University of Palermo
PhD joint program:
University of Catania - University of Messina
XXXVI cycle

Doctoral Thesis

Schreier extensions of Steiner loops and extensions of Bol loops arising from Bol reflections

---

Author:
Mario Galici

Supervisor:
Prof. Giovanni Falcone

A thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

in

Mathematics and Computational Sciences

UNIVERSITY OF PALERMO

Abstract

Department of Mathematics and Computer Sciences

Doctor of Philosophy

Schreier extensions of Steiner loops and extensions of Bol loops arising from Bol reflections

by Mario Galici

This dissertation explores two constructions of loop extensions: Schreier extensions of Steiner loops and a new extension formula for right Bol loops arising from Bol reflections.

Steiner loops are a key tool in studying Steiner triple systems. We investigate extensions of Steiner loops, focusing in particular on the case of Schreier extensions, which provides a powerful method for constructing Steiner triple systems containing Veblen points. We determine the number of the Steiner triple systems of sizes 19, 27 and 31 with Veblen points, presenting some examples.

Furthermore, we study a new extension formula for right Bol loops. We prove the necessary and sufficient conditions for the extension to be right Bol as well. We describe the most important invariants: right multiplication group, nuclei, center. We show that the core is an involutory quandle which is the disjoint union of two isomorphic involutory quandles. Lastly, we derive further results on the structure group of the core of the extension.

Acknowledgements

As I reach the conclusion of this journey, there are many people I want to express my gratitude to.

First and foremost, I would like to thank my family, especially my mother, for believing in me since day zero and providing constant support.

A heartfelt thank you goes to my doctoral supervisor, Professor Giovanni Falcone, whose support, guidance and trust have been crucial in this path. He has provided valuable insights and has been a source of inspiration and encouragement.

Another significant figure to whom I want to express my gratitude is Professor Claudio Bartolone, a fundamental and inspiring person without whom I might not have made the decision to embark on this journey.

To two special people, Giovanna and Ivana, I want to say thank you. Starting as colleagues and becoming great friends, we have been together since the very first day.

To Gianmarco, Manuel, and Alessandro, with whom I shared these three years of the doctoral program, thank you for being a source of mutual support and the best companions I could wish for on this journey. Thanks also to old and new friendships made along the way: Eleonora, Sara, Peppe, Lydia, Federica, and Bruno.

The last, but not least, expression of gratitude goes to my co-authors whom I have not yet mentioned: Ágota Figula, Gábor Nagy and Giuseppe Filippone. Our collaborative work has been truly inspiring.

Contents

List of Figures

List of Tables

Chapter 1

Backgrounds

1.1 Introduction

As of now, a *general* extension theory for loops still does not exist. The lack of associativity makes the situation less controllable and very different from the theory of group extensions. Many authors have contributed in this field, working on *specific* kinds of extensions for some classes of loops. Examples include nuclear extensions [30], [56], Schreier extensions [74] or the famous Chein's extensions for Moufang loops [15]. See also [17], [26], [55], [72], [31], [50].

This dissertation primarily focuses on two constructions of loop extensions. The initial focus of our study is on the Schreier extensions of Steiner loops, which offer a highly effective approach to construct and classify specific Steiner triple systems which present similarities to the point-line designs of projective spaces over the field GF(2). Additionally, we are going to consider a new extension formula for Bol loops, arising from the Bol reflections of the associated 3-nets.

This dissertation is based on research papers written by the author during his Ph.D. program. Specifically, Chapter 2 derives from the work presented in [32], Chapter 3 from [36], and Chapter 4 from [38]. The structure of the thesis is as follows.

After this introduction, in the first chapter, we present a brief history of Steiner triple systems and loops, the two main topics of this thesis. Additionally, we provide the fundamental concepts which are essential to a clear and comprehensive understanding of the dissertation.

In Chapter 2 we study Steiner triple systems by means of the associated Steiner loops, using a classic algebraic technique, that is, reducing their structure to that of suitable normal subloops and the corresponding factor loops. In fact, subloops correspond to Steiner triple subsystems and normal subloops give in turn quotient loops which are associated with *quotient* Steiner triple systems, as well.

We must remark, to this extent, that recursive methods for the construction of "products" of Steiner triple systems are very well known [20, Ch. 3], but among these methods only one, the so-calling *doubling* construction, coincides with the extension provided by our construction in the trivial case where the factor loop corresponds to the *degenerate* Steiner triple system with only one point. This is as well the case where the normal subloop corresponds to a *projective hyperplane*, a topic which in turn was firstly studied by Teirlinck [93] and later by Doyen, Hubaut, and Vandensavel [29].

We distinguish the case where the normal subloop is central: after showing that central elements correspond to *Veblen points* (see Definition 2.1.7), we introduce an extension theory which takes inspiration by the well-known cohomology theory for commutative groups. This specific theory provides a constructive approach to describe Steiner triple systems containing Veblen points. In particular, the set of Veblen points, which corresponds to the center of the loop, always gives a Steiner triple subsystem of size 2^n-1 which is the point-line design of a projective space over the field GF(2). The whole Steiner loop, in this case, is a Schreier extension of its center by the corresponding quotient loop, which can be described by a factor system f as in Lemma 2.5.1. In Section 2.6 we face with the problem of defining equivalent and isomorphic extensions.

It is worthwhile to point out that the center of a Steiner loop different from an elementary abelian 2-group has index at least eight (see Theorem 2.5.3). This means that projective geometries over GF(2) are the only Steiner triple systems of size v with more than $\frac{v-7}{8}$ Veblen points (see Corollary 2.5.4).

In Chapter 3, we use the theoretical methods introduced previously with the aim of classifying Steiner triple systems with Veblen points. Counting all Steiner triple systems of a given order is a problem which becomes very challenging as the order increases. The last full result in this direction is by P. Kaski and P. R. J. Östergård [51]: they determined that the number of non-isomorphic STS(19)s is $11,084,874,829$. In [52] and [47], the authors classified STS(21)s containing subsystems of order 7 and 9, and also gave an estimation of the total number of all STS(21)s, but a complete classification seems (for now) out of hand. For this reason, we decided to focus on the number of Steiner triple systems containing Veblen points, which can be seen as a generalization of projective STSs. We found results for the cases of size 19, 27 and 31, respectively.

In Chapter 4 we deal with a new extension formula for right Bol loops, giving a construction method arising from *Bol reflections*. Before going into the details, we provide the necessary notions, with the main focus on the geometric and group theoretical tools. We will use Aschbacher's efficient Bol loop folder method to describe the extension. Starting from a Bol loop L, we denote with $\widetilde{L}$ the resulting extension loop. In Section 4.4, we study $\widetilde{L}$ and find necessary and sufficient conditions for it to be right Bol as well, Moufang or associative. In Section 4.5, we describe the most important invariants of $\widetilde{L}$: right multiplication group, nuclei, center. Finally, in Section 4.6, we prove some results about the *core* of $\widetilde{L}$, which is an involutory quandle and investigate its structure group.

1.2 Preliminaries

Here we present some preliminaries about Steiner triple systems and the basic notions of loop theory, together with a brief historical introduction to both topics.

1.2.1 A brief historical introduction to Steiner triple systems

The study of block designs can be traced back to 1835 when Plücker [82] investigated algebraic curves and came across a Steiner triple system of order 9. Initially, he claimed that an STS(v) could exist only if $v \equiv 3 \pmod 6$, but he later corrected this to $v \equiv 1, 3 \pmod 6$ in 1839 [83]. Plücker's results shed light on the early relation of designs and geometry.

In England, Woolhouse presented a question about the number of possible combinations of v symbols in subsets of order p such that no combination of q symbols which may appear in any one of them shall be repeated in any other.

In 1847, Kirkman investigated the existence of such a system when $p = 3$ and $q = 2$, constructing STS(v)s for all $v \equiv 1, 3 \pmod 6$ [58]. However, the expression *Kirkman triple systems* was not used. Steiner, who was unaware of Kirkman's research, inquired about their existence in 1853 [89]. Following that, Reiss [87] proved their existence, and Witt [95] later named them after Steiner. Kirkman's name is now associated with *solvable* Steiner systems after his famous problem with fifteen schoolgirls: fifteen young ladies from a school walk out in five rows of three consecutively for seven days; the task is to arrange them daily so that no two of them walk together twice.

In 1850, Cayley first published his solution to the schoolgirls problem [14], which was followed in the same year by Kirkman's solution [59]. Although the two solutions are distinct as Kirkman triple systems, they are isomorphic as Steiner triple systems and represent different resolutions into parallel classes of the point-line design of the projective geometry PG$(3, 2)$. In 1860, Peirce identified all three solutions to the 15-schoolgirls problem admitting an automorphism of order 7 [79]. In 1917 and 1922, Mulder [66] and Cole [21], respectively, independently enumerated the seven non-isomorphic solutions to the problem. Ray-Chaudhuri and Wilson proved the existence of Kirkman triple systems of order v, denoted as KTS(v), for all $v \equiv 3 \pmod 6$ in 1971 [85]. Denniston ultimately resolved the problem in 1974 [24].

Early discoveries revealed that there are unique STS(7) and STS(9). In 1897, Zulauf [96] showed that the known STS(13)s can be divided into two isomorphism classes, and in 1899 De Pasquale [23] proved that these are the only two possible isomorphism classes. In a groundbreaking memoir from 1919, White, Cole, and Cummings [22] classified precisely 80 non-isomorphic STS(15)s. Their results were confirmed in 1955 when Hall and Swift [45] used computers: this represents one of the first cases where computers were used to catalog combinatorial designs. Many years later, in 2004, the number of non-isomorphic STS(19)s was found to be $11,084,874,829$ by P. Kaski and P. R. J. Östergård [51].

In 1891, Netto [76], without knowledge of Kirkman's work, presented four methods for constructing Steiner triple systems:

(i) an STS($2n + 1$) from an STS(n) (previously studied by Kirkman);

(ii) an STS(nm) from an STS(m) and an STS(n);

(iii) an STS(p) where p is a prime number of the form $6m + 1$;

(iv) an STS($3p$) where p is of the form $6m + 5$.

These methods enabled the construction of STS(v)s for all admissible values of $v < 100$, except for 25 and 85. In 1893, Moore [64] extended Netto's work by providing a formula for constructing STS($w + u(v - w)$) using an STS(u) and an STS(v) with an STS(w) subsystem. In this same work, Moore also proved that for all admissible $v > 13$ there exist at least two non-isomorphic STS(v)s.

Three of the most famous and cited sources on Steiner triple systems include the book "Triple Systems" by C. J. Colbourn and A. Rosa [20], C. J. Colbourn and J.H. Dinitz's "Handbook of Combinatorial Designs" [19], and "Design Theory" by T. Beth, D. Jungnickel, and H. Lenz [6].

1.2.2 Some basic notions about Steiner triple systems

Steiner triple systems are among the most studied objects in design theory and more in general in the field of combinatorics.

Definition 1.2.1. A *triple system* $(\mathcal{S}, \mathcal{T})$ consists of a set $\mathcal{S}$ of v elements (*points*) and a family $\mathcal{T}$ of 3-subsets of $\mathcal{S}$, called *triples* (also *blocks* or *lines*), with the property that every 2-subset of $\mathcal{S}$ occurs in exactly λ triples of $\mathcal{T}$. The size v of the set $\mathcal{S}$ is called the *order* of the triple system. If $\lambda = 1$ we speak about *Steiner triple systems*, denoted by STS(v) for short.

Throughout this work, we will denote a Steiner triple system $(\mathcal{S}, \mathcal{T})$ by just its set of points $\mathcal{S}$. The order of a STS(v) is necessarily an odd number. Indeed, fixed an element, it occurs in one block with every other point of $\mathcal{S}$, and within every block in which it occurs it appears with two other elements, hence the number $v - 1$ must be even. Moreover, since each block contains three pairs, the number $\binom{v}{2}$ must be divisible by 3. These two conditions together say that a Steiner triple systems of order v can exist only when $v \equiv 1, 3 \pmod 6$. This condition was proved to be also sufficient in 1847 (inserire reference). If v is 1 or 3 (mod 6), we call it *admissible*. The number of 2-subsets of $\mathcal{S}$ is $\binom{v}{2} = \frac{v(v-1)}{2}$, of which 3 appear in one same triple $B \in \mathcal{B}$, hence the total number of blocks of a STS(v) is $b = \frac{v(v-1)}{6}$.

We remark here that we also consider the trivial cases of a STS(1) with one point and no blocks, and of a STS(3) with three points and a unique triple.

Example 1.2.1.1 (Projective systems)**.** Let V be an $(n+1)$-dimensional vector space over the field GF(2). A *punctured subspace* of V is a subspace of V without the zero vector. The set of all the punctured subspace of V is the *n-dimensional projective geometry* PG$(n, 2)$. Punctured subspaces of dimension 1 are the *points* and the ones of dimension 2 are the lines of the projective space. Since each line contains three points and for two distinct points there is exactly on line passing through them, the points and lines of a projective space PG$(n, 2)$ are respectively the elements and the triples of a STS$(2^{n+1} - 1)$. The Steiner triple systems of this kind are called *projective*. The smallest significant example is the so called *Fano plane* shown in Figure 1.1, that is the projective plane PG$(2, 2)$.

$$P_1 = [0, 0, 1], \quad P_2 = [0, 1, 0], \quad P_3 = [0, 1, 1], \quad P_4 = [1, 0, 0],$$

$$P_5 = [1, 0, 1], \quad P_6 = [1, 1, 0], \quad P_7 = [1, 1, 1].$$

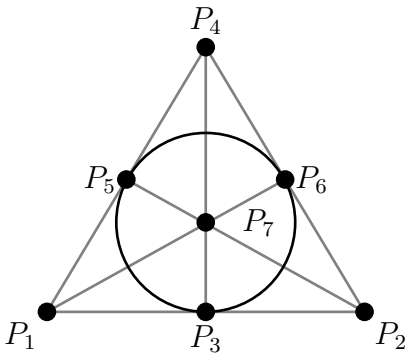

FIGURE 1.1: The Fano plane PG(2, 2)

The seven points and lines represent the elements and triples of a STS(7).

Example 1.2.1.2 (Affine systems)**.** Let V be an n-dimensional vector space over the field GF(3). The *n-dimensional affine geometry* $\mathrm{AG}(n, 3)$ is the set of all the subspaces of V and their cosets. The points of the affine space are the vectors of V and the lines of the affine space are translates of the 1-dimensional subspaces of V. Since each affine line contains three points and for two distinct points there is exactly on line passing through them, the points and lines of an affine space $\mathrm{AG}(n, 3)$ are respectively the elements and the triples of a $\mathrm{STS}(3^n)$. The Steiner triple systems of this kind are called *affine*. The smallest significant example is the affine plane $\mathrm{AG}(3, 2)$, shown in Figure 1.2.

$$P_1 = (-1, 1), \quad P_2 = (0, 1), \quad P_3 = (1, 1), \quad P_4 = (-1, 0), \quad P_5 = (0, 0),$$
$$P_6 = (1, 0), \quad P_7 = (-1, -1), \quad P_8 = (0, -1), \quad P_9 = (1, -1),$$

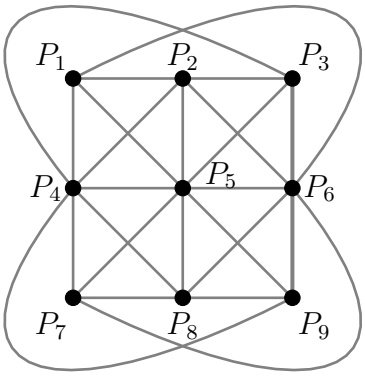

FIGURE 1.2: The affine plane AG(2, 3)

The nine points and twelve lines represent the elements and triples of a STS(9).

An $\mathrm{STS}(u)$ $(\mathcal{V}, \mathcal{B})$ is a *subsystem* of an $\mathrm{STS}(v)$ $(\mathcal{S}, \mathcal{T})$ if $\mathcal{V} \subseteq \mathcal{S}$ and $\mathcal{B} \subseteq \mathcal{T}$. Two Steiner triple systems $(\mathcal{S}, \mathcal{T})$ and $(\mathcal{V}, \mathcal{B})$ are *isomorphic* if there is a bijection

$\phi\colon \mathcal{S} \leftrightarrows \mathcal{V}$ between the sets of points which induces a bijection $\mathcal{T} \leftrightarrows \mathcal{B}$ between the families of triples as well. Up to isomorphism, the Fano plane $\mathrm{PG}(2,2)$ and the affine plane $\mathrm{AG}(2,3)$ are the only Steiner triple systems of orders 7 and 9. The number of non-isomorphic $\mathrm{STS}(v)$s grows really quickly with v. Indeed, up to isomorphism, there are only 2 STS(13)s, 80 STS(13)s and $11,084,874,829$ STS(19). For the next admissible order, which is 21, the non-isomorphic STSs is still unknown. In general, the number of non-isomorphic $\mathrm{STS}(v)s$ is $v^{v^2\left(\frac{1}{6}+o(1)\right)}$ as $v \to \infty$ [53].

We conclude this section with the definitions of an important class of Steiner triple Systems, which generalize the affine ones.

Definition 1.2.2. A *Hall triple system* (HTS) is a Steiner triple system in which any three points not in a triple generate a sub-STS(9).

The cardinality of any HTS is 3^m for some integer $m \geq 2$. The first example of a non-affine HTS has order 81, and there exists an HTS of order 3^m for any $m \geq 4$.

1.2.3 A brief historical introduction to loop theory

The most simple description of a loop is "a group without associativity". This explanation is true, but it merely provides a basic definition. In fact, loop theory is not just a generalization of group theory, but a distinct discipline rooted in algebra, geometry, topology, and combinatorics.

Throughout the history of science, revolutionary ideas have emerged independently in different places. The concept of non-associative operations dates back to simple subtraction of natural numbers, but the first abstract example, the Cayley numbers, emerged in 1845, later generalized into Cayley-Dickson algebras by Dickson.

Anton K. Suschkewitsch, a Russian mathematician, discussed non-associativity explicitly in 1929 [92]. Suschkewitsch conjectured the existence of non-associative binary systems satisfying the Lagrange property, since he noticed that in the proof of the Lagrange Theorem for groups, the associativity law is not used. Despite his insights, his ideas were not widely appreciated in his home country at the time.

Turning to 1930s Germany, our next milestone emerges simultaneously from algebra, geometry, and topology. Two key papers, Ruth Moufang's "Zur Struktur von Alternativkörpern" (1934) [65] and Gerrit Bol's "Gewebe und Gruppen" (1937) [7], established a formal beginning for loop theory. These works defined the foundations of the two most important classes of loops as we know them now: Moufang loops and Bol loops.

Now, let us examine Moufang's paper. She introduces a structure named a quasigroup Q^* satisfying the following properties:

(1) closure under the operation $\cdot$;

(2) existence of an identity element 1 and unique inverse x^{-1} for each x;

(3) $a(a^{-1}b) = (aa^{-1})b$ and $(ba^{-1}) = b(aa^{-1})$ for every a, b;

(4) $(a(ca))b = a(c(ab))$ for every a, b, c.

She also defines a further system Q^{**}, believing it to be different from Q^*, satisfying the following additional identity:

(5) $(ab)(ca) = a((bc)a)$ for every a, b, c.

Bol soon demonstrated that condition (4) leads to (5), and later Bruck showed that both are equivalent to the following identity:

(6) $((ab)c)b = a(b(cb))$ for every a, b, c.

The structure introduced as Q^* is now known as a Moufang loop, which can be defined by any of the Moufang identities (4) through (6). Ruth Moufang, together with Sofia Kovalevskaya and Emmy Noether, is known as a pioneering woman who made significant contributions to mathematics.

The next major contribution to quasigroups following Moufang's work appeared in Gerrit Bol's paper, three years later. Here, Bol takes a web-geometric approach to the topic. He presents the first non-associative, commutative Moufang loop (of order 81) constructed by Zassenhaus. Moreover, Bol explains the algebraic meaning of specific configurations and how they relate to the laws that nowadays we call the right and left Bol identities, respectively:

$$a((bc)b) = ((ab)c)b \quad \text{and} \quad (b(cb))a = b(c(ba)). \tag{1.1}$$

Bol's work effectively split the Moufang identity in two, proving that a loop is Moufang if and only if it satisfies both the right and left Bol properties. Moreover, it is noteworthy that Bol did not have knowledge of Moufang's work when he was writing his paper; as mentioned in a footnote, he only became aware of it after he had finished his paper. It was Zassenhaus again who constructed the first instance of a right Bol loop.

Despite their early contributions, neither Moufang nor Bol returned to further studies on quasigroups. Bol instead redirected his publications towards questions on differential geometry.

After quasigroups declined in Germany, the United States became the new center for quasigroup research. American publications on quasigroups such as the works by Hausmann and Ore in 1937 [46], Murdoch in 1939 [67], and Garrison in 1940 [40] had already emerged. In 1942, there was a significant transformation in the terminology of quasigroup theory as it became essential to differentiate between systems with and without an identity element. The term "loop" was created by Albert's circle in Chicago, drawing inspiration from the *Chicago Loop*, the city's central business area, and its elevated train system. Albert introduced this term in his 1943 publications, "Quasigroups. I" [1] and "Quasigroups. II" [2]. The former also marked the introduction of *isotopy* for quasigroups. Soon thereafter, Richard Hubert Bruck contributed significantly to the field with his papers in 1944 [11] and 1946 [9], and later in 1958 with the book "A Survey of Binary Systems" [8]. This book still remains one of the most cited work on loops, together with Hala O. Pflugfelder's "Quasigroups and loops: introduction" [81].

During this time in England, Latin squares were a major research area, even though this subjects is much older than loop theory. There appeared links between the combinatorial aspects of Latin squares and quasigroup theory. Additionally, combinatorial structures such as block designs and Steiner triple systems are related to algebraic varieties of Steiner quasigroups and totally symmetric loops.

Belousov had a crucial role in the development of quasigroup and loop theory for the Soviet Union and the nations under its influence. His book, "Foundations of the Theory of Quasigroups and Loops" [5], published in 1967, had a comparable influence to that of Bruck in the United States. However, Belousov's remarkable achievements are less recognized in the West due to the language barrier as the book is in Russian and never been translated.

While Bruck's focus was on loops, Belousov's emphasis shifted towards quasigroups in general. His contributions had a significant impact on the spread of loop theory throughout Central Europe, specifically in Hungary, Romania, and the former Czechoslovakia.

1.2.4 Some basic notions about loops

A *quasigroup* is a set L endowed with a binary operation $x \cdot y$ such that the equations $a \cdot x = b$, $y \cdot a = b$ have unique solutions for x, y. The solutions are denoted by divisions on the left and on the right $x = a\backslash b$, $y = b/a$. *Loops* are quasigroups with a unit element 1. The multiplication sign is often ignored, $(x \cdot y) \cdot z$ is written as $xy \cdot z$. The *left* and *right multiplication maps*

$$L_a : x \longmapsto ax, \quad R_a : x \longmapsto xa \tag{1.2}$$

are invertible maps of L into itself.

The operation of a loop does not need to be associative: when associativity holds, the loop is in fact a group. A subloop $N \leq L$ is *normal* if it is the kernel of a homomorphism or, equivalently, if the relations

$$xN = Nx, \quad x \cdot Ny = xN \cdot y, \quad x \cdot yN = xy \cdot N,$$

hold for any $x, y \in L$. If L is commutative, the three normality conditions reduce to the only $x \cdot yN = xy \cdot N$.

The *left*, *middle* and *right nuclei* of a loop L are, respectively, the subloops

$$\begin{aligned} N_\lambda(L) &= \{n \in L \mid na \cdot b = n \cdot ab, \text{ for all } a, b \in L\}, \\ N_\mu(L) &= \{n \in L \mid an \cdot b = a \cdot nb, \text{ for all } a, b \in L\}, \\ N_\rho(L) &= \{n \in L \mid ab \cdot n = a \cdot bn, \text{ for all } a, b \in L\}. \end{aligned}$$

The intersection of the three nuclei $N = N_\lambda \cap N_\mu \cap N_\rho$ is called the *nucleus* of L. The *commutant* of a loop L is

$$C(L) = \{z \in L \mid xz = zx \text{ for all } x \in L\}.$$

The *center* of L is the intersection of the commutant and the nucleus:

$$Z(L) = C(L) \cap N(L)$$

The center is always a normal subloop in L.

A loop L is said *totally symmetric* (TS) if it is commutative and the identity

$$x(xy) = y \tag{1.3}$$

holds for every $x, y \in L$. In a TS loop the left and right inverses $x\backslash 1$ and $1/x$ of any element x coincide; we call it the *inverse* of x, denoted by x^{-1}. Every TS loop has exponent 2. Furthermore, the three nuclei of a TS loop coincide. For loops of exponent two, the totally symmetric property $x(xy) = y$ is equivalent to the weak associativity which says that $x(yz) = 1$ whenever $(xy)z = 1$, for any $x, y, z \in L$.

A loop is said a *right Bol* loop if it satisfies the following identity for all $x, y, z \in L$:

$$(((xy)z)y) = x((yz)y). \tag{1.4}$$

Also in a right Bol loop the left and right inverses $x\backslash 1$ and $1/x$ of any element x coincide, and we denote the inverse by x^{-1}. Furthermore, any right Bol loop is power associative, meaning that every element generates a cyclic group. In particular, $(xy)y^{-1} = x$ for all x, y. If a loop satisfies the right Bol property (1.4) and its opposite $x(y(xz)) = (x(yx))z$, then it is called a *Moufang loop.* Moufang loops are *diassociative,* that is, any two elements generate an associative subloop. In particular, the inverse map is an anti-automorphism: $(xy)^{-1} = y^{-1}x^{-1}$.

Chapter 2

Steiner loops

Although it has been known since the 1950s ([44], [8]) that Steiner triple systems can be endowed with the algebraic structure of a loop, a comprehensive extension theory for these systems has not been explored yet. Surprisingly, the potential of loop theory in this context appears to have been underestimated. For instance, prominent results in [60], [80] not only can be significantly simplified but also strengthened, as highlighted in Section 2.3.

Considering a Steiner triple system, there are two approaches of defining an operation which gives a loop structure. In one case, the resulting loop is called a *Steiner loop of projective type* (or simply a *Steiner loop*), while in the other, it is called a *Steiner loop of affine type* (see Definition 2.2.1). The former involves an additional element for the unit, whereas in the latter the identity element is a (chosen) fixed point within the Steiner triple system. Here, we provide the definition for the projective case, which will be our main focus. However, in Section 2.2 we will present the definition of the Steiner loop of affine type and discuss analogies and differences between the two cases.

Definition 2.0.1. Consider a Steiner triple system $\mathcal{S}$ and let Ω be a further element not belonging to $\mathcal{S}$. We define $\mathcal{L}_{\mathcal{S}}$ as the set $\mathcal{S} \cup \{\Omega\}$ endowed with the binary operation $\cdot$ described as follows:

- for any distinct x and y in $\mathcal{S}$, their product $x \cdot y$ is defined as the third point in the triple of $\mathcal{S}$ containing x and y;
- for any $x \in \mathcal{L}_{\mathcal{S}}$, we set $x^2 = \Omega$ and $x \cdot \Omega = \Omega \cdot x = x$.

$\mathcal{L}_{\mathcal{S}}$ is called a *Steiner loop of projective type* (or simply a *Steiner loop*).

If there is no ambiguity, the multiplication sign is usually dropped. Clearly, using the commutative operation defined above, the equation $ax = b$ has a unique solution, which is the third point of the triple through a and b. Additionally, Ω is the unit of $\mathcal{L}_{\mathcal{S}}$, confirming that $\mathcal{L}_{\mathcal{S}}$ is indeed a loop. Moreover, Steiner loops of projective type are precisely the finite totally symmetric loops, as defined in § 1.2.4. Indeed, for any triple $\{x, y, z\}$ of $\mathcal{S}$, the totally symmetric property holds:

$$x(xy) = xz = y.$$

Although the concept of a loop arising from a Steiner triple system is well established, the name *of projective type* is a relatively recent terminology. We have chosen to use this name in alignment with the ideas in [33], where the

authors deal with an alternative construction, previously introduced by Chein in [15], of a loop associated with a given STS, which they call *of affine type*. We will deal with this other construction in Sections 2.2 and 2.3. However, when there is no ambiguity, we will use the term "Steiner loop" specifically to denote those of projective type.

The concept of Steiner loops of projective type gives a one-to-one correspondence between Steiner triple systems and finite totally symmetric loops. In fact, already in 1958, Bruck in [8] observed that a totally symmetric loop is essentially the algebraic version of an Steiner triple system. This concepts have been studied, for instance, in [84] and [91].

Moreover, $\mathcal{L}_\mathcal{S}$ fulfills the weak inverse property. Indeed, the triples $\{x, y, z\}$ of $\mathcal{S}$ are characterized by

$$xyz = \Omega, \tag{2.1}$$

and the elements in each triple associate. A Steiner loop of projective type $\mathcal{L}_\mathcal{S}$ turns out to be a group, specifically an elementary abelian 2-group, precisely when the Steiner triple system $\mathcal{S}$ is projective (see [27]).

2.1 Substructures, quotients and multiplication group

It is natural now to talk about isomorphism, ask if there is some correspondence between subloops and subsystems, and investigating normality and quotient loops. Let $\mathcal{L}_{\mathcal{S}_1}$ and $\mathcal{L}_{\mathcal{S}_2}$ be two Steiner loops of projective type with identities Ω_1 and Ω_2 respectively. The homomorphisms $\mathcal{L}_{\mathcal{S}_1} \to \mathcal{L}_{\mathcal{S}_2}$ are exactly the maps sending Ω_1 to Ω_2 and any triple of $\mathcal{S}_1$ either into a triple of $\mathcal{S}_2$ or into Ω_2. If $\mathcal{S}_1$ and $\mathcal{S}_2$ have the same order, then the isomorphisms of loops $\mathcal{L}_{\mathcal{S}_1} \leftrightarrows \mathcal{L}_{\mathcal{S}_2}$ correspond exactly to the isomorphisms of Steiner triple systems $\mathcal{S}_1 \leftrightarrows \mathcal{S}_2$. Naturally, the group $\mathrm{Aut}(\mathcal{L}_\mathcal{S})$ can be identified with $\mathrm{Aut}(\mathcal{S})$.

Moreover, there is a one-to-one correspondence between subloops of $\mathcal{L}_\mathcal{S}$ and Steiner triple subsystems of $\mathcal{S}$. In addition, when a subloop is normal, the quotient loop gives in turn a further Steiner triple system, as shown in the following Theorem.

Theorem 2.1.1. *Let $\mathcal{S}$ be a Steiner triple system and $\mathcal{L}_\mathcal{S}$ the corresponding Steiner loop with identity Ω.*

i) $\mathcal{L}'$ is a subloop of $\mathcal{L}_\mathcal{S}$ if, and only if, it is the Steiner loop $\mathcal{L}_\mathcal{R}$ associated with a subsystem $\mathcal{R}$ of $\mathcal{S}$.

ii) If $\mathcal{L}_\mathcal{N}$ is a normal subloop of $\mathcal{L}_\mathcal{S}$, then each non-trivial coset $x\mathcal{L}_\mathcal{N}$ generates a subsystem of $\mathcal{S}$ containing $\mathcal{N}$.

iii) If $\mathcal{L}_\mathcal{N}$ is a normal subloop of $\mathcal{L}_\mathcal{S}$, then the factor loop $\mathcal{L}_\mathcal{S}/\mathcal{L}_\mathcal{N}$ is a Steiner loop $\mathcal{L}_\mathcal{Q}$, with $\mathcal{Q}$ the Steiner triple system consisting of the non-trivial cosets of $\mathcal{L}_\mathcal{N}$.

Proof. i) $\mathcal{L}'$ is a subloop of $\mathcal{L}_\mathcal{S}$ if, and only if, it is closed under the operation of $\mathcal{L}_\mathcal{S}$, which is equivalent to saying that if two distinct elements of $\mathcal{S}$ are

contained in $\mathcal{R} := \mathcal{L}' \setminus \{\Omega\}$, then the third point $z = xy$ of the triple through x and y is in $\mathcal{R}$ as well.

ii) Let $\mathcal{L}_\mathcal{N}$ be a normal subloop of $\mathcal{L}_\mathcal{S}$ and $x \notin \mathcal{L}_\mathcal{N}$. The non-trivial coset $x\mathcal{L}_\mathcal{N}$ generates the Steiner triple subystems $x\mathcal{L}_\mathcal{N} \cup \mathcal{N}$.

In fact, if xn_1 and xn_2 are two distinct elements of $x\mathcal{L}_\mathcal{N}$, then $(xn_1) \cdot (xn_2) = n_3 \in \mathcal{L}_\mathcal{N}$, since $(x\mathcal{L}_\mathcal{N}) \cdot (x\mathcal{L}_\mathcal{N}) = \mathcal{L}_\mathcal{N}$. This means that the third poit in the triple through xn_1 and xn_2 is an element of $\mathcal{N}$. Hence, the subsystem of $\mathcal{S}$ generate by $\mathcal{N}$ must be contained in $x\mathcal{L}_\mathcal{N} \cup \mathcal{N}$.

Moreover, if $xn_1 \in x\mathcal{L}_\mathcal{N}$ and $n_2 \in \mathcal{N}$, then we have that $(xn_1) \cdot n_2 = xn_3$ since $(x\mathcal{L}_\mathcal{N}) \cdot \mathcal{L}_\mathcal{N} = x\mathcal{L}_\mathcal{N}$, that is $\{xn_1, n_2, xn_3\}$ is a triple $\mathcal{S}$ contained in $\mathcal{N} \cup x\mathcal{L}_\mathcal{N}$.

This proves that $x\mathcal{L}_\mathcal{N}$ generates the subsystem $x\mathcal{L}_\mathcal{N} \cup \mathcal{N}$. Furthermore, we note that the order of $\mathcal{N} \cup x\mathcal{L}_\mathcal{N}$ is admissible: indeed, if w is the size of $\mathcal{N}$, then $|\mathcal{N} \cup x\mathcal{L}_\mathcal{N}| = |\mathcal{N}| + |x\mathcal{L}_\mathcal{N}| = w + w + 1 = 2w + 1$, and $2w + 1 \equiv 3$ or $1 \mod 6$ whenever $w \equiv 1$ or $3 \mod 6$, respectively.

iii) The last assertion follows from the fact that the quotient $\mathcal{L}_\mathcal{S}/\mathcal{L}_\mathcal{N}$ is a finite totally symmetric loop.

