Finite geometries and related loops and quasigroups

Diana Rasskazova

Tese apresentada
ao
Instituto de Mathemática e Estatística
da
Universidade de São Paulo
para obtenção do título
Doutor em Ciênçias

Programa: Doutorado em Matematica do IME-USP
Orientador: Prof. Ivan Chestakov
Co-orientador: Prof. Alexandre Grichkov

Durante o desenvolvimento deste trabalho o autor recebeu financeiro da Fundação de Amparo à Pesquisa do Estado de São Paulo

Setembro 2018

Finite geometries and related loops and quasigroups

Comissão Julgadora:

- Ivan Chestakov(Presidente), IME-USP.
- Alexandre Kornev, UFABC,
- Dmitry Logachev, UFAM,
- Plamen Emilov Kochloukov, UNICAMP,
- Henrique Guzzo Junior, IME-USP.

Acknowledgement

I thank my family for the support has been given me during all these years of study.

I am very grateful to my supervisor and co-supervisor, Profs. Ivan Chestakov and Alexander Grichkov, for their patience, confidence, coaching and opportunities.

I thank the Research Support Foundation of the State of Sao Paulo (FAPESP) for financial support during the PhD (Process 2015 / 17611-8).

Agradecimentos

Agradeço o apoio que minha família dispensou a mim durante todos esses anos de estudo.

Agradeço imensamente meu orientador e corientador, Profs. Ivan Chestakov e Alexandre Grichkov, pela paciência, pela confiança, pelos ensinamentos e pelas oportunidades.

Agradeço à Fundação de Amparo à Pesquisa do Estado de São Paulo pelo apoio financeiro durante o Doutorado (Processo 2015/17611-8).

Absract

RASSKAZOVA D. **Finite geometries and related loops and quasigroups** 2018. 40 pp. PhD thesis- Instituto de Matematica e Estatitica, Universidade de São Paulo, São Paulo, 2018

This work is about finite geometries with 3 or 4 points on every line and related loops and quasigroups.

In the case of 3 points on any line we describe the structure of free loops in the variety of corresponding Steiner loops and we calculate the group of automorphisms of free Steiner loop with three generators.

We describe the structure of nilpotent class two Steiner loops and classifiy all such loops with three generators.

In the case of 4 points on a line we constructe new series of such geometries as central extension of corresponding non-commutative Steiner quasigroups. We conjecture that those geometries are universal in some sense.

Key-words: Steiner systems, Steiner loops, nilpotent loops, central extension, Steiner quasigroups.

Resumo

RASSKAZOVA D.L. **Geometrias finitas, loopos e quasigrupos relacionados** 2018. 40 pp. Tese(Doutorado)- Instituto de Matemática e Estatítica, Universidade de São Paulo, São Paulo, 2018

Este trabalho é sobre as geométrias finitas com 3 ou 4 pontos na cada reta e os loops e qiasigrupos relacionados. Em caso de 3 pontos na cada reta descrevemos o loop de Steiner correspondente livre e calculamos o grupo de automorfismos em caso de 3 geradores livres. Além disso descrevemos os loopos de Steiner nilpotentes de clase dois e classificamos estes loopos com 3 geradores.

Em caso de 4 pontos na cada reta construimos as geometrias novas atraves de expanção central de um análogo não comutativo do quasigrupo de Steiner. Temos fortes indícios que esta construção é universal em algum sentido.

Palavras-chave: Sitemas de Steiner, loopos de Steiner, loopos nilpotentes, expanção central, quasigrupo de Steiner.

Contents

Chapter 1

Introduction

Steiner triple systems as special block designs are a major part of combinatorics, and there are many interesting connections developed between these combinatorial structures and their algebraic aspects. In this thesis we consider Steiner triple systems from algebraic point of view, i.e., we study the corresponding Steiner loops. Diassociative loops of exponent 2 are commutative, and the variety of all diassociative loops of exponent 2 is precisely the variety of all Steiner loops, which are in a one-to-one correspondence with Steiner triple systems (see [2], p. 310).

Since Steiner loops form a variety (moreover a Schreier variety), we can deal with free objects. Consequently, we use the term *free Steiner triple systems* for the combinatorial objects corresponding to free Steiner loops. A summary of results about varieties of Steiner loops, Steiner quasigroups and free objects in the varieties can be found in [13].

We give a construction of free Steiner loops, determine their multiplication groups (which is a useful knowledge for loops, see [17], Section 1.2)). The problem of calculation of multiplication group for finite Steiner loops have been represented in [8] and in [19] in the case of finite oriented Steiner loops. We also show that the nucleus of the free Steiner loops are trivial, which is an indicator of how distant these loops are from groups.

The automorphism group of a Steiner triple system $\mathfrak{S}$ coincides with the automorphism group of the Steiner quasigroup as well as with the automorphism group of the Steiner loop associated with $\mathfrak{S}$. Any finite group is the automorphism group of a Steiner triple system ([16], Theorem 8, p. 103). This motivated

the goal of our paper to study automorphisms of the free Steiner triple systems. We prove that (i) all automorphisms of the free Steiner loops are tame, and (ii) the automorphism group of a free Steiner loop is not finitely generated when the loop is generated by more than 3 elements.

We also determine the generators of the automorphism group of the 3-generated free Steiner loop and give conjectures about automorphisms of this loop. Recall that in the case of linear Nielsen-Schreier varieties of algebras in the the work [20] was proved that the all automorphisms are tame and all relation are "trivial." We formulate conjecture that all relations in the group of automorphisms of the free $3-$generated Steiner loop has the same "trivial" form.

The results of second chapter are published in article [3].

The results of third chapter are accepted in article [4].

The results of fourth chapter are not published yet.

1.1 Preliminaries

A set L with a binary operation $L \times L \longrightarrow L : (x, y) \mapsto x \cdot y$ is called a *loop*, if for given a, b, the equations $a \cdot y = b$ and $x \cdot a = b$ are uniquely solvable, and there is an element $e \in L$ such that $e \cdot x = x \cdot e = x$ for all $x \in L$. A loop is called *diassociative* if every two elements generate a group.

A loop L is called *Steiner loop* if $x \cdot (x \cdot y) = y$ holds for all $x, y \in L$ and $x^2 = e$ for all $x \in L$, where e is the identity of L.

A *Steiner triple system* $\mathfrak{S}$ is an incidence structure consisting of set of points and blocks such that every two distinct points are contained in precisely one block, and any block has precisely three points. It means that every Steiner system $\mathfrak{S}$ is a set with fixed subsets $L(\mathfrak{S})$ such that for every $\sigma \in L(\mathfrak{S})$ we have $|\sigma| = 3$ and for every two elements $x, y \in \mathfrak{S}$ there exists unique $\sigma \in L(\mathfrak{S})$ such that $x, y \in \sigma$. It is a well-known fact that a Steiner triple system of order m (where m is a number of points), exists if and only if $m \equiv 1, 3 \bmod (6)$ (cf. [7], Definition V.1.9).

To a given Steiner triple system, there correspond two different constructions leading to distinct algebraic structures.

A Steiner triple system $\mathfrak{S}$ determines a multiplication $x \cdot y$ on the pairs of

different points x, y taking as a product the third point of the block joining x and y, in other word $x \cdot y = z$, if $\{x, y, z\}$ is a block of this Steiner system. Define $x \cdot x = x$ we get a *Steiner quasigroup* associated with $\mathfrak{S}$. Recall that a Steiner quasigroup P is a set with commutative multiplication $\cdot$ such that $x \cdot x = x$ and $y \cdot z = x$, $x \cdot z = y$, if $x \cdot y = z$. Adjoining an element e with $ex = xe = x$, $xx = e$ we obtain the Steiner loop S.

Conversely, a Steiner loop S determines a Steiner triple system whose points are the elements of $S \setminus \{e\}$, and the blocks are the triples $\{x, y, xy\}$ for $x \neq y \in S \setminus \{e\}$. The quasigroup or loop obtained in this way is called an *exterior* Steiner quasigroup or an *exterior* Steiner loop. This yields the first of the aforementioned constructions. Because it is more popular than the other one, the term 'exterior' will be omitted.

Let describe the construction of *interior Steiner loop*. Let a be some fixed element of $\mathfrak{S}$ and $IS(\mathfrak{S}) = (\mathfrak{S}, a, \cdot)$ be a main isotope of the corresponding to $\mathfrak{S}$ Steiner quasigroup. It means that the multiplication in $\mathfrak{S}$ is given by the formula $x \cdot y = y \cdot x = (ax)(ay)$. Then $x^2 = x \cdot x = (ax)(ax) = ax$, and hence $x^2 \cdot y^2 = xy$, $x^3 = x(ax) = a$ and $(xy)y = (x^2 \cdot y^2)^2 \cdot y^2 = x$.

Conversely, from a commutative loop S with identities $x^3 = 1, (x^2y^2)^2y^2 = x$, a Steiner triple system can be recovered, with blocks $\{x, y, x^2y^2\}$, if $a \neq x \neq y \neq a$ and $\{a, x, x^2\}$ for any $x \neq a$. This construction in a different framework appears in [13] p. 23. A loop obtained in this way is called an *interior Steiner loop*.

A loop L is said to be *totally symmetric* if $x \cdot y = y \cdot x$ and $x \cdot (x \cdot y) = y$ for all $x, y \in L$. A totally symmetric loop of exponent 2 is called a *Steiner loop*. A variety of universal algebras is called a *Schreier variety* if every subalgebra of any free algebra in that variety is also free in that variety. Steiner loops form a Schreier variety; it is precisely the variety of all diassociative loops of exponent 2 (see in [2] p. 310). Steiner loops are in a one-to-one correspondence with Steiner triple systems. Multiplication groups of Steiner loops have been studied in [8]. Central extensions of Steiner loops and quasigroups yielding algebraic structures of Steiner triple systems with cyclic orientations on each triple have been introduced in [9, 10].

The *left, right*, respectively, *middle nucleus* of a loop L are the subgroups of

L defined by

$$N_l(L) = \{u;\ (u \cdot x) \cdot y = u \cdot (x \cdot y),\ x, y \in L\},$$

$$N_r(L) = \{u;\ (x \cdot y) \cdot u = x \cdot (y \cdot u),\ x, y \in L\},$$

$$N_m(L) = \{u;\ (x \cdot u) \cdot y = x \cdot (u \cdot y),\ x, y \in L\}.$$

The intersection $N(L) = N_l(L) \cap N_r(L) \cap N_m(L)$ is the *nucleus* of L.

The *commutant* $C(L)$ of a loop L is the subset consisting of all elements $c \in L$ such that $c \cdot x = x \cdot c$ for all $x \in L$. The *center* $Z(L)$ of L is the intersection $C(L) \cap N(L)$.

A loop L is *nilpotent* if the series L, $L/Z(L)$, $[L/Z(L)]/Z[L/Z(L)]$ ... terminates at 1 in finitely many steps. In particular, L is of *nilpotency class two* if $L/Z(L) \neq 1$ and is an abelian group.

For $x, y, z \in L$, define the *associator* (x, y, z) of x, y, z as the unique element in L such that $(xy)z = (x(yz))(x, y, z)$. The *associator subloop* $Ass(L)$ of L is the smallest normal subloop H of L such that L/H is a group. Thus, $Ass(L)$ is the smallest normal subloop of L containing associators (x, y, z) for all $x, y, z \in L$.

For any $x \in L$ the maps $\lambda_x : y \mapsto x \cdot y$ and $\rho_x : y \mapsto y \cdot x$ are the *left* and the *right translation*s, respectively. The permutation group generated by the left and right translations of loop L is called the *multiplication group* of L, and the stabilizer of the neutral element is called the *inner mapping group* of L. More facts about this objects can be found in [12].

1.2 Constructions of free Steiner loops

Constructions of free Steiner loops have been given by several authors: see e.g., [13], [15]. Nevertheless, we provide here a specific construction; it will help to incorporate a transparent interpretation and to establish a natural system of notation.

