Quasigroups and Related Systems **27** (2019), 161 – 174

On (semi)topological hoops

Mona Aaly Kologani, Rajab Ali Borzooei and Nader Kouhestani

Abstract. Hoops are naturally ordered commutative residuated integral monoids, introduced by Bosbach in [6, 7], that BL-algebras are particular cases of hoops. Now, in this paper, we introduce the concept of (semi)topological hoop and we get some related results. Then we derive here conditions that imply a hoop to be a semitopological or a topological hoop and we study some properties of them. Specially, we show that in a hoop A, if $(A, \to, \mathcal{T})$ is a semitopological hoop and $\{1\}$ is an open set or A is bounded and satisfies the double negation property, then $(A, \mathcal{T})$ is a topological hoop. Finally, we construct a discrete topology on quotient hoops, under suitable conditions.

1. Introduction

Algebra and topology, the two fundamental domains of mathematics, play complementary roles. Topology studies continuity and convergence and provides a general framework to study the concept of a limit. Algebra studies all kinds of operations and provides a basis for algorithms and calculations. In applications, in higher level domains of mathematics, such as functional analysis, dynamical systems, representation theory, and others, topology and algebra come in contact most naturally. Many of the most important objects of mathematics represent a blend of algebraic and of topological structures. Topological function spaces and linear topological spaces in general, topological groups and topological fields, transformation groups, topological lattices are objects of this kind. Very often an algebraic structure and a topology come naturally together; this is the case when they are both determined by the nature of the elements of the set considered. The rules that describe the relationship between a topology and algebraic operation are almost always transparent and natural the operation has to be continuous, jointly continuous, jointly or separately. In the 20th century many topologists and algebraists have contributed to the topological algebra. Some outstanding mathematicians were involved, among them Dieudonné, Pontryagin, Weyl. Hoops are naturally ordered commutative residuated integral monoids, introduced by Bosbach in [6, 7]. In the last years, the hoops theory have enriched with deep structure theorems [1, 2, 3, 4, 5, 6, 7, 12]. Many of these results have a strong impact with fuzzy logic. Particularly, from the structure theorem of finite basic hoops ([2], Corollary 2.10) one obtains an elegant short proof of the completeness theorem for

2010 Mathematics Subject Classification: 06F99, 03G25, 18B35 , 22A26.
Keywords: Hoop, (semi)topological hoop, connected space, locally connected space.

the propositional basic logic ([2], Theorem 3.8), introduced by Hájek in [9]. The algebraic structures corresponding to Hájek's propositional (fuzzy) basic logic, BL-algebras, are particular cases of hoops. Now, in this paper, we introduce the concept of (semi)topological hoops and we bring some useful examples of them.

2. Preliminaries

In this section, we gather some basic notions relevant to hoop which will need in the next sections.

A *hoop* is an algebraic structure $(A, \odot, \to, 1)$ of type $(2, 2, 0)$ such that, for all $x, y, z \in A$:
$(HP1)$ $(A, \odot, 1)$ is a commutative monoid.
$(HP2)$ $x \to x = 1$.
$(HP3)$ $(x \odot y) \to z = x \to (y \to z)$.
$(HP4)$ $x \odot (x \to y) = y \odot (y \to x)$.

On a hoop A we define $x \leqslant y$ if and only if $x \to y = 1$. Then " $\leqslant$ " is a partial order on A. A hoop A is *bounded* if, for all $x \in A$, there is an element $0 \in A$ such that $0 \leqslant x$. Let A be a bounded hoop. For all $x \in A$, we define a negation " $'$ " on A by, $x' = x \to 0$. If $(x')' = x$, for all $x \in A$, then the bounded hoop A is said to have the *double negation property*, or (DNP) for short. Finally, we let $x^0 = 1$, $x^n = x^{n-1} \odot x$, for any $n \in \mathbb{N}$ (cf. [2]).

Example 2.1. (cf. [8]) (i) Let $\mathbf{G} = (G, +, -, 0, \vee, \wedge)$ be an ℓ-group and $0 \leqslant u \in G$. Suppose that operations $\odot$ and $\to$ on $G[u] = [0, u]$ are defined as follows:

$$x \odot y = (x - u + y) \vee 0 \quad , \quad x \to y = (y - x + u) \wedge 0.$$

Then by routine calculations we can see that $\mathbf{G}[\mathbf{u}] = (G[u], \odot, \to, u)$ is a hoop.
(ii) Let $A = \{0, a, b, c, d, 1\}$ and operations $\odot$ and $\to$ on A are defined as follows:

$\to$	0	a	b	c	d	1
0	1	1	1	1	1	1
a	c	1	b	c	b	1
b	d	a	1	b	a	1
c	a	a	1	1	a	1
d	b	1	1	b	1	1
1	0	a	b	c	d	1

$\odot$	0	a	b	c	d	1
0	0	0	0	0	0	0
a	0	a	d	0	d	a
b	0	d	c	c	0	b
c	0	0	c	c	0	c
d	0	d	0	0	0	d
1	0	a	b	c	d	1

Then with these operations A is a bounded hoop with (DNP).

The following proposition provides some properties of hoops.

Proposition 2.2. (cf. [6, 7]) *Let A be a hoop. Then, for all $x, y, z \in A$, the following conditions hold:*

(i) $(A, \leqslant)$ *is a meet-semilattice with* $x \wedge y = x \odot (x \to y)$.
(ii) $x \odot y \leqslant z$ *if and only if* $x \leqslant y \to z$.
(iii) $x \odot y \leqslant x, y$.
(iv) $x \leqslant y \to x$.
(v) $x \to 1 = 1$.
(vi) $1 \to x = x$.
(vii) $x \leqslant y \to (x \odot y)$.
$(viii)$ $x \odot (x \to y) \leqslant y$.
(ix) $x \leqslant (x \to y) \to y$.
(x) $x \leqslant y$ *implies* $x \odot z \leqslant y \odot z$.
(xi) $x \leqslant y$ *implies* $z \to x \leqslant z \to y$.
(xii) $x \leqslant y$ *implies* $y \to z \leqslant x \to z$.
$(xiii)$ $(x \to y) \leqslant (y \to z) \to (x \to z)$.

Proposition 2.3. (cf. [8]) *Let A be a bounded hoop. Then, for all $x, y \in A$, the following conditions hold:*

(i) $1' = 0$ *and* $0' = 1$.
(ii) $x \leqslant x''$.
(iii) $x \odot x' = 0$.
(iv) $x''' = x'$.
(v) $x' \leqslant x \to y$.
(vi) *If* $x = x''$, *then* $x \to y = y' \to x'$.
(vii) $x = x''$ *if and only if* $(x \to y) \to y = (y \to x) \to x$.

Proposition 2.4. (cf. [8]) *Let A be a hoop and for any $x, y \in A$, we define,*

$$x \sqcup y = ((x \to y) \to y) \wedge ((y \to x) \to x)$$

Then, for all $x, y, z \in A$, the following conditions are equivalent:

(i) $\sqcup$ *is associative operation on* A,
(ii) $x \leqslant y$ *implies* $x \sqcup z \leqslant y \sqcup z$,
(iii) $x \sqcup (y \wedge z) \leqslant (x \sqcup y) \wedge (x \sqcup z)$,
(iv) $\sqcup$ *is the join operation on* A.

A hoop A is called a $\sqcup$-*hoop*, if $\sqcup$ is a join operation on A.

Remark 2.5. (cf. [8]) $\sqcup$-hoop $(A, \sqcup, \wedge)$ is a distributive lattice.

Let A be a hoop. A non-empty subset F of A is called a *filter* of A if,
$(F1)$ $x, y \in F$ implies $x \odot y \in F$.
$(F2)$ $x \leqslant y$ and $x \in F$ imply $y \in F$, for any $x, y \in A$.

We use $\mathcal{F}(A)$ to denote the set of all filters of A. Clearly, $1 \in F$, for all $F \in \mathcal{F}(A)$. $F \in \mathcal{F}(A)$ is called a *proper filter* if $F \neq A$. It can be easily seen that, if A is a bounded hoop, then a filter is proper if and only if it does not contain 0 (cf. [8]).

Proposition 2.6. (cf. [8]) *Let A be a hoop and F be a non-empty subset of A. Then $F \in \mathcal{F}(A)$ if and only if $1 \in F$ and if, for any $x, y \in A$, $x \in F$ and $x \to y \in F$, then $y \in F$.*

Let A be a hoop and $F \in \mathcal{F}(A)$. We define a binary relation $\sim_F$ on A by $x \sim_F y$ if and only if $x \to y,\ y \to x \in F$, for any $x, y \in A$. Then $\sim_F$ is a congruence relation on A. Let $A/F = \{\overline{x} \mid x \in A\}$, where $\overline{x} = \{y \in A \mid x \sim_F y\}$. Then the binary relation $\leqslant$ on A/F defined by:

$$\overline{x} \leqslant \overline{y} \text{ if and only if } x \to y \in F,$$

is a partial order on A/F (cf. [9]). Thus $(A/F, \otimes, \rightsquigarrow, 1_{A/F})$ is a hoop, where for any $x, y \in A$:

$$1_{A/F} = \overline{1}, \quad \overline{x} \otimes \overline{y} = \overline{x \odot y}, \quad \overline{x} \rightsquigarrow \overline{y} = \overline{x \to y}.$$

In the follows, we recall some definitions of topological spaces.
A set X with a family $\mathcal{T}$ of its subsets is called a *topological space*, denoted by $(X, \mathcal{T})$, if $X, \emptyset \in \mathcal{T}$ and $\mathcal{T}$ is closed under a finite intersection and arbitrary union. The members of $\mathcal{T}$ are called *open sets* of X and the complement of $U \in \mathcal{T}$, that is U^c, is said to be a *closed set*. If B is a subset of X, the smallest closed set containing B is called the *closure* of B and denoted by $\overline{B}$. A subfamily $\{U_\alpha\}$ of $\mathcal{T}$ is said to be a *base* of U if for any $x \in U \in \mathcal{T}$, there exists an α such that $x \in U_\alpha \subseteq U$, or equivalently, each $U \in \mathcal{T}$ is the union of members of $\{U_\alpha\}$. A subset P of a topological space $(X, \mathcal{T})$ is said to be a *neighborhood* of $x \in X$ if there exists an open set U such that $x \in U \subseteq P$. A topological space X is said to be *disconnected* if it is the union of two disjoint non-empty open sets. Otherwise, X is said to be *connected* (cf. [10, 11]).

Let $(A, *)$ be an algebra of type 2 and $\mathcal{T}$ be a topology on A. Then $\mathcal{A} = (A, *, \mathcal{T})$ is called:
• *left (right) topological algebra* if for each $a \in A$, the map $l_a \colon A \to A (r_a \colon A \to A)$ is defined by $x \to a * x (x \to x * a)$ is continuous, or equivalently, for any $x \in A$, and any open neighborhood U of $a * x (x * a)$, there exists an open neighborhood V of x such that $a * V \subseteq U (V * a \subseteq U)$. In this case we also call that the operation $*$ is continuous in the second (first) variable.
• *semitopological algebra* if $\mathcal{A}$ is a right and left topological algebra. In this case we also call that the operation $*$ is continuous in each variable separately.
• *topological algebra* if the operation $*$ is continuous, or equivalently, if for any $x, y \in A$ and any open neighborhood W of $x * y$, there exist two open neighborhoods U and V of x and y, respectively, such that $U * V \subseteq W$ (cf. [11]).

Proposition 2.7. (cf. [11]) *Let $(A, *)$ be a commutative algebra of type 2 and $\mathcal{T}$ be a topology on A. Then, right and left topological algebras are equivalent. Moreover, $(A, *, \mathcal{T})$ is a semitopological algebra if and only if it is right or left topological algebra.*

Let A be a non-empty set, $\{*_i\}_{i \in I}$ be a family of operations of type 2 on A and $\mathcal{T}$ be a topology on A. Then:

(*i*) $(A, \{*_i\}_{i\in I}, \mathcal{T})$ is a *right(left) topological algebra* if for any $i \in I$, $(A, *_i, \mathcal{T})$ is a right (left) topological algebra,

(*ii*) $(A, \{*_i\}_{i\in I}, \mathcal{T})$ is a *(semi)topological algebra* if for all $i \in I$, $(A, *_i, \mathcal{T})$ is a (semi)topological algebra (cf. [11]).

Note: From now one, A is a hoop and $\mathcal{T}$ is a topology on A.

3. (Semi)topological hoop

In this section we define the notions of (semi)topological hoop and state and prove some related results.

Definition 3.1. Let $(A, \{*_i\}, \mathcal{T})$, where $\{*_i\} \subseteq \{\odot, \to\}$, be a (semi)topological algebra. Then $(A, \{*_i\}, \mathcal{T})$ is called a *(semi)topological hoop*. Moreover, we say $(A, \mathcal{T})$ is a *(semi)topological* hoop if $(A, \odot, \to, \mathcal{T})$ is a (semi)topological hoop.

Note: Let $U, V \subseteq A$. Then we define $U \odot V$, $U \to V$ and $U \times V$ as follows:

$$U \odot V = \{x \odot y \mid x \in U, y \in V\}, \qquad U \to V = \{x \to y \mid x \in U, y \in V\}.$$

Example 3.2. (*i*) Every hoop with the discrete topology is a topological hoop.

(*ii*) Let $A = \{0, a, b, 1\}$ be a set. Define the operations $\odot$ and $\to$ on A as follows:

$\odot$	0	a	b	1
0	0	0	0	0
a	0	a	a	a
b	0	a	b	b
1	0	a	b	1

$\to$	0	a	b	1
0	1	1	1	1
a	0	1	1	1
b	0	a	1	1
1	0	a	b	1

Then A with these operations and the topology $\mathcal{T} = \{\emptyset, \{0\}, \{1, a, b\}, A\}$ is a bounded topological hoop.

Note: We know that, any topological hoop is always a semitopological hoop. In the following example we show that every semitopological hoop is not a topological hoop, in general.

Example 3.3. Let $A = \{0, a, b, 1\}$ be a set. Define the operations $\odot$ and $\to$ on A as follows:

$\odot$	0	a	b	1
0	0	0	0	0
a	0	0	a	a
b	0	a	b	b
1	0	a	b	1

$\to$	0	a	b	1
0	1	1	1	1
a	a	1	1	1
b	0	a	1	1
1	0	a	b	1

Then A with these operations and the topology $\mathcal{T} = \{\emptyset, \{1, b\}, \{1, a, b\}, A\}$ is a semitopological hoop, but it is not a topological hoop. Because $0 \to 0 = 1 \in \{1, b\}$ and $A \to A = A$ and it is clear that $A \nsubseteq \{1, b\}$.

Example 3.4. Let $\odot$ and $\to$ on the real unit interval $A = [0,1]$ be defined as follows:

$$x \odot y = \min\{x, y\} \quad \text{and} \quad x \to y = \begin{cases} 1 & x \leqslant y \\ y & otherwise \end{cases}$$

Then A with these operations is a bounded hoop.

Now, let $\mathcal{T}$ be a topology on A with the base $B = \{(a, b] \cap A \mid a, b \in \mathbb{R}\}$. Then $V = (a, 0] \cap A = \{0\}$ for $a < 0$, and so $\{0\}$ is an open neighborhood of 0.

We prove $(A, \odot, \mathcal{T})$ is a topological hoop. For this, let $x, y \in A$ and $U \in \mathcal{T}$ such that $x \odot y \in U$.

Case 1: Let $x = y = 0$. Then $\{0\}$ is an open neighborhood of 0 and $x \odot y \in \{0\} \odot \{0\} \subseteq U$.

Case 2: Let $x = 0$ and $0 \neq y$. Then $x \odot y = 0 \in U$. Since $\{0\}$ is an open neighborhood of 0 and $y \in (0, y]$, we have $x \odot y \in \{0\} \odot (0, y] = \{0\} \subseteq U$.

Case 3: Let $0 \neq x = y$. Then $x \odot x = x \in U$. Hence $(0, x] \cap U$ is an open neighborhood of x such that $x \odot x \in ((0, x] \cap U) \odot ((0, x] \cap U) \subseteq U$.

Case 4: Let $x < y$. Then $x \odot y = x \in U$. Since $x \in (0, x] \cap U \in \mathcal{T}$ and $y \in (x, y] \in \mathcal{T}$, we obtain $x \odot y \in ((0, x] \cap U) \odot (x, y] = (0, x] \cap U \subseteq U$.

Case 5: Let $x > y$. Then $x \odot y = y \in U$. Since $x \in (y, x]$ and $y \in (0, y] \cap U$, $x \odot y \in (y, x] \odot ((0, y] \cap U) = (0, y] \cap U \subseteq U$.

Hence, $(A, \odot, \mathcal{T})$ is a topological hoop. Now, we prove that $(A, \to, \mathcal{T})$ is not a topological hoop. For this, we consider $1/2 \to 1/2 = 1 \in (1/2, 1]$. Let $a \in \mathbb{R}$ and $(a, 1/2]$ be a neighborhood of $1/2$. Suppose $b = (a + 1/2)/2$. Then $b \in (a, 1/2]$, and so $b < 1/2$. Hence, $1/2 \to b = b \notin (1/2, 1]$.

Proposition 3.5. *Let $x^2 = x$, for all $x \in A$. Then there exists a topology $\mathcal{T}$ on A such that $\odot$ is continuous.*

Proof. Let $a \in A$. Define $A_a = \{x \in A \mid x \odot a = a\}$. Clearly, $a \in A_a$. We prove that $A_a \in \mathcal{F}(A)$. For this, let $x, y \in A_a$. Then $x \odot a = y \odot a = a$. By (HP1),

$$(x \odot y) \odot a = x \odot (y \odot a) = x \odot a = a.$$

Hence, $x \odot y \in A_a$. Also, suppose $x \leqslant y$ and $x \in A_a$, for some $x, y \in A$. Then by Proposition 2.2(*iii*) and (x), we have $a = x \odot a \leqslant y \odot a \leqslant a$. Thus, $y \odot a = a$. Hence, $y \in A_a$, and so $A_a \in \mathcal{F}(A)$, for all $a \in A$. Let $B = \{A_a \mid a \in A\}$. Suppose $a \in A_x \cap A_y$ and z be an arbitrary element of A_a. Then

$$z \odot x = z \odot (a \odot x) = (z \odot a) \odot x = a \odot x = x$$

and

$$z \odot y = z \odot (a \odot y) = (z \odot a) \odot y = a \odot y = y.$$

Thus, $z \in A_x \cap A_y$, and so B is a basis. Let $\mathcal{T}$ be a topology generated by B. We prove that $\odot$ is continuous. Let $x, y \in A$. Then $x \odot y \in A_{x \odot y}$. Since $x \in A_x$ and $y \in A_y$, it is enough to prove that $A_x \odot A_y \subseteq A_{x \odot y}$. Let $\alpha \in A_x \odot A_y$. Then there

exist $a \in A_x$ and $b \in A_y$ such that $\alpha = a \odot b$. Since $a \in A_x$ and $b \in A_y$, $a \odot x = x$ and $b \odot y = y$, respectively. Thus, by (HP1),

$$\alpha \odot (x \odot y) = (a \odot b) \odot (x \odot y) = (a \odot x) \odot (b \odot y) = x \odot y.$$

Hence, $\alpha \in A_{x \odot y}$. Therefore, $\odot$ is continuous. □

Proposition 3.6. *Let A be bounded with (DNP). Then $(A, \to, \mathcal{T})$ is a semitopological hoop if and only if $(A, \odot, ', \mathcal{T})$ is a semitopological hoop.*

Proof. ($\Rightarrow$) Let $(A, \to, \mathcal{T})$ be a semitopological hoop. It is clear that $'$ is continuous. Now, we prove that $\odot$ is continuous in the second variable. Let $x \odot y \in U \in \mathcal{T}$. Since A has (DNP), by (HP3)

$$x \odot y = (x \odot y)'' = ((x \odot y) \to 0) \to 0 = (x \to (y \to 0)) \to 0 = (x \to y')',$$

hence $(x \to y')' \in U$. Since $'$ is continuous, there exists $V \in \mathcal{T}$, such that $x \to y' \in V$ and $V' \subseteq U$. Also, since $\to$ is continuous in the second variable, there exists $W \in \mathcal{T}$, such that $y' \in W$ and $x \to y' \in x \to W \subseteq V$. Again, since $'$ is continuous, there is $Q \in \mathcal{T}$ such that $y \in Q$ and $y' \in Q' \subseteq W$. Now, $Q \in \mathcal{T}$ is an open neighborhood of $y \in Q$ and $x \odot y \in x \odot Q \subseteq U$, because if $z \in Q$, then

$$x \odot z = (x \to z')' \in (x \to Q')' \subseteq (x \to W)' \subseteq V' \subseteq U.$$

Since the operator $\odot$ is commutative, $\odot$ is continuous in each variable. Hence, $(A, \odot, ', \mathcal{T})$ is a semitopological hoop.

($\Leftarrow$) Let $(A, \odot, ', \mathcal{T})$ be a semitopological hoop. We prove that $(A, \to, \mathcal{T})$ is a semitopological hoop. For this, we prove that $\to$ is continuous in two variables. At first, we show that $\to$ is continuous in the second variable. Let $x \to y \in U \in \mathcal{T}$. Since A has (DNP), by (HP3),

$$(x \odot y')' = x \to y'' = x \to y \in U$$

Since $'$ is continuous, there exists an open neighborhood V of $x \odot y'$ such that $V' \subseteq U$. Also, since $\odot$ is continuous in the second variable, there exists an open neighborhood W of y' such that $x \odot y' \in x \odot W \subseteq V$. Again, since $'$ is continuous, there is $Q \in \mathcal{T}$, such that $y \in Q$ and $Q' \subseteq W$. Now, Q is an open neighborhood of y such that $x \to y \in x \to Q \subseteq U$, because if $z \in Q$, then

$$x \to z = (x \odot z')' \in (x \odot Q')' \subseteq (x \odot W)' \subseteq V' \subseteq U.$$

Now, we prove that $\to$ is continuous in the first variable. For this, let $x \to y \in U \in \mathcal{T}$. Then $x \to y = (x \odot y')' \in U$. Since $'$ is continuous, there is $V \in \mathcal{T}$ such that $x \odot y' \in V$ and $V' \subseteq U$. Since $\odot$ is continuous in the first variable, there exists $Q \in \mathcal{T}$, $x \in Q$ and $x \odot y' \in Q \odot y' \subseteq V$. Thus, Q is an open neighborhood of x such that

$$x \to y = (x \odot y')' \in (Q \odot y')' \subseteq V' \subseteq U$$

Hence, $\to$ is continuous in the first variable. □

Theorem 3.7. *Let A be bounded with (DNP). If $(A, \to, \mathcal{T})$ is a topological hoop, then $(A, \mathcal{T})$ is a topological hoop.*

Proof. Let $\to$ be continuous. Then the maps $'$ and $f : A \times A \hookrightarrow A \times A$ by $f(x, y) = (x, y')$, both, are continuous. Since for each $x, y \in A$, $x \odot y = (x \to y')'$, we get that $\odot$ is the composite of continuous maps f, $\to$ and $'$. Hence $\odot$ is continuous. □

For an arbitrary element $a \in A$ we define the subset

$$V(a) = \{x \in A \mid x \to a, a \to x \in V\}.$$

Theorem 3.8. *There is a nontrivial topology $\mathcal{T}$ on A such that $(A, \mathcal{T})$ is a topological hoop.*

Proof. Let

$$\mathcal{T} = \{U \subseteq A \mid \text{for every } a \in U, \text{there exists } F \in \mathcal{F}(A) \text{ such that } F(a) \subseteq U\}.$$

Suppose $\{U_i : i \in I\}$ is a collection of members of $\mathcal{T}$. For any $x \in \bigcup U_i$, there are $F \in \mathcal{F}(A)$ and $j \in I$ such that $F(x) \subseteq U_j \subseteq \bigcup U_i$. Hence $\bigcup U_i \in \mathcal{T}$. On the other hand, for any $x \in \bigcap U_i$ and any $i \in I$, there are $F_i \in \mathcal{F}(A)$ such that $x \in F_i(x) \subseteq U_i$. Let $F = \bigcap F_i$. Then $x \in F(x) \subseteq \bigcap U_i$. Hence $\bigcap U_i \in \mathcal{F}(A)$. Thus, $\mathcal{T}$ is a topology on A. Let $F \in \mathcal{F}(A)$, $x \in A$ and $y \in F(x)$. If $z \in F(y)$, then $z \to y$ and $y \to z$, both, are in F. Since $y \to x$ and $x \to y$, both, are in F, we get that $z \to x \in F$ and $x \to z \in F$. Hence $F(y) \subseteq F(x)$ and so $F(x)$ is in $\mathcal{T}$. Therefore, $\mathcal{T}$ is nontrivial topology. Let $* \in \{\odot, \to\}$, $F \in \mathcal{F}(A)$ and $x, y \in A$. Since $F(x) = \overline{x}$ and $F(y) = \overline{y}$, $F(x * y) = F(x) * F(y)$. This proves that $*$ is continuous. □

Corollary 3.9. *Let $\mathcal{T}$ be as in Theorem 3.8 and $X \subseteq A$. Then:*

(i) for each $F \in \mathcal{F}(A)$, $F(X)$ is an open and closed subset of A. Moreover, each filter is an open and closed set,

(ii) $\overline{X} = \bigcap\{F(X) \mid F \in \mathcal{F}(A)\}$.

