Journal of Algebraic Combinatorics

Extensions of Steiner Loops

--Manuscript Draft--

Manuscript Number:	JACO-D-23-00149
Full Title:	Extensions of Steiner Loops
Article Type:	Manuscript
Keywords:	Steiner triple systems, Steiner loops, Veblen points, Schreier extensions.
Corresponding Author:	Mario Galici University of Palermo Palermo, Sicily ITALY
Corresponding Author Secondary Information:	
Corresponding Author's Institution:	University of Palermo
Corresponding Author's Secondary Institution:	
First Author:	Giovanni Falcone
First Author Secondary Information:	
Order of Authors:	Giovanni Falcone
	Ágota Figula
	Mario Galici
Order of Authors Secondary Information:	
Funding Information:	Università degli Studi di Palermo (FFR2023 Falcone) — Prof. Giovanni Falcone
	Università degli Studi di Palermo — Dr. Mario Galici
	National Research, Development and Innovation Office (K132951) — Prof. Ágota Figula
Abstract:	In this paper we study Steiner triple systems S as extensions of Steiner normal subsystems N by the quotient Steiner systems Q, by means of the associated Steiner loops L S (of projective type). On the one hand, we deal with non-central extensions L S of normal subloops L N of index 2, which form projective hyperplanes N of the Steiner triple systems S. On the other hand, we realize that the set of Veblen points of a Steiner triple system S corresponds to the center of the Steiner loop L S and the loop L S is a Schreier extension of its center by the quotient loop L Q , which is determined by a factor system f. For Schreier extensions we provide in fact a small cohomology theory.

Extensions of Steiner Loops [1]

Giovanni Falcone[2]
Dipartimento di Matematica e Informatica
Università degli Studi di Palermo, Via Archirafi 34, 90123 Palermo, Italy
giovanni.falcone@unipa.it

Agota Figula[3]
Institute of Mathematics
University of Debrecen, P.O. Box 400, H-4002 Debrecen, Hungary
figula@science.unideb.hu

Mario Galici[4]
Dipartimento di Matematica e Informatica
Università degli Studi di Palermo, Via Archirafi 34, 90123 Palermo, Italy
mario.galici@unipa.it

Abstract

In this paper we study Steiner triple systems $\mathcal{S}$ as extensions of Steiner *normal* subsystems $\mathcal{N}$ by the *quotient* Steiner systems $\mathcal{Q}$, by means of the associated Steiner loops $\mathcal{L}_{\mathcal{S}}$ (of projective type). On the one hand, we deal with non-central extensions $\mathcal{L}_{\mathcal{S}}$ of normal subloops $\mathcal{L}_{\mathcal{N}}$ of index 2, which form projective hyperplanes $\mathcal{N}$ of the Steiner triple systems $\mathcal{S}$. On the other hand, we realize that the set of Veblen points of a Steiner triple system $\mathcal{S}$ corresponds to the center of the Steiner loop $\mathcal{L}_{\mathcal{S}}$ and the loop $\mathcal{L}_{\mathcal{S}}$ is a Schreier extension of its center by the quotient loop $\mathcal{L}_{\mathcal{Q}}$, which is determined by a factor system f. For Schreier extensions we provide in fact a small cohomology theory.

Introduction

Steiner triple systems $\mathcal{S} = (\mathcal{P}, \mathcal{T})$, where $\mathcal{P}$ is a set and $\mathcal{T}$ is a family of (unordered) triples (also called blocks or lines) of elements of $\mathcal{P}$ such that any two distinct elements of $\mathcal{P}$ are contained in exactly one triple of $\mathcal{T}$, are among the most acknowledged structures in combinatorics, often appearing at the very beginning in any history of this discipline. Although it has been known since the 50's of the last century ([15], [3]) that, for any triple $\{a, b, c\}$ in a Steiner triple system $\mathcal{S}$, the operation $a \cdot b = c$ (together with $a \cdot a = \Omega \cdot \Omega = \Omega$ and $a \cdot \Omega = \Omega \cdot a = a$, for a further element Ω not in $\mathcal{S}$) gives in turn a commutative loop, an extension theory for Steiner triple systems has not been explored.

Also it seems that the tools provided by loop theory have been underestimated, to the extent that, for instance, a couple of notable results in [17], [22] can be, not only significantly simplified, but even strengthened (see Remark 1.2).

In this paper we study Steiner triple systems by means of a classic algebraic technique, that is, by reducing their structure to that of suitable normal subloops and the corresponding factor loops, leaving the classification of simple Steiner loops to a future investigation. In this respect, we provide only one result, that is, Theorem 1.7, which connects our paper to [23].

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 [9, Ch. 3], but among these methods only one coincides with the extension provided by our construction, that is, the case where the factor loop corresponds to the *degenerate* STS with only one point. This is, as well, the case of *projective hyperplanes*, which in turn were firstly studied by Teirlinck [24] and later by Doyen, Hubaut, and Vandensavel [12].

[1] AMS MSC 05B07, 20N05, 51E10
Keywords: Steiner triple systems, Steiner loops, Veblen points, Schreier extensions.
[2] Supported by Università di Palermo (FFR2023 Falcone)
[3] Supported by the National Research, Development and Innovation Office (NKFIH) Grant No. K132951.
[4] Supported by Università di Palermo

We distinguish the case where the normal subloop is central: after proving that central elements correspond to Veblen points (see Def. 2.7), 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, being the center of the loop, always gives a Steiner triple subsystem of size $2^c - 1$, which is a projective geometry over the field GF(2). The whole Steiner loop, in this case, is a Schreier extension of its center by the quotient loop, which can be described by a factor system f as in Lemma 2.13. In Section 2.3.1 we face with the problem of defining equivalent and isomorphic extensions by means of *coboundaries*, because for loops it is not necessary nor sufficient, for a function ϕ to be a coboundary, that $\delta^2\phi = 0$. Surprisingly enough, we could still use some tools from group theory to classify Steiner triple systems containing Veblen points (see Remark 2.9 and Example 2.18.1).

It is worthwhile to point out that the center of a Steiner loop $\mathcal{L}_\mathcal{S}$ which is not an elementary abelian 2-group has index at least eight (see Theorem 2.14). This means that projective geometries over GF(2) are the only Steiner triple systems of size v with more than $\lceil \frac{v}{16} \rceil$ Veblen points (see Corollary 2.15).

In the case of non-central extensions a significant place is held by extensions of subloops of index 2 (which are normal, see Theorem 1.5): the corresponding subsystems are called projective hyperplanes in the pioneering papers by L. Teirlink [24] and J. Doyen, X. Hubaut and by M. Vandensavel [12]. By means of Theorem 2.5 these extensions are thoroughly characterized by the projective hyperplane and a (further) suitable symmetric Latin square on $\frac{v-1}{2}$ elements (see e.g. Example 2.6.1).

1 General facts

In this section we want to give some classic definitions and prove the basic properties of the main topic of this work: Steiner loops.

We remind the reader that a loop is a set L equipped with a binary operation $\circ$ such that the equations $a \circ x = b$ and $y \circ a = b$ have precisely one solution, for all $a, b \in L$, and having an identity element $\Omega \in L$. The operation of a loop does not need to be associative: when associativity holds, the loop turns out to be a group. A subloop $N \leq L$ is *normal* if it is the kernel of a homomorphism or, equivalently, if the relations

$$x \circ N = N \circ x, \quad x \circ (N \circ y) = (x \circ N) \circ y, \quad x \circ (y \circ N) = (x \circ y) \circ N,$$

hold for any $x, y \in L$. If L is commutative (as it will always be in our case), normality conditions reduce to the only $x \circ (y \circ N) = (x \circ y) \circ N$.

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

$$\begin{aligned} N_\lambda &= \{x \in L \mid (x \circ a) \circ b = x \circ (a \circ b) \text{ for all } a, b \in L\}, \\ N_\mu &= \{x \in L \mid (a \circ x) \circ b = a \circ (x \circ b) \text{ for all } a, b \in L\}, \\ N_\rho &= \{x \in L \mid (a \circ b) \circ x = a \circ (b \circ x) \text{ for all } a, b \in L\}. \end{aligned}$$

The intersection of the three nuclei $N = N_\lambda \cap N_\mu \cap N_\rho$ is called the *nucleus* of L and the subloop

$$Z = \{x \in N \mid x \circ y = y \circ x \text{ for all } y \in L\}$$

is the *center* of L. For a commutative loop, the center coincides with the nucleus.

In the introduction we have already given the definition of Steiner triple systems $\mathcal{S} = (\mathcal{P}, \mathcal{T})$, where any two distinct elements of $\mathcal{P}$ are contained in exactly one triple of $\mathcal{T}$. Throughout the paper we denote, for short, by STS(v) a Steiner triple system of cardinality v. A STS(v) exists if, and only if, $v \equiv 1, 3 \mod 6$ (**in this cases** v **is said to be *admissible***). We point out that in this definition we include the trivial case of the STS(1) having one point and no triple.

Classic examples of Steiner triple systems are given by the point-line designs of projective geometries PG(d, 2) over the field GF(2), or affine geometries AG(d, 3) over the field GF(3), for some $d \geq 0$.

These two items, loops and Steiner triple systems, are closely related, as shown by the following definition.

Definition 1.1. Let $\mathcal{S}$ be a Steiner triple system and let $\Omega \notin \mathcal{S}$ be a further element. The set $\mathcal{L}_\mathcal{S} = \mathcal{S} \cup \{\Omega\}$, with the binary operation $\cdot$ defined by

- for any distinct $x, y \in \mathcal{S}$, $x \cdot y = z$, where z is the third point in the triple of $\mathcal{S}$ containing x and y;
- for any $x \in \mathcal{L}_\mathcal{S}$, $x \cdot x = \Omega$ and $x \cdot \Omega = \Omega \cdot x = x$,

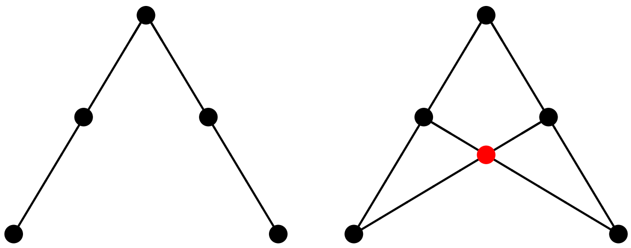
is called a *Steiner loop of projective type*.