Let $\mathtt{X}$ be a finite ordered set and let $W(\mathtt{X})$ be a set of non-associative $\mathtt{X}$-words. For every word $v \in W(\mathtt{X})$ its length $|v|$ is a number of letters which it contains. The set $W(\mathtt{X})$ has an order such that $v > w$ if and only if $|v| > |w|$ or

$|v| = |w| > 1$, $v = v_1v_2$, $w = w_1w_2$, $v_1 > w_1$ or $v_1 = w_1, v_2 > w_2$. Next, we define the set $S(\mathtt{X})^* \subset W(\mathtt{X})$ of S-words by induction on the length of word:

- $\mathtt{X} \subset S(\mathtt{X})^*$,
- $vw \in S(\mathtt{X})^*$ precisely if, $v, w \in S(\mathtt{X})^*$, $|v| \leq |w|$, $v \neq w$ and if $w = w_1 \cdot w_2$, then $v \neq w_i$, $(i = 1, 2)$.

On $S(\mathtt{X}) = S(\mathtt{X})^* \cup \{\emptyset\}$ we define a multiplication in the following manner:

1. $v \cdot w = w \cdot v = vw$ if $vw \in S(\mathtt{X})$,
2. $(vw) \cdot w = w \cdot (vw) = w \cdot (wv) = (wv) \cdot w = v$,
3. $v \cdot v = \emptyset$.

A word $v(x_1, x_2, ..., x_n)$ is *irreducible*, if $v \in S(\mathtt{X})^*$.

Lets consider some facts which are proved in the second chapter:

Proposition 1. *The set $S(\mathtt{X})$ with the multiplication as above is a free Steiner loop with free generators $\mathtt{X}$.*

Proposition 2. *Let $G = \mathrm{Mult}(S(\mathtt{X}))$ be the group of right multiplications of the free Steiner loop $S(\mathtt{X})$. Then*

1. *$G = \underset{v \in S(\mathtt{X})^*}{*} C_v$ is a free product of cyclic groups of order 2;*
2. *G acts on $S(\mathtt{X})$, and $G = \{R_v | v \in S(\mathtt{X})\}\mathrm{Stab}_G(\emptyset)$. Moreover, the inner mapping group $\mathrm{Stab}_G(\emptyset)$ is a free subgroup of G generated by $R_vR_wR_{vw}$, $v, w \in S(\mathtt{X})$.*

Proposition 3. *If x, y are different elements of the free Steiner loop $S(\mathtt{X})$ and $|\mathtt{X}| > 2$, then there is an element $z \in S(\mathtt{X})$ such that*

$$(xy)z \neq x(yz).$$

Chapter 2

Free Steiner systems and its automorphisms

2.1 Free Steiner loops

In this chapter we are going to prove propositions formulated above at 1.2.

The proof of proposition 1.

The definition implies that $S(\mathtt{X})$ is commutative, $a \cdot (a \cdot b) = b$ for all $a, b \in S(\mathtt{X})$ and if $a, b \in S(\mathtt{X})$ then $\{a, b, a \cdot b, \emptyset\}$ is a group of order 4 and exponent 2. Hence $S(\mathtt{X})$ is free diassociative of exponent 2, i.e., a free Steiner loop. $\square$

Let (G, H, B) be a Baer triple (see [11]), i.e., $G = BH$ is a group, H is a subgroup in G, B is a set of transversals for G/H with $b^2 = 1, b \in B, B \cap H = 1$. For any $b_1, b_2 \in B$ the product $b_1 b_2$ may be written uniquely in the form $b_1 b_2 = b_3 h_1$, where $b_3 \in B$, $h_1 \in H$. Then B admits a multiplication $b_1 * b_2 = b_3$. Let suppose that this multiplication is commutative. Clearly $b * b = 1$ and $(b_1 * b_2) * b_2 = b_1$. Indeed, $(b_1 * b_2) * b_2 = b_3 * b_2 = b_2 * b_3 = b_2 * (b_2 b_1 {h_2}^{-1}) = b_1$ since $b_2 b_2 b_1 {h_2}^{-1} = b_1 {h_2}^{-1}$. This yields that $(B, *)$ is a Steiner loop. We call such a decomposition $G = BH$ an *S-decomposition*.

If the intersection $\underset{x \in G}{\cap} H^x = \{1\}$ then $G \simeq \mathrm{Mult}((B, *))$.

We note that any Steiner loop can be constructed in the above fashion. Indeed, let $G = \mathrm{Mult}(B)$ be the multiplication group of the Steiner loop B and let $B_0 = \{R_b | b \in B\}$, $H =< R_a R_b R_{ab} | a, b \in B >$. Then $G = B_0 H$ is an S-decomposition.

The proof of proposition 2.

Let $G = \mathrm{Mult}(S(\mathtt{X}))$ be the group of right multiplications of the free Steiner loop $S(\mathtt{X})$. Then

1. $G \simeq \underset{v \in S(\mathtt{X})^*}{*} C_v$ is a free product of cyclic groups of order 2;

   Indeed, if $x \in S(\mathtt{X})$, $g \in \underset{v \in S(\mathtt{X})^*}{*} C_v$, where $C_v = \{e, R_v\}$, then $g = \prod_v R_v = R_{v_1}...R_{v_m}$ and $y = x^g = (...(xv_1)...)v_m)$. By definition of the free product we have that $v_i \neq v_{i+1}, 1 \leq v < m$. Hence for some chose of X we get $y \neq x$. Hence $g \neq 1$ as element of $\mathrm{Mult}(S(\mathtt{X}))$.

   Inverse, if $h \in \mathrm{Mult}(S(\mathtt{X}))$, then $h = R_{v_1}...R_{v_m}$, $v_i \neq v_{i+1}, 1 \leq v < m$. Hence $h \in \underset{v \in S(\mathtt{X})^*}{*} C_v$, where $C_v = \{e, R_v\}$.

2. G acts on $S(\mathtt{X})$, and $G = \{R_v | v \in S(\mathtt{X})\}\mathrm{Stab}_G(\emptyset)$. Moreover, the inner mapping group $\mathrm{Stab}_G(\emptyset)$ is a free subgroup of G generated by $R_v R_w R_{vw}$, $v, w \in S(\mathtt{X})$.

   It is clear that $(\emptyset)R_v R_w R_{vw} = \emptyset$, moreover, since $R_v = L_v$, then $\mathrm{Stab}_G(\emptyset)$ is generated by the set $\{R_v R_w R_{vw} | v, w \in S(\mathtt{X})\}$.

   The subgroup $\mathrm{Stab}_G(\emptyset)$ is free by the Kurosh subgroup theorem [14] p. 17.

□

The proof of proposition 3.

If x, y are different elements of the free Steiner loop $S(\mathtt{X})$ and $|\mathtt{X}| > 2$, then there is an element $z \in S(\mathtt{X})$ such that $(xy)z \neq x(yz)$.

Let $x = v_1(x_1, ..., x_n)$ and $y = v_2(x_1, ..., x_n)$. Suppose we choose the element z in the shape $z = v_2(x_1, ..., x_n) \cdot x_j$, where x_j is one of the generators different from the last letter of $v_2(x_1, ..., x_n)$. Then we have that

$$(xy)z = (v_1(x_1, ..., x_n) \cdot v_2(x_1, ..., x_n))(v_2(x_1, ..., x_n)x_j)$$

$$\neq v_1(x_1, ..., x_n) \cdot (v_2(x_1, ..., x_n) \cdot v_2(x_1, ..., x_n)x_j) = v_1(x_1, ..., x_n)x_j = x(yz).$$

□

As was mentioned earlier, the nucleus of a loop can be interpreted as a 'measure' of the non-associativity. As a corollary of the previous Proposition, we can conclude that the free Steiner loops are 'very far' from groups:

Corollary 4. *The nucleus and therefore the center of free Steiner loops are trivial.*

2.2 Automorphisms

Let $\mathtt{Y} = \{y_1, y_2, ..., y_n\}$ be a set of free generators of $S(\mathtt{X})$. Then $\varphi_i : \mathtt{Y} \longrightarrow S(\mathtt{X})$, $\varphi_i(y_i) = y_i \cdot v$, $\varphi_i(y_j) = y_j$, $j \neq i$, $v \in S(\mathtt{Y} \setminus y_i)$ As φ_i is defined on the set $\mathtt{Y}$ of free generators, it may be extended to some automorphism of $S(\mathtt{X})$, called an *elementary automorphism* (or an $\mathtt{Y}$-*elementary automorphism*) and we will denote it by $\varphi_i = e_i(v)$. Let $\mathrm{T}(\mathtt{X})$ denote a subgroup of the group of automorphisms $\mathrm{Aut}(S(\mathtt{X}))$ of loop $S(\mathtt{X})$ generated by the $\mathtt{X}$-elementary automorphisms. Automorphisms contained in $\mathrm{T}(\mathtt{X})$ are called $tame$ (or $\mathtt{X} - tame$). In Theorem 7 below we show that $\mathrm{Aut}(S(\mathtt{X})) = \mathrm{T}(\mathtt{X})$.

Let $\mathtt{Y} = \{y_1, y_2, ..., y_m\} \subset S(\mathtt{X})$, then set $\mathtt{Y}$ is said to be *reducible*, if there exist i and $v \in S(\mathtt{Y} \setminus y_i)$ such that $|y_i \cdot v| < |y_i|$. The set $\mathtt{Y}$ is said to be *irreducible*, if it is not reducible.

Let $S(\mathtt{Z})$ be a free Steiner loop with free generators $\mathtt{Z} = \{z_1, ..., z_m\}$, let $\mathtt{Y} = \{y_1, \ldots, y_m\}$ be a set of elements of $S(\mathtt{X})$ and let $\varphi : S(\mathtt{Z}) \longrightarrow S(\mathtt{Y}) : z_i \mapsto y_i$ be a homomorphism. A set $\mathtt{Y}$ is called *free isometric*, if φ is an isomorphism and $|\varphi(v(z_1, ..., z_m))| = ||v(z_1, ..., z_m)||$. Here $||v(z_1, ..., z_m)||$ is the length with weights $|y_1|$, ..., $|y_m|$, it means that $||v(z_1, ..., z_m)|| = n_1|y_1| + ... + n_m|y_m|$, where n_i is the number of times that the letter z_i appears in the word $v(z_1, ..., z_m)$.

Proposition 5. *A set* $\mathtt{Y}$ *is irreducible if and only if* $\mathtt{Y}$ *is free isometric.*

Proof. Let $\mathtt{Y}$ be an irreducible subset of $S(\mathtt{X})$, $S(\mathtt{Z})$ be a free Steiner loop with free generators $\mathtt{Z} = \{z_1, ..., z_m\}$ and let $\varphi : S(\mathtt{Z}) \longrightarrow S(\mathtt{Y}) : z_i \mapsto y_i$ be a homomorphism. We show that φ is an isometric isomorphism.

Let us choose $v \in \mathrm{Ker}\varphi$ of minimal length and set $v = v_1 \cdot v_2$, then $\varphi(v_1) = \varphi(v_2)$. Assume that $v_1 = w_1 \cdot w_2$ and $v_2 = w_3 \cdot w_4$ are irreducible, then we have $\varphi(w_1) \cdot \varphi(w_2) = \varphi(w_3) \cdot \varphi(w_4)$. Suppose that these decompositions are irreducible. Then we get that $\varphi(w_4) = \varphi(w_1)$ or $\varphi(w_4) = \varphi(w_2)$. This yields a contradiction with the minimality of the choice of v in both cases.