Proof. *(i)*. Let $F \in \mathcal{F}(A)$, and $y \in \overline{F(X)}$. Then, $F(y) \cap F(X) \neq \emptyset$. Hence there is $x \in X$, such that $F(y) = F(x)$ and so $y \in F(x) \subseteq F(X)$. Therefore, $F(X)$ is closed. But $F(X)$ is open because it is a union of open sets.

(ii). Let $X \subseteq A$ and $x \in \overline{X}$. Since for all $F \in \mathcal{F}(A)$, $x \to x = 1 \in F$, we have $x \in F(x)$, and so $x \in \bigcap\{F(X) \mid F \in \mathcal{F}(A)\}$.

Conversely, let $x \in \bigcap\{F(X) \mid F \in \mathcal{F}(A)\}$. Then, for all $F \in \mathcal{F}(A)$, $x \in F(X)$. Since $F(X) = \bigcup_{a \in X} F(a)$, there exists $b \in X$ such that $x \in F(b)$. Moreover, since $x \to b \in F$ and $b \to x \in F$, we have $b \in F(x) \cap X$. Hence, $x \in \overline{X}$. □

Theorem 3.10. *Let Ω be a family of nonempty subsets of A such that Ω is closed under intersection and for each $x, y \in A$ and $V \in \Omega$,*

(i) if $x \in V$ and $x \leqslant y$, then $y \in V$,

(ii) if $x \in V$, then there exists $U \in \Omega$ such that $U(x) \subseteq V$,

(iii) there exists $W \in \Omega$ such that $W(x) \subseteq V$, for any $x \in W$ or equivalently,

$W(W) \subseteq V$.

Then there is a nontrivial topology $\mathcal{T}$ on A such that $(A, \mathcal{T})$ is a topological hoop.

Proof. It is easy to prove that $\mathcal{F}(A) \subseteq \Omega$. Let

$$\mathcal{T} = \{O \subseteq A \mid \text{for every } a \in O, \text{there exists } V \in \Omega \text{ such that } V(a) \subseteq O\}.$$

Firstly, we prove that $\mathcal{T}$ is closed under union and intersection. For this let $\{O_i : i \in I\} \subseteq \mathcal{T}$. Then, for every $a \in \bigcup O_i$, there exist $i \in I$ and $V \in \Omega$ such that $a \in V(a) \subseteq O_i \subseteq \bigcup O_i$. Hence $\mathcal{T}$ is closed under union. For any $a \in \bigcap O_i$ and any $i \in I$, there exists $V_i \in \Omega$ such that $a \in V_i(a) \subseteq O_i$. Put $V = \bigcap V_i$, then $V(a) \subseteq \bigcap V_i(a) \subseteq \bigcap O_i$ and so $\mathcal{T}$ is closed under intersection. Hence, $\mathcal{T}$ is a topology on A. Now, we prove that for each $V \in \Omega$ and $a \in A$, $V(a)$ is an open set. Let $a \in A$, $V \in \Omega$ and $x \in V(a)$. Then, $x \to a, a \to x \in V$. By (ii), there exist U_1 and $U_2 \in \Omega$ such that $U_1(a \to x) \subseteq V$ and $U_2(x \to a) \subseteq V$. Put $W = U_1 \cap U_2 \in \Omega$. If $y \in W(x)$, then $x \to y$ and $y \to x \in W$. By Proposition 2.2$(xiii)$,

$$x \to y \leqslant (y \to a) \to (x \to a), \qquad y \to x \leqslant (x \to a) \to (y \to a).$$

By (i),

$$(y \to a) \to (x \to a) \in W, \qquad (x \to a) \to (y \to a) \in W$$

Thus,

$$y \to a \in W(x \to a) \subseteq (U_1 \cap U_2)(x \to a) \subseteq U_2(x \to a) \subseteq V.$$

By the similar way, we can see that $a \to y \in V$. Then obviously, $W(x) \subseteq V(a)$. Hence, $V(a)$ is an open set and $\mathcal{T}$ is a nontrivial topology. Clearly, the set $B = \{V(a) : V \in \Omega, a \in A\}$ is a base for $\mathcal{T}$.

Now we prove that $(A, \mathcal{T})$ is a topological hoop. At first, we show that $\odot$ is continuous. Let $x \odot y \in O \in \mathcal{T}$. Consider $V \in \Omega$ such that $V(x \odot y) \subseteq O$. By (i), $1 \in V$, so $x \odot y \in V(x \odot y)$. By (iii), there is $W \in \Omega$ such that $W(W) \subseteq V$. Let $u \in W(x)$ and $v \in W(y)$. Then $u \to x, x \to u, v \to y$ and $y \to v$, all, belong to W. By Proposition 2.2(iv), $(x \to u) \leqslant [(x \odot y) \to (u \odot v)] \to (x \to u)$ and by (i), $[(x \odot y) \to (u \odot v)] \to (x \to u) \in W$. On the other hand, we have

$$\begin{aligned}
(x \to u) \to ((x \odot y) \to (u \odot v)) &= (x \to u) \to [x \to (y \to (u \odot v))], \text{ by (HP3)} \\
&= [x \odot (x \to u)] \to [y \to (u \odot v)], \text{ by Prop. 2.2} \\
&\geqslant u \to [y \to (u \odot v)], \text{ by Prop. 2.2} \\
&\geqslant y \to v.
\end{aligned}$$

Since $W \in \Omega$ and $y \to v \in W$, by (i), $(x \to u) \to ((x \odot y) \to (u \odot v)) \in W$. Thus, $(x \odot y) \to (u \odot v) \in W(x \to u) \subseteq W(W) \subseteq V$. Hence, $(x \odot y) \to (u \odot v) \in V$. By the similar way, we have $(u \odot v) \to (x \odot y) \in V$. Therefore, $W(x) \odot W(y) \subseteq V(x \odot y)$. This proves that $\odot$ is continuous.

Now, we prove that $\to$ is continuous. Let $x \to y \in V(x \to y)$. By (iii), there is $W \in \Omega$ such that $W(W) \subseteq V$. Let $u \in W(x)$ and $v \in W(y)$. Then $u \to x, x \to u, v \to y$ and $y \to v \in W$. By (HP3) we have,

$$\begin{aligned}(v \to y) \to ((u \to v) \to (x \to y)) &= [(u \to v) \odot (v \to y)] \to (x \to y), \text{ by Prop. 2.2}\\ &\geq (u \to y) \to (x \to y), \text{ by (HP3)}\\ &= x \to ((u \to y) \to y), \text{ by Prop. 2.2}\\ &\geq x \to u\end{aligned}$$

Since $W \in \Omega$ and $x \to u \in W$, by (i), $(v \to y) \to ((u \to v) \to (x \to y)) \in W$. Also, by Proposition 2.2(iv), $v \to y \leqslant ((u \to v) \to (x \to y)) \to (v \to y)$. Again, since $W \in \Omega$ and $v \to y \in W$, by (i), $((u \to v) \to (x \to y)) \to (v \to y) \in W$. Thus, $(u \to v) \to (x \to y) \in W(v \to y) \subseteq W(W) \subseteq V$. This implies that $(u \to v) \to (x \to y) \in V$. By the similar way, we have $(x \to y) \to (u \to v) \in V$. Therefore, $W(x) \to W(y) \subseteq V(x \to y)$ which implies that $\to$ is continuous. □

Corollary 3.11. *Let $\mathcal{T}$ be the topology in Theorem* 3.10 *and $X \subseteq A$. Then:*
(i) *for each $V \in \Omega$, $V(X)$ is an open and closed subset of A,*
(ii) $\overline{X} = \bigcap\{F(X) \mid F \in \mathcal{F}(A)\}$.

Proof. (i). Let $V \in \Omega$ and $y \in \overline{V(X)}$. Then there exists a net $\{y_i : i \in I\}$ which convergence to y. Since $\to$ is continuos, the nets $\{y_i \to y\}$ and $\{y \to y_i\}$, both, convergence to 1. Since $1 \in V$, $y_i \to y$ and $y \to y_i$, both, are in V, for some $i \in I$. Hence $y \in V(y_i) \subseteq V(X)$. Therefore, $V(X)$ is closed. But it is open because it is the union of open sets.

(ii). The proof is similar to the proof of Corollary 3.9(ii). □

Proposition 3.12. *If $(A, \mathcal{T})$ is a topological hoop, then $(A, \wedge, \mathcal{T})$ is a topological hoop.*

Proof. Let $f : A \times A \to A \times A$ by $f(x, y) = (x, x \to y)$, for all $x, y \in A$. Since $(A, \to, \mathcal{T})$ is a topological hoop, f is continuous. Also, by Proposition 2.2(i),

$$\wedge(x, y) = x \wedge y = x \odot (x \to y) = (\odot \circ f)(x, y).$$

Since $\odot$ and f are continuous, $\wedge$ is continuous. Therefore, $(A, \wedge, \mathcal{T})$ is a topological hoop. □

Proposition 3.13. *Let A be a $\sqcup$-hoop and $\mathcal{T}$ be a topology on A. Then:*
(i) *if $(A, \wedge, \to, \mathcal{T})$ is a topological hoop, then $(A, \sqcup, \mathcal{T})$ is a topological hoop,*
(ii) *if A has (DNP) and $(A, \to, \mathcal{T})$ is a topological hoop, then $(A, \sqcup, \mathcal{T})$ is a topological hoop.*

Proof. (i). Let $f : A \times A \to A$ is defined by $f(x, y) = (x \to y) \to y$ and $g : A \times A \to A$ by $g(x, y) = (y \to x) \to x$, for all $x, y \in A$. Since $(A, \to, \mathcal{T})$ is a topological hoop, f and g are continuous. Also, define $f \wedge g : A \times A \to A$ by

$(f \wedge g)(x,y) = f(x,y) \wedge g(x,y)$, for all $x, y \in A$. Since $(A, \to, \mathcal{T})$ is a topological hoop, by Proposition 3.12, $\wedge$ is continuous. Then $f \wedge g$ is continuous. Moreover,

$$\sqcup(x,y) = x \sqcup y = ((x \to y) \to y) \wedge ((y \to x) \to x) = f(x,y) \wedge g(x,y) = (f \wedge g)(x,y).$$

Hence, $\sqcup = f \wedge g$ is continuous.

(ii). Let $x, y \in A$, $U \in \mathcal{T}$ and $x \sqcup y \in U$. Since A has (DNP), by Proposition 2.3(vii), $x \sqcup y = (x \to y) \to y$. Moreover, since $(A, \to, \mathcal{T})$ is a topological hoop, $\sqcup$ is continuous. □

Theorem 3.14. *Let $\mathcal{T}$ be a topology on A and $h : A^3 \to A^2$ is defined by $h(a,b,c) = (a \to b, b \to c)$, for all $a, b, c \in A$. If $\{1\}$ is an open set and h is continuous, then $(A, \mathcal{T})$ is a topological hoop.*

Proof. Let $a \in A$ and $h_a(b) = (a \to b, b \to a)$. Since h is continuous, h_a is continuous. Now, since $\{1\}$ is open, $\{1\} \times \{1\}$ is open in A^2. On the other hand,

$$\begin{aligned} h_a^{-1}(1,1) &= \{b \in A \mid h_a(b) = (1,1)\} = \{b \in A \mid (a \to b, b \to a) = (1,1)\} \\ &= \{b \in A \mid a \to b = 1, b \to a = 1\} = \{b \in A \mid b = a\} = \{a\}. \end{aligned}$$

Hence, $\{a\}$ is an open set and $\mathcal{T}$ is a discrete topology. Therefore, $(A, \mathcal{T})$ is a topological hoop. □

Theorem 3.15. *Let $(A, \to, \mathcal{T})$ be a semitopological hoop. If $\{1\}$ is an open set, then $(A, \mathcal{T})$ is a topological hoop.*

Proof. Let $\{1\}$ be an open set and $x \in A$. Since $(A, \mathcal{T})$ is a semitopological hoop and $x \to x = 1 \in \{1\}$, there is an open sets U such that $x \in U$, $x \to U = 1$ and $U \to x = \{1\}$, which implies that $U = \{x\}$. Hence $\mathcal{T}$ is a discrete topology on A and so $(A, \mathcal{T})$ is a topological hoop. □

Proposition 3.16. *Let $(A, \to, \mathcal{T})$ be a topological hoop and $F \in \mathcal{F}(A)$. Then:*

(i) if 1 is an interior point of F, then F is an open set,

(ii) if F is an open set, then F is closed,

(iii) if A is connected, then A has no open proper filter.

Proof. Let $(A, \to, \mathcal{T})$ be a topological hoop and $F \in \mathcal{F}(A)$.

(i). Suppose $x \in F$. Since 1 is an interior point of F, there exists $U \in \mathcal{T}$ such that $x \to x = 1 \in U \subseteq F$. Since $\to$ is continuous, there exists $V \in \mathcal{T}$ such that $x \in V$ and $V \to V \subseteq F$. Now, for all $y \in V$, we have $x \to y \in V \to V \subseteq F$, and so $x \to y \in F$. Since $F \in \mathcal{F}(A)$ and $x \in F$, by Proposition 2.6, $y \in F$. Thus, $y \in V \subseteq F$ which implies that F is an open set.

(ii). Let F be an open set. We prove that F is closed. For this, we show that F^c is an open set. Let $x \in F^c$. Then $x \notin F$. Since $x \to x = 1 \in F \in \mathcal{T}$ and $\to$ is continuous, there exists $U \in \mathcal{T}$ such that $x \in U$ and $U \to U \subseteq F$. Now, we prove that $U \subseteq F^c$. For this, let $U \cap F \neq \emptyset$. Then there is $y \in U \cap F$ such that

$y \to U \subseteq F$. So, for all $z \in U$, $y \to z \in F$. Since $F \in \mathcal{F}(A)$, by Proposition 2.6, $z \in F$, and so $U \subseteq F$. Thus, $x \in F$, which is a contradiction. Then $U \cap F = \emptyset$. Hence, $x \in U \subseteq F^c$ shows that F^c is an open set and so F is closed.

(*iii*). Suppose F is an open filter of A. Then by (ii), F is closed. Since A is connected, we have $A = F$. □

A topological space A is called *totally disconnected*, if every connected subset $X \subseteq A$ is either empty or a singleton. A subset X of A is called a *component subspace*, if it is the maximal connected subspace (cf. [11]).

Proposition 3.17. *Let $(A, \to, \mathcal{T})$ be a semitopological hoop. Then A is totally disconnected if and only if every its connected subset containing 1 consists just 1.*

Proof. ($\Rightarrow$) Suppose A is totally disconnected and $X \subseteq A$ is a connected of 1. Then it is clear that $X = \{1\}$.

($\Leftarrow$) Let D be a connected subset of A and $x \in D$. Then by (HP2), $1 \in (D \to x) \cap (x \to D)$. Since $(A, \to, \mathcal{T})$ is a semitopological hoop and D is connected, it is clear that $x \to D$ and $D \to x$ are connected. By assumption, $D \to x = \{1\}$ and $x \to D = \{1\}$ and so $D = \{x\}$. Therefore, A is totally disconnected. □

Proposition 3.18. *Let $(A, \mathcal{T})$ be a topological hoop and $C \subseteq A$ be a component of 1 which contains all connected subset of A. Then C is a filter of A.*

Proof. Let $a \in C$. Since $(A, \odot, \mathcal{T})$ is a topological hoop, $a \odot C$ is a connected subset of A. Since $a \in C \cap (a \odot C)$, the set $C \cup (a \odot C)$ is a connected subset of A which contains 1. By assumption, $C \cup (a \odot C) \subseteq C$, and so $a \odot C \subseteq C$. Hence, $C \odot C \subseteq C$. Now, suppose that $x \leqslant y$ and $x \in C$, for some $x, y \in A$. Then $x \wedge y = x \in C$. Thus, $x = x \wedge y \in C \wedge y$. Since $(A, \mathcal{T})$ is a topological hoop, by Proposition 3.12, $(A, \wedge, \mathcal{T})$ is a topological hoop. Thus, $C \wedge y$ is a connected set, and so $C \wedge y \subseteq C$. Hence, $y = 1 \wedge y \in C \wedge y \subseteq C$, and so $y \in C$. Therefore, $C \in \mathcal{F}(A)$. □

Let A be a hoop and $F \in \mathcal{F}(A)$. In the preliminary, we saw that A/F is a quotient hoop and $\pi_F : A \to A/F$ is a canonical epimorphism. Let $\mathcal{T}$ be a topology on A and U be a subset of A/F. Then we say that U is an open subset of A/F if and only if $\pi_F^{-1}(U)$ is an open subset of A. Now, if we consider

$$\overline{\mathcal{T}} = \{U \subseteq A/F \mid \pi_F^{-1}(U) \in \mathcal{T}\}$$

then it is easy to show that $\overline{\mathcal{T}}$ is a topology on A/F. This topology on A/F is called *the quotient topology induced by π_F*. It is well known that it is the largest topology on A/F making π_F continuous.

Theorem 3.19. *Let A be a hoop and $F \in \mathcal{F}(A)$. If $(A, \mathcal{T})$ is a (semi)topological hoop and π_F is an open set, then $(A/F, \overline{\mathcal{T}})$ is a (semi)topological hoop.*

Proof. Let $(A,\mathcal{T})$ be a topological hoop, $\star \in \{\otimes, \rightsquigarrow\}$ and $\overline{x} \star \overline{y} \in V \in \overline{\mathcal{T}}$, for $\overline{x}, \overline{y} \in A/F$. Then $\overline{x * y} \in V$, for some $* \in \{\odot, \rightarrow\}$. Since π_F is continuous, $x * y \in \pi_F^{-1}(V) \in \mathcal{T}$. Since $(A,\mathcal{T})$ is a topological hoop, there exist $U, W \in \mathcal{T}$ such that $x \in U$, $y \in W$ and $x * y \in U * W \subseteq \pi_F^{-1}(V)$. Since π_F is an open map, $\pi_F(U)$ and $\pi_F(W)$ are in $\overline{\mathcal{T}}$, $\overline{x} \in \pi_F(U)$, $\overline{y} \in \pi_F(W)$ and $\overline{x} \star \overline{y} \in \pi_F(U) \star \pi_F(W) \subseteq V$. Hence, $(A/F, \star, \overline{\mathcal{T}})$ is a topological hoop. □

Proposition 3.20. *Let $(A,\mathcal{T})$ be a topological hoop and $F \in \mathcal{F}(A)$. Then:*

(i) A/F has a discrete topology if and only if F is open,

(ii) if $(A,\mathcal{T})$ is a compact topological hoop, then A/F is a discrete finite topological hoop if and only if F is open.

Proof. (i). Since A/F has a discrete topology, every single set such as $\{x/F\}$ is open, for any $x \in A$. Since $1 \in A$, $\{1/F\}$ is open. Since $\{1/F\} = F$, F is open. Conversely, if F is an open set, then $\{1/F\}$ is an open set, too. Since A/F is a hoop, by Theorem 3.15, A/F has a discrete topology.

(ii). Suppose A is compact. Since π is a continuous epimorphism, $\pi(A) = A/F$ is compact. Let F is open. Then by (i), A/F has a discrete topology and so every single subset is open. Moreover, since A/F is compact, A/F is equal to union of finite open subsets. Thus A/F is finite. The converse, by (i) is clear. □

Definition 3.21. (cf. [11]) Let $(X,\mathcal{T})$ be a topological space and $x \in X$. A *local basis at x* is a set B of open neighborhoods of x such that for all $U \in \mathcal{T}$ if $x \in U$, then there exists $H \in B$ such that $x \in H \subseteq U$.

Lemma 3.22. *Let $F \in \mathcal{F}(A)$. If $\mathcal{T}$ is a topology on A and $\overline{\mathcal{T}}$ is the quotient topology on A/F, then for each $x \in A$, $\pi_F^{-1}(\pi_F(\overline{x})) = \overline{x}$. Moreover, if $V \in \overline{\mathcal{T}}$, then there exists $U \in \mathcal{T}$ such that $\pi_F(U) = V$.*

Proof. The proof is easy. □

Theorem 3.23. *Let $(A,\mathcal{T})$ be a semitopological hoop and $F \in \mathcal{F}(A)$. Then*

$$B = \{\pi(U * x) \mid U \in \mathcal{T}, 1 \in U, x \in A\}$$

is a local base of the space A/F at the point $x/F \in A/F$, such that $* \in \{\odot, \rightarrow\}$ and the map $\pi : A \to A/F$ is open.