Clearly, the equations $ax = b$ and $ya = b$ have the third point of the triple through a and b as the unique solution, and Ω is the identity element of $\mathcal{L}_\mathcal{S}$.

Remark 1.1. While the idea of a loop arising from a STS is classic, the name *of projective type* is new, and we decided to adopt this terminology based on [13], in which the authors study a different loop, corresponding to a given STS, which they call *of affine type*, and which was defined by Chein in [7], putting $x + y + z = \Omega$ whenever $\{x, y, z\}$ is a triple (here Ω is a fixed element of $\mathcal{P}$ and the triples $\{x, \Omega, -x\}$ through Ω define the opposites). Moreover, in our case, the Steiner loop of projective type $\mathcal{L}_\mathcal{S}$ turns out to be a group (more precisely, an elementary abelian 2-group) exactly when the STS $\mathcal{S}$ is a projective geometry $\mathrm{PG}(d, 2)$ over $\mathrm{GF}(2)$, as well as the Steiner loop of affine type $\mathcal{L}_\mathcal{S}$ turns out to be a group (more precisely, an elementary abelian 3-group) exactly when the STS $\mathcal{S}$ is an affine geometry $\mathrm{AG}(d, 3)$ over $\mathrm{GF}(3)$. On the contrary we report in passing that, for $k > 3$, non-trivial Steiner k-tuple systems (that is, v-sets $\mathcal{D}$ admitting a family of k-subsets, called *blocks*, such that any two elements belong to exactly one block) have been recently constructed in [6], with the following property: $\mathcal{D}$ can be given the structure of a commutative group such that the sum of the elements in any block is zero.

Remark 1.2. Here we want to support, with the following examples, our initial assertion that loop theory turns out to be an effective tool for the study of Steiner triple systems.

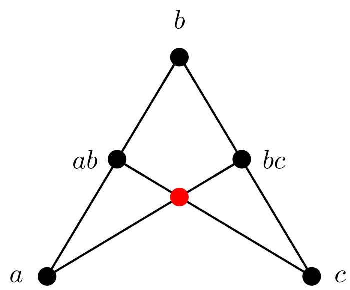
On the one hand, it is very well known that, if any three non-collinear points determine always a Pasch configuration, then the STS is a $\mathrm{PG}(d, 2)$. On the other hand, the same property can be formulated in terms of lack of the anti-Pasch configuration C_{14}.



C_{16} (Pasch) $\quad$ C_{14}

because the lack of the anti-Pasch configuration C_{14} is equivalent to the fact that any three non-collinear points determine always a Pasch configuration.

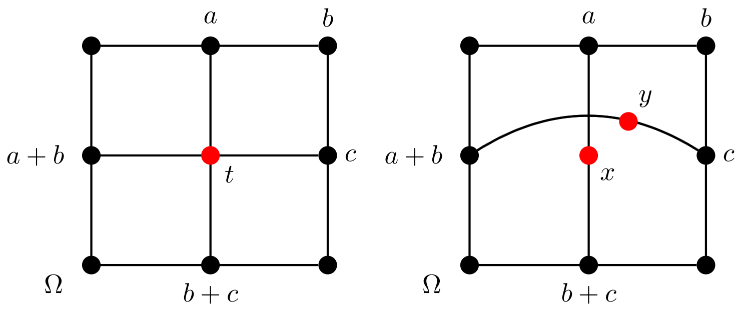
If we translate the Pasch configuration in the setting of loop theory, it simply corresponds to the associativity $a(bc) = (ab)c$:



C_{16} (Pasch)

and this makes the two above characterizations much more direct. Moreover this fact will be sensibly strengthened in Corollary 2.15.

Trying to find a corresponding characterization for $\mathrm{AG}(d,3)$, M. Hall ended up discovering Hall triple systems, which form a family of STS's properly containing the affine geometries over GF(3), and for which in fact any three points belong to an affine plane $\mathrm{AG}(2,3)$. As shown by M. Pavone in [21], the corresponding characterization for Steiner triple systems as affine geometries over GF(3) is that any *four* points belong to an $\mathrm{AG}(3,3)$, 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 noted that if the Steiner loop of affine type associated to a Steiner triple system is not a group (equivalently, the Steiner triple system is not an $\mathrm{AG}(d,3)$), then the three non associating elements form, together with zero, a C_S^1 configuration:



Grid $\qquad$ C_S^1

where $-t=(a+b)+c=a+(b+c)$, $-x=a+(b+c)$, $-y=(a+b)+c$.

This allowed him to strengthen a result by Kral et alii [17] characterizing affine geometries over GF(3) as Steiner triple systems where the configurations C_{16}, C_S^1 and C_S^2 are missing, as well as Hall triple systems where the configurations C_S^1 and C_S^2 are missing. In fact, 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.

If $\mathcal{S}$ is a Steiner triple system, the resulting Steiner loop of projective type $\mathcal{L}_{\mathcal{S}}$ is a commutative loop of exponent 2. Also, it satisfies the totally symmetric property, that is

$$x(xy)=y, \quad \text{for all } x,y\in\mathcal{L}_{\mathcal{S}}.$$

In fact, if $\{x,y,z\}$ is a triple of $\mathcal{S}$, then
$$x(xy)=xz=y.$$
The statement is clearly trivial when $x=\Omega$ or $y=\Omega$.

Remark 1.3. In the case of Steiner loops of projective type, since $\mathcal{L}_{\mathcal{S}}$ fulfills the totally symmetric property, the left, middle and right nuclei coincide, and because of commutativity one has trivially that the nucleus coincides with the center $\mathcal{Z}$ of $\mathcal{L}_{\mathcal{S}}$.

Proposition 1.2. *Let L be a commutative loop of exponent 2. Then the following assertions are equivalent:*

1. *for all $x,y\in L$ one has $x(xy)=y$;*

2. *for all $x,y,z\in L$ one has that $x(yz)=\Omega$ if, and only if, $(xy)z=\Omega$.*

Proof. Assume that 1. is true. If $x(yz)=\Omega$, then $x=yz=zy$, since L is commutative with exponent 2. We compute
$$(xy)z=((zy)y)z=zz=\Omega.$$
If $(xy)z=\Omega$ with a similar computation we obtain that $x(yz)=\Omega$, hence 2. holds.

Assume now that 2. is true. For all $x, y \in L$, putting $z = yx$, we have that $(yx)z = \Omega$, that is equivalent to $y(xz) = \Omega$. From the last equality we obtain that $y = xz$, that is, substituting z, $y = x(xy)$. Hence 1. holds. $\square$

This construction of a loop $\mathcal{L}_{\mathcal{S}}$ arising from a Steiner triple system $\mathcal{S}$ is reversible. Indeed, if $\mathcal{L}$ is a commutative loop of exponent 2 fulfilling the totally symmetric property, then the set $\mathcal{S}_{\mathcal{L}} := \mathcal{L} \setminus \{\Omega\}$ has the structure of a Steiner triple system where the triples $\{x, y, z\}$ are defined by $z := xy$. It is a Steiner triple system since the third point in the triple through x and z is y since $xz = x(xy) = y$. According to Proposition 1.2 the triples $\{x, y, z\}$ of $\mathcal{S}_{\mathcal{L}}$ are characterized by the property that

$$xyz = \Omega,$$

and we want to stress the fact that for any triple in $\mathcal{S}_{\mathcal{L}}$ the associative property holds.
Naturally we have that $\mathcal{S}_{\mathcal{L}_{\mathcal{S}}} = \mathcal{S}$ and $\mathcal{L}_{\mathcal{S}_{\mathcal{L}}} = \mathcal{L}$.

Now we want to settle the basic correspondences between Steiner triple systems and their associated Steiner loops of projective type.

Theorem 1.3. *Let $\mathcal{S}$ be a Steiner triple system and $\mathcal{L}_{\mathcal{S}}$ the corresponding Steiner loop of projective type with identity Ω.*

i) $\mathcal{L}'$ is a subloop of $\mathcal{L}_{\mathcal{S}}$ if, and only if, it holds $\mathcal{L}' = \mathcal{L}_{\mathcal{R}}$, where $\mathcal{R}$ is the Steiner triple subsystem of $\mathcal{S}$ given by $\mathcal{L}' \setminus \{\Omega\}$.

ii) If $\mathcal{L}_{\mathcal{N}}$ is a normal subloop of $\mathcal{L}_{\mathcal{S}}$, then each non-trivial coset $x\mathcal{L}_{\mathcal{N}}$ defines a subsystem $\mathcal{N} \cup x\mathcal{L}_{\mathcal{N}}$ 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 $\mathcal{L}_{\mathcal{S}}/\mathcal{L}_{\mathcal{N}} = \mathcal{L}_{\mathcal{Q}}$, where $\mathcal{Q}$ is 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 $\mathcal{L}_{\mathcal{S}}$, that 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 $x \notin \mathcal{L}_{\mathcal{N}}$. Firstly we note that the cardinality of $\mathcal{N} \cup x\mathcal{L}_{\mathcal{N}}$ is admissible: indeed, if w is the cardinality 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.

Now we want to show that through any two distinct points of $\mathcal{N} \cup x\mathcal{L}_{\mathcal{N}}$ there exists precisely one triple of the STS $\mathcal{S}$ contained in $\mathcal{N} \cup x\mathcal{L}_{\mathcal{N}}$.

Firstly, if xn_1, xn_2 are two distinct elements in the coset $x\mathcal{L}_{\mathcal{N}}$, then $(xn_1) \cdot (xn_2) = n_3 \in \mathcal{L}_{\mathcal{N}}$, since $(x\mathcal{L}_{\mathcal{N}}) \cdot (x\mathcal{L}_{\mathcal{N}}) = \mathcal{L}_{\mathcal{N}}$, that is $\{xn_1, xn_2, n_3\}$ is a triple of $\mathcal{S}$ contained in $\mathcal{N} \cup x\mathcal{L}_{\mathcal{N}}$.

If $xn_1 \in x\mathcal{L}_{\mathcal{N}}$, $n_2 \in \mathcal{N}$, then we have $(xn_1) \cdot n_2 = xn_3$ 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 block $\mathcal{S}$ contained in $\mathcal{N} \cup x\mathcal{L}_{\mathcal{N}}$.