Now we assume, that the decomposition $\varphi(w_1) \cdot \varphi(w_2)$ is reducible, then $\varphi(w_1) = u_1 \cdot \varphi(w_2)$. Hence $u_1 = \varphi(w_5)$ and $\varphi(w_1) = \varphi(w_5 \cdot w_2)$. Since the decomposition $w_1 \cdot w_2$ is irreducible, $w_1 = w_6 \cdot w_7$, $\varphi(w_6) = w_5$ and $\varphi(w_7) = \varphi(w_2)$. Moreover, $w_7 \neq w_2$ and therefore $w_2 \cdot w_7 \in \mathrm{Ker}\varphi$ and $|w_2 \cdot w_7| > |v_1 \cdot v_2|$. But since $|v_1| > |w_2|$, we have $|v_2| < |w_7| < |w_1| < |v_1|$. This proves the assertion. $\square$

Corollary 6. *If* $\mathtt{Y}$ *is irreducible then* $S(\mathtt{Y}) = S(\mathtt{X})$ *precisely if* $\mathtt{Y} = \mathtt{X}$.

Later on we will prove that all automorphisms of the free Steiner loops are tame.

Theorem 7. *Let* $S(\mathtt{X})$ *be a free Steiner loop with a finite set of free generators* $\mathtt{X}$. *Then* $\mathrm{Aut}(S(\mathtt{X})) = \mathrm{T}(\mathtt{X})$.

Proof. Let φ be an automorphism of $S(\mathtt{X})$ and let $\mathtt{Y} = \varphi(\mathtt{X})$. We prove that $\varphi \in \mathrm{T}(\mathtt{X})$ by induction on $|\mathtt{Y}| = \sum_{i=1}^{n} |y_i|$.

First we note that the permutations of $\mathtt{X}$ are tame automorphisms. For any transposition $(ij) \in \mathcal{S}_n(\mathtt{X})$ we have $(ij) = \phi\psi\phi$ with

$$\phi = e_i(x_j) \quad \text{and} \quad \psi = e_j(x_i).$$

Since the symmetric group $\mathcal{S}_n(\mathtt{X})$ of permutations of $\mathtt{X}$ is generated by transpositions, one has $\mathcal{S}_n(\mathtt{X}) \subset \mathrm{T}(\mathtt{X})$.

If $|\mathtt{Y}| = n$ then $\varphi \in \mathcal{S}_n(\mathtt{X})$ and therefore $\varphi \in \mathrm{T}(\mathtt{X})$. Now suppose that $|\mathtt{Y}| > n$. By Corollary 6 the set $\mathtt{Y}$ is reducible and hence for some i and $v = v(y_1, ..., \widehat{y_i}, ..., y_n)$ we have $|y_i \cdot v| < |y_i|$. By the induction assumption the map $\psi(x_1, \ldots, x_n) = (y_1, \ldots, y_{i-1}, y_i \cdot v, \ldots, y_n)$ induces an $\mathtt{X}$-tame automorphism of $S(\mathtt{X})$. Set

$$w = v(y_1, ..., \widehat{y_i}, ..., y_n)^{\psi^{-1}} = v(x_1, ..., \widehat{x_i}, ..., x_n).$$

Then $\lambda(x_1, ..., x_i, ..., x_n) = (x_1, ..., x_i \cdot w, ..., x_n)$ is an $\mathtt{X}$-elementary automorphism. Then $\varphi = \lambda\psi$ since $x_j^{\lambda\psi} = x_j^{\psi} = y_j$ for $j \neq i$ and $x_i^{\lambda\psi} = (x_i \cdot w)^{\psi} = (y_i \cdot v) \cdot w^{\psi} = (y_i \cdot v) \cdot v = y_i$.

Consequently, $\varphi \in \mathrm{T}(\mathtt{X})$; this completes the proof of the theorem. $\square$

Lemma 8. *Let $\phi = e_i(v)$, $v \in S(\mathtt{X} \setminus i)$ be an $\mathtt{X}$-elementary automorphism and suppose $u = u_1u_2$ is an $\mathtt{X}-$irreducible decomposition of a word $u \in S(\mathtt{X})$. Then either $u_1^\phi u_2^\phi$ is an $\mathtt{X}-$irreducible decomposition of u^ϕ or $u^\phi = x_i$, in this case $u_1 = x_i$ and $u_2 = v$.*

Proof. We will use induction on the length $|u|$ of the word u. First suppose that $u_1^\phi u_2^\phi$ is an $\mathtt{X}$-reducible decomposition of u^ϕ. It means that $u_1^\phi = u_3u_2^\phi$ is also an $\mathtt{X}$-irreducible decomposition, and hence $u_1 = u_3^\phi u_2$. If $u_1 = u_3^\phi u_2$ is an $\mathtt{X}$-irreducible decomposition then $u = u_1u_2$ is $\mathtt{X}$-reducible, which yields a contradiction.

Therefore, $u_1 = u_3^\phi u_2$ is $\mathtt{X}$-reducible, where $u_1 = x_i$, $u_2 = v$, $u_3 = x_i$. Suppose $|u_3| > 1$, $|u_2| > 1$, $u_3 = wx_i$ and $u_2 = yv$, it is clear that $w \neq x_i \neq v \neq y$. Then $u_3^\varphi u_2 = [w(x_iv)] \cdot yv$ is $\mathtt{X}$-reducible if and only if $w = yv$ or $x_i = y$. In the first case we get that $u_1^\varphi u_2^\varphi = x_i \cdot yv$ is $\mathtt{X}$-irreducible. In the second case $u_1 = u_3^\phi u_2 = w$ and $u_1u_2 = w(x_iv)$ is $\mathtt{X}$-irreducible. Hence, $u_1^\varphi u_2^\varphi = wx_i$ is also $\mathtt{X}$-irreducible decomposition of u^ϕ. $\square$

Define a normal chain of characteristic ($\mathrm{Aut}(S(\mathtt{X}))-$invariant) subloops of $S(\mathtt{X})$:

$$S_0 = S(\mathtt{X}) > S_1 > S_2 > \cdots > S_i > \ldots \quad . \tag{2.1}$$

Here S_0/S_1 is a group, and for any i, $Z_i = S_i/S_{i+1}$ is the center of the factor loop S_0/S_{i+1}. Moreover, each S_i is a minimal subloop with these properties.

Now we deal with the question whether the automorphism group of a free Steiner loop with n generators is finitely generated for $n > 3$.

Theorem 9. *The automorphism group $\mathrm{Aut}(S(\mathtt{X}))$ of the free Steiner loop $S(\mathtt{X})$ is not finitely generated when $|\mathtt{X}| > 3$.*

Proof. Owing to Theorem 7 and by a discussion afterwards, the group $G = \mathrm{Aut}(S(\mathtt{X}))$ is generated by $\{e_i(v) | v \in S(\mathtt{X})\}$. If G is finitely generated then G is generated by a set $P = \{e_{j_i}(v_i) | v_i \in S(\mathtt{X}), i = 1, \ldots, m\}$.

Let $S(\mathtt{X}) > S_1 > S_2 > \cdots > S_i > \ldots$ be a chain of normal characteristic subloops as in (2.1). Choose a number p such that $v_i \notin S_p$, $i = 1, \ldots, m$, and $1 \neq v \in S_p$. We assume that

$$e_j(v) = e_{j_1}(v_1) \cdot \cdots \cdot e_{j_m}(v_m).$$

For any $w \in S(\mathtt{X})$ we set (i) $||w|| = (s,t)$, if $w = w_1 w_2$ is an $\mathtt{X}-$irreducible decomposition, $w_1 > w_2 \neq 1$, $w_1 \in S_s \setminus S_{s+1}$, $w_2 \in S_t \setminus S_{t+1}$ and (ii) $||x|| = (1,0)$, if $x \in \mathtt{X}$.

We prove that $||x_j e_{j_1}(v_1) \cdot \dots \cdot e_{j_r}(v_r)|| = (1,s)$, with $s < m$, by induction on r. For $r = 1$ this is clear, and we suppose that for r this fact is true.

Set:

$$u = x_1 e_{j_1}(v_1) \cdot \dots \cdot e_{j_r}(v_r) e_i(w), \quad q = x_1 e_{j_1}(v_1) \cdot \dots \cdot e_{j_r}(v_r) = q_1 q_2.$$

By the induction hypothesis we have $||q_1|| = 1$, $||q_2|| = s < m$.

If $q_1^{e_i(w)} q_2^{e_i(w)}$ is an $\mathtt{X}-$irreducible decomposition then $||q^{e_i(w)}|| = ||q|| = (1,s)$, since S_s is a characteristic subloop. If $q_1^{e_i(w)} q_2^{e_i(w)}$ is an $\mathtt{X}-$reducible decomposition then, by Lemma 8, $q^{e_i(w)} = u = x_i$ and $||u|| = (1,0)$. We obtain that $x_j^{e_j(v)} = x_j v$ and $||x_j e_{j_1}(v_1) \cdot \dots \cdot e_{j_m}(v_m)|| = (1,s)$, with $s < m$. However, this contradicts to the fact $||x_j v|| = (1,m)$. This completes the inductional step.

Therefore our assumption that G is finitely generated does not hold. $\square$

The group $\mathrm{Aut}(S(\mathtt{X})) = \mathrm{T}(\mathtt{X})$ is generated by $\mathtt{X}$-elementary automorphisms $e_i(v)$, $v \in S(\mathtt{X} \setminus \{i\})$, with $e_i(v)^2 = 1$; this follows from the definition. Thus, a natural question arises:

Problem 1. Which relations exist between $\mathtt{X}$-elementary automorphisms of the free Steiner loop $S(\mathtt{X})$?

We stress, that there is no relation among the elements $\{e_i(v) | v \in S(\mathtt{X} \setminus x_i)\}$.

In what follows we focus on the 3-generated free Steiner loop $S(x_1, x_2, x_3)$. Contrary to the case of the automorphism group of free Steiner loop with $n > 3$-generators, we prove that the group $\mathrm{Aut}(S(x_1, x_2, x_3))$ is generated by three involutions (12), (13) and $\varphi = e_1(x_2)$.

Theorem 10. *Let $S(\mathtt{X})$ be a free Steiner loop with free generators $\mathtt{X} = \{x_1, x_2, x_3\}$. Then the group of automorphisms $\mathrm{Aut}(S(\mathtt{X}))$ is generated by the symmetric group $\mathcal{S}_3$ and by the elementary automorphism $\varphi = e_1(x_2)$.*

Proof. Let G_0 be the subgroup of $\mathrm{Aut}(S(\mathtt{X}))$ generated by $\mathcal{S}_3$ and φ. If G_0 is a proper subgroup, then let ϕ be an element of $\mathrm{Aut}(S(\mathtt{X})) \setminus G_0$. The length of $\phi(x_1, x_2, x_3) = (u, v, w)$ is the sum of the length of the generators under ϕ, i.e., $|\phi| = |u| + |v| + |w|$.

The claim of Theorem 10 can be verified by induction on the length of element $\phi \in \mathrm{Aut}(S(\mathtt{X})) \setminus G_0$. For $|\phi| = 3$, it is trivial. Now if $|\phi| > 3$ then by the induction hypothesis we have that if $|\psi| < |\phi|$ then $\psi \in G_0$. By Corollary 6 the collection $\{u, v, w\}$ is reducible, and we can suppose that $u = u_0 \cdot u_1$, $u_1 \in \{v, w, v \cdot w\}$. There is an automorphism α such that $\alpha(x_1, x_2, x_3) = (u_0, v, w)$; $\alpha \in G_0$ since $|\alpha| < |\phi|$. If $u = u_0 \cdot v$ then $\phi = \varphi\alpha$. Further, if $u = u_0 \cdot (v \cdot w)$ then

$$\phi = (13)\varphi(123)\varphi(132)\varphi(13)\alpha. \tag{2.2}$$

Finally, if $u = u_0 \cdot w$ then $\phi = (23)\varphi(23)\alpha$. In all three cases ϕ is contained in the group G_0; this implies the assertion of the theorem. $\square$

Theorem 10 implies

Corollary 11. *Let $S(\mathtt{X})$ be the Steiner loop with free generators $\mathtt{X} = \{a, b, c\}$. Let Q be the stabilizer $\mathrm{Stab}_{\mathrm{Aut}(S(\mathtt{X}))}(c)$ of element c in the automorphism group of $S(\mathtt{X})$. Then*

$$Q =< \varphi, \tau, \xi >$$

with

$$\varphi(a, b, c) = (ab, b, c), \quad \xi(a, b, c) = (ac, b, c), \quad \tau(a, b, c) = (b, a, c).$$

Proof. Denote by Q_0 the subgroup of Q generated by ξ, φ, τ and let $\lambda \in Q$ be the map $\lambda(a, b, c) = (v, w, c)$, with $|\lambda| = |v| + |w|$. Suppose that for every $\gamma \in Q$ with $|\gamma| < |\lambda|$, γ is contained in Q_0.