Proof. Let $U \in \mathcal{T}$. Since $1 \in U$, it is clear that $x \in U * x$, for all $x \in A$. Thus, $x/F \in \pi(U * x)$. Now, suppose that $x/F \in A/F$. Then there exists $W \in \overline{\mathcal{T}}$ such that $x/F \in W$. Since W is open and π is continuous, we have $x \in \pi^{-1}(W) = O$. On the other hand, by (HP1), $x = 1 * x \in O$. Since $*$ is continuous, there exists $U \in \mathcal{T}$ such that $1 \in U$ and $x \in U * x \subseteq O$. Thus,

$$x/F \in \pi(U * x) \subseteq \pi(O) = \pi(\pi^{-1}(W)) = W$$

and so $\pi^{-1}(\pi(U*x)) \subseteq O$. By Lemma 3.22, $\pi^{-1}(\pi(U*x)) = (U*x)/F \subseteq O$. Thus, $\pi(U*x) \subseteq W$. Hence, B is a local basis. By definition of quotient topology, $\pi(U*x) = (U*x)/F = \bigcup_{y\in U*x} y/F$ and by Lemma 3.22,

$$\pi^{-1}(\pi(U*x)) = (U*x)/F = \bigcup_{y\in U*x} y/F.$$

Since $\bigcup_{y\in U*x} y/F$ is open in A and π is continuous, we get $\pi(U*x)$ is open in $\overline{\mathcal{T}}$. Therefore, π is open. □

References

[1] **M. Aaly Kologani, N. Kouhestani, R.A. Borzooei**, *On topological semi-hoops*, Quasigroups Related Systems, **25** (2017), 165 – 179.

[2] **P. Agliano, I.M.A. Ferreirim, F. Montagna**, *Basic hoops: an algebraic study of continuous t-norm*, draft, (2000).

[3] **R.A. Borzooei, G.R. Rezaei, N. Kouhestani**, *On (semi)topological BL-algebras*, Iran. J. Math. Sci. Info. **6** (2011), 59 – 77.

[4] **R.A. Borzooei, G.R. Rezaei, N. Kouhestani**, *Metrizability on (semi)topological BL-algebras*, Soft. Comput., **16** (2012), 1681 – 1690.

[5] **R.A. Borzooei, G.R. Rezaei, N. Kouhestani**, *Separation axioms in (semi)topological quotient BL-algebras*, Soft. Comput. **16** (2012), 1219 – 1227.

[6] **B. Bosbach**, *Komplementäre Halbgruppen. Axiomatik und Arithmetik*, Fundamenta Math. **64** (1969), 257 – 287.

[7] **B. Bosbach**, *Komplementäre Halbgruppen. Kongruenzen and Quotienten*, Fundamenta Math. **69** (1970), 1 – 14.

[8] **G. Georgescu, L. Leustean, V. Preoteasa**, *Pseudo-hoops*, J. Mult.-Val. Log. Soft Comput., **11** (2005), 153 – 184.

[9] **P. Hájek**, *Metamathematics of fuzzy logic*, Springer, (1998).

[10] **K. D. Joshi**, *Introduction to general topology*, New Age Inter. Pub. India. (1983).

[11] **J. R. Munkres**, *Topology a first course*, Engle. Cliffs. NJ: Prentice-Hall. **23** (1975).

[12] **A. Namdar, R.A. Borzooei, A. Borumand Saeid, M. Aaly Kologani**, *Some results in hoop algebras*, J. Intell. Fuzzy Syst. **32** (2017), 1805 – 1813.

Received March 26, 2019

M. Aaly Kologani
Hatef Higher Education Institute, Zahedan, Iran
E-mail: mona4011@gmail.com

R.A. Borzooei
Department of Mathematics, Shahid Beheshti University, Tehran, Iran
E-mail: borzooei@sbu.ac.ir

N. Kouhestani
Department of Mathematics, University of Sistan and Baluchestan, Zahedan, Iran
E-mail: Kouhestani@math.usb.ac.ir

Quasigroups and Related Systems **27** (2019), 175 – 180

A characterization of elementary abelian 3-groups

Chimere S. Anabanti

The author dedicates this paper to Professor Sarah Hart with admiration and respect.

Abstract. We give a characterization of elementary abelian 3-groups in terms of their maximal sum-free sets. A corollary to our result is that the number of maximal sum-free sets in an elementary abelian 3-group of finite rank n is $3^n - 1$.

1. Preliminaries

The well-known result of Schur which says that whenever we partition the set of positive integers into a finite number of parts, at least one of the parts contains three integers x, y and z such that $x + y = z$ introduced the study of sum-free sets. Schur [13] gave the result while showing that the Fermat's last theorem does not hold in F_p for sufficiently large p. The concept was later extended to groups as follows: A non-empty subset S of a group G is sum-free if for all $s_1, s_2 \in S$, $s_1 s_2 \notin S$. (Note that the case $s_1 = s_2$ is included in this restriction.) An example of a sum-free set in a finite group G is any non-trivial coset of a subgroup of G. Sum-free sets have applications in Ramsey theory and are also closely related to the widely studied concept of caps in finite geometry.

Some questions that appear interesting in the study of sum-free sets are:

(i) How large can a sum-free set in a finite group be?

(ii) Which finite groups contain maximal by inclusion sum-free sets of small sizes?

(iii) How many maximal by cardinality sum-free sets are there in a given finite group?

Each of these questions has been attempted by several researchers; though none is fully answered. For question (i), Diananda and Yap [7], in 1969, following an earlier work of Yap [18], determined the sizes of maximal by cardinality sum-free sets in finite abelian groups G, where $|G|$ is divisible by a prime $p \equiv 2(\mathrm{mod}\, 3)$, and where $|G|$ has no prime factor $p \equiv 2(\mathrm{mod}3)$ but 3 is a factor of $|G|$. They gave a good bound in the case where every prime factor of $|G|$ is congruent to

2010 Mathematics Subject Classification: 11B75; 20D60; 20K01; 05E15.
Keywords: Sum-free sets, maximal sum-free sets, elementary abelian groups.
The author was supported by a Birkbeck PhD Scholarship during this study.

$1 (\mathrm{mod}\, 3)$. Green and Ruzsa [10] in 2005 completely answered question (i) in the finite abelian case. The question is still open for the non-abelian case, even though there has been some progress by Kedlaya [11, 12], Gowers [9], amongst others.

For question (ii), Street and Whitehead [14] began research in that area in 1974. They called a maximal by inclusion sum-free set, a locally maximal sum-free set (LMSFS for short), and calculated all LMSFS in groups of small orders, up to 16 in [14, 15] as well as a few higher sizes. In 2009, Giudici and Hart [8] started the classification of finite groups containing LMSFS of small sizes. Among other results, they classified all finite groups containing LMSFS of sizes 1 and 2, as well as some of size 3. The size 3 problem was resolved in [5]. Question (ii) is still open for sizes $k \geqslant 4$; though some progress has been made in [1]. For other works on LMSFS, the reader may see [2, 3, 4, 6].

To be consistent with our notations, we will use the term 'maximal' to mean 'maximal by cardinality' and 'locally maximal' to mean 'maximal by inclusion'. Tărnăuceanu [16] in 2014 gave a characterization of elementary abelian 2-groups in terms of their maximal sum-free sets. His theorem (see Theorem 1.1 of [16]) states that "a finite group G is an elementary abelian 2-group if and only if the set of maximal sum-free sets coincides with the set of complements of the maximal subgroups". The author of [16] didn't define the term maximal sum-free sets. Unfortunately, the theorem is false whichever definition is used. If we take "maximal" in the theorem to mean 'maximal by cardinality', then a counterexample is the cyclic group C_4 of order 4, given by $C_4 = \langle x \mid x^4 = 1\rangle$. Here, there is a unique maximal (by cardinality) sum-free set namely $\{x, x^3\}$, and it is the complement of the unique maximal subgroup. But C_4 is not elementary abelian. On the other hand, if we take "maximal" to mean 'maximal by inclusion', then the theorem will still be wrong since $S = \{x_1, x_2, x_3, x_4, x_1x_2x_3x_4\}$ is a maximal by inclusion sum-free set in $C_2^4 = \langle x_1, x_2, x_3, x_4 \mid x_i^2 = 1, x_ix_j = x_jx_i \text{ for } 1 \leqslant i, j \leqslant 4\rangle$, but does not coincide with any complement of a maximal subgroup of C_2^4. These counterexamples were first pointed out in the arXiv manuscript at https://arxiv.org/abs/1611.06546, which prompted an erratum to be published by the author (see [17]).

For a prime p and $n \in \mathbb{N}$, we write $\mathbb{Z}_p^n$ for the elementary abelian p-group of finite rank n. We recall here that the number of maximal subgroups of $\mathbb{Z}_p^n$ is $\sum_{k=0}^{n-1} p^k$. Corollary 1.2 of [16] is that the number of maximal sum-free sets in $\mathbb{Z}_2^n$ is $2^n - 1$. This result is correct in its own right and can be proved by showing that each maximal sum-free set in $\mathbb{Z}_2^n$ is the non-trivial coset of a maximal subgroup of $\mathbb{Z}_2^n$, and every maximal subgroup of $\mathbb{Z}_2^n$ is the complement of a maximal sum-free set in $\mathbb{Z}_2^n$. In this paper, we give a characterization of elementary abelian 3-groups in terms of their maximal sum-free sets. Moreover, for prime $p > 3$, we show that there is no direct analogue of our result for elementary abelian p-groups of finite ranks. For the rest of this section, we state the main result of this paper and its immediate corollary. We remind the reader that $\Phi(G)$ denotes the Frattini subgroup of G.

Theorem 1.1. *A finite group G is an elementary abelian 3-group if and only if the set of non-trivial cosets of each maximal subgroup of G coincides with two maximal sum-free sets in G, every maximal sum-free set is a non-trivial coset of a maximal subgroup, and $\Phi(G) = 1$.*

Corollary 1.2. *The number of maximal sum-free sets in $\mathbb{Z}_3^n$ is $3^n - 1$.*

2. Proof of Theorem

Let S be a sum-free set in a finite group G. We define $SS = \{xy \mid x, y \in S\}$, $S^{-1} = \{x^{-1} \mid x \in S\}$ and $SS^{-1} = \{xy^{-1} \mid x, y \in S\}$. Clearly, $S \cap SS = \varnothing$. Moreover, $S \cap SS^{-1} = \varnothing$ as well; for if $x, y, z \in S$ with $x = yz^{-1}$, then $xz = y$, contradicting the fact that S is sum-free.

Lemma 2.1. *Let S be sum-free in $G = \mathbb{Z}_3^n$ ($n \in \mathbb{N}$), and let $x \in S$. Then the following hold:*

(*i*) *any two sets in $\{S, x^{-1}S, xS\}$ are disjoint;*

(*ii*) *any two sets in $\{S, SS^{-1}, S^{-1}\}$ are disjoint.*

Moreover, if S is maximal, then the following also hold:

(*iii*) *$S \cup x^{-1}S \cup xS = G$ and $|S| = \frac{|G|}{3}$;*

(*iv*) *$S \cup SS^{-1} \cup S^{-1} = G$.*

Proof. (*i*). As S is sum-free, $S \cap xS = \varnothing = S \cap x^{-1}S$. So we only need to show that $xS \cap x^{-1}S = \varnothing$. Suppose for contradiction that $xS \cap x^{-1}S \neq \varnothing$. Then there exist $y, z \in S$ such that $xy = x^{-1}z$. This means that $y = xz$; a contradiction. Therefore $xS \cap x^{-1}S = \varnothing$.

The proof of (*ii*) is similar to (*i*).

For (*iii*), as $S \cup x^{-1}S \cup xS \subseteq G$, we have that $3|S| \leq |G|$; whence $|S| \leq \frac{|G|}{3}$. Each maximal subgroup of G has size $\frac{|G|}{3}$. As any non-trivial coset of such a subgroup is sum-free and has size $\frac{|G|}{3}$; such a coset of the maximal subgroup must be maximal sum-free. Thus, $|S| = \frac{|G|}{3}$, and $S \cup x^{-1}S \cup xS = G$.

The proof of (*iv*) is similar. □

Proposition 2.2. *Suppose S is a maximal sum-free set in an elementary abelian 3-group G, and let $x \in S$. Then $xS = S^{-1} = SS$.*

Proof. Let S be a maximal sum-free set in an elementary abelian 3-group G, and $x \in S$. In the light of Lemma 2.1(*iv*), we deduce that $x^{-1}S = S^{-1}S$. Let $y \in xS$. By Lemma 2.1(*i*) therefore $y \notin S \dot{\cup} SS^{-1}$. So Lemma 2.1(iv) tells us that $y \in S^{-1}$,

and we conclude that $xS \subseteq S^{-1}$. On the other hand, if $y \in S^{-1}$, then Lemma 2.1(ii) and Lemma 2.1(iii) yield $y \in xS$; so $S^{-1} \subseteq xS$. Therefore $xS = S^{-1}$. Now,

$$SS = \bigcup_{x \in S} xS = \bigcup_{x \in S} S^{-1} = S^{-1}. \tag{1}$$

Thus, $xS = S^{-1} = SS$ as required. □

Suppose p is the smallest prime divisor of the order of a finite group G, and H is a subgroup of index p in G. Then H is normal in G. This fact is well-known but we include a short proof for the reader's convenience. Suppose for a contradiction that H is not normal. Then for some $g \in G$, we have $H^g \neq H$. But $|H^gH| = \frac{|H^g||H|}{|H^g \cap H|} = \frac{|H|^2}{|H^g \cap H|} = |H|\frac{|H|}{|H^g \cap H|} \geqslant |H|p = |G|$; thus $H^gH = G$. Therefore, $g = (gh_1g^{-1})h_2$ for some $h_1, h_2 \in H$. So $g = h_2h_1 \in H$, and we conclude that $H^g = H$; a contradiction. Therefore H is normal in G.

We now prove Theorem 1.1

Proof. Let G be an elementary abelian 3-group of finite rank n. Clearly, every maximal subgroup of G has size 3^{n-1}, and the non-trivial cosets of any maximal subgroup of G yield two maximal sum-free sets in G. Next, we show that every maximal sum-free set in G is a non-trivial coset of a maximal subgroup of G. Suppose S is a maximal sum-free set in G. Let $x \in S$ be arbitrary, and define $H := x^{-1}S$. We show that H is a subgroup of G. Let a and b be elements of H. Then $a = x^{-1}y$ and $b = x^{-1}z$ for some $y, z \in S$. Since $ab = x^{-1}(x^{-1}yz)$, it is sufficient to show that $x^{-1}yz \in S$. Recall from Lemma 2.1(iii) that $G = S \cup x^{-1}S \cup xS$. From Proposition 2.2 therefore, $G = S \cup x^{-1}S \cup S^{-1}$. Now, suppose $x^{-1}yz \in x^{-1}S$. Then there exists $q \in S$ such that $x^{-1}yz = x^{-1}q$. This implies that $yz = q$; a contradiction. Next suppose $x^{-1}yz \in S^{-1}$. Then there exists $q \in S$ such that $x^{-1}yz = q^{-1}$. So $yz = xq^{-1}$, and we obtain that $x^{-1}q = y^{-1}z^{-1} = (yz)^{-1}$; a contradiction as $x^{-1}q \in x^{-1}S$, $(yz)^{-1} \in (SS)^{-1} = S$ by Equation 1, and Lemma 2.1(i) tells us that $x^{-1}S \cap S = \varnothing$. We have shown that $x^{-1}yz \notin x^{-1}S \cup S^{-1}$. In the light of $G = S \cup x^{-1}S \cup S^{-1}$ therefore, $x^{-1}yz \in S$; whence, H is closed. So H is a subgroup of G. As $|H| = |x^{-1}S| = |S| = \frac{|G|}{3}$, we conclude that H is a maximal subgroup of G, and $S = xH$ is a non-trivial coset of H in G. So we have shown now that every maximal sum-free set in G is a non-trivial coset of a maximal subgroup of G. The third part that $\Phi(G) = 1$ follows from the fact that the intersection of maximal subgroups of G is trivial.

Conversely, suppose G is a finite group such that the set of non-trivial cosets of each maximal subgroup of G coincides with two maximal sum-free sets in G, every maximal sum-free set of G is a coset of a maximal subgroup of G, and $\Phi(G) = 1$. First and foremost, G has no subgroup of index 2; otherwise it will have a maximal sum-free set which is not a coset of a subgroup of index 3. As the smallest index

of a maximal subgroup of G is 3, any such subgroup must be normal in G. Let H be a Sylow 3-subgroup of G. Then either $H = G$ or H is contained in a maximal subgroup (say M) of G. Suppose H is contained in such maximal subgroup M. As $|G/M| = 3$, we deduce immediately that $|G : H|$ is divisible by 3; a contradiction! Therefore, $H = G$, and we conclude that G is a 3-group. Now, G is an elementary abelian 3-group follows from the fact that $\Phi(G) = 1$ and $P/\Phi(P)$ is elementary abelian for every p-group P. □

Let $p > 3$ and prime, and suppose $n \in \mathbb{N}$. If $G = \mathbb{Z}_p^n$, then there exists a normal subgroup N of G such that $G/N \cong \mathbb{Z}_p$, and $\mathbb{Z}_p$ has a maximal sum-free set of size at least 2 (the latter fact follows from the classification of groups containing maximal by inclusion sum-free sets of size 1 in [8, Theorem 4.1]). The union of non-trivial cosets of N corresponding to this maximal sum-free set of $\mathbb{Z}_p$ is itself sum-free in G. So G has a maximal sum-free set of size at least $2|N|$. This argument shows that for $p > 3$, no direct analogue of Theorem 1.1 holds for elementary abelian p-groups of finite ranks.

References

[1] **C.S. Anabanti**, *On finite groups containing locally maximal product-free sets of size* 4, Algebra Discrete Math., to appear.

[2] **C.S. Anabanti**, *Three questions of Bertram on locally maximal sum-free sets*, Appl. Algebra Engineering, Comm. Comput., **30** (2019), 127–134.

[3] **C.S. Anabanti**, *On filled soluble groups*, Commun. Algebra, **46** (2018), 4914–4917.

[4] **C.S. Anabanti, G Erskine and S.B. Hart**, *Groups whose locally maximal product-free sets are complete*, Australas. J. Combin. **71** (2018), 544–563.

[5] **C.S. Anabanti and S.B. Hart**, *Groups containing small locally maximal product-free sets*, Int. J. Comb. 2016, Art. ID 8939182, 5 pp.

[6] **C.S. Anabanti and S. B. Hart**, *On a conjecture of Street and Whitehead on locally maximal product-free sets*, Australas. J. Combin. **63** (2015), 385–398.

[7] **P.H. Diananda and H. P. Yap**, *Maximal sum-free sets of elements of finite groups*, Proc. Japan Acad., **45** (1969), 1–5.

[8] **M. Giudici and S. Hart**, *Small maximal sum-free sets*, Electronic J. Combin., **16** (2009), 17pp.

[9] **W.T. Gowers**, *Quasirandom groups*, Combin., Probability Computing, **17** (2008), 363–387.

[10] **B. Green and I. Z. Ruzsa**, *Sum-free sets in abelian groups*, Israel J. Math., **147** (2005), 157–188.

[11] **K.S. Kedlaya**, *Large product-free subsets of finite groups*, J. Combin. Theory Series A, **77** (1997), 339–343.

[12] **K.S. Kedlaya**, *Product-free subsets of groups*, Amer. Math. Monthly, **105** (1998), 900–906.

[13] **I. Schur**, *Über die Kongruenz* $x^m + y^m \equiv z^m (\mathrm{mod}\ p)$, Jahresbericht der Deutschen Mathematiker-Vereinigung, **25** (1917), 114–116.

[14] **A.P. Street and E.G. Whitehead Jr.**, *Group Ramsey Theory*, J. Combin. Theory Series A, **17** (1974), 219–226.

[15] **A.P. Street and E.G. Whitehead, Jr.**, *Sum-free sets, difference sets and cyclotomy*, Comb. Math., Lect. Notes Math., **403** (1974), 109–124.

[16] **M. Tărnăuceanu**, *A characterization of elementary abelian* 2*-groups*, Archiv Math., **102** (2014), 11–14.

[17] **M. Tărnăuceanu**, *Erratum: A characterization of elementary abelian* 2*-groups*, Archiv Math., **108** (2017), 223–224.

[18] **H.P. Yap**, *Maximal sum-free sets of group elements*, J. London Mat. Soc., **44** (1969), 131–136.

Received May 31, 2019

Department of Mathematics
University of Nigeria
Nsukka (UNN), Enugu State
Nigeria
E-mail: chimere.anabanti@unn.edu.ng

Quasigroups and Related Systems **27** (2019), 181 – 200

Characterization of obstinate $\mathsf{H}_v\mathsf{MV}$-ideals

Mahmood Bakhshi and Akefe Radfar

Abstract. One motivation to study obstinate ideals in any algebra of logic is that the induced quotient algebra by these ideals is the two-element Boolean algebra. In this paper, we introduce two types of obstinate ideals in $\mathsf{H}_v\mathsf{MV}$-algebras; obstinate $\mathsf{H}_v\mathsf{MV}$-ideals and obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideals. Giving several theorems and examples we characterize these $\mathsf{H}_v\mathsf{MV}$-ideals. For example, we prove that an $\mathsf{H}_v\mathsf{MV}$-ideal (if exists) must be maximal, and any $\mathsf{H}_v\mathsf{MV}$-algebra with odd number of elements does not contatin an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal. Also, we characterize these $\mathsf{H}_v\mathsf{MV}$-ideals in finite $\mathsf{H}_v\mathsf{MV}$-algebras with at most six elements; we investigate that which subsets can be an obstinate (weak) $\mathsf{H}_v\mathsf{MV}$-ideal. In the sequel, we investigate the relationships between obstinate (weak) $\mathsf{H}_v\mathsf{MV}$-ideals, and Boolean and prime $\mathsf{H}_v\mathsf{MV}$-ideals. Finally, we prove that in a commutative $\mathsf{H}_v\mathsf{MV}$-algebra, the quotient $\mathsf{H}_v\mathsf{MV}$-algebra induced by an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal must be a two-elements Boolean algebra.

1. Introduction

In 1958, Chang [8] introduced the concept of an MV-algebra as an algebraic proof of completeness theorem for $\aleph_0$-valued Łukasiewicz propositional calculus, see also [9]. Many mathematicians have worked on MV-algebras and obtained significant results. Mundici [21] proved that MV-algebras and Abelian ℓ-groups with strong unit are categorically equivalent. He also proved that MV-algebras and bounded commutative BCK-algebras are categorically equivalent (see [20]). The ideal theory have an important role in studying algebras of logics such as MV-algebras because they are correspond to the sets of provable formulas in the correspond logics. In this respect various researches have published by many authors (see for example [14, 15, 16, 17]).

The hyperstructure theory (called also multialgebras) was introduced in 1934 by Marty [19]. Around the 40's, several authors worked on hypergroups, especially in France and in the United States, but also in Italy, Russia and Japan. Hyperstructures have many applications to several sectors of both pure and applied sciences. A short review of the theory of hyperstructures appear in [10]. In [11] a wealth of applications can be found, too. There are applications to the following subjects: geometry, hypergraphs, binary relations, lattices, fuzzy set and rough sets, automata, cryptography, combinatorics, codes, artificial intelligence and probabilities.

2010 Mathematics Subject Classification: 06F35, 20N20
Keywords: MV-algebra, $\mathsf{H}_v\mathsf{MV}$-algebra, obstinate $\mathsf{H}_v\mathsf{MV}$-ideal

Borzooei et al. [6, 18] applied the hyperstructures to BCK-algebras and introduced the notion of a hyper BCK-algebra and a hyper K-algebra, which is a hyperstructure weaker than hyper BCK-algebras. Recently, Ghorbani et al. [13] applied the hyperstructures to MV-algebras and introduced the concept of hyper MV-algebra and investigated some related results, see also [22]. Particularly, they investigated the relationships between hyper MV-algebras and hyper K-algebras. They proved that any hyper MV-algebra together with suitable (hyper) operations is a hyper K-algebra, and any hyper K-algebra satisfying some conditions can be viewed as a hyper MV-algebra.