Finally, if n_1, n_2 are two different elements in $\mathcal{N}$, then trivially there exists precisely one triple $\{n_1, n_2, n_1n_2\}$ of $\mathcal{N}$.

Hence the set $\mathcal{N} \cup x\mathcal{L}_{\mathcal{R}}$ is a subsystem of STS $\mathcal{S}$.

iii) This follows from the fact that $\mathcal{L}_{\mathcal{S}}/\mathcal{L}_{\mathcal{N}}$ is a commutative loop of exponent 2 with the totally symmetric property.

$\square$

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 STS.

Definition 1.4. Let v be the cardinality of a STS. 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 1.4.1. Since the factorization $14 = 2 \cdot 7$ is not admissible, we see that the two non-isomorphic STS(13) cannot have normal subsystem, hence the corresponding Steiner loops of projective type are simple.

The next result is known in loop theory, but in this case of Steiner loops we want to give an alternative proof from a more combinatorial point of view.

Theorem 1.5. *If the index of a subloop $\mathcal{L}_\mathcal{N}$ of $\mathcal{L}_\mathcal{S}$ is two, then $\mathcal{L}_\mathcal{N}$ is normal.*

Proof. Since $\mathcal{L}_\mathcal{S}$ is the disjoint union of $\mathcal{L}_\mathcal{N}$ and $\mathcal{L}_\mathcal{S} \backslash \mathcal{L}_\mathcal{N} = {\mathcal{L}_\mathcal{N}}^C$, for each $x \notin \mathcal{L}_\mathcal{N}$, the intersection $x\mathcal{L}_\mathcal{N} \cap \mathcal{L}_\mathcal{N} = \emptyset$ because $x \cdot n \notin \mathcal{L}_\mathcal{N}$ for any $n \in \mathcal{L}_\mathcal{N}$. Hence ${\mathcal{L}_\mathcal{N}}^C = x\mathcal{L}_\mathcal{N}$.

If $x, y \in \mathcal{L}_\mathcal{N}$, then one has $x \cdot (y\mathcal{L}_\mathcal{N}) = x \cdot \mathcal{L}_\mathcal{N} = \mathcal{L}_\mathcal{N} = (x \cdot y)\mathcal{L}_\mathcal{N}$.

If $x \notin \mathcal{L}_\mathcal{N}$ and $y \in \mathcal{L}_\mathcal{N}$, then one has $x \cdot (y\mathcal{L}_\mathcal{N}) = x\mathcal{L}_\mathcal{N} = {\mathcal{L}_\mathcal{N}}^C$ and $(x \cdot y)\mathcal{L}_\mathcal{N} = {\mathcal{L}_\mathcal{N}}^C$ because $x \cdot y$ is not in $\mathcal{L}_\mathcal{N}$.

If $x, y \notin \mathcal{L}_\mathcal{N}$, then we prove that $xy \in \mathcal{L}_\mathcal{N}$ by the following counting argument. The triples $\{x, y, xy\}$ with $x \in \mathcal{S}'$, $y \notin \mathcal{S}'$ (and necessarily $xy \notin \mathcal{S}'$) are exactly

$$\binom{\frac{v+1}{2}}{2}$$

out of the $b = \frac{v(v-1)}{6}$ triples of $\mathcal{S}$. Since the difference is equal to

$$\frac{v(v-1)}{6} - \binom{\frac{v+1}{2}}{2} = \frac{(v-1)(v-3)}{24},$$

which is the number of triples of $\mathcal{N}$. Hence, the triples of $\mathcal{S}$ which are not triples of $\mathcal{N}$ have exactly one point in $\mathcal{N}$. This means that, if $x, y \notin \mathcal{L}_\mathcal{N}$, then $xy \in \mathcal{L}_\mathcal{N}$, hence $(x \cdot y)\mathcal{L}_\mathcal{N} = \mathcal{L}_\mathcal{N}$. Moreover, $x \cdot (y\mathcal{L}_\mathcal{N}) = x{\mathcal{L}_\mathcal{N}}^C = \mathcal{L}_\mathcal{N}$ for the same reason.

We can conclude that $\mathcal{L}_\mathcal{N}$ is a normal subloop in $\mathcal{L}_\mathcal{S}$. □

The same statement is not true when we let the index rise to 4, as shown in the next example.

Example 1.5.1. Let $\mathcal{S} = \{0, 1, \ldots, 9, a, \ldots, e\}$ be the STS(15) with the triples given by the columns of the following table:

$$\boxed{\begin{array}{ccccccccccccccccccccccccccccccccccc}
0&0&0&0&0&0&0&1&1&1&1&1&1&2&2&2&2&2&2&3&3&3&3&4&4&4&4&5&5&5&5&6&6&6&6\\
1&3&5&7&9&b&d&3&4&7&8&b&c&3&4&7&8&9&a&7&8&9&a&7&8&9&c&7&8&a&b&7&8&9&a\\
2&4&6&8&a&c&e&5&6&9&a&d&e&6&5&b&c&d&e&e&d&c&b&a&b&e&d&d&9&c&e&c&e&b&d
\end{array}}\,.$$

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 $\mathcal{L}_\mathcal{N}$.

The following Theorem characterizes normality in small cases.

Theorem 1.6. *Let $\mathcal{S}$ be a Steiner triple system.*

- *If a sub-*STS(1) *$\mathcal{N} = \{x\}$ is normal, then any two different lines through it generate a Fano plane (so x is a so-called* Veblen point*, see Definition 2.7).*
- *If a sub-*STS(3) *is normal, then any outer point generates with it a Fano plane.*

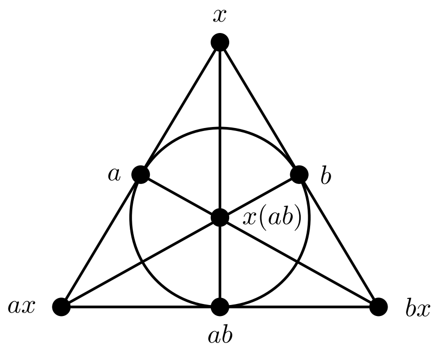
Proof. Let $\mathcal{N} = \{x\}$ be a normal subsystem of $\mathcal{S}$. Then, from the condition

$$y(z\mathcal{L}_{\mathcal{N}}) = (yz)\mathcal{L}_{\mathcal{N}}, \qquad \text{for any } y, z \in \mathcal{L}_{\mathcal{S}},$$

it follows that $y(zx) = (yz)x$, that is, x associates with every other couple of elements of $\mathcal{L}_{\mathcal{S}}$. Let $\ell_1 = \{x, a, xa\}$ and $\ell_2 = \{x, b, xb\}$ be two triples through x with $a \neq b$. Then

$$(bx)a = b(xa) = x(ab), \qquad \text{and} \qquad (ax)(bx) = ab,$$

hence x, ℓ_1 and ℓ_2 generate a Fano plane, as shown in the next figure:



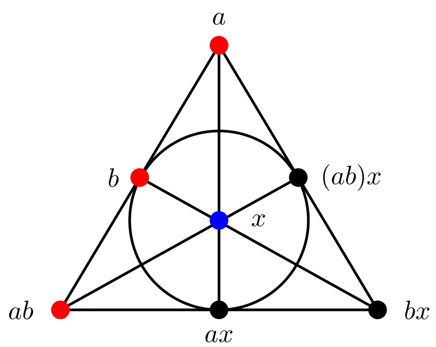
Let $\mathcal{N} = \{a, b, ab\}$ be a normal subsystem of $\mathcal{S}$ and x an outer point. From normality condition, we know that the solutions n_1, n_2, n_3 of the equations

$$x(ab) = (xa)n_1, \quad x(ba) = (xb)n_2, \quad (ax)(xb) = an_3,$$

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

$$x(ab) = (xa)b, \quad x(ba) = (xb)a, \quad (ax)(xb) = ab.$$

This means that $\mathcal{N}$ and x generate a Fano plane, as shown in the next figure:



□

Let $\mathcal{L}_{\mathcal{S}_1}$ and $\mathcal{L}_{\mathcal{S}_2}$ be two Steiner loops with identity Ω_1 and Ω_2 respectively. A homomorphism $\mathcal{L}_{\mathcal{S}_1} \to \mathcal{L}_{\mathcal{S}_2}$ is a map sending Ω_1 to Ω_2 and any triple of $\mathcal{S}_1$ into either a triple of $\mathcal{S}_2$ or into Ω_2.

If $\mathcal{S}_1$ and $\mathcal{S}_2$ have the same cardinality, then the isomorphisms of loops $\mathcal{L}_{\mathcal{S}_1} \to \mathcal{L}_{\mathcal{S}_2}$ corresponds exactly to the isomorphisms of Steiner triple systems $\mathcal{S}_1 \to \mathcal{S}_2$.

If M is a permutation matrix corresponding to an automorphism of a Steiner loop of projective type $\mathcal{L}_{\mathcal{S}}$ with multiplication table T, then M^tTM is the multiplication table of the image loop.

Now we want to give some remarks about the multiplication group of a Steiner loop. In [23] 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 [10]. They also remark that in the Steiner triple systems constructed in [11] from a cyclic group the order of any product of two different translations is odd, as well.

Theorem 1.7. *Let $\mathcal{S}$ be a Steiner triple system with v points, and let $\mathcal{L}_\mathcal{S}$ be the associated Steiner loop of projective type with identity Ω. Then each translation of $\mathcal{L}_\mathcal{S}$ has the form*

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

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. Each translation is products of transpositions because of the definition of Steiner loop of projective type.