Since (v, w, c) is reducible, we have three possibilities: $v = v_0 w$, $v = v_0 c$ or $v = v_0(wc)$.

Consider the map $\lambda_0(a, b, c) = (v_0, w, c)$; it is contained in Q_0 by induction because $|\lambda_0| < |\lambda|$.

In the first case $\lambda = \varphi\lambda_0$. In the second case $\lambda = \xi\lambda_0$, and for the mapping $\phi(a, b, c) = (a(bc), b, c)$ we have by Eqn (2.2) (see the proof of Theorem 10). In the third case $\phi = \tau\xi\varphi\tau\varphi\xi\tau \in Q_0$.

In each case $\lambda \in Q_0$; this fact yields that $Q_0 = Q$. $\square$

Let us return to Problem 1. As was mentioned in the proof of Theorem 10, any transposition of the symmetric group $\mathcal{S}_n(\mathtt{X})$ on $\mathtt{X}$ can be written as a product of $\mathtt{X}$-elementary automorphisms

$$(ij) = e_i(x_j)e_j(x_i)e_i(x_j).$$

Using this description of translations and the equation

$$(i-1,i)(i,i+1)(i-1,i) = (i,i+1)(i-1,i)(i,i+1),$$

we get that

$$e_{i-1}(x_i)e_i(x_{i-1})e_{i-1}(x_i)e_i(x_{i+1})e_{i+1}(x_i)e_i(x_{i+1})e_{i-1}(x_i)e_i(x_{i-1})e_{i-1}(x_i) =$$

$$e_i(x_{i+1})e_{i+1}(x_i)e_i(x_{i+1})e_{i-1}(x_i)e_i(x_{i-1})e_{i-1}(x_i)e_i(x_{i+1})e_{i+1}(x_i)e_i(x_{i+1}).$$

This yields the relation

$$(e_i(x_j)e_j(x_i))^3 = 1.$$

In the proof of Theorem 10 we showed a further relation

$$e_1(x_2 \cdot x_3) = (13)\varphi(123)\varphi(132)\varphi(13) =$$

$$e_1(x_3)e_3(x_1)e_1(x_3)e_2(x_1)e_1(x_2)e_1(x_3)e_3(x_1)e_1(x_3)e_1(x_2)e_1(x_3)e_3(x_1)$$

$$\cdot e_1(x_3)e_1(x_2)e_2(x_1)e_1(x_3)e_3(x_1)e_1(x_3).$$

These facts suggest the following

Conjecture 12. *The group* $\mathrm{Aut}(S(x_1,x_2,x_3))$ *is generated by three involutions* $(12),(13)$ *and* $\varphi = e_1(x_2)$ *with relations*

$$(12)(13)(12) = (13)(12)(13), \qquad (\varphi(12))^3 = (\varphi(13))^4 = 1.$$

The analysis of computerised calculations shows that if the Conjecture 12 is false then some new relations might exist, among the above involutions, of the type

$$\varphi\sigma_1\varphi\sigma_2\cdots\varphi\sigma_n = 1.$$

Here $\sigma_i \in S_3 =< (12),(13) >$. Moreover, $\sigma_i \neq (12)$ or 1; if $\sigma_i = (13)$ then $\sigma_{i+1} \neq (13)$. Finally, $n > 50$ (for $n \leq 50$ new relations were not found).

In paper [20] it has been proved that the automorphism group of a free algebra of an arbitrary linear Nielsen–Schreier variety is generated by elementary automorphisms with some specific relations (2)–(4) ([20], pages 210–211). If Conjecture 12 holds, we will have a similar result for the group $\mathrm{Aut}(S(\mathtt{X}))$ of the free Steiner loop $S(\mathtt{X})$ in the case $|\mathtt{X}| = 3$.

Remark 13. *If Conjecture 12 is true, group* $\mathrm{Aut}(S(x_1, x_2, x_3))$ *is the Coxeter group*

$$< (12), (13), \varphi \,|(\varphi(12))^3 = (\varphi(13))^4 = ((12)(13))^3 = 1 > .$$

Conjecture 14. $Q = \{\varphi, \tau, \xi | \xi^2 = \varphi^2 = \tau^2 = (\tau\varphi)^3 = 1\}$.

Theorem 15. *If Conjecture 12 is true then Conjecture 14 is also true.*

Proof. Suppose that Conjecture 12 is true but Conjecture 14 is not. Then there exists a non-trivial word $w = w_1 \dots w_n$ formed by the letters $\{\tau, \xi, \varphi\}$ such that $a^w = a, b^w = b$. Here the "non-trivial" means that w does not contain the subwords $\varphi\tau\varphi$ and $\xi\tau\xi\tau$.

Applying induction on n, assume that for any non-trivial word v constructed from $\{\tau, \xi, \varphi\}$, of length less than n, the corresponding word in $\{\tau, \pi, \varphi\}$ is non-trivial, where $\pi = (23)$. Observe that $\xi = \pi\varphi\pi$. Hence, $w_0 = w_1 \dots w_{n-1}$ is a non-trivial word in $\{\tau, \pi, \varphi\}$. We focus on the case where w is not non-trivial word in $\{\tau, \pi, \varphi\}$. The choice $w_{n-1} = \tau$ implies that $w_n \neq \tau$ and $w_{n-2} \neq \tau$. Furthermore, if $w_n = \xi = \pi\varphi\pi$ then $w = w_1 \dots w_{n-2}\tau\pi\varphi\pi$ is a non-trivial word in $\{\tau, \pi, \varphi\}$. If $w_n = \varphi$ and $w_{n-2} = \xi$ then w is again a non-trivial word in $\{\tau, \pi, \varphi\}$. Finally, if $w_n = \varphi$ and $w_{n-2} = \varphi$ then w is not a non-trivial word in $\{\tau, \xi, \varphi\}$, since w contains the subword $w_{n-2}w_{n-1}w_n = \varphi\tau\varphi$. □

Next, we present as a consequence of the preliminary results, a connection between the groups of automorphisms of

(a) free Steiner quasigroups and the corresponding Steiner loops;

(b) the free exterior Steiner loops and free interior Steiner loops.

Theorem 16. *Let* $S(\mathtt{X})$ *be a free Steiner quasigroup with free generators* $\mathtt{X}$*. Let* $ES(\mathtt{X}) = S(\mathtt{X}) \cup e$ *and* $IS(\mathtt{X})$ *be its corresponding free exterior and interior Steiner loop, respectively.*

Then $\mathrm{Aut}(S(\mathtt{X})) = \mathrm{Aut}(ES(\mathtt{X}))$ *and* $\mathrm{Aut}(IS(\mathtt{X})) \simeq \mathrm{Stab}_{\mathrm{Aut}(ES(\mathtt{X}))}(a)$*, where* $a \in IS(\mathtt{X})$ *is the unit element of loop* $IS(\mathtt{X})$*.*

Proof. Let ϕ be an automorphism of $S(\mathtt{X})$, then we can define the corresponding automorphism $\bar{\phi}$ of $ES(\mathtt{X}) = \{e\} \cup S(\mathtt{X})$, such that $\bar{\phi}(e) = e$, $\bar{\phi}(x) = \phi(x)$, $x \in S(\mathtt{X})$. It is clear that the map $\phi \to \bar{\phi}$ is an isomorphism of the groups $\mathrm{Aut}(S(\mathtt{X}))$ and $\mathrm{Aut}(ES(\mathtt{X}))$.

Let $\phi \in Aut(IS(\mathtt{X}))$ be an automorphism of $IS(\mathtt{X})$, then $\phi(a) = a$, since a is the unit of $IS(\mathtt{X})$. Moreover, $\phi(x \circ y) = \phi((x.a).(a.y)) = (\phi(x).a).(a.\phi(y))$ for all $x, y \in IS(\mathtt{X})$. Since $x.y = x.a \circ y.a$, then $\phi(x.y) = \phi(x.a) \circ \phi(y.a) = (\phi(x.a).a).(\phi(y.a).a) = \phi(x).\phi(y)$, as $\phi(xa) = \phi(x \circ x) = \phi(x) \circ \phi(x) = \phi(x)a$. Hence ϕ is an automorphism of $S(\mathtt{X})$ and $\phi(a) = a$.

Inverse, let $\phi \in Aut(S(\mathtt{X}))$ and $\phi(a) = a$. Then

$\phi(x \circ y) = \phi((x.a).(a.y)) = (\phi(x).a).(\phi(y).a) = \phi(x) \circ \phi(y)$,

hence $\phi \in Aut(IS(\mathtt{X}))$.

□

2.3 Computations

Steiner Triple Systems are easily represented as combinatorial objects, thus we used some computational approach to make hypothesis about the group of automorphisms of a free Steiner loop with three free generators. The purpose of the program was to construct different series of involutions, such as

$$\varphi\sigma_1\varphi\sigma_2 \cdots \varphi\sigma_n$$

which may act on some set of words reducing it back to itself, it means we have a kind of equation:

$$\varphi\sigma_1\varphi\sigma_2 \cdots \varphi\sigma_n = 1.$$

Thus the program has to generate a set of non-associative words from primitives using the rules for the loop $S(\mathtt{X})$, then make an action on the set and look for any intersections between new set and old set. If there are no equal words, we may make a new iteration.

Algorithm

1. Construct a set of already generated words

$$Y \subset W = \{(w_1, w_2, w_3) : w_i \in S(\mathtt{X}), i = 1, 2, 3\}$$

For first iteration Y is a set of generators of loop $S(\mathtt{X})$.

2. Act on every word with a pair of involutions $\varphi\sigma_i$. We have to remember there exist some simple relations between involutions:

$$(12)(13)(12) = (13)(12)(13), \qquad (\varphi(12))^3 = (\varphi(13))^4 = 1.$$

   So order of actions is important: we can't use, for example, a pair $\varphi(12)$ three times one by one, the program has to remember the "history" of word's creation. This implements rather big volume of data we have to keep in memory at every iteration.

3. Verify if there appears any word we already have in Y :

   - If we have some repeated word, we should check its "history" for the series which may give us a new relation between elements of a group.
   - If there are no such words, the program is adding all new words to set Y.

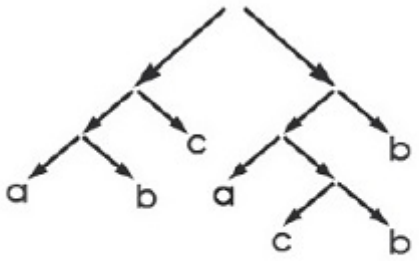
4. Go to the first step.

Data structures

Usually for keeping any symbolic data it is common to use string types of data structures. But, as we noticed, the value of data we are keeping at every step is big and it grows with every iteration exponentially.

Another way we want to keep words in a special tree-structures which has lighter weight, are easily readable and give us information about the word. Using these structures is an option if only we have non-associative objects like our generated words.