In 1995, Vougiouklis introduced a generalization of hyperstructures so-called H_v-structure (see [23, 24]). Indeed, H_v-structures are a generalization of the well-known algebraic hyperstructures (hypergroup, hyperring, hypermodule and so on). Actually some axioms concerning the above hyperstructures such as the associative law, the distributive law and so on are replaced by their corresponding weak axioms. Since then the study of H_v-structure theory has been pursued in many directions by Vougiouklis, Davvaz, Spartalis and others. To investigate the relationships between H_v-structures such as H_v-groups and suitable generalizations of MV-algebras, the first author introduced $\mathsf{H}_v\mathsf{MV}$-algebras and gave various results. He introduced some types of ideals such as (fuzzy) $\mathsf{H}_v\mathsf{MV}$-ideals and (fuzzy) weak $\mathsf{H}_v\mathsf{MV}$-ideals and their generalizations (see [1, 2, 3, 4, 5]).

2. Preliminaries

This section is devoted to give some definitions and results from the literature. For more details we refer to the references.

Definition 2.1. An $\mathsf{H}_v\mathsf{MV}$-*algebra* is a nonempty set H endowed with a binary hyperoperation '$\oplus$', a unary operation '*' and a constant '0' satisfying the following conditions:

($\mathsf{H}_v\mathsf{MV}1$) $x \oplus (y \oplus z) \cap (x \oplus y) \oplus z \neq \emptyset$, (weak associativity)
($\mathsf{H}_v\mathsf{MV}2$) $(x \oplus y) \cap (y \oplus x) \neq \emptyset$, (weak commutativity)
($\mathsf{H}_v\mathsf{MV}3$) $(x^*)^* = x$,
($\mathsf{H}_v\mathsf{MV}4$) $(x^* \oplus y)^* \oplus y \cap (y^* \oplus x)^* \oplus x \neq \emptyset$,
($\mathsf{H}_v\mathsf{MV}5$) $0^* \in (x \oplus 0^*) \cap (0^* \oplus x)$,
($\mathsf{H}_v\mathsf{MV}6$) $0^* \in (x \oplus x^*) \cap (x^* \oplus x)$,
($\mathsf{H}_v\mathsf{MV}7$) $x \in (x \oplus 0) \cap (0 \oplus x)$,
($\mathsf{H}_v\mathsf{MV}8$) $0^* \in (x^* \oplus y) \cap (y \oplus x^*)$ and $0^* \in (y^* \oplus x) \cap (x \oplus y^*)$ imply $x = y$.

On any $\mathsf{H}_v\mathsf{MV}$-algebra H, the binary relation '$\preceq$' is defined as

$$x \preceq y \;\Leftrightarrow\; 0^* \in x^* \oplus y \cap y \oplus x^*.$$

Proposition 2.2. *In any* $\mathsf{H}_v\mathsf{MV}$-*algebra* H, *the following hold:* $\forall x, y \in H$ *and* $\forall A, B \subseteq H$,

(1) $A \preceq A$, $0 \preceq A \preceq 1$, *where* $1 = 0^*$,

(2) $A \preceq B$ *implies* $B^* \preceq A^*$,

(3) $(A^*)^* = A$,

(4) $A \cap B \neq \emptyset$ *implies that* $A \preceq B$,

(5) $x \odot (y \odot z) \cap (x \odot y) \odot z \neq \emptyset$, *where* $x \odot y = (x^* \oplus y^*)^*$,

(6) $(x \odot y) \cap (y \odot x) \neq \emptyset$,

(7) $0 \in (x \odot 0) \cap (0 \odot x)$,

(8) $0 \in (x \odot x^*) \cap (x^* \odot x)$,

(9) $x \in (x \odot 1) \cap (1 \odot x)$,

(10) $0 \in (x \wedge 0) \cap (0 \wedge x)$, *where* $x \wedge y = (x \oplus y^*) \odot y$,

(11) $x \preceq y$ *and* $y \preceq x$ *imply* $x = y$.

Definition 2.3. Let I be a nonempty subset of $\mathsf{H}_v\mathsf{MV}$-algebra H satisfying
(I_0) $x \preceq y$ and $y \in I$ imply $x \in I$.

I is called

(1) an $\mathsf{H}_v\mathsf{MV}$-*ideal* if $x \oplus y \subseteq I$, for all $x, y \in I$,

(2) a *weak* $\mathsf{H}_v\mathsf{MV}$-*ideal* if $x \oplus y \preceq I$, for all $x, y \in I$.

Obviously, any $\mathsf{H}_v\mathsf{MV}$-ideal is a weak $\mathsf{H}_v\mathsf{MV}$-ideal, but the converse is not true in general (see [1], for more details).

The set of all $\mathsf{H}_v\mathsf{MV}$-ideals of $\mathsf{H}_v\mathsf{MV}$-algebra H is denoted by $\mathbf{Id}(H)$.

From Proposition 2.2(4) it follows that

Theorem 2.4. *Every* $\mathsf{H}_v\mathsf{MV}$-*ideal is a weak* $\mathsf{H}_v\mathsf{MV}$-*ideal.*

From $(\mathsf{H}_v\mathsf{MV}7)$ it follows that $0 \in 0 \oplus 0$, whence $\{0\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal, in any $\mathsf{H}_v\mathsf{MV}$-algebra H. Generally $\{0\}$ is not an $\mathsf{H}_v\mathsf{MV}$-ideal, while H is itself an $\mathsf{H}_v\mathsf{MV}$-ideal (and so a weak $\mathsf{H}_v\mathsf{MV}$-ideal). Hence H is called trivial $\mathsf{H}_v\mathsf{MV}$-ideal, and $\{0\}$ and H are called the trivial weak $\mathsf{H}_v\mathsf{MV}$-ideals of H. Any (weak) $\mathsf{H}_v\mathsf{MV}$-ideal of H (except H itself) is called proper.

Definition 2.5. Let θ be an equivalence relation in $\mathsf{H}_v\mathsf{MV}$-algebra H.

- θ is called a *congruence* if
  (1) $x\theta y$ and $u\theta v$ imply that $x \oplus u\ \theta y \oplus v$, where $A\theta B$ means that for all $a \in A$ there exists $b \in B$ and for all $b \in B$ there exists $a \in A$ such that $a\theta b$.
  (2) $x\theta y$ implies that $x^*\theta y^*$,

- θ is said to be *regular* if $x^* \oplus y \cap y \oplus x^* \theta_w \{0^*\}$ and $y^* \oplus x \cap x \oplus y^* \theta_w \{0^*\}$ imply $x \theta y$, where $A \theta_w B$ means that there exist $a \in A$ and $b \in B$ such $a \theta b$.
- The congruence class $0/\theta$ is called the congruence kernel of θ.

Throughout the paper, H will denotes an $\mathsf{H}_v\mathsf{MV}$-algebra, unless otherwise stated.

3. Main results

Definition 3.1. A proper $\mathsf{H}_v\mathsf{MV}$-ideal I of H is called an *obstinate* $\mathsf{H}_v\mathsf{MV}$-*ideal* if it satisfies (OI), where

$$\text{(OI)} \quad (\forall x, y \in H \setminus I) \qquad x \odot y^* \cup y^* \odot x \subseteq I \text{ and } x^* \odot y \cup y \odot x^* \subseteq I$$

Definition 3.2. A proper weak $\mathsf{H}_v\mathsf{MV}$-ideal I of H is called an *obstinate* weak $\mathsf{H}_v\mathsf{MV}$-*ideal* if it satisfies (WOI), where

$$\text{(WOI)} \quad (\forall x, y \in H \setminus I) \qquad x \odot y^* \cup y^* \odot x \preceq I \text{ and } x^* \odot y \cup y \odot x^* \preceq I$$

From the definition it immediately follows that every obstinate $\mathsf{H}_v\mathsf{MV}$-ideal is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal, whereas the converse may not be true, in general.

Example 3.3. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra $\langle H; \oplus, ^*, 0\rangle$, where $H = \{0, a, b, 1\}$ and $\oplus$ and * are defined as given in Table 1. It is not difficult to check that $I = \{0, a\}$ is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H, while it is not an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal because $b, 1 \in H \setminus I$ but $1^* \odot b \cup b \odot 1^* = \{0, a, 1\} \not\subseteq I$.

$\oplus$	0	a	b	1
0	$\{0, a, b\}$	$\{a, b\}$	$\{b\}$	$\{0, a, b, 1\}$
a	$\{a\}$	$\{a\}$	$\{1\}$	$\{1\}$
b	$\{b\}$	$\{1\}$	$\{a, b, 1\}$	$\{a, 1\}$
1	$\{0, a, b, 1\}$	$\{0, b, 1\}$	$\{0, b, 1\}$	$\{a, b, 1\}$
$*$	1	b	a	0

Table 1: Cayley table of Example 3.3

Example 3.4. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra $\langle H; \oplus, ^*, 0\rangle$, where $H = \{0, a, b, 1\}$ and $\oplus$ and * are defined as given in Table 2.

$\oplus$	0	a	b	1
0	$\{0\}$	$\{a\}$	$\{b\}$	$\{1\}$
a	$\{a\}$	$\{a\}$	$\{1\}$	$\{1\}$
b	$\{b\}$	$\{1\}$	$\{b\}$	$\{1\}$
1	$\{1\}$	$\{1\}$	$\{1\}$	$\{b, 1\}$
$*$	1	b	a	0

Table 2: Cayley table of Example 3.4

It is not difficult to check that $I = \{0, a\}$ is an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal of H.

Theorem 3.5. *In an $\mathsf{H}_v\mathsf{MV}$-algebra with at least three elements, the singleton $\{0\}$ can not be an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal.*

Proof. Let H be an $\mathsf{H}_v\mathsf{MV}$-algebra with $|H| \geqslant 3$ and assume that $\{0\}$ is an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal of H, by contrary. Then for $x \in H \setminus \{0,1\}$ we have $x^* \odot 1 \cup 1 \odot x^* \subseteq \{0\}$; i.e., $x^* \odot 1 = \{0\}$, whence $x \oplus 0 = \{1\}$. This contradicts ($\mathsf{H}_v\mathsf{MV}7$). Thus $\{0\}$ is not an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal. □

Theorem 3.6. *Any obstinate $\mathsf{H}_v\mathsf{MV}$-ideal I of H satisfies*

$$x \in I \text{ or } x^* \in I \quad (\forall x \in H). \tag{3.1}$$

Proof. Assume that I is an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal of H and $x \in H \setminus I$. Since $1 \notin I$, so $x^* \in x^* \odot 1 \subseteq I$. □

Example 3.7. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra $\langle H; \oplus, ^*, 0\rangle$ in which $H = \{0, a, b, 1\}$ and $\oplus$ and * are defined as in Table 3. It is easily seen that $\{0, a\}$ is an $\mathsf{H}_v\mathsf{MV}$-ideal of H satisfying (3.1), while it is not an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal because $b, 1 \notin \{0, a\}$, but $1^* \odot b \cup b \odot 1^* = \{0, b, 1\} \not\subseteq \{0, a\}$. This example shows that the converse of Theorem 3.6 is not true in general.

$\oplus$	0	a	b	1
0	$\{0\}$	$\{a\}$	$\{b\}$	$\{1\}$
a	$\{a\}$	$\{0, a\}$	$\{0, b, 1\}$	$\{0, 1\}$
b	$\{b\}$	$\{0, 1\}$	$\{b\}$	$\{0, 1\}$
1	$\{0, 1\}$	$\{a, 1\}$	$\{0, b, 1\}$	$\{0, 1\}$
$*$	1	b	a	0

Table 3: Cayley table of Example 3.7

Theorem 3.8. *An $\mathsf{H}_v\mathsf{MV}$-algebra with $2n + 1$ elements, where n is a positive integer, does not contain any obstinate $\mathsf{H}_v\mathsf{MV}$-ideal.*

Proof. Let H be an $\mathsf{H}_v\mathsf{MV}$-algebra with $2n+1$ elements, where $n \geqslant 1$ is a positive integer, and let I be an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal of H (by contrary). Then there exists $x \in H$ such that $x^* = x$. On the other hand, by Theorem 3.6 we must have $x^* = x \in I$. Hence $0^* \in x^* \oplus x \subseteq I$, which a contradiction. Therefore, H can not contain any obstinate $\mathsf{H}_v\mathsf{MV}$-ideal. □

Theorem 3.9. *In an $\mathsf{H}_v\mathsf{MV}$-algebra, every obstinate $\mathsf{H}_v\mathsf{MV}$-ideal, if exists, is maximal.*

Proof. Let I be an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal of H and J be an $\mathsf{H}_v\mathsf{MV}$-ideal of H such that properly contains I. Let $a \in J \setminus I$. By Theorem 3.6, $a^* \in I \subset J$. Hence $1 \in a \oplus a^* \subseteq J$, whence $J = H$. Therefore I is a maximal $\mathsf{H}_v\mathsf{MV}$-ideal of H. □

Theorem 3.10. (Extension Theorem) *Let I and J be $\mathsf{H}_v\mathsf{MV}$-ideals of H such that $I \subseteq J$. If I is an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal, J is also an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal.*

Proof. Assume that $x, y \notin J$, for $x, y \in H$. Then $x, y \notin I$ and so $x^* \odot y \cup y \odot x^* \subseteq I \subseteq J$. Similarly, $y^* \odot x \cup x \odot y^* \subseteq J$, proving J is an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal of H. □

Example 3.11 shows that the converse of Theorem 3.9 does not hold in general.

Example 3.11. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra $\langle H, \oplus, ^*, 0\rangle$, where $H = \{0, a, b, c, 1\}$ and $\oplus$ and * are defined as in Table 4. It is easy to verify that the only proper $\mathsf{H}_v\mathsf{MV}$-ideals of H are $\{0\}$ and $\{0, a\}$. Hence $\{0, a\}$ is a maximal $\mathsf{H}_v\mathsf{MV}$-ideal of H, while it is not obstinate because $b, c \in H \setminus \{0, a\}$ and $b^* \odot c \cup c \odot b^* = H \not\subseteq \{0, a\}$.

$\oplus$	0	a	b	c	1
0	$\{0\}$	$\{a\}$	$\{b\}$	$\{c\}$	$\{1\}$
a	$\{a\}$	$\{0, a\}$	$\{b, 1\}$	$\{0, a, c\}$	$\{1\}$
b	$\{b\}$	$\{b, 1\}$	$\{b, 1\}$	H	$\{1\}$
c	$\{c\}$	$\{0, a, c\}$	$H \setminus \{1\}$	$\{c, 1\}$	$\{1\}$
1	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$
$*$	1	b	a	c	0

Table 4: Cayley table of Example 3.11

Example 3.12. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra $\langle H, \oplus, ^*, 0\rangle$, where $H = \{0, a, b, 1\}$ and $\oplus$ and * are defined as in Table 5. Routine calculations show that $\{0, a\}$ and $\{0, a, b\}$ are obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideals of H. This example shows that Theorem 3.9 does not hold for obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideals, in general.

$\oplus$	0	a	b	1
0	$\{0\}$	$\{a\}$	$\{a, b\}$	H
a	$\{a\}$	$\{a, 1\}$	$\{a, b\}$	H
b	$\{0, b\}$	$\{0, a, b\}$	H	$\{1\}$
1	H	$\{0, a, 1\}$	$\{0, a, 1\}$	$\{b, 1\}$
$*$	1	a	b	0

Table 5: Cayley table of Example 3.12

Theorem 3.13. *Let $H = \{0, a, 1\}$ be an $\mathsf{H}_v\mathsf{MV}$-algebra.*

(i) *If $|a \oplus a| = 1$, H does not contain any obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal.*

(ii) *If $|a \oplus a| > 1$, $\{0, a\}$ is the maximal obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal.*

Proof. Let $H = \{0, a, 1\}$ be an $\mathsf{H}_v\mathsf{MV}$-algebra with three elements.

(i) We observe that $a^* = a$ and since $0^* \in a^* \oplus a = a \oplus a$, hence $a \oplus a = \{0^*\}$. This implies that $a \oplus a \not\preceq \{0, a\}$. Hence $\{0, a\}$ can not be a weak $\mathsf{H}_v\mathsf{MV}$-ideal and so is not an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal.

(ii) We assume that $|a \oplus a| > 1$. Then

$$\{0, 1\} \subseteq a \oplus a \text{ or } \{a, 1\} \subseteq a \oplus a \text{ or both.} \tag{3.2}$$

We prove that $I = \{0, a\}$ is a maximal obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. From ($\mathsf{H}_v\mathsf{MV}7$) it follows that $0 \oplus 0 \preceq I$, $0 \oplus a \preceq I$ and $a \oplus 0 \preceq I$ and from (3.2) it follows that $a \oplus a \preceq I$. Obviously, I satisfies (I_0). Thus I is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. Now, from $1 \notin I$ and that $0 \in 1^* \odot 1 \cup 1 \odot 1^*$ it follows that $1^* \odot 1 \cup 1 \odot 1^* \preceq I$. Hence I is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal. It is obvious that I is maximal. □

Remark 3.14. We mention that the intersection of two $\mathsf{H}_v\mathsf{MV}$-ideals is again an $\mathsf{H}_v\mathsf{MV}$-ideal (see [1, Theorem 4.14]), while it is not true for obstinate $\mathsf{H}_v\mathsf{MV}$-ideals. To see this consider Example 3.4. It is easy to check that $\{0, a\}$ and $\{0, b\}$ are obstinate $\mathsf{H}_v\mathsf{MV}$-ideals of H, while their intersection, $\{0\}$, is not an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal because $a, b \in H \setminus \{0\}$ but $a \odot b^* \cup b^* \odot a = \{a\} \not\subseteq \{0\}$.

On the other hand, the union of two $\mathsf{H}_v\mathsf{MV}$-ideals may not be an $\mathsf{H}_v\mathsf{MV}$-ideal, in general (see Example 3.7 in which $\{0, a\}$ and $\{0, b\}$ are $\mathsf{H}_v\mathsf{MV}$-ideals of H but the union, $\{0, a, b\}$, is not an $\mathsf{H}_v\mathsf{MV}$-ideal because $a \oplus b = \{0, b, 1\} \not\subseteq \{0, a, b\}$). If this is true it is easily proved that the union of two obstinate $\mathsf{H}_v\mathsf{MV}$-ideals is again an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal. Indeed we have

Theorem 3.15. *Assume that A is a nonempty family of obstinate $\mathsf{H}_v\mathsf{MV}$-ideals of H such that $\cup A$ is closed with respect to '$\oplus$'. If each member of A is an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal, $\cup A$ is again an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal of H.*

Proof. The proof is routine. We only observe that if $\cup A$ is closed with respect to $\oplus$, $\cup A$ satisfies Definition 2.3(1). □

Corollary 3.16. *If $\mathbf{Id}(H)$ is closed with respect to the union, then $\mathbf{OId}(H)$, the set of all obstinate $\mathsf{H}_v\mathsf{MV}$-ideals of H, is an upper semilattice with respect to set inclusion as the partial ordering.*

In the sequel, we give several characterizations of obstinate week $\mathsf{H}_v\mathsf{MV}$-ideals.

Definition 3.17. We say that an $\mathsf{H}_v\mathsf{MV}$-algebra H satisfies the condition (AP) if for all $n \in \mathbb{N}$ and for all $x, y_1, y_2, \ldots, y_n \in H$ we have

$$x \preceq (\cdots (x \oplus y_1) \oplus \cdots) \oplus y_n \text{ and } x \preceq (\cdots (y_1 \oplus y_2) \oplus \cdots \oplus y_n) \oplus x$$

Remark 3.18. We observe that if H satisfies (AP), then $x \preceq x \oplus y$ and $x \preceq y \oplus x$, for all $x, y \in H$ and so $x \odot y \preceq x$ and $x \odot y \preceq y$, by Proposition 2.2(2).

Example 3.19. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra $\langle H; \oplus, ^*, 0\rangle$, where $H = \{0, a, 1\}$ and $\oplus$ and * are defined as given in Table 6.

$\oplus$	0	a	1
0	$\{0, a\}$	$\{0, a\}$	$\{1\}$
a	$\{0, a\}$	$\{0, a, 1\}$	$\{1\}$
1	$\{1\}$	$\{a, 1\}$	$\{0, 1\}$
$*$	1	a	0

Table 6: Cayley table of Example 3.19

It is easy to verify that H satisfies (AP). This example shows that those $\mathsf{H_vMV}$-algebras satisfying (AP) do exist.

Theorem 3.20. *Every $\mathsf{H_vMV}$-algebra with three elements satisfies (AP).*

Proof. It follows from ($\mathsf{H_vMV5}$)-($\mathsf{H_vMV7}$) and Proposition 2.2(1). □

Definition 3.21. An element $a \in H$ is said to be a *scalar* if $|x \oplus a| = |a \oplus x| = 1$, where the vertical lines means the cardinality.

Theorem 3.22. *Let I be a nonempty subset of H.*

(i) *Assume that H satisfies (AP). If I is a proper weak $\mathsf{H_vMV}$-ideal satisfying* (3.1)*, then it is an obstinate weak $\mathsf{H_vMV}$-ideal.*

(ii) *If 0 is a scalar, every obstinate weak $\mathsf{H_vMV}$-ideal satisfies* (3.1).

Proof. (i) We assume that H satisfies (AP) and I is a proper weak $\mathsf{H_vMV}$-ideal of H satisfying (3.1). For $x, y \in H \setminus I$ we have $x^*, y^* \in I$. On the other hand $x \odot y^* \preceq y^*$ and $y^* \odot x \preceq y^*$, whence $x \odot y^* \cup y^* \odot x \preceq I$. Similarly, it is proved that $x^* \odot y \cup y \odot x^* \preceq I$, completes the proof.

(ii) Assume that 0 is a scalar, I is an obstinate weak $\mathsf{H_vMV}$-ideal of H and $x \in H \setminus I$. Since $1 \notin I$, so $\{x^*\} = x^* \odot 1 \cup 1 \odot x^* \preceq I$, whence $x^* \in I$. □

The next corollary is immediately follows.

Corollary 3.23. *In an $\mathsf{H_vMV}$-algebra satisfying (AP) and in which 0 is a scalar, a proper weak $\mathsf{H_vMV}$-ideal is obstinate if and only if it satisfies* (3.1).

Example 3.24. Consider the $\mathsf{H_vMV}$-algebra $\langle H; \oplus, ^*, 0\rangle$ with $H = \{0, a, b, c, d, 1\}$ and $\oplus$ and * are defined as in Table 7.