Since $v \equiv 1, 3, \mod 6$, then $v \equiv 1, 3, 7, 9, \mod 12$. If $v \equiv 3, 7, \mod 12$, then for the cardinality 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 λ_x for all $x \neq \Omega$ is $\frac{|\mathcal{L}_\mathcal{S}|}{2}$ which is even. Therefore the permutation λ_x is even. Hence the multiplication group $\mathrm{Mult}(\mathcal{L}_\mathcal{S})$ is contained in the group A_{v+1}. Conversely, if $v \equiv 1, 9, \mod 12$, the cardinality of $|\mathcal{L}_\mathcal{S}|$ is not divisible by 4. The number of transpositions in λ_x is odd. Hence the multiplication group $\mathrm{Mult}(\mathcal{L}_\mathcal{S})$ is not contained in the group A_{v+1}. $\square$

Theorem 1.8. *Let $\mathcal{S}$ be a Steiner triple system containing a* STS(9) *and such that the Steiner loop $\mathcal{L}_\mathcal{S}$ is simple. Then $\mathrm{Mult}(\mathcal{L}_\mathcal{S})$ is the alternating group or the symmetric group on $v+1$ elements, according to the cases where v is $3, 7$ or $1, 9 \mod 12$.*

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 [23]. 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. $\square$

2 Extensions of Steiner loops of projective type

In this section we reduce the structure of Steiner loops of projective type to consecutive extensions of simple ones. As one can expect, by considering that the number of Steiner triple systems with n elements increases as $\big(n/e^2 + o(n)\big)^{n^2/6}$ (see [16]), this construction is very flexible, compared with the corresponding extension theory for commutative groups.

We begin by recalling a standard result, which introduces the reader to the idea of studying extensions and simple Steiner loops, that is the motivation of our paper.

Theorem 2.1. *Any Steiner loop $\mathcal{L}_\mathcal{S}$ of projective type has a subnormal series*

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

where the factors $\mathcal{L}_{\mathcal{S}_{i+1}}/\mathcal{L}_{\mathcal{S}_i}$ are simple Steiner loops of projective type.

In Theorem 2.16 we will characterize projective geometries over the field GF(2) in terms of subcentral series.

More generally, we want to study extensions of Steiner loops of projective type. Extensions of normal subloops by (quotient) loops are much more relaxed than in the case of groups (cf. [2] and [4], [18]). For instance, the only extension already considered for Steiner triple systems, that is, the case of a STS(v) $\mathcal{S}$ containing a projective hyperplane, that is STS($\frac{v-1}{2}$), is determined by any given 1-factorization of the complete graph $K_{\frac{v+1}{2}}$ [9].

Definition 2.2. Let $\mathcal{L}_\mathcal{N}$ and $\mathcal{L}_\mathcal{Q}$ be Steiner loops of projective type of order n and m with identity elements Ω' and $\bar{\Omega}$ respectively, and let $\mathrm{Sq}(\mathcal{L}_\mathcal{N})$ be the set of $n \times n$ Latin squares with coefficients in the set $\mathcal{L}_\mathcal{N}$.

An operator $\Phi : \mathcal{L}_\mathcal{Q} \times \mathcal{L}_\mathcal{Q} \longrightarrow \mathrm{Sq}(\mathcal{L}_\mathcal{N})$, which maps the pair (P, Q) to 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 $(P,x),(Q,y) \in \mathcal{L}_{\mathcal{Q}} \times \mathcal{L}_{\mathcal{N}}$.

Remark 2.1. With $P = Q$ and $x = y$, conditions iii) and iv) yield

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

Theorem 2.3. *Let $\mathcal{L}_{\mathcal{N}}$ and $\mathcal{L}_{\mathcal{Q}}$ be two Steiner loops of projective type of order $u+1$, $w+1$ and with identities Ω', $\bar{\Omega}$, respectively. Let $\Phi : \mathcal{L}_{\mathcal{Q}} \times \mathcal{L}_{\mathcal{Q}} \longrightarrow \mathrm{Sq}(\mathcal{L}_{\mathcal{N}})$ be a Steiner operator of projective type.*

If we define on $\mathcal{L}_{\mathcal{S}} = \mathcal{L}_{\mathcal{Q}} \times \mathcal{L}_{\mathcal{N}}$ the multiplication

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

then $\mathcal{L}_{\mathcal{S}}$ is a Steiner loop of projective type 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 $\mathcal{L}_{\mathcal{S}}/\overline{\mathcal{L}_{\mathcal{N}}}$ isomorphic to $\mathcal{L}_{\mathcal{Q}}$. Conversely, any Steiner loop of projective type $\mathcal{L}_{\mathcal{S}}$ having a normal subloop $\mathcal{L}_{\mathcal{N}}$ with corresponding factor loop $\mathcal{L}_{\mathcal{Q}} = \mathcal{L}_{\mathcal{S}}/\mathcal{L}_{\mathcal{N}}$, is isomorphic, for some given Steiner operator Φ, to the above described construction.

Proof. Let $\mathcal{L}_{\mathcal{S}}$ be defined as above.

If (Q,y) and (R,z) are two given elements in $\mathcal{L}_{\mathcal{S}}$, then the equation

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

has a unique solution (P,x), where P is the solution of $QP = R$ in $\mathcal{L}_{\mathcal{Q}}$ 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 Remark 2.1, the element $(\bar{\Omega}, \Omega')$ is the identity of $\mathcal{L}_{\mathcal{S}}$. By Definition 2.2, condition ii), the operation is commutative, by condition iii) $\mathcal{L}_{\mathcal{S}}$ has exponent 2 and condition iv) yields that $(P,x) \cdot \big((P,x) \cdot (Q,y)\big) = (Q,y)$, that is, $\mathcal{L}_{\mathcal{S}}$ fulfills the totally symmetric property.
Thus $\mathcal{L}_{\mathcal{S}}$ is a Steiner loop of projective type. By Definition 2.2, condition i), the subloop

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

is isomorphic to $\mathcal{L}_{\mathcal{N}}$, and it is normal because both $\big((Q,y)(R,z)\big)\overline{\mathcal{L}_{\mathcal{N}}}$ and $(Q,y)\big((R,z)\overline{\mathcal{L}_{\mathcal{N}}}\big)$ coincide with the set

$$\{(PQ,x) : x \in N\}.$$

Conversely, for any Steiner loop $\mathcal{L}_{\mathcal{S}}$ of projective type having a normal subloop $\mathcal{L}_{\mathcal{N}}$ and a corresponding factor loop $\mathcal{L}_{\mathcal{Q}} = \mathcal{L}_{\mathcal{S}}/\mathcal{L}_{\mathcal{N}}$, let $\pi \colon \mathcal{L}_{\mathcal{S}} \longrightarrow \mathcal{L}_{\mathcal{Q}}$ be the canonical epimorphism and $\sigma \colon \mathcal{L}_{\mathcal{Q}} \longrightarrow \mathcal{L}_{\mathcal{S}}$ be 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

$$X = \sigma(\pi(X)) \cdot x, \tag{1}$$

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 $\pi(X),\pi(Y),x,y$. 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 with rows and columns indexed by $\mathcal{L}_{\mathcal{N}}$ as well. Thus we can define an operator $\Phi\colon \mathcal{L}_{\mathcal{Q}} \times \mathcal{L}_{\mathcal{Q}} \longrightarrow \mathrm{Sq}(\mathcal{L}_{\mathcal{N}})$ 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 the couple (P,x) defined in (1), where $P = \pi(X)$. With this representation, the operation of $\mathcal{L}_{\mathcal{S}}$ is given by

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

The first condition of Definition 1.1 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 we say that $\mathcal{L}_{\mathcal{S}}$ is an extension of $\mathcal{L}_{\mathcal{N}}$ by $\mathcal{L}_{\mathcal{Q}}$ or, equivalently, that the short sequence

$$\Omega' \to \mathcal{L}_{\mathcal{N}} \to \mathcal{L}_{\mathcal{S}} \to \mathcal{L}_{\mathcal{Q}} \to \bar{\Omega} \tag{2}$$

is exact.

The next theorem follows from well known facts (cf. [1], § 10 and 11).

Theorem 2.4. *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* $\mathrm{Mult}(\mathcal{L}_{\mathcal{S}})/\mathrm{Mult}(\mathcal{L}_{\mathcal{N}})$.

Theorem 2.5. *Let*

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

be an extension of Steiner loop of projective type with $|\mathcal{L}_{\mathcal{N}}| = u+1$ and $|\mathcal{L}_{\mathcal{Q}}| = w+1$. Then the $(u+1)(w+1) \times (u+1)(w+1)$ multiplication table of $\mathcal{L}_{\mathcal{S}}$ is thoroughly determined by its $w+1$ diagonal $(u+1)\times(u+1)$ symmetric blocks and other $\frac{w(w-1)}{6}$ tables.

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

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

for some Steiner operator Φ, the multiplication table of $\mathcal{L}_{\mathcal{S}}$ is described by the $(w+1)^2$ $(u+1)\times(u+1)$ tables corresponding to the Latin squares $\Phi_{P,Q}$, with $P,Q \in \mathcal{L}_{\mathcal{Q}}$. Every Latin square $\Phi_{P,Q}$ in the main diagonal uniquely determines the Latin squares $\Phi_{\bar{\Omega},P}$ and $\Phi_{P,\bar{\Omega}}$. If $P,Q,R \in \mathcal{L}_{\mathcal{Q}}$ are such that $PQ = R$, 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 in detail.

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

.

□

2.1 Projective hyperplanes

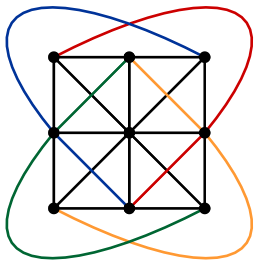
A proper subsystem $\mathcal{S}'$ of $\mathcal{S}$ is called a *projective hyperplane* if every block of $\mathcal{S}$ has a non empty intersection with $\mathcal{S}'$. Equivalently, a subsystem $\mathcal{S}'$ of an STS(v) is a projective hyperplane if, and only if, $|\mathcal{S}'| = \frac{v-1}{2}$: indeed, each of the $\frac{v-1}{2}$ blocks through a point x outside $\mathcal{S}'$ must have exactly one point in common with $\mathcal{S}'$. By cardinality reasons, projective hyperplanes correspond exactly to subloops of index 2, which are normal by Theorem 1.5.

Corollary 2.6. *If $\mathcal{L}_\mathcal{S}$ is a simple loop, then $\mathcal{S}$ does not contain a projective hyperplane. If $\mathcal{L}_\mathcal{S}$ is not simple, and $\mathcal{L}_\mathcal{N}$ is a proper normal subloop of $\mathcal{L}_\mathcal{S}$, then $\mathcal{N}$ is a projective hyperplane of the subsystem $\mathcal{M}$ of $\mathcal{S}$ generated by $\mathcal{N}$ and x, for any $x \in \mathcal{S} \setminus \mathcal{N}$.*

Proof. The first assertion is trivial, and the second follows from the fact that $\mathcal{L}_\mathcal{M}$ turns out to be the union of $\mathcal{L}_\mathcal{N}$, $x\mathcal{L}_\mathcal{N}$. $\square$

Remark 2.2. The problem of classification of STS(v) with a projective hyperplane reduces to the classification of STS$(\frac{v-1}{2})$ together with the classification of symmetric Latin squares of $\frac{v-1}{2}$ letters, where one inserts Ω in the main diagonal.