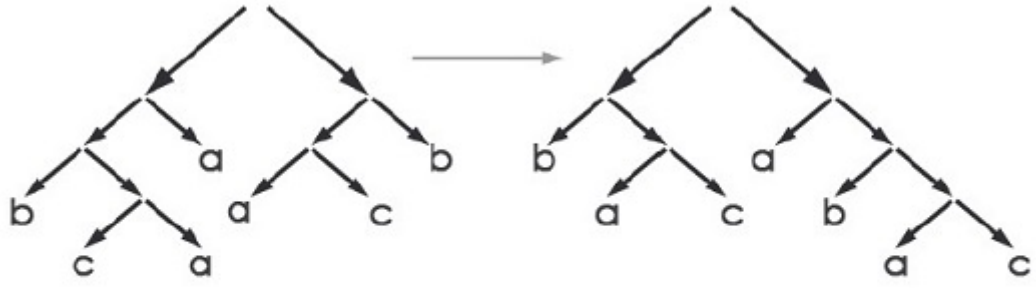
The picture below shows how the word w is represented in a tree-structure:



w = (ab*c)*((a*cb)*b)

Leaves of the tree are always generators of the loop and every pair of branches with common parent corresponds to a multiplication of two words (one is represented by the left branch and another by the right).

The order on the set of words produces order in the set of trees. Then one can compare two trees if they have a common view (i.e right branches are always "heavier" than left ones). "Weight" of the branch (or of the tree) means the number of leaves (symbols) it has. The picture below shows the process of re-structuring a tree, which is used as one of subprograms:



((b*ca)*a) * (b*ac) ⟶ (b*ac)*(a*(b*ac)) = a

There exists only one common form for every tree (every generated word), because our objects are non-associative. Also our words are irreducible, thus generated trees shouldn't have any sub-branch equal to a branch. If it's so, we would have a new relation in a group of automorphisms.

Program result analysis.

At first 50 iterations we have found no relations between automorphisms except for different compositions of already known. Therefore the length of

$$\varphi\sigma_1\varphi\sigma_2\cdots\varphi\sigma_n = 1.$$

have to be more than 50. Also we noticed that the weight of a tree doesn't increase linearly, it has peaks and falls. The new hypothesis is that there exists a series of automorphisms which increases a weight for any tree it's applied on.

Chapter 3

Nilpotent class two Steiner loops

In what follows we discuss Steiner loops of nilpotency class 2.

3.1 Centrally nilpotent Steiner loops of class two

Let $S(\mathtt{X}) > S_1(\mathtt{X}) > S_2(\mathtt{X}) > ...$ be a central series of the free Steiner loop $S(\mathtt{X})$ with free generators $\mathtt{X} = \{x_1, ..., x_n\}$. Then $V = S(\mathtt{X})/S_1(\mathtt{X})$ is an elementary abelian $2-$group and may be identified with $\mathbf{F}_2$-space of dimension $n := |\mathtt{X}|$, $\mathbf{F}_2 = \{0, 1\}$ is the field of two elements. Given $\sigma = \{i_1 > i_2 > ... > i_s\} \subseteq I_n$ define the corresponding element $\sigma = (((x_{i_2}x_{i_1})x_{i_3})...x_{i_s})$ of $S(\mathtt{X})$. As $S(\mathtt{X})/S_1(\mathtt{X})$ is an abelian 2-group, it is isomorphic to $\mathbf{F}_2^n$. Hence, to any element $v \in \mathbf{F}_2^n$ an element $\sigma = (i, j, ...)$ can be related, where $i, j, ...$ are the numbers of coordinates having value 1 of the vector v. Therefore, $\{\sigma | \sigma \subseteq I_n\}$ is a set of representatives of $S(\mathtt{X})/S_1(\mathtt{X})$. Determine a set of representatives of $Z = S_1(\mathtt{X})/S_2(\mathtt{X})$.

Set L_f to be a central extension of $\mathbf{F}_2$-spaces V and Z in the variety of Steiner loops. It means that $Z < Z(L_f)$ and $L_f/Z \simeq V$, where $Z(L_f)$ is the center of L_f. It is well known that L_f is a central extension of Z by V if and only if L_f is isomorphic to a loop defined on $V \times Z$ by the multiplication

$$(v_1, z_1) \circ (v_2, z_2) = (v_1 + v_2, f(v_1, v_2) + z_1 + z_2). \tag{3.1}$$

Here $f : V \times V \longrightarrow Z$ is a *Steiner loop cocycle*, that is, a map satisfying

$$f(0_V, v_1) = f(v_1, v_1) = 0_Z,\ f(v_1, v_2) = f(v_2, v_1),\ f(v_1 + v_2, v_2) = f(v_1, v_2) \tag{3.2}$$

for all $v_1, v_2 \in V$. Denote by $\mathcal{Z}^2(V, Z)$ the set of all Steiner loop cocycles. Next, let $\mathcal{C}^1(V, Z)$ be the set of all functions $g : V \longrightarrow Z$ and $\delta : \mathcal{C}^1(V, Z) \longrightarrow \mathcal{Z}^2(V, Z)$ such that

$$\delta(g)(v_1, v_2) = g(v_1 + v_2) + g(v_1) + g(v_2) \qquad \text{and} \qquad g(0_V) = 0_Z.$$

for all $v_1, v_2 \in V$. Let

$$\mathcal{B}^2(V, Z) = \delta(\mathcal{C}^1(V, Z))$$

and

$$\mathcal{H}^2(V, Z) = \mathcal{Z}^2(V, Z)/\mathcal{B}^2(V, Z).$$

Central extensions L_1 and L_2 are called *equivalent* precisely if, there is an isomorphism $\phi : L_{f_1} \longrightarrow L_{f_2}$ such that $\phi(v, *) = (v, *)$ if $v \in V$ and $\phi(*, z) = (*, z + \lambda(*))$ where $z, \lambda(*) \in Z$.

Any two equivalent extensions L_1 and L_2 are clearly isomorphic, but the converse is not true in general (for an example see the proof of Theorem 21).

Lemma 17. *Central extensions L_{f_1} and L_{f_2} corresponding to cocycles f_1 and f_2 are equivalent if and only if $f_1 = f_2$ in $\mathcal{H}^2(V, Z)$.*

Proof. The map $\varphi = (\varphi_1, \varphi_2) : L_{f_1} \longrightarrow L_{f_2}$, with $\varphi_1(v, z) = v$ and $\varphi_2(v, z) = z + g(v)$, determines an isomorphism if and only if $f_1(v_1, v_2) = f_2(v_1, v_2) + g(v_1 + v_2) + g(v_1) + g(v_2)$, i.e., $f_1 = f_2$ in $\mathcal{H}^2(V, Z)$. This is because

$$\varphi((v_1, z_1) \circ (v_2, z_2)) = (v_1 + v_2, f_1(v_1, v_2) + z_1 + z_2 + g(v_1 + v_2)) =$$

$$(v_1 + v_2, f_2(v_1, v_2) + z_1 + z_2 + g(v_1) + g(v_2)) = \varphi(v_1, z_1) \circ \varphi(v_2, z_2).$$

□

Let $\{v_1, ..., v_n\}$ be a basis of $V_{\mathbf{F}_2}$; as before, we can identify V with P_n - the set of all subsets of I_n. The set P_n has an ordering: $\sigma > \tau$ if $|\sigma| > |\tau|$ or $|\sigma| = |\tau|$, $\sigma = \{i_1 < ... < i_k\}$, $\tau = \{j_1 < ... < j_k\}$ with $i_1 = j_1, ..., i_s = j_s, i_{s+1} > j_{s+1}$.

Consider a subset $\mathcal{Z}_0^2(V, Z) \subset \mathcal{Z}^2(V, Z)$, where $f \in \mathcal{Z}_0^2(V, Z)$ if and only if $f(\sigma, \{i\}) = 0$, $\{i\} \geq \max(\sigma)$, $\sigma \in P_n = V$. In what follows $\triangle$ stands for the set-theoretical difference.

Lemma 18. $\mathcal{Z}^2(V,Z) = \mathcal{Z}_0^2(V,Z) \oplus \mathcal{B}^2(V,Z)$.

Proof. First, consider the case when $f \in \mathcal{Z}_0^2(V,Z) \cap \mathcal{B}^2(V,Z)$.

Then $g(\sigma) = \sum_{i\in\sigma} g(\{i\})$. Hence,

$$f(\sigma,\tau) = g(\sigma\triangle\tau) + g(\sigma) + g(\tau) = \sum_{i\in\sigma\triangle\tau} g(\{i\}) + \sum_{i\in\sigma} g(\{i\}) + \sum_{i\in\tau} g(\{i\})$$

Then $g(\sigma) = \sum_{i\in\sigma} g(\{i\})$. Hence,

$$f(\sigma,\tau) = g(\sigma\triangle\tau) + g(\sigma) + g(\tau) = \sum_{i\in\sigma\triangle\tau} g(\{i\}) + \sum_{i\in\sigma} g(\{i\}) + \sum_{i\in\tau} g(\{i\})$$

$$= \sum_{i\in\sigma\setminus\tau} g(\{i\}) + \sum_{i\in\tau\setminus\sigma} g(\{i\}) + \sum_{i\in\sigma\cap\tau} g(\{i\})$$

$$+ \sum_{i\in\sigma\setminus\tau} g(\{i\}) + \sum_{i\in\tau\cap\sigma} g(\{i\}) + \sum_{i\in\tau\setminus\sigma} g(\{i\}) = 0.$$

Now, suppose $f \in \mathcal{Z}^2(V,Z)$. For $\sigma = (i_1,...,i_k)$ we define $\sigma^s = (i_1,...,i_{s-1})$, $s > 1$, and $g(\sigma) = \sum_{s=2}^{k} f(\sigma^s, \{i_s\})$, assuming that $|\sigma| > 1$ and $g(\{i\}) = 0$. Then $f + \delta(g) \in \mathcal{Z}_0^2(V,Z)$. Indeed, if $\{i\} = \{i_{k+1}\} > \{i_k\} = \max(\sigma)$ then

$$(f+\delta(g))(\sigma,\{i\}) = f(\sigma,\{i\}) + g(\sigma\cup\{i\}) + g(\sigma) + g(\{i\})$$

$$= f(\sigma,\{i\}) + \sum_{s=2}^{k+1} f(\sigma^s,\{i_s\}) + \sum_{s=2}^{k} f(\sigma^s,\{i_s\}) = 0,$$

as $\sigma^{k+1} = \sigma$ and $\{i_{k+1}\} = \{i\}$. This yields that $f+\delta(g) \in \mathcal{Z}_0^2(V,Z)$ completing the proof of the lemma. □

We call a pair (σ,τ) *regular* if and only if $\sigma\triangle\tau > \sigma > \tau$. Note, that if $\emptyset \neq \sigma \neq \tau \neq \emptyset$ then precisely one of the pairs $(\sigma,\sigma\triangle\tau)$, (σ,τ), $(\sigma\triangle\tau,\tau)$, $(\sigma\triangle\tau,\sigma)$, (τ,σ), $(\tau,\sigma\triangle\tau)$ is regular. A regular pair is called *strongly regular* if $|\sigma| \geq |\tau| > 1$ or $|\sigma| \geq |\tau| = 1$ but $\{i\} < \max(\sigma)$, where $\tau = \{i\}$ and $|\sigma| > 1$.

Lemma 19. *The cardinality of elements of the set of all strongly regular pairs is*

$$\frac{1}{3}(2^{2n-1}+1) - 3\cdot 2^{n-1} + n + 1.$$

Proof. Let P be the set of all ordered pairs (σ, τ), $\sigma > \tau \neq \emptyset$. Then $|P| = C_m^2, m = 2^n - 1$ and hence, the number of regular pairs is $\frac{1}{3}C_m^2 = \frac{1}{3}(2^n - 1)(2^{n-1} - 1)$.