□

Now we give some remarks about the multiplication group of a Steiner loop. In [91] it is proved that if the order of any product of two different translations of a Steiner triple system $\mathcal{S}$ of size $v > 3$ is odd, then $\mathrm{Mult}(\mathcal{L}_\mathcal{S})$ contains the alternating group of degree $v+1$. In particular, the order of any product of two different translations of a Hall triple system is three, a fact proved in [25]. They also remark that in the Steiner triple systems constructed in [28] from a cyclic group the order of any product of two different translations is odd, as well.

Theorem 2.1.2. *Let $\mathcal{S}$ be a Steiner triple system of order v. Each translation of $\mathcal{L}_\mathcal{S}$ has the form*

$$R_x = (\Omega, x)(y_1, y_2)(y_3, y_4) \cdots (y_{v-1}, y_n). \tag{2.2}$$

Moreover, the multiplication group $\mathrm{Mult}(\mathcal{L}_\mathcal{S})$ is contained in the alternating group A_{v+1} if and only if $v \equiv 3$ or $7, \mod 12$.

Proof. Since $\mathcal{L}_\mathcal{S}$ has exponent two, in every translation R_x we find the transposition (Ω, x). Every triple $\{x, y_1, y_2\}$ gives a transposition (y_1, y_2) in R_x. Hence R_x has the form expressed in (2.2).

Since $v \equiv 1, 3 \mod 6$, we have $v \equiv 1, 3, 7, 9 \mod 12$. If $v \equiv 3, 7, \mod 12$, then one has $|\mathcal{L}_\mathcal{S}| \equiv 4, 8 \mod 12$. Therefore in both cases $|\mathcal{L}_\mathcal{S}|$ is divisible by 4. The number of transpositions in R_x for all $x \neq \Omega$ is $\frac{|\mathcal{L}_\mathcal{S}|}{2}$ which is even. Therefore, the permutation R_x is even and the group $\mathrm{Mult}(\mathcal{L}_\mathcal{S})$ is contained in A_{v+1}. On the other hand, if $v \equiv 1, 9 \mod 12$, the cardinality $|\mathcal{L}_\mathcal{S}|$ is not divisible by 4. Therefore, number of transpositions in R_x is odd. □

To take an initial step toward reducing the problem of studying STSs to the case of simple Steiner loops, we present the following theorem, in which we characterize the multiplication group in a specific case.

Theorem 2.1.3. *Let $\mathcal{S}$ be a Steiner triple system containing an* STS(9) *with the Steiner loop $\mathcal{L}_\mathcal{S}$ being simple. If $v \equiv 3, 7 \mod 12$, then* $\mathrm{Mult}(\mathcal{L}_\mathcal{S}) = A_{v+1}$. *If $v \equiv 1, 9 \mod 12$ then* $\mathrm{Mult}(\mathcal{L}_\mathcal{S}) = S_{v+1}$.

Proof. Since $\mathcal{L}_\mathcal{S}$ is simple, $\mathrm{Mult}(\mathcal{L}_\mathcal{S})$ is primitive. Let $\mathcal{R}$ be the sub-STS(9) of $\mathcal{S}$, then $\mathrm{Mult}(\mathcal{L}_\mathcal{S})$ contains $\mathrm{Mult}(\mathcal{L}_\mathcal{R})$, which is the symmetric group on 10 elements [91]. In particular, $\mathrm{Mult}(\mathcal{L}_\mathcal{S})$ contains a 3-cycle, and by Jordan's theorem on primitive groups of permutations the assert is proved. □

2.1.1 Normal subsystems and Veblen points

If $\mathcal{L}_\mathcal{N}$ is a normal subloop of $\mathcal{L}_\mathcal{S}$ and $\mathcal{L}_\mathcal{Q}$ is the corresponding quotient loop, we say that $\mathcal{N}$ is a *normal subsystem* of $\mathcal{S}$ and $\mathcal{Q}$ is the corresponding *quotient system*. We remind the reader that the normality of a subloop $\mathcal{L}_\mathcal{N}$ is described by the relation $x(y\mathcal{L}_\mathcal{N}) = (xy)\mathcal{L}_\mathcal{N}$, hence for every $x, y \in \mathcal{L}_\mathcal{S}$ and $n \in \mathcal{L}_\mathcal{N}$, there exists a unique $m \in \mathcal{L}_\mathcal{N}$ such that

$$x \cdot yn = xy \cdot m.$$

With a combinatorial point of view, we can visualize the normality of a subsystem $\mathcal{N}$ of $\mathcal{S}$ with the following Figure (2.1), where $t = x \cdot yn = xy \cdot m$.

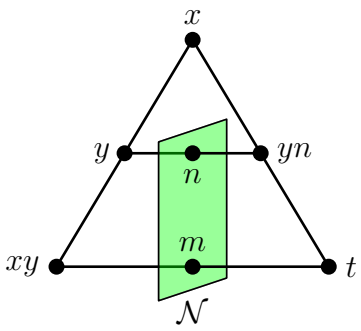

FIGURE 2.1: Normality of a subsystem $\mathcal{N}$

Definition 2.1.4. Let v be the order of a Steiner triple system. We say that $v + 1 = (u + 1)(w + 1)$ is an *admissible factorization* if u and w are admissible in the sense of Steiner triple systems.

Example 2.1.4.1. Since the factorization $14 = 2 \cdot 7$ is not admissible, we can say that the two non-isomorphic STS(13)s cannot have normal subsystem, or equivalently, the corresponding Steiner loops are simple.

A class of subsystems which are always normal is that of *projective hyperplanes*.

Definition 2.1.5. A proper subsystem $\mathcal{N}$ of $\mathcal{S}$ is called a *projective hyperplane* if every triple of $\mathcal{S}$ has a non empty intersection with $\mathcal{N}$.

Equivalently, a subsystem $\mathcal{N}$ of an STS(v) is a projective hyperplane if and only if $|\mathcal{N}| = \frac{v-1}{2}$. In fact, each of the $\frac{v-1}{2}$ blocks through a point x outside $\mathcal{N}$ must have exactly one point in common with $\mathcal{N}$. By cardinality reasons, projective hyperplanes correspond exactly to subloops of index 2, which are always normal. Therefore, we can say that If $\mathcal{L}_{\mathcal{S}}$ is a simple loop, then $\mathcal{S}$ does not contain any projective hyperplane.

On the other hand, when raise the index to 4, a subloop of $\mathcal{L}_{\mathcal{S}}$ is not necessarily normal.

Example 2.1.5.1. Let $\mathcal{S}$ be the STS(15) with the set of points $\{0, 1, \ldots, 9, a, \ldots, e\}$ and the triples given by the columns of the following table.

0	0	0	0	0	0	0	1	1	1	1	1	1	2	2	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5	6	6	6	6
1	3	5	7	9	b	d	3	4	7	8	b	c	3	4	7	8	9	a	7	8	9	a	7	8	9	c	7	8	a	b	7	8	9	a
2	4	6	8	a	c	e	5	6	9	a	d	e	6	5	b	c	d	e	e	d	c	b	a	b	e	d	d	9	c	e	c	e	b	d

In the classification of the 80 non-isomorphic Steiner triple systems of order 15 in [19], pp. 31-33, it is presented as #2. $\mathcal{S}$ contains the sub-STS(7) given by the the following Figure 2.2,

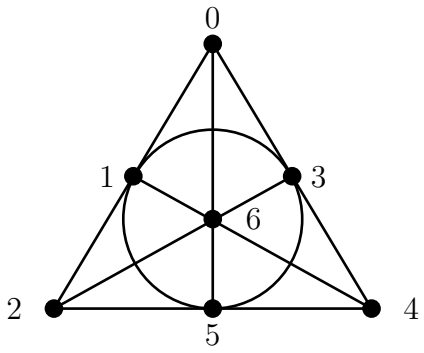

FIGURE 2.2: Sub-STS(7)

which is a projective hyperplane, hence normal. On the other hand, any triple $\mathcal{N}$ of $\mathcal{S}$ gives a subloop $\mathcal{L}_{\mathcal{N}} < \mathcal{L}_{\mathcal{S}}$ of index 4. Let $\mathcal{N}$ be, for instance, the triple $\{3, 9, c\}$. Normality requires that for any $x, y \in \mathcal{L}_{\mathcal{S}}$ and any $n_1 \in \mathcal{L}_{\mathcal{N}}$, $x(yn_1) = (xy)n_2$ for some $n_2 \in \mathcal{L}_{\mathcal{N}}$. If we choose $x = 5$, $y = 7$, $n_1 = 3$, then

$$x(yn_1) = 5(7 \cdot 3) = 5 \cdot e = b,$$

but the equation $(5 \cdot 7)n_2 = b$, being equivalent to $d \cdot n_2 = b$, leads to $n_2 = 1$, that is not an element of $\mathcal{L}_{\mathcal{N}}$.

We want to describe normality of subloops with a combinatorial prospective, especially in small cases. Before going into this, it is important to recall that in Steiner loops of projective type the nuclei and the center coincide, since they are totally symmetric. On the one hand, the center $\mathcal{Z}$ of a Steiner loop $\mathcal{L}_{\mathcal{S}}$ has order 2^t, for some non-negative integer t, since it is an elementary abelian 2-group. On the other hand, being $\mathcal{Z}$ a normal subloop, its order must divide that

of $\mathcal{L}_\mathcal{S}$. Thus, when its center is not trivial, $\mathcal{L}_\mathcal{S}$ has an admissible factorization $v+1 = 2^t(w+1)$ with $t \geq 1$.

Now we give the definition of particular configurations of points and lines in Steiner triple systems, giving us the instruments to describe normality of subloops and later to prove the power of loops in the study of STSs.

Definition 2.1.6. Let $\{x, a, b\}$, $\{x, c, d\}$, $\{y, a, c\}$, $\{y, b, d\}$ be a configuration of four distinct triples of a Steiner triple system $\mathcal{S}$.

(i) If $z = y$, then the configuration is called a *Pasch configuration* (or C_{16}).

(ii) If $z \neq y$, then the configuration is called an *anti-Pasch configuration* (or C_{14}).

A visual representation of a Pasch and an anti-Pasch configurations is given the following Figure 2.3.

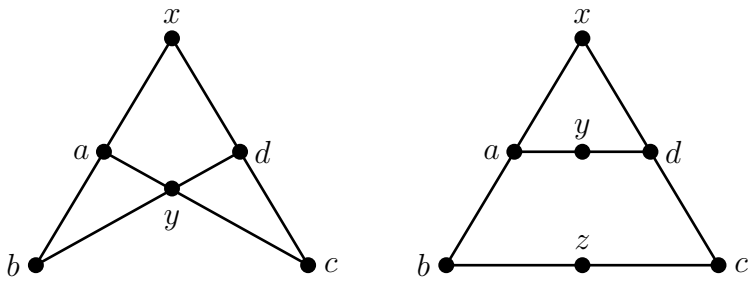

FIGURE 2.3: A Pasch (left) and an anti-Pasch (right) configurations

Definition 2.1.7. [20, p. 147] A point x in a Steiner triple system $\mathcal{S}$ is a *Veblen point* if whenever $\{x, a, b\}$, $\{x, c, d\}$, $\{y, a, c\}$ are triples of $\mathcal{S}$, also $\{y, b, d\}$ is a triple of $\mathcal{S}$.

Definition 2.1.7 says that any two distinct triples through a Veblen point x produce a Pasch configuration. Equivalently we can say that x is a Veblen point if and only if any two different triples containing x generate an STS(7). Indeed, if in a Pasch configuration there is a Veblen point, it generates a Fano plane, but in general this is not true. A result concerning this topic deals with Steiner loops satisfying *Moufang's theorem*. It is known that a Steiner loops is a Moufang loop if and only if it is associative. However, some non-associative Steiner loops can satisfy Moufang's theorem, that is, every three associating elements generate a group. In [18], the authors proved that a Steiner loop $\mathcal{L}_\mathcal{S}$ satisfies Moufang's theorem if and only if every Pasch configuration in $\mathcal{S}$ generates a sub-STS(7).

Veblen points give a characterization of projective Steiner triple systems, which was presented in its original form as part of the *Veblen-Young axioms* for projective spaces (see [94]). However, the version we give here was presented by C.J. Colbourn and A. Rosa.

Theorem 2.1.8. *[20, Th. 8.15] Let $\mathcal{S}$ be a Steiner triple system of order v, and suppose that $2^n \leq v < 2^{n+1}$. The system $\mathcal{S}$ is isomorphic to $\mathrm{PG}(n+1,2)$, and $v = 2^{n+1} - 1$, if and only if every element of $\mathcal{S}$ is a Veblen point.*

The previous Theorem 2.1.8 will be sensibly improved by Corollary 2.5.4, but first we need to show some results about normality and Veblen points. The next theorem characterizes explicitly normal subsystems consisting of a singleton, and gives also an algebraic meaning to Veblen points in the contest of Steiner loops.

Theorem 2.1.9. *Let $\mathcal{S}$ be a Steiner triple system. The following are equivalent.*

*(i) The sub-*STS(1) *$\mathcal{N} = \{x\}$ is a normal subsystem of $\mathcal{S}$;*

(ii) x is a Veblen point of $\mathcal{S}$;

(iii) x is a non-trivial central element of $\mathcal{L}_{\mathcal{S}}$.

Proof. Let $\mathcal{N} = \{x\}$ be a normal subsystem of $\mathcal{S}$. The normality condition of the corresponding Steiner subloop $\mathcal{L}_{\mathcal{N}}$, that is

$$a \cdot b\mathcal{L}_{\mathcal{N}} = ab \cdot \mathcal{L}_{\mathcal{N}} \quad \text{for all } a, b \in \mathcal{L}_{\mathcal{S}},$$

is equivalent, in this case, to

$$a \cdot bx = ab \cdot x \quad \text{or all } a, b \in \mathcal{L}_{\mathcal{S}}.$$

Hence, (i) and (iii) are equivalent.

Let now x be a Veblen point of $\mathcal{L}_{\mathcal{S}}$. Consider two triples $\{x, a, ax\}$ and $\{x, b, bx\}$. Since $\{a, bx, a \cdot bx\}$ is a triple, then $\{ax, b, a \cdot bx\}$ is a triple as well, which means that $ax \cdot b = a \cdot xb$. The next figure 2.4 helps in visualizing the situation.

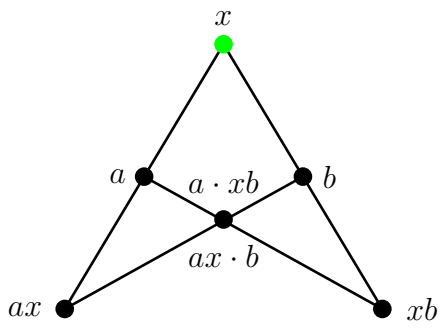

FIGURE 2.4: Centrality of a Veblen point

This proves the equivalence between (ii) and (iii). □

The following result is an immediate consequence of Theorem 2.1.9, more precisely it follows from the fact that the set of Veblen points of a Steiner triple system is precisely the set of non-trivial central elements of the associated Steiner loop.

Corollary 2.1.10. *The Veblen points of a Steiner triple system of order v form a normal subsystem of order $2^{n+1}-1 \leq v$, isomorphic to* $\mathrm{PG}(n,2)$.

We want to describe in combinatorial terms also normality of subsystems of order three.

Theorem 2.1.11. *Let $\mathcal{S}$ be a Steiner triple system. If a triple is normal, then any outer point generates with it a Fano plane.*

Proof. Let $\mathcal{N} = \{x, y, xy\}$ be a normal triple of $\mathcal{S}$ and a an outer point. From the normality condition, we know that the solutions n_1, n_2, n_3 of the equations

$$a(xy) = (ax)n_1, \quad a(yx) = (ay)n_2, \quad (xa)(ya) = xn_3,$$

belong to $\mathcal{L}_{\mathcal{N}}$. It is easy to check that the only possibilities which do not lead to any contradiction are $n_1 = y$, $n_2 = x$ and $n_3 = y$, giving the identities

$$a(xy) = (ax)y, \quad a(yx) = (ay)x, \quad (xa)(ya) = xy.$$

This means that $\mathcal{N}$ and a generate a Fano plane, as shown in figure 2.5.

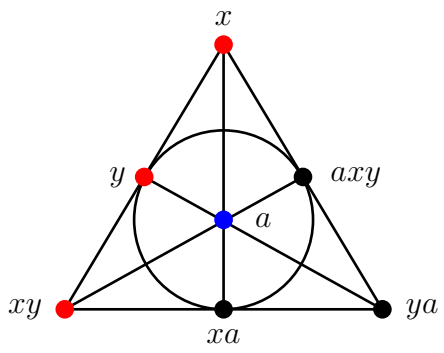

FIGURE 2.5: Fano plane generated by a normal triple and an outer point

□

Using the characterization of Veblen points in Theorem 2.1.9, we can give a necessary condition on the existence of Steiner triple systems with such points.

Proposition 2.1.12. *If $v+1 = 2^t(w+1)$ is an admissible factorization only for $t = 0$, then any* $\mathrm{STS}(v)$ *contains no Veblen points.*

Proof. The claim follows from the fact that, if the center has cardinality 2^c, then $\frac{v+1}{2^c}$ must be the order of the quotient Steiner loop. □

After the definition of Schreier extension, in Section 2.5, we will be able to give a necessary and sufficient condition on the existence of Steiner triple systems of order v with (at least) $2^c - 1$ Veblen points, and we will present a constructive method for obtaining all such STSs .

Now we prove a more general fact about Veblen points, Pasch configurations and Fano planes which can be useful in the classification of Steiner triple systems with Veblen points.

Lemma 2.1.13. *If $\mathcal{S}$ is a* STS(v)*, then:*

(i) The number of Pasch configurations through a fixed Veblen point is $\frac{(v-1)(v-3)}{4}$.

(ii) The number of Fano planes containing a fixed Veblen point is $\frac{(v-1)(v-3)}{24}$.

(iii) If $\mathcal{S}$ has two distinct Veblen points a, b, then the third point $c = ab$ in their triple is a Veblen point as well. Moreover, there are $\frac{v-3}{4}$ *Fano planes containing the line $\ell = \{a, b, ab\}$.*

Proof. If a is a Veblen point, then for all points $b \in$ STS(v), $a \neq b$, there are $\frac{v-3}{4}$ Pasch configurations through b and a which do not contain the block $\{a, b, ab\}$.

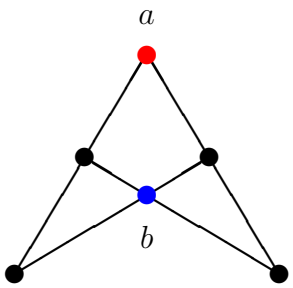

FIGURE 2.6: Pasch configuration containing two a and b but not their triple

This follows from the fact that we cannot choose ab to be in the Pasch configuration, so we are left with $v - 3$ points of the STS(v). In a Pasch configuration there are 4 further points different from a and b. Fixing one of these 4 points, the others are uniquely determined: indeed, if we fix x to be in the configuration, the other must necessarily be ax, bx and $a(bx) = (ax)b$, and rearranging these four points we obtain the same configuration. Finally, since the point b can be chosen in $v - 1$ different ways we obtain the first assertion.

The second assertion follows from the fact that any sub-Fano plane containing the Veblen point x is obtained by 6 Pasch configurations, as shown in figure 2.7.

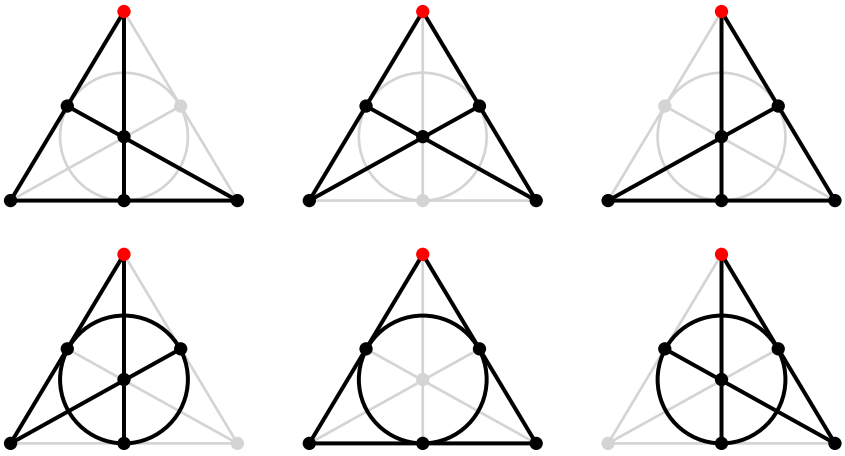

FIGURE 2.7: The six Pasch configurations through x forming a Fano plane

We notice here that the number $\frac{(v-1)(v-3)}{24}$ is in fact an integer. Indeed, v can be $1, 3, 7, 9 \mod 12$: if $v \equiv 1, 3 \mod 12$, one between $v-1$ and $v-3$ is divisible by 12 and the other is even; if $v \equiv 7, 9 \mod 12$, one between $v-1$ and $v-3$ is divisible by 4 and the other by 6.

Fixed the Veblen line $\ell = \{a, b, ab\}$, let x be a point of $\mathcal{S}$ not in ℓ. Since ℓ is a Veblen line, together with x it generates the Fano plane. We can choose x in $v-3$ different ways, but replacing it with ax, bx or with $(ab)x = b(ax) = a(bx)$ we obtain the same Fano plane. Hence there are $\frac{v-3}{4}$ different Fano planes containing the Veblen line $\ell = \{a, b, ab\}$.

□

Remark 2.1.1. These results can simplify the counting of Veblen point in a Steiner triple system. To illustrate this, we consider Steiner triple systems of order 15. We use the classification of the 80 non-isomorphic STS(15)s and their main properties listed in [19, Tables 1.28 and 1.29, pp. 30 - 32]

If $\mathcal{S}$ is an STS(15) with a Veblen point, then it contains at least 7 Fano planes. The only STS(15)s with that many sub-Fano planes are #1 and #2. If $\mathcal{S}$ has more than one Veblen point, then it contains at least one triple $\{a, b, ab\}$ of Veblen points. For each of these Veblen points, there are 7 Fano planes passing through it, 3 of which contain the entire line $\{a, b, ab\}$. Thus, $\mathcal{S}$ contains at least $3(7-3)+3 = 15$ Fano planes. The only STS(15) with this many sub-Fano planes is #1, that is, PG(3, 2), therefore all of its element are Veblen points. Moreover, the STS(15)#2 has precisely one Veblen point, and it is easy to see that it is the element labeled with 0, by checking that it is a central element of the Steiner loop.

2.2 Steiner loops of affine type

aaaa

Definition 2.2.1. Consider a Steiner triple system $\mathcal{S}$, and let Ω be a fixed element of $\mathcal{S}$. We define $\mathcal{A}_\mathcal{S}$ as the set $\mathcal{S}$ endowed with the binary operation $+$ defined as follows:

- for any element $x \neq \Omega$, the opposite $-x$ is the third point in the triple through x and Ω, and we set $-\Omega = \Omega$;
- for any element x, $\Omega + x = x + \Omega = x$ and $x + x = -x$;
- for any distinct x and y in $\mathcal{S} \setminus \{\Omega\}$, $x + y = -z$ whenever $\{x, y, z\}$ is a triple of $\mathcal{S}$.

$\mathcal{A}_\mathcal{S} = (\mathcal{S}, +)$ is called called *Steiner loop of affine type.*

Clearly, with the above commutative operation, the unique solution of the equation $a + x = b$ is the third point in the triple through a and $-b$. Also, Ω is the identity element of $\mathcal{A}_\mathcal{S}$, hence $\mathcal{A}_\mathcal{S}$ is indeed a loop. Moreover, Steiner loops of affine type have exponent 3 and fulfill the weak inverse property. Indeed, the triples $\{x, y, z\}$ of $\mathcal{S}$ are characterized by the relation

$$x + y + z = \Omega,$$

and, as in the projective case, we note here that the elements in each triple associate. Two Steiner loops of affine type associated with the same Steiner triple system $\mathcal{S}$, say $\mathcal{A}_\mathcal{S}$ and $\mathcal{A}'_\mathcal{S}$, with different identity elements Ω and Ω' respectively, are isotopic but not isomorphic in general. Indeed, let μ and ν be the maps defining the inverse elements in $\mathcal{A}_\mathcal{S}$ and $\mathcal{A}'_\mathcal{S}$ respectively, that is, $\mu(x)$ and $\nu(x)$ define the triples $\{x, \Omega, \mu(x)\}$ and $\{x, \Omega', \nu(x)\}$. Then the map $\gamma = \nu\mu \colon \mathcal{A}_\mathcal{S} \to \mathcal{A}'_\mathcal{S}$ induces an isotopism $(\mathrm{id}, \mathrm{id}, \gamma) \colon \mathcal{A}_\mathcal{S} \to \mathcal{A}'_\mathcal{S}$.

Similarly to the projective case, a Steiner loop of affine type $\mathcal{A}_\mathcal{S}$ turns out to be a group, specifically an elementary abelian 3-group, exactly when $\mathcal{S}$ is affine Steiner triple system. Moreover, $\mathcal{S}$ is a Hall triple system whenever $\mathcal{A}_\mathcal{S}$ is a Moufang loop, more precisely a commutative Moufang loop of exponent 3, a class of loops usually denoted with 3-CML. Since isotopic commutative loops are isomorphic (see [8]), any two Steiner loops of affine type associated with the same Hall triple system $\mathcal{S}$ with different identities are actually isomorphic.

Proposition 2.2.2. *Let $\mathcal{A}_\mathcal{S}$ and $\mathcal{A}'_\mathcal{S}$ be two Steiner loops of affine type defined on the same Steiner triple system $\mathcal{S}$ with different identities Ω and Ω', respectively. $\mathcal{A}_\mathcal{S}$ and $\mathcal{A}'_\mathcal{S}$ are isomorphic if and only if there exists $\varphi \in \mathrm{Aut}(\mathcal{S})$ such that $\varphi(\Omega) = \Omega'$.*

Proof. If $\varphi \colon \mathcal{A}_\mathcal{S} \longrightarrow \mathcal{A}'_\mathcal{S}$ is an isomorphism, then naturally $\varphi(\Omega) = \Omega'$. The triples of $\mathcal{S}$ are characterized by the condition

$$x + y + z = \Omega, \tag{2.3}$$

where $+$ is the operation in $\mathcal{A}_\mathcal{S}$. Applying φ to equation (2.3), we obtain

$$\varphi(x) \oplus \varphi(y) \oplus \varphi(z) = \Omega', \tag{2.4}$$

where $\oplus$ is the operation in $\mathcal{A}'_\mathcal{S}$. Thus $\{\varphi(x), \varphi(y), \varphi(z)\}$ is still a triple of $\mathcal{S}$ and φ is an automorphism of $\mathcal{S}$.

Conversely, let φ be an automorphism of $\mathcal{S}$ mapping Ω into Ω'. The triples

$$\{x, y, -(x+y)\} \quad \text{and} \quad \{-(x+y), \Omega, x+y\} \tag{2.5}$$

are mapped by φ into the triples

$$\{\varphi(x), \varphi(y), \varphi(-(x+y))\} \quad \text{and} \quad \{\varphi(-(x+y)), \Omega', \varphi(x+y)\}, \tag{2.6}$$

respectively. Hence $\varphi(x+y) = \varphi(x) \oplus \varphi(y)$, that is, φ is an isomorphism of loops $\mathcal{A}_\mathcal{S} \longrightarrow \mathcal{A}'_\mathcal{S}$. □

As a direct consequence of Proposition 2.2.2, we have the following characterization for Steiner triple systems defining an isomophism class of Steiner loops of affine type.

Corollary 2.2.3. *A Steiner triple system $\mathcal{S}$ has the property that any two Steiner loops of affine type defined on $\mathcal{S}$ are isomorphic if and only if the group $\mathrm{Aut}(\mathcal{S})$ acts transitively on $\mathcal{S}$.*

Corollary 2.2.3 indicates that not only does any HTS (and consequently any affine STS) define an isomorphism class of Steiner loops of affine type, but also any projective STS has the same property, due to its transitive automorphism group. Additionally, it is worth noting a correction to a small mistake in [33]. On page 148, the authors present an example of two Steiner loops of affine type defined on the STS(7), saying that they are isotopic but not isomorphic. However, this assertion is not true as they are, in fact, isomorphic by Corollary 2.2.3.

Since the two STS(13)s have transitive automorphism groups, for the smallest example of two isotopic but non isomorphic Steiner loops of affine type defined on the same STS(v) one has to consider $v = 15$. For instance, the STS(15) #2 $\mathcal{S}$ has a unique Veblen point, which is fixed by any automorphism of $\mathcal{S}$ since it is the only non-trivial central point in the Steiner loop of projective type $\mathcal{L}_{\mathcal{S}}$. For this reason the Steiner loop of affine type $\mathcal{A}_{\mathcal{S}}$ with identity the Veblen point is isotopic, but not isomorphic, to any other loop $\mathcal{A}'_{\mathcal{S}}$ with a different identity element. Furthermore, since the STS(15) #23 have trivial automorphism group (see [19]), it gives 15 non-isomorphic Steiner loops of affine type.

For Steiner loops of affine type, unlike the projective case, the subloops of $\mathcal{A}_{\mathcal{S}}$ are exactly the subsystems of $\mathcal{S}$ containing Ω. If $\mathcal{A}_{\mathcal{S}}$ has a normal subloop, then each coset corresponds to a subsystem of $\mathcal{S}$, and the corresponding quotient yields a Steiner triple system as well. While in the projective case the groups $\mathrm{Aut}(\mathcal{L}_{\mathcal{S}})$ and $\mathrm{Aut}(\mathcal{S})$ coincides, in this case the automorphisms of the loop $\mathcal{A}_{\mathcal{S}}$ are the automorphism of the Steiner triple system $\mathcal{S}$ fixing the element Ω.

Another difference between Steiner loops of affine and projective type concerns the normality of maximal subloops. While in a Steiner loop of projective type every maximal subloop, that is of index 2, is normal, this is not true in the affine case. In this context, maximal means of index 3. Now we give an example arising from an STS(21) called B.3 in [63].

Example 2.2.3.1. Let $\mathcal{S}$ be an STS(21) given by the set of points $\mathbb{Z}/7\mathbb{Z} \times \{1,2,3\}$. For an easier notation, in [63], the authors denote with x_i the couple $(x,i) \in \mathbb{Z}/7\mathbb{Z} \times \{1,2,3\}$. Let the family of triples of $\mathcal{S}$ be generated by the following base blocks,

$$\begin{array}{lllll} \{0_1,1_1,3_1\}, & \{0_1,0_2,0_3\}, & \{0_1,1_2,2_3\}, & \{0_1,2_2,5_3\}, & \{0_1,3_2,6_2\}, \\ \{0_1,4_2,5_2\}, & \{0_1,1_3,6_3\}, & \{0_1,3_3,4_3\}, & \{0_2,2_2,6_3\}, & \{0_2,2_3,5_3\}, \end{array}$$

together with the automorphism

$$\alpha = (0_1,1_1,\ldots,6_1)(0_2,1_2,\ldots,6_2)(0_3,1_3,\ldots,6_3) \tag{2.7}$$

Let us fix $\Omega := 0_1$ as the identity element of the Steiner loop of affine type $\mathcal{A}_{\mathcal{S}}$. The subset $\mathcal{N} := \mathbb{Z}/7\mathbb{Z} \times \{1\}$ is the unique sub-STS(7) of $\mathcal{S}$ and it contains Ω, thus $\mathcal{A}_{\mathcal{N}}$ is a subloop of $\mathcal{A}_{\mathcal{S}}$ of index 3.

The normality condition requires that for every $x_i, y_j \in \mathcal{A}_{\mathcal{S}}$, $n_1 \in \mathcal{A}_{\mathcal{N}}$, there exists an element $m_1 \in \mathcal{A}_{\mathcal{N}}$ such that

$$x_i + (y_j + n_1) = (x_i + y_j) + m_1.$$

If we choose $x_i = 2_2$ and $y_j = -x_i = 5_3$ we have that the normality condition requires that $2_2 + (5_3 + n_1) \in \mathcal{A}_\mathcal{N}$ for every $n_1 \in \mathcal{A}_\mathcal{N}$. Choosing $n_1 = 2_1$ we have that

$$2_2 + (5_3 + n_1) = 2_2 + (5_3 + 2_1) = 2_2 + (-6_3) = 2_2 + 1_3 = -4_2 = 5_2 \notin \mathcal{A}_\mathcal{N}.$$

It follows that $\mathcal{A}_\mathcal{N}$ is not a normal subloop of $\mathcal{A}_\mathcal{S}$.

2.3 Some applications of Steiner loops

In this section, through the following examples, we intend to support the assertion regarding the effectiveness of loop theory in the study of Steiner triple systems.

We give now a first evidence of the strength of using Steiner loops. A $t-(v,k,\lambda)$ design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is said *additive* if it is possible to embed $\mathcal{P}$ into a suitable (commutative) group $(\mathcal{G}_\mathcal{D}, +)$ such that the sum of the elements in each block is zero. Additivity of block designs has been studied by A. Caggegi, G. Falcone and M. Pavone in [13]. They show that, with only one exception, any symmetric $2-(v,k,\lambda)$ design is additive, and its blocks are the only k-subsets in which the elements sum up to zero. Furthermore, they proved that the automorphism group of $\mathcal{D}$ is the subgroup of $\mathrm{Aut}(\mathcal{G}_\mathcal{D})$ which leaves $\mathcal{P}$ invariant. A special case is when $\mathcal{D}$ has prime order p which do not divide k: in this situation the group $\mathcal{G}_\mathcal{D}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\frac{v-1}{2}}$. Moreover, they proved that the only additive Steiner triple systems are the projective and affine STSs. We report in passing that M. Buratti and A. Nakić in [12] studied *super-regular* design, that are additive designs $\mathcal{D}$ such that their point-set is exactly $\mathcal{G}_\mathcal{D}$, and any translate of any block is still a block. Their main result says that there are infinitely many values of v for which there exists a super-regular $2-(v,k,1)$ design whenever k is neither singly even nor of the form $2^n 3 \geq 12$. They also find super-regular $2-(p^n,p,1)$ designs different from $\mathrm{AG}(n,p)$, for $p = 5, 7$.