Example 2.6.1. Here we give an example of a STS(19) having a subsystem $\mathcal{N}$ (of order 9) as a projective hyperplane, corresponding to a normal subloop $\mathcal{L}_\mathcal{N}$ of index 2 in a Steiner loop of projective type of order 20. We can see $\mathcal{N}$ as the affine plane over the field GF(3) with the following configuration.



For $\mathcal{L}_\mathcal{N}$ we fix the following multiplication table:

$\mathcal{L}_\mathcal{N}$:

$\cdot$	Ω'	1	2	3	4	5	6	7	8	9
Ω'	Ω'	1	2	3	4	5	6	7	8	9
1	1	Ω'	6	7	8	9	2	3	4	5
2	2	6	Ω'	9	7	8	1	4	5	3
3	3	7	9	Ω'	5	4	8	1	6	2
4	4	8	7	5	Ω'	3	9	2	1	6
5	5	9	8	4	3	Ω'	7	6	2	1
6	6	2	1	8	9	7	Ω'	5	3	4
7	7	3	4	1	2	6	5	Ω'	9	8
8	8	4	5	6	1	2	3	9	Ω'	7
9	9	5	3	2	6	1	4	8	7	Ω'

The factor loop $\mathcal{L}_\mathcal{Q}$ of order 2 has the multiplication table:

$$\mathcal{L}_\mathcal{Q} : \begin{array}{c|cc} \cdot & \bar{\Omega} & \bar{1} \\ \hline \bar{\Omega} & \bar{\Omega} & \bar{1} \\ \bar{1} & \bar{1} & \bar{\Omega} \end{array}.$$

The elements of $\mathcal{L}_\mathcal{S}$ will be represented by pairs (Px) in $\mathcal{L}_\mathcal{Q} \times \mathcal{L}_\mathcal{N}$ and the addition table of $\mathcal{L}_\mathcal{S}$ will be given by the four 10×10 block matrices $\Phi_{P,Q}$.

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

Note that the Latin square $\Phi_{\bar{\Omega},\bar{\Omega}}$ is the multiplication table of $\mathcal{L}_{\mathcal{N}}$. The Latin square $\Phi_{\bar{1},\bar{1}}$ is a symmetric table such that the identity element Ω is in the main diagonal. We choose for $\Phi_{\bar{1},\bar{1}}$ the table

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

$\cdot$	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'

.

Each of the 45 entries in the upper triangular matrix of $\Phi_{\bar{1},\bar{1}}$ determines a triple of the STS(19), for instance we can read from the table that $(\bar{1},4)+(\bar{1},1)=(\bar{\Omega},2)$ that is $\{(\bar{1},4),(\bar{1},1),(\bar{\Omega},2)\}$ is a triple, we find 45 triples. Each of the found triples gives two entries in the Latin square $\Phi_{\bar{\Omega},\bar{1}}$, as well as in $\Phi_{\bar{1},\bar{\Omega}}=\Phi^t_{\bar{\Omega},\bar{1}}$, respectively, for instance the $\{(\bar{1},4),(\bar{1},1),(\bar{\Omega},2)\}$ triple gives the two entries $\Phi_{\bar{\Omega},\bar{1}}(2,4)=1$ and $\Phi_{\bar{\Omega},\bar{1}}(2,1)=4$. The entries in $\Phi_{\bar{\Omega},\bar{\Omega}}$ yields 12 triples of the STS(19). Hence we obtained all of the 57 triples. Therefore the Latin square $\Phi_{\bar{\Omega},\bar{1}}$ is thoroughly determined as follows

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

$\cdot$	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

.

2.2 Center and Veblen points

In this section we want to characterize the notion of *Veblen points* in an algebraic way and to study a particular class of loop extensions called *Schreier extensions*, that in our case correspond to Steiner triple systems with Veblen points.

We remind the reader that for Steiner loops of projective type the nuclei and the center coincide. On the one hand, the center $\mathcal{Z}$ of a Steiner loop $\mathcal{L}_{\mathcal{S}}$ has cardinality 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 cardinality must divide that of $\mathcal{L}_{\mathcal{S}}$. Thus, one gets $v+1=2^t(w+1)$, where $w+1$ must be the cardinality of the quotient Steiner loop.

Now we want to stress the fact that the non-zero central points of a Steiner loop of projective type are exactly the *Veblen points* of the corresponding Steiner triple system.

Definition 2.7. A point x in a STS $\mathcal{S}$ is a *Veblen point* if whenever $\{x,a,b\}$, $\{x,c,d\}$, $\{t,a,c\}$ are triples of $\mathcal{S}$, also $\{t,b,d\}$ is a triple of $\mathcal{S}$.

The following theorem, that gives an algebraic characterization of Veblen points, leads to a much more general version of the Veblen and Young theorem for STS.

Theorem 2.8. *Let $\mathcal{L}_{\mathcal{S}}$ be a Steiner loop of projective type and $\mathcal{Z}$ be its center. A point $x\in\mathcal{S}$ is a Veblen point if, and only if, $x\in\mathcal{Z}$.*

Proof. Let $x \in \mathcal{S}$ be a Veblen point. If we consider the triples $\{x, xy, y\}$, $\{x, z, xz\}$, $\{t, xy, z\}$ in $\mathcal{S}$, we have that also $\{t, y, xz\}$ is a triple in $\mathcal{S}$. Hence one has that $(xy)z = t = y(xz)$, that is, using commutativity, $z(xy) = (zx)y$. Therefore, x is in central element.

Conversely, let $x \neq \Omega$ be in the center $\mathcal{Z}$. If $\{x, y, xy\}$, $\{x, z, xz\}$ and $\{t, y, xz\}$ are triples of $\mathcal{S}$, then the element $t = y(xz)$ coincides with $(xy)z$, meaning that $\{t, xy, z\}$ is also a triple of $\mathcal{S}$. □

Corollary 2.9. *The set of Veblen points of an* STS(v) *is always a Steiner sub-system, in particular it is a projective geometry of cardinality* $2^c - 1$*, for some integer* $c \geq 0$*.*

Theorem 2.10. *If* $v + 1 = 2^t(w + 1)$ *is an admissible factorization only for* $t = 0$*, then any* 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 cardinality of the quotient projective Steiner loop. □

After the definition of Schreier extensions we will give a necessary and sufficient condition on the existence of STS(v) with (at least) $2^c - 1$ Veblen points.

Further in this paper we will give a construction method to obtain such STS's containing Veblen points.

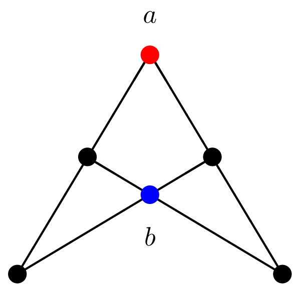
Remark 2.3. If $\mathcal{S}$ is a STS(15), then the cardinality of $\mathcal{Z}$ could be $1, 2, 4, 8$ or 16. Actually, we will see that a STS(15), different from PG$(3, 2)$, can have at most one Veblen point. In particular, in relation to the classification in [8], the STS(15) number 1 is PG$(3, 2)$, the STS(15) number 2 has precisely one Veblen point, which is the point 0, and all the STS(15) from number 3 to 80 have no Veblen points.

Now, in order to show what we claimed in advance in the previous Remark 2.3, we prove a more general fact about Veblen points, Pasch configurations and Fano planes.

Lemma 2.11. *If* $\mathcal{S}$ *is a* STS(v)*, then:*

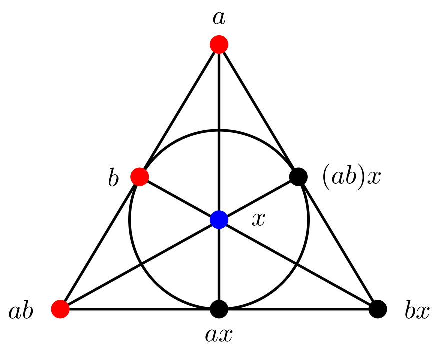
1. *The number of Pasch configurations through a Veblen point is* $\frac{(v-1)(v-3)}{4}$*.*
2. *If* $\mathcal{S}$ *has 2 Veblen points* a, b*, then the third point* $c = ab$ *in the line through them is also a Veblen point, and there are* $\frac{v-3}{4}$ *Fano planes containing the line* $\ell_1 = \{a, b, ab\}$*.*

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 $\{a, b, ab\}$.



This follows from the fact that we cannot choose a, b, ab to be in the Pasch configuration, so we are left with $v-3$ points of the STS(v), and in a Pasch configuration there are 4 further points. 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.

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 shown in the next picture.



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 planes. Hence there are $\frac{v-3}{4}$ different Fano planes containing the Veblen line $\ell = \{a, b, ab\}$.

□

Remark 2.4. If STS(15) $\mathcal{S}$ has more than one Veblen point, then it contains at least a line $\ell = \{a, b, ab\}$ of Veblen points. Fixed another line through a, say $\ell' = \{a, x, ax\} \neq \ell$, there are exactly 2 different Pasch configurations containing both ℓ and ℓ'. Since the number of lines different from ℓ is 6, we can affirm that there are precisely 12 Pasch configurations containing ℓ_1. Since we have 42 different Pasch configurations through every Veblen point a, b or ab, 12 of which contain the whole line ℓ, $\mathcal{S}$ has at least $30 \cdot 3 + 12 = 102$ Pasch configurations. By the table in [8], we can affirm that the only STS(15) with more than one Veblen point is PG$(3, 2)$ (in which every point is a Veblen point).