If (σ, τ) is regular but not strongly regular then $\tau = \{i\}$, $i \geq max(\sigma)$ or $\sigma = \{j\}$, $j > i$. Hence, for given i we have $(2^{i-1} + n - 2i)$ regular but not strongly regular pairs. Then the number of strongly regular pairs equals

$$\frac{1}{3}(2^n - 1)(2^{n-1} - 1) - \sum_{i=2}^{n}(2^{i-1} + n - 2i)$$

$$= \frac{1}{3}(2^n - 1)(2^{n-1} - 1) - 2^n - n^2 + n(n+1) + 1$$

$$= \frac{1}{3}(2^{2n-1} + 1) - 3 \cdot 2^{n-1} + n + 1.$$

□

Theorem 20. *The union of sets*

$$\big\{(\{i\}, \sigma \setminus \{i\}, \tau) \;\big|\; (\sigma, \tau) \text{ or } (\tau, \sigma) \text{ strongly regular},$$

$$\sigma \cap \tau = \emptyset,\ \{i\} = \max(\sigma \cup \tau) \in \sigma\big\}$$

and

$$\big\{(\{j\}, \mu, \lambda) \;\big|\; (\mu, \lambda) \text{ strongly regular},\ \mu \cap \lambda \neq \emptyset,\ \{j\} = \max(\mu \cap \lambda)\big\}.$$

is a basis of the $\mathbf{F}_2$*-space* $S_1(\mathtt{X})/S_2(\mathtt{X})$*,*

Moreover,

$$\dim_{\mathbf{F}_2}(S_1(\mathtt{X})/S_2(\mathtt{X})) = \frac{1}{3}(2^{2n-1} + 1) - 3 \cdot 2^{n-1} + n + 1,$$

where $n := |\mathtt{X}|$.

Proof. Let $F(\mathtt{X})$ be a free 2-step nilpotent Steiner loop with free generators $\mathtt{X} = \{x_1, ..., x_n\}$. $F(\mathtt{X})$ can be realized as a central extension L_f on $V \times Z$ for some Steiner loop cocycle $f \in \mathcal{Z}_0^2(V, Z)$.

For any elements $(\sigma, s), (\mu, m), (\tau, t) \in L_f$ we have

$$\big((\sigma, s), (\mu, m), (\tau, t)\big) = \big[\big((\sigma, s) \circ (\mu, m)\big) \circ (\tau, t)\big] \circ \big[(\sigma, s) \circ \big((\mu, m) \circ (\tau, t)\big)\big]$$

$$= \big[(\sigma \triangle \mu, f(\sigma, \mu) + s + m) \circ (\tau, t)\big] \circ \big[(\sigma, s) \circ (\mu \triangle \tau, f(\mu, \tau) + m + t)\big]$$

$$= (\sigma \triangle \mu \triangle \tau, f(\sigma, \mu) + f(\sigma \triangle \mu, \tau) + s + m + t)$$

$$\circ(\sigma \triangle \mu \triangle \tau, f(\mu, \tau) + f(\sigma, \mu \triangle \tau) + s + m + t)$$

$$= (\sigma \triangle \mu \triangle \tau \triangle \sigma \triangle \mu \triangle \tau, f(\sigma, \mu) + f(\sigma \triangle \mu, \tau) + f(\mu, \tau) + f(\sigma, \mu \triangle \tau))$$

$$= (\emptyset, f(\sigma, \mu) + f(\sigma \triangle \mu, \tau) + f(\mu, \tau) + f(\sigma, \mu \triangle \tau)).$$

Taking $s = m = t = 0$ and identifying $(\sigma, 0), (\mu, 0)$ and $(\tau, 0)$ with σ, μ and τ, respectively, we obtain the following relation involving associators:

$$(\sigma, \mu, \tau) = f(\sigma, \mu) + f(\mu, \tau) + f(\sigma \triangle \mu, \tau) + f(\sigma, \mu \triangle \tau). \tag{3.3}$$

Set $Z_f = f(V, V)$. Then by (3.3) we get that $Ass(F(\mathtt{X})) \subseteq Z_f$.

Next, we show that $Z_f \subseteq Ass(F(\mathtt{X}))$. Let $\sigma, \tau \in V$ be such that $\sigma > \tau$. If the pair (σ, τ) is not regular, then $\sigma > \sigma \triangle \tau$ and $f(\sigma, \tau) = f(\sigma \triangle \tau, \sigma)$ by the properties of Steiner loop cocycles. Note that the pair $(\sigma \triangle \tau, \sigma)$ is already regular. Now, suppose that (σ, τ) is regular but not strongly regular. Then $\tau = \{i\}$ and $\{i\} \geq max(\sigma)$ or $\sigma = \{j\}$, $\tau = \{i\}$ and $j > i$. In this case $f(\sigma, \{i\}) = 0$ by the definition of $\mathcal{Z}^2_0(V, Z)$. This means that it is enough to show that $f(\sigma, \tau) \in Ass(F(\mathtt{X}))$ for any strongly regular pair (σ, τ).

Let (σ, τ) be a strongly regular pair, that is, $|\sigma| \geq |\tau| > 1$ or $|\sigma| \geq |\tau| = 1$ but $\{i\} < max(\sigma)$, $\tau = \{i\}$ and $|\sigma| > 1$. Furthermore, let $\{i\} = max(\sigma \cup \tau)$. In what follows we use induction in $r := |\sigma| + |\tau|$. Assume that $f(\sigma, \tau) \in Ass(F(\mathtt{X}))$ if (σ, τ) is strongly regular and $|\sigma| + |\tau| < r$. Consider the case where the pair (σ, τ) is strongly regular and $|\sigma| + |\tau| = r$.

If $\sigma \cap \tau = \emptyset$ and $\{i\} \in \sigma$, then by (3.3) we have:

$$(\{i\}, \sigma \setminus \{i\}, \tau) = f(\{i\}, \sigma \setminus \{i\}) + f(\sigma \setminus \{i\}, \tau)$$

$$+ f(\{i\} \triangle (\sigma \setminus \{i\}), \tau) + f(\{i\}, (\sigma \setminus \{i\}) \triangle \tau)$$

and

$$f(\sigma,\tau) = (\{i\}, \sigma \setminus \{i\}, \tau) + f(\{i\}, \sigma \setminus \{i\}) + f(\sigma \setminus \{i\}, \tau) \\ + f(\{i\}, (\sigma \setminus \{i\}) \triangle \tau) = (\{i\}, \sigma \setminus \{i\}, \tau) + f(\sigma \setminus \{i\}, \tau), \tag{3.4}$$

since $f(\{i\}, \sigma \setminus \{i\}) = 0$ and $f(\{i\}, (\sigma \setminus \{i\}) \triangle \tau) = 0$. By the induction assumption, $f(\sigma \setminus \{i\}, \tau) \in Ass(F(\mathtt{X}))$ as $|\sigma \setminus \{i\}| + |\tau| < |\sigma| + |\tau|$ and hence $f(\sigma, \tau) \in Ass(F(\mathtt{X}))$. Similarly, we can prove the same fact in the case where $\sigma \cap \tau = \emptyset$ and $\{i\} \in \tau$.

If $\sigma \cap \tau \neq \emptyset$ and $\{j\} = max(\sigma \cap \tau)$, then by (3.3) we obtain that

$$(\{j\}, \sigma, \tau) = f(\{j\}, \sigma) + f(\sigma, \tau) + f(\{j\} \triangle \sigma, \tau) + f(\{j\}, \sigma \triangle \tau)$$

and

$$f(\sigma,\tau) = (\{j\}, \sigma, \tau) + f(\{j\}, \sigma) + f(\sigma \setminus \{j\}, \tau) + f(\{j\}, \sigma \triangle \tau). \tag{3.5}$$

Each summand in the right-hand side is contained in $Ass(F(\mathtt{X}))$. Namely, as f is a Steiner loop cocycle, we have $f(\{j\}, \sigma) = f(\sigma, \{j\}) = f(\sigma \setminus \{j\}, \{j\})$. Then $|\sigma \setminus \{j\}| + |\{j\}| = |\sigma| < |\sigma| + |\tau|$ yields by the induction hypothesis that $f(\{j\}, \sigma) \in Ass(F(\mathtt{X}))$. Similarly, we have that $f(\sigma \setminus \{j\}, \tau) \in Ass(F(\mathtt{X}))$ by induction, since $\{j\} \in \sigma$ and $|\sigma \setminus \{j\}| + |\tau| < |\sigma| + |\tau|$. Also, $f(\{j\}, \sigma \triangle \tau) \in Ass(F(\mathtt{X}))$ by the induction, since $|\{j\}| + |\sigma \triangle \tau| = 1 + |\sigma| + |\tau| - 2|\sigma \cap \tau| < |\sigma| + |\tau|$ as $\sigma \cap \tau \neq \emptyset$. This implies that $f(\sigma, \tau) \in Ass(F(\mathtt{X}))$.

Summarizing the above discussions, we get that $Z_f \subseteq Ass(F(\mathtt{X}))$. Hence $Z_f = f(V, V) = Ass(F(\mathtt{X})) = S_1(\mathtt{X})/S_2(\mathtt{X})$.

Moreover, by (3.4) and (3.5) we obtain that

$$f(V,V) \subseteq Span_{\mathbf{F}_2}\Big\{(\{i\}, \sigma \setminus \{i\}, \tau), (\{j\}, \mu, \lambda) \\ \Big| (\sigma,\tau), (\mu,\lambda) \text{ strongly regular}, \sigma \cap \tau = \emptyset, \{i\} = max(\sigma \cup \tau) \\ \text{and } \mu \cap \lambda \neq \emptyset, \{j\} = max(\mu \cap \lambda)\Big\} =: W.$$

Finally, we have that $f(V,V) \subseteq W \subseteq Ass(F(\mathtt{X})) = f(V,V)$ which implies $Ass(F(\mathtt{X})) = W$ and

$$dim(S_1(\mathtt{X})/S_2(\mathtt{X})) = dim(f(V,V)) = dim(Ass(F(\mathtt{X}))) = dim(W)$$

$$= \big|\{\text{strongly regular pairs}\}\big| = \tfrac{1}{3}(2^{2n-1}+1) - 3\cdot 2^{n-1} + n + 1$$

where the last equality holds by Lemma 19. □

3.2 Classification of nilpotent Steiner loops of class 2 with three generators

Note that there are exactly 80 non-isomorphic Steiner triple systems of order 15. Moreover, there is only one nilpotent non-associative Steiner loop S_{16} of order 16 (cf. [6]), and it corresponds to the system N.2 in [5] p. 19. Furthermore, S_{16} has the GAP id $\mathtt{SteinerLoop}(16,2)$; the label 2 indicates the system order as in the list established in monograph [1]. The Steiner loop S_{16} is 3-generated and has the nilpotency class 2. In what follows we describe all 3-generated Steiner loops of nilpotency class 2.

Theorem 21. *There exist three non-isomorphic non-associative* 3*-generated Steiner loops of nilpotency class* 2 *and their orders are* 16, 32 *and* 64*, respectively.*

Proof. Let $S(\mathtt{X} = \{x_1, x_2, x_3\})$ be the 3-generated free Steiner loop of nilpotency class 2 and $Z =< (z_1, z_2, z_3) >$ be the center of $S(\mathtt{X})$. By Theorem 20, we can choose $z_1 = (x_1, x_2, x_3)$, $z_2 = (x_2, x_1, x_3)$, $z_3 = (x_3, x_2, x_1x_3)$.

Let $G = AutS(\mathtt{X})$ be the group of automorphisms of the loop $S(\mathtt{X})$. Since $S(\mathtt{X})$ is free and Z is a $G-$invariant subloop of $S(\mathtt{X})$, we have an epimorphism $\phi : G \to GL_3(\mathbf{F}_2)$ with $ker(\phi) = \{\rho \in G | x^\rho = xz, z \in Z\}$.

The group G acts on the $\mathbf{F}_2-$space Z, and this action depends only on the images of the elements of G in $GL_3(\mathbf{F}_2)$. As the group $GL_3(\mathbf{F}_2)$ is simple and has no non-trivial $2-$dimensional $\mathbf{F}_2-$representations, the $G-$module Z is irreducible.