The proof in [13] of affine and projective geometries being the only additive STSs takes several pages, but using Steiner loops it can be sensibly improved. In fact, if we want to define a binary operation $+$ on a Steiner triple system $\mathcal{S}$ such that $x+y+z=0$ for each block $\{x,y,z\}$ of $\mathcal{S}$, then the construction gives in turn a Steiner loop of either affine or projective type. Indeed, if the identity 0 is an element of $\mathcal{S}$, then this construction corresponds exactly to the Steiner loop of affine type. This loop is associative precisely when $\mathcal{S}$ is the point-line design of an affine geometry $\mathrm{AG}(d,3)$. If 0 is not an element of $\mathcal{S}$, since the triples must be the only 3-subsets of the group that sum up to 0, we have that every element has order 2. Hence, this construction coincides with the Steiner loop of projective type, which is associative precisely when $\mathcal{S}$ is the point-line design of a projective geometry $\mathrm{PG}(d,2)$.

Now we provide another example which proves again the strength of Steiner loops of both types. It is very well known that if any set of three non-collinear points always determines a Pasch configuration, then the Steiner triple system

is a projective geometry over GF(2). Conversely, the same property can be formulated in terms of lack of the anti-Pasch configuration C_{14}.

Trying to find a corresponding characterization for affine geometries AG$(d, 3)$, M. Hall ended up discovering Hall triple systems (HTS), a family of STSs that contains properly the affine geometries over GF(3). For HTSs, in fact, any three points belong to an affine plane AG$(2, 3)$. As shown by M. Pavone in [78], the corresponding characterization for Steiner triple systems as affine geometries over GF(3) is that any *four* points belong to an AG$(3, 3)$, simply because the associated Steiner loop of affine type fulfills, for any three points (together with the zero element) the associative law, hence being a group. In the same lecture, he noticed that if the Steiner loop of affine type is not a group (equivalently, the associated Steiner triple system is not an affine space AG$(d, 3)$), then three non associating elements form, together with the element Ω, a C_S^1 configuration (instead of a grid), as displayed in the next Figure 2.8,

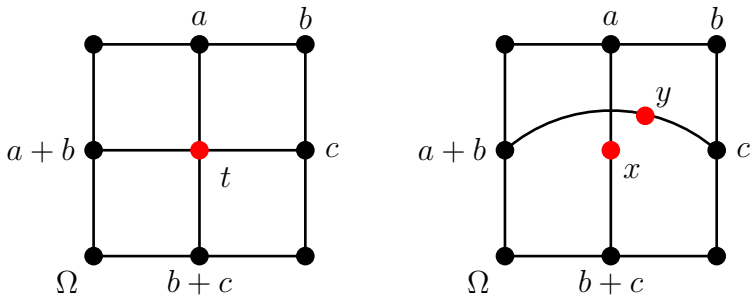

FIGURE 2.8: A grid (left) and a C_S^1 configuration (right)

where $-t = (a + b) + c = a + (b + c)$, $-x = a + (b + c)$, $-y = (a + b) + c$. This insight allowed him to strengthen a result by Kral et alii in [60] characterizing affine spaces over the field GF(3). Their results say that a Steiner triple system is affine if and only if it contains neither of the configurations C_{16} (Pasch), C_S^1 and C_S^2 (see Figure 2.9), and that a Hall triple systems is affine if and only if it contains none of the configurations C_S^1 and C_S^2. Whereas, M. Pavone was able to strengthen the previous results by removing the hypothesis on the C_S^2 configuration. Indeed, he proved that the affine geometries over GF(3) are exactly the Steiner triple systems where the configurations C_{16} and C_S^1 are missing, as well as the Hall triple systems where the configuration C_S^1 is missing.

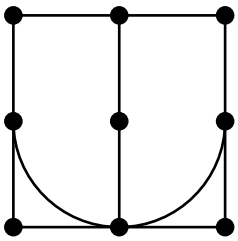

FIGURE 2.9: A C_S^2 configuration

2.4 Extensions of Steiner loops

The theory of group extensions has a rich history in group theory, and it played a crucial role in various areas of mathematics from its early development in the 20th century. The concept involves understanding how groups can be constructed by *extending* one group by another. While the theory of group extensions is a milestone in algebra, a general extension theory for loops does not exist. Indeed, the lack of associativity changes the situation very drastically.

In this section we want to study extensions of Steiner loops of projective type. As one can expect by considering that the number of Steiner triple systems with v elements increases as $\big(v/e^2+o(v)\big)^{v^2/6}$ (see [53]), this construction is more flexible than the corresponding extension theory for commutative groups (cf. [2] and [10], [73]).

It is worthwhile here to recall the next theorem, which follows from [1], § 10 and 11, and which links the extension theory for loop with the extension theory for the corresponding multiplication groups.

Theorem 2.4.1. *Let $\mathcal{L}_\mathcal{S}$ be an extension of $\mathcal{L}_\mathcal{N}$ by $\mathcal{L}_\mathcal{Q}$. Then* $\mathrm{Mult}(\mathcal{L}_\mathcal{N})$ *is a normal subgroup of* $\mathrm{Mult}(\mathcal{L}_\mathcal{S})$ *and* $\mathrm{Mult}(\mathcal{L}_\mathcal{Q})$ *is isomorphic to* $\mathrm{Mult}(\mathcal{L}_\mathcal{S})/\mathrm{Mult}(\mathcal{L}_\mathcal{N})$.

2.4.1 Steiner operators

The most general way of constructing an extension of Steiner triple System is via a *Steiner operator*. It allows us to construct, starting from a $\mathrm{STS}(u)$ and $\mathrm{STS}(w)$ a further Steiner triple system of order $(u+1)(w+1)-1$, with one of them as normal subsystem and the the other one as the corresponding quotient. Eventually, our focus we will be on d *Schreier extensions*, a specific kind of extensions which provides a powerful tool for constructing and classifying Steiner triple systems that contain Veblen points. However, before delving into the details of these extensions, we present the general case.

Definition 2.4.2. Let $\mathcal{L}_\mathcal{N}$ and $\mathcal{L}_\mathcal{Q}$ be Steiner loops of order $n = u+1$ and $m = w+1$ with identity elements Ω' and $\bar{\Omega}$ respectively, and let $\mathrm{LS}(\mathcal{L}_\mathcal{N})$ be the set of $n \times n$ Latin squares with entries in the set $\mathcal{L}_\mathcal{N}$.

An operator $\Phi : \mathcal{L}_\mathcal{Q} \times \mathcal{L}_\mathcal{Q} \longrightarrow \mathrm{LS}(\mathcal{L}_\mathcal{N})$, which maps the couple (P,Q) into a Latin square $\Phi_{P,Q} : \mathcal{L}_\mathcal{N} \times \mathcal{L}_\mathcal{N} \longrightarrow \mathcal{L}_\mathcal{N}$, is called a *Steiner operator (of projective type)* if it fulfills the following conditions:

(i) the Latin square $\Phi_{\bar{\Omega},\bar{\Omega}}$ is the (symmetric) multiplication table of $\mathcal{L}_\mathcal{N}$;

(ii) $\Phi_{Q,P}(y,x) = \Phi_{P,Q}(x,y)$, that is, $\Phi_{Q,P}$ is the transpose of $\Phi_{P,Q}$;

(iii) $\Phi_{P,P}(x,x) = \Omega'$;

(iv) $\Phi_{P,PQ}(x, \Phi_{P,Q}(x,y)) = y$

for all $(P,x),(Q,y) \in \mathcal{L}_\mathcal{Q} \times \mathcal{L}_\mathcal{N}$.

Steiner operators can also be defined in the context of Steiner loops of affine type, they have been studied in [33].

We note here that with $P = Q$ and $x = y$, conditions iii) and iv) lead to

$$\Phi_{P,\bar{\Omega}}(x, \Omega') = x. \tag{2.8}$$

Theorem 2.4.3. *Let $\mathcal{L}_\mathcal{N}$ and $\mathcal{L}_\mathcal{Q}$ be two Steiner loops of order $u+1$, $w+1$ and with identities Ω' and $\bar{\Omega}$, respectively. Let $\Phi : \mathcal{L}_\mathcal{Q} \times \mathcal{L}_\mathcal{Q} \longrightarrow \mathrm{LS}(\mathcal{L}_\mathcal{N})$ be a Steiner operator. If we define on the set $\mathcal{L}_\mathcal{Q} \times \mathcal{L}_\mathcal{N}$ the following operation,*

$$(P, x) \circ (Q, y) := \big(PQ, \Phi_{P,Q}(x, y)\big), \tag{2.9}$$

we obtain a Steiner loop $\mathcal{L}_\mathcal{S}$ of order $v+1 = (u+1)(w+1)$ with identity $\Omega = (\bar{\Omega}, \Omega')$. The subloop

$$\overline{\mathcal{L}_\mathcal{N}} = \{(\bar{\Omega}, x) \mid x \in \mathcal{L}_\mathcal{N}\}$$

is a normal subloop of $\mathcal{L}_\mathcal{S}$ isomorphic to $\mathcal{L}_\mathcal{N}$, with corresponding quotient $\mathcal{L}_S/\overline{\mathcal{L}_\mathcal{N}}$ isomorphic to $\mathcal{L}_\mathcal{Q}$.

Conversely, any Steiner loop with a proper normal subloop is isomorphic to the construction described above, for a suitable Steiner operator.

Proof. Let $\mathcal{L}_\mathcal{S}$ be defined by a Steiner operator Φ as above. If (Q, y) and (R, z) are two given elements in $\mathcal{L}_\mathcal{S}$, then the equation

$$(Q, y) \circ (P, x) = (R, z)$$

has a unique solution (P, x), where $P = QR$ and x is the unique element in $\mathcal{L}_\mathcal{N}$ such that $\Phi_{Q,QR}(y, x) = z$, that is, the column index of the element z in row y in the Latin square $\Phi_{Q,QR}$.
By (2.8), the element $(\bar{\Omega}, \Omega')$ is the identity of $\mathcal{L}_\mathcal{S}$. By Definition 2.4.2, condition ii), the operation is commutative, by condition iii) $\mathcal{L}_\mathcal{S}$ has exponent 2 and condition iv) is equivalent to $(P, x) \circ \big((P, x) \circ (Q, y)\big) = (Q, y)$, that is the totally symmetric property. Thus, $\mathcal{L}_\mathcal{S}$ is a Steiner loop. By Definition 2.4.2, condition i), the subloop

$$\overline{\mathcal{L}_\mathcal{N}} = \{(\bar{\Omega}, x) \mid x \in \mathcal{L}_\mathcal{N}\}$$

is isomorphic to $\mathcal{L}_\mathcal{N}$. For every $(Q, y), (R, z) \in \mathcal{L}_\mathcal{S}$, $(\bar{\Omega}, n) \in \mathcal{L}_\mathcal{N}$ the equation

$$\left((Q, y)\,(R, z)\right) \circ \big(\bar{\Omega}, n\big) = (Q, y) \circ \left((R, z)\,(P, x)\right), \tag{2.10}$$

that is,

$$\left(QR, \Phi_{Q,R}\,(y, z)\right) \circ \big(\bar{\Omega}, n\big) = (Q, y) \circ \left(RP, \Phi_{R,P}\,(z, x)\right),$$

is equivalent to

$$\big(QR, \Phi_{QR,\bar{\Omega}}\left(\Phi_{Q,R}\,(y, z)\,, n\right)\big) = \left(Q \cdot RP, \Phi_{Q,RP}\left(y, \Phi_{R,P}\,(z, x)\right)\right). \tag{2.11}$$

The equation (2.11) implies $P = \bar{\Omega}$, that is, the solution (P, x) of the equation (2.10) belongs to $\mathcal{L}_\mathcal{N}$ which, as a consequence, is normal.

Conversely, consider a Steiner loop $\mathcal{L}_\mathcal{S}$ with a normal subloop $\mathcal{L}_\mathcal{N}$ and corresponding quotient loop $\mathcal{L}_\mathcal{Q}$. Let $\pi\colon \mathcal{L}_\mathcal{S} \longrightarrow \mathcal{L}_\mathcal{Q}$ be the canonical epimorphism and $\sigma\colon \mathcal{L}_\mathcal{Q} \longrightarrow \mathcal{L}_\mathcal{S}$ a section with $\sigma(\mathcal{L}_\mathcal{N}) = \Omega$ and $\pi\sigma = \mathrm{id}_{\mathcal{L}_\mathcal{Q}}$. Since for every $\pi(X) \in \mathcal{L}_\mathcal{Q}$ it holds $\pi(X) = \pi(\sigma(\pi(X)))$, we have that

$$X = \sigma(\pi(X)) \cdot x, \tag{2.12}$$

with $x \in \mathcal{L}_\mathcal{N}$. By normality of $\mathcal{L}_\mathcal{N}$ and using the fact that $\sigma(\pi(X))\sigma(\pi(Y))$ and $\sigma(\pi(X)\pi(Y))$ are in the same coset, we obtain that

$$XY = (\sigma(\pi(X)) \cdot x)\,(\sigma(\pi(Y)) \cdot y) = (\sigma(\pi(X)\pi(Y))) \cdot \Phi_{\pi(X),\pi(Y)}(x, y)$$

for a suitable element $\Phi_{\pi(X),\pi(Y)}(x, y)$ of $\mathcal{L}_\mathcal{N}$ depending on $\pi(X)$, $\pi(Y)$, x and y. Since $\mathcal{L}_\mathcal{S}$ is a loop, for any $\pi(X), \pi(Y) \in \mathcal{L}_\mathcal{Q}$, $\Phi_{\pi(X),\pi(Y)}(-,-)$ defines a Latin square with entries in $\mathcal{L}_\mathcal{N}$ and rows and columns indexed by $\mathcal{L}_\mathcal{N}$ as well. Thus, we can define an operator $\Phi\colon \mathcal{L}_\mathcal{Q} \times \mathcal{L}_\mathcal{Q} \longrightarrow \mathrm{LS}(\mathcal{L}_\mathcal{N})$ such that $\Phi\colon (\pi(X), \pi(Y)) \longmapsto \Phi_{\pi(X),\pi(Y)}$. Up to renaming the elements of $\mathcal{L}_\mathcal{Q}$, every $X \in \mathcal{L}_\mathcal{S}$ can be represented by a couple (P, x) defined as in (2.12), where $P = \pi(X)$. With this representation, the operation of $\mathcal{L}_\mathcal{S}$ is described by

$$(P, x) \circ (Q, y) = (PQ, \Phi_{P,Q}(x, y))\,.$$

The first condition of Definition 2.0.1 is trivially fulfilled since $x = (\bar{\Omega}, x)$ for every $x \in \mathcal{L}_\mathcal{N}$. Condition ii) holds for commutativity, condition iii) comes from the exponent 2 and condition iv) reflects the totally symmetric property.

□

In this case $\mathcal{L}_\mathcal{S}$ is called an extension of $\mathcal{L}_\mathcal{N}$ by $\mathcal{L}_\mathcal{Q}$ or, equivalently, that the short sequence

$$\Omega' \to \mathcal{L}_\mathcal{N} \to \mathcal{L}_\mathcal{S} \to \mathcal{L}_\mathcal{Q} \to \bar{\Omega} \tag{2.13}$$

is exact. The size of the quotient loop $\mathcal{L}_\mathcal{Q}$ is called the *index* of the extension. We say that the Steiner triple system $\mathcal{S}$ is an extension of $\mathcal{N}$ by $\mathcal{Q}$ as well.

Roughly speaking, a Steiner operator Φ replaces the entry PQ in the multiplication table of $\mathcal{L}_\mathcal{Q}$ with the Latin square $\Phi_{P,Q}$.

	$\cdots$	Q	$\cdots$
$\vdots$		$\vdots$	
P	$\cdots$	PQ	$\cdots$
$\vdots$		$\vdots$	

$\rightsquigarrow$

	$\cdots$	$\overbrace{\quad}^{Q}$	$\cdots$
$\vdots$		$\vdots$	
$P\Big\{$	$\cdots$	$\boxed{\Phi_{P,Q}}$	$\cdots$
$\vdots$		$\vdots$	

In this way, we obtain the multiplication table of $\mathcal{L}_\mathcal{S}$ by gluing together all the tables $\Phi_{P,Q}$ and recalling that in the first component we simply have the multiplication of $\mathcal{L}_\mathcal{Q}$.

Theorem 2.4.4. *Consider an extension*

$$\Omega' \to \mathcal{L}_\mathcal{N} \to \mathcal{L}_\mathcal{S} \to \mathcal{L}_\mathcal{Q} \to \bar{\Omega},$$

of Steiner loops with $\mathcal{N}$ and $\mathcal{Q}$ of order u and w respectively. The $(u+1)(w+1) \times (u+1)(w+1)$ multiplication table of the Steiner loop $\mathcal{L}_\mathcal{S}$ is completely determined by its $w+1$ diagonal symmetric blocks of size $(u+1) \times (u+1)$, and additional $\frac{w(w-1)}{6}$ tables.

Proof. Since the multiplication of $\mathcal{L}_\mathcal{S}$ is given by

$$(P, x) \circ (Q, y) = (PQ, \Phi_{P,Q}(x, y)),$$

for a suitable Steiner operator Φ, the multiplication table of $\mathcal{L}_\mathcal{S}$ is described by the $(w+1)^2$ tables of size $(u+1) \times (u+1)$ corresponding to the Latin squares $\Phi_{P,Q}$, with $P, Q \in \mathcal{L}_\mathcal{Q}$. Every Latin square $\Phi_{P,P}$ in the main diagonal uniquely determines the Latin squares $\Phi_{\bar{\Omega},P}$ and $\Phi_{P,\bar{\Omega}}$. If $\{P, Q, R\}$ is a triple of $\mathcal{Q}$, then $\Phi_{P,Q}$ uniquely determines $\Phi_{P,R}$, $\Phi_{Q,R}$, and consequently $\Phi_{Q,P}$,$\Phi_{R,P}$,$\Phi_{R,Q}$. Hence, once the blocks on the main diagonal are fixed, the remaining $w(w-1)$ blocks can be determined by specifying just $\frac{1}{6}$ of them.

	$\bar{\Omega}$	$\dots$	P	$\dots$	Q	$\dots$	R	$\dots$
$\bar{\Omega}$	$\Phi_{\bar{\Omega},\bar{\Omega}}$		$\Phi_{\bar{\Omega},P}$		$\Phi_{\bar{\Omega},Q}$		$\Phi_{\bar{\Omega},R}$	$\dots$
$\vdots$		$\ddots$						
P	$\Phi_{P,\bar{\Omega}}$		$\Phi_{P,P}$		$\Phi_{P,Q}$		$\Phi_{P,R}$	
$\vdots$				$\ddots$				
Q	$\Phi_{Q,\bar{\Omega}}$		$\Phi_{Q,P}$		$\Phi_{Q,Q}$		$\Phi_{Q,R}$	
$\vdots$						$\ddots$		
R	$\Phi_{R,\bar{\Omega}}$		$\Phi_{R,P}$		$\Phi_{R,Q}$		$\Phi_{R,R}$	
$\vdots$								$\ddots$

TABLE 2.1: Multiplication table of $\mathcal{L}_\mathcal{S}$

□

For example, with the tool provided by the notion of extensions of Steiner triple systems, the problem of classifying STS(v)s containing a projective hyperplane can be reduced to classifying STS($\frac{v-1}{2}$)s and symmetric Latin squares on $\frac{v-1}{2}$ letters with a fixed element in the main diagonal.

Example 2.4.4.1. Here we give an example of an STS(19), denoted with $\mathcal{S}$, having a projective hyperplane $\mathcal{N}$, which has order 9. The corresponding Steiner loop $\mathcal{L}_\mathcal{N}$ is a normal subloop of index 2 in the Steiner loop of order 20. The corresponding quotient loop is $\mathcal{L}_\mathcal{Q} = \{\bar{\Omega}, \bar{1}\}$. For $\mathcal{L}_\mathcal{N}$ we fix the following multiplication table.

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

TABLE 2.2: Multiplication table of $\mathcal{L}_{\mathcal{N}}$

The Latin square $\Phi_{\bar{1},\bar{1}}$ is a symmetric table with the identity element Ω' occurring the whole main diagonal. We choose, for instance, $\Phi_{\bar{1},\bar{1}}$ to be the table

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

TABLE 2.3: $\Phi_{\bar{1},\bar{1}}$

Each of the 45 entries in the upper triangular part of $\Phi_{\bar{1},\bar{1}}$ determines a triple of the STS(19). For instance, we can read from the table that

$$(\bar{1}, 4) \circ (\bar{1}, 1) = (\bar{\Omega}, 2), \tag{2.14}$$

meaning that $\{(\bar{1}, 4), (\bar{1}, 1), (\bar{\Omega}, 2)\}$ is a triple of $\mathcal{S}$. Therefore, $\Phi_{\bar{\Omega},\bar{1}}(2, 1) = 4$ and $\Phi_{\bar{\Omega},\bar{1}}(2, 4) = 1$. In this way we find 45 triples of $\mathcal{S}$, each of which gives two entries in the Latin square $\Phi_{\bar{\Omega},\bar{1}}$. The table $\Phi_{\bar{1},\bar{\Omega}}$ is the transpose of $\Phi_{\bar{\Omega},\bar{1}}$.

The Latin square $\Phi_{\bar{\Omega},\bar{1}}$ is thoroughly determined as shown in the next table.

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

TABLE 2.4: $\Phi_{\bar{\Omega},\bar{1}}$

The entries in $\Phi_{\bar{\Omega},\bar{\Omega}}$, which is the multiplication table of $\mathcal{L}_{\mathcal{N}}$, yield the 12 triples of the hyperplane $\mathcal{N}$, thus we have all of the 57 triples of the STS(19). The elements of $\mathcal{L}_{\mathcal{S}}$ are represented by couples (P, x) in $\mathcal{L}_{\mathcal{Q}} \times \mathcal{L}_{\mathcal{N}}$ and the multiplication table of $\mathcal{L}_{\mathcal{S}}$ is given by the four 10×10 block matrices $\Phi_{P,Q}$.

$$\mathcal{L}_{\mathcal{S}} : \begin{array}{c|c} \Phi_{\bar{\Omega},\bar{\Omega}} & \Phi_{\bar{1},\bar{\Omega}} \\ \hline \Phi_{\bar{\Omega},\bar{1}} & \Phi_{\bar{1},\bar{1}} \end{array}$$

2.5 Schreier extensions of Steiner loops

As mentioned in the beginning of this section, we are interested in the study of the class of loop extensions called *Schreier extensions*, introduced in [75].

Let N be a group with identity Ω' and Q be a loop with identity $\bar{\Omega}$. Consider a map $T\colon Q \to \mathrm{Aut}(N)$ with $T(\bar{\Omega}) = \mathrm{Id}$, and $f\colon Q \times Q \to N$ a function with the property $f(P, \bar{\Omega}) = f(\bar{\Omega}, P) = \Omega'$, for every $P \in Q$. From now on, we will use the additive notation for N and the multiplicative notation for Q. The operation

$$(P, x) \circ (R, y) := \big(PR, f(P, R) + x^{T(R)} + y\big), \tag{2.15}$$

defines on $Q \times N$ a loop L, usually denoted by $L(T, f)$. This loop L gives an extension

$$\Omega' \longrightarrow N \longrightarrow L \longrightarrow Q \longrightarrow \bar{\Omega} \tag{2.16}$$

called a *Schreier extension* of N by Q. Indeed, the loop L contains

$$\overline{N} = \{(\bar{\Omega}, x) \mid x \in N\} \simeq N$$

as a normal subgroup with corresponding quotient loop isomorphic to Q. The function f defining the extension is called a *factor system*.

This construction is very similar to the corresponding definition for groups, but as we anticipated before the lack of associativity makes things less controllable. The following Proposition 2.5.1 gives necessary and sufficient conditions for Schreier extensions of Steiner loops to be a Steiner loops as well.

Theorem 2.5.1. *A Schreier extension of an associative Steiner loop $\mathcal{L}_\mathcal{N}$ by a Steiner loop $\mathcal{L}_\mathcal{Q}$, defined by functions T and f, gives in turn a Steiner loop $\mathcal{L}_\mathcal{S}$ if and only if the following hold:*

1. *$\mathcal{L}_\mathcal{N}$ is central;*
2. *T is trivial;*
3. *f is symmetric and*

$$f(P,Q) = f(P,PQ) = f(Q,PQ), \quad \text{for every } P,Q \in \mathcal{L}_\mathcal{Q}. \tag{2.17}$$

In particular, the operation of $\mathcal{L}_\mathcal{S}$ becomes

$$(P,x)\circ(Q,y) = \big(PQ, x+y+f(P,Q)\big).$$

Proof. By Proposition 3.2. in [75], we find that the map T is trivial, $\mathcal{L}_\mathcal{N}$ is a central subgroup of $\mathcal{L}_\mathcal{S}$ and f is symmetric.

In the resulting loop, the totally symmetric property

$$(P,x)\circ\big((P,x)\circ(Q,y)\big) = (Q,y),$$

for every $P,Q \in \mathcal{L}_\mathcal{Q}$, $x,y \in \mathcal{L}_\mathcal{N}$, is equivalent to

$$\big(Q, y + f\,(P,Q) + f\,(P,PQ)\,\big) = (Q,y)\,.$$

This last condition holds exactly when $f(P,Q) = f(P,PQ)$ for every $P,Q \in \mathcal{Q}$. Of course, by the symmetry of f, $f(P,Q)$ coincides also with $f(Q,PQ)$. □

Schreier extensions are used, for exmple in the study, of *oriented* Steiner triple system. An *oriented Steiner triple system* is an STS in which to each triple is assigned a cyclic order. This concept has been studied in [90]. In such systems, if $\{a_1,a_2,a_3\}$ is a triple, it is represented in an oriented way as (a_1,a_2,a_3), meaning it is oriented with respect to the permutation (1 2 3). An *oriented Steiner loop* L is defined as a Schreier extension of the group $\{1,-1\}$ of order two by a Steiner loop with associated Steiner triple system being oriented. Moreover, the factor system f must be compatible with the orientation structure, that is, $f(a_1,a_2) = 1$ and $f(a_2,a_1) = -1$ whenever a_1 and a_2 are two distinct points of $\mathcal{S}$ determining an oriented triple (a_1,a_2,a_3), and $f(x,x) = -1$, or respectively $f(x,x) = 1$, for every $x \in \mathcal{S}$. The authors describe the left, right and full translation groups of L, and they also study its group of automorphisms.

Schreier extensions play a crucial role also in the study of nilpotent Steiner loops of class 2, which are Steiner loops $\mathcal{L}_\mathcal{S}$ such that $\mathcal{L}_\mathcal{S}/Z(\mathcal{L}_\mathcal{S}) \neq 1$ and is an abelian group. Of course these loops can be seen as Schreier extensions of their center by the group $\mathcal{L}_\mathcal{S}/Z(\mathcal{L}_\mathcal{S})$. For more about this topic, the interested reader can refer to [42].

From now on, by Schreier extensions of Steiner loops, denoted as in the general case with an exact short sequence

$$\Omega' \longrightarrow \mathcal{L}_\mathcal{N} \longrightarrow \mathcal{L}_\mathcal{S} \longrightarrow \mathcal{L}_\mathcal{Q} \longrightarrow \bar{\Omega}, \tag{2.18}$$

we will mean Schreier extensions satisfying the conditions of Proposition 2.5.1. We say that the Seiner triple system $\mathcal{S}$ is a Schreier extension of $\mathcal{N}$ by $\mathcal{Q}$ as well.

The condition (2.17) can be reformulated by saying that

$$f(P,P) = f(P,\bar{\Omega}) = \Omega' \text{ for every } P \in \mathcal{L}_{\mathcal{Q}}, \tag{2.19}$$

and that f is constant on the triples of $\mathcal{Q}$, that is,

$$f(P,Q) = f(P,R) = f(Q,R) \text{ whenever } \{P,Q,R\} \text{ is a triple of } \mathcal{Q}. \tag{2.20}$$

We want to stress the fact that since $\mathcal{L}_{\mathcal{N}}$ is in the center of $\mathcal{L}_{\mathcal{S}}$, the elements of $\mathcal{N}$ are Veblen points of $\mathcal{S}$.

Now we give an example of a Schreier extension resulting in a Steiner triple system of order 15 with precisely one Veblen point.

Example 2.5.1.1. Consider the STS(7) $\mathcal{Q}$ with points and triples as shown in the following figure (2.10).

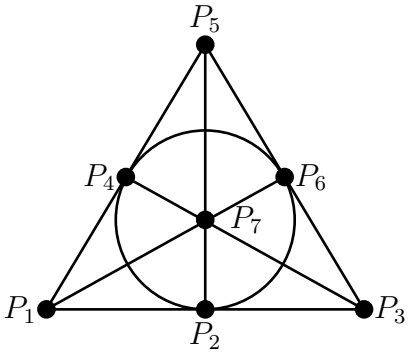

FIGURE 2.10: STS(7) $\mathcal{Q}$

Let $\mathcal{L}_{\mathcal{S}}$ be the Schreier extension of $\mathcal{L}_{\mathcal{N}} = \{\Omega', 1\}$ by $\mathcal{L}_{\mathcal{Q}}$ given by the factor system f with

$$f(P_3,P_5) = f(P_3,P_6) = f(P_5,P_6) = 1,$$
$$f(P_3,P_4) = f(P_3,P_7) = f(P_4,P_7) = 1,$$

and $f(P,Q) = \Omega'$ elsewhere. If we rename the elements of $\mathcal{L}_\mathcal{S}$ as follows,

$$\begin{aligned} \Omega &= (\bar{\Omega}, \Omega'), & 0 &= (\bar{\Omega}, 1), \\ 1 &= (P_1, \Omega'), & 2 &= (P_1, 1), \\ 3 &= (P_2, \Omega'), & 4 &= (P_2, 1), \\ 5 &= (P_3, \Omega'), & 6 &= (P_3, 1), \\ 7 &= (P_4, \Omega'), & 8 &= (P_4, 1), \\ 9 &= (P_5, \Omega'), & a &= (P_5, 1), \\ b &= (P_6, \Omega'), & c &= (P_6, 1), \\ d &= (P_7, \Omega'), & e &= (P_7, 1), \end{aligned}$$

we obtain the presentation of the STS(15) #2 given in [19], where the triples are organized as columns of the following table 2.5.

0	0	0	0	0	0	0	1	1	1	1	1	1	2	2	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5	6	6	6	6
1	3	5	7	9	b	d	3	4	7	8	b	c	3	4	7	8	b	c	7	8	9	a	7	8	9	a	7	8	9	a	7	8	9	a
2	4	6	8	a	c	e	5	6	9	a	d	e	6	5	a	9	e	d	b	c	d	e	c	b	e	d	e	d	c	b	d	e	b	c

TABLE 2.5: STS(15) #2

The theory of Schreier extensions offers a constructive method to obtain Steiner triple systems with Veblen points. On the other hand, if $\mathcal{L}_\mathcal{N}$ is a central subgroup of $\mathcal{L}_\mathcal{S}$, then $\mathcal{L}_\mathcal{S}$ can be obtained as a Schreier extension of $\mathcal{L}_\mathcal{N}$ by $\mathcal{L}_\mathcal{Q} = \mathcal{L}_\mathcal{S}/\mathcal{L}_\mathcal{N}$ (cf. [9], p. 334). This means that any Steiner triple system $\mathcal{S}$ containing Veblen points can be regarded as a Schreier extension of the projective STS consisting of its Veblen points, or a proper subsystem of it.

This provides a necessary and sufficient condition on an admissible positive integer v for the existence of a Steiner triple system of order v containing (at least) a specified number of Veblen points.

Theorem 2.5.2. *There exists an* STS(v) *with (at least)* $2^c - 1$ *Veblen points if, and only if,* $\frac{v+1}{2^c} \equiv 2, 4 \pmod 6$.

Proof. One direction of the claim follows from the fact that, if the center of a Steiner loop has cardinality 2^c, then $\frac{v+1}{2^c}$ must be the cardinality of the quotient projective Steiner loop. The other direction is true because we can construct a Steiner loop $\mathcal{L}_\mathcal{S}$ with non-trivial center by considering a Schreier extension of an elementary abelian 2-group $\mathcal{L}_\mathcal{N}$ of cardinality 2^c by a (suitable) Steiner loop $\mathcal{L}_\mathcal{Q}$ of order $\frac{v+1}{2^c}$. □

Remark 2.5.1. By Theorem 2.5.2, we can determine whether a Steiner triple system can have Veblen points simply by looking at its order. Presented below there is a list of the first 100 admissible integers v for which any STS(v) cannot have Veblen points.

9, 13, 21, 25, 33, 37, 45, 49, 57, 61, 69, 73, 81, 85, 93, 97, 105, 109, 117, 121, 129, 133, 141, 145, 153, 157, 165, 169, 177, 181, 189, 193, 201, 205, 213, 217,

225, 229, 237, 241, 249, 253, 261, 265, 273, 277, 285, 289, 297, 301, 309, 313, 321, 325, 333, 337, 345, 349, 357, 361, 369, 373, 381, 385, 393, 397, 405, 409, 417, 421, 429, 433, 441, 445, 453, 457, 465, 469, 477, 481, 489, 493, 501, 505, 513, 517, 525, 529, 537, 541, 549, 553, 561, 565, 573, 577, 585, 589, 597, 601.

Regarding the orders not mentioned in Remark 2.5.1, Theorem 2.5.2 demonstrates, for instance, that each STS(19) and each STS(27) can have at most one Veblen point. Additionally, any STS(31) can have (at least) 1, 3, 7, 15 or 31 Veblen points. However, we will see that not for all of these numbers it is possible to have an STS(31) with this precise amount of Veblen points. In fact, there is a crucial threshold: exceeding a certain number of Veblen points forces an STS to be projective, and hence to have all its elements as Veblen points. This will be a consequence of Theorem 2.5.3. More specifically, We will delve into Steiner triple systems of size 19, 27 and 31 containing Veblen points in Chapter 3.