Now we want to see if there are STS(15) with exactly one Veblen point. If $\mathcal{S}$ is such, then it contains at least 42 Pasch configurations. With this argument, using the table in [8], we can cut out all the STS(15) from number 6 to 80. For the STS(15) number 3, 4 and 5, we note that in the corresponding Steiner loops of projective type the following holds:

$$
\begin{aligned}
7 \cdot (1 \cdot 6) &\neq (7 \cdot 1) \cdot 6, \\
7 \cdot (3 \cdot 1) &\neq (7 \cdot 3) \cdot 1, \\
4 \cdot (0 \cdot 8) &\neq (4 \cdot 0) \cdot 8, \\
1 \cdot (d \cdot a) &\neq (1 \cdot d) \cdot a, \\
c \cdot (9 \cdot 0) &\neq (c \cdot 9) \cdot 0, \\
2 \cdot (b \cdot 5) &\neq (2 \cdot b) \cdot 5.
\end{aligned}
$$

This means that the center of these loops is trivial, and consequently STS(15) number 3, 4 and 5 have no Veblen points.

Finally, if $\mathcal{S}$ is STS(15) number 2, it is easy to see that the point 0 is its only Veblen point by checking that it is in the center of $\mathcal{L}_{\mathcal{S}}$.

2.3 Schreier extensions

As mentioned in the beginning of this section, we are interested in the study of the class of loop extensions called *Schreier extension*, introduced in [20].

Let N be a group with identity Ω', Q be a loop with identity $\bar{\Omega}$, $T\colon Q \to \mathrm{Aut}(N)$ a function of Q into the automorphism group of 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, for a notation in accordance with the literature, we assume the operation of N to be additive and that of Q to be multiplicative. The operation

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

defines on $Q \times N$ a loop L called Schreier extension of N by Q, which contains $\overline{N} = \{(\bar{\Omega}, x) \mid x \in N\} \simeq N$ as a normal subgroup with corresponding quotient loop isomorphic to Q.

In the case of Steiner loops of projective type, if $\mathcal{L}_{\mathcal{S}}$ is a Schreier extension of $\mathcal{L}_{\mathcal{N}}$ by $\mathcal{L}_{\mathcal{Q}}$, $\mathcal{N}$ must be a projective geometry over GF(2), and by Proposition 3.2. in [20] we have that the function T is trivial, $\mathcal{L}_{\mathcal{N}}$ is central and f is symmetric. Hence in Schreier extensions for Steiner loops the multiplication is given by

$$(P,x)\circ(R,y)=\big(PR,x+y+f(P,R)\big),$$

and function f is called a *factor system*. In this case we say that the Steiner triple system $\mathcal{S}$ is a Schreier extension of $\mathcal{N}$ by $\mathcal{Q}$. 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 $\mathcal{S}$. Hence, Schreier extensions allow us to construct Steiner triple systems containing Veblen points. Conversely, 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. [5], p. 334), and this means that any STS $\mathcal{S}$ containing Veblen points can be seen as a Schreier extension of the projective geometry consisting of its Veblen points (or a smaller subsystem).

We note that, if a central subgroup $\mathcal{L}_{\mathcal{N}}\leq\mathcal{L}_{\mathcal{S}}$ has cardinality 2, say $\mathcal{L}_{\mathcal{N}}=\{\Omega',1\}$, then the factor system $f:\mathcal{L}_{\mathcal{Q}}\times\mathcal{L}_{\mathcal{Q}}\to\mathcal{L}_{\mathcal{N}}$ is simply $f(P,R)=\Phi_{P,R}(\Omega,1)+1$, where Φ is the Steiner operator describing $\mathcal{L}_{\mathcal{S}}$ as an extension of $\mathcal{L}_{\mathcal{N}}$ by $\mathcal{L}_{\mathcal{Q}}$.

Theorem 2.12. *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 has cardinality 2^c, then $\frac{v+1}{2^c}$ must be the cardinality of the quotient projective Steiner loop.

The other direction is proved because we can construct such a loop considering a Schreier extension of an elementary abelian 2-group $\mathcal{L}_{\mathcal{N}}$ of cardinality 2^c by a Steiner loop $\mathcal{L}_{\mathcal{Q}}$ of order $\frac{v+1}{2^c}$. $\square$

Remark 2.5. A list of the first 100 cardinalities of STS's which cannot have Veblen points follows:
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.

As for the unmentioned cardinalities, by Theorem 2.12 we can say: any STS(19) has at most one Veblen point, any STS(27) has at most one Veblen point, any STS(39) has at most 3 Veblen points.

Lemma 2.13. *If a Steiner loop of projective type is a Schreier extension of a group* $\mathcal{L}_{\mathcal{N}}$ *by a loop* $\mathcal{L}_{\mathcal{Q}}$, *then the corresponding factor system* f *must be constant on the triples of* $\mathcal{Q}$, *that is*

$$f(P,Q)=f(P,R)=f(Q,R) \tag{3}$$

whenever $\{P,Q,R\}$ *is a triple of* $\mathcal{Q}$. *Moreover, it holds* $f(P,P)=\Omega'$ *for every* $P\in\mathcal{L}_{\mathcal{Q}}$.

Proof. Since $\mathcal{L}_{\mathcal{S}}$ fulfills the totally symmetric property

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

for every $P,Q\in\mathcal{L}_{\mathcal{Q}}$, $x,y\in\mathcal{L}_{\mathcal{N}}$, we have that

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

that is

$$(Q,y+f(P,Q)+f(P,PQ))=(Q,y),$$

which implies

$$f(P,Q)=f(P,PQ).$$

With a similar argument it is easy to check that also $f(P,Q)=f(Q,PQ)$ holds. So, if P and Q are two distinct points of the STS $\mathcal{Q}$, then $\{P,Q,R=PQ\}$ is a triple and we obtain equation (3). If $P=Q\in\mathcal{L}_{\mathcal{Q}}$, then it follows that

$$f(P,P)=f(P,\bar{\Omega})=\Omega'.$$

$\square$

Now we prove a theorem which characterizes Schreier extensions of index at most 4.

Theorem 2.14. *Any Schreier extension $\mathcal{L}_\mathcal{S}$ of index at most 4 is a group.*

Proof. Since the factor loop $\mathcal{L}_\mathcal{Q}$ has cardinality 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

$$(P,x)\circ((Q,y)\circ(R,z)) = ((P,x)\circ(Q,y))\circ(R,z) \tag{4}$$

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 trivial and the extension is splitting, hence $\mathcal{L}_\mathcal{S}$ 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

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

on the other hand we have

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

Hence we have to check that

$$f(P,QR)+f(Q,R) = f(PQ,R)+f(P,Q). \tag{5}$$

- If the three points form the only triple in the underlying STS(3) $\mathcal{Q}$, then by Lemma 2.13 we obtain (5).
- If one of the three points is the identity element, say $P=\bar{\Omega}$ without loss of generality, then $f(\bar{\Omega},QR)+f(Q,R) = f(Q,R)+f(\bar{\Omega},Q)$, recalling that $f(\bar{\Omega},QR)=\Omega'=f(\bar{\Omega},Q)$ by definition of f.
- If two of the three points coincide, say $P=Q$ without loss of generality, then the equation (5) reduces to $f(P,PR)+f(P,R) = f(\bar{\Omega},R)+f(P,P)$. Its right-hand side is Ω', and since $\{P,R,PR\}$ is a triple one has that $f(P,PR)=f(P,R)$, therefore the left-hand side is equal to Ω' as well.

□

It is well known that Steiner triple systems where all points are Veblen points are projective geometries over GF(2), but in the following we give much more relaxed hypotheses.

Corollary 2.15. *If a Steiner triple system $\mathcal{S}$ with cardinality $|\mathcal{S}|<2^d-1$, $d>0$, contains at least 2^{d-4} Veblen points, then it is a projective geometry.*

Proof. Indeed, if we suppose that $\mathcal{S}$ has at least 2^{d-4} Veblen points, the center $\mathcal{Z}$ of $\mathcal{L}_\mathcal{S}$ has at least 2^{d-3} elements. If $|\mathcal{S}|<2rd-1$, then one has $|\mathcal{L}_\mathcal{S}/\mathcal{Z}|<8$. Hence $\mathcal{L}_\mathcal{S}$ is a group and $\mathcal{S}$ is a projective geometry which contains a STS$(2^{d-3}-1)$ as a subsystem. Therefore, $\mathcal{S}$ can either be PG$(d-4,2)$, PG$(d-3,2)$ or PG$(d-2,2)$. □

Remark 2.6. As a consequence of Corollary 2.15, 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. In fact, now we can say even more. If we let d be 5, we have that the only STS(v) with $v<31$ having more than one Veblen point are PG$(1,2)$, PG$(2,2)$ or PG$(3,2)$.

As mentioned after Theorem 2.1, in the next Theorem we characterize projective geometries over GF(2) in terms of subcentral series.

Theorem 2.16. *A Steiner loop $\mathcal{L}_\mathcal{S}$ of projective type has a subcentral series*

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

where the factors $\mathcal{L}_{\mathcal{S}_{i+1}}/\mathcal{L}_{\mathcal{S}_i}$ are Steiner loops of projective type of cardinality 2 if, and only if, $\mathcal{S}$ is a projective geometry PG$(t-1,2)$.

Proof. We prove the first part of the assertion by induction. If $t = 1$, then $\mathcal{L}_\mathcal{S} = \mathrm{GF}(2)$, so $\mathcal{S} = \mathrm{PG}(0, 2)$.

Let now $t > 1$ and assume that $\mathcal{L}_{\mathcal{S}_{t-1}}$ is a projective geometry. Since $\mathcal{L}_{\mathcal{S}_{t-1}}$ is central and of index 2, then by Theorem 2.14 $\mathcal{L}_{\mathcal{S}_t}$ is a group and therefore the STS $\mathcal{S}$ is a projective geometry. In particular, $\mathcal{S} = \mathrm{PG}(t-1, 2)$.

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

Now we give an example of a Steiner loop of projective type $\mathcal{L}_\mathcal{S}$ corresponding to the STS(15) number 2, as a Schreier extension of its center (which has cardinality 2) by the factor loop $\mathcal{L}_\mathcal{Q}$ corresponding to the STS(7).

Example 2.16.1. Let $\mathcal{L}_\mathcal{S}$ be the Schreier extension of $\mathcal{L}_\mathcal{N} = \{\Omega', 1\}$ by $\mathcal{L}_\mathcal{Q} = \{\bar{\Omega}, P_1, \dots, P_7\}$ given by the factor system f such that

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

and f is trivial elsewhere.