$\oplus$	0	a	b	c	d	1
0	$\{0, a, c\}$	$\{a\}$	$\{b\}$	$\{c\}$	$\{d\}$	$\{1\}$
a	$\{a\}$	$\{0, a\}$	H	$\{0, a, c\}$	$H \setminus \{1\}$	H
b	$\{b\}$	H	$H \setminus \{1\}$	$\{0, a, c\}$	$H \setminus \{1\}$	H
c	$\{c\}$	$\{0, a, c\}$	$\{0, a, c\}$	$H \setminus \{1\}$	$\{1\}$	H
d	$\{d\}$	$H \setminus \{1\}$	$H \setminus \{1\}$	$\{1\}$	$H \setminus \{1\}$	H
1	H	H	H	H	H	H
$*$	1	b	a	d	c	0

Table 7: Cayley table of Example 3.24

Then H does not satisfy (AP) because $b \not\preceq \{0, a, c\} = b \oplus c$. Moreover, $\{0, a, c\}$ is a weak $\mathsf{H_vMV}$-ideal satisfying (3.1), while it is not an obstinate weak $\mathsf{H_vMV}$-ideal because $b, d \notin \{0, a, c\}$ but $b^* \odot d \cup d \odot b^* = \{1, b, d\} \not\preceq \{0, a, c\}$. This example shows that the condition (AP) is necessary in Theorem 3.22(i).

Example 3.25. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra $\langle H; \oplus, ^*, 0\rangle$ in which $H = \{0, a, b, c, 1\}$ and $\oplus$ and * are defined as in Table 8. Routine calculations show that H satisfies (AP). Moreover, $\{0, a\}$ is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H, which does not satisfy (3.1) because $c = c^* \notin \{0, a\}$. This example shows that the converse of Theorem 3.22(i) may not be true in general.

$\oplus$	0	a	b	c	1
0	$\{0\}$	$\{a\}$	$\{b\}$	$\{c\}$	H
a	$\{a\}$	$\{0,a,b,c\}$	H	$\{0,a,b,c\}$	H
b	$\{0,a,b,c\}$	H	$\{0,a,b,c\}$	$\{0,a,b,c\}$	H
c	$\{0,a,b,c\}$	$\{0,a,b,c\}$	$\{0,a,b,c\}$	$\{1\}$	H
1	H	H	H	$\{0,a,c,1\}$	$\{0,b,1\}$
$*$	1	b	a	c	0

Table 8: Cayley table of Example 3.25

Example 3.26. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra $\langle H; \oplus, ^*, 0\rangle$ in which $H = \{0, a, b, 1\}$ and $\oplus$ and * are defined as in Table 9. Obviously, 0 is not a scalar. Moreover, $\{0, a\}$ is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H, which does not satisfy (3.1) because $b = b^* \notin \{0, a\}$. This example shows that if 0 is not a scalar, Theorem 3.22(ii) may not be true.

$\oplus$	0	a	b	1
0	$\{0\}$	$\{a\}$	$\{a,b\}$	H
a	$\{a\}$	$\{a,1\}$	$\{b\}$	H
b	$\{0,b\}$	$\{0,a,b\}$	H	$\{1\}$
1	H	$\{0,a,1\}$	$\{a,1\}$	H
$*$	1	a	b	0

Table 9: Cayley table of Example 3.26

Example 3.27. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra H given in Example 3.12. It is not difficult to check that H satisfies (AP) and $\{0, b\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H, which is not an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal because $a, 1 \notin \{0, b\}$, while $a^* \odot 1 \cup 1 \odot a^* = \{a\} \not\preceq \{0, b\}$. We observe that $a, a^* \notin \{0, b\}$. This example shows that the condition (3.1) is necessary in Theorem 3.22(i).

Lemma 3.28. *For $a \in H \setminus \{0\}$, if $H \setminus \{a, 1\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H satisfying* (3.1)*, it is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal, too.*

Proof. Let $I = H \setminus \{a, 1\}$ (with $a \neq 0$) be a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H which satisfies (3.1). Now, we prove that I satisfies (WOI), for $x, y \in \{a, 1\}$. If $a = 1$, from $0 \in 1^* \odot 1 \cup 1 \odot 1^*$, the proof is complete. Assume that $a \neq 1$. Again from $0 \in 1^* \odot 1 \cup 1 \odot 1^*$ and that $0 \in a^* \odot a \cup a \odot a^*$ and $0 \in 1^* \odot a \cup a \odot 1^*$ it follows that $1^* \odot 1 \cup 1 \odot 1^* \preceq I$, $a^* \odot a \cup a \odot a^* \preceq I$ and $1^* \odot a \cup a \odot 1^* \preceq I$. Also, since $a^* \in a^* \odot 1 \cup 1 \odot a^*$ and $a^* \in I$, so $a^* \odot 1 \cup 1 \odot a^* \preceq I$, completes the proof. □

Now, we give more general case than Lemma 3.28.

Lemma 3.29. *Let $n \geqslant 2$ be a positive integer and $a_1, a_2, \ldots, a_n, a_{n+1} = 1 \in H$ be such that*

$$(\exists k \in \{1, 2, \ldots, n, n+1\})\ a_k^* \in a_i^* \odot a_j \cup a_j \odot a_i^*,\ \forall i, j \in \{1, 2, \ldots, n, n+1\}. \quad (3.3)$$

If $H \setminus \{a_1, a_2, \ldots, a_n, 1\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H satisfying (3.1)*, it is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal, too.*

Proof. Let $I = H \setminus \{a_1, a_2, \ldots, a_n, a_{n+1} = 1\}$ be a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. We know that $0 \in 1^* \odot a_i \cup a_i \odot 1^*$ and $0 \in a_i^* \odot a_i \cup a_i \odot a_i^*$, whence $1^* \odot a_i \cup a_i \odot 1^* \preceq I$ and $a_i^* \odot a_i \cup a_i \odot a_i^* \preceq I$, for all $i \in \{1, 2, \ldots, n+1\}$. From (3.1) it follows that $a_i^* \in I$, for all $i \in \{1, 2, \ldots, n+1\}$, whence combining $a_i^* \in 1 \odot a_i^* \cup a_i^* \odot 1$ we get $1 \odot a_i^* \cup a_i^* \odot 1 \preceq I$. Moreover, from (3.3) and that $a_k^* \in I$ for $k \in \{1, 2, \ldots, n+1\}$, it follows that $a_i^* \odot a_j \cup a_j \odot a_i^* \preceq I$, completes the proof. □

Example 3.30. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra $\langle H; \oplus, ^*, 0\rangle$ in which $H = \{0, a, b, c, 1\}$ and $\oplus$ and * are defined as in Table 10.

$\oplus$	0	a	b	c	1
0	$\{0\}$	$\{a\}$	$\{b\}$	$\{c\}$	$\{1\}$
a	$\{a\}$	$\{0, a, b, c\}$	H	$\{0, a, b, c\}$	H
b	$\{b\}$	H	$\{0, a, b, c\}$	$\{0, a, b, c\}$	H
c	$\{c\}$	$\{0, a, b, c\}$	$\{0, a, b, c\}$	H	H
1	$\{1\}$	H	H	$\{0, a, 1\}$	$\{0, a, b, 1\}$
$*$	1	b	a	c	0

Table 10: Cayley table of Example 3.30

(i) It is obvious that $H \setminus \{b, 1\} = \{0, a, c\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H satisfying (3.1). This example shows that those weak $\mathsf{H}_v\mathsf{MV}$-ideals satisfying the conditions of Lemma 3.28 do exist.

(ii) It is not difficult to check that $I = \{0, a, b\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H but it is not an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal because $c, 1 \notin I$, while $c^* \odot 1 \cup 1 \odot c^* = \{c\} \not\preceq I$. Also, obviously $\{0, a, b\}$ does not satisfy (3.1). Hence the condition (3.1) is necessary in Lemma 3.28.

(iii) Routine calculations show that $J = \{0, a\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H, which is not an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal because $c, 1 \notin J$, while $c^* \odot 1 \cup 1 \odot c^* = \{c\} \not\preceq J$. We observe that J satisfies (3.3) but does not satisfy (3.1) because $c = c^* \notin \{0, a\}$. This example shows that the condition (3.1) is necessary in Lemma 3.29.

Theorem 3.31. *Let H be an $\mathsf{H}_v\mathsf{MV}$-algebra with $|H| < 6$. Then every proper weak $\mathsf{H}_v\mathsf{MV}$-ideal of H satisfying (3.1) is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal.*

Proof. Assume that H is an $\mathsf{H}_v\mathsf{MV}$-algebra with at most five elements. We consider the following cases.

Case 1: $|H| = 2$ or 3. If $H = \{0, 1\}$ or $H = \{0, a, 1\}$, then the only possible proper weak $\mathsf{H}_v\mathsf{MV}$-ideals of H satisfying (3.1) are $\{0\}$ and $\{0, a\}$, whence by Lemma 3.28, they are obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideals.

Case 2: Assume that $H = \{0, a, b, 1\}$ with four elements. If $a^* = a$ and $b^* = b$, the only possible proper weak $\mathsf{H}_v\mathsf{MV}$-ideal of H satisfying (3.1) is $\{0, a, b\}$, whence by Lemma 3.28, it follows that it is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal. If $a^* = b$ (whence $b^* = a$), the only possible proper weak $\mathsf{H}_v\mathsf{MV}$-ideals satisfying (3.1) are $\{0, a\}$ and $\{0, b\}$, whence by Lemma 3.28 it follows that they are obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideals of H.

Case 3: Assume that $H = \{0, a, b, c, 1\}$ with five elements. We first assume that $a^* = a$, $b^* = b$ and $c^* = c$. Then the only possible proper weak $\mathsf{H}_v\mathsf{MV}$-ideal of H satisfying (3.1) is $\{0, a, b, c\}$, whence by Lemma 3.28 it follows that it is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal. Let $a^* = b$, $b^* = a$ and $c^* = c$. Then $\{0, a, c\}$ and $\{0, b, c\}$ can be the only proper weak $\mathsf{H}_v\mathsf{MV}$-ideals of H satisfying (3.1), whence by Lemma 3.28 it follows that they are obstinate $\mathsf{H}_v\mathsf{MV}$-ideals. □

Now, we give some conditions under which those weak $\mathsf{H}_v\mathsf{MV}$-ideals mentioned in Lemma 3.28 there exist.

Theorem 3.32. *Let H be an $\mathsf{H}_v\mathsf{MV}$-algebra. Then $H \setminus \{1\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal if and only if*

$$(\forall x, y \in H \setminus \{1\}) \quad x \oplus y \neq \{1\}. \tag{3.4}$$

Proof. Assume that $I = H \setminus \{1\}$ satisfies (3.4) and let $x \preceq y$ and $y \in I$, for some $x, y \in I$. It is clear that $x \neq 1$, whence $x \in I$. Now, let $x, y \in I$. Since $x \oplus y \neq \{1\}$, so there exists $a \in x \oplus y$ such that $a \neq 1$. This implies that $a \in I$. Hence $x \oplus y \preceq I$, proving I is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H.

The converse is obvious. □

Corollary 3.33. *In an $\mathsf{H}_v\mathsf{MV}$-algebra H, $H \setminus \{1\}$ is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal if and only if $x \oplus y \neq \{1\}$, for all $x, y \in H \setminus \{1\}$.*

Proof. Assume that $x \oplus y \neq \{1\}$, for all $x, y \in H \setminus \{1\}$. We must prove that $0 \odot 1 \cup 1 \odot 0 \preceq I$. But this follows from the fact that $0 \in 0 \odot 1 \cup 1 \odot 0$. Considering Theorem 3.32, we conclude that $H \setminus \{1\}$ is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. The converse follows from Theorem 3.32 and the fact that any obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal is a weak $\mathsf{H}_v\mathsf{MV}$-ideal. □

Example 3.34. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra H given in Example 3.30. It is easy to check that $H \setminus \{1\} = \{0, a, b, c\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal satisfying (3.4). This example shows that those weak $\mathsf{H}_v\mathsf{MV}$-ideals satisfying the conditions of Theorem 3.32 do exist.

Example 3.35. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra H given in Example 3.4. Then $H \setminus \{1\} = \{0, a, b\}$ is not a weak $\mathsf{H}_v\mathsf{MV}$-ideal because $a \oplus b = \{1\} \not\preceq H \setminus \{1\}$. This example shows that the condition (3.4) is necessary in Theorem 3.32.

Definition 3.36. An element $a \in H$ is called a *coatom* if there is not any element $b \in H \setminus \{1\}$ such that $a \prec b$.

Theorem 3.37. *Let $a \in H$ be a coatom. Then $H \setminus \{a, 1\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H if and only if*

$$(\forall x, y \in H \setminus \{a, 1\}) \quad x \oplus y \not\subseteq \{a, 1\}. \tag{3.5}$$

Proof. Assume that (3.5) holds and let $I = H \setminus \{a, 1\}$. Also, let $x \preceq y$ and $y \in I$, for $x, y \in H$. Since $y \notin \{a, 1\}$ and a and 1 are coatoms, then $x \notin \{a, 1\}$, whence $x \in I$. Now, let $x, y \in I$. By hypothesis, there exists $z \in x \oplus y$ such that $z \notin \{a, 1\}$, whence $z \in I$. Hence $x \oplus y \preceq I$.

The converse follows from the fact that a and 1 are coatoms. □

Corollary 3.38. *Assume that $a \in H$ is a coatom with $a^* \neq a$. If $H \setminus \{a, 1\}$ satisfies* (3.1) *and* (3.5)*, then it is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H.*

Proof. It follows from Lemma 3.28 and Theorem 3.37. □

Example 3.39. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra H given in Example 3.11.

(i) Obviously, c is a coatom with $c^* = c$. Moreover, $\{0, a, b\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H, which is not obstinate because $c^* \odot 1 \cup 1 \odot c^* = \{c\} \not\preceq \{0, a, b\}$. Hence the condition '$a^* \neq a$, for all coatoms a' is necessary in Corollary 3.38.

(ii) Obviously, b is also a coatom with $b^* = a \neq b$. It is easily checked that $H \setminus \{b, 1\} = \{0, a, c\}$ satisfies (3.1) and (3.5). Hence it is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H.

Theorem 3.40. *Assume that $a_1, \ldots, a_n$ be coatoms of H. Then $H \setminus \{a_1, \ldots, a_n, 1\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H if and only if*

$$(\forall x, y \in H \setminus \{a_1, \ldots, a_n, 1\}) \quad x \oplus y \not\subseteq \{a_1, \ldots, a_n, 1\}. \tag{3.6}$$

Proof. It is similar to the proof of Theorem 3.37. □

Corollary 3.41. *Let $a_1, \ldots, a_n$ be coatoms of H which satisfy the conditions of Lemma* 3.29*. If $H \setminus \{a_1, \ldots, a_n, 1\}$ satisfies* (3.1) *and* (3.6)*, then it is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal.*

Proof. It follows from Lemma 3.29 and Theorem 3.40. □

Example 3.42. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra H given in Example 3.25. It is easy to check that a, b and c are coatoms of H. Moreover, $H \setminus \{b, c, 1\} = \{0, a\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H and (3.6) satisfied. This example shows that those weak $\mathsf{H}_v\mathsf{MV}$-ideals satisfying (3.6) do exist.

4. Boolean, prime and obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideals

In this section, the notions of Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideals and prime weak $\mathsf{H}_v\mathsf{MV}$-ideals are introduced and the relationships between them and obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideals are investigated.

Definition 4.1. Let I be a proper weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. I is called a

(i) *prime* weak $\mathsf{H}_v\mathsf{MV}$-ideal if $x \wedge y \preceq I$ implies that $x \in I$ or $y \in I$, for all $x, y \in H$,

(ii) *Boolean* weak $\mathsf{H}_v\mathsf{MV}$-ideal if $x \wedge x^* \cup x^* \wedge x \preceq I$, for all $x, y \in H$.

Example 4.2. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra $\langle H; \oplus, ^*, 0\rangle$ in which $\oplus$ and * are defined as in Table 11. It is not difficult to check that $\{0, a, b, c\}$ is prime weak $\mathsf{H}_v\mathsf{MV}$-ideal of H but it is not a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal because $a \wedge b \cup b \wedge a = \{1\} \not\preceq \{0, a, b, c\}$.

$\oplus$	0	a	b	c	1
0	$\{0\}$	$\{a\}$	$\{b\}$	$\{c\}$	$\{1\}$
a	$\{a\}$	$\{c\}$	H	$\{0, a, b, c\}$	H
b	$\{b\}$	H	$\{c\}$	$\{0, a, b, c\}$	H
c	$\{c\}$	$\{0\}$	$\{0\}$	H	H
1	$\{1\}$	H	H	$\{0, a, c, 1\}$	$\{0, a, c, 1\}$
$*$	1	b	a	c	0

Table 11: Cayley table of Example 4.2

Example 4.3. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra $\langle H; \oplus, ^*, 0\rangle$, where $H = \{0, a, b, 1\}$ and $\oplus$ and * are defined as in Table 12. It is not difficult to check that $I = \{0, b\}$ is a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal of H, while it is not a prime weak $\mathsf{H}_v\mathsf{MV}$-ideal because $a \wedge a = H \preceq I$ but $a \notin I$.

$\oplus$	0	a	b	1
0	$\{0\}$	$\{0, a\}$	$\{0, a, b\}$	$\{0, a, b, 1\}$
a	$\{0, a\}$	$\{0, a\}$	$\{0, a, b, 1\}$	$\{0, a, b, 1\}$
b	$\{0, a, b\}$	$\{0, a, b, 1\}$	$\{0, a, b\}$	$\{0, a, b, 1\}$
1	$\{0, 1\}$	$\{a, 1\}$	$\{b, 1\}$	$\{a, b, 1\}$
$*$	1	b	a	0

Table 12: Cayley table of Example 4.3

Theorem 4.4. *Let H be an $\mathsf{H}_v\mathsf{MV}$-algebra with the property (AP) and assume that 0 is a scalar. Then every obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H is a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal.*

Proof. Let I be an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. By Theorem 3.22(ii), we have $x \in I$ or $x^* \in I$, for all $x \in H$. On the other hand, since H satisfies (AP), so $x \wedge x^* \preceq x^*$ and $x^* \wedge x \preceq x$, whence $x \wedge x^* \cup x^* \wedge x \preceq I$. Hence I is a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. □

Example 4.5. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra H given in Example 4.2. Obviously, 0 is a scalar. Also, H does not satisfy (AP) because $a \not\preceq \{c\} = a \oplus a$. It is not difficult to check that $\{0, a, b\}$ is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H but it is not a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal because $a \wedge b = \{1\} \not\preceq \{0, a, b\}$. This example shows that the condition (AP) is necessary in Theorem 4.4.

Example 4.6. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra H given in Example 3.25. Obviously, 0 is not a scalar. Routine calculations show that H satisfies (AP). Moreover, $\{0, b\}$ is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H but it is not a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal because $c \wedge c = \{c\} \not\preceq \{0, b\}$. This example shows that if 0 is not a scalar, Theorem 4.4 may not be true in general.

Example 4.7. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra H given in Example 3.30. Obviously, 0 is a scalar. Also, it is not difficult to check that H satisfies (AP). Moreover $\{0, a, b\}$ is a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal of H but it is not an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal because $c, 1 \notin \{0, a, b\}$, while $c^* \odot 1 \cup 1 \odot c^* = \{c\} \not\preceq \{0, a, b\}$. This example shows that the converse of Theorem 4.4 does not true in general.

Theorem 4.8. *In an $\mathsf{H}_v\mathsf{MV}$-algebra with the property (AP), every proper weak $\mathsf{H}_v\mathsf{MV}$-ideal which is both Boolean and prime is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal.*

Proof. Let H be an $\mathsf{H}_v\mathsf{MV}$-algebra with the property (AP) and let I be a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal and a prime weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. Then $x \wedge x^* \cup x^* \wedge x \preceq I$, for all $x \in H$. This implies that $x \wedge x^* \preceq I$ or $x^* \wedge x \preceq I$, for all $x \in H$. In any case, we get $x \in I$ or $x^* \in I$. Now, by Theorem 3.22(i) the proof is complete. □

Example 4.9. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra $\langle H; \oplus, ^*, 0\rangle$, where $H = \{0, a, b, 1\}$ and $\oplus$ and * are defined as given in Table 13. It is not difficult to check that H satisfies (AP). Also, $I = \{0, a\}$ is a prime weak $\mathsf{H}_v\mathsf{MV}$-ideal of H, while it is neither a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal nor an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal because $b \wedge b^* = b^* \wedge b = \{b\} \not\preceq I$ and $b, 1 \notin I$, while $b^* \odot 1 \cup 1 \odot b^* = \{b\} \not\preceq I$, respectively. This example shows that the condition 'Boolean' is necessary in Theorem 4.8.

$\oplus$	0	a	b	1
0	$\{0\}$	$\{0, a, b\}$	$\{b\}$	H
a	$\{a\}$	H	$\{a, b\}$	H
b	$\{b\}$	$\{a, b\}$	$\{1\}$	$\{1\}$
1	$\{b, 1\}$	$\{0, 1\}$	$\{1\}$	$\{a, b, 1\}$
$*$	1	a	b	0

Table 13: Cayley table of Example 4.9

Example 4.10. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra H given in Example 3.30. It is easily seen that H satisfies (AP). Also, it is not difficult to check that $\{0, b\}$ is a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal, while it is neither an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal nor a prime weak $\mathsf{H}_v\mathsf{MV}$-ideal because $c, 1 \notin \{0, b\}$ but $c^* \odot 1 \cup 1 \odot c^* = \{c\} \not\preceq \{0, b\}$ and $a \wedge c = H \preceq \{0, b\}$, while $a, c \notin \{0, b\}$. This example shows that the condition 'prime' is necessary in Theorem 4.8.

Example 4.11. Consider Example 3.3. Routine calculations show that H satisfies (AP). Moreover, $I = \{0, a\}$ is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H but it is not a prime weak $\mathsf{H}_v\mathsf{MV}$-ideal because $1 \wedge b = \{0, a, b, 1\} \preceq I$, while $b, 1 \notin I$. Also, it is not a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal because $b \wedge b = \{a, b\} \preceq I$, while $b \notin I$. Hence the converse of Theorem 4.8 is not true in general.

In $\mathsf{H}_v\mathsf{MV}$-algebras with at most five elements we have more strong result:

Theorem 4.12. *In any $\mathsf{H}_v\mathsf{MV}$-algebra H with $|H| < 6$, every proper weak $\mathsf{H}_v\mathsf{MV}$-ideal which is both Boolean and prime is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal.*

Proof. It is obvious that every proper weak $\mathsf{H}_v\mathsf{MV}$-ideal which is both Boolean and prime satisfies (3.1). The remains follows from Theorem 3.31. □

Theorem 4.13. *Let $H = \{0, a, 1\}$ be an $\mathsf{H}_v\mathsf{MV}$-algebra satisfying*

$$a \in a \oplus a \quad or \quad 0 \in a \oplus a. \tag{4.7}$$

Then $\{0, a\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H.

Proof. Let $I = \{0, a\}$. Obviously, (I_0) is satisfied. From $0 \in 0 \oplus 0$ and $a \in a \oplus 0 \cap 0 \oplus a$ it follows that $0 \oplus 0 \preceq I$, $a \oplus 0 \preceq I$ and $0 \oplus a \preceq I$. Under condition (4.7) it is obvious that $a \oplus a \preceq I$, as well. Hence I is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. □

Theorem 4.14. *Let $H = \{0, a, 1\}$ be an $\mathsf{H}_v\mathsf{MV}$-algebra satisfying* (4.7). *Then $\{0\}$ and $\{0, a\}$ are Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideals of H.*

Proof. We know that $\{0\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal, in any $\mathsf{H}_v\mathsf{MV}$-algebra. From Proposition 2.2(10), it follows that $1 \wedge 1^* \cup 1^* \wedge 1 \preceq \{0\}$. If $a \in a \oplus a$, then $0 \in (a^* \oplus a)^* \subseteq ((a \oplus a)^* \oplus a)^* = a \wedge a$, whence $a^* \wedge a = a \wedge a \preceq \{0\}$. Similarly, if $0 \in a \oplus a$, then $0 \in (0^* \oplus a)^* \subseteq ((a \oplus a)^* \oplus a)^* = a \wedge a = a^* \wedge a$. Hence $a^* \wedge a \preceq \{0\}$. Thus, $\{0\}$ is a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal of H.