If P is a 3-generated Steiner loop of nilpotency class 2, then there is a canonical epimorphism $\pi : S(\mathtt{X}) \to P$ and $ker(\pi) \subseteq Z$. Note that for any other 3-generated Steiner loop Q and canonical epimorphism $\psi : S(\mathtt{X}) \to Q$ the loops P and Q are isomorphic if and only if there exists $\varrho \in GL_3(\mathbf{F}_2)$ such that $ker(\pi)^{\varrho} = ker(\psi)$. Indeed, if $ker(\pi)^{\varrho} = ker(\psi)$ then ϱ induces an isomorphism $\bar{\varrho} : P = S(\mathtt{X})/ker(\pi) \longrightarrow S(\mathtt{X})/ker(\psi) = Q$. Conversely, let $\bar{\varrho} : P = S(\mathtt{X})/ker(\pi) \longrightarrow S(\mathtt{X})/ker(\psi) = Q$ be an isomorphism between P and Q. Then $\bar{\varrho}$ induces a homomorphism $\upsilon : S(\mathtt{X}) \longrightarrow S(\mathtt{X})/ker(\psi)$ with $\upsilon = \bar{\varrho} \circ \pi$. For every $x \in \mathtt{X}$ one can choose $\sigma(x) \in \mathtt{X}$ such that $\upsilon(x) = \sigma(x)ker(\psi) \in S(\mathtt{X})/ker(\psi)$. Since the loop $S(\mathtt{X})$ is free, there is a unique homomorphism $\bar{\upsilon} : S(\mathtt{X}) \longrightarrow S(\mathtt{X})$ satisfying $\bar{\upsilon}(x) = \upsilon(x)$ for all $x \in \mathtt{X}$. It is easy to see that $\bar{\upsilon} \in AutS(\mathtt{X})$ and $\bar{\upsilon}(ker(\pi)) = ker(\psi)$.

The group $GL_3(\mathbf{F}_2)$ acts transitively on $Z \setminus \{1\}$ and on the set of the two dimensional $\mathbf{F}_2-$subspaces of Z. As Z is a three dimensional irreducible $GL_3(\mathbf{F}_2)-$module, there exists a unique 3-generated Steiner loop of nilpotency class 2 for each of the orders 16, 32 and 64. $\square$

Chapter 4

New constructions of finite geometries with four point on a line

4.1 Generalized Steiner loops.

Lets remind that $3-$geometries are actually the same objects as Steiner Triple Systems, so $3-$geometries are connected with Steiner loops and Steiner quasigroups. In this section we will show that in the same way the $4-$geometries are connected with $Generalized\ Steiner$ loops and quasigroups.

Definition 22. *A loop P is $Generalized\ Steiner$ or for short $Q-$loop iff*

(i) $x.yx = xy.x = y$,

(ii) $xy.y = yx$, *if* $x \neq e$,

We note that the set of all $Q-$loops is not a variety, but only quasivariety, since (ii) is not identity, but quasi-identity.

Definition 23. *A quasigroup P is $Generalized\ Steiner$ quasigroup or for short $Qq-$quasigroup [21] iff*

(i) $x.yx = xy.x = y$,

(ii) $xy.y = yx$,

(iii) $x.x = x$.

There exists relation between $Q-$loops and $Qq-$quasigroups as between Steiner loops and quasigroups.

Proposition 24. *If P is a $Q-$loop, then*

a) $S = P \setminus \{e\}$ *is a Steiner system of the type* $(2, 4)$*, (it means that every line contains four points) where a line that passed by* x, y *is* $l(x, y) = \{x, y, xy, yx\}$.

b) S *is a* $Qq-$*quasigroup with multiplication:*

$x \circ x = x$, $x \circ y = x.y$, *if* $x \neq y$.

Proof. a) It is enough to prove that

$l(x, y) = l(x, xy) = l(x, yx) = l(xy, yx)$.

By (i) we get

(iii) $y/x = xy$, $x\backslash y = yx$.

Then by (ii) and (iii):

$(xy)\backslash(yx) = y = yx.xy$, or

(iv) $yx.xy = y$.

We get $(xy)/(yx) = yx.xy = y$, then

(v) $y.yx = xy$.

We have

1. $l(x, xy) = \{x, xy, x.xy, xy.x\} = \{x, xy, yx, y\} = l(x, y)$.

2. $l(x, yx) = \{x, yx, x.yx, yx.x\} = \{x, yx, y, xy\} = l(x, y)$.

3. $l(xy, yx) = \{xy, yx, xy.yx, yx.xy\} = \{xy, yx, x, y\} = l(x, y)$.

b) By definition 22 we have the identities (i) and (iii) in the definition 23. Moreover, the identity (ii) in the quasigroup S is the same as quiasi-identity (ii) in P, since $e \notin S$ by definition.

The proposition is proved. □

4.2 Central extension of Qq-quasigroups

The simplist example of $Qq-$quasigroup is a $\mathbf{F}_4-$vector space V, where $\mathbf{F}_4 = \{0, 1, \tau, \tau^2 = 1 + \tau\}$ is the field of 4 elements.

In this case

$$v.w = w + \tau(v + w) = \tau v + \tau^2 w \tag{4.1}$$

Lemma 25. *The set* V *with multiplication defined above is a* $Qq-$*quasigroup.*

Proof. By definition:
1) $x.x = x + \tau(x + x) = x$,
since $x + x = 2x = 0$ in $\mathbf{F}_4$.
2) $x.(y.x) = x + \tau(x + y + \tau(x + y)) = x + \tau x + \tau y + \tau^2 x + \tau^2 y = y$,
since $\tau + \tau^2 = 1$.
3) $(x.y).y = x + \tau(x + y) + \tau(x + \tau(x + y) + y) =$
$\tau^2 y + \tau x = y + \tau(x + y) = y.x$.
Hence $(V, .)$ is a $Qq-$quasigroup.
Lemma 25 is proved. □

Definition 26. *Let Q be a $Qq-$quasigroup. It is called $group-like$ if $Q = (V, .)$, where V is a $\mathbf{F}_4-$space with multiplication (4.1)*

If $Q = (V, .)$ is group-like $Qq-$quasigroup then in the corresponding $4-$geometry the line $l(x, y)$, $x, y \in V$, is the line of the affine geometry on $V = \mathbf{F}_4^n : l(x, y) = \{x, y, \tau x + \tau^2 y, \tau y + \tau^2 x\}$.

Let V, W be group-like $Qq-$quasigroups and $\psi : V \times V \to W$ a map (not necessary linear!) $U = V \oplus W$ is a direct sum of the corresponding $\mathbf{F}_4-$spaces. We can define on U a multiplication

$$(v_1, w_1).(v_2, w_2) = (v_1.v_2, w_1.w_2 + \psi(v_1, v_2)). \tag{4.2}$$

Definition 27. *A map $\psi : V \times V \to W$ is a cocycle if the set $U = V \oplus W$ with multiplication (4.2) is $Qq-$quasigroup.*

Remark. If ψ is a cocycle then $\psi(v, v) = 0$. Indeed, we have
$(v, w).(v, w) = (v, w) = (v.v, w.w + \psi(v, v))$,
hence $\psi(v, v) = 0$.

As a corollary of this note we get that in $Qq-$quasigroup U constructed above for any $v \in V$ we have a normal subquasigroup $W_v = \{(v, w) | w \in W\} \simeq W$, moreover, $U/W_v \simeq V$. In some sense the subloops $W_v, v \in V$, are $central$ and U is central extension.

The main object of this chapter (see Theorem 28 below) is construction of central extension of two group-like $Qq-$quasigroups.

If $w_0, ..., w_{N-1}$ is a basis of the $\mathbf{F}_4-$vector space W then any element $w \in W$ has the unique form

$$w = \sum_{i=0}^{N-1} \alpha_i w_i,\ \alpha_i \in \mathbf{F}_4.$$

We can write any element of $\mathbf{F}_4$ in the form τ^s, $s = 0, 1, 2, 3$, where, by definition $\tau^0 = 0$. Hence every $w \in W$ has the unique form

$w = \sum_{i=0}^{N-1} \tau^{n_i} w_i$, $n_i \in \{0, 1, 2, 3\}$.

Then we have the bijection

$\phi : W \to W_N = \{(n_{N-1}n_{N-2}...n_1n_0) | n_i \in \{0, 1, 2, 3\}\}$, $\phi(w) = n_{N-1}...n_1n_0$. Below we will use this identification W and W_N.

Let $B = B_N$ be a set of lines in W which does not contain 0. Note that a line l contains 0 iff $l = \{0, v, \tau v, \tau^2 v\}$, $v \in W \setminus \{0\}$. For any $l \in B$ consider a $1-$dimensional $\mathbf{F}_4-$space U_l with a basis a_l. We identify U_l with $\mathbf{F}_4 = \mathbf{F}_4 a_l$.

Let $T = \{(i, j) | i \neq j \in \{0, 1, 2, 3\}\}-$ the set of all ordered pairs from $\{0, 1, 2, 3\}$. We fix a symmetric map $\psi_l = \psi : T \to U_l$, $\psi(i, j) = \psi(j, i)$, and a partial map $\lambda : W \times W \to T$,

$\psi(1, 0) = 1$, $\psi(2, 0) = \tau^2$, $\psi(3, 0) = \tau$,

$\psi(2, 1) = \tau$, $\psi(3, 1) = \tau^2$, $\psi(3, 2) = 1$.

The map $\lambda : W \times W \to T$, is defined only if $v \neq w, \tau w, \tau^2 w \in W$.

By definition

$\lambda(v, w) = (i, j)$, if $\phi(v) = n_{N-1}...n_1n_0$, $\phi(w) = m_{N-1}...m_1m_0$, $n_{N-1} = m_{N-1}, ..., n_t = m_t$,

$n_{t-1} = i \neq j = m_{t-1}$, $t \leq N - 1$.

Finally, we define a map $\pi : W_N \times W_N \to U_N = \sum_{l \in B_N} \oplus U_l$, such that

$\pi(n, m) = 0$, iff $n, m \in \{0, k, k^\tau, k^{\tau^2}\}$ for some k.

$\pi(n, m) = \psi_l(\lambda(n, m))$, if $n, m \in l = \{n, m, n \cdot m, m \cdot n\} \in B_N$.

We can consider U_N as a group like $Qq-$quasigroup.

We define a central extension of W_N with U_N :

$S_N = W_N \oplus U_N$,

$$(v, x).(w, y) = (v \cdot w, x \cdot y + \pi(v, w)). \tag{4.3}$$

Theorem 28. *The set S_N with multiplication above is a non-commutative Steiner quasigroup.*

Proof. We need to prove that the quasigroup S_N satisfies the identities (i)-(iii) from the definition of $Qq-$quasigroups.For this we have to prove

Lemma 29. *The map π is cocycle iff*

(1) $\tau^2\pi(v,w) = \pi(w,vw)$,

(2) $\tau\pi(v,w) = \pi(vw,v)$,

(3) $\pi(v,w) + \pi(v,wv) + \pi(w,wv) = 0$.

Proof. Let us suppose that π is a cocycle and, hence, S_N is a $Qq-$quasigroup. We will use the following connection between the two operations on group-like $Qq-$quasigroup V :

$$v.(w+u) = v.w + \tau^2 u, \tag{4.4}$$

$$(v+w).u = v.u + \tau w, \tag{4.5}$$

For example: $v.(w+u) = \tau v + \tau^2(w+u) = \tau v + \tau^2 w + \tau^2 u = v.w + \tau^2 u$.

Let us prove that relations (1) and (2) are equivalent to the identities (i). Using (4.5) we get:

$((v,x).(w,y)).(v,x) = (v.w, x.y + \pi(v,w)).(v,x) =$

$((v.w).v, (x.y+\pi(v,w)).x+\pi(v.w,v)) = (w, y.x+\tau\pi(v,w)+\pi(v.w,v)) =$ (w,y).

Then the relation (2) is equivalent to the identity $(x.y).x = y$.

Analogously we can prove that the relation (1) is equivalent to the identity $x.(y.x) = y$, and (3) to $(x.y).y = y.x$.

The Lemma is proved. □

Now we have to deduce the relations (1)-(3) from Lemma 29.

Suppose that $\lambda(v,w) = (1,0)$. Let

$$v = \sum_{i=0}^{N-1} \tau^{n_i} w_i, n_i \in \{0,1,2,3\},$$

$$w = \sum_{i=0}^{N-1} \tau^{m_i} w_i, m_i \in \{0,1,2,3\}.$$

If $m_{N-1} = n_{N-1}, ..., m_{i+1} = n_{i+1}, n_i = 1, m_i = 0$.