Theorem 2.5.3. *If a Schreier extension of Steiner loops*

$$\Omega' \longrightarrow \mathcal{L}_{\mathcal{N}} \longrightarrow \mathcal{L}_{\mathcal{S}} \longrightarrow \mathcal{L}_{\mathcal{Q}} \longrightarrow \bar{\Omega}, \tag{2.21}$$

has index at most 4*, then the resulting Steiner triple system* $\mathcal{S}$ *is projective.*

Proof. Since the factor loop $\mathcal{L}_{\mathcal{Q}}$ has order less or equal 4, it can be either the elementary abelian 2-group of order 2 or 4. We want to prove that the associative property

$$(P, x) \circ ((Q, y) \circ (R, z)) = ((P, x) \circ (Q, y)) \circ (R, z) \tag{2.22}$$

holds for every $P, Q, R \in \mathcal{L}_{\mathcal{Q}}$ and $x, y, z \in \mathcal{L}_{\mathcal{N}}$. Let f be the factor system defining the Schreier extension. If $\mathcal{L}_{\mathcal{Q}}$ has cardinality 2, then f is the null function and $\mathcal{L}_{\mathcal{S}}$ is a group. Let now $\mathcal{L}_{\mathcal{Q}}$ be the elementary abelian 2-group of order 4. On the left-hand side we have

$$\begin{aligned}(P, x) \circ ((Q, y) \circ (R, z)) &= (P, x) \circ (QR, y + z + f(Q, R)) \\ &= (PQR, x + y + z + f(P, QR) + f(Q, R)),\end{aligned}$$

and on the right-hand side

$$\begin{aligned}((P, x) \circ (Q, y)) \circ (R, z) &= (PQ, x + y + f(P, Q)) \circ (R, z) \\ &= (PQR, x + y + z + f(PQ, R) + f(P, Q)).\end{aligned}$$

Hence we have to check that

$$f(P, QR) + f(Q, R) = f(PQ, R) + f(P, Q). \tag{2.23}$$

- If the three points form the only triple in the underlying STS(3) $\mathcal{Q}$, then by condition (2.20) we obtain (2.23).
- If one out of the three points is the identity element, say $P = \bar{\Omega}$ without loss of generality, the equation (2.23) reduces to

$$f(\bar{\Omega}, QR) + f(Q, R) = f(Q, R) + f(\bar{\Omega}, Q), \tag{2.24}$$

which is true since $f(\bar{\Omega}, QR) = \Omega' = f(\bar{\Omega}, Q)$ by condition (2.19).

- If two out of the three points coincide, say $P = Q$ without loss of generality, then the equation (2.23) reduces to

$$f(P, PR) + f(P, R) = f(\bar{\Omega}, R) + f(P, P), \tag{2.25}$$

which holds since both sides are equal to Ω'.

□

As a direct consequence, Theorem 2.5.3 enables us to strengthen the Veblen-Young Theorem 2.1.8, setting a threshold for the maximum number of Veblen points in a non-projective Steiner triple system.

Corollary 2.5.4. *Let $\mathcal{S}$ be a Steiner triple system of order $v \geq 7$. $\mathcal{S}$ is projective if and only if it has more than $\frac{v-7}{8}$ Veblen points.*

Proof. If an STS(v) $\mathcal{S}$ has more than $\frac{v-7}{8}$ Veblen points, the center of $\mathcal{L}_{\mathcal{S}}$ has order more than $\frac{v+1}{8}$, hence index at most 4, and by Theorem 2.5.3 $\mathcal{S}$ is projective. □

Corollary 2.5.4 specifically addresses Steiner triple systems of order $v \geq 7$. However, it is worth noting that Steiner triple systems of order 1 and 3, which are the only cases left out by the result, are inherently projective.

Another similar consequence of Theorem 2.5.3 is given by the following result.

Corollary 2.5.5. *If a Steiner triple system of order v, with $2^n - 1 \leq v < 2^{n+1} - 1$ and $n > 1$, contains at least 2^{n-3} Veblen points, then it is isomorphic to* PG$(n-1, 2)$.

Proof. If we suppose that $\mathcal{S}$ has at least 2^{n-3} Veblen points, then, since they form a projective subsystem, the number of Veblen points is at least $2^{n-2} - 1$. Hence, the center $Z(\mathcal{L}_{\mathcal{S}})$ of $\mathcal{L}_{\mathcal{S}}$ has at least 2^{n-2} elements. If $v < 2^{n+1} - 1$, then one has $|\mathcal{L}_{\mathcal{S}}/Z(\mathcal{L}_{\mathcal{S}})| < \frac{2^{n+1}}{2^{n-2}} = 8$. Therefore, $\mathcal{S}$ is a projective and by cardinality reasons it is isomorphic to PG$(n-1, 2)$. □

Remark 2.5.2. In view of the last two results, we can easily see the fact that the only STS(15) with more than one Veblen point is PG$(3, 2)$, as we showed before. Actually, now we can say even more: the only STS(v)s with $v < 31$ having more than one Veblen point are PG$(1, 2)$, PG$(2, 2)$ and PG$(3, 2)$.

In the next result we characterize projective geometries over GF(2) in terms of subcentral series.

Theorem 2.5.6. *A Steiner loop $\mathcal{L}_{\mathcal{S}}$ has a subcentral series*

$$\Omega \trianglelefteq \mathcal{L}_{\mathcal{S}_1} \trianglelefteq \cdots \trianglelefteq \mathcal{L}_{\mathcal{S}_n} = \mathcal{L}_{\mathcal{S}},$$

where the factors $\mathcal{L}_{\mathcal{S}_{i+1}}/\mathcal{L}_{\mathcal{S}_i}$ have order 2 if, and only if, $\mathcal{S}$ is isomorphic to PG$(n-1, 2)$.

Proof. We prove the first part of the assertion by induction. If $n = 1$, then $\mathcal{L}_{\mathcal{S}} = \mathrm{GF}(2)$, so $\mathcal{S}$ consists of a single point and we can see it as $\mathrm{PG}(0, 2)$. Let now $n > 1$ and assume that $\mathcal{S}_{n-1}$ is projective. Since $\mathcal{L}_{\mathcal{S}_{n-1}}$ is central and of index 2, then by Theorem 2.5.3 $\mathcal{S}$ is projective as well. In particular, $\mathcal{S}$ is isomorphic to $\mathrm{PG}(n-1, 2)$.

Conversely, if $\mathcal{S}$ is a projective geometry $\mathrm{PG}(n-1, 2)$, then the corresponding Steiner loop is an elementary abelian 2-group and the assertion follows directly. □

In the final part of this section we want to give a result concerning Steiner loops of cardinality $v + 1$ which have only one admissible factorization of the type $v + 1 = 2(w + 1)$.

Theorem 2.5.7. *Let $\mathcal{L}_{\mathcal{S}}$ be a Steiner loop with cardinality $v + 1$ and suppose that it has a unique admissible factorization $v + 1 = 2(w + 1)$. Then one of the following holds:*

- *$\mathcal{L}_{\mathcal{S}}$ is simple;*
- *$\mathcal{S}$ has precisely one Veblen point, and hence it is a Schreier extension of this point by an $\mathrm{STS}(w)$;*
- *has a projective hyperplane as a subsystem, and therefore it is an extensions of this hyperplane by an $\mathrm{STS}(1)$.*

Proof. If $\mathcal{L}_{\mathcal{S}}$ is not a simple loop, then it has a normal subloop $\mathcal{L}_{\mathcal{N}}$ of size 2 or w. In the former case, $\mathcal{L}_{\mathcal{N}}$ is actually central. Therefore $\mathcal{S}$ has a Veblen point and $\mathcal{L}_{\mathcal{S}}$ is a Schreier extension of $\mathcal{L}_{\mathcal{N}}$ by a quotient loop $\mathcal{L}_{\mathcal{Q}}$ of order $w + 1$. In the latter case, $\mathcal{N}$ is a projective hyperplane, hence normal, and $\mathcal{L}_{\mathcal{S}}$ is an extension of $\mathcal{L}_{\mathcal{N}}$ by the loop $\mathcal{L}_{\mathcal{Q}}$ of order 2 for a suitable Steiner operator. □

As a consequence of the above Corollary it is possible, in principle, to construct all the non-simple $\mathrm{STS}(v)$ admitting the unique factorization $v + 1 = 2(w + 1)$.

2.6 An introductive cohomology theory for Steiner triple systems

In this section, we will introduce a (small) cohomology theory for Schreier extensions of Steiner loops. This approach offers a systematic way to construct Steiner triple systems containing Veblen points. We will apply these methods in Chapter 3. In order to stay constructive and not be too theoretical, fixed $\mathcal{L}_{\mathcal{N}}$ and $\mathcal{L}_{\mathcal{Q}}$, we identify each Schreier extension with the corresponding factor system. We denote the set of all factor systems with

$$\mathrm{Ext}_{\mathrm{S}}(\mathcal{L}_{\mathcal{N}}, \mathcal{L}_{\mathcal{Q}}).$$

We recall that the output values of factor systems lie in $\mathcal{L}_{\mathcal{N}}$, which is associative. Therefore, $\mathrm{Ext}_{\mathrm{S}}(\mathcal{L}_{\mathcal{N}}, \mathcal{L}_{\mathcal{Q}})$ forms a group under the addition of functions. Since

a factor system is completely determined by the values it takes on the triples of the quotient system $\mathcal{Q}$, it is easy to see that the total number of possible Schreier extensions of $\mathcal{L}_\mathcal{N}$ by $\mathcal{L}_\mathcal{Q}$ is

$$|\mathrm{Ext}_\mathrm{S}(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})| = 2^{tb}, \tag{2.26}$$

where b is the number of triples of $\mathcal{Q}$ and 2^t is the cardinality of the elementary abelian 2-group $\mathcal{L}_\mathcal{N}$. An important subgroup of $\mathrm{Ext}_\mathrm{S}(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})$ is given by the so called *coboundaries*, defined by the cohomology operator δ^1. If φ is a map $\mathcal{L}_\mathcal{Q} \longrightarrow \mathcal{L}_\mathcal{N}$ sending $\Omega' \longmapsto \bar{\Omega}$, then $\delta^1\varphi$ is the map $\mathcal{L}_\mathcal{Q} \times \mathcal{L}_\mathcal{Q} \longrightarrow \mathcal{L}_\mathcal{N}$ defined by

$$(\delta^1\varphi)(P, Q) := \varphi(PQ) - (\varphi(P) + \varphi(Q)). \tag{2.27}$$

We notice here that in the last equation (2.27), the parentheses and the minus sign are redundant, since the Steiner loop $\mathcal{L}_\mathcal{N}$ is associative and of exponent 2, but we decided to present a more general definition for a non-associative context. We notice that, by the definition of the operator δ^1, every function $\delta^1\varphi$ as above is in fact a factor system. Indeed, $\delta^1\varphi$ is of course symmetric since $\mathcal{L}_\mathcal{Q}$ is commutative. Furthermore, for every $P, Q \in \mathcal{L}_\mathcal{Q}$,

$$(\delta^1\varphi)(P, P) = (\delta^1\varphi)(P, \bar{\Omega}) = \phi(\bar{\Omega}) = \Omega'$$

and

$$\begin{aligned}(\delta^1\varphi)(P, PQ) &= \varphi(P \cdot PQ) + \varphi(P) + \varphi(PQ)\\ &= \varphi(Q) + \varphi(P) + \varphi(PQ)\\ &= (\delta^1\varphi)(P, Q),\end{aligned}$$

since $\mathcal{L}_\mathcal{Q}$ is totally symmetric. Analogously, $(\delta^1\varphi)(PQ, Q) = (\delta^1\varphi)(P, Q)$. Moreover, naturally $\delta^1(\varphi + \psi) = \delta^1\varphi + \delta^1\psi$ holds, hence the set

$$\mathrm{B}^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N}) := \left\{\delta^1\varphi \mid \varphi\colon \mathcal{L}_\mathcal{Q} \to \mathcal{L}_\mathcal{N},\ \varphi(\Omega') = \bar{\Omega}\right\} \tag{2.28}$$

is a subgroup of $\mathrm{Ext}_\mathrm{S}(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})$. Since δ^1 is additive, two coboundaries $\delta^1\varphi$ and $\delta^1\psi$ coincides if and only if they differ by a function g such that $\delta^1 g$ is zero, that is, an homomorphism $\mathcal{L}_\mathcal{Q} \longrightarrow \mathcal{L}_\mathcal{N}$. Therefore, the size of this subgroup is

$$|\mathrm{B}^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})| = \frac{|\{\varphi : \mathcal{L}_\mathcal{Q} \to \mathcal{L}_\mathcal{N} \mid \varphi(\bar{\Omega}) = \Omega'\}|}{|\mathrm{Hom}(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})|} = \frac{2^{wt}}{|\mathrm{Hom}(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})|},$$

where $2^t = |\mathcal{L}_\mathcal{N}|$ and $w = |\mathcal{Q}|$. This subgroup will turn out to be useful for the classification of factor systems up to *equivalence*.

Definition 2.6.1. Two Schreier extensions

$$\Omega' \longrightarrow \mathcal{L}_\mathcal{N} \longrightarrow \mathcal{L}_{\mathcal{S}_1} \longrightarrow \mathcal{L}_\mathcal{Q} \longrightarrow \bar{\Omega},$$

$$\Omega' \longrightarrow \mathcal{L}_\mathcal{N} \longrightarrow \mathcal{L}_{\mathcal{S}_2} \longrightarrow \mathcal{L}_\mathcal{Q} \longrightarrow \bar{\Omega},$$

are called *equivalent* if there is an isomorphism $\mathcal{L}_{\mathcal{S}_1} \longrightarrow \mathcal{L}_{\mathcal{S}_2}$ which induces the identity homomorphism both on $\mathcal{L}_\mathcal{N}$ and $\mathcal{L}_\mathcal{Q}$. In this case, the corresponding

factor systems f_1 and f_2 are called also equivalent and we write $f_1 \sim f_2$.

The following result gives a characterization of equivalent factor systems.

Lemma 2.6.2. *Two factor systems $f_1, f_2 \in \mathrm{Ext_S}(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})$ are equivalent if and only if they differ by a suitable coboundary $\delta^1\varphi$. Moreover, the isomorphism between the corresponding loops realizing the equivalence has the following form:*

$$(P, x) \longmapsto (P, x + \varphi(P)) \,. \tag{2.29}$$

Proof. Let $\Phi\colon \mathcal{L}_{\mathcal{S}_1} \longrightarrow \mathcal{L}_{\mathcal{S}_2}$ be an isomorphism between the Steiner loops corresponding, respectively, to the factor systems f_1 and f_2. Let us suppose that Φ defines an equivalence of extensions. We have that

$$\begin{aligned} \Phi(P, x) &= \Phi\left((P, \Omega') \circ (\bar{\Omega}, x)\right) && (2.30)\\ &= \Phi(P, \Omega') \circ (\bar{\Omega}, x) && (2.31)\\ &= (P, \varphi(P)) \circ (\bar{\Omega}, x) && (2.32)\\ &= (P, x + \varphi(P)), && (2.33) \end{aligned}$$

for a suitable function $\varphi : \mathcal{L}_\mathcal{Q} \longrightarrow \mathcal{L}_\mathcal{N}$. Since $\Phi(\bar{\Omega}, \Omega') = (\bar{\Omega}, \Omega')$, the map φ sends $\bar{\Omega} \mapsto \Omega'$. If we multiply two elements in $\mathcal{L}_{\mathcal{S}_1}$,

$$(P, x) \circ (Q, y) = (PQ, x + y + f_1(P, Q)), \tag{2.34}$$

the isomorphism Φ maps the left-hand side of the equation (2.34) into

$$(P, x + \varphi(P)) \circ (Q, y + \varphi(Q)) = (PQ, x + \varphi(P) + y + \varphi(Q) + f_2(P, Q)),$$

and the the right-hand side into

$$(PQ, x + y + f_1(P, Q) + \varphi(PQ)).$$

Hence, $f_2 = f_1 + \delta^1\varphi$.

Conversely, if $f_2 = f_1 + \delta^1\varphi$, then the function $\Phi(P, x) := (P, x + \varphi(P))$ defines an isomorphism $\Phi\colon \mathcal{L}_{\mathcal{S}_1} \longrightarrow \mathcal{L}_{\mathcal{S}_2}$ which induces the identity both on $\mathcal{L}_\mathcal{N}$ and $\mathcal{L}_\mathcal{Q}$. Hence, the factor systems f_1 and f_2 are equivalent. □

Using the characterization obtained with the previous Lemma 2.6.2, we can find the number of non-equivalent extensions of $\mathcal{L}_\mathcal{N}$ by $\mathcal{L}_\mathcal{Q}$, that is,

$$\left|\frac{\mathrm{Ext_S}(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})}{\mathrm{B}^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})}\right| = \frac{2^{tb}}{|\mathrm{B}^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})|}.$$

Since $|\mathrm{B}^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})| = 2^{wt}/|\mathrm{Hom}(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})|$ and $b = \frac{w-1}{6}$, this number is

$$\left|\frac{\mathrm{Ext_S}(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})}{\mathrm{B}^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})}\right| = 2^{tw\left(\frac{w-7}{6}\right)}|\mathrm{Hom}(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})|.$$

Example 2.6.2.1. We want to construct a Steiner triple system of order 15 with (at least) one Veblen point. Let $\mathcal{L}_{\mathcal{N}}$ be of order 2 and $\mathcal{Q}$ be STS(7). The number of functions $\varphi : \mathcal{L}_{\mathcal{Q}} \to \mathcal{L}_{\mathcal{N}}$ with $\varphi(\bar{\Omega}) = \Omega'$ is 2^7, and the cardinality of $\mathrm{Hom}(\mathcal{L}_{\mathcal{Q}}, \mathcal{L}_{\mathcal{N}})$ is 2^3, hence $|\mathrm{B}^2(\mathcal{L}_{\mathcal{Q}}, \mathcal{L}_{\mathcal{N}})| = 2^4$. Therefore, the number of non-equivalent Schreier extensions of $\mathcal{L}_{\mathcal{N}}$ by $\mathcal{L}_{\mathcal{Q}}$ is $\frac{2^7}{2^4} = 8$. Actually, we know that among the resulting 8 Steiner triple systems, we have only 2 isomorphism classes, since the only STS(15) with Veblen points are #1 and #2, and for this we need a further reduction.

Definition 2.6.3. Two Schreier extensions

$$\Omega' \longrightarrow \mathcal{L}_{\mathcal{N}} \longrightarrow \mathcal{L}_{\mathcal{S}_1} \longrightarrow \mathcal{L}_{\mathcal{Q}} \longrightarrow \bar{\Omega},$$

$$\Omega' \longrightarrow \mathcal{L}_{\mathcal{N}} \longrightarrow \mathcal{L}_{\mathcal{S}_2} \longrightarrow \mathcal{L}_{\mathcal{Q}} \longrightarrow \bar{\Omega},$$

are called *isomorphic* if there is an isomorphism $\mathcal{L}_{\mathcal{S}_1} \longrightarrow \mathcal{L}_{\mathcal{S}_2}$ leaving $\mathcal{L}_{\mathcal{N}}$ invariant. In this case, the corresponding factor systems f_1 and f_2 are called also isomorphic and we write $f_1 \simeq f_2$.

By definition, two isomorphic Schreier extensions give in turn two isomorphic Steiner loops, and consequently, isomorphic Steiner triple systems. However, it is important to notice that the converse is not always true. Since the isomorphism between the Steiner loops might not preserve $\mathcal{L}_{\mathcal{N}}$, it is possible to have two isomorphic Steiner loops arising from non-isomorphic Schreier extensions. This situation may occur when the Steiner triple systems produced by the two Schreier extensions have additional Veblen points not contained in $\mathcal{N}$. In the following Remark 2.6.1, we provide a criterion to determine if this is the case. Of course this cannot happen if $\mathcal{L}_{\mathcal{N}}$ coincides with the whole center of the resulting Steiner loops, since it must be preserved. Therefore, in this last case, two extensions are isomorphic if and only if the resulting loops are isomorphic as well.

Remark 2.6.1. Let the Steiner loop $\mathcal{L}_{\mathcal{S}}$ be a Schreier extension of $\mathcal{L}_{\mathcal{N}}$ by $\mathcal{L}_{\mathcal{Q}}$ with factor system f. The Steiner triple system $\mathcal{S}$ has a Veblen point (P, x) not contained in $\mathcal{N}$ if and only if P is itself a Veblen point of $\mathcal{Q}$ and

$$f(P, Q) + f(PQ, R) = f(Q, R) + f(P, QR), \tag{2.35}$$

for every $Q, R \in \mathcal{Q}$. The condition (2.35) reflects the centrality of the element (P, x) in $\mathcal{L}_{\mathcal{S}}$.

Of course, two equivalent extensions are also isomorphic, but the converse is not always true. However, reducing up to equivalence is useful in order to easily characterize isomorphism of extensions, as we show in the next result. For simplicity of notation, if β is an automorphism of $\mathcal{L}_{\mathcal{Q}}$ and $f \in \mathrm{Ext}_{\mathrm{S}}(\mathcal{L}_{\mathcal{N}}, \mathcal{L}_{\mathcal{Q}})$, we denote with $f\beta$ the factor system defined by

$$(P, Q) \longmapsto f\left(\beta(P), \beta(Q)\right).$$

Proposition 2.6.4. *Two factor systems $f_1, f_2 \in \mathrm{Ext}_{\mathrm{S}}(\mathcal{L}_{\mathcal{N}}, \mathcal{L}_{\mathcal{Q}})$ are isomorphic if and only if*

$$\alpha f_1 \sim f_2 \beta \tag{2.36}$$

for suitable $\alpha \in \mathrm{Aut}(\mathcal{L}_\mathcal{N})$ *and* $\beta \in \mathrm{Aut}(\mathcal{L}_\mathcal{Q})$. *Moreover, the isomorphism between the corresponding loops has, up to equivalence, the following form*

$$(P, x) \longmapsto (\beta(P), \alpha(x)). \tag{2.37}$$

Proof. Let $\Phi\colon \mathcal{L}_{\mathcal{S}_1} \longrightarrow \mathcal{L}_{\mathcal{S}_2}$ be an isomorphism between the Steiner loops corresponding, respectively, to the factor systems f_1 and f_2, and let us suppose that Φ defines an isomorphism of extensions. Since $\Phi(\mathcal{L}_\mathcal{N}) = \mathcal{L}_\mathcal{N}$ and of course $\Phi(\mathcal{L}_\mathcal{Q}) = \mathcal{L}_\mathcal{Q}$, we obtain that

$$\Phi(\bar{\Omega}, x) = (\bar{\Omega}, \alpha(x)), \text{ for every } x \in \mathcal{L}_\mathcal{N}, \tag{2.38}$$

where α is an automorphism of $\mathcal{L}_\mathcal{N}$, and

$$\Phi(P, \Omega') = (\beta(P), \varphi(P)), \text{ for every } P \in \mathcal{L}_\mathcal{Q},$$

where β is a suitable automorphism of $\mathcal{L}_\mathcal{Q}$ and φ is a function $\mathcal{L}_\mathcal{Q} \to \mathcal{L}_\mathcal{N}$ mapping $\bar{\Omega} \mapsto \Omega'$. Hence

$$\begin{aligned}\Phi(P, x) &= \Phi\left((P, \Omega') \circ (\bar{\Omega}, x)\right)\\ &= (\beta(P), \varphi(P)) \circ (\bar{\Omega}, \alpha(x))\\ &= (\beta(P), \alpha(x) + \varphi(P)).\end{aligned}$$

If we multiply two elements in $\mathcal{L}_{\mathcal{S}_1}$,

$$(P, x) \circ (Q, y) = (PQ, x + y + f_1(P, Q)), \tag{2.39}$$

the isomorphism Φ maps the left-hand side of the last equation into

$$\begin{aligned}&(\beta(P), \alpha(x) + \varphi(P)) \circ (\beta(Q), \alpha(y) + \varphi(Q))\\ =&\,(\beta(PQ), \alpha(x + y) + \varphi(P) + \varphi(Q) + f_2\left(\beta(P), \beta(Q)\right))\end{aligned}$$

and the the right-hand side into

$$\big(\beta(PQ), \alpha(x + y) + \alpha f_1(P, Q) + \varphi(PQ)\big).$$

Therefore, for evrey $P, Q \in \mathcal{L}_\mathcal{Q}$, the following holds

$$f_2\left(\beta(P), \beta(Q)\right) = \alpha f_1(P, Q) + \varphi(PQ) + \varphi(P) + \varphi(Q).$$

Thus,

$$f_2\beta = \alpha f_1 + \delta^1\varphi,$$

that is, $f_2\beta \sim \alpha f_1$. By Lemma 2.6.2, up to equivalence Φ has the form in Equation (2.37).

Conversely, if $f_2\beta \sim \alpha f_1$, the map in (2.37) defines an isomorphism of extensions. □

An immediate consequence of the last result is that the isomorphism class of the null factor system f_0 coincides with its equivalence class. One direction, as

pointed out before, is clear, since the equivalence is a stronger concept than the isomorphism. Conversely, if a factor system f is isomorphic to the null function f_0, and $\Phi\colon (P,x) \mapsto (\beta(P), \alpha(x))$ defines, up to equivalence, an isomorphism of extensions, then from

$$\Phi\left((P,x) \circ (Q,y)\right) = \Phi(P,x) \circ \Phi(Q,y),$$

we obtain

$$(\beta(PQ), \alpha(x+y)) = (\beta(PQ), \alpha(x+y) + f\beta(P,Q))\,, \tag{2.40}$$

which says that f coincides (up to an equivalence) with f_0.

Now we give an example of two isomorphic but not equivalent Schreier extensions.

Example 2.6.4.1. Now we give an example of two isomorphic but non-equivalent Schreier extensions of cardinality 20. Let $\mathcal{L}_{\mathcal{N}} = \{\Omega', 1\}$ be the unique loop of cardinality 2 and $\mathcal{L}_{\mathcal{Q}}$ the Steiner loop corresponding to the STS(9). We can represent $\mathcal{Q}$ as the affine plane AG$(3,2)$ with points and lines given by the following Figure 2.11.

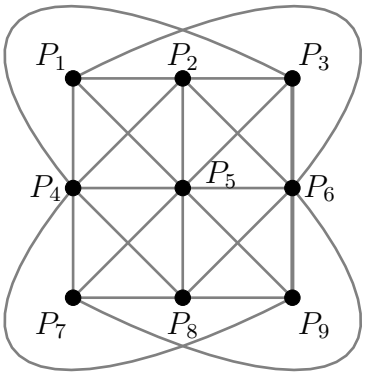

FIGURE 2.11: STS(9) $\mathcal{Q}$

Consider the Schreier extension $\mathcal{L}_{\mathcal{S}_1}$ associated with the factor system f_1 such that

$$f_1(P_3,P_6) = f_1(P_3,P_9) = f_1(P_6,P_9) = 1$$

and f_1 is null elsewhere. The automorphism β of $\mathcal{L}_{\mathcal{Q}}$ induced by the affine map $x \mapsto Ax + b$ of AG$(3,2)$, with

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$$

permutes the points of $\mathcal{Q}$ as

$$\beta(P_i) = P_{\sigma(i)}, \qquad \text{with} \qquad \sigma = (465)(789).$$

Consider the Steiner loop $\mathcal{L}_{\mathcal{S}_2}$ which is the Schreier extension associated with the factor system $f_2 := f_1\beta$, which clearly satisfies

$$f_2(P_3, P_4) = f_2(P_3, P_8) = f_2(P_4, P_8) = 1$$

and is null elsewhere. By construction, f_1 and f_2 are isomorphic, but they are not equivalent. In fact, by Lemma 2.6.2, f_1 and f_2 are equivalent if and only if $f_1 + f_2 = \delta^1\varphi$, for a suitable function φ. If this would be the case, for every triple $\{P_i, P_j, P_k = P_iP_j\}$ of $\mathcal{Q}$, the following must hold

$$\varphi(P_i) + \varphi(P_j) + \varphi(P_k) = (f_1 + f_2)(P_i, P_j). \tag{2.41}$$

Denoting $\varphi(P_i)$ with X_i, for every $i = 1, \ldots, 9$, from (2.41), we obtain the following linear system in equation (2.42) with scalar in the field GF(2) and twelve linear equations in the nine unknowns X_i.

$$\begin{pmatrix} 1&1&1&0&0&0&0&0&0\\ 1&0&0&1&0&0&1&0&0\\ 1&0&0&0&1&0&0&0&1\\ 1&0&0&0&0&1&0&1&0\\ 0&1&0&1&0&0&0&0&1\\ 0&1&0&0&1&0&0&1&0\\ 0&1&0&0&0&1&1&0&0\\ 0&0&1&1&0&0&0&1&0\\ 0&0&1&0&1&0&1&0&0\\ 0&0&1&0&0&1&0&0&1\\ 0&0&0&1&1&1&0&0&0\\ 0&0&0&0&0&0&1&1&1 \end{pmatrix} \begin{pmatrix} X_1\\X_2\\X_3\\X_4\\X_5\\X_6\\X_7\\X_8\\X_9 \end{pmatrix} = \begin{pmatrix} 0\\0\\0\\0\\0\\0\\1\\0\\1\\0\\0 \end{pmatrix} \tag{2.42}$$

By straightforward arguments of linear algebra, it is easy to see that the system in (2.42) has no solution, implying that such a function φ does not exist.

By Proposition 2.6.4, non-equivalent but isomorphic factor systems f_1, f_2 are characterized by the relation $\alpha f_1 = f_2\beta$, for suitable $\alpha \in \mathrm{Aut}(\mathcal{L}_{\mathcal{N}})$ and $\beta \in \mathrm{Aut}(\mathcal{L}_{\mathcal{Q}})$. This relation can be rewritten as

$$f_2 = \alpha f_1 \beta^{-1}. \tag{2.43}$$

In this way, we can define a left action of the group $\mathrm{Aut}(\mathcal{L}_{\mathcal{N}}) \times \mathrm{Aut}(\mathcal{L}_{\mathcal{Q}})$ on the set $\mathrm{Ext}_S(\mathcal{L}_{\mathcal{N}}, \mathcal{L}_{\mathcal{Q}})/\mathrm{B}^2(\mathcal{L}_{\mathcal{Q}}, \mathcal{L}_{\mathcal{N}})$ of non-equivalent extensions given by

$$(\alpha, \beta)(f) = \alpha f \beta^{-1},$$

whose orbits are the isomorphism classes of all the factor systems. In Chapter 3, we will apply this method in order to classify Steiner triple systems of order 19, 27 and 31 containing Veblen points.

Chapter 3

Counting Steiner triple systems with Veblen points

Counting all Steiner triple systems of a given order is a wild problem. The last full computation was done by P. Kaski and P. R. J. Östergård in [51], in which they determined the number of non-isomorphic STS(19)s, that is $11,084,874,829$. Attempting to compute the number of all Steiner triple systems for the next admissible order, which is 21, appears currently unfeasible. However, in [52] and [47], the authors classified STS(21)s containing subsystems of order 7 and 9, and also gave an estimation of the total number of all STS(21)s.

For this reason, instead of an extensive enumeration, it is better to look for classifying Steiner triple systems presenting some regular structures, for examples having some given subsystems. We focus our investigation on the number of STSs containing Veblen points. Since such a point has the property that any two distinct triples through it generate a Fano plane, in this sense Steiner triple systems containing Veblen points are close to projective STSs. The latter, as pointed in Theorem 2.1.8, are indeed characterized by the fact every element is a Veblen point. For this reason, we can say that Steiner triple systems with Veblen points preserve some sort of regularity resembling the structure of the point-line design of a projective geometry. In Chapter 2 we provided a theoretical algebraic technique for constructing Steiner triple systems containing Veblen points by using tools from the theory of loop extensions. In this chapter, we will use this approach to investigate the cases of sizes 19, 27 and 31, respectively.

3.1 Description of the algorithms

In order to make the results presented in this chapter more clear, we describe the algorithms used for classifying the Steiner triple systems of order 19, 27 and 31 with Veblen points. The computations were done by computer, using python programming. The pseudocodes of the programs can be found in Appendix A.

In general, we begin with an associative Steiner loop $\mathcal{L}_{\mathcal{N}}$, which, being an elementary abelian 2-group, we represent by $\mathrm{GF}(2)^t$. In our specific cases, t will be either 1 or 2. Additionally, we have a Steiner loop $\mathcal{L}_{\mathcal{Q}}$ whose the operation is defined by the triples of $\mathcal{Q}$ arranged as columns of a table. Fixed an order for the b triples of $\mathcal{Q}$, we define the ordered set of *fundamental pairs*, denoted

with $\mathcal{Q}_2$, as the family of 2-subsets obtained by removing one element from each triple and fixing an order.

Since a factor system $f \in \mathrm{Ext}_S(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})$ is defined by the value it takes in every fundamental pair, in order to improve the efficiency of our implementation we can represent f with an integer in the following way. Let $n_i \in \mathrm{GF}(2)^t$ be the image of the fundamental pair c_i under f, $i = 1, \ldots, b$. Then f can be identified uniquely with the vector $(n_1, n_2, \ldots, n_b) \in (\mathrm{GF}(2)^t)^b$. Of course f can be compressed into a binary vector of length tb, which is the binary representation of an integer.

On the other hand, every vector v of $\mathrm{GF}(2)^{tb}$ defines uniquely a factor system f, precisely the one mapping the i-th fundamental pair into the i-th sub-vector of v of length t, $i = 1, \ldots, b$. In this way, we can uniquely describe every factor system as an integer $0 \leq k \leq 2^{tb} - 1$.

Example 3.1.0.1. For instance, let $\mathcal{L}_\mathcal{N}$ be $\mathrm{GF}(2)^2$, and $\mathcal{Q}$ be the STS(9) with points $\{1, \ldots, 9\}$ and triples given by the columns of the following Table 3.1.