Now, from $0^* \in a^* \oplus a = a \oplus a$ it follows that $a \in 0 \oplus a \subseteq (a \oplus a)^* \oplus a$, whence $a = a^* \in ((a \oplus a)^* \oplus a)^* = a^* \wedge a$. Hence $a^* \wedge a \preceq I$. Therefore I is a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. □

Lemma 4.15. *In an $\mathsf{H}_v\mathsf{MV}$-algebra, every two distinct elements a, b with $a^* = a$ and $b^* = b$ are incomparable.*

Proof. Let a, b be two distinct elements of H. Then

$$a \preceq b \;\Leftrightarrow\; 0^* \in a^* \oplus b \cap b \oplus a^* = a \oplus b \cap b \oplus a = a \oplus b^* \cap b^* \oplus a \;\Leftrightarrow\; b \preceq a,$$

which is a contradiction. □

Lemma 4.16. *In any $\mathsf{H}_v\mathsf{MV}$-algebra H, for every $x \in H$ the following hold:*

(i) *if $x^* = x$, then $x \in x \wedge x$,*

(ii) *if* $x \in x \oplus x$ *or* $0 \in x \oplus x$, *then* $0 \in x \wedge x^*$,

(iii) *if* $x^* \in x \oplus x$, *then* $x \in x \wedge x^*$,

(iv) *if* $0^* \in x \oplus x$, *then* $x^* \in x \wedge x^*$,

Proof. (i) Assume that $x^* = x$, for $x \in H$. From $0^* \in x^* \oplus x$ and $x \in 0 \oplus x$ it follows that $x = x^* \subseteq (0 \oplus x)^* \subseteq ((x^* \oplus x)^* \oplus x)^* = x \wedge x$.

(ii) Assume that $x \in x \oplus x$. Then $0 \in x \odot x^* \subseteq (x \oplus x) \odot x^* = x \wedge x^*$. Similarly, if $0 \in x \oplus x$, then $0 \in 0 \odot x^* \subseteq (x \oplus x) \odot x^* = x \wedge x^*$.

(iii) If $x^* \in x \oplus x$, then $x \in (x \oplus x)^* \subseteq ((x \oplus x)^* \oplus x)^* = x \wedge x^*$.

(iv) If $0^* \in x \oplus x$, then $x^* \in 0^* \odot x^* \subseteq (x \oplus x) \odot x^* = x \wedge x^*$. □

Theorem 4.17. *Let* $H = \{0, a, b, 1\}$ *be an* $\mathsf{H}_v\mathsf{MV}$*-algebra.*

(i) *If* $a^* = a$ *and* $b^* = b$, $\{0, a\}$ *and* $\{0, b\}$ *can not be simultaneously a prime weak* $\mathsf{H}_v\mathsf{MV}$*-ideal and an obstinate weak* $\mathsf{H}_v\mathsf{MV}$*-ideal.*

(ii) *Let* $a^* = b$. *Then* $\{0, a\}$ *and* $\{0, b\}$*) are weak* $\mathsf{H}_v\mathsf{MV}$*-ideals of* H *if and only if they are Boolean weak* $\mathsf{H}_v\mathsf{MV}$*-ideals of* H.

(iii) $\{0, a, b\}$ *is a weak* $\mathsf{H}_v\mathsf{MV}$*-ideal of* H *if and only if it is a Boolean weak* $\mathsf{H}_v\mathsf{MV}$*-ideal.*

Proof. (i) By contrary, we assume that $I = \{0, a\}$ is a prime weak $\mathsf{H}_v\mathsf{MV}$-ideal and an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. From $b, 1 \notin I$ it follows that $(b \oplus 0)^* \cup (0 \oplus b)^* = b^* \odot 1 \cup 1 \odot b^* \preceq I$, whence $(b \oplus 0)^* \preceq I$ or $(0 \oplus b)^* \preceq I$. Considering Lemma 4.15, it follows that $a \in b \oplus 0$ or $0^* \in b \oplus 0$ or $a \in 0 \oplus b$ or $0^* \in 0 \oplus b$. From the two first cases it follows that $b \wedge b \preceq I$ and from the two second cases it follows that $b \wedge 1 \preceq I$. This contradicts the hypothesis that I is a prime weak $\mathsf{H}_v\mathsf{MV}$-ideal of H.

Similarly, it is proved that $\{0, b\}$ can not be simultaneously a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal and an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal.

(ii) Assume that $a^* = b$ (whence $b^* = a$) and $I = \{0, a\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. From $0 \in 0 \wedge 1 \cup 1 \wedge 0$ it follows that $0 \wedge 1 \cup 1 \wedge 0 \preceq I$. It remains that to show that $a \wedge b \cup b \wedge a \preceq I$. Since $a \in I$ and I is a weak $\mathsf{H}_v\mathsf{MV}$-ideal, so $a \oplus a \preceq I$, whence $0 \in a \oplus a$ or $a \in a \oplus a$, or $b \in a \oplus a$ and $b \preceq a$. In the first two cases it follows that $0 \in a \wedge b$, whence $a \wedge b \preceq I$. In the last case, we have $0^* \in b^* \oplus a = a \oplus a$ and so $0 \in (a \oplus a)^* \subseteq ((a \oplus a)^* \oplus a)^* = a \wedge b$. Hence $a \wedge b \preceq I$, proving I is a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal of H.

Similar argument shows that if $\{0, b\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal, it is also a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal.

The converse is obvious.

(iii) Assume that$I = \{0, a, b\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. Obviously, $0 \wedge 0^* \cup 0^* \wedge 0 = 1^* \wedge 1 \cup 1 \wedge 1^* \preceq I$. Now, if $a^* = a$ and $b^* = b$, from Lemma 4.16(i) it follows that $a \in a \wedge a^* \cup a^* \wedge a$ and $b \in b \wedge b^* \cup b^* \wedge b$, whence $a \wedge a^* \cup a^* \wedge a \preceq I$ and $b \wedge b^* \cup b^* \wedge b \preceq I$. Otherwise, since I is a weak $\mathsf{H}_v\mathsf{MV}$-ideal, so we must have

$a \oplus a \preceq I$ and $b \oplus b \preceq I$, whence $\{0, a, b\} \subseteq a \oplus a$ and similarly $\{0, a, b\} \subseteq b \oplus b$. If $a^* = b \in a \oplus a$, then $a \in a \wedge a$, by Lemma 4.16(iii), otherwise $0 \in a \wedge a^*$, by Lemma 4.16(ii). In any case $a \wedge a^* \preceq I$. Similarly, we can show that $b \wedge b^* \preceq I$. Hence I is a Boolean $\mathsf{H}_v\mathsf{MV}$-ideal.

The converse is obvious. □

Example 4.18. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra H given in Example 3.26. Obviously, H satisfies the conditions of Theorem 4.17(i). Also, it is easily checked that $\{0, a\}$ is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H, which is not a prime weak $\mathsf{H}_v\mathsf{MV}$-ideal because $b \wedge b = H \preceq \{0, a\}$, while $b \notin \{0, a\}$.

Example 4.19. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra H given in Example 4.9. Then $a^* = a$ and $b^* = b$ and $\{0, a\}$ is a prime weak $\mathsf{H}_v\mathsf{MV}$-ideal, while it is not an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal. This example shows that those $\mathsf{H}_v\mathsf{MV}$-algebras satisfying the conditions of Theorem 4.17 do exist.

Example 4.20. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra H given in Example 3.3. Obviously, $\{0, a\}$ and $\{0, b\}$ are weak $\mathsf{H}_v\mathsf{MV}$-ideals of H and so by Theorem 4.17 are Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideals of H.

Example 4.21. Consider the $\mathsf{H}_v\mathsf{MV}$-algebra H given in Example 3.7. Then $\{0, a, b\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H and so by Theorem 4.17, it is a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal of H.

Example 4.22. As Example 4.9 shows $\{0, a\}$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H, while it is not a Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideal. We observe that $a^* \neq a$ does not hold in H. So, this condition is necessary in Theorem 4.17(ii).

In connection with quotient $\mathsf{H}_v\mathsf{MV}$-algebras induced by obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideals we have the following result. Before, we state it we observe that an $\mathsf{H}_v\mathsf{MV}$-algebra H is said to be *commutative* if $x \oplus y = y \oplus x$, for all $x, y \in H$.

Theorem 4.23. *Assume that H is commutative and let I be an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. If there exists a regular congruence θ in H such that $0/\theta = I$, then*

(i) *H/θ is the two-elements Boolean algebra,*

(ii) *I is an $\mathsf{H}_v\mathsf{MV}$-ideal,*

(iii) *$x^* \neq x$, for all $x \in H$,*

(iv) *$|H|$ is an even positive integer.*

Proof. Let I be an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal of H and θ be a regular congruence in H such that $0/\theta = I$.

(i) Let $x, y \in H$ be such that $x/\theta, y/\theta \neq 0/\theta$. Then $x, y \notin I$, whence $x^* \odot y = y \odot x^* \preceq I$ and $y^* \odot x = x \odot y^* \preceq I$. This implies that $(x \oplus y^*)^* = x^* \odot y \cap I \neq \emptyset$ and

$(y \oplus x^*)^* = y^* \odot x \cap I \neq \emptyset$. Hence there exist $a \in x \oplus y^*$ and $b \in y \oplus x^*$ such that $a^*, b^* \in I = 0/\theta$, whence $a, b \in 0^*/\theta$. This means that $x \oplus y^* \theta \{0^*\}$ and $y \oplus x^* \theta \{0^*\}$. Since θ is regular, so $x \theta y$; i.e., $x/\theta = y/\theta$. Therefore, $H/\theta = \{0/\theta, 0^*/\theta\}$.

(ii) We observe that in an $\mathsf{H}_v\mathsf{MV}$-algebra $0^* \notin 0 \oplus 0$, otherwise we must have $0^* \preceq 0$, which is impossible. Hence in H/θ we have $I \oplus I = 0/\theta \oplus 0/\theta = \{0/\theta\}$. This implies that for every $x, y \in I$, $x \oplus y \subseteq I$, which implies that I is an $\mathsf{H}_v\mathsf{MV}$-ideal.

(iii) Assume that $x^* = x$, for some $x \in H$. Considering (i) we have $x \in 0/\theta$ or $x \in 0^*/\theta$. In the first case we have $x = x^* \theta 0^*$, whence $0 \theta 0^*$, which is a contradiction. Similarly, if $x \in 0^*/\theta$ we get $0 \theta 0^*$, which is a contradiction.

(iv) Considering (iii), the proof is obvious. □

Remark 4.24. We notice that Theorem 4.23 does not state that an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal which is the kernel of a congruence is an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal. It just states that, as a weak $\mathsf{H}_v\mathsf{MV}$-ideal, it must be an $\mathsf{H}_v\mathsf{MV}$-ideal. To see this consider the $\mathsf{H}_v\mathsf{MV}$-algebra given in Table 14. It is not difficult to check that H is a commutative $\mathsf{H}_v\mathsf{MV}$-algebra in which $I = \{0, a\}$ is an $\mathsf{H}_v\mathsf{MV}$-ideal (and so a weak $\mathsf{H}_v\mathsf{MV}$-ideal) of H which is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal, while it is not an obstinate $\mathsf{H}_v\mathsf{MV}$-ideal because $1 \notin I$ but $1^* \odot 1 = \{0, b\} \not\subseteq I$. It is not difficult to verify that the relation $\theta = \triangle_H \cup \{(0, a), (a, 0), (b, 1), (1, b)\}$ is a regular congruence in H such that $0/\theta = I$.

$\oplus$	0	a	b	1
0	$\{0\}$	$\{a\}$	$\{b\}$	$\{a, 1\}$
a	$\{a\}$	$\{0\}$	$\{1\}$	$\{b, 1\}$
b	$\{b\}$	$\{1\}$	$\{a, 1\}$	H
1	$\{a, 1\}$	$\{b, 1\}$	H	$\{0, a, 1\}$
$*$	1	a	b	0

Table 14: A commutative $\mathsf{H}_v\mathsf{MV}$-algebra

5. Conclusions

We introduced a new type of $\mathsf{H}_v\mathsf{MV}$-ideals (obstinate $\mathsf{H}_v\mathsf{MV}$-ideals and obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideals) and gave a deep characterization of them. We proved that in any $\mathsf{H}_v\mathsf{MV}$-algebra with odd number of elements there does not exist any obstinate $\mathsf{H}_v\mathsf{MV}$-ideal. Especially, in an $\mathsf{H}_v\mathsf{MV}$-algebra with at least three elements, the singleton $\{0\}$ is not an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal. Moreover, obstinate $\mathsf{H}_v\mathsf{MV}$-ideals are maximal (if exist). Next, we studied the properties of obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideals. We proved that every proper weak $\mathsf{H}_v\mathsf{MV}$-ideal satisfying suitable conditions is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal. In the sequel, we introduced the notions of prime weak $\mathsf{H}_v\mathsf{MV}$-ideals and Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideals and gave some basic properties. Furthermore, we investigated the relationships between obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideals, prime weak $\mathsf{H}_v\mathsf{MV}$-ideals and Boolean weak $\mathsf{H}_v\mathsf{MV}$-ideals. We proved that every proper weak $\mathsf{H}_v\mathsf{MV}$-ideal which is both Boolean and prime is an obstinate weak $\mathsf{H}_v\mathsf{MV}$-ideal, under suitable conditions, but the converse may not be

true. We also characterized obstinate weak H_vMV-ideals and the relationships between prime weak H_vMV-ideals and Boolean weak H_vMV-ideals in H_vMV-algebras with at most five elements and investigated what subsets can be a suitable candidate to be an obstinate weak H_vMV-ideal, Boolean weak H_vMV-ideal or a prime weak H_vMV-ideal.

References

[1] **M. Bakhshi**, H_vMV-*algebras I*, Quasigroups Related Systems, **22** (2014), 9 – 18.

[2] **M. Bakhshi**, H_vMV-*algebras II*, J. Algebraic Systems, **3** (2015), 49 – 64.

[3] **M. Bakhshi**, *Fuzzy* H_vMV-*algebras*, Afr. Mat. **27** (2016), 379 – 392.

[4] **M. Bakhshi**, $(\alpha, \beta)_T$-*fuzzy* H_vMV-*ideals*, Ann. Fuzzy Math. Inform. **13** (2017), 73 – 90.

[5] **M. Bakhshi** and **J. Mohammadi**, *Intuitionistic fuzzy ideals in* H_vMV-*algebras*, Int. J. Math. Comput. **28** (2017), 31 – 47.

[6] **R.A. Borzooei**, **M.M. Zahedi**, **Y.B. Jun** and **A. Hasankhani**, *On Hyper K-algebra*, Math. Japon. **52** (2000), 113 – 121.

[7] **D. Buşneag and D. Piciu**, *On the lattice of ideals of an* MV-*algebra*, Sci. Math. Jpn. **56** (2002), 367 – 372.

[8] **C.C. Chang**, *Algebraic analysis of many valued logics*, Trans. Amer. Math. Soc. **88** (1958), 467 – 490.

[9] **C.C. Chang**, *A new proof of the completeness of the Lukasiewicz axioms*, Tran. Amer. Math. Soc. **93** (1959), 74 – 80.

[10] **P. Corsini**, *Prolegomena of Hypergroup Theory*, Aviani Editore, 1993.

[11] **P. Corsini and V. Leoreanu**, *Applications of Hyperstructure Theory*, Kluwer Academic Publishers, Dordrecht, 2003.

[12] **F. Forouzesh**, **E. Eslami and A. Borumand Saeid**, *On obstinate ideals in* MV-*algebras*, U. P. B. Sci. Bull. Series A, **76** (2014), 53 – 62.

[13] **Sh. Ghorbani**, **A. Hassankhani and E. Eslami**, *Hyper MV-algebras*, Set-Valued Mathematics and Applications, **1** (2008), 205 – 222.

[14] **C.S. Hoo**, *Maximal and essential ideals of MV-algebras*, Mathware Soft Comput. **2** (1995), 181 – 196.

[15] **C.S. Hoo**, *Fuzzy implicative and Boolean ideals of MV-algebras*, Fuzzy Sets and Systems, **66** (1994), 316 – 327.

[16] **C.S. Hoo and S. Sessa**, *Implicative and Boolean ideals in MV-algebras*, Math. Japon. **39** (1994), 215 – 219.

[17] **C.S. Hoo and S. Sessa**, *Fuzzy maximal ideals of BCIand MV-algebras*, Math. Japon. **39** (1994), 215 – 219.

[18] **Y.B. Jun, X.L. Xin, M.M. Zahedi and R.A. Borzooei**, *On Hyper* BCK-*algebras*, Italian J. Pure and Appl. Math. **8** (2000), 127 – 136.

[19] **F. Marty**, *Sur une generalization de la notion de groups*, 8th congress Math. Scandinaves, Stockhholm, (1934), 45 – 49.

[20] **D. Mundici**, MV-*algebras are categorically equivalent to bounded commutative* BCK-*algebras*, Math. Japon. **31** (1986), 889 – 894.

[21] **D. Mundici**, *Interpretation of AFC*-algebras in Łukasiewicz sentential calsulus*, J. Funct. Anal. **65** (1986), 15 – 63.

[22] **L. Torkzadeh**, **A. Ahadpanah**, *Hyper MV-ideals in hyper MV-algebras*, Math. Log. Quart. **56** (2010), 51 – 62.

[23] **T. Vougiouklis**, *Hyperstructures and Their Representations*, Hadronic, Florida, 1994.

[24] **T. Vougiouklis**, *A new class of hyperstructures*, J. Combin. inform. Syst. Sci. **20** (1995), 229235.

Received May 17, 2019

M.Bakhshi
Department of Mathematics, University of Bojnord, Bojnord, Iran
E-mail: bakhshi@ub.ac.ir

A.Radfar
Department of Mathematics, Payame Noor University, P. O. Box 19395-3697, Tehran, Iran
E-mail: radfar@pnu.ac.ir

Quasigroups and Related Systems **27** (2019), 201 – 210

Complete graph decompositions and P-groupoids

John Carr and Mark Greer

Abstract. We study P-groupoids that arise from certain decompositions of complete graphs. We show that left distributive P-groupoids are distributive, quasigroups. We characterize some P-groupoids when the corresponding decomposition is a Hamiltonian decomposition for complete graphs of odd, prime order. We also study a specific example of a P-quasigroup constructed from cyclic groups of odd order. We show that the right multiplication group of such P-quasigroups is isomorphic to the dihedral group.

1. Introduction

The concept of graph amalgamation was introduced in 1984 by Anthony Hilton [5]. Recently, the subject has gained more attention and is becoming more widely studied. We aim to provide insight into graph amalgamation by considering the results of amalgamation in Latin squares. First, we cover some preliminaries.

Recall that a graph is an ordered pair $G = (V, E)$ comprising a set V of vertices with a set E of edges. A *complete graph*, denoted by K_n where n is the number of vertices in the graph, is a graph where every pair of vertices is connected by an edge. An *edge coloring* of a graph G is a function $\gamma : C \to E(G)$, where C is a set of colors. A *Hamiltonian decomposition* of K_{2n+1} is an edge-coloring of K_{2n+1} with n colors in which each color class is a C_{2n+1} cycle, called *Hamiltonian cycles*.

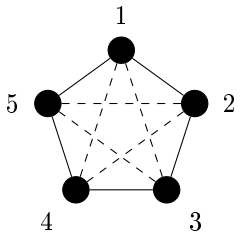
We define *graph amalgamation* in the following way.

Definition 1.1. Let G and H be two graphs with the same number of edges where G has more vertices than H. We say that H is an *amalgamation* of G if there exists a bijection $\phi : E(G) \to E(H)$ and a surjection $\psi : V(G) \to V(H)$ where the following hold

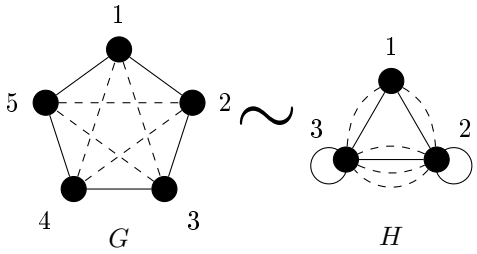
1. If x, y are two vertices in G where $\psi(x) \neq \psi(y)$, and both x and y are adjacent by edge e in G, then $\psi(x)$ and $\psi(y)$ are adjacent by edge $\phi(e)$ in H.
2. If e is a loop on a vertex $x \in V(G)$, then $\phi(e)$ is a loop on $\psi(x) \in H$.
3. If e joins $x, y \in V(G)$ where $x \neq y$, but $\psi(x) = \psi(y)$, then $\psi(e)$ is a loop on $\psi(x)$.

2010 Mathematics Subject Classifications: 20N05, 05C25
Keywords: Complete graphs, Hamiltonian decompositions, P-groupoids, P-quasigroups, quandles.
Research of the first author was partially supported by University of North Alabama QEP Undergraduate Research Grant

Example 1.2. K_5 and a Hamiltonian decomposition.



Example 1.3. The following is an example of a graph amalgamation of the complete graph on 5 vertices with the amalgamation $\psi(1) = 1$, $\psi(2) = 2$, $\psi(3) = 2$, $\psi(4) = 3$, $\psi(5) = 3$.

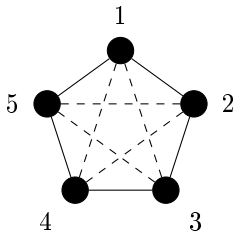


Note that since the edges between two amalgamated graphs are in bijection with each other, edge colorings are invariant to amalgamation; that is, edge colors are unchanged by amalgamation. However, more interesting is the fact that if G is a complete graph of the form K_{2n+1} and the edges are colored in such a way as to specify a Hamiltonian decomposition, then the edges also form a Hamiltonian decomposition in H.

The concept of amalgamating a larger graph down into a smaller graph is a well understood concept in graph theory. Likewise, one can *disentangle* vertices of a graph to create a larger graph. To disentangle a vertex is to split the vertex into multiple vertices. Using example 3, we could disentangle vertex 2 of graph H into vertices 2 and 3, while disentangling vertex 3 into vertices 4 and 5 to create graph G. Some graph theorists are currently studying how to take a graph with a Hamiltonian decomposition such as graph G, and to disentangle G to create a new graph, say G', where G' also has a Hamiltonian decomposition. Since the concept of amalgamation also exists in the Latin square setting, we approach the problem from an algebraic perspective.

Let K_n be a complete graph. It is well known that the edges in K_n can be decomposed into distinct cycles if and only if n is odd [9]. In this setting, Kotzig gave a complete characterization of a groupoid (termed P-groupoid) that would describe the decomposition. Indeed, let Q be a set with n elements (corresponding to the vertices in K_n) and define $xy = z$ if and only if edges (x, y) and (y, z) are in the same cycle where $x \neq y$. If $x = y$, then set $x^2 = x$.

