div2)] >;$
$b14 := f14(pts);$
$f15 := func < pts|\{\{a, b, c\} : a \text{ in } b4, b \text{ in } b10, c \text{ in } b11|pts[b][1] \text{ eq } ((mdiv2)+$
$pts[c][1]) \text{ and pts } \ [b][1]nepts[c][1]\} >;$
$b15 := f15(pts);$
$f16 := func < pts|\{\{a, b, c\} : a \text{ in } b4, b \text{ in } b12, c \text{ in } b13|pts[b][1] \text{ eq } ((mdiv2)+$
$pts[c][1]) \text{ and pts } \ [b][1]nepts[c][1]\} >;$
$b16 := f16(pts);$
$f17 := func < pts|\{\{a, b, c\} : a \text{ in } b4, b \text{ in } b14, c \text{ in } b9|pts[b][1] \text{ eq } ((mdiv2)+$
$pts[c][1]) \text{ and pts } \ [b][1]nepts[c][1]\} >;$
$b17 := f17(pts);$
$bb2 := b15 \text{ join } b16 \text{ join } b17;$
$vbb2 := Setseq(bb2);$
$f18 := func < pts|[e : e \text{ in } b1|pts[e][1] \text{ eq } (m - 1)] >;$
$b18 := f18(pts);$
$f19 := func < pts|[e : e \text{ in } b1|pts[e][1] \text{ eq } 0] >;$
$b19 := f19(pts);$
$dpts1 := Seqset(b1) \text{ diff } Seqset(b18);$
$dpts2 := Seqset(b1) \text{ diff } Seqset(b19);$
$f21 := func < pts|\{\{a, b, c\} : a \text{ in } dpts1, b \text{ in } dpts2, c \text{ in } b2|pts[c][1]$
$\text{ eq } convert((pts[a][1] + pts[b][1]) \text{ mod } m) \text{ and pts } \ [a][1]nepts[b][1]\} >;$
$b21 := f21(pts);$

```
f22 := func < pts|[e : e in b2|pts[e][1] eq (m − 1)] >;
b22 := f22(pts);
f23 := func < pts|[e : e in b2|pts[e][1] eq 0] >;
b23 := f23(pts);
dpts3 := Seqset(b2) diff Seqset(b22);
dpts4 := Seqset(b2) diff Seqset(b23);
f25 := func < pts|{{a, b, c} : a in dpts3, b in dpts4, c in b3|pts[c][1] eq
 convert ((pts[a][1] + pts[b][1]) mod m) and pts  [a][1]nepts[b][1]} >;
b25 := f25(pts);
f26 := func < pts|[e : e in b3|pts[e][1] eq (m − 1)] >;
b26 := f26(pts);
f27 := func < pts|[e : e in b3|pts[e][1] eq 0] >;
b27 := f27(pts);
dpts5 := Seqset(b3) diff Seqset(b26);
dpts6 := Seqset(b3) diff Seqset(b27);
f29 := func < pts|{{a, b, c} : a in dpts5, b in dpts6, c in b1|pts[c][1] eq
 convert ((pts[a][1] + pts[b][1]) mod m) and pts  [a][1]nepts[b][1]} >;
b29 := f29(pts);
bb3 := b21 join b25 join b29;
vbb3 := Setseq(bb3);
bb := Setseq(bb1 join bb2 join bb3);
skodes := Design < 2, #pts|bb >;
 end for ;
```

Bibliography

[1] A. E. Brouwer, D. M. Mesner, The connectivity of strongly regular graphs, *European J. Comb.* **6** (1985) 215-216.

[2] A. J. Weir, Sylow p-subgroups of the general linear group over finite fields of characteristic p. *Proc. Amer. Math. Soc.* **6**(3) (1955) 454-464.

[3] B. Norman, *Algebraic Graph Theory,* Cambridge University, 1993.

[4] C. J. Colbourn, A. Rosa, *Triple Systems,* Oxford University, New York, 1999.

[5] C. J. Hillar, D. L. Rhea, Automorphisms of finite abelian groups, *The Amer. Math. Monthly*, **1**14 (2007) 917-923.

[6] D. R. Hughes, F. C. Piper *Projective Planes,* Springer-Verlag, New York, 1973.

[7] D. R. Stinson, *Combinatorial Designs: Construction and Analysis,* Springer, New York, 2003.

[8] G. J. Lovegrove, The automorphism groups of Steiner triple systems obtained by the Bose construction, *J. Alg. Comb.* **1**8 (2003) 159-170.

[9] J. D. Dixon,*The Structure of Linear Groups,* Van Nostrand Reinhold, London, 1971.

[10] J. D. Key, Note on a consequence for affine groups of the classification theorem for finite simple groups, *Geometriae Dedicata,* **1**4 (1983) 81-86.

[11] J. D. Key, E. E. Shult, Steiner triple systems with doubly transitive automorphism groups: A corollary to the classification theorem for finite simple groups, *J. Combin. Theory,* **3**6 (1984) 105-110.

[12] J. Šiftar, H. Zeitler, On the automorphism group of special class of quasigroups, *Results in Math.* **3**0 (1996) 160-164.

[13] N. L. Biggs, E. K. Lloyd, R. J. Wilson, *Graph Theory 1736 -1936,* Oxford University, Oxford, 1976.

[14] P. J. Cameron, *Combinatorics,* Cambridge University, Cambridge, 1994.

[15] P. J. Cameron, *Projective spaces and polar spaces,* University of London, Queen Mary and Westfield College, 1992.

[16] R. A. Mathon, K. T. Phelps, A. Rosa, Small Steiner triple systems and their properties, *Ars Combinatoria* **1**5 (1983) 3110.

[17] R. A. Mathon, K. T. Phelps, A. Rosa, Small Steiner triple systems and their properties, *Ars Combinatoria* **1**6 (1983) 286.

[18] R. C. Bose, On the construction of balanced incomplete designs, *Ann. Eugenics* **9** (1939) 353-399.

[19] R. J. Wilson, *Introduction to Graph Theory,* Longman, England, 1996.

[20] S. Lang, *Algebra,* Addison-Wesley, New York, 1993.

[21] S. MacLane, G. Birkhoff, *Algebra,* MacMillan, London, 1967.

[22] T. P. Kirkman, On a problem in combinations, *Camb. & Dublin Math. J.* **2** (1847) 191-204.

[23] T. Skolem, On certain distributions of integers in pairs with given differences, *Math. Scand.* **5** (1957) 57-58.

[24] T. Skolem, Some remarks on the triple system of Steiner, *Math. Scand.* **6** (1958) 273-280.

[25] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **2**4 (1997), 235-265.

[26] W. S. B. Woolhouse , The Prize question, *Lady's and Gentlemen's Diary,* 1844.