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

TABLE 3.1: Triples of the STS(9)

The fundamental pairs of $\mathcal{Q}$ are given in lexicographic order as follows:

$$\{1,2\},\ \{1,4\},\ \{1,5\},\ \{1,6\},\ \{2,4\},\ \{2,5\},$$
$$\{2,6\},\ \{3,4\},\ \{3,5\},\ \{3,6\},\ \{4,5\},\ \{7,8\}.$$

Let f be the factor system defined by:

$$f(1,2) = (0,0),\ f(1,4) = (0,0),\ f(1,5) = (0,0),\ f(1,6) = (0,0),$$
$$f(2,4) = (0,1),\ f(2,5) = (1,1),\ f(2,6) = (0,0),\ f(3,4) = (1,1),$$
$$f(3,5) = (1,0),\ f(3,6) = (0,1),\ f(4,5) = (0,0),\ f(7,8) = (0,0).$$

We can represent f as the vector

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

of $(\mathrm{GF}(2)^2)^6$ which can be compacted into the binary vector

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

representing the integer 29584.

In the same way, after computing the set $\mathrm{B}^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N}) = \{\delta^1\varphi \mid \varphi\colon \mathcal{L}_\mathcal{Q} \to \mathcal{L}_\mathcal{N},\ \varphi(\bar{\Omega}) = \Omega\}$, we can represent every coboundary as one of the integers k, $0 \leq k \leq 2^{tb} - 1$. In order to find the cosets in $\mathrm{Ext}_S(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})/\mathrm{B}^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})$, we compute the sum $f + \delta^1\varphi$ as the operation XOR between binary vectors. Consequently, we can find the set of non-equivalent extensions by taking one representative in each coset.

In order to find the set of non-isomorphic extensions, we compute the automorphism group $\mathrm{Aut}(\mathcal{L}_\mathcal{N})$ and $\mathrm{Aut}(\mathcal{L}_\mathcal{Q})$. In our cases, the former is either the trivial group or $\mathrm{GL}(2,2)$. For the latter, since the quotient system $\mathcal{Q}$ in our cases have order w either 7, 9, 13 or 15, it presents more possibilities.

If $\mathcal{Q}$ is the STS(7), STS(9) or STS(15) #1, then the group $\mathrm{Aut}(\mathcal{L}_\mathcal{Q})$ is $\mathrm{GL}(3,2)$, $\mathrm{Aff}(2,3)$ or $\mathrm{GL}(4,2)$, respectively. If $\mathcal{Q}$ is an STS(13), then the group $\mathrm{Aut}(\mathcal{L}_\mathcal{Q})$ is either symmetric group S_3 or the unique non-abelian group of order 39 denoted with F_{39}, if $\mathcal{Q}$ is the STS(13) #1 or #2, respectively. Let us denote, in both cases, the set of points of the STS(13) with $\{0,1,\ldots,12\}$. In the first case, where the triples are given by the table A.1, $\mathrm{Aut}(\mathcal{L}_\mathcal{Q})$ is computed as the group generated by the function $x \mapsto x \pmod{13}$ and the permutation (6 8)(2 11)(3 9)(4 12)(5 7). In the second case, where the triples are given by the table A.2, $\mathrm{Aut}(\mathcal{L}_\mathcal{Q})$ is computed as the group of functions $x \mapsto ax + b \pmod{13}$, where $a \in \{1,3,9\}$ and $b \in \{0,\ldots,12\}$. If $\mathcal{Q}$ is a non-projective STS, we compute the group $\mathrm{Aut}(\mathcal{L}_\mathcal{Q})$ as the group of permutations of the 15 points which induce a permutation of the 35 triples as well.

Let us now consider a factor systems f represented as a vector $(n_1, n_2, \ldots, n_b) \in (\mathrm{GF}(2)^t)^b$ and two automorphisms $\alpha \in \mathrm{Aut}(\mathcal{L}_\mathcal{N})$, $\beta \in \mathrm{Aut}(\mathcal{L}_\mathcal{N})$. The factor systems αf and $f\beta^{-1}$ are represented, respectively, by the vectors

$$(\alpha(n_1), \alpha(n_2), \ldots, \alpha(n_b)) \quad \text{and} \quad \left(n_{\sigma(1)}, n_{\sigma(2)}, \ldots, n_{\sigma(b)}\right).$$

where $\sigma \in S_b$ is the permutation induced by the automorphism β on the set of indexes of the the fundamental pairs. After computing the action of both $\mathcal{L}_\mathcal{N}$ and $\mathcal{L}_\mathcal{Q}$ on the set of non-equivalent extensions, we take one representative for each orbit.

Let us now see how to apply this algorithms in order to find some a classification for Steiner triple systems of order 19, 27 or 31 containing Veblen points.

3.2 STS(19) with one Veblen point

By Theorem 2.5.2, which says there exists an STS(v) with (at least) $2^c - 1$ Veblen points if and only if $\frac{v+1}{2^c} \equiv 2, 4 \pmod 6$, we deduce that the number of Veblen points of an STS(19) is at most 1. The following result classify all such Steiner triple systems with Veblen points.

Theorem 3.2.1. *Among the* 11,084,874,829 *non-isomorphic* STS(19)*s, there are only* 3 *Steiner triple systems with (precisely) one Veblen point.*

Proof. If an STS(19) $\mathcal{S}$ has one Veblen point, then this point is the only non-trivial central element of the Steiner loop $\mathcal{L}_\mathcal{S}$. Hence, we can obtain $\mathcal{L}_\mathcal{S}$ as a Schreier extension of its center $\mathcal{L}_\mathcal{N}$, which is the group of order 2, by the unique Steiner loop $\mathcal{L}_\mathcal{Q}$ of order 10 corresponding to the STS(9). Since the order of $\mathcal{L}_\mathcal{N}$ is 2 and $\mathcal{Q}$ has 12 triples, the total number of possible factor systems in $\mathrm{Ext}_S(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})$ is $2^{12} = 4096$. Using Algorithm 9 in A, we computed the set of co-boundaries $\mathrm{B}^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N}) = \{\delta^1\varphi \mid \varphi\colon \mathcal{L}_\mathcal{Q} \to \mathcal{L}_\mathcal{N},\ \varphi(\bar{\Omega}) = \Omega\}$, which has order

$2^9 = 512$. Consequently, the number of non-equivalent extensions is 8, and we found the corresponding factor systems using Algorithm 10 in A. We note now that, since $\mathrm{Aut}(\mathcal{L}_\mathcal{N})$ is trivial, the action of the group $\mathrm{Aut}(\mathcal{L}_\mathcal{N}) \times \mathrm{Aut}(\mathcal{L}_\mathcal{Q})$ can be reduced to the action of just $\mathrm{Aut}(\mathcal{L}_\mathcal{Q}) = \mathrm{Aff}(2,3)$, which has order 432. We computed this group with Algorithm 14. The 8 equivalence classes of factor systems are divided, under this action, into 3 orbits, found explicitly using Algorithm 13. Each of these orbits represents one isomorphism class of extensions of $\mathcal{L}_\mathcal{N}$ by $\mathcal{L}_\mathcal{Q}$. Since $\mathcal{L}_\mathcal{N}$ is the whole center of $\mathcal{L}_\mathcal{S}$, these orbits correspond to the isomorphism classes of STS(19)s with precisely one Veblen point. □

In order to provide a full description of the Steiner triple systems of size 19 containing one Veblen point, let us fix the following presentation of the STS(9) as the affine plane $\mathrm{AG}(2,3)$, as in the next Figure 3.1.

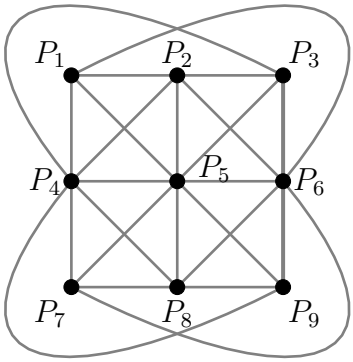

FIGURE 3.1: STS(9)

Let us denote the 3 non-isomorphic STS(19)s containing one Veblen point with $\mathcal{S}_i$, $i = 0, 1, 2$. The corresponding Steiner loops $\mathcal{L}_{\mathcal{S}_i}$ are given as Schreier extensions of $\mathcal{L}_\mathcal{N} = \{\Omega, 1\}$ by $\mathcal{L}_\mathcal{Q}$, by the following factor systems, respectively:

f_0, the null function;

f_1, defined by $f_1(P_3, P_6) = f_1(P_3, P_9) = f_1(P_6, P_9) = 1$, and Ω elsewhere;

f_2, defined by $f_2(P_3, P_6) = f_2(P_3, P_9) = f_2(P_6, P_9) = 1$,
$f_2(P_7, P_8) = f_2(P_7, P_9) = f_2(P_8, P_9) = 1$, and Ω elsewhere.

The following Figure 3.2 provides a visual representation of the non-trivial factor systems f_1 and f_2, where the triples of the STS(9) $\mathcal{Q}$ in which f_i is non-zero, $i = 1, 2$, are drawn in red.

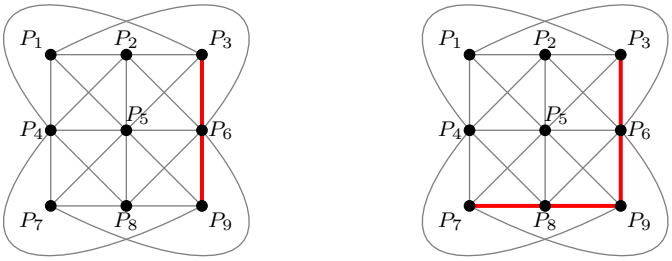

FIGURE 3.2: Factor systems f_1 (left) and f_2 (right)

Now we want to exhibit explicitly the points and triples of each of these Steiner triple systems $\mathcal{S}_i$, $i = 1, 2, 3$.

Since the factor systems f_0 is the null function, in the loop $\mathcal{L}_{\mathcal{S}_0}$ the operation is simply described by

$$(P_i, x) \circ (P_j, y) = (P_i P_j, x + y).$$

Hence the triples are given by the union of the following three families:

$$\begin{aligned}
&\big\{(P_i, \Omega),\ (P_j, \Omega),\ (P_i P_j, \Omega) \mid P_i, P_j \in \mathcal{Q},\ i \neq j\big\},\\
&\big\{(P_i, 1),\ (P_j, 1),\ (P_i P_j, \Omega) \mid P_i, P_j \in \mathcal{Q},\ i \neq j\big\},\\
&\big\{(P_i, 1),\ (P_i, \Omega),\ (\Omega, 1) \mid P_i \in \mathcal{Q}\big\}.
\end{aligned}$$

It is worth noticing that the first family has 12 triples, the second one has 36 and the third one has 9, for a total of 57, which is the exact number of triples of an STS(19). Renaming the elements as follows,

$$\begin{aligned}
0 &:= (\bar{\Omega}, 1) && \text{(the Veblen point)},\\
i &:= (P_i, \Omega), && i = 1, \ldots, 9\\
i + 9 &:= (P_i, 1), && i = 1, \ldots, 9
\end{aligned}$$

we obtain the representation of the STS(19) $\mathcal{S}_0$ as in the table 3.2, where each column corresponds to one triple.

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

2	2	2	2	2	3	3	3	3	3	3	3	4	4	4	4	4	5	5
6	10	13	14	15	4	5	6	10	13	14	15	5	10	11	12	14	10	11
7	12	18	17	16	8	7	9	11	17	16	18	6	16	18	17	15	18	17

5	5	6	6	6	6	7	7	7	7	7	8	8	8	8	9	9	9	9
12	13	10	11	12	13	8	10	11	12	17	10	11	12	16	10	11	12	16
16	15	17	16	18	14	9	13	15	14	18	15	14	13	18	14	13	15	17

TABLE 3.2: STS(19) $\mathcal{S}_0$ with one Veblen point

Since the factor systems f_1 is zero everywhere except for any pair of points in the triple $\{P_3, P_6, P_9\}$ of the STS(9) $\mathcal{Q}$, the operation in $\mathcal{L}_{\mathcal{S}_1}$ is the same as in $\mathcal{L}_{\mathcal{S}_0}$ except for:

$$(P_3,\Omega)\circ(P_6,\Omega)\circ(P_9,1)=(\bar{\Omega},\Omega),\quad (P_3,\Omega)\circ(P_6,1)\circ(P_9,\Omega)=(\bar{\Omega},\Omega),$$
$$(P_3,1)\circ(P_6,\Omega)\circ(P_9,\Omega)=(\bar{\Omega},\Omega),\quad (P_3,1)\circ(P_6,1)\circ(P_9,1)=(\bar{\Omega},\Omega).$$

Hence the triples of $\mathcal{S}_1$ are obtained by those of $\mathcal{S}_0$ by performing the *Pasch switch* corresponding to replacing the triples $\{3,6,9\}$, $\{3,15,18\}$, $\{6,12,18\}$ and $\{9,12,15\}$ with the triples $\{3,6,18\}$, $\{3,15,9\}$, $\{6,9,12\}$ and $\{12,15,18\}$, as in Figure 3.3.

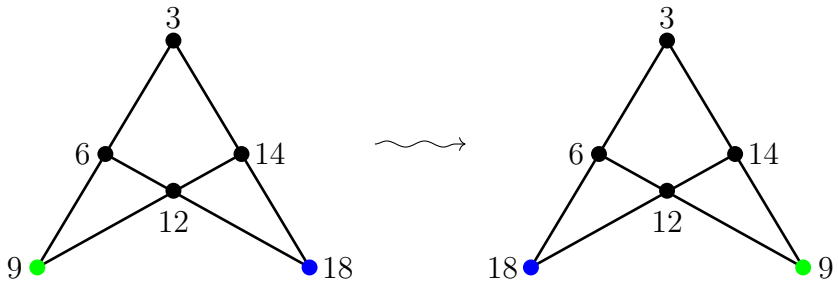

FIGURE 3.3: Pasch switch

We provide the representation of the STS(19) $\mathcal{S}_1$ shown in the table 3.3, where each column corresponds to one triple.

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

2	2	2	2	2	3	3	3	3	3	3	3	4	4	4	4	4	5	5
6	10	13	14	15	4	5	6	9	10	13	14	5	10	11	12	14	10	11
7	12	18	17	16	8	7	18	15	11	17	16	6	16	18	17	15	18	17

5	5	6	6	6	6	7	7	7	7	7	8	8	8	8	9	9	9	12
12	13	9	10	11	13	8	10	11	12	17	10	11	12	16	10	11	16	15
16	15	12	17	16	14	9	13	15	14	18	15	14	13	18	14	13	17	18

TABLE 3.3: STS(19) $\mathcal{S}_1$ with one Veblen point

Since the factor system f_2 coincides with f_1 everywhere except for any two points in the triple $\{P_7, P_8, P_9\}$ of the STS(9) $\mathcal{Q}$, the operation in $\mathcal{L}_{\mathcal{S}2}$ is the

same as in $\mathcal{L}_{\mathcal{S}1}$ except for

$$(P_7, \Omega) \circ (P_8, \Omega) \circ (P_9, 1) = (\bar{\Omega}, \Omega'),$$
$$(P_7, \Omega) \circ (P_8, 1) \circ (P_9, \Omega) = (\bar{\Omega}, \Omega'),$$
$$(P_7, 1) \circ (P_8, \Omega) \circ (P_9, \Omega) = (\bar{\Omega}, \Omega'),$$
$$(P_7, 1) \circ (P_8, 1) \circ (P_9, 1) = (\bar{\Omega}, \Omega').$$

Hence the triples of $\mathcal{S}_2$ are obtained by those of $\mathcal{S}_1$ by the *Pasch switch* corresponding to substituting the triples $\{7, 8, 9\}$, $\{7, 17, 18\}$, $\{8, 16, 18\}$ and $\{9, 16, 17\}$ with the triples $\{7, 8, 18\}$, $\{7, 9, 17\}$, $\{8, 9, 16\}$ and $\{16, 17, 18\}$, as in Figure 3.4.

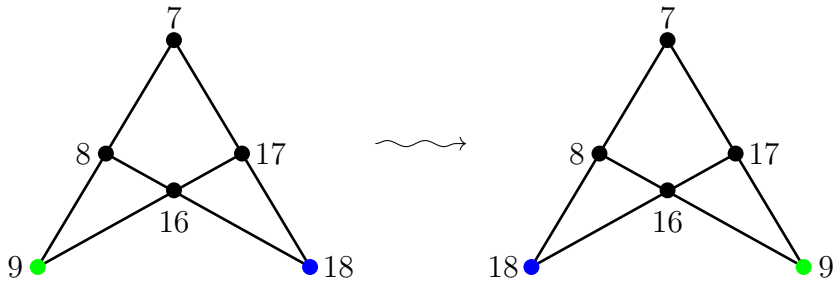

FIGURE 3.4: Pasch switch

We provide the representation of the STS(19) $\mathcal{S}_2$ shown in the table 3.4, where each column corresponds to one triple.

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

2	2	2	2	2	3	3	3	3	3	3	3	4	4	4	4	4	5	5
6	10	13	14	15	4	5	6	9	10	13	14	5	10	11	12	14	10	11
7	12	18	17	16	8	7	18	15	11	17	16	6	16	18	17	15	18	17

5	5	6	6	6	6	7	7	7	7	7	8	8	8	8	9	9	12	16
12	13	9	10	11	13	8	9	10	11	12	9	10	11	12	10	11	15	17
16	15	12	17	16	14	18	17	13	15	14	16	15	14	13	14	13	18	18

TABLE 3.4: STS(19) $\mathcal{S}_2$ with one Veblen point

3.3 STS(27) with one Veblen point

Again, using the formula $\frac{v+1}{2^c} \equiv 2, 4 \pmod 6$, we deduce that the number of Veblen points of an STS(v), with $v = 27$, is at most 1. Hence, we can obtain $\mathcal{L}_{\mathcal{S}}$ as a Schreier extension of its center $\mathcal{L}_{\mathcal{N}}$, which is the group of order 2, by a Steiner loop $\mathcal{L}_{\mathcal{Q}}$ of order 14 corresponding to one of the two non-isomorphic

STS(13)s. The following Theorem determines the number of such STS(27)s, investigating both cases for the quotient system $\mathcal{Q}$.

Theorem 3.3.1. *There are* 1736 *non-isomotphic* STS(27)*s containing one Veblen point, among which* 1504 *present the non-cyclic* STS(13) *as the quotient system, and* 232 *present the cyclic* STS(13) *as the quotient system.*

Proof. Let $\mathcal{S}$ be an STS(27) with one Veblen point, let $\mathcal{L}_\mathcal{N}$ be the center of $\mathcal{L}_\mathcal{S}$ and $\mathcal{L}_\mathcal{Q}$ the corresponding quotient loop. Since $\mathcal{L}_\mathcal{N}$ has order 2 and $\mathcal{Q}$ has 26 triples, the total number of all possible factor systems in $\mathrm{Ext}_S(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})$ is 2^{26}. Using Algorithm 9 in A, we computed the set of co-boundaries $\mathrm{B}^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N}) = \{\delta^1\varphi \mid \varphi\colon \mathcal{L}_\mathcal{Q} \to \mathcal{L}_\mathcal{N},\ \varphi(\bar{\Omega}) = \Omega\}$, which has order 2^{13}. Consequently, the number of non-equivalent extensions is 2^{13}, and we computed them using Algorithm 10 in A. We note now that, since $\mathrm{Aut}(\mathcal{L}_\mathcal{N})$ is trivial, the action of the group $\mathrm{Aut}(\mathcal{L}_\mathcal{N}) \times \mathrm{Aut}(\mathcal{L}_\mathcal{Q})$ can be reduced to the action of just $\mathrm{Aut}(\mathcal{L}_\mathcal{Q})$, which we computed using Algorithm 2.

If $\mathcal{Q}$ is the non-cyclic STS(13) (see [19, Table II.1.27, n. 1]), then $\mathrm{Aut}(\mathcal{L}_\mathcal{Q})$ is the symmetric group Sym(3) (see [77]). Under its action, the set of non-equivalent extensions is divided into 1504 orbits, computed using Algorithm 13. Each of these orbits represents one isomorphism class of extensions of $\mathcal{L}_\mathcal{N}$ by $\mathcal{L}_\mathcal{Q}$. Since $\mathcal{L}_\mathcal{N}$ is the center of $\mathcal{L}_\mathcal{S}$, these orbits are exactly the isomorphism classes of STS(27)s with one Veblen point and quotient system the non-cyclic STS(13).

Let now $\mathcal{Q}$ be the cyclic STS(13) (see [19, Table II.1.27, n. 2]), then $\mathrm{Aut}(\mathcal{L}_\mathcal{Q})$ is the unique non-abelian group of order 39 F_{39} (see [77]). Under its action, the set of non-equivalent extension is divided into 232 orbits, computed using Algorithm 13. Each of these orbits represents one isomorphism class of extensions of $\mathcal{L}_\mathcal{N}$ by $\mathcal{L}_\mathcal{Q}$. Since $\mathcal{L}_\mathcal{N}$ is the center of $\mathcal{L}_\mathcal{S}$, these orbits are exactly to the isomorphism classes of STS(27)s with one Veblen point and quotient system the cyclic STS(13). □

3.4 STS(31) with one or three Veblen points

Lastly, using the formula $\frac{v+1}{2^c} \equiv 2, 4 \pmod 6$ and the fact that an STS(v) with more than $\frac{v-7}{8}$ Veblen points is a projective geometry, we deduce that the number of Veblen points of an STS(31) can be either one, three, or thirty-one. In the last case, the Steiner triple system is the point-line design of the projective geometry PG(4, 2), thus we confine ourselves to the cases of STS(31)s with one or three Veblen points.

If a Steiner triple system of size 31 contains one Veblen point, then the corresponding quotient system $\mathcal{Q}$ is an STS(15). Since there are 80 possibilities for such a quotient system (see [19]), we focus our attention on six cases that in our opinion are the most interesting, namely:

1. STS(15) #1, that is PG(3, 2);
2. STS(15) #2, which is the only other one with a Veblen point itself;

3. STS(15) #3, which is the one with the largest number of Pasch configurations without containing Veblen points;

4. STS(15) #7, which is the one with the second-largest automorphism group after PG(3, 2));

5. STS(15) #61, which, among the ones containing a Fano plane, is the one with the least number of Pasch configurations;

6. STS(15) #80, which is the only one containing no Pasch configurations.

Theorem 3.4.1. *The number of non-isomorphic* STS(31)*s with precisely one Veblen point and given quotient system* $\mathcal{Q}$ *of order* 15 *is:*

$\mathcal{Q}$	count
PG(3, 2)	278
STS(15)#2	48072
STS(15)#3	47744
STS(15)#7	16520
STS(15)#61	99952
STS(15)#80	17888

TABLE 3.5: STS(31)s with one Veblen point and corresponding quotient system $\mathcal{Q}$

Proof. Let $\mathcal{S}$ be an STS(31) with (at least) 1 Veblen point. We can obtain the Steiner loop $\mathcal{L}_\mathcal{S}$ as a Schreier extension of its central subloop $\mathcal{L}_\mathcal{N}$ corresponding to the given Veblen point by a Steiner loop $\mathcal{L}_\mathcal{Q}$ of order 16 corresponding to one of the eighty STS(15)s. Since $\mathcal{L}_\mathcal{N}$ has order 2 and $\mathcal{Q}$ has 35 triples, in any case, the total number of all possible factor systems in $\mathrm{Ext}_S(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})$ is 2^{35}.

Using Algorithm 9 in A, we computed, in every case, the set of co-boundaries $\mathrm{B}^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N}) = \{\delta^1\varphi \mid \varphi\colon \mathcal{L}_\mathcal{Q} \to \mathcal{L}_\mathcal{N},\ \varphi(\bar{\Omega}) = \Omega\}$, whose order is listed in the following table 3.6.

$\mathcal{Q}$	$\lvert\mathrm{B}^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})\rvert$
PG(3, 2)	2^{11}
STS(15)#2	2^{12}
STS(15)#3	2^{13}
STS(15)#7	2^{13}
STS(15)#61	2^{14}
STS(15)#80	2^{15}

TABLE 3.6: Number of coboundaries for the corresponding $\mathcal{Q}$

We computed the associated factor system using Algorithm 10 in A.

We note now that, since $\mathrm{Aut}(\mathcal{L}_\mathcal{N})$ is trivial, the action of the group $\mathrm{Aut}(\mathcal{L}_\mathcal{N}) \times \mathrm{Aut}(\mathcal{L}_\mathcal{Q})$ can be reduced to the action of just $\mathrm{Aut}(\mathcal{L}_\mathcal{Q})$. We computed this group in every case using Algorithm 3. The possible orders of this group are listed in the following table 3.7.

$\mathcal{Q}$	$\lvert\mathrm{Aut}(\mathcal{Q})\rvert$
PG(3, 2)	20160
STS(15)#2	192
STS(15)#3	96
STS(15)#7	288
STS(15)#61	21
STS(15)#80	60

TABLE 3.7: Order of the automorphism group of $\mathcal{Q}$

Under this action, the equivalence classes of factor systems are divided into 1240 orbits for the STS(15) #1, 48080 for #2, 47744 for #3, 16520 for #7, 99952 for #61, and 17888 for #80, computed using Algorithm 15. These orbits are exactly the isomorphism classes of extensions of $\mathcal{L}_{\mathcal{N}}$ by $\mathcal{L}_{\mathcal{Q}}$.

Since STS(15) #3, 7, 61, 80 have no Veblen points, in these cases $\mathcal{L}_{\mathcal{N}}$ is the whole center of $\mathcal{L}_{\mathcal{S}}$. This implies that the isomorphism classes of extension coincide with the isomorphism classes of the corresponding STS(31)s. In conclusion we can say that, for these four cases, the numbers listed above are exactly the numbers of non-isomorphic STS(31)s with precisely one Veblen point and factor system $\mathcal{Q}$.

For the STS(15)s #1 and 2, the situation is different, due to the fact that they have Veblen points as well. This means that $\mathcal{L}_{\mathcal{N}}$ could be (in general) just a proper subgroup of the center of $\mathcal{L}_{\mathcal{S}}$, that is, $\mathcal{S}$ could have more than 1 Veblen point. Therefore, the isomorphism classes of extension do not coincide, in these two cases, with the isomorphism classes of the corresponding STS(31)s. For this reason we need a further reduction, in order to cut out all the factor systems which produce an STS(31) with more than 1 Veblen point. As seen in Remark 2.6.1, we need to count just the factor systems f for which does not exist any point $P \in \mathcal{Q}$ that fulfills the following condition

$$f(P,Q) + f(PQ,R) = f(Q,R) + f(P,QR),$$

for every $Q, R \in \mathcal{Q}$. Using Algorithm 16, we performed this analysis on all the 1240 factor systems for the case #1 as well as on all the 48080 factor systems for the case #2. Since the STS(15) #1 is a projective geometry, this study needs to be done considering all the points of the Steiner triple system. For the STS(15) #2 we can consider just the point labeled with 0 (see [19, Table 1.28, p. 30]) since, in this case, it is the only Veblen point. After the computation, we found out that there are 278 non-isomorphic STS(31)s with precisely 1 Veblen point and corresponding quotient system the STS(15) #1 and 48072 non-isomorphic STS(31)s with precisely 1 Veblen point and corresponding quotient system the STS(15) #2.

□

As we observed in this last case of an STS(31) with precisely one Veblen point, the problem of constructing all Steiner triple systems of given size and number of Veblen points using Schreier extensions becomes progressively challenging with size growth, in particular when the ratio of the order and the

number of Veblen points becomes larger. This is due to the fact that, if the number of Veblen points is relatively small, the number of non-isomorphic cases for the quotient system $\mathcal{Q}$ increases sensibly. Indeed, the problem of STS(31)s with 3 number of Veblen points is way easier to deal with, as shown in the next result.

Theorem 3.4.2. *There are only* 2 *non-isomorphic* STS(31)*s with precisely three Veblen points.*

Proof. Let $\mathcal{S}$ be an STS(31) with (at least) 3 Veblen points. We can obtain the Steiner loop $\mathcal{L}_\mathcal{S}$ as a Schreier extension of its central subloop $\mathcal{L}_\mathcal{N}$ corresponding to the given 3 Veblen points, which is the elementary abelian 2-group of order 4, by the unique Steiner loop $\mathcal{L}_\mathcal{Q}$ of order 8 corresponding to the STS(7). Since $\mathcal{L}_\mathcal{N}$ has order 4 and $\mathcal{Q}$ has 7 triples, the total number of all possible factor systems in $\mathrm{Ext}_S(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})$ is $4^7 = 16383$. Using Algorithm 9 in A, we computed the set of co-boundaries $\mathrm{B}^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N}) = \{\delta^1\varphi \mid \varphi\colon \mathcal{L}_\mathcal{Q} \to \mathcal{L}_\mathcal{N},\ \varphi(\bar{\Omega}) = \Omega\}$, which has order $2^8 = 256$. Consequently, the number of non-equivalent extensions is $2^6 = 64$, and we explicitly found them using Algorithm 10 in A. The group $\mathrm{Aut}(\mathcal{L}_\mathcal{N}) \times \mathrm{Aut}(\mathcal{L}_\mathcal{Q})$ is $\mathrm{PGL}(2,2) \times \mathrm{PGL}(3,2)$, which has order 1008. Under its action,the 64 equivalence classes of factor systems are divided into 3 orbits, computed using Algorithm 13. Each of these orbits represents one isomorphism class of extensions of $\mathcal{L}_\mathcal{N}$ by $\mathcal{L}_\mathcal{Q}$.

Since $\mathcal{Q}$ has Veblen points itself, $\mathcal{L}_\mathcal{N}$ could be, in general, a proper subgroup of the center of $\mathcal{L}_\mathcal{S}$. Hence $\mathcal{S}$ could have more than 3 Veblen points, and that would be the case where it is $\mathrm{PG}(4,2)$. Therefore, these orbits do not necessarily coincide with the isomorphism classes of STS(19)s with three Veblen points. We need to perform an analysis to see if some of these 3 resulting factor systems produce a projective geometry.

In order to do this, let us to describe explicitly the three obtained factor systems. We see $\mathcal{L}_\mathcal{N}$ as $\mathrm{GF}(2)^2$ and $\mathcal{L}_\mathcal{Q}$ as $\mathrm{GF}(2)^3$, and we give the Fano plane $\mathcal{Q}$ the following coordinates:

$$P_1 = [0,0,1], \quad P_2 = [0,1,0], \quad P_3 = [0,1,1], \quad P_4 = [1,0,0],$$

$$P_5 = [1,0,1], \quad P_6 = [1,1,0], \quad P_7 = [1,1,1].$$

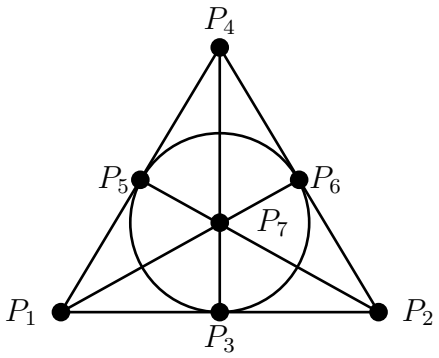

FIGURE 3.5: Fano plane

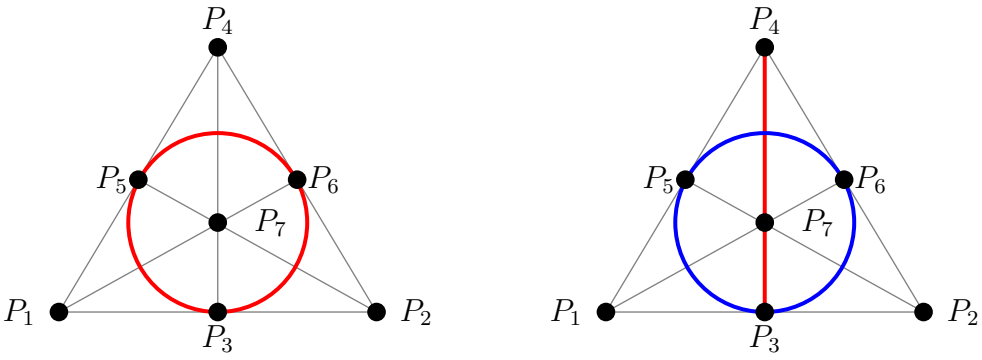

FIGURE 3.6: The factor systems f_1 (left) and f_2 (right)

The three orbits that we obtained, are represented, respectively, by the following three factor systems:

f_0, the null function;
f_1, defined by $f_1(P_3, P_5) = f_1(P_3, P_6) = f_1(P_5, P_6) = (0, 1)$, and Ω elsewhere;
f_2, defined by $f_2(P_3, P_4) = f_2(P_3, P_7) = f_2(P_4, P_7) = (0, 1)$,
$f_2(P_3, P_5) = f_2(P_3, P_6) = f_2(P_5, P_6) = (1, 0)$ and Ω elsewhere.

The Steiner loop defined by the null factor system f_0 is a group, hence the corresponding STS(31) is PG$(4, 2)$, which has 31 Veblen points.

The following figure 3.6 provides a visual representation of the non-trivial factor systems f_1 and f_2, where the triples of $\mathcal{Q}$ in which f_i is equal to $(0, 1)$ are drawn in red, and the ones in which f_i is equal to $(1, 0)$ are drawn in blue, $i = 1, 2$.

For $i = 1, 2$, it is easy to check by hand that for any $P \in \mathcal{Q}$, no element of the form (P, x) can be a Veblen point of $\mathcal{S}_i$ since the following condition is never satisfied:

$$f_i(P, Q) + f_i(PQ, R) = f_i(Q, R) + f_i(P, QR) \quad \text{for every } Q, R \in \mathcal{Q}.$$

Hence, $\mathcal{L}_\mathcal{N}$ is in both cases the whole center of $\mathcal{L}_{\mathcal{S}_i}$, $i = 1, 2$. In conclusion, there are only 2 non-isomorphic STS(31)s with precisely 3 Veblen points. □

The two non-trivial factor systems defined in the proof of Theorem 3.4.2 give a compact representation of all the 155 triples of each of the two STS(31)s with exactly 3 Veblen points.

Chapter 4

An extension formula for right Bol loops arising from Bol reflections

In this chapter we are going to work with right Bol loops, and for this reason in is more convenient to use the right notation. For example, if α is a map defined on a loop L, then x^α is the image of x under α. Moreover, $x^{\alpha\beta} = (x^\alpha)^\beta$, meaning that in the composition of two maps $\alpha\beta$, we first apply α and consequently β.