If we identify 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) number 2 given in [8], where the triples are given by the columns of the table

$$\boxed{\begin{array}{ccccccccccccccccccccccccccccccccccc}
0&0&0&0&0&0&0&1&1&1&1&1&1&2&2&2&2&2&2&3&3&3&3&4&4&4&4&5&5&5&5&6&6&6&6\\
1&3&5&7&9&b&d&3&4&7&8&b&c&3&4&7&8&b&c&7&8&9&a&7&8&9&a&7&8&9&a&7&8&9&a\\
2&4&6&8&a&c&e&5&6&9&a&d&e&6&5&a&9&e&d&b&c&d&e&c&b&e&d&e&d&c&b&a&e&b&c
\end{array}}\,.$$

2.3.1 A small cohomology theory for Steiner triple systems

In this subsection we want to study a small cohomology theory for Steiner loops of projective type $\mathcal{L}_\mathcal{S}$ which are a Schreier extension of a central subloop $\mathcal{L}_\mathcal{N}$ by a factor loop $\mathcal{L}_\mathcal{Q}$. We denote the group of all factor systems (or, equivalently, of all Schreier extensions) with

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

In fact, in order to stay constructive, we just identify an extension with the corresponding factor system defining the operation.

Remark 2.7. Since a factor system is simply defined by the values it takes on the triples of $\mathcal{Q}$, one easily finds that the number of all possible Schreier extensions of $\mathcal{L}_\mathcal{N}$ by $\mathcal{L}_\mathcal{Q}$ is

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

where b is the number of triples of $\mathcal{Q}$ and 2^t is the cardinality of the elementary abelian 2-group $\mathcal{L}_\mathcal{N}$.

Definition 2.17. Two Schreier extensions $\mathcal{L}_{\mathcal{S}_1}$ and $\mathcal{L}_{\mathcal{S}_2}$ of $\mathcal{L}_\mathcal{N}$ by $\mathcal{L}_\mathcal{Q}$ are *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, if f_1 and f_2 are the corresponding factor systems we write $f_1 \sim f_2$.

Let δ^1 be the cohomology operator defined on the set of all functions $\mathcal{L}_\mathcal{Q} \to \mathcal{L}_\mathcal{N}$ by

$$(\delta^1\varphi)(P,Q) := \varphi(PQ) - (\varphi(P) + \varphi(Q)),$$

adapted from group theory to the non-associative frame of loop theory (recall that $\mathcal{L}_\mathcal{N}$ is a central subgroup of $\mathcal{L}_\mathcal{S}$).

For any $\varphi\colon \mathcal{L}_\mathcal{Q} \to \mathcal{L}_\mathcal{N}$ mapping $\bar\Omega \mapsto \Omega'$, we have that its *coboundary*, that is $\delta^1\varphi$, belongs to $\mathrm{Ext}_\mathrm{S}(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})$, because $(\delta^1\varphi)(P,P) = (\delta^1\varphi)(\bar\Omega, P) = (\delta^1\varphi)(P,\bar\Omega) = \Omega'$ and it is constant on the triples of $\mathcal{Q}$.

Lemma 2.18. *Two factor systems $f_1, f_2 \in \mathrm{Ext}_\mathrm{S}(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})$ are equivalent if, and only if, they differ by a coboundary.*

Proof. If we assume that Φ is an equivalence between the extension given by the factor system f_1 and the one given by f_2, then we have that

$$\Phi(P,x) = \Phi((P,\Omega')(\Omega,x)) = \Phi(P,\Omega')(\Omega,x) = (P,\varphi(P))(\Omega,x) = (P, x+\varphi(P)),$$

for a suitable function $\varphi : \mathcal{L}_\mathcal{Q} \longrightarrow \mathcal{L}_\mathcal{N}$, and, computing the multiplication of two elements, one sees directly that $f_2 = f_1 + \delta^1(\varphi)$. Conversely, if $f_2 = f_1 + \delta^1(\varphi)$, then the map $\Phi(P,x) := (P, x+\varphi(P))$ gives in turn an isomorphism which fixes both $\mathcal{L}_\mathcal{N}$ and $\mathcal{L}_\mathcal{Q}$, hence an equivalence, from the extension corresponding to f_1 to that corresponding to f_2. □

Remark 2.8. In the setting of loop theory, as for groups, factor systems are thoroughly determined by a given section σ, that is a function $\mathcal{L}_\mathcal{Q} \to \mathcal{L}_\mathcal{S}$ such that $\pi\sigma = \mathrm{id}$, where $\pi : \mathcal{L}_\mathcal{S} \to \mathcal{L}_\mathcal{Q}$ is the canonical projection, hence $\sigma(P) = (P, \varphi(P))$, for a suitable function $\varphi : \mathcal{L}_\mathcal{Q} \to \mathcal{L}_\mathcal{N}$. In fact, computing both

$$\sigma(P) + \sigma(Q) = (P,\varphi(P)) + (Q,\varphi(Q)) = (PQ, \varphi(P) + \varphi(Q) + f(P,Q)) \text{ and}$$

$$\sigma(PQ) = (PQ, \varphi(PQ)),$$

we find the difference

$$\sigma(PQ) - (\sigma(P) + \sigma(Q)) = (\bar\Omega, (f + \delta^1\varphi)(P,Q)).$$

Note that we used the fact that $f(PQ,PQ) = \Omega'$ and that $\mathcal{L}_\mathcal{N}$ is a group.

Remark 2.9. Let us denote by $B^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})$ the set $\{\delta^1\varphi \mid \varphi : \mathcal{L}_\mathcal{Q} \to \mathcal{L}_\mathcal{N} \text{ with } \varphi(\bar\Omega) = \Omega'\}$. One has

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

hence the number of non-equivalent Schreier extensions of $\mathcal{L}_\mathcal{N}$ by $\mathcal{L}_\mathcal{Q}$ is

$$\frac{|\mathrm{Ext}_\mathrm{S}(\mathcal{L}_\mathcal{N}, \mathcal{L}_\mathcal{Q})|}{|B^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})|} = \frac{2^{tb} \cdot |\mathrm{Hom}(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})|}{|B^2(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})|}$$

Example 2.18.1. If the loop $\mathcal{L}_\mathcal{S}$ is a Schreier extension of $\mathcal{L}_\mathcal{N}$ by $\mathcal{L}_\mathcal{Q}$, where $|\mathcal{L}_\mathcal{N}| = 2$ and $\mathcal{Q}$ is the Fano plane. One has $|\{\varphi : \mathcal{L}_\mathcal{Q} \to \mathcal{L}_\mathcal{N} \mid \varphi(\bar\Omega) = \Omega'\}| = 2^7$ and $|\mathrm{Hom}(\mathcal{L}_\mathcal{Q}, \mathcal{L}_\mathcal{N})| = 2^3$ and hence $|B^2| = 2^4$. Hence in this case the number of non-equivalent Schreier extensions is $\frac{2^7}{2^4} = 8$.

Definition 2.19. Two Schreier extensions $\mathcal{L}_{\mathcal{S}_1}$ and $\mathcal{L}_{\mathcal{S}_2}$ of $\mathcal{L}_\mathcal{N}$ by $\mathcal{L}_\mathcal{Q}$ are *isomorphic* if there is an isomorphism $\mathcal{L}_{\mathcal{S}_1} \longrightarrow \mathcal{L}_{\mathcal{S}_2}$ which fixes globally both $\mathcal{L}_\mathcal{N}$ and $\mathcal{L}_\mathcal{Q}$.

Of course two equivalent extensions are isomorphic, but the converse is not always true. However, if f_0 is the trivial factor system, that is the map $f_0(P,Q) = \Omega'$ for every $P, Q \in \mathcal{L}_\mathcal{Q}$, then being isomorphic to f_0 and being equivalent to f_0 mean the same thing.

Proposition 2.20. *Let $\mathcal{L}_{\mathcal{S}_1}$ and $\mathcal{L}_{\mathcal{S}_2}$ be two Schreier extensions of $\mathcal{L}_{\mathcal{N}}$ by $\mathcal{L}_{\mathcal{Q}}$. Every isomorphism of extensions $\mathcal{L}_{\mathcal{S}_1} \to \mathcal{L}_{\mathcal{S}_2}$ has, up to equivalence, the following form*

$$(P, x) \longmapsto (\beta(P), \alpha(x)), \tag{6}$$

for some suitable $\alpha \in \mathrm{Aut}(\mathcal{L}_{\mathcal{N}})$ and $\beta \in \mathrm{Aut}(\mathcal{L}_{\mathcal{Q}})$.

Proof. Since for any isomorphism of extension $\Psi : \mathcal{L}_{\mathcal{S}_1} \to \mathcal{L}_{\mathcal{S}_2}$ we have $\Psi(\mathcal{L}_{\mathcal{N}}) = \mathcal{L}_{\mathcal{N}}$ and $\Psi(\mathcal{L}_{\mathcal{Q}}) = \mathcal{L}_{\mathcal{Q}}$, we obtain that

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

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 $\bar{\Omega} \mapsto \Omega'$, and also that

$$\Psi(\bar{\Omega}, x) = (\bar{\Omega}, \alpha(x)), \text{ for any } x \in \mathcal{L}_{\mathcal{N}}, \tag{7}$$

where α is a suitable automorphism of $\mathcal{L}_{\mathcal{N}}$. Hence

$$\Psi(P, x) = \Psi\big((P, \Omega') \circ (\bar{\Omega}, x)\big) = (\beta(P), \varphi(P)) \circ (\bar{\Omega}, \alpha(x)) = (\beta(P), \alpha(x) + \varphi(P)).$$

By Lemma 2.18, up to an equivalence we can suppose φ to be trivial and the assert is proved. □

Fixed $\mathcal{L}_{\mathcal{N}}$ and $\mathcal{L}_{\mathcal{Q}}$, if f_1 and f_2 are two isomorphic factor systems and Ψ is an isomorphism of the corresponding extensions, by Proposition 2.20, from the relation

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

we obtain that

$$\Psi(PQ, x + y + f_1(P, Q)) = (\beta(P), \alpha(x)) \circ (\beta(Q), \alpha(y)),$$

that is

$$\big(\beta(PQ), \alpha(x) + \alpha(y) + (\alpha f_1)(P, Q)\big) = \big(\beta(P)\beta(Q), \alpha(x) + \alpha(y) + f_2(\beta(P), \beta(Q))\big).$$

Hence, we have (up to a co-boundary) the relation

$$\alpha f_1 = f_2 \beta, \tag{8}$$

where with $f\beta : \mathcal{L}_{\mathcal{Q}} \times \mathcal{L}_{\mathcal{Q}} \to \mathcal{L}_{\mathcal{N}}$ we denote, for simplicity, the factor system $(P, Q) \mapsto f(\beta(P), \beta(Q))$. Equation (8) can be rewritten as

$$f_1 = \alpha^{-1} f_2 \beta. \tag{9}$$

This defines an action of the group $\mathrm{Aut}(\mathcal{L}_{\mathcal{N}}) \times \mathrm{Aut}(\mathcal{L}_{\mathcal{Q}})$ on the set $\mathrm{Ext}_S(\mathcal{L}_{\mathcal{N}}, \mathcal{L}_{\mathcal{Q}})/\sim$ of non-equivalent extensions given by

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

whose orbits are the isomorphism classes of all the factor systems.