Hence

$\tau^p v = \sum_{i=0}^{N-1} \tau^{n_i+p} w_i$, $\tau^p w = \sum_{i=0}^{N-1} \tau^{m_i+p} w_i$, $p = 1, 2$.

Here the sum $n_i + p$ is calculated modulo 3, since $\tau^3 = 1$. Then $n_j + p \neq m_j + p$, $j < i$, and all values of $\lambda(x, y)$ for $x, y \in \{v, w, v.w, w.v\}$ are defined by the coefficient before w_i. Hence

$\lambda(w, v) = (0, 1)$, $\lambda(v.w, w) = (2, 0)$, $\lambda(v.w, v) = (2, 1)$, $\lambda(w.v, v.w) = (3, 2)$,

$\lambda(v.w, w.v) = (2, 3)$, $\lambda(w.v, v) = (3, 1)$, $\lambda(w.v, w) = (3, 0)$.

We are ready to prove that π is cocycle, using the Lemma 29. Let consider the cases:

1) **Case** $(1, 0)$.

(i) $\tau^2\pi(v, w) = \tau^2\psi(\lambda(v, w)) = \tau^2\psi(1, 0) = \tau^2$,

$\pi(w, v.w) = \psi(\lambda(w, v.w)) = \psi(0, 2) = \tau^2$,

hence $\tau^2\pi(v, w) = \pi(w, v.w)$.

(ii) $\tau\pi(v, w) = \tau\psi(\lambda(v, w)) = \tau\psi(1, 0) = \tau$,

$\pi(v.w, v) = \psi(\lambda(v.w, w)) = \psi(2, 1) = \tau$,

hence $\tau\pi(v, w) = \pi(v.w, v)$.

(iii) $\pi(v, w) + \pi(v, w.v) + \pi(w, w.v) =$

$\psi(\lambda(v, w)) + \psi(\lambda(v, w.v)) + \psi(\lambda(w, w.v) =$

$\psi(1, 0) + \psi(3, 1) + \psi(3, 0) = 1 + \tau^2 + \tau = 0$.

2) **Case** $(1, 2)$.

(i) $\tau^2\pi(v, v.w) = \tau^2\psi(\lambda(v, v.w)) = \tau^2\psi(1, 2) = 1$,

$\pi(v.w, v.(v.w)) = \psi(\lambda(v.w, w.v)) = \psi(2, 3) = 1$,

hence $\tau^2\pi(v, v.w) = \pi(v.w, w.v)$.

(ii) $\tau\pi(v, v.w) = \tau\psi(\lambda(v, v.w)) = \tau\psi(1, 0) = \tau$,

$\pi(v.w, v) = \psi(\lambda(v.w, w)) = \psi(2, 1) = \tau$,

hence $\tau\pi(v, v.w) = \pi(w.v, v)$.

(iii) $\pi(v, v.w) + \pi(v, (v.w).v) + \pi(v.w, (v.w).v) =$

$\pi(v, v.w) + \pi(v, w) + \pi(v.w, w) =$

$\psi(\lambda(v, v.w)) + \psi(\lambda(v, w)) + \psi(\lambda(v.w, w) =$

$\psi(1, 2) + \psi(0, 1) + \psi(2, 0) = \tau + 1 + \tau^2 = 0$.

3) **Case** $(0, 2)$.

(i) $\tau^2\pi(w, v.w) = \tau^2\psi(\lambda(w, v.w)) = \tau^2\psi(0, 2) = \tau^2\tau^2 = \tau$,

$\pi(v.w, w.(v.w)) = \psi(\lambda(v.w, v)) = \psi(2,1) = \tau,$
hence $\tau^2\pi(w, v.w) = \pi(v.w, w.(v.w))$.
(ii) $\tau\pi(w, v.w) = \tau\psi(\lambda(w, v.w)) = \tau\psi(2,0) = 1,$
$\pi(w.(v.w), w) = \psi(\lambda(v, w)) = \psi(1,0) = 1,$
hence $\tau\pi(w, v.w) = \pi(w.(v.w), w)$.
(iii) $\pi(v.w, w) + \pi(v.w, w.(v.w)) + \pi(w, w.(v.w)) =$
$\pi(v.w, w) + \pi(v.w, v) + \pi(w, v) =$
$\psi(\lambda(v.w, w)) + \psi(\lambda(v.w, v)) + \psi(\lambda(w, v) =$
$\psi(0,2) + \psi(2,1) + \psi(1,0) = \tau^2 + \tau + 1 = 0.$
4) **Case** $(3,2)$.
(i) $\tau^2\pi(w.v, v.w) = \tau^2\psi(\lambda(w.v, v.w)) = \tau^2\psi(3,2) = \tau^2,$
$\pi(w.v, (w.v).(v.w)) = \psi(\lambda(w.v, w)) = \psi(3,1) = \tau^2,$
hence $\tau^2\pi(w.v, v.w) = \pi(w.v, (w.v).(v.w))$.
(ii) $\tau\pi(w.v, v.w) = \tau\psi(\lambda(w.v, v.w)) = \tau\psi(2,3) = \tau,$
$\pi((v.w).(w.v), v.w) = \psi(\lambda(v, v.w)) = \psi(1,2) = \tau,$
hence $\tau\pi(w.v, v.w) = \pi((v.w).(w.v), v.w)$.
(iii) $\pi(v.w, w.v) + \pi(v.w, (w.v).(v.w)) + \pi(v.w, (w.v).(v.w)) =$
$\pi(v.w, w.v) + \pi(v.w, w) + \pi(w.v, w) =$
$\psi(\lambda(v.w, w.v)) + \psi(\lambda(v.w, w)) + \psi(\lambda(w.v, w) =$
$\psi(3,2) + \psi(2,0) + \psi(3,0) = 1 + \tau^2 + \tau = 0.$
5) **Case** $(3,1)$.
(i) $\tau^2\pi(w.v, v) = \tau^2\psi(\lambda(w.v, v)) = \tau^2\psi(3,1) = \tau,$
$\pi(v, (w.v).v) = \psi(\lambda(v, v.w)) = \psi(1,2) = \tau,$
hence $\tau^2\pi(w.v, v) = \pi(v, (w.v).v)$.
(ii) $\tau\pi(w.v, v) = \tau\psi(\lambda(w.v, v)) = \tau\psi(1,3) = 1,$
$\pi((w.v).v, w.v) = \psi(\lambda(v.w, w.v)) = \psi(3,2) = 1,$
hence $\tau\pi(w.v, v) = \pi((w.v).v, w.v)$.
(iii) $\pi(w.v, v) + \pi(w.v, v.(w.v)) + \pi(v, v.(w.v)) =$
$\pi(w.v, v) + \pi(w.v, w) + \pi(v, w) =$
$\psi(3,1) + \psi(3,0) + \psi(1,0) = \tau^2 + \tau + 1 = 0.$
6) **Case** $(3,0)$.
(i) $\tau^2\pi(w.v, w) = \tau^2\psi(\lambda(w.v, w)) = \tau^2\psi(3,0) = 1,$
$\pi(w, (w.v).w) = \psi(\lambda(w, v)) = \psi(1,0) = 1,$

hence $\tau^2\pi(w.v, w) = \pi(w, (w.v).w)$.
(ii) $\tau\pi(w.v, w) = \tau\psi(\lambda(w.v, w)) = \tau\psi(0, 3) = \tau^2$,
$\pi((w.v).w, w.v) = \psi(\lambda(v, w.v)) = \psi(3, 1) = \tau^2$,
hence $\tau\pi(w.v, w) = \pi((w.v).w, w.v)$.
(iii) $\pi(w.v, w) + \pi(w.v, w.(w.v)) + \pi(w, v.w) =$
$\pi(w.v, w) + \pi(w.v, v.w) + \pi(w, v.w) =$
$\psi(3, 0) + \psi(3, 2) + \psi(2, 0) = \tau + 1 + \tau^2 = 0$.
Theorem is proved. □

Conjecture 30. *Let ψ be a cocycle $\psi : V \times V \to Z$, where V, Z are $Qq-$quasigroups of group-like type.*

Then $\psi(v, w) = \psi(w, v)$.

Conjecture 31. *Let S be a $Qq-$quasigroup and $S \ncong S_1 \times S_2$ for any non-trivial $Qq-$quasigroups S_1 and S_2. Moreover, S is an central extension of two group-like $Qq-$quasigroups V, W.*

Then $\dim W \leq \frac{(4^n-1)(4^{n-1}-1)}{3}$, *where* $\dim V = n$.

Bibliography

[1] Ch. J. Colbourn, A. Rosa, Triple systems. *Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, (1999).*

[2] B. Ganter, U. Pfüller, A remark on commutative di-associative loops. *Algebra Universalis, 21, (1985), 310 – 311.*

[3] A. Grishkov, D. Rasskazova, M. Rasskazova, I. Stuhl, Free Steiner triple systems and their automorphism groups. *Journal of Algebra and its Applications, 14, (2015).*

[4] A. Grishkov, D. Rasskazova, M. Rasskazova, I. Stuhl, Nilpotent Steiner loops of class 2. *Communication in algebra, accepted*

[5] R. A. Mathon, K. T. Phelps, A. Rosa, Small Steiner triple systems and their properties. *Ars. Combinatoria, 15, (1983), 3 – 110.*

[6] G. P. Nagy, P. Vojtěchovský, LOOPS: Computing with quasigroups and loops in GAP. *available at http://www.math.du.edu/ petr/loops*

[7] H. O. Pflugfelder, Quasigroups and Loops: Introduction. *Heldermann Verlag, Berlin (1990).*

[8] K. Strambach, I. Stuhl, Translation groups of Steiner loops. *Discrete Mathematics, 309, (2009), 4225 – 4227.*

[9] K. Strambach, I. Stuhl, Oriented Steiner loops. *Beiträge zur Algebra und Geometrie, 54, (2013), 131–145.*

[10] I. Stuhl, Oriented Steiner quasigroups. *Journal of Algebra and its Applications, 13, (2014).*

[11] R. Baer, Nets and Groups, *Transactions of the American Mathematical Society, 46, (1939), 110-141.*

[12] O. Chein, Examples and methods of construction, in *Quasigroups and Loops: Theory and Applications*, ed. O. Chein, H.O. Pflugfelder, J.D.H. Smith, *Heldermann Verlag, Berlin, (1990), 27-95.*

[13] T. Evans, Varieties of loops and quasigroups, in *Quasigroups and Loops: Theory and Applications*, ed. O. Chein, H.O. Pflugfelder, J.D.H. Smith, *Heldermann Verlag, Berlin, (1990), 1-26.*

[14] A.G. Kurosh, The theory of groups, Vol. 2., *Chelsea publishing company, New York (1960).*

[15] S. Markovski, A. Sokolova, Free Steiner loops, *Glasnik Matematički, 36, (2001), 85-93.*

[16] E. Mendelsohn, On the Groups of Automorphisms of Steiner Triple and Quadruple Systems, *Journal of Combinatorial Theory, 25 Ser.A, (1978), 97-104.*

[17] P. T. Nagy, K. Strambach, Loops in Group Theory and Lie Theory, Expositions in Mathematics 35, *Walter de Gruyter, Berlin–New York (2002).*

[18] J. D. Smith, An introduction to Quasigroups and Their Representations, *Chapman Hall/CRC, Boca Raton, FL, (2006).*

[19] K. Strambach, I. Stuhl, Oriented Steiner loops, *Beiträge zur Algebra und Geometrie, 54, (2013), 131-145.*

[20] U. U. Umirbaev, Defining relations for automorphism groups of free algebras, *Journal of Algebra, 314, (2007), 209-225.*

[21] B.Ganter, H. Werner, Equational classes of Steiner Systems , *Algebra Universalis, 5, (1975), 125-140.*