We recall that a loop is called a *right Bol* loop if it satisfies the following identity for all $x, y, z \in L$:

$$(((xy)z)y) = x((yz)y). \tag{4.1}$$

Equivalently, $R_y R_z R_y = R_{yz\cdot y}$ for every $y, z \in L$. A loop is said to be *right conjugacy closed* if $R_x R_y R_x^{-1} = R_{xy/x}$ holds for all x, y, z.

In right Bol loops, the right and middle nuclei coincide, and in Moufang loops, they coincide with the left nucleus as well. In groups, the commutant is the same as the center, hence normal. In Moufang loops, the commutant is a subloop, but not necessarily normal ([43]). However, there are infinite classes of right Bol loops, in which the commutant is not even a subloop ([57]).

This chapter deals with a new extension formula for right Bol loops. Let $(L, \cdot)$ be such a loop, and let

$$\mathcal{T} = \{t_a \mid a \in L\},$$
$$\mathcal{V} = \{v_a \mid a \in L\},$$

be two disjoint copies of L. If we define a product on $\widetilde{L} = \mathcal{T} \cup \mathcal{V}$ by

$$t_a \cdot t_b = t_{ab}, \quad t_a \cdot v_b = v_{ab}, \quad v_a \cdot t_b = v_{ab^{-1}}, \quad v_a \cdot v_b = t_{ab^{-1}}. \tag{4.2}$$

then we have that $(\widetilde{L}, \cdot)$ is a loop with unit t_1, and $\mathcal{T}$ is a normal subloop of index 2, isomorphic to L.

The *core* of a right Bol loop is the binary operation

$$x + y = (yx^{-1})y. \tag{4.3}$$

It satisfies the identities

$$x + x = x \qquad \text{(idempotent)}, \tag{4.4}$$
$$(x + y) + y = x \qquad \text{(involutorial)}, \tag{4.5}$$
$$(x + y) + z = (x + z) + (y + z) \qquad \text{(right distributive)}, \tag{4.6}$$

A binary structure with these properties is also called an *involutorial quandle.* Quandles (see Definition 4.6.1) are algebraic structures associated to knots: given a finite quandle and a cocycle, one can construct a knot invariant. Involutorial quandles are also called abstract symmetric spaces (in the sense of Loos [62]).

Not all involutorial quandles happen to be the core of some right Bol loop. For example, if the core of $(L, \cdot)$ is a trivial involutorial quandle, that is $x+y = x$ for all x, y, then L has to be an elementary abelian 2-group. Hence, a trivial involutorial quandle whose order is not a 2-power cannot be the core of a right Bol loop.

Problem 4.0.1. Let $(Q, \triangleleft)$ be an involutorial quandle. Find necessary or sufficient conditions for the existence of a right Bol loop whose core is isomorphic to $(Q, \triangleleft)$.

This problem is settled for finite involutorial quandles of odd order: they are the core of a right Bol loop if and only if they are quasigroups, see [54, Theorem 6.14]. Notice that an involutorial quandle is a quasigroup if and only if its left multiplication maps $x \mapsto a + x$ are invertible.

Let us call the $(Q, \triangleleft)$ a *RB-quandle,* if it is the core of some right Bol loop $(Q, \cdot)$. One future long term goal could be to study RB-quandles which are disjoint unions of two proper RB-subquandles. The right Bol loop extension $\widetilde{L}$ has some relevant property. Indeed, in the case where $\widetilde{L}$ is a right Bol loop, its core decomposes to the disjoint union of two subquandles both isomorphic to the core of L.

The structure of this chapter is as follows. First, we give the necessary definitions and properties. Our focus is on the geometric and group theoretical tools, which enable us to use Aschbacher's efficient Bol loop folder method to study the extension. In Section 4.4, we study $\widetilde{L}$ and derive conditions for it to be right Bol, Moufang or associative. Surprisingly enough, $\widetilde{L}$ cannot be a proper Moufang loop, but only a group (see Theorem 4.4.1). In Section 4.5, we prove results on the center as well as on the right and the left nuclei. Finally, in Section 4.6, we prove Theorem 4.6.2 about the core of the extension and find further results on its structure group.

4.1 Loop folders

In [3], Aschbacher studied the correspondence between loops and certain triples of group theoretic data in order to investigate finite loops using techniques from finite group theory.

Let L be a loop, $K = \{R_x \mid x \in L\}$ be the set of right translations of L, $G = \langle K \rangle$ be the right multiplication group of L, and $H = G_1$ the stabilizer of the unit 1 of L. The triple $\epsilon(L) = (G, H, K)$ is called the *envelope* of the loop L. It is known that a loop L with envelope $\epsilon(L)$ is a Bol loop if and only if K is a twisted subgroup of G.

Definition 4.1.1. A *loop folder* is a triple $\xi = (G, H, K)$ where G is a group, H is a subgroup of G and K is a subset of G containing 1 such that K is a set of coset representatives for $G/H^g = \{H^g x \mid x \in G\}$ for each $g \in G$.

A morphism $\xi \to \xi'$ of loop folders $\xi = (G, H, K)$ and $\xi' = (G', H', K')$ is a group homomorphism $\pi\colon G \to G'$ such that $H^\pi \leq H'$ and $K^\pi \subseteq K'$.

A folder is said *faithful* if $\ker_H(G) = 1$, that is, if G acts faithfully on the set $\{Hx \mid x \in G\}$. A *loop envelope* is a loop folder (G, H, K) such that $G = \langle K \rangle$. If L is a loop, then $\epsilon(L) = (G, H, K)$ is a faithful loop envelope.

Let $\xi = (G, H, K)$ be a loop folder and define a binary operation $*$ on K by taking $a * b$ to be the unique element in K such that $H(a * b) = H(ab)$. Then $\ell(\xi) := (K, *)$ is a loop with identity the unit 1 of G. The loop $\ell(\xi)$ is called the *loop of the loop folder* ξ. For $\pi\colon \xi \to \xi'$ a homomorphism of loop folders, define $\ell(\pi)\colon \ell(\xi) \to \ell(\xi')$ as the restriction of π to K.

If L is a loop, then $\ell(\epsilon(L)) \cong L$. Moreover, for a faithful loop envelope ξ, one has $\epsilon(\ell(\xi)) \cong \xi$.

Let G be a group acting transitively on a set Q. The subset $S \subseteq G$ is *sharply transitive set,* if for any $x, y \in Q$ there is a unique $s \in S$ such that $x^s = y$. The set $R(L) = \{R_a \mid a \in L\}$ of the right translations of a loop L is a sharply transitive on L and contains the identity $\mathrm{Id} = R_1$.

Definition 4.1.2. Let $S \subseteq G$ be a sharply transitive set on Q, $1 \in S$. Fix an element $e \in Q$. Then $\xi = (G, G_e, S)$ is a loop folder. The associated loop $\ell(\xi)$ will be denoted by $\lambda(G, S, e)$.

The operation of $\lambda(G, S, e)$ can be given as follows: $x * y := x^s$, where $s \in S$ such that $e^s = y$ for every $x, y \in Q$.

Finally, notice that $\ell(G, H, K)$ is a right Bol loop if and only if for all $a, b \in K$, $a^{-1}, aba \in K$. In this case, (G, H, K) is called a *Bol loop folder.*

4.2 Moufang loops by Chein extension

In [16], Chein showed a general method of constructing non-associative Moufang loops as extensions of non-abelian groups by the cyclic group of order 2. In the context of the next theorem, a set of generators is called *minimal* if it contains the smallest number of elements, and not if no proper subset is a set of generators.

Theorem 4.2.1. *[16] If L is a non-associative Moufang loop for which every minimal set of generators contains an element of order 2, then there exist a non-abelian group G and an element $x \in L$ of order 2 such that each element*

of L may be expressed in the form gx^α, where $g \in G$, $\alpha = 0, 1$, and the product of two elements of L is given by

$$\left(g_1 x^\delta\right)\left(g_2 x^\epsilon\right) = \left(g_1^\nu g_2^\mu\right) x^{\delta+\epsilon}.$$

where $\nu = (-1)^\epsilon$ and $\mu = (-1)^{\delta+\epsilon}$.

Conversely, given any non-abelian group G, the loop constructed as indicated above is a non-associative Moufang loop.

The Moufang loop of order $2n$ arising as from a group G of order n as in Theorem 4.2.1 is denoted by $M_{2n}(G, 2)$. Chein's purpose was to find all non-associative Moufang loop of order ≤ 31. The choice of this stopping point is not casual. Indeed, in order to find the Moufang loops of order n with his method one needs to know the groups of order $\leq \frac{n}{2}$, and while the group of order ≤ 15 are well known, the ones of order 16 or larger start to become wild.

We can express Chein's formula so that it can be compared to (4.2). Replacing g with t_g and gx with v_g, we have, for every $g, h \in G$

$$t_g t_h = t_{gh}, \quad t_g v_h = v_{g^{-1}h^{-1}}, \quad v_g t_h = v_{gh^{-1}}, \quad v_g v_h = t_{g^{-1}h}. \tag{4.7}$$

Conversely, (4.2) can also be reformulated for a direct comparison with Chein's formula. We identify t_a with a and denote v_1 with x. Then, every $\ell \in \widetilde{L}$ can be written as ax^ϵ, with $\epsilon = 0, 1$, and the product becomes

$$(ax^\delta)(bx^\epsilon) = (ab^\mu)x^{\delta+\epsilon}, \tag{4.8}$$

with $\mu = (-1)^\delta$.

4.3 Nets and Bol reflections

This section has the aim of introducing the concept of a *3-net*, specifically of a 3-net associated with a loop, and showing some relations between these two items are related. For further information on 3-nets and loops, interested readers can refer to [81] or [74]. An incidence structure is a triple $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ where $\mathcal{P}$ and $\mathcal{L}$ are sets whose elements are called points and lines, respectively, and $\mathcal{I}$ is a subset of the product $\mathcal{P} \times \mathcal{L}$. A point P and a line ℓ are called *incident* if $(P, \ell) \in \mathcal{I}$.

Definition 4.3.1. A *3-net* $\mathcal{N}$ is an incidence structure $(\mathcal{P}, \mathcal{L}, \in)$ in which a point P and a line ℓ are incident if and only if $P \in \ell$, satisfying the following axioms.

1. $\mathcal{P} \neq \emptyset$.
2. $\mathcal{L}$ is the union of 3 families (*pencils*), namely the *horizontal*, *vertical* and *transversal* lines, such that:
   (i) the lines from each pencil partition $\mathcal{P}$;
   (ii) two lines of distinct pencils have a unique point in common.

3. Every line has exactly $n = |\mathcal{P}|$ points.

We denote the families of horizontal, vertical, and transversal lines, respectively, by $\mathcal{H}$, $\mathcal{V}$, and $\mathcal{T}$. A *collineation* of a 3-net is a bijection on both $\mathcal{P}$ and $\mathcal{L}$ which preserves the incidence relations between points and lines.

It is well known that any loop L can be associated with a 3-net $\mathcal{N}(L)$ where the set of points is $\mathcal{P} = L \times L$, and the lines given by:

$$\begin{aligned}\mathcal{H} &= \big\{h_a = \{(x, y) \mid y = a\} \mid a \in L\big\},\\ \mathcal{V} &= \big\{v_b = \{(x, y) \mid x = b\} \mid b \in L\big\},\\ \mathcal{T} &= \big\{t_c = \{(x, y) \mid xy = c\} \mid c \in L\big\}.\end{aligned}$$

Conversely, to any 3-net corresponds an isotopy class of loops (cf. [4], p. 10 and [5], p. 20).

The most common way to represent the points of the 3-net $\mathcal{N}(L)$ is to use their usual two coordinates (a, b). However, when computing with collineations, representing points by three coordinates such as (a, b, ab) can be more convenient. In this way, we can keep track of all the three lines containing the given points, which are h_a, v_b, and t_{ab}.

Let us now fix an arbitrary horizontal line h_d. For each point $P = (a, b) \in \mathcal{P}$, consider the vertical line v_a and the transversal line t_{ab} incident in P. In particular v_a and t_{ab} intersect h_d, respectively, in the points $Q = (a, d)$ and $R = (ab/d, d)$. The intersection between the transversal line through Q and the vertical line through R consists of the point $P' = (ab/d, u)$, with $u \in L$ depending on a, b and d, and fulfilling the equation

$$(ab)/d \cdot u = ad. \tag{4.9}$$

The next figure provides a visual representation of these points and lines.

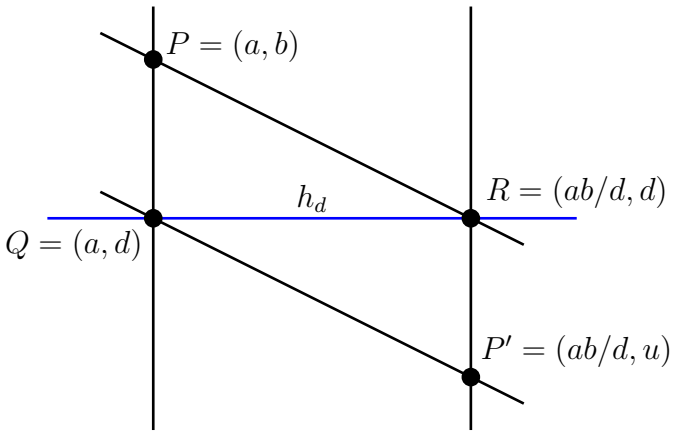

FIGURE 4.1: Bol reflection through the line h_d

For any $d \in L$, the map

$$\sigma_d \colon (a, b) \mapsto \big((ab)/d,\ u(a, b, d)\big)$$

is called the *Bol reflection* through the line h_d. A Bol reflection is a collineation of the 3-net $\mathcal{N}(L)$ if, and only if, the corresponding element u in the image of a point $P = (a, b)$ does not depend on the first coordinate of P. This means that the whole line h_b is mapped into the line h_u.

It is easy to prove that the Bol reflections σ_d are collineations of the 3-net $\mathcal{N}(L)$ exactly when L is a right Bol loop. In this case, for any $d \in L$, the Bol reflection σ_d is given by the map

$$\sigma_d \colon (x, y, xy) \longmapsto \left(xy \cdot d^{-1},\ dy^{-1} \cdot d,\ xd\right). \tag{4.10}$$

Since in a right Bol loop L the property $(ab \cdot a)^{-1} = a^{-1}b^{-1} \cdot a^{-1}$ holds for every $a, b \in L$, we have that each Bol reflection σ_d has order 2. In particular, the Bol reflection through the horizontal line containing the unit of L is

$$\sigma_1 \colon (x, y, xy) \longmapsto \left(xy,\ y^{-1},\ x\right). \tag{4.11}$$

Its action consist of swapping the first and third coordinates and inverting the second. If we compute the composition $\sigma_1\sigma_d$ we obtain the following map

$$\sigma_1\sigma_d \colon (x, y, xy) \longmapsto \left(xd^{-1},\ dy \cdot d,\ xy \cdot d\right), \tag{4.12}$$

which coincides with the autotopism $(R_d^{-1},\ L_dR_d,\ R_d)$ of the right Bol loop L. It is easy to check that for every $d \in L$, $\sigma_d\sigma_1 = \sigma_1\sigma_{d^{-1}}$.

Let us consider the following sets

$$\Sigma := \{\sigma_d,\ \sigma_1\sigma_d \mid d \in L\} \quad \text{and} \quad \Sigma_0 := \{\sigma_d \mid d \in L\}.$$

Σ_0 is invariant under conjugation by all collineations that preserves the pencil $\mathcal{H}$. For proper Bol loops, these are all the collineations of the associated 3-net. In general, we can say that Σ_0 is invariant under the *direction preserving collineations*. The group Γ generated by Σ_0 is a subgroup of the full group of the collineations, and its subgroup $G := \langle \sigma_1\sigma_d \mid d \in L \rangle$ is a subgroup of the full group of autotopisms of L. The reader is referred to [69] or [37] for insights into the collineation group.

4.4 Algebraic properties of the extension

In this section, L is a right Bol loop, with associated 3-net $\mathcal{N}$. The vertical and transversal lines are $v_b : x = b$ and $t_c : xy = c$. The sets of transversal and vertical lines of $\mathcal{N}$ are $\mathcal{T}$, $\mathcal{V}$. The Bol reflection on the horizontal line $y = a$ is denoted by σ_a. We will prove the following result.

Theorem 4.4.1. *$\widetilde{L}$ is a Bol loop if and only if L is right conjugacy closed right Bol loop with $x^2 \in Z(L)$ for every $x \in L$. Moreover, the following are equivalent:*

(i) $\widetilde{L}$ is Moufang.

(ii) $\widetilde{L}$ is associative.

(iii) L is an abelian group.

The class of right conjugacy closed right Bol loops with central squares contains the class of Bol loops of exponent 2. The latter is a very rich class, containing simple proper finite Bol loops of exponent 2 ([3], [68]). Right conjugacy closed Moufang loops are also called *extra loops* ([34], [35]). In extra loops, all squares are in the nucleus. An important subclass is the class of *code loops,* which are related to doubly even binary linear codes ([70], [41], [48]).

Lemma 4.4.2. *The subset*

$$\Sigma = \{\sigma_d,\ \sigma_1\sigma_d \mid d \in L\}$$

of the group $\Gamma = \langle \sigma_d \mid d \in L\rangle$ *is a sharply transitive set on* $\mathcal{T} \cup \mathcal{V}$.

Proof. Within the 3-net $\mathcal{N}(L)$, for every vertical line $v \in \mathcal{V}$ and transversal line $t \in \mathcal{T}$, there exists a unique horizontal line $h \in \mathcal{H}$, such that the associated Bol reflection interchanges v and t. In fact, let $v_a \in \mathcal{V}$ and $t_c \in \mathcal{T}$. The intersection $v_a \cap t_c$ is the unique point (a, b), where $b = a^{-1}c$. For every $y \in L$,

$$\begin{aligned}(a,\ y,\ ay)^{\sigma_b} &= (ay \cdot b^{-1},\ by^{-1} \cdot b, ab)\\ &= (ay \cdot b^{-1},\ by^{-1} \cdot b,\ c) \in t_c,\end{aligned}$$

and

$$\begin{aligned}(cy^{-1},\ y,\ c)^{\sigma_b} &= (cb^{-1}, by^{-1} \cdot b, cy^{-1} \cdot b)\\ &= (a, by^{-1} \cdot b, cy^{-1} \cdot b) \in v_a.\end{aligned}$$

Hence, the Bol reflection σ_b thorough the horizontal line h_b interchanges the points of v_a with the points of t_c.

Consequently any composition $\sigma_1\sigma_b$ induces a permutation on the vertical lines, as well as on the transversal lines. In fact, If we consider now two vertical lines, v_a and v_c, the autotopism $\sigma_1\sigma_b = (R_{b^{-1}}, L_bR_b, R_b)$ of L, with $ab^{-1} = c$, maps v_a into v_c. Indeed,

$$\begin{aligned}(a,\ x,\ ax)^{\sigma_1\sigma_b} &= (ab^{-1},\ bx \cdot b, ax \cdot b)\\ &= (c,\ bx \cdot b, ax \cdot b) \in v_c.\end{aligned}$$

Similarly, the autotopism $\sigma_1\sigma_b$ of L, with $ab = c$, maps the transversal line t_a into t_b.Indeed,

$$\begin{aligned}(ay^{-1},\ y,\ a)^{\sigma_1\sigma_b} &= (ay^{-1} \cdot b^{-1},\ by \cdot y,\ ab)\\ &= (ay^{-1} \cdot b^{-1},\ by \cdot y,\ c) \in t_c.\end{aligned}$$

□

Lemma 4.4.3. *Let* $\widetilde{L} = (\mathcal{T} \cup \mathcal{V}, \cdot)$, *with product defined in* (4.2). *Then* $\widetilde{L} = \lambda(\Gamma, \mathcal{T} \cup \mathcal{V}, t_1)$.

Proof. The loop $\lambda(\Gamma, \mathcal{T} \cup \mathcal{V}, t_1)$ is well-defined by Lemma 4.4.2, its unit element is t_1. The unique element of Σ mapping t_1 into t_d and v_d is $\sigma_1\sigma_d$ and $\sigma_{d^{-1}}$,

respectively. Hence, the loop operation is

$$\begin{aligned} t_a \cdot t_b &= t_a^{\sigma_1\sigma_b} = t_{ab}, \\ t_a \cdot v_b &= t_a^{\sigma_{b^{-1}}} = v_{ab}, \\ v_a \cdot t_b &= v_a^{\sigma_1\sigma_b} = v_{ab^{-1}}, \\ v_a \cdot v_b &= v_a^{\sigma_{b^{-1}}} = t_{ab^{-1}}. \end{aligned}$$ □

Lemma 4.4.4. *The loop $\widetilde{L}$ has size $|\widetilde{L}| = 2|L|$. It contains $\mathcal{T}$ as a normal subloop of index 2, which is isomorphic to L. Every element v_a (a vertical line) has order two.*

Proof. These properties follow from the product formulas. □

Clearly, any equation which holds identically in $\widetilde{L}$, does hold in L as well. For example, if $\widetilde{L}$ is right Bol, then L is right Bol too. The converse is not true in general.

Proposition 4.4.5. *$\widetilde{L}$ is a right Bol loop if, and only if, L is right conjugacy closed right Bol loop with the property*

$$ab \cdot a^{-1} = a^{-1}b \cdot a, \quad \forall\ a, b \in L. \tag{4.13}$$

Proof. It is known that a loop is a right Bol loop if, and only if, the set of its right translations is a twisted subgroup of the group of right multiplications. In our case, since Σ is the set of right translations, we have that $\widetilde{L}$ is a right Bol loop if, and only if, for any $a, b \in L$

$$\left\{\sigma_a\sigma_b\sigma_a,\ \sigma_1\sigma_a\sigma_1\sigma_b\sigma_1\sigma_a,\ \sigma_1\sigma_a\sigma_b\sigma_1\sigma_a,\ \sigma_a\sigma_1\sigma_b\sigma_a\right\} \subset \Sigma. \tag{4.14}$$

Let us compute $(x, y, xy)^{\sigma_a\sigma_b\sigma_a}$.

$$\begin{aligned} (x, y, xy)^{\sigma_a\sigma_b\sigma_a} &= \left(xy \cdot a^{-1},\ ay^{-1} \cdot a,\ xa\right)^{\sigma_b\sigma_a} \\ &= \left(xa \cdot b^{-1},\ b\left(a^{-1}y \cdot a^{-1}\right) \cdot b,\ \left(xy \cdot a^{-1}\right) b\right)^{\sigma_a} \\ &= \left(\left(xy \cdot a^{-1}\right) b \cdot a^{-1},\ a\left(b^{-1}\left(ay^{-1} \cdot a\right) \cdot b^{-1}\right) \cdot a,\ \left(xa \cdot b^{-1}\right) a\right) \\ &= \left((xy)\left(ab^{-1} \cdot a\right)^{-1},\ \left(ab^{-1} \cdot a\right) y^{-1} \cdot \left(ab^{-1} \cdot a\right),\ x\left(ab^{-1} \cdot a\right)\right). \end{aligned}$$

Hence we have that

$$\sigma_a\sigma_b\sigma_a = \sigma_{ab^{-1}\cdot a} \in \Sigma.$$

Furthermore,

$$\sigma_1\sigma_a\sigma_1\sigma_b\sigma_1\sigma_a = \sigma_1\sigma_a\sigma_{b^{-1}}\sigma_a = \sigma_1\sigma_{ab\cdot a} \in \Sigma.$$

Now, let us compute $(x, y, xy)^{\sigma_1\sigma_a\sigma_b\sigma_1\sigma_a}$.

$$\begin{aligned}(x, y, xy)^{\sigma_1\sigma_a\sigma_b\sigma_1\sigma_a} &= \Big(xa^{-1},\ ay \cdot a,\ xy \cdot a\Big)^{\sigma_b\sigma_1\sigma_a} \\ &= \Big(\,(xy \cdot a)\, b^{-1},\ b\left(a^{-1}y^{-1} \cdot a^{-1}\right) \cdot b,\ xd^{-1} \cdot f\Big)^{\sigma_1\sigma_a} \\ &= \Big(\,(xy \cdot a)\, b^{-1} \cdot a^{-1},\ a\left(b\left(a^{-1}y^{-1} \cdot a^{-1}\right) \cdot b\right) \cdot a,\ \left(xa^{-1} \cdot b\right) a\Big).\end{aligned}$$

The composition $\sigma_1\sigma_a\sigma_b\sigma_1\sigma_a$ belongs to Σ exactly when it is equal to σ_ε, for a suitable $\varepsilon \in L$, since the first component depends on the product xy. By setting $x = 1$, we can deduce from the third component that ε must be equal to $a^{-1}b \cdot a$. Moreover, L needs to satisfy the condition

$$R_a^{-1}R_bR_a = R_{a^{-1}b\cdot a}, \quad \forall\ a, b \in L,$$

which means that L must be right conjugacy closed. Furthermore, since the first component must be equal to $xy \cdot \varepsilon^{-1}$, we find that

$$(a^{-1}b \cdot a)^{-1} = ab^{-1} \cdot a^{-1} \quad \forall\ a, b \in L. \tag{4.15}$$

Since a right conjugacy closed loop satisfies the property that for any a, b, $(a^{-1}b \cdot a)^{-1} = a^{-1}b^{-1} \cdot a$, we can rewrite the condition (4.15) as

$$ab^{-1} \cdot a^{-1} = a^{-1}b^{-1} \cdot b \quad \forall\ a, b \in L. \tag{4.16}$$

Lastly, the second component of $(x, y, xy)^{\sigma_1\sigma_a\sigma_b\sigma_1\sigma_a}$ must be $\varepsilon y^{-1} \cdot \varepsilon$, and by an easy computation it is possible to see that this is equivalent to (4.16). Hence, with these properties, for all $a, b \in L$ we have that

$$\sigma_1\sigma_a\sigma_b\sigma_1\sigma_a = \sigma_{a^{-1}b\cdot a} \in \Sigma,$$

and also

$$\sigma_a\sigma_1\sigma_b\sigma_a = \sigma_1\sigma_1\sigma_a\sigma_b^{-1}\sigma_1\sigma_a = \sigma_1\sigma_{a^{-1}b^{-1}\cdot a} \in \Sigma. \tag{4.17}$$

□

We can now prove the first part of our first main result of this chapter, which replaces the equation (4.13) by the condition $x^2 \in Z(L)$ for all x.

Proof of the first assertion of Theorem 4.4.1. Let L be a right conjugacy closed right Bol loop. Assume that (4.13) holds. Then

$$ab = (bb^{-1})a \cdot b = b(b^{-1}a \cdot b) = b(ba \cdot b^{-1}) = b^2a \cdot b^{-1}.$$

Hence for every $a, b \in L$ we have that $ab = b^2a \cdot b^{-1}$, which is equivalent to $ab^2 = b^2a$. Conversely, if $ab^2 = b^2a$ for every $a, b \in L$, then we have

$$ba \cdot b^{-1} = ba \cdot bb^{-2} = (ba \cdot b)b^{-2} = b^{-2}(ba \cdot b) = (b^{-2}b \cdot a)b = b^{-1}a \cdot b.$$

Hence, since in every right conjugacy closed right Bol loops every square is in the nucleus $N(L)$, (4.13) is equivalent with the fact that $x^2 \in Z(L)$ for every x. Proposition 4.4.5 implies the first assertion of Theorem 4.4.1. □

All of the six non-associative right Bol loops of order 8 are right conjugacy closed and every square element x^2 is central. In conclusion, if L is any right Bol loop of order 8, the corresponding $\widetilde{L}$ is a right Bol loop of order 16.

None of the proper Bol loops of order 12 is right conjugacy closed, and none of the proper Bol loops of order 15 has all squares in the center. As a result, it follows that the corresponding loop $\widetilde{L}$ cannot be a right Bol loop in either of these cases.

The situation changes for the Bol loops of order 16. Of the 2038 proper Bol loops L with this size, using the GAP [39] package LOOPS [71], we found that a significant majority of them, precisely 1940, satisfy the conditions of Theorem 4.4.1. Consequently, the corresponding $\widetilde{L}$ in these cases are in fact Bol loops.

Remark 4.4.1. In this scenario, if L is an abelian group, then $\widetilde{L}$ is the semidirect product $L \rtimes C_2$, where $L \cong \mathcal{T}$, $C_2 \cong \{t_1, v_1\}$, and the action on L is $x \mapsto x^{-1}$. This allows us to say that if L is an abelian group, then $\widetilde{L}$ is associative, but not necessarily abelian. $\widetilde{L}$ is an abelian group exactly when L is an elementary abelian 2-group.

Proposition 4.4.6. *Let L be a right conjugacy closed right Bol loop with central squares. The following are equivalent:*

(i) $\widetilde{L}$ is Moufang.

(ii) $\widetilde{L}$ is associative.

(iii) L is an abelian group.

Proof. Of course, for $\widetilde{L}$ to be Moufang, we need L to be Moufang as well. Since L is right conjugacy closed, it is an extra loop.

$\widetilde{L}$ is a right Bol loop, therefore it is Moufang if and only if

$$(\ell_1\ell_2)^{-1} = \ell_2^{-1}\ell_1^{-1} \tag{4.18}$$

for every $\ell_1, \ell_2 \in \widetilde{L}$. The relation $(ab)^{-1} = b^{-1}a^{-1}$ holds in L, so (4.18) is trivially satisfied for every pair of transversal lines. For vertical lines, the following holds.

$$(v_a v_b)^{-1} = t_{ab^{-1}}^{-1} = t_{(ab^{-1})^{-1}} = t_{ba^{-1}} = v_b v_a = v_b^{-1} v_a^{-1}.$$

If ℓ_1 and ℓ_2 are not both transversal nor both vertical, say $\ell_1 = t_a$ and $\ell_2 = v_b$, then

$$(t_a v_b)^{-1} = v_{ab}^{-1} = v_{ab} \quad \text{and} \quad v_b^{-1} t_a^{-1} = v_b t_{a^{-1}} = v_{ba}.$$

Hence $(t_a v_b)^{-1} = v_b^{-1} t_a^{-1}$ if, and only if, L is commutative. The same condition is obtained by letting $(v_a t_b)^{-1} = t_b^{-1} v_a^{-1}$. The equivalence between (i) and (iii) follows from the fact that a commutative extra loop is an abelian group. From Remark 4.4.1, we have the equivalence between (ii) and (iii). □

This completes the proof of Theorem 4.4.1.

4.5 Nuclei and center of the extension

Our next aim is to describe the nuclei and center of $\widetilde{L}$.

Proposition 4.5.1. *Let L be a right conjugacy closed Bol loop with $x^2 \in Z(L)$ for every $x \in L$. The right nucleus of $\widetilde{L}$ is*

$$N_\rho(\widetilde{L}) = \{t_z,\ v_z \mid z \in Z(L)\}. \tag{4.19}$$

Proof. Consider $t_z \in N_\rho(\widetilde{L})$. Since $\mathcal{T}$ is isomorphic to L, the equation

$$t_a(t_b t_z) = (t_a t_b)t_z, \quad \forall\ a, b \in L,$$

is equivalent to saying that z belongs to $N_\rho(L)$. One can easily check that requiring $t_a(v_b t_z) = (t_a v_b)t_z$ leads to the same condition. Now, by setting

$$v_a(v_b t_z) = (v_a v_b)t_z, \quad \forall\ a, b \in L,$$

we obtain

$$v_a v_{bz^{-1}} t_z = (t_{ab}^{-1})t_z.$$

This last equation is equivalent to

$$a(bz^{-1})^{-1} = (ab^{-1})z, \quad \forall\ a, b \in L, \tag{4.20}$$

which, since z is a right-nuclear element of L, means that $a(bz^{-1})^{-1} = a(b^{-1}z)$, which can be further simplified to

$$(bz^{-1})^{-1} = b^{-1}z, \quad \forall\ b \in L. \tag{4.21}$$

Since again z belongs to $N_\rho(L)$, in L the equation $(bz^{-1})^{-1} = zb^{-1}$ holds for every b, allowing us to rewrite (4.21) as

$$zb^{-1} = b^{-1}z, \quad \forall\ b \in L,$$

that is, z belongs to the commutant $C(L)$. In conclusion, we have that

$$t_z \in N_\rho(\widetilde{L}) \iff z \in N_\rho(L) \cap C(L) = Z(L).$$

Let now $v_z \in N_\rho(\widetilde{L})$. Both the conditions

$$t_a(v_b v_z) = (t_a v_b)v_z \quad \text{and} \quad t_a(t_b v_z) = (t_a t_b)v_z, \quad \forall\ a, b \in L,$$

lead easily to $z \in N_\rho(L)$. The remaining conditions $v_a(v_b v_z) = (v_a v_b)v_z$ and $v_a(t_b v_z) = (v_a t_b)v_z$ are both equivalent to (4.20), leading to $z \in C(L)$. Therefore, we can say that also for vertical lines it holds

$$v_z \in N_\rho(\widetilde{L}) \iff z \in N_\rho(L) \cap C(L) = Z(L). \qquad \square$$

While Proposition 4.5.1 provides a complete description of the right nucleus of the Bol loop $\widetilde{L}$, which remains the same for all suitable L, the situation is

different for the left nucleus, as shown by the next result.