Example 1.4. Consider the previous example of K_5, along with its associated P-groupoid.



(Q,·)	1	2	3	4	5
1	1	3	5	2	4
2	5	2	4	1	3
3	4	1	3	5	2
4	3	5	2	4	1
5	2	4	1	3	5

Kotzig then showed that all decompositions of complete graphs are given by *P-groupoids*, defining them as follows.

Definition 1.5 ([9])**.** Let $(Q, \cdot)$ be a groupoid. Then $(Q, \cdot)$ is a P-groupoid if for all $x, y, z \in Q$,

(1.5.1) $x^2 = x$ (Idempotent).

(1.5.2) $x \neq y \Rightarrow xy \neq x$ and $xy \neq y$.

(1.5.3) $xy = z \Leftrightarrow zy = x$.

For the rest of the paper we only consider finite groupoids and P-groupoids. One can quickly show that the order of every P-groupoid is odd [9] and that the equation $xa = b$ is always uniquely solvable for x. Indeed, $xa = b \Leftrightarrow ba = x$. Hence, P-groupoids are idempotent, right quasigroups. We show that if the P-groupoid is left distributive, then it is right distributive and a quasigroup (Theorem 2.2).

Dénes and Keedwell gave the first specific example of a P-quasigroup relating to the decomposition [2]. We also note that this P-quasigroup is a quandle and use results from [10] to describe the right multiplication group and automorphism group of Dénes and Keedwell's example. We then show that if $H \leq Q$ is a subquasigroup, then $|H|$ must divide $|Q|$ (Theorem 2.6). If the graph has prime order, then Dénes and Keedwell's example is an example of a P-quasigroup relating a Hamiltonian decomposition.

2. P-groudpoids and quasigroups

A *groupoid* $(Q, \cdot)$ is a set Q with a binary operation $\cdot : Q \times Q \to Q$. A *quasigroup* $(Q, \cdot)$ is a groupoid such that for all $a, b \in Q$, the equations $ax = b$ and $ya = b$ have unique solutions $x, y \in Q$. We denote these unique solutions by $x = a\backslash b$ and $y = b/a$, respectively. Standard references in quasigroup theory are [1, 13]. All groupoids (quasigroups) considered here are finite.

To avoid excessive parentheses, we use the following convention:

- multiplication $\cdot$ will be less binding than divisions $/, \backslash$.

- divisions are less binding than juxtaposition.

For example $xy/z \cdot y\backslash xy$ reads as $((xy)/z)(y\backslash(xy))$.

For $x \in Q$, where Q is a quasigroup, we define the *right* and *left translations* by x by, respectively, $yR_x = yx$ and $yL_x = xy$ for all $y \in Q$. The fact that these mappings are permutations of Q follows easily from the definition of a quasigroup. It is easy to see that $yL_x^{-1} = x\backslash y$ and $yR_x^{-1} = y/x$. We define the *left multiplication group of* Q, $\mathrm{Mlt}_\lambda(Q) = \langle L_x \mid \forall x \in Q\rangle$, the *right multiplication group of* Q, $\mathrm{Mlt}_\rho(Q) = \langle R_x \mid \forall x \in Q\rangle$ and the *multiplication group of* Q, $\mathrm{Mlt}(Q) = \langle Mlt_\lambda(Q), \mathrm{Mlt}_\rho(Q)\rangle$.

Lemma 2.1. *Let Q be a P-groupoid. Then $|R_x| = 2$ for all $x \in Q$* (i.e. $R_x^2 = id_Q$).

Proof. Let $|Q| = 2n+1$ for some $n \in \mathbb{Z}$ and suppose $q_1 x = q_2$ for some $x, q_1, q_2 \in Q$. Then $q_1 R_x^2 = q_2 R_x = q_1$. Moreover, $xR_x = x$. Hence,

$$R_x = (x)(q_1q_2)(q_3q_4)\dots(q_{2n})(q_{2n+1}).$$

The desired result follows. □

A groupoid Q is *left distributive* if it satisfies $x(yz) = (xy)(xz)$ for all $x, y, z \in Q$. Similarly, it is *right distributive* if it satisfies $(yz)x = (yx)(zx)$. A *distributive* groupoid is a groupoid that is both left and right distributive.

Theorem 2.2. *Let Q P-groupoid. If Q is left distributive, then Q is a distributive quasigroup.*

Proof. Let Q be a left distributive, P-groupoid. Note that by left distributivity, we have $x \cdot yx = xy \cdot x$. Suppose that $xa = xb$ for some $x, a, b \in Q$. Then we compute

$$\begin{aligned}
(ax)(ab \cdot x) &= [(ax)(ab)](ax \cdot x) && \text{by left distributivity,}\\
&= [(ax)(ab)]a && \text{by Lemma 2.1,}\\
&= [(a \cdot xb)]a && \text{by left distributivity,}\\
&= a(xb \cdot a) = a(xa \cdot a) && \text{by assumption,}\\
&= ax && \text{by Lemma 2.1}
\end{aligned}$$

Hence, we have $ab \cdot x = ax$ by (1.5.2). Thus, $ab = a$ and hence, $b = a$ by (1.5.2) again. Thus, Q is a quasigroup.

For right distributive, we first note that by left distributivity $x(xy \cdot z) = (xy \cdot y)(xy \cdot z) = (xy)(yz)$. Using (1.5.3), we have

$$[x(xy \cdot z)](yz) = xy. \tag{1}$$

Similarly, $(xy \cdot z)x = (xy \cdot z)(xy \cdot y) = (xy)(zy)$ and $x(xy \cdot z) = (xy \cdot y)(xy \cdot z) = (xy)(yz)$ both by left distributivity again, thus

$$(xy \cdot z)x = (xy)(zy), \tag{2}$$

$$x(xy \cdot z) = (xy)(yz). \tag{3}$$

Hence we have

$$\begin{aligned}(x \cdot yz)(xz \cdot u) &= [(xy)(xz)](xz \cdot u) && \text{by left distributivity,}\\ &= (xy)[(xy)(xz) \cdot u] && \text{by (3) with } x \to xy, y \to yz, z \to u,\\ &= (xy)[(x \cdot yz) \cdot u] && \text{by left distributivity,}\end{aligned}$$

thus

$$(x \cdot yz)(xz \cdot u) = (xy)[(x \cdot yz) \cdot u]. \tag{4}$$

Substituting $y \to yz$ in (1) give $x(yz) = [x(x(yz) \cdot z)][yz \cdot z] = x(x(yz) \cdot z) \cdot y$. So

$$x(yz) = x(x(yz) \cdot z) \cdot y. \tag{5}$$

Hence we compute

$$\begin{aligned}x &= [x \cdot x(yz)][\underline{x(yz)}]\\ &= [x \cdot x(yz)][x(x(yz) \cdot z) \cdot y] && \text{by (5),}\\ &= [x(x(yz) \cdot z)][xz \cdot y] && \text{by (4) with } y \to x(yz), u \to y.\end{aligned}$$

Thus

$$x = [x(x(yz) \cdot z)][xz \cdot y]. \tag{6}$$

Replacing $x \to xy$ and $y \to x$ in (6) gives

$$\begin{aligned}xy &= [(xy) \cdot (xy \cdot xz)z][\underline{(xy \cdot z)x}] && \text{by (6) with } x \to xy,\\ &= [(xy) \cdot (xy \cdot xz)z](xy \cdot zy) && \text{by (2),}\\ &= [(xy) \cdot (x \cdot yz)z](xy \cdot zy) && \text{by left distributivity,}\end{aligned}$$

and therefore

$$xy = [(xy) \cdot (x \cdot yz)z](xy \cdot zy). \tag{7}$$

Recalling (3) and substituting $y \to yz$, we have $(x \cdot yz)y = (x \cdot yz)(yz \cdot z) = x \cdot (x \cdot yz)z$, so

$$(x \cdot yz)y = x \cdot (x \cdot yz)z. \tag{8}$$

We compute

$$\begin{aligned}x(yz \cdot x) = (x \cdot yz)x = (xy \cdot xz)x && \text{by left distributivity,}\\ = (xy) \cdot (xy \cdot xz)z && \text{by (8) } x \to xy, y \to x,\end{aligned}$$

and hence

$$x(yz \cdot x) = (xy)[(x \cdot yz)z]. \tag{9}$$

Hence, the right hand side of (7) can be rewritten as

$$xy = [x(yz \cdot x)](xy \cdot zy). \tag{10}$$

Using left distributivity, we have

$$\begin{aligned}(xy)\cdot(xz\cdot y)(zy) &= [(xy)(xz\cdot y)](xy\cdot zy) && \text{by left distributivity,}\\ &= [(xy\cdot xz)(xy\cdot y)](xy\cdot zy) && \text{by left distributivity,}\\ &= [(x\cdot yz)(xy\cdot y)](xy\cdot zy) && \text{by left distributivity,}\\ &= [(x\cdot yz)x](xy\cdot zy)\\ &= [x(yz\cdot x)](xy\cdot zy),\end{aligned}$$

and thus

$$[x(yz\cdot x)][(xy\cdot zy)] = (xy)[(xz\cdot y)(zy)]. \tag{11}$$

Therefore, the right hand side of (10) can be rewritten as $xy = (xy)[(xz\cdot y)(zy)]$

Finally, since $(xy)[(xz\cdot y)(zy)] = xy$, we have $(xz\cdot y)(zy) = xy$ by (1.5.2) and thus $(xy)(zy) = xz\cdot y$ by (1.5.3). □

We now focus on the first specific constructions of a P-quasigroup dealing with Hamiltonian decompositions given by Deńes and Keedwell [2].

Theorem 2.3 ([2]). *Consider* $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ *where* $n = 2k+1$ *for some* $k \in \mathbb{Z}$. *Define* $r \circ s = 2s - r \mod n$. *Then* $(\mathbb{Z}_n, \circ)$ *is a P-quasigroup of order* n.

Proposition 2.4. *For* $(\mathbb{Z}_n, \circ)$, *the following hold:*

(*i*) $yL_x^n = 2^n(y-x) + x$ *for all* $x, y \in Q$.

(*ii*) $|L_x| = k$ *where* k *is the smallest integer such that* $2^k \equiv 1 \mod n$.

(*iii*) $L_x^n R_x = R_x L_x^n$.

Proof. Let $x, y \in Q$. For (*i*), $yL_x = 2y - x = 2(y-x) + x$. By induction,

$$yL_x^{n+1} = (2y-x)L_x^n = 2^n((2y-x)-x) + x = 2^{n+1}(y-x) + x.$$

For (*ii*), let $k > 0$ be the smallest integer such that $yL_x^k = y$. Then, by (1),

$$2^k(y-x) + x \equiv y \Leftrightarrow 2^k y - y - 2^k x + x \equiv 0 \Leftrightarrow (y-x)(2^k - 1) \equiv 0.$$

Hence, $2^k \equiv 1 \mod n$. Finally,

$$yL_xR_x = (2y-x)R_x = 3x - 2y = (2x-y)L_x = yR_xL_x.$$

Since $\mathrm{Mlt}(Q)$ is a group, (*iii*) follows. □

$(\mathbb{Z}_n, \circ)$ is well known. A quasigroup Q is medial (or entropic) if $(xy)(zw) = (xz)(yw)$ for all $x, y, z, w \in Q$. Idempotent medial quasigroups are distributive [15]. There is a well-known correspondence between abelian groups and medial quasigroups, the Toyoda-Bruck theorem. That is, $(Q, \cdot)$ is a medial quasigroup if

and only if there is an abelian group $(Q,+)$ such that $x\cdot y = f(x)+g(y)+c$ for all $x,y\in Q$ for some commuting $f,g\in \mathrm{Aut}(Q)$ and $c\in Q$ [14]. If $(G,+)$ is an abelian group of odd order, then both $f(x)=-x$ and $g(y)=2y$ are automorphisms of G. Hence, Deńes and Keedwell's P-quasigroup is precisely the medial quasigroup of the form $x\circ y = f(x)+g(y)+0$.

Definition 2.5. A groupoid $(Q,\cdot)$ is a *quandle* if

1. $a^2=a$ for all $a\in Q$,
2. For all $a,b\in Q$, the equations $xa=b$ have a unique solution,
3. $(ab)c=(ac)(bc)$ for all $a,b,c\in Q$.

Note that quandles are idempotent, right distributive, and right quasigroups.

$(\mathbb{Z}_n,\circ)$ is also referred to as the *dihedral quandle* of order n with $\mathrm{Mlt}_\rho(Q)\cong D_{2n}$ [10], the dihedral group of order $2n$. For a quandle Q, the *inner automorphism group of* Q, $\mathrm{Inn}(Q)$ is the subgroup generated by L_x for all $x\in Q$. Thus, $\mathrm{Inn}(\mathbb{Z}_n,\circ)$ is isomorphic to the dihedral group of order n. Moreover, both L_x and R_y are affine maps for all x,y. Indeed,

$$[(1-t)a+tb]L_x = 2[(1-t)a+tb]-x = (1-t)(2a-x)+j(2b-x) = (1-t)(aL_x)+t(bL_x),$$

$$[(1-t)a+tb]R_y = 2y-[(1-t)a+tb] = (1-t)(2y-a)+t(2y-b) = (1-t)(aR_y)+t(bR_y),$$

for all $a,b,t\in\mathbb{Z}_n$. That is $\mathrm{Aut}(\mathbb{Z}_n,\circ)$ is isomorphic to the affine group $\mathrm{Aff}(\mathbb{Z}_n)$ [10].

Note that P-quasigroups always have subgroups $\langle x\rangle$ for all x. It is well-known that in general, the order of a subquasigroup doesn't divide the order of the quasigroup. However, for $Q=(\mathbb{Z}_n,\circ)$, the order of the subquasigroup always divides the order of the quasigroup.

Theorem 2.6. *Let $Q=(\mathbb{Z}_n,\circ)$. If $H\le Q$, then $|H|$ divides $|Q|$. Hence, if Q has prime order and $|H|\le|Q|$, then $H=\langle x\rangle$ for some $x\in Q$ or $H=Q$.*

Proof. Let $H\le Q$. If $|H|=\langle x\rangle$, then $|H|=1$ and we are done. Let $x,y\in Q$. Then $y=x+k$, since both $x,y\in\mathbb{Z}_n$. Then $x\circ y = x+2k\in H$. Continuing, $x\circ(x+2k)=x+3k$, and thus, elements of H are of the form $x+lk$. Since Q is finite, we must have $x+l_1k=x+l_2k$. Thus, $k(l_1-l_2)\equiv 0 \mod n$. Thus, k is a divisor of n. Let $kl=n$. Then $H=\{x,x+k,x+2k,\dots x+(l-1)k\}$, and therefore $|H|=l$, a divisor of n. □

The following is a minimal example of a P-groupoid that is not a quandle, found by Mace4 [11].

Example 2.7. A P-groupoid of order 5 that is not a quandle.

$(Q,\cdot)$	1	2	3	4	5
1	1	3	2	3	4
2	3	2	1	5	3
3	2	1	3	1	2
4	5	5	5	4	1
5	4	4	4	2	5

3. Hamiltonian decompostions and P-quasigroups

Theorem 3.1. *Let Q_1 and Q_2 be two P-groupoids. Then, $Q_1 \cong Q_2$ if and only if the corresponding decompositions of the associated complete graph is isomorphic.*

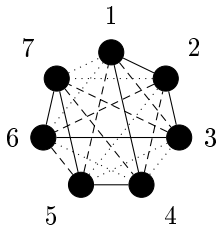
Proof. Suppose ϕ is an isomorphism between Q_1 and Q_2 where both Q_1 and Q_2 correspond to decompositions of K_n. By definition $(a,b)(b,c)$ belong to the same cycle in the decomposition of K_n if and only if $ab = c$ for all $a, b, c \in Q_1$. Then $(\phi(a), \phi(b))(\phi(b), \phi(c))$ belong to the same cycle in K_n if and only if $\phi(a)\phi(b) = \phi(c)$. Since this is precisely the correspondence between Q_2 and its Hamiltonian decompostion of K_n, the decompositions must be isomorphic.

Alternatively, suppose ϕ is an isomorphism between two decompositions of K_n. If $(\phi(a), \phi(b))(\phi(b), \phi(c))$ belong to the same cycle in K_n for some $a, b, c \in Q_1$, then $\phi(a)\phi(b) = \phi(c)$ for $\phi(a), \phi(b), \phi(c) \in Q_2$. Again, since this is precisely how we establish a correspondence between P-groupoids and complete undirected graphs, we conclude that $Q_1 \cong Q_2$. □

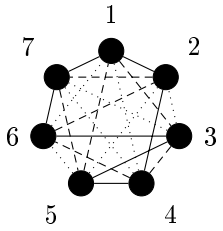
Theorem 3.2. ([2]) *Let p be an odd prime. Then $(\mathbb{Z}_n, \circ)$ corresponds to a Hamiltonian decomposition in K_p.*

Note that Theorem 3.1 does not imply all P-groupoids of prime order corresponding to a Hamiltonian decomposition of K_p are quasigroups. Below are two Hamiltonian decompositions of K_7 with non isomorphic corresponding P-groupoids.

Example 3.3. Two non-isomorphic Hamiltonian decompositions and their corresponding P-groupoids.



Q_1	1	2	3	4	5	6	7
1	1	3	7	5	6	4	2
2	4	2	6	7	3	5	1
3	5	1	3	6	2	7	4
4	2	6	5	4	7	1	3
5	3	7	4	1	5	2	6
6	7	4	2	3	1	6	5
7	6	5	1	2	4	3	7



Q_2	1	2	3	4	5	6	7
1	1	4	4	7	7	5	6
2	7	2	7	5	6	4	5
3	5	5	3	6	4	7	4
4	6	1	1	4	3	2	3
5	3	3	6	2	5	1	2
6	4	7	5	3	2	6	1
7	2	6	2	1	1	3	7

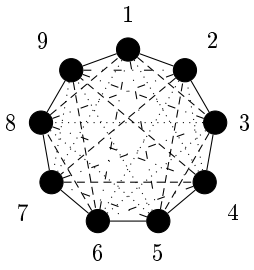
The following is motivated by Theorem 2.6.

Theorem 3.4. *Let K_n have a Hamiltonian decomposition and let Q be the corresponding P-groupoid. Then Q doesn't contain any nontrivial subgroupoids.*

Proof. Let $|Q| = n$ correspond to a complete graph K_n with a Hamiltonian decomposition. For the sake of contradiction, suppose $\exists H < Q$ where $|H| > 1$. Since H is a subgroupoid, H is closed and multiplying the elements of H will create a cycle with length less than n. However, this contradicts our assumption that K_n has a Hamiltonian decomposition. Therefore, we conclude that Q doesn't contain any subgroupoids with order greater than 1. □

The following is an example of a P-groupoid corresponding to a Hamiltonian decomposition of K_9. It is currently unknown if a P-quasigroup exists that corresponds to a Hamiltonian decomposition of K_9 (note that $(\mathbb{Z}_9, \circ)$) is not a quasigroup).

Example 3.5. A P-groupoid of order 9 corresponding to a Hamiltonian decomposition.



K_9	1	2	3	4	5	6	7	8	9
1	1	3	5	2	7	4	9	6	8
2	9	2	4	1	3	3	4	4	3
3	8	1	3	5	2	2	5	5	2
4	7	6	2	4	6	1	2	2	6
5	6	7	1	3	5	7	3	3	7
6	5	4	8	8	4	6	8	1	4
7	4	5	9	9	1	5	7	9	5
8	3	9	6	6	9	9	6	8	1
9	2	8	7	7	8	8	1	7	9

Further work would consist of finding all necessary and sufficient conditions such that a P-groupoid of odd nonprime order corresponds to a Hamiltonian decomposition of a complete graph. Hilton gave necessary and sufficient conditions for a Hamiltonian decomposition of K_{2n+1} corresponding to a Hamiltonian circuit [5]. The proof relies heavily on Hall's work with completing partial Latin squares [4]. Thus, using P-groups to classify Hamiltonian decompositions is a natural choice. Moreover, due to the connection to quandles in the prime order case, perhaps finding a relationship between P-groupoids and quandles could lead to new results in both fields.

Acknowledgment. Some investigations in this paper were assisted by the automated deduction tool, Prover9, and the finite model builder, Mace4, both developed by McCune [11]. Similarly, all presented examples were found and verified using the GAP system [3] together with the LOOPS package [12]. We also thank the anonymous referee for several comments that improved the manuscript.

References

[1] **R.H. Bruck**, *A Survey of Binary Systems*, Springer-Verlag, Berlin, 1971.

[2] **J. Deńes and A.D. Keedwell**, *On P-Quasigroups and Decompositions of Complete Undirected Graphs*, J. Combin. Theory (B) **13** (1972), 270 – 275.

[3] **The GAP Group**, *Groups, Algorithms, and Programming*, http://www.gap-system.org, 2008.

[4] **M. Hall Jr.**, *An existence theorem for latin squares*, Amer. Math. Monthly. **67** (1960), 958 – 961.

[5] **A.J.W. Hilton**, *Hamilton Decompositions of Complete Graphs*, J. Combin. Theory, **36** (1984), 125 – 134.

[6] **H. Hilton**, *An Introduction to the Theory of Groups of Finite Order*, Oxford: Clarendon press, **159**, 1908.

[7] **D. Joyce**, *A Classifying Invariant of Knots, The Knot Quandle*, J. Pure Appl. Algebra **23** (1982), 37 – 65.

[8] **T. Kepka**, *Structure of triabelian quasigroups*, Comment. Math. Univ. Carolin. **17** (1976), no. 2, 229 – 240.

[9] **A. Kotzig**, *Groupoids and Partitions of Complete Graphs*, Combinatorial Structures and their Applications (Proc. Calgary Internal. Conf., Calgary, Alta), 215 – 221, 1970.

[10] **J. Macquarrie**, *Automorphism groups of quandles*, Graduate Theses and Dissertations, http://scholarcommons.usf.edu/etd/3226, 2011.

[11] **W.W. McCune**, *Prover9, Mace4*, http://www.cs.unm.edu/~mccune/prover9/, 2009.

[12] **G.P. Nagy and P. Vojtěchovský**, *Loops: Computing with quasigroups and loops*, http://www.math.du.edu/loops, 2008.

[13] **H.O. Pflugfelder**, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math, Berlin, 1990.

[14] **D. Stanovský**, *A guide to self-distributive quasigroups, or latin quandles,* Quasigroups and Related Systems **23** (2015), 91 – 128.

[15] **S. Stein**, *On the Foundations of quasigroups,* Trans. Am. Math. Soc. **85** (1956), 228 – 256.

Received April 01, 2019

J. Carr
Department of Mathematics and Statistics, Auburn University, 221 Parker Hall, Auburn, AL 36849, USA
e-mail: jac0017@auburn.edu

M. Greer
Department of Mathematics, University of North Alabama, One Harrison Plaza, Florence, AL 35632. USA
e-mail: mgreer@una.edu

Quasigroups and Related Systems **27** (2019), 211 – 226

Categorical equivalences in the theory of sharp transitivity

Timothy L. Clark

Abstract. There are well-known correspondences between loops and regular permutation sets; neardomains and sharply 2-transitive groups; and KT-fields and sharply 3-transitive groups. Initially, these correspondences only considered isomorphisms. However, the first two correspondences were realized as more general categorical equivalences. In this note, we offer a simplified development of these equivalences and extend the results to a categorical equivalence between KT-fields and sharply 3-transitive groups. We then show how these three equivalences are related to one another via a diagram of functors.