Example 2.20.1. 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) having the points

$$\begin{aligned} \{P_1 = (-1, 1),\ P_2 = (0, 1),\ P_3 = (1, 1),\ P_4 = (-1, 0),\ P_5 = (0, 0), \\ P_6 = (1, 0),\ P_7 = (-1, -1),\ P_8 = (0, -1),\ P_9 = (1, -1)\} \end{aligned}$$

and the triples

$$\begin{array}{cccc} \{P_1, P_2, P_3\}, & \{P_1, P_4, P_7\}, & \{P_1, P_5, P_9\}, & \{P_1, P_6, P_8\}, \\ \{P_2, P_4, P_9\}, & \{P_2, P_5, P_9\}, & \{P_2, P_6, P_7\}, & \{P_3, P_4, P_8\}, \\ \{P_3, P_5, P_7\}, & \{P_3, P_6, P_9\}, & \{P_4, P_5, P_6\}, & \{P_7, P_8, P_9\}. \end{array}$$

Let us consider the Schreier extension given by the factor system 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' for any other couple of points.

The automorphism β of $\mathcal{L}_{\mathcal{Q}}$ induced by the affine map $x \mapsto Ax + b$ of AG(3, 2), with $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $b = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$, permutes the points of $\mathcal{Q}$ as follows:

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

Let us consider the factor system $f_2 := f_1\beta$, that is given by

$$f_1(P_3, P_4) = f_1(P_3, P_8) = f_1(P_4, P_8) = 1$$

and Ω' for any other couple of points. Clearly f_1 and f_2 are isomorphic. Furthermore, they are equivalent if, and only if, $f_1 - f_2 = \delta^1\varphi$ for a suitable function $\varphi : \mathcal{L}_{\mathcal{Q}} \to \mathcal{L}_{\mathcal{N}}$. A straightforward computer calculation shows that such a function φ does not exist.

2.3.2 Steiner triple systems with a unique factorization

In this last section we want to give some results concerning Steiner loops of cardinality $v + 1$ which admit just one admissible factorization of the type $v + 1 = 2(w + 1)$.

Theorem 2.21. *All the Steiner loops $\mathcal{L}_{\mathcal{S}}$ of projective type with cardinality $n = v + 1$ are simple if $n \not\equiv 4$ and $8 \mod 12$. On the contrary, if $n \equiv 4$ or $8 \mod 12$, then there exists a Steiner loop $\mathcal{L}_{\mathcal{S}_1}$ of order n which is a Schreier extension of a normal subgroup $\mathcal{L}_{\mathcal{N}_1}$ of order 2, and there exists also a Steiner loop $\mathcal{L}_{\mathcal{S}_2}$ of order n which is an extension of a normal subloop $\mathcal{L}_{\mathcal{N}_2}$ (corresponding to a projective hyperplane) of order $\frac{n-2}{2}$ by a factor loop $\mathcal{L}_{\mathcal{Q}}$ of order 2.*

Proof. Since the STS $\mathcal{S}$ has cardinality $v \equiv 1$ or $3 \mod 6$, one has $v \equiv 1, 3, 7,$ or $9 \mod 12$. If $n = v+1 \equiv 4$, or $8 \mod 12$, then $n = 2\cdot(w+1)$ is an admissible factorization and w is the cardinality of a projective hyperplane. Hence we can construct both a Steiner loop $\mathcal{L}_{\mathcal{S}_1}$ of order n, which has a normal subgroup $\mathcal{L}_{\mathcal{N}_1}$ of order 2 (hence central), and also we can construct a Steiner loop $\mathcal{L}_{\mathcal{S}_2}$ of projective type of order n which has a normal subgroup $\mathcal{L}_{\mathcal{N}_2}$ corresponding to a projective hyperplane.

On the contrary, if $n \equiv 2$ or $10 \mod 12$, then $n = 2 \cdot (w + 1)$ with w an even integer, meaning that n do not have any admissible factorization, hence any Steiner loop of cardinality n must be simple. □

Corollary 2.22. *Let $\mathcal{L}_{\mathcal{S}}$ be a Steiner loop of projective type with cardinality $v + 1$ and suppose that it has a unique admissible factorization $v + 1 = 2(w + 1)$. Then $\mathcal{L}_{\mathcal{S}}$ belongs to one of the following families:*

- *Simple Steiner loops;*
- *Schreier extensions of the group of order 2 by a Steiner loop corresponding to a* STS(w)*;*
- *Extensions of a Steiner loop corresponding to a projective hyperplane by the group of order 2.*

As a consequence of the above Corollary it is possible, in principle, to construct all the non-simple STS(v) admitting the unique factorization $v+1 = 2(w+1)$. In [14] this has been done for the two smallest meaningful cases $v = 19, 27$, as well as for six (out of 80) most interesting cases with $v = 31$, represented as Schreier extensions of a group with two elements by a Steiner loop of order 16 chosen among the 80 STS(15) given in [8].

Data availability
We do not analyse or generate any datasets, because our work proceeds within a theoretical and mathematical approach. One can obtain the relevant materials from the references below.

Conflict of interest statement
All authors have no conflicts of interest.

References

[1] A. A. Albert, *Quasigroups I*, Trans. Amer. Math. Soc. 54 (3), 507-519, DOI 10.1090/s0002-9947-1943-0009962-7 (1943)

[2] A. A. Albert, *Quasigroups II*, Trans. Amer. Math. Soc. 55 (1944), 401–419.

[3] R. H. Bruck, A survey of binary systems. Ergebnisse der Math. und ihrer Grenz., 20, Springer, (1958)

[4] R. H. Bruck, *Some results in the theory of linear non-associative algebras*, Trans. Amer. Math. Soc. **56**, (1944), 141–199.

[5] R. H. Bruck, Contributions to the Theory of Loops, *Trans. Amer. Math. Soc.*, **60** (1946) 245–354.

[6] M. Buratti and A. Nakić, *Super-regular Steiner 2-designs,* Finite Fields Appl. **85**, Article ID 102116, 29 p. (2023)

[7] O. Chein, *Examples and methods of construction*, in: *Quasigroups and Loops: Theory and Applications*, eds: O. Chein, H. O. Pflugfelder, J. D. H. Smith, Heldermann (1990), pp. 27-93.

[8] Ch. J. Colbourn, J. H. Dinitz, *Handbook of Combinatorial Designs*, Discrete mathematics and its applications, CRC Press, Taylor and Francis Group, 2007

[9] Ch. J. Colbourn, A. Rosa, *Triple Systems*, Oxford mathematical monographs, Clarendon Press, 1999

[10] M. Deza, G. Sabidussi, Combinatorial structures arising from commutative Moufang loops, in: O. Chein, H.O. Pflugfelder, J.D.H. Smith (Eds.), Quasigroups and Loops: Theory and Applications, Heldermann Verlag, Berlin, 1990, pp. 151-160.

[11] J. Doyen, Sur la structure de certains systèmes triples de Steiner, Math. Z. 111 (1969) 289-300.

[12] J. Doyen, X. Hubaut, M. Vandensavel, *Ranks of Incidence Matrices of Steiner Triple Systems.* Mathematische Zeitschrift 163: 251-260, DOI 10.1007/bf01174898 (1978)

[13] G. Falcone, A. Figula, C. Hannusch, *Steiner Loops of Affine Type.* Results in Mathematics, 75 (4), DOI 10.1007/s00025-020-01273-6 (2020).

[14] G. Falcone, G. Filippone, M. Galici, *On the number of small Steiner triple systems with Veblen points* (Preprint) (2023)

[15] W. D. Hale, *Quasi-Groups and Loops Associated with Steiner Systems.* PhD Dissertation, University of Cambridge, https://doi.org/10.17863/CAM.11455 (1952).

[16] P. Keevash, Counting designs, J. Eur. Math. Soc. 20, 903-927 (2018)

[17] D. Král, E. Máčajová, A. Pór, and J.-S. Sereni, *Characterization results for Steiner triple systems and their application to edge-colorings of cubic graphs*, Canad. J. Math., 62 (2), pp. 355-381, (2010)

[18] P. T. Nagy, *Nuclear Properties of Loop Extensions*, Results in Math. 74:100, DOI 0.1007/s00025-019-1026-7 (2019)

[19] P. T. Nagy and K. Strambach, *Loops in Group Theory and Lie Theory*, De Gruyter Exposition in Mathematics 35, Berlin, New York, DOI 10.1515/9783110900583 (2002)

[20] P. T. Nagy and K. Strambach, *Schreier Loops*, Czechoslovak Math. J. 58 (133), 759–786, DOI 10.1007/s10587-008-0050-7 (2008)

[21] M. Pavone, *Small configurations and some structure theorems for Steiner triple systems*, contributed communication, Combinatorics 2022 (Mantua May 31, 2022)

[22] K.Petelczyc, M.Prażmowska, K.Prażmowski, M.Żynel *A note on characterizations of affine and Hall triple systems*, Discrete Mathematics 312 (15) 2394-2396, DOI 10.1016/j.disc.2012.03.037 (2012)

[23] K. Strambach, I. Stuhl, *Translation groups of Steiner loops.* Discrete Mathematics, 309(13), 4225-4227. DOI 10.1016/j.disc.2008.12.019 (2009)

[24] L. Teirlinck, *On Projective and Affine Hyperplanes.* J. Comb. Th. A, 28, 290-306 (1980).