Proposition 4.5.2. *Let L be a right conjugacy closed Bol loop with $x^2 \in Z(L)$ for every $x \in L$. For the left nucleus of $\widetilde{L}$ it holds that*

$$N_\lambda(\widetilde{L}) \cap \mathcal{T} = \{t_n \mid n \in N_\lambda(L)\} \cong N_\lambda(L).$$

Furthermore,

$$N_\lambda(\widetilde{L}) \cap \mathcal{V} = \{v_n \mid n = ((na)b)(a^{-1}b^{-1}) \quad \forall a, b \in L\}$$

In particular:

(i) if L is a non-abelian group, then

$$N_\lambda(\widetilde{L}) = \mathcal{T} \cong L; \tag{4.22}$$

(ii) if L is an AIP loop, then

$$N_\lambda(\widetilde{L}) = \{t_n,\ v_n \mid n \in N_\lambda(L)\}. \tag{4.23}$$

Proof. Since $\mathcal{T}$ is isomorphic to L,

$$N_\lambda(\widetilde{L}) \cap \mathcal{T} \subseteq \{t_n \mid n \in N_\lambda(L)\} \cong N_\lambda(L).$$

The conditions

$$t_n(v_a v_b) = (t_n v_a)v_b, \quad t_n(t_a v_b) = (t_n t_a)v_b, \quad t_n(v_a t_b) = (t_n v_a)t_b$$

are satisfied for any $a, b \in L$ and $n \in N_\lambda(L)$. Hence, we can conclude that

$$N_\lambda(\widetilde{L}) \cap \mathcal{T} = \{t_n \mid n \in N_\lambda(L)\}.$$

Consider now $v_n \in N_\lambda(\widetilde{L})$. The equation $v_n(v_a v_b) = (v_n v_a)v_b$ is equivalent to

$$n(ab^{-1})^{-1} = (na^{-1})b \quad \forall\ a, b \in L. \tag{4.24}$$

It is easy to see that the remaining associativity conditions

$$v_n(t_a t_b) = (v_n t_a)t_b, \quad v_n(t_a v_b) = (v_n t_a)v_b, \quad v_n(v_a t_b) = (v_n v_a)t_b,$$

are all equivalent to (4.24). Furthermore, (4.24) is equivalent to

$$n = ((na)b)(a^{-1}b^{-1}) \quad \forall\ a, b \in L. \tag{4.25}$$

If L is a non-abelian group, then (4.25) is impossible, therefore the left nucleus of $\widetilde{L}$ contains no vertical lines, that is,

$$N_\lambda(\widetilde{L}) \cap \mathcal{V} = \emptyset,$$

and (i) is proved. Lastly, if L is an AIP loop, then (4.25) requires n to belong to the left nucleus $N_\lambda(L)$. Hence

$$N_\lambda(\widetilde{L}) \cap \mathcal{V} = \{v_n \mid \in N_\lambda(L)\},$$

which proves the assertion (ii). □

By Proposition 4.5.2 we can see that, differently than the right nucleus, the left nucleus has a less schematic description. We can say that, if L is not AIP and n belongs to $N_\lambda(L)$, then, from equation (4.24), v_n cannot be an element of $N_\lambda(\widetilde{L})$. That is, the following holds

$$N_\lambda(\widetilde{L}) \cap \mathcal{V} \subseteq \{v_n \mid n \in L \setminus N_\lambda(L)\}. \tag{4.26}$$

Among the 2038 right Bol loops of size 16, 1940 are RCC with central squares. We performed an analysis using the GAP package LOOPS [71] and identified 1773 of them that are neither associative nor AIP loops. Out of these, there are 14 cases where the left nucleus of the corresponding $\widetilde{L}$ has largest intersection possible with $\mathcal{V}$, that is $N_\lambda(\widetilde{L}) \cap \mathcal{V} = \{v_n \mid n \in L \setminus N_\lambda(L)\}$. For example L =RightBolLoop(16,181) has the following left nucleus

$$N_\lambda(L) = \{1, 3, 4, 7, 9, 11, 12, 15\}$$

and $\widetilde{L}$ has

$$N_\lambda(\widetilde{L}) \cap \mathcal{V} = \{v_2, v_5, v_6, v_8, v_{10}, v_{13}, v_{14}, v_{16}\}$$

Let L be a RCC right Bol loop of order 16 with central squares which is not AIP, and $\nu(L) := |N_\lambda(L) \cap \mathcal{V}|$. Also, let us denote with μ_k the size of the family $\{L \mid \nu(L) = k\}$, $k = 0, \ldots, 16$. With LOOPS [71] we found the output listed in Table 4.1.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
μ_k	1145	0	454	0	160	0	0	0	14	0	0	0	0	0	0	0	0

TABLE 4.1: Number of loops with $\nu(L) = k$

Proposition 4.5.3. *Let L be a right conjugacy closed Bol loop with $x^2 \in Z(L)$ for every $x \in L$, and let $Z(\widetilde{L})$ be the center of $\widetilde{L}$. The following assertions hold:*

(i) if L has not exponent 2, then

$$Z(\widetilde{L}) = \{t_z \mid z \in Z(L), \text{ and } z^2 = 1\}; \tag{4.27}$$

(ii) if L has exponent 2, then

$$Z(\widetilde{L}) = \{t_z,\ v_z \mid z \in Z(L)\}. \tag{4.28}$$

Proof. By Proposition 4.5.1,

$$Z(\widetilde{L}) \subseteq \{t_z, v_z \mid z \in Z(L)\}.$$

If L has not exponent 2, no vertical line can be in the commutant, since the condition $v_z t_a = t_a v_z$, for any $a \in L$, is equivalent to $za^{-1} = az$, that is $a = a^{-1}$ for any $a \in L$. Hence the center of $\widetilde{L}$ consists only of transversal lines t_z for some $z \in Z(L)$. The condition $t_z t_a = t_a t_z$ is naturally satisfied, and $t_z v_a = v_a t_z$ requires that $z^2 = 1$. Hence

$$Z(\widetilde{L}) = \{t_z \mid z \in Z(L), \text{ and } z^2 = 1\}.$$

If instead L has exponent 2, then

$$N(\widetilde{L}) = \{t_z,\ v_z \mid z \in Z(L)\},$$

and with the same arguments we obtain that $Z((\widetilde{L}) = N((\widetilde{L})$. □

4.6 The core of the extension

Now we want to see how to define a *quandle* starting from a Bol loop. A quandle, which is a special case of a rack, is a set with a binary operation satisfying axioms reflecting the three Reidemeister moves (c.f. [86]) in knot theory. Although mainly used to study invariants for knots, quandles hold intrinsic interest as algebraic structures. In particular, the definition of a quandle axiomatizes the properties of conjugation within a group.

Definition 4.6.1. A *quandle* $(Q, \triangleleft)$ is a set Q with a binary operation $\triangleleft$: $Q \times Q \longrightarrow Q$ which satisfies the following axioms:

1. for all $a \in Q$, $a \triangleleft a = a$ (idempotence);
2. for all $a, b \in Q$, there exists a unique $x \in Q$ such that $x \triangleleft a = b$;
3. for all $a, b, c \in Q$, $(a \triangleleft b) \triangleleft c = (a \triangleleft c) \triangleleft (b \triangleleft c)$ (right self-distributivity).

In other words, a quandle can be described as a right quasigroup Q where the right translations are automorphism of Q, with the element a itself being fixed by R_a.

Example 4.6.1.1. If $(G, \cdot)$ is a group, the conjugation $a \triangleleft b := b^{-1}ab$ gives a quandle structure.

A quandle Q is said *involutory* if $(a \triangleleft b) \triangleleft b$ for every $a, b \in Q$, and it is said *connected* if the right multiplication group

$$\mathrm{RMlt}(Q) = \langle R_b \mid b \in Q,\ a^{R_b} = a \triangleleft b \rangle$$

acts transitively on Q. Connected quandles are the main objects in [49], where the authors present a correspondence between with certain configuration in transitive groups, called quandle envelopes.

If $(L,\cdot)$ is a loop, the *core* $(L,+)$ of L is defined by the operation

$$x+y := (yx^{-1})y. \tag{4.29}$$

If L is a right Bol loop, its core is a quandle (see [88]). Indeed, while the core is trivially idempotent by the definition of $+$, let us show the other two axioms.

For every $x,y \in L$

$$\begin{aligned}(x+y)+y &= (yx^{-1}\cdot y)+y\\ &= y(yx^{-1}\cdot y)^{-1}\cdot y\\ &= y(y^{-1}x\cdot y^{-1})\cdot y\\ &= (yy^{-1}\cdot x)y^{-1}\cdot y\\ &= x.\end{aligned}$$

Also, for every $x,y,z \in L$,

$$(x+y)+z = (yx^{-1}\cdot y)+z = z(yx^{-1}\cdot y)^{-1}\cdot z,$$

and

$$\begin{aligned}(x+z)+(y+z) &= (zx^{-1}\cdot z)+(zy^{-1}\cdot z)\\ &= (zy^{-1}\cdot z)(zx^{-1}\cdot z)^{-1}\cdot(zy^{-1}\cdot z)\\ &= (zy^{-1}\cdot z)(z^{-1}x\cdot z^{-1})\cdot(zy^{-1}\cdot z)\\ &= \left(\left(\left(\left(zy^{-1}\cdot z\right)z^{-1}\right)x\right)z^{-1}\right)z\Big)\,y^{-1}\cdot z\\ &= \left(\left(zy^{-1}\cdot x\right)y^{-1}\right)z\\ &= z(yx^{-1}\cdot y)^{-1}\cdot z.\end{aligned}$$

If L is a right conjugacy closed right Bol loop with central squares, we define the core of $\widetilde{L}$ in the same way, denoting it with the same symbol $+$.

Theorem 4.6.2. *Let L be a right conjugacy closed right Bol loops with central squares. The core of $\widetilde{L}$ decomposes to the disjoint union of two subquandles $\mathcal{T}$ and $\mathcal{V}$, both isomorphic to the core of L.*

Proof. Since the subloop $\mathcal{T}$ of $\widetilde{L}$ is L, $t_a + t_b = t_{a+b}$. Moreover,

$$v_a + v_b = v_b v_a \cdot v_b = t_{ba^{-1}}v_b = v_{ba^{-1}\cdot b} = v_{a+b}.$$

Hence, the core of $\widetilde{L}$ decomposes into the disjoint union of two cores $\mathcal{T}$ and $\mathcal{V}$ both isomorphic to the core of L. □

Furthermore, for the mixed computations it holds

$$t_a + v_b = t_{ba\cdot b^{-1}}, \qquad v_a + t_b = v_{ba\cdot b^{-1}}. \tag{4.30}$$

We note here that the equation $t_a + \ell = t_{ba \cdot b^{-1}}$ has v_b and $v_{b^{-1}}$ as solutions, so in general the quandle $(\widetilde{L}, +)$ is not a quasigroup.

Definition 4.6.3. The *structure group* of a quandle $(Q, \triangleleft)$ is

$$\mathrm{STR}(Q, \triangleleft) = \langle g_a,\ a \in Q \mid g_a g_b = g_b g_{a \triangleleft b},\ a, b \in Q \rangle.$$

The structure group of a finite quandle is either free abelian of rank r, where r is the number of orbits of Q with respect to all the right translations, or non-abelian and with torsion. In the latter case, $\mathrm{STR}(Q, \triangleleft)$ has a finite index free abelian subgroup of rank r; see [61] for more details.

If L is a Bol loop, then the idempotence of the core implies

$$g_a = g_{(a+b)+b} = g_b^{-1} g_{a+b} g_b = g_b^{-2} g_a g_b^2.$$

Hence, $g_b^2 \in Z(\mathrm{STR}(L, +))$ for all $b \in L$. Moreover,

$$g_{a+b}^2 = (g_b^{-1} g_a g_b)^2 = g_b^{-1} g_a^2 g_b = g_a^2.$$

Let $a_1, \ldots, a_r$ be orbit representatives of the right translation group of the core. The subgroup $T = \langle g_{a_1}^2, \ldots, g_{a_r}^2 \rangle$ is a free abelian group of rank r, which is contained in the center of the structure group. As shown above, T contains every g_a^2, $a \in L$. We call the factor $\mathrm{STR}(L, +)/T$ the *restricted structure group*

$$\mathrm{rSTR}(L, +) = \langle \hat{g}_a,\ a \in L \mid \hat{g}_b \hat{g}_a \hat{g}_b = \hat{g}_{a+b},\ \hat{g}_a^2 = 1\ a, b \in L \rangle.$$

The Bol reflections σ_a satisfy $\sigma_a^2 = \mathrm{Id}$ and $\sigma_{a+b} = \sigma_b \sigma_a \sigma_b$. Thus, $\hat{g}_a \longmapsto \sigma_a$ extends to a surjective homomorphism from the restricted structure group onto the collineation group

$$\Gamma = \langle \sigma_a \mid a \in L \rangle$$

generated by Bol reflections.

Lemma 4.6.4. *Let L be a right Bol loop, and denote by r the number of orbits of the right multiplication group of the core. Write $G = \mathrm{rSTR}(L, +)$. Then $G/G' \cong C_2^r$.*

Proof. Let $a_1, \ldots, a_r$ be orbit representatives and let $h_1, \ldots, h_r$ be the free generators of the elemenatry abelian 2-group C_2^r. For an element a in the orbit of a_i, we define the map $\Phi : \hat{g}_a \to h_i$. It is clear that Φ extends to a surjective homomorphism $G \to C_2^r$. Hence, G/G' is elementary abelian of rank at least r. If $a, b \in L$ are in the same orbit, then $\hat{g}_a^t = \hat{g}_b$ for some $t \in \mathrm{rSTR}(L, +)$. This implies $\hat{g}_a \hat{g}_b \in G'$, or equivalently $\hat{g}_a G' = \hat{g}_b G'$. Therefore, the rank of G/G' cannot be more than r. □

We finish this section by computing the restricted structure group of the cores of right Bol loops in some cases.

Proposition 4.6.5. *Let L be a right Bol loop, and denote by r the number of orbits of the right multiplication group of the core. Then*

$$\mathrm{rSTR}(L \times C_2, +) \cong \mathrm{rSTR}(L, +) \times C_2^r.$$

Proof. We denote the generators of $\mathrm{rSTR}(L \times C_2, +)$ by $\hat{g}_{a,i}$ with $a \in L$, $i \in \mathbb{F}_2$. $\hat{g}_{b,j}\hat{g}_{a,i}\hat{g}_{b,j} = \hat{g}_{a+b,i}$ implies that $\hat{g}_{b,0}, \hat{g}_{b,1}$ have the same action on all generators. This means that $c_b = \hat{g}_{b,0}\hat{g}_{b,1}$ is in the center, and

$$\mathrm{rSTR}(L \times C_2, +) \cong \mathrm{rSTR}(L, +) \times \langle c_b \mid b \in L \rangle.$$

On the one hand, $c_b^2 = 1$. On the other hand,

$$c_b = \hat{g}_{a,0}c_b\hat{g}_{a,0} = \hat{g}_{a,0}\hat{g}_{b,0}\hat{g}_{b,1}\hat{g}_{a,0} = \hat{g}_{b+a,0}\hat{g}_{b+a,1} = c_{b+a}.$$

These show that $\langle c_b \mid b \in L \rangle$ is an elementary abelian 2-group of rank at most r. Lemma 4.6.4 implies that the rank is equal to r. □

As for a right Bol loop L of exponent 2, the extension $\widetilde{L}$ is simply the direct product $L \times C_2$, the following result is immediate.

Corollary 4.6.6. *Let L be a finite right Bol loop of exponent 2. Then*

$$\mathrm{rSTR}(\widetilde{L}, +) \cong \mathrm{rSTR}(L, +) \times C_2^r,$$

where r is the number of orbits of the right multiplicarion group of the core.

The restricted structure group can also be computed for another class, which is rather trivial from the point of view of the theory of loops, namely for the class of abelian groups. However, in this case, the formula for the restricted structure group is surprisingly different.

Proposition 4.6.7. *Let L be an abelian group. Then*

$$\mathrm{rSTR}(\widetilde{L}, +) \cong \mathrm{rSTR}(L, +) \times \mathrm{rSTR}(L, +).$$

Proof. Define the subgroups

$$G_T = \langle \hat{g}_{t_a} \mid a \in L \rangle,$$
$$G_V = \langle \hat{g}_{v_a} \mid a \in L \rangle$$

of $\mathrm{rSTR}(\widetilde{L}, +)$. Clearly $\mathrm{rSTR}(\widetilde{L}, +) = \langle G_T, G_V \rangle$, and $G_T \cong G_V \cong \mathrm{rSTR}(L, +)$. (4.30) implies that $\hat{g}_{v_b}$ commutes with G_T, and $\hat{g}_{t_b}$ commutes with G_V. The claim $\mathrm{rSTR}(\widetilde{L}, +) \cong G_T \times G_V$ follows. □

Appendix A

Pseudocodes of the Algorithms used in Chapter 3

In this Appendix, we present the pseudocodes utilized to derive the results in chapter 3. The following tables are used in the pseudo-codes.

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

Table A.1: STS(13) #1

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

Table A.2: STS(13) #2

0	0	0	0	0	0	0	1	1	1	1	1	1	2	2	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5	6	6	6	6
1	3	5	7	9	b	d	3	4	7	8	b	c	3	4	7	8	b	c	7	8	9	a	7	8	9	a	7	8	9	a	7	8	9	a
2	4	6	8	a	c	e	5	6	9	a	d	e	6	5	a	9	e	d	b	c	d	e	c	b	e	d	e	d	c	b	d	e	b	c

Table A.3: STS(15) #2

0	0	0	0	0	0	0	1	1	1	1	1	1	2	2	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5	6	6	6	6
1	3	5	7	9	b	d	3	4	7	8	b	c	3	4	7	8	b	c	7	8	9	a	7	8	9	a	7	8	9	a	7	8	9	a
2	4	6	8	a	c	e	5	6	9	a	d	e	6	5	a	9	e	d	b	c	d	e	d	e	b	c	e	d	c	b	c	b	e	d

Table A.4: STS(15) #3

0	0	0	0	0	0	0	1	1	1	1	1	1	2	2	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5	6	6	6	6
1	3	5	7	9	b	d	3	4	7	8	b	c	3	4	7	8	b	c	7	8	9	a	7	8	9	a	7	8	9	a	7	8	9	a
2	4	6	8	a	c	e	5	6	9	a	d	e	6	5	a	9	e	d	b	d	e	c	e	c	b	d	c	e	d	b	d	b	c	e

Table A.5: STS(15) #7

0	0	0	0	0	0	0	1	1	1	1	1	1	2	2	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5	6	6	6	6
1	3	5	7	9	b	d	3	4	7	8	a	c	3	4	7	8	9	b	7	8	9	c	7	8	9	a	7	8	a	b	7	8	9	a
2	4	6	8	a	c	e	5	6	9	b	d	e	6	5	a	e	c	d	b	a	e	d	e	c	d	b	d	9	c	e	c	d	b	e

Table A.6: STS(15) #61

0	0	0	0	0	0	0	1	1	1	1	1	1	2	2	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	6	6	6	7	8
1	3	5	7	9	b	d	3	4	6	9	a	c	3	4	5	7	8	b	6	7	8	a	5	8	a	b	7	8	9	7	9	c	9	a
2	4	6	8	a	c	e	5	7	8	b	d	e	9	6	a	e	c	d	b	c	d	e	d	9	c	e	b	e	c	a	e	d	d	b

Table A.7: STS(15) #80

Algorithm 1: Pseudocode to compute the list of all the automorphisms for STS(9)

```
Function STS-9-AUT() { // this function computes all the
 automorphisms for STS(9)
{
  Result: the list of all the automorphisms for STS(9)
  A ⟵ ∅          // initialize the list of automorphisms as empty
  // take all the triples (a,b,c) with elements in {1,...,9}
  foreach((a,b,c) ∈ {1,...,9}^3)do
  {
    // ignore all the triples that do not meet the criteria
    if(a ≠ b)
    {
      r ⟵ STS-9-SUM(a,b)
      if(c ≠ a ∧ c ≠ b ∧ c ≠ r)
      {
        C ⟵ 0 ∈ {0,...,9}^10    // initialize an empty vector of 10
         zeros
        // fix the three elements (a,b,c) and the neutral element
           0
        C[0] ⟵ 0                          // set the image of 0 as 0
        C[1] ⟵ a                          // set the image of 1 as a
        C[2] ⟵ b                          // set the image of 2 as b
        C[3] ⟵ c                          // set the image of 3 as c
        // compute the remaing images
        C[8] ⟵ STS-9-SUM(C[1],C[2])
        C[6] ⟵ STS-9-SUM(C[1],C[3])
        C[7] ⟵ STS-9-SUM(C[6],C[8])
        C[4] ⟵ STS-9-SUM(C[2],C[3])
        C[5] ⟵ STS-9-SUM(C[4],C[6])
        C[9] ⟵ STS-9-SUM(C[1],C[5])
        Append C to A
      }
    }
  }
  return A
}
```

Algorithm 2: Pseudocode to compute the list of all the automorphisms for STS(13)

```
Function STS-13-AUT(i) { // this function computes all the
 automorphisms for STS(13)
{
  Data: i ∈ {1, 2} is the index of the table sum to use
  Result: the list of all the automorphisms for STS(13)
  A ⟵ ∅          // initialize the list of automorphisms as empty
  if(i = 1)
  {
    Ω ⟵ (1)                                  // the identity permutation
    P ⟵ (6 8)(2 11)(3 9)(4 12)(5 7)    // permutation of the elements
     of STS(13)
    ρ(x) ⟵ 3x (mod 13)                              // ρ is a function
    σ(x) ⟵ P(x)  // function that apply the permutation P to the
     element x
    A ⟵ {Ω, ρ, ρ^2, σ, ρ ∘ σ, ρ^2 ∘ σ}
  }
  else // i = 2
  {
    foreach(a ∈ {1, 3, 9})do
    {
      foreach(b ∈ {0, ..., 12})do
      {
        f(x) ⟵ (ax + b) (mod 13)
        Append f(x) to A
      }
    }
  }
  return A
}
```

Algorithm 3: Pseudocode to compute the list of all the automorphisms for STS(15)

```
Function STS-15-AUT(i) { // this function computes all the automorphisms for STS(15)
{
  Data: i ∈ {2, 3, 7, 61, 80} is the index of the table sum to use
  Result: the list of all the automorphisms for STS(15)
  A ⟵ ∅                                   // initialize the list of automorphisms as empty
  if( i ≠ 80 )
  {
    r ⟵ 4
  }
  else
  {
    r ⟵ 3
  }
  foreach( l ∈ {0, ..., 9, a, b, c, d, e}^r )do
  {
    // check if the elements in l are independent
    if( l contains repeated elements )
    {
      continue              // ignore l and go to the next element in {0, ..., 9, a, b, c, d, e}^r
    }
    if( i ≠ 80 )
    {
      (e1, e2, e3, e4) ⟵ l
      t1 ⟵ STS-15-SUM (i, e1, e2)    // sum e1 and e2 according to the table of STS(15)#i
      t2 ⟵ STS-15-SUM (i, e1, e3)
      t3 ⟵ STS-15-SUM (i, e2, e3)
      t4 ⟵ STS-15-SUM (i, t1, e3)
      if( e3 = t1 ∨ e4 ∈ {t1, t2, t3, t4} )
      {
        continue            // ignore l and go to the next element in {0, ..., 9, a, b, c, d, e}^r
      }
    }
    else // i = 80
    {
      (e1, e2, e3) ⟵ l
      t1 ⟵ STS-15-SUM (i, e1, e2)
      if( e3 = t1 )
      {
        continue            // ignore l and go to the next element in {0, ..., 9, a, b, c, d, e}^r
      }
    }
    C ⟵ STS-15-AUT-TABLE(i, l)                          // see algorithms 4 and 5
    // check if C is an automorphism
    flag ⟵ true
    foreach( l' ∈ STS-15-TABLE-COLUMNS(i) )do // consider all the columns of the table
      STS(15)#i
    {
      (e1, e2, e3) ⟵ l'
      H ⟵ (C[e1], C[e2], C[e3])
      if( H ∉ STS-15-TABLE-COLUMNS(i) ) // if H is not a column of the table i
      {
        flag ⟵ false
        break                                           // exit from the loop
      }
    }
    if( flag is true )
    {
      Append C to A
    }
  }
  return A
}
```

Algorithm 4: Compute a bijection of STS(15) that could potentially be an automorphism - Part I

```
Function STS-15-AUT-TABLE(i, l) { // this function computes a possible
 automorphism of STS(15)
{
  Data: i ∈ {2, 3, 7, 61, 80} is the index of the table sum to use, and l is a vector
        with 3 or 4 elements used to compute the automorphism
  Result: a possible automorphism of STS(15) for the table i and a fixed element l
  C ⟵ ∅                                          // initialize an empty set
  if(i ≠ 80)
  {
    (e1, e2, e3, e4) ⟵ l
    C[Ω] ⟵ Ω                                     // set the image of Ω as Ω
    C[1] ⟵ a                                     // set the image of 1 as e1
    C[2] ⟵ b                                     // set the image of 2 as e2
    C[3] ⟵ c                                     // set the image of 3 as e3
    C[7] ⟵ d                                     // set the image of 3 as e4
  }
  else
  {
    (e1, e2, e3) ⟵ l
    C[Ω] ⟵ Ω                                     // set the image of Ω as Ω
    C[1] ⟵ a                                     // set the image of 1 as e1
    C[2] ⟵ b                                     // set the image of 2 as e2
    C[3] ⟵ c                                     // set the image of 3 as e3
  }
  // compute the remaing images
  if(i = 2)
  {
    C[2] ⟵ STS-15-SUM (i, C[0], C[1])
    C[4] ⟵ STS-15-SUM (i, C[0], C[3])
    C[5] ⟵ STS-15-SUM (i, C[1], C[3])
    C[6] ⟵ STS-15-SUM (i, C[1], C[4])
    C[8] ⟵ STS-15-SUM (i, C[0], C[7])
    C[9] ⟵ STS-15-SUM (i, C[1], C[7])
    C[a] ⟵ STS-15-SUM (i, C[2], C[7])
    C[b] ⟵ STS-15-SUM (i, C[3], C[7])
    C[c] ⟵ STS-15-SUM (i, C[4], C[7])
    C[d] ⟵ STS-15-SUM (i, C[6], C[7])
    C[e] ⟵ STS-15-SUM (i, C[5], C[7])
  }
  else if(i = 3)
  {
    C[2] ⟵ STS-15-SUM (i, C[0], C[1])
    C[4] ⟵ STS-15-SUM (i, C[0], C[3])
    C[5] ⟵ STS-15-SUM (i, C[1], C[3])
    C[6] ⟵ STS-15-SUM (i, C[2], C[3])
    C[8] ⟵ STS-15-SUM (i, C[0], C[7])
    C[9] ⟵ STS-15-SUM (i, C[1], C[7])
    C[a] ⟵ STS-15-SUM (i, C[2], C[7])
    C[b] ⟵ STS-15-SUM (i, C[3], C[7])
    C[c] ⟵ STS-15-SUM (i, C[6], C[7])
    C[d] ⟵ STS-15-SUM (i, C[4], C[7])
    C[e] ⟵ STS-15-SUM (i, C[5], C[7])
  }
  // continue on algorithm 5
}
```

Algorithm 5: Compute a bijection of STS(15) that could potentially be an automorphism - Part II

Function `STS-15-AUT-TABLE`(i, l) **{** `// this function computes a possible automorphism of` STS(15)

{

Data: $i \in \{2, 3, 7, 61, 80\}$ is the index of the table sum to use, and l is a vector with 3 or 4 elements in used to compute the automorphism

Result: a possible automorphism of STS(15) for the table i and a fixed element l

`// see algorithm 4 for the first part of the algorithm`

else if$(i = 7)$

{

C[2] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[0], \mathrm{C}[1])$
C[4] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[0], \mathrm{C}[3])$
C[5] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[1], \mathrm{C}[3])$
C[6] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[2], \mathrm{C}[3])$
C[8] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[0], \mathrm{C}[7])$
C[9] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[1], \mathrm{C}[7])$
C[a] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[2], \mathrm{C}[7])$
C[b] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[3], \mathrm{C}[7])$
C[c] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[5], \mathrm{C}[7])$
C[d] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[6], \mathrm{C}[7])$
C[e] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[4], \mathrm{C}[7])$

}

else if$(i = 61)$

{

C[2] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[0], \mathrm{C}[1])$
C[4] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[0], \mathrm{C}[3])$
C[5] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[1], \mathrm{C}[3])$
C[6] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[2], \mathrm{C}[3])$
C[8] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[0], \mathrm{C}[7])$
C[9] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[1], \mathrm{C}[7])$
C[a] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[2], \mathrm{C}[7])$
C[b] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[3], \mathrm{C}[7])$
C[c] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[6], \mathrm{C}[7])$
C[d] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[5], \mathrm{C}[7])$
C[e] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[4], \mathrm{C}[7])$

}

else if$(i = 80)$

{

C[2] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[0], \mathrm{C}[1])$
C[4] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[0], \mathrm{C}[3])$
C[5] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[1], \mathrm{C}[3])$
C[6] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[0], \mathrm{C}[5])$
C[7] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[1], \mathrm{C}[4])$
C[8] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[1], \mathrm{C}[6])$
C[9] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[2], \mathrm{C}[3])$
C[a] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[2], \mathrm{C}[5])$
C[b] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[3], \mathrm{C}[6])$
C[c] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[3], \mathrm{C}[7])$
C[d] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[4], \mathrm{C}[5])$
C[e] $\longleftarrow$ STS-15-SUM $(i, \mathrm{C}[2], \mathrm{C}[7])$

}

return C

}

Algorithm 6: Main program

Function `Main(`$\mathcal{L}_{\mathcal{N}}$, $\mathcal{L}_{\mathcal{Q}}$, r, i`)` **{**
{
Data: $r \in \mathbb{N}$ is the number of expected coset representatives, and i is the sum-table index

$\mathcal{Q}_2 \longleftarrow$ `Compute-Fundamental-Pairs(`$\mathcal{L}_{\mathcal{Q}}$, i`)` `// see algorithm 7`
`Compute-Delta-1(`$\mathcal{L}_{\mathcal{N}}$, $\mathcal{L}_{\mathcal{Q}}$, $\mathcal{Q}_2$, i`)` `// see algorithm 9`
`Compute-Cosets(`$\mathcal{L}_{\mathcal{N}}$, $\mathcal{Q}_2$, r`)` `// see algorithm 10`
`Compute-Alpha-F(`$\mathcal{L}_{\mathcal{N}}$`)` `// see algorithm 11`
`Compute-F-Beta(`$\mathcal{L}_{\mathcal{Q}}$, $\mathcal{Q}_2$, i`)` `// see algorithm 13`
`Join-Alpha-F-Beta()` `// see algorithm 15`
}

Algorithm 7: Compute the fundamental pairs of $\mathcal{Q} \times \mathcal{Q}$

Function `Compute-Fundamental-Pairs(`$\mathcal{L}_{\mathcal{Q}}$, i`)` **{**
{
Data: i is the sum-table index
Result: the list $\mathcal{Q}_2$ of fundamental pairs in $\mathcal{Q} \times \mathcal{Q}$

$\mathcal{Q}_2 \longleftarrow \emptyset$ `// initialize an empty list`
$\mathcal{Q}'_2 \longleftarrow \binom{\mathcal{Q}}{2}$ `// the set of 2-combinations of elements` $\mathcal{Q}$
foreach$((A, B) \in \mathcal{Q}'_2)$**do**
{
$C \longleftarrow$ `Sum-Table(`$\mathcal{L}_{\mathcal{Q}}$, i, A, B`)` `// see algorithm 8`
$i_1 \longleftarrow$ `Index-Of(`$\{A, B\}$, $\mathcal{Q}'_2$`)` `// look for the index of the pair` $\{A, B\}$ `in` $\mathcal{Q}'_2$
$i_2 \longleftarrow$ `Index-Of(`$\{A, C\}$, $\mathcal{Q}'_2$`)` `// look for the index of the pair` $\{A, C\}$ `in` $\mathcal{Q}'_2$
$i_3 \longleftarrow$ `Index-Of(`$\{B, C\}$, $\mathcal{Q}'_2$`)` `// look for the index of the pair` $\{B, C\}$ `in` $\mathcal{Q}'_2$
$I \longleftarrow \{i_1, i_2, i_3\}$ `// create a set` I `with the three indices` i_1, i_2, `and` i_3
Remove $\{A, B\}$, $\{A, C\}$, and $\{B, C\}$ from $\mathcal{Q}'_2$
Append the pair related to `Min(`I`)` to $\mathcal{Q}_2$
}
return $\mathcal{Q}_2$
}

Algorithm 8: Compute the sum between two elements in $\mathcal{L}_{\mathcal{Q}}$

```
Function Sum-Table(L_Q, i, A, B) {
{
  Data: i is the sum-table index, and (A, B) ∈ L_Q^2
  Result: the sum A * B according to the sum table of L_Q
  if(L_Q is GF(2)^t for some t)
  {
    return A ⊕ B   // (⊕) is the standard addition of vectors over
     GF(2)^t
  }
  else if(L_Q is STS(9))
  {
    Use the table 3.1 to sum A and B and return the result
  }
  else if(L_Q is STS(13))
  {
    if(i = 1)
    {
      Use the table A.1 to sum A and B and return the result
    }
    else
    {
      Use the table A.2 to sum A and B and return the result
    }
  }
  else if(L_Q is STS(15))
  {
    if(i = 1)
    {
      return A ⊕ B      // (⊕) is the standard addition of vectors
       over GF(2)^4
    }
    else if(i = 2)
    {
      Use the table A.3 to sum A and B and return the result
    }
    else if(i = 3)
    {
      Use the table A.4 to sum A and B and return the result
    }
    else if(i = 7)
    {
      Use the table A.5 to sum A and B and return the result
    }
    else if(i = 61)
    {
      Use the table A.6 to sum A and B and return the result
    }
    else if(i = 80)
    {
      Use the table A.7 to sum A and B and return the result
    }
  }
}
```

Algorithm 9: Compute the functions B^2

Function `Compute-Delta-1(`$\mathcal{L}_\mathcal{N}$, $\mathcal{L}_\mathcal{Q}$, $\mathcal{Q}_2$, i`)` **{**

{

Data: $\mathcal{Q}_2$ is the list of fundamental pairs in $\mathcal{Q} \times \mathcal{Q}$, and i is the sum-table index

$B^2 \longleftarrow \emptyset$ `// initialize an empty list`

`// generate all the homomorphisms between` $\mathcal{L}_\mathcal{Q}$ `and` $\mathcal{L}_\mathcal{N}$

foreach$(e \in \{0, \ldots, |\mathcal{L}_\mathcal{N}| - 1\}^{|\mathcal{L}_\mathcal{Q}|-1})$**do**

{

`//` ϕ `is a vector of indices`

$j \longleftarrow 1$

$\lambda \longleftarrow$ `Concatenate(`0, e`)` `// fix the mapping between the neutral elements of` $\mathcal{L}_\mathcal{Q}$ `and` $\mathcal{L}_\mathcal{N}$

$\delta^1\phi \longleftarrow \mathbf{\Omega} \in \mathcal{L}_\mathcal{N}{}^{|\mathcal{Q}_2|}$

foreach$((R, S) \in \mathcal{Q}_2)$**do**

{

$T \longleftarrow$ `Sum-Table(`$\mathcal{L}_\mathcal{Q}$, i, R, S`)` `// see algorithm 8`

$i_R \longleftarrow$ `Index-Of(`R, $\mathcal{L}_\mathcal{Q}$`)` `// look for the index of` R `in` $\mathcal{L}_\mathcal{Q}$

$i_S \longleftarrow$ `Index-Of(`S, $\mathcal{L}_\mathcal{Q}$`)` `// look for the index of` S `in` $\mathcal{L}_\mathcal{Q}$

$i_T \longleftarrow$ `Index-Of(`T, $\mathcal{L}_\mathcal{Q}$`)` `// look for the index of` T `in` $\mathcal{L}_\mathcal{Q}$

`//` $\delta^1\phi$`-`ϕ

`//` $\delta^1\phi = \phi(R) * \phi(S) * \phi(R+S)$`, where` ϕ `is the composition of the arrays` $\mathcal{L}_\mathcal{N}$ `and` λ

$\delta^1\phi_j \longleftarrow \mathcal{L}_\mathcal{N}[\lambda[i_R]] * \mathcal{L}_\mathcal{N}[\lambda[i_S]] * \mathcal{L}_\mathcal{N}[\lambda[i_T]]$ `//` $(*)$ `is the sum for the elements in` $\mathcal{L}_\mathcal{N}$

$j \longleftarrow j + 1$

}

$l \longleftarrow$ `As-Integer(`$\delta^1\phi$`)` `// represent the vector` $\delta^1\phi$ `of elements in` $\mathcal{L}_\mathcal{N}$ `as an integer`

Append l to B^2

}

Save B^2 into a file

}

Algorithm 10: Compute the cosets of the factor systems modulo the functions $\delta^1\phi$

```
Function Compute-Cosets(L_N, Q_2, r) {
{
  Data: Q_2 is the list of fundamental pairs in Q × Q, and r is the number of cosets
  B^2 ⟵ load from disk
  n ⟵ |L_N|^|Q_2|                          // total number of factor systems
  b ⟵ |B^2|
  s ⟵ n/b
  i ⟵ 0
  STEP_INC ⟵ 50
  MAX_STEPS ⟵ ⌊s/100⌋
  cosets ⟵ ∅
  while(i < b ∧ |cosets| < r)do
  {
    j ⟵ 0
    l ⟵ |cosets|
    F ⟵ {i · s + k: 0 ≤ k < s}
    while(j < MAX_STEPS ∧ |F| > 0 ∧ |cosets| < r)do
    {
      coset ⟵ null
      f ⟵ Pop-Random-Element(F)     // remove a random element from F
       and returns it
      foreach(c ∈ {f ⊕ δ^1φ: ∀ δ^1φ ∈ B^2})do // (⊕) is the binary XOR
       operation
      {
        if(c ∈ F)
        {
          Remove c from F
        }
        if(c ∈ cosets)
        {
          coset ⟵ c
        }
      }
      if(coset is null)
      {
        j ⟵ 0
        cosets ⟵ cosets ∪ {f}
      }
      else
      {
        j ⟵ j + 1
      }
    }
    if(j < MAX_STEPS)
    {
      i ⟵ i + 1
    }
    else
    {
      i ⟵ i + STEP_INC
    }
    if(l < |cosets|)
    {
      Save/update cosets in a file
    }
  }
}
```

Algorithm 11: Compute the classes from the automorphism α

```
Function Compute-Alpha-F(L_N) {
{
  α_F ⟵ {}                                  // initialize empty dictionary
  B^2 ⟵ load from disk
  cosets ⟵ load from disk
  while( |cosets| > 0 )do
  {
    f ⟵ Pop-Random-Element(cosets)
    if( f is not key of α_F )
    {
      // α_F[f] is the set of factor systems which are isomorphic
         to f by α
      α_F[f] ⟵ ∅                             // initialize as an empty set
    }
    f' ⟵ As-Vector(f)                        // cast the integer f into its
     representation as list of elements in L_N
    // since L_N = GF(2)^t, Alpha-Automorphisms generates all the
       binary invertible matrices of order t
    foreach( α ∈ Alpha-Automorphisms(L_N) )do
    {
      α_F^(i) ⟵ {}                                          // empty list
      for( j = 0 to |f'| − 1 )do
      {
        c ⟵ α(f'[j])
        Append c to α_F^(i)
      }
      f^(i) ⟵ As-Integer(α_F^(i))            // represent α_F^(i) as an integer
      coset ⟵ Get-Coset(f^(i), cosets, B^2)          // see algorithm 12
      if( coset is not null )
      {
        α_F[f] ⟵ α_F[f] ∪ {coset}
      }
    }
    Save α_F in a file as a backup
  }
  // determine the classes by using α_F
  alpha_cosets ⟵ ∅                           // initialize as an empty set
  foreach( f ∈ Get-Dictionary-Keys(α_F) )do
  {
    k ⟵ Get-Smallest-Element(α_F[f])  // get the smallest element
     in α_F[f]
    alpha_cosets ⟵ alpha_cosets ∪ {k}
  }
  Save alpha_cosets to the disk
}
```

Algorithm 12: Compute the coset representative

Function `Get-Coset(`$f^{(i)}$, cosets, B^2`)` **{**
{
Data: $f^{(i)}$ is an integer representing a factor system, cosets is the set of cosets modulo $\delta^1\phi$, and B^2 is the list of $\delta^1\phi$ functions
foreach$(c \in \{f^{(i)} \oplus \delta^1\phi \colon \forall\ \delta^1\phi \in \mathrm{B}^2\})$**do** `//` $(\oplus)$ `is the binary XOR operation`
{
if$(c \in$ cosets$)$
{
return c
}
}
return ***null***
}

Algorithm 13: Compute the classes from the automorphism β

```
Function Compute-F-Beta(L_Q, Q_2, i) {
{
  Data: Q_2 is the list of fundamental pairs in Q × Q, and i is the sum-table
        index
  F_β ⟵ {}                                   // initialize empty dictionary
  B^2 ⟵ load from disk
  if( alpha_cosets is on disk ) // see algorithm 11
  {
    cosets ⟵ load alpha_cosets from disk
  }
  else
  {
    cosets ⟵ load cosets from disk
  }
  while( |cosets| > 0 )do
  {
    f ⟵ Pop-Random-Element(cosets)
    if( f is not key of F_β )
    {
      // F_β[f] is the set of factor systems which are isomorphic
         to f by β
      F_β[f] ⟵ ∅                              // initialize as an empty set
    }
    f' ⟵ As-Vector(f)                        // cast the integer f into its
     representation as list of elements in L_N
    foreach( β ∈ Beta-Automorphisms(L_Q, i) )do // see algorithm 14
     for Beta-Automorphisms
    {
      l ⟵ 0
      // compute the permutation ρ by applying the automorphism
         β to each pair (A, B) ∈ Q_2
      ρ ⟵ 0 ∈ {0, |f'| − 1}^|Q_2|                // vector of |Q_2| zeros
      foreach( (A, B) ∈ Q_2 )do
      {
        A' ⟵ β(A)                            // apply the automorphism β to A
        B' ⟵ β(B)                            // apply the automorphism β to B
        j ⟵ Index-Of( { A', B' }, Q_2)       // look for the index of the
         pair {A', B'} in Q_2
        ρ[l] ⟵ j
      }
      f_β ⟵ Permute(ρ, f')   // permute f' by using the permutation
       ρ
      f_β ⟵ As-Integer(f_β)
      coset ⟵ Get-Coset(f_β, cosets, B^2)          // see algorithm 12
      if(coset is not null)
      {
        F_β[f] ⟵ F_β[f] ∪ {coset}
      }
    }
    Save F_β in a file as a backup
  }
}
```

Algorithm 14: Compute the automorphisms β for $\mathcal{L}_{\mathcal{Q}}$

```
Function Beta-Automorphisms(L_Q, i) {
{
  Data: i is the sum-table index
  if(L_Q is GF(2)^c for some c)
  {
    Generate and return all the binary invertible matrices of order c
  }
  else if(L_Q is STS(9))
  {
    return STS-9-AUT()                          // see algorithm 1
  }
  else if(L_Q is STS(13))
  {
    return STS-13-AUT(i)                        // see algorithm 2
  }
  else if(L_Q is STS(15))
  {
    if(i = 1)
    {
      Generate and return all the binary invertible matrices of order 4
    }
    else
    {
      return STS-15-AUT(i)                      // see algorithm 3
    }
  }
}
```

Algorithm 15: Compute the final classes by joining the classes from the automorphism α and β

```
Function Join-Alpha-F-Beta() {
{
  classes ⟵ {}                          // inizialize an empty list
  α_F ⟵ load α_F from disk
  F_β ⟵ load F_β from disk
  foreach( f_1 ∈ Get-Dictionary-Keys(F_β) )do
  {
    S ⟵ ∅                                // initialize an empty set
    foreach( f_2 ∈ Get-Dictionary-Keys(α_F) )do
    {
      if(|F_β[f_1] ∩ α_F[f_2]| > 0)
      {
        S ⟵ S ∪ α_F[f_2]
      }
    }
    Append S to classes
  }
  Save classes to the disk
}
```

Algorithm 16: Compute the precise number of factor systems which produces exactly one Veblen point in the cases: $\mathcal{Q} = \mathrm{STS}(15)$ #1, and $\mathcal{Q} = \mathrm{STS}(15)$ #2

```
Function Classes-Reduction(L_Q, Q_2, i) {
{
  Data: Q_2 is the list of fundamental pairs in Q × Q, and i is the STS(15) table index
  F_β ⟵ load F_β for STS(31) with Q = STS(15) #i from disk
  FS ⟵ ∅                                                  // initialize an empty list of factor systems
  foreach( f ∈ Get-Dictionary-Keys(F_β) )do // take a representative f for each orbit
  {
    c ⟵ As-Vector(f)                                      // represent f as a binary vector (since L_N = GF(2))
    Append c to FS
  }
  good_factor_systems ⟵ ∅    // initialize an empty list of factor systems which do not produce further Veblen
    points
  foreach( f ∈ FS )do
  {
    if( i = 1 )
    {
      // in the case Q = STS(15) #1, any point can produce another Veblen point of S
      S ⟵ Copy(L_Q) \ {Ω}                                 // make a copy of L_Q removing the neutral element
    }
    else if( i = 2 )
    {
      // in the case Q = STS(15) #2, only the point 0 can produce a Veblen point of S
      S ⟵ {0}
    }
    T ⟵ Copy(Q_2)                                         // make a copy of the fundamental pairs
    bad_factor_system_flag ⟵ false
    while( Length(S) > 0 )do
    {
      good_pair ⟵ null
      P ⟵ S[0]                                            // set P as the first element of the list S
      T ⟵ {(A, B) ∈ T : A ≠ P ∧ B ≠ P ∧ A * B ≠ P}        // (*) is the sum in L_Q
      if( Length(T) = 0 ) // f is a good factor system
      {
        break                                             // exit from the S loop
      }
      foreach( (A, B) ∈ T )do
      {
        // check if f(P, A) ⊕ f(P * A, B) ≠ f(A, B) ⊕ f(P, A * B), where (⊕) is the binary addition since
          L_N = GF(2)
        P_A_idx ⟵ Index-Of({P, A}, Q_2)                   // look for the index of the pair {P, A} in Q_2
        PA_B_idx ⟵ Index-Of({P * A, B}, Q_2)              // look for the index of the pair {P * A, B} in Q_2
        A_B_idx ⟵ Index-Of({A, B}, Q_2)                   // look for the index of the pair {A, B} in Q_2
        P_AB_idx ⟵ Index-Of({P, A * B}, Q_2)              // look for the index of the pair {P, A * B} in Q_2
        left_side ⟵ f[P_A_idx] ⊕ f[PA_B_idx]              // compute the left side of the equivalence to check
        right_side ⟵ f[A_B_idx] ⊕ f[P_AB_idx]             // compute the right side of the equivalence to check
        if( left_side ≠ right_side )
        {
          good_pair = (A, B)
          break                                           // exit from the T loop
        }
      }
      if( good_pair is not null)
      {
        (A, B) ⟵ good_pair
        S ⟵ S \ {P, A, B}
      }
      else
      {
        bad_factor_system_flag ⟵ true
        break                                             // exit from the S loop
      }
    }
    if( bad_factor_system_flag is false )
    {
      f' ⟵ As-Integer(f)                                  // represent the vector f of elements in L_N as an integer
      Append f' to good_factor_systems
    }
  }
  Save good_factor_systems to the disk
  Print the number of good_factor_systems
}
```

Bibliography

[1] A. A. Albert. "Quasigroups. I". In: *Transactions of the American Mathematical Society* 54.3 (1943), pp. 507–519. ISSN: 00029947. URL: http://www.jstor.org/stable/1990259.

[2] A. A. Albert. "Quasigroups. II". In: *Transactions of the American Mathematical Society* 55.3 (1944), pp. 401–419. ISSN: 00029947. URL: http://www.jstor.org/stable/1990300.

[3] M. Aschbacher. "On Bol loops of exponent 2". In: *Journal of Algebra - J ALGEBRA* 288 (June 2005), pp. 99–136. DOI: 10.1016/j.jalgebra.2005.03.005.

[4] A. Barlotti and K. Strambach. "The geometry of binary systems". In: *Advances in Mathematics* 49.1 (1983), pp. 1–105. ISSN: 0001-8708. DOI: https://doi.org/10.1016/0001-8708(83)90013-0.

[5] V.D. Belousov. *Foundations of the Theory of Quasigroups and Loops*. 1967.

[6] T. Beth, D. Jungnickel, and H. Lenz. *Design theory*. English. Cambridge etc.: Cambridge University Press. 688 p.; (Orig. publ. by Bibliographisches Institut, Zürich etc.). 1986.

[7] G. Bol. "Gewebe und Gruppen. (Topologische Fragen der Differentialgeometrie LXV)". German. In: *Math. Ann.* 114 (1937), pp. 414–431. ISSN: 0025-5831. DOI: 10.1007/BF01594185.

[8] R. H. Bruck. *A Survey of Binary Systems*. A Survey of Binary Systems v. 20. Springer, 1958. ISBN: 9780387034973. URL: https://books.google.it/books?id=skwfAQAAIAAJ.

[9] R. H. Bruck. "Contributions to the Theory of Loops". In: *Transactions of the American Mathematical Society* 60.2 (1946), pp. 245–354. ISSN: 00029947. URL: http://www.jstor.org/stable/1990147.

[10] R. H. Bruck. "Some Results in the Theory of Linear Non-Associative Algebras". In: *Transactions of the American Mathematical Society* 56.2 (1944), pp. 141–199. ISSN: 00029947. URL: http://www.jstor.org/stable/1990248.

[11] R. H. Bruck. "Some results in the theory of quasigroups." English. In: *Trans. Am. Math. Soc.* 55 (1944), pp. 19–52. ISSN: 0002-9947. DOI: 10.2307/1990138.

[12] M. Buratti and A. Nakić. "Super-regular Steiner 2-designs". English. In: *Finite Fields Appl.* 85 (2023). Id/No 102116, p. 29. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2022.102116.

[13] A. Caggegi, G. Falcone, and M. Pavone. "On the additivity of block designs". English. In: *J. Algebr. Comb.* 45.1 (2017), pp. 271–294. ISSN: 0925-9899. DOI: 10.1007/s10801-016-0707-5.

[14] A. Cayley. "On the Triadic Arrangements of Seven and Fifteen Things". In: *The Collected Mathematical Papers*. Vol. 1. Cambridge Library Collection - Mathematics. Cambridge University Press, 2009, 481–484. DOI: 10.1017/CBO9780511703676.083.

[15] O. Chein. *Examples and methods of construction*. English. Quasigroups and loops: theory and applications, Sigma Ser. Pure Math. 8, 27-93 (1990). 1990.

[16] O. Chein. "Moufang loops of small order. I". English. In: *Trans. Am. Math. Soc.* 188 (1974), pp. 31–51. ISSN: 0002-9947. DOI: 10.2307/1996765.

[17] O. Chein, H. O. Pflugfelder, and J. D. H. Smith, eds. *Quasigroups and loops: theory and applications*. English. Vol. 8. Sigma Ser. Pure Math. Heldermann Verlag, Lemgo; de Gruyter, Berlin, 1990. ISBN: 3-88538-008-0.

[18] C. J. Colbourn, M. Merlini Giuliani, A. Rosa, and I. Stuhl. "Steiner loops satisfying Moufang's theorem". English. In: *Australas. J. Comb.* 63 (2015), pp. 170–181. ISSN: 1034-4942. URL: ajc.maths.uq.edu.au//pdf/63/ajc_v63_p170.pdf.

[19] C.J. Colbourn and J.H. Dinitz. *Handbook of Combinatorial Designs*. Discrete Mathematics and Its Applications. Taylor & Francis, 2006. ISBN: 9781584885061. URL: https://books.google.it/books?id=uu_EngEACAAJ.

[20] C.J. Colbourn and A. Rosa. *Triple Systems*. Oxford mathematical monographs. Clarendon Press, 1999. ISBN: 9780198535768. URL: https://books.google.it/books?id=brpLTq_NMRUC.

[21] F. N. Cole. "Kirkman parades." English. In: *Bull. Am. Math. Soc.* 28 (1922), pp. 380, 435–437. ISSN: 0002-9904. DOI: 10.1090/S0002-9904-1922-03599-9.

[22] F. N. Cole, L. D. Cummings, and H. S. White. "The Complete Enumeration of Triad Systems in 15 Elements." In: *Proceedings of the National Academy of Sciences of the United States of America* 3 3 (1917), pp. 197–9. URL: https://api.semanticscholar.org/CorpusID:39592344.

[23] V. De Pasquale. "Sui sistemi ternari di 13 elementi." Italian. In: *Ist. Lombardo, Rend., II. Ser.* 32 (1899), pp. 213–221. ISSN: 0393-893X.

[24] R. H. F. Denniston. "Sylvester's problem of the 15 schoolgirls". English. In: *Discrete Math.* 9 (1974), pp. 229–233. ISSN: 0012-365X. DOI: 10.1016/0012-365X(74)90004-1.

[25] M. Deza and G. Sabidussi. *Combinatorial structures arising from commutative Moufang loops*. English. Quasigroups and loops: theory and applications, Sigma Ser. Pure Math. 8, 151-160 (1990). 1990.

[26] A. Dharwadker and J. D. H. Smith. "Split extensions and representations of Moufang loops". English. In: *Commun. Algebra* 23.11 (1995), pp. 4245–4255. ISSN: 0092-7872. DOI: 10.1080/00927879508825461.

[27] J. W. Di Paola. "When is a totally symmetric loop a group?" English. In: *Am. Math. Mon.* 76 (1969), pp. 249–252. ISSN: 0002-9890. DOI: 10.2307/2316364.

[28] J. Doyen. "Sur la structure de certains systèmes triples de Steiner". French. In: *Math. Z.* 111 (1969), pp. 289–300. ISSN: 0025-5874. DOI: 10.1007/BF01110238.

[29] J. Doyen, X. Hubaut, and M. Vandensavel. "Ranks of incidence matrices of Steiner triple systems". English. In: *Math. Z.* 163 (1978), pp. 251–259. ISSN: 0025-5874. DOI: 10.1007/BF01174898.

[30] A. Drápal and P. Vojtěchovský. "Explicit constructions of loops with commuting inner mappings." English. In: *Eur. J. Comb.* 29.7 (2008), pp. 1662–1681. ISSN: 0195-6698. DOI: 10.1016/j.ejc.2007.10.001.

[31] S. Eilenberg and S. MacLane. "Algebraic cohomology groups and loops". English. In: *Duke Math. J.* 14 (1947), pp. 435–463. ISSN: 0012-7094. DOI: 10.1215/S0012-7094-47-01437-3.

[32] G. Falcone, Á. Figula, and M. Galici. *Extensions of Steiner loops.* English. Preprint (submitted for publication). 2023.

[33] G. Falcone, Á. Figula, and C. Hannusch. "Steiner loops of affine type". English. In: *Result. Math.* 75.4 (2020). Id/No 148, p. 24. ISSN: 1422-6383. DOI: 10.1007/s00025-020-01273-6.

[34] F. Fenyves. "Extra loops. I". English. In: *Publ. Math. Debr.* 15 (1968), pp. 235–238. ISSN: 0033-3883.

[35] F. Fenyves. "Extra loops. II: On loops with identities of Bol-Moufang type". English. In: *Publ. Math. Debr.* 16 (1970), pp. 187–192. ISSN: 0033-3883.

[36] G. Filippone and M. Galici. *On the number of small Steiner triple systems with Veblen points.* English. Preprint (submitted for publication). 2023.

[37] M. Funk and P. T. Nagy. "On collineation groups generated by Bol reflections". In: *Journal of Geometry* 48.1 (1993), pp. 63–78. DOI: 10.1007/BF01226801. URL: https://doi.org/10.1007/BF01226801.

[38] M. Galici and G. P. Nagy. *An extension formula for right Bol loops arising from Bol reflections.* English. Preprint (submitted for publication). 2023.

[39] *GAP – Groups, Algorithms, and Programming, Version 4.12.2.* The GAP Group, Dec. 2022. URL: https://www.gap-system.org.

[40] G. N. Garrison. "Quasi-groups". English. In: *Ann. Math. (2)* 41 (1940), pp. 474–487. ISSN: 0003-486X. DOI: 10.2307/1968729.

[41] R. L. jun. Griess. "Code loops". English. In: *J. Algebra* 100 (1986), pp. 224–234. ISSN: 0021-8693. DOI: 10.1016/0021-8693(86)90075-X.

[42] A. Grishkov, D. Rasskazova, M. Rasskazova, and I. Stuhl. "Nilpotent Steiner loops of class 2". English. In: *Commun. Algebra* 46.12 (2018), pp. 5480–5486. ISSN: 0092-7872. DOI: 10.1080/00927872.2018.1470243.

[43] A. N. Grishkov and A. V. Zavarnitsine. "commutative center of Moufang loops". In: *arXiv: Group Theory* (2017). URL: https://api.semanticscholar.org/CorpusID:119669337.

[44] W. D. Hale. "Quasi-Groups and Loops Associated with Steiner Systems". In: (1952). DOI: 10.17863/CAM.11455. URL: https://www.repository.cam.ac.uk/handle/1810/265303.

[45] M. Hall and J. D. Swift. "Determination of Steiner Triple Systems of Order 15". In: *Mathematical Tables and Other Aids to Computation* 9.52 (1955), pp. 146–152. ISSN: 08916837. URL: http://www.jstor.org/stable/2002050.

[46] B. A. Hausmann and Ø. Ore. "Theory of quasi-groups". English. In: *Am. J. Math.* 59 (1937), pp. 983–1004. ISSN: 0002-9327. DOI: 10.2307/2371362.

[47] D. Heinlein and P. R. J. Östergård. *Steiner Triple Systems of Order 21 with Subsystems*. 2022. arXiv: 2104.06825 [math.CO].

[48] T. Hsu. "Explicit constructions of code loops as centrally twisted products". English. In: *Math. Proc. Camb. Philos. Soc.* 128.2 (2000), pp. 223–232. ISSN: 0305-0041. DOI: 10.1017/S030500419900403X.

[49] A. Hulpke, D. Stanovský, and P. Vojtěchovský. "Connected quandles and transitive groups". English. In: *J. Pure Appl. Algebra* 220.2 (2016), pp. 735–758. ISSN: 0022-4049. DOI: 10.1016/j.jpaa.2015.07.014.

[50] K. W. Johnson and C. R. Leedham-Green. "Loop cohomology". English. In: *Czech. Math. J.* 40.2 (1990), pp. 182–194. ISSN: 0011-4642.

[51] P. Kaski and P. R. J. Östergård. "The Steiner triple systems of order 19". English. In: *Math. Comput.* 73.248 (2004), pp. 2075–2092. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-04-01626-6.

[52] P. Kaski, P. R. J. Östergård, and A. Popa. "Enumeration of Steiner triple systems with subsystems". English. In: *Math. Comput.* 84.296 (2015), pp. 3051–3067. ISSN: 0025-5718. DOI: 10.1090/mcom/2945.

[53] P. Keevash. "Counting designs". English. In: *J. Eur. Math. Soc. (JEMS)* 20.4 (2018), pp. 903–927. ISSN: 1435-9855. DOI: 10.4171/JEMS/779.

[54] H. Kiechle. *Theory of K-loops*. Vol. 1778. Lecture Notes in Mathematics. Springer-Verlag, Berlin, 2002, pp. x+186. ISBN: 3-540-43262-0. DOI: 10.1007/b83276.

[55] H. Kiechle and G. P. Nagy. "On the extension of involutorial Bol loops". English. In: *Abh. Math. Semin. Univ. Hamb.* 72 (2002), pp. 235–250. ISSN: 0025-5858. DOI: 10.1007/BF02941674.

[56] M. K. Kinyon, J. D. Phillips, and P. Vojtěchovskỳ. "C-loops: extensions and constructions." English. In: *J. Algebra Appl.* 6.1 (2007), pp. 1–20. ISSN: 0219-4988. DOI: 10.1142/S0219498807001990.

[57] M. K. Kinyon, J. D. Phillips, and P. Vojtěchovský. "When is the commutant of a Bol loop a subloop?" English. In: *Trans. Am. Math. Soc.* 360.5 (2008), pp. 2393–2408. ISSN: 0002-9947. DOI: 10.1090/S0002-9947-07-04391-7.

[58] T. P. Kirkman. "On a problem in combinations". In: *Cambridge and Dublin Mathematical Journal* 2 (1847), pp. 191–204. URL: https://cir.nii.ac.jp/crid/1570854175518705920.

[59] T. P. Kirkman. "XIX. On the triads made with fifteen things". In: *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 37.249 (1850), pp. 169–171.

[60] D. Král', E. Máčajová, A. Pór, and J. Sereni. "Characterisation results for Steiner triple systems and their application to edge-colourings of cubic graphs". English. In: *Can. J. Math.* 62.2 (2010), pp. 355–381. ISSN: 0008-414X. DOI: 10.4153/CJM-2010-021-9.

[61] V. Lebed and A. Mortier. "Abelian quandles and quandles with abelian structure group". English. In: *J. Pure Appl. Algebra* 225.1 (2021). Id/No 106474, p. 21. ISSN: 0022-4049. DOI: 10.1016/j.jpaa.2020.106474.

[62] O. Loos. *Symmetric Spaces: General theory*. Mathematics lecture note series. W. A. Benjamin, 1969. ISBN: 9780805366211. URL: https://books.google.it/books?id=TtKU68ZB5GoC.

[63] R. A. Mathon, K. T. Phelps, and A. Rosa. "Addendum to: A class of Steiner triple systems of order 21 and associated Kirkman systems". English. In: *Math. Comput.* 64.211 (1995), pp. 1355–1356. ISSN: 0025-5718. DOI: 10.2307/2153510.

[64] E. H. Moore. "Concerning triple systems." English. In: *Math. Ann.* 43 (1893), pp. 271–285. ISSN: 0025-5831. DOI: 10.1007/BF01443649.

[65] R. Moufang. "Zur Struktur von Alternativkörpern". German. In: *Math. Ann.* 110 (1934), pp. 416–430. ISSN: 0025-5831. DOI: 10.1007/BF01448037.

[66] P. Mulder. Kirkman-*Systemen. (*Kirkman*sche Systeme.)*. Dutch. Groningen, Leiden: P. J. Mulder en Zoon, 308 S. gr. 8° (1917). 1917.

[67] D. C. Murdoch. "Quasi-groups which satisfy certain generalized associative laws". English. In: *Am. J. Math.* 61 (1939), pp. 509–522. ISSN: 0002-9327. DOI: 10.2307/2371517.

[68] G. P. Nagy. "A class of finite simple Bol loops of exponent 2." English. In: *Trans. Am. Math. Soc.* 361.10 (2009), pp. 5331–5343. ISSN: 0002-9947. DOI: 10.1090/S0002-9947-09-04646-7.

[69] G. P. Nagy. "Collineation groups of the smallest Bol 3-nets". In: (Dec. 2004).

[70] G. P. Nagy. "Direct construction of code loops." English. In: *Discrete Math.* 308.23 (2008), pp. 5349–5357. ISSN: 0012-365X. DOI: 10.1016/j.disc.2007.09.056.

[71] G. P. Nagy and P. Vojtěchovský. *LOOPS, Computing with quasigroups and loops in GAP, Version 3.4.3*. https://gap-packages.github.io/loops/. Refereed GAP package. Nov. 2022.

[72] G. P. Nagy and P. Vojtěchovský. "The Moufang loops of order 64 and 81." English. In: *J. Symb. Comput.* 42.9 (2007), pp. 871–883. ISSN: 0747-7171. DOI: 10.1016/j.jsc.2007.06.004.

[73] P. T. Nagy. "Nuclear properties of loop extensions". English. In: *Result. Math.* 74.3 (2019). Id/No 100, p. 27. ISSN: 1422-6383. DOI: 10.1007/s00025-019-1026-7.

[74] P. T. Nagy and K. Strambach. *Loops in Group Theory and Lie Theory*. Berlin, New York: De Gruyter, 2002. ISBN: 9783110900583. DOI: doi:10.1515/9783110900583.

[75] P. T. Nagy and K. Strambach. "Schreier loops." English. In: *Czech. Math. J.* 58.3 (2008), pp. 759–786. ISSN: 0011-4642. DOI: 10.1007/s10587-008-0050-7.

[76] E. Netto. "Zur Theorie der Tripelsysteme." English. In: *Math. Ann.* 42 (1893), pp. 143–152. ISSN: 0025-5831. DOI: 10.1007/BF01443448.

[77] M. Pavone. "A visual representation of the Steiner triple systems of order 13". English. In: *Art Discrete Appl. Math.* 6.3 (2023). Id/No p3.04, p. 22. ISSN: 2590-9770. DOI: 10.26493/2590-9770.1564.2b8.

[78] M. Pavone. "Small configurations and some structure theorems for Steiner triple systems". In: *Combinatorics 2022*. Contributed communication. 2022.

[79] B. Peirce. "Cyclic solutions of the school-girl puzzle". In: *Astronomical Journal, vol. 6, iss. 142, p. 169-174 (1860)*. 6 (1860), pp. 169–174.

[80] K. Petelczyc, M. Prażmowska, K. Prażmowski, and M. Żynel. "A note on characterizations of affine and Hall triple systems". English. In: *Discrete Math.* 312.15 (2012), pp. 2394–2396. ISSN: 0012-365X. DOI: 10.1016/j.disc.2012.03.037.

[81] H.O. Pflugfelder. *Quasigroups and Loops: Introduction*. Sigma series in pure mathematics. Heldermann, 1990. ISBN: 9783885380078. URL: https://books.google.hu/books?id=MQbvAAAAMAAJ.

[82] J. Plücker. *System der analytischen geometrie, auf neue betrachtungsweisen gegründet, und insbesondere eine ausführliche theorie der curven dritter ordnung enthaltend*. Nineteenth Century Collections Online (NCCO): Science, Technology, and Medicine: 1780-1925. Duncker und Humblot, 1835. URL: https://books.google.it/books?id=RYhEy_Bq5jQC.

[83] J. Plücker. *Theorie der algebraischen Curven, gegründet auf eine neue Behandlungsweise der analytischen Geometrie*. Nineteenth Century Collections Online (NCCO): Science, Technology, and Medicine: 1780-1925. A. Marcus, 1839. URL: https://books.google.it/books?id=qNRDWg6fBncC.

[84] R. W. Quackenbush. "Varieties of Steiner loops and Steiner quasigroups". English. In: *Can. J. Math.* 28 (1976), pp. 1187–1198. ISSN: 0008-414X. DOI: 10.4153/CJM-1976-118-1.

[85] D. K. Ray-Chaudhuri and R. M. Wilson. *Solution of Kirkman's schoolgirl problem*. English. Combinatorics, Proc. Sympos. Pure Math. 19, 187-203 (1971). 1971.

[86] K. Reidemeister. *Knotentheorie. Reprint*. German. Berlin-Heidelberg-New York: Springer-Verlag. VI, 74 S. DM 24.00; $ 9.80 (1974). 1974.

[87] M. Reiss. "Ueber eine Steinersche combinatorische Aufgabe, welche im 45sten Bande dieses Journals, Seite 181, gestellt worden ist." ger. In: *Journal für die reine und angewandte Mathematik* 56 (1859), pp. 326–344. URL: http://eudml.org/doc/147768.

[88] D. Stanovský. "Left distributive left quasigroups". PhD thesis. Charles University in Prague, 2004.

[89] J. Steiner. "Combinatorische Aufgaben." ger. In: *Journal für die reine und angewandte Mathematik* 45 (1853), pp. 181–182. URL: http://eudml.org/doc/147524.

[90] K. Strambach and I. Stuhl. "Oriented Steiner loops." English. In: *Beitr. Algebra Geom.* 54.1 (2013), pp. 131–145. ISSN: 0138-4821. DOI: 10.1007/s13366-012-0119-1.

[91] K. Strambach and I. Stuhl. "Translation groups of Steiner loops." English. In: *Discrete Math.* 309.13 (2009), pp. 4225–4227. ISSN: 0012-365X. DOI: 10.1016/j.disc.2008.12.019.

[92] A. Suschkewitsch. "On a generalization of the associative law." English. In: *Trans. Am. Math. Soc.* 31 (1929), pp. 204–214. ISSN: 0002-9947. DOI: 10.2307/1989406.

[93] L. Teirlinck. "On projective and affine hyperplanes". English. In: *J. Comb. Theory, Ser. A* 28 (1980), pp. 290–306. ISSN: 0097-3165. DOI: 10.1016/0097-3165(80)90072-2.

[94] O. Veblen and J. Young. *Projective geometry. Vol. I, II*. English. New York-Toronto-London: Blaisdell Publishing Company. X, 345 p. (1965). 1965.

[95] E. Witt. "Über Steinersche Systeme". In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 12.1 (1937), pp. 265–275. DOI: 10.1007/BF02948948. URL: https://doi.org/10.1007/BF02948948.

[96] K. Zulauf. *Ueber Tripelsysteme von 13 Elementen*. German. Giessen. 22 S. 8° (1897). 1897.