1. Introduction and overview

Given a loop L, its set of left translations $T_1L = \{\lambda_a : x \mapsto ax \mid a \in L\}$ acts *regularly* on L, meaning for every $x, y \in L$, there is a unique $\lambda_a \in T_1L$ such that $\lambda_a(x) = y$. It turns out, not only is this construction *functorial*, it forms an equivalence between the category of loops (denoted **Loop**) and the category of regular permutation sets (denoted **RPS**) [1].

There is a related correspondence between neardomains and sharply 2-transitive groups. Here, a neardomain essentially consists of $(F, +, \cdot)$ where $(F, +)$ is a loop and $(F \setminus \{0\}, \cdot)$ is a group, while a sharply 2-transitive group is a group action that is regular on pairs of distinct points. Given a neardomain, its group of affine transformations $T_2F = \{x \mapsto a + bx \mid b \neq 0\}$ acts sharply 2-transitively on F (cf. [2] (6.1)). In [1], this correspondence was proven to be an equivalence between the category of neardomains (denoted **nDomain**) and a category of sharply 2-transitive groups (denoted **s2tGroup**). Proving that T_2 is a categorical equivalence hinges on the definition of **s2tGroup**; the crucial realization in [1] is that not every conceivable morphism of sharply 2-transitive groups corresponds to a neardomain morphism, so we must pare down our morphisms of sharply 2-transitive groups accordingly.

Finally, there is another correspondence between KT-fields and sharply 3-transitive groups, where KT-fields are neardomains with a distinguished invo-

2010 Mathematics Subject Classification: 20N05; 12K05; 16Y99; 20B22; 18A99.
Keywords: loops; neardomains; nearfields; KT-fields; sharply multiply transitive groups; equivalence of categories.

lution (thought of as a generalized *inversion*) and sharply 3-transitive groups are groups that act regularly on triples of distinct points. As shown in [2] (11.1), given a KT-field F, one can form the group of generalized fractional affine transformations T_3F which acts sharply 3-transitively on F. The name "generalized fractional affine transformations" comes from the fact that, if F is a field, then $T_3F = \left\{x \mapsto \frac{a+bx}{c+dx} \mid ad - bc \neq 0\right\}$. In general, T_3F is generated as a subgroup of the permutations on F by T_2F and the distinguished involution of F. Our main result is that, not only is T_3 functorial, the category of KT-fields (denoted **KTfield**) is equivalent to a category of sharply 3-transitive groups (denoted **s3tGroup**); cf. Theorem 3.13. Moreover the three equivalences T_1, T_2, and T_3 enjoy a particularly nice interdependence.

As is the case for T_2, proving that T_3 is an equivalence of categories largely depends on the morphisms we allow in **s3tGroup**. In particular, the construction of T_3F demands that morphisms in **s3tGroup** induce morphisms in **s2tGroup** on stabilizers. Once this is done, however, the argument proceeds swiftly. This is substantially a consequence of the general scheme in which T_1, T_2, and T_3 fit. As we will see:

- Given a neardomain F, the functor T_2 is essentially two applications of T_1 – once to $(F \setminus \{0\}, \cdot)$ and once to $(F, +)$.
- Given a KT-field F with distinguished involution σ, the functor T_3 is essentially T_2 after forgetting and then remembering σ.

So, overall, our categorical equivalences T_2 and T_3 are built in a very tangible way from the comparatively simple equivalence $T_1 : \mathbf{Loop} \xrightarrow{\simeq} \mathbf{RPS}$; this is formalized in Theorem 3.14.

Organization. Section 2 focuses on preliminary definitions and basic results from category theory, non-associative algebra, and sharply multiply transitive actions. In particular, we have the lemma:

Lemma 1.1. *Let* $\mathbf{C}$ *and* $\mathbf{D}$ *be categories and suppose there are functors* $F : \mathbf{C} \to \mathbf{D}$ *and* $G : \mathbf{D} \to \mathbf{C}$ *such that* $GF = id_{\mathbf{C}}$. *If* G *is faithful, then* F *is an equivalence of categories with inverse* G.

We also have the lemma:

Lemma 1.2. *Let* $\mathbf{C}$ *be one of the categories* **RPS**, **s2tGroup**, *or* **s3tGroup**. *Then two morphisms* (f, Φ) *and* (g, Ψ) *are equal in* $\mathbf{C}$ *if and only if* $\Phi = \Psi$.

These two lemmas combine in Section 3 to shorten the proofs of Theorems 3.4, 3.9, and 3.13 regarding the assortment of categorical equivalences mentioned above. In particular, in Section 3 we prove:

Theorem 1.3. *There is an equivalence of categories* $T_3\colon \mathbf{KTfield} \xrightarrow{\simeq} \mathbf{s3tGroup}$.

We also concisely exhibit the relationship between T_1, T_2, and T_3 in Section 3 via the following theorem:

Theorem 1.4. *There is a commutative diagram of functors:*

$$\begin{array}{ccc} \mathbf{KTfield} & \xrightarrow[T_3]{\simeq} & \mathbf{s3tGroup} \\ \downarrow & & \downarrow \\ \mathbf{nDomain} & \xrightarrow[T_2]{\simeq} & \mathbf{s2tGroup} \\ \downarrow & & \downarrow \\ \mathbf{Loop} & \xrightarrow[T_1]{\simeq} & \mathbf{RPS}. \end{array}$$

2. Preliminaries

This section is dedicated to some definitions and basic results for reference in the development to follow.

2.1. Category theory

We assume familiarity with the notions of category and functor; the standard reference is [4]. We recall some basic definitions here, namely that of *natural equivalence* and *categorical equivalence*. We also prove Lemma 2.1 that helps us provide succinct proofs of our main theorems in Section 3.

Natural and categorical equivalences. Given two functors $F, G\colon \mathbf{C} \to \mathbf{D}$, a **natural transformation** $\eta : F \to G$ is an assignment for each object X of $\mathbf{C}$ a morphism $\eta_X : F(X) \to G(X)$ in $\mathbf{D}$ such that, for every morphism $f\colon X \to Y$ in $\mathbf{C}$, the following diagram commutes

$$\begin{array}{ccc} F(X) & \xrightarrow{\eta_X} & G(X) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow[\eta_Y]{} & G(Y). \end{array}$$

A natural transformation in which each η_X is an equivalence is called a **natural equivalence**.

We are primarily interested in exhibiting pairs of categories as equivalent, in a sense we will make precise immediately: A functor $F\colon \mathbf{C} \to \mathbf{D}$ is an **equivalence of categories** if there is a functor $G\colon \mathbf{D} \to \mathbf{C}$ and natural equivalences $FG \xrightarrow{\cong} \mathrm{id}_{\mathbf{D}}$

and $GF \xrightarrow{\cong} \mathrm{id}_{\mathbf{C}}$. In this case, we write $F\colon \mathbf{C} \xrightarrow{\simeq} \mathbf{D}$ or simply $\mathbf{C} \simeq \mathbf{D}$, and we call G the **inverse** of F. Assuming the Axiom of Choice, $F\colon \mathbf{C} \to \mathbf{D}$ is an equivalence of categories if and only if F is full, faithful, and essentially surjective ([4] Theorem IV.4.1).

The faithful retract lemma. We will call a category $\mathbf{C}$ a **retract** of a category $\mathbf{D}$ provided there are functors $F\colon \mathbf{C} \to \mathbf{D}$ and $G\colon \mathbf{D} \to \mathbf{C}$ such that $GF = \mathrm{id}_{\mathbf{C}}$. In this case, the functor G is called a **retraction**. If, additionally, there is a natural equivalence $FG \xrightarrow{\cong} \mathrm{id}_{\mathbf{D}}$, we call $\mathbf{C}$ a **deformation retract** of $\mathbf{D}$. We recognize deformation retract as a stronger notion of categorical equivalence. This next lemma is an adaptation of a familiar result from category theory that if a retraction has a left inverse, then it has a two sided inverse.

Lemma 2.1 (Faithful Retract Lemma)**.** *Suppose* $\mathbf{C}$ *is a retract of* $\mathbf{D}$ *via* $F\colon \mathbf{C} \to \mathbf{D}$ *and* $G\colon \mathbf{D} \to \mathbf{C}$*. If* G *is faithful, then there exists a natural transformation* $FG \xrightarrow{\cong} id_{\mathbf{D}}$*. In particular,* F *is an equivalence of categories with inverse* G*.*

Proof. Suppose G is a retraction. We claim G is essentially surjective and full. To see this, let X be an object in $\mathbf{C}$. Then $GF(X) = X$ since $GF = \mathrm{id}_{\mathbf{C}}$, thus G is (essentially) surjective on objects. Now suppose $f : G(X) \to G(Y)$ is a morphism in $\mathbf{C}$ where X and Y are objects of $\mathbf{D}$. Then, $GFf = f\colon G(X) \to G(Y)$, hence G is full.

So, if G is also faithful, then G is an equivalence of categories. This means there exists a functor $H\colon \mathbf{C} \to \mathbf{D}$ and a natural equivalence $HG \xrightarrow{\cong} \mathrm{id}_{\mathbf{D}}$. Thus, there is a natural equivalence $HGF \xrightarrow{\cong} \mathrm{id}_{\mathbf{D}}F$, i.e. a natural equivalence $H \xrightarrow{\cong} F$. Therefore, we induce a natural equivalence $FG \xrightarrow{\cong} HG \xrightarrow{\cong} \mathrm{id}_{\mathbf{D}}$ as claimed. □

2.2. Loops, neardomains, and KT-fields

In this section, we briskly review some basic definitions from non-associative algebra and define categories of loops, neardomains, and KT-fields.

Loops. A **loop** is a nonempty set L with a binary operation $(a, b) \mapsto ab$ such that:

1. The operation has a two-sided identity element $e \in L$;

2. For every $a, b \in L$, there exist unique $x, y \in L$ such that $ax = b$ and $ya = b$.

A **morphism of loops** is a function $f\colon L \to L'$ that preserves the loop operation. The category whose objects are loops and whose arrows are loop homomorphisms will be denoted **Loop**.

Neardomains. A set F with operations $+$ and $\cdot$ is called a **neardomain** if:

1. F is a loop under $+$ with identity 0;
2. For all $a, b \in F$: $a + b = 0$ implies $b + a = 0$;
3. $F - \{0\}$ is a group under $\cdot$ with identity 1;
4. For all $a \in F$: $0 \cdot a = 0$;
5. For all $a, b, c \in F$: $a \cdot (b + c) = a \cdot b + a \cdot c$;
6. For all $a, b \in F$, there exists $d_{a,b} \in F - \{0\}$ such that, for all $x \in F$, $a + (b + x) = (a + b) + d_{a,b} \cdot x$.

A **morphism of neardomains** $f : F \to F'$ is a function that preserves both operations. The category of neardomains and neardomain morphisms is denoted **nDomain**. Note: F is a **nearfield** if and only if all of the $d_{a,b} = 1$ (i.e., if and only if F is a group under $+$). Every finite neardomain is a nearfield. Whether there exists a neardomain that is not a nearfield was a long-standing open question, but the construction provided in [5] confirms the existence of proper neardomains.

It can be shown (cf. [1] Property 3.2) that all neardomain morphisms are injective. Consequently, if there exists a neardomain morphism $f\colon F \to F'$, then char $F = 2$ if and only if char $F' = 2$. This fact turns out to be essential for defining the appropriate category of sharply 2-transitive groups in Section 3.

KT-fields. A **KT-field** is quadruple $(F, +, \cdot, \sigma)$ such that

1. $(F, +, \cdot)$ is a neardomain;
2. $\sigma : F \to F$ is an involutary automorphism of $(F \setminus \{0\}, \cdot)$ satisfying
$$\sigma(1 + \sigma(x)) = 1 - \sigma(1 + x) ,$$
for all $x \in F \setminus \{0, -1\}$.

The characteristic of F as a KT-field is defined to be the characteristic of the neardomain F. A **morphism** of KT-fields $(F, +, \cdot, \sigma)$ and $(F', +, \cdot, \sigma')$ is a neardomain morphism $f\colon F \to F'$ such that $\sigma' \circ f = f \circ \sigma$ on $F \setminus \{0\}$. KT-fields and KT-field morphisms constitute a category denoted **KTfield**. We note that if F is a field, then $\sigma(x) = x^{-1}$ ([2] Theorem 13.2).

2.3. Sharply multiply transitive actions

We now review some basic definitions and results from the theory of sharply transitive actions. We then define categories of regular permutations sets, sharply 2-transitive groups, and sharply 3-transitive groups, utilizing the crucial insight from [1] regarding which morphisms to allow between sharply 2-transitive groups. The section ends with a proof of Lemma 2.4 that allows us to more easily identify when two morphisms in these categories are equal.

Regular permutation sets. A **regular permutation set** is a triple $(M, \Omega, *)$ where Ω is a set, $* \in \Omega$ is a chosen base point, and M is a subset of the set of all permutations on Ω such that:

1. The identity map $\mathrm{id}_\Omega : \alpha \mapsto \alpha$ is in M;
2. M **acts regularly** on Ω: for every $\alpha, \beta \in \Omega$, there is a unique $m \in M$ such that $m(\alpha) = \beta$.

A **morphism of regular permutation sets** $(M, \Omega, *)$ and $(N, \Sigma, *)$ is a pair of functions (f, Φ) where $f : M \to N$ and $\Phi : \Omega \to \Sigma$ such that $\Phi(*) = *$, and the following diagram commutes:

$$\begin{array}{ccc} M \times \Omega & \xrightarrow{\mathrm{ev}} & \Omega \\ {\scriptstyle f\times\Phi}\downarrow & & \downarrow{\scriptstyle \Phi} \\ N \times \Sigma & \xrightarrow[\mathrm{ev}]{} & \Sigma, \end{array}$$

where the horizontal maps are the evaluation maps. Regular permutation sets and morphisms of regular permutation sets (with composition defined componentwise) assemble into a category which we denote **RPS**.

An action of a group G on a set Ω is said to be **sharply transitive** provided for every $\alpha, \beta \in \Omega$, there exists a unique $g \in G$ such that $g\alpha = \beta$. A sharply transitive group action of a group G on a set Ω corresponds (via the standard identification of $G \leq \mathrm{SYM}\Omega$) to a regular permutation set $(G, \Omega, *)$ for a chosen base point $* \in \Omega$. In this way, we can define the category **s1tGroup** as the full subcategory of **RPS** whose objects are sharply transitive group actions.

Sharply 2-transitive groups. Suppose a group G acts on a set Ω. The action is **sharply 2-transitive** provided: for every $(\alpha_1, \alpha_2), (\beta_1, \beta_2) \in \Omega \times \Omega$ where $\alpha_1 \neq \alpha_2$ and $\beta_1 \neq \beta_2$, there is a unique $g \in G$ with $g\alpha_1 = \beta_1$ and $g\alpha_2 = \beta_2$.

It is tempting at this point to try to define a category of sharply 2-transitive groups analogous to the category **RPS**. To start, we might say the objects of this category are of the form $(G, \Omega, 0, 1)$ where G acts sharply 2-transitively on Ω and $0, 1 \in \Omega$ are distinct base points. Then, we could define a morphism to be a pair of functions $(f, \Phi) : (G, \Omega, 0, 1) \to (H, \Sigma, 0, 1)$ with $f : G \to H$ a group homomorphism, $\Phi : \Omega \to \Sigma$ a function sending $0 \mapsto 0$ and $1 \mapsto 1$, such that the following diagram commutes:

$$\begin{array}{ccc} G \times \Omega & \longrightarrow & \Omega \\ {\scriptstyle f\times\Phi}\downarrow & & \downarrow{\scriptstyle \Phi} \\ H \times \Sigma & \longrightarrow & \Sigma. \end{array}$$

This defines a perfectly reasonable category. However, as shown in [1], this category has "too many" morphisms to be equivalent to the category of neardomains!

So, we must eliminate morphisms between sharply 2-transitive groups that do not correspond to neardomain morphisms. Recall: all neardomain morphisms are injective and, consequently, the existence of a neardomain morphism $f\colon F \to F'$ implies char $F = 2$ if and only if char $F' = 2$. The characterestic of a neardomain turns out to be related to what is called the *type* of its corresponding sharply 2-transitive group, which we explore forthwith.

Suppose a group G acting sharply 2-transitively on a set Ω and consider the involutions of G, $\mathrm{INV}G = \{g \in G \mid g \neq \mathrm{id}_\Omega,\ g^2 = \mathrm{id}_\Omega\}$. Note: $\mathrm{INV}G$ is never empty if Ω has at least two elements. It can be shown that exactly one of the following conditions holds: (1) every $g \in \mathrm{INV}G$ has a unique fixed point; or (2) no $g \in \mathrm{INV}G$ has a fixed point ([2] Section 2).

If each $g \in \mathrm{INV}G$ has a unique fixed point we say G **is of type** 1, and if no $g \in \mathrm{INV}G$ has a fixed point, we say G **is of type** 0. We can now define the appropriate category of sharply 2-transitive groups as follows: The category **s2tGroup** has objects $(G, \Omega, 0, 1)$ where G is a group that acts sharply 2-transitively on a set Ω, and $0, 1 \in \Omega$ are distinct base points. The morphisms in **s2tGroup** are pairs of maps $(f, \Phi)\colon (G, \Omega, 0, 1) \to (H, \Sigma, 0, 1)$ where

1. G and H are of the same type;
2. $f\colon G \to H$ is a group homomorphism;
3. $\Phi\colon \Omega \to \Sigma$ is injective, mapping $0 \mapsto 0$ and $1 \mapsto 1$; and
4. the following diagram commutes:

$$\begin{array}{ccc} G \times \Omega & \longrightarrow & \Omega \\ {\scriptstyle f\times\Phi}\downarrow & & \downarrow{\scriptstyle \Phi} \\ H \times \Sigma & \longrightarrow & \Sigma\,, \end{array}$$

where the horizontal maps are evaluation.

Let $(G, \Omega, 0, 1)$ be a sharply 2-transitive group on a set Ω. In the case G has type 1, call ι the unique (by [2] (3.1)) involution fixing the base point $0 \in \Omega$. We define a subset $\mathrm{A}G \subseteq G$ by $\mathrm{A}G = \mathrm{INV}G \circ \iota$ if G has type 1, and $\mathrm{A}G = \mathrm{INV}G \cup \{\mathrm{id}_\Omega\}$ if G has type 0. It is shown in [2] that $(\mathrm{A}G, \Omega, 0)$ is a regular permutation set. Moreover, this construction is functorial:

Proposition 2.2. *There is a functor* $\mathrm{A}\colon$ **s2tGroup** $\to$ **RPS**.

Proof. For a sharply 2-transitive group $(G, \Omega, 0, 1)$ define $\mathrm{A}(G, \Omega, 0, 1) = (\mathrm{A}G, \Omega, 0)$ as above. The fact that $(\mathrm{A}G, \Omega, 0)$ is a regular permutation set is shown in [2] Theorem 3.3. To show that A is functorial, let $(f, \Phi)\colon (G, \Omega, 0, 1) \to (H, \Sigma, 0, 1)$ be a morphism in **s2tGroup**. By Lemma 3.8 in [1], we have $f(\mathrm{A}G) \subseteq \mathrm{A}H$. Thus, we define $\mathrm{A}f$ as the restriction $f|_{\mathrm{A}G}\colon \mathrm{A}G \to \mathrm{A}H$. We are left to show that

$(\mathrm{A}f, \Phi) : (\mathrm{A}G, \Omega, 0) \to (\mathrm{A}H, \Sigma, 0)$ is a morphism in **RPS**, as verifying that A is functorial is then routine.

First, we note that $\Phi(0) = 0$ by assumption. Now, consider the following commutative diagram:

$$\begin{array}{ccccc} \mathrm{A}G \times \Omega & \hookrightarrow & G \times \Omega & \longrightarrow & \Omega \\ \downarrow{\scriptstyle \mathrm{A}f \times \Phi} & & \downarrow{\scriptstyle f \times \Phi} & & \downarrow{\scriptstyle \Phi} \\ \mathrm{A}H \times \Sigma & \hookrightarrow & H \times \Sigma & \longrightarrow & \Sigma. \end{array}$$

The left square commutes by definition of $\mathrm{A}f$, while the right square commutes since (f, Φ) is a morphism in **s2tGroup**. Thus, the total rectangle commutes, verifying that $(\mathrm{A}f, \Phi)$ is a morphism in **RPS**. □

Sharply 3-transitive groups. A group action of G on a set Ω is said to be **sharply 3-transitive** if, for all 3-tuples of distinct elements of Ω, $(\alpha_1, \alpha_2, \alpha_3)$ and $(\beta_1, \beta_2, \beta_3)$, there is a unique $g \in G$ such that $g\alpha_i = \beta_i$ for $i = 1, 2, 3$. We can recognize sharply 3-transitive groups in terms of sharply 2-transitive groups as follows:

Proposition 2.3. *A group G acts sharply 3-transitively on a set Ω if and only if for every $\alpha \in \Omega$ the stabilizer G_α acts sharply 2-transitively on $\Omega \setminus \{\alpha\}$.*

Proof. See [2] (1.1)(a). □

As with the category of sharply 2-transtive groups, we must be careful to avoid excess morphisms in our category of sharply 3-transitive groups. Let (G, Ω) be a sharply 3-transitive group. As shown in [2] Section 2, each stabilizer $(G_a, \Omega \setminus \{a\})$ is a sharply 2-transitive group of the same type. This allows us to define the appropriate category of sharply 3-transitive groups, as follows: The category **s3tGroup** has objects $(G, \Omega, 0, 1, \infty)$ where G is a group that acts sharply 3-transitively on a set Ω, and $0, 1, \infty \in \Omega$ are distinct base points. The morphisms in **s3tGroup** are pairs of maps $(f, \Phi) \colon (G, \Omega, 0, 1, \infty) \to (H, \Sigma, 0, 1, \infty)$ where:

1. The stabilizers G_∞ and H_∞ have the same type as sharply 2-transitive groups;
2. $f \colon G \to H$ is a group homomorphism;
3. $\Phi \colon \Omega \to \Sigma$ is injective, mapping $0 \mapsto 0$, $1 \mapsto 1$, and $\infty \mapsto \infty$; and
4. the following diagram commutes:

$$\begin{array}{ccc} G \times \Omega & \longrightarrow & \Omega \\ \downarrow{\scriptstyle f \times \Phi} & & \downarrow{\scriptstyle \Phi} \\ H \times \Sigma & \longrightarrow & \Sigma\,, \end{array}$$

where the horizontal maps are evaluation.

The sharp morphism lemma. We now prove a lemma that allows us to more easily recognize when two morphisms in **RPS**, **s2tGroup**, and **s3tGroup** are equal. Together with Lemma 2.1, this result greatly expedites the proofs of Theorems 3.4, 3.9, and 3.13.

Lemma 2.4 (Sharp Morphism Lemma)**.** *Let* $\mathbf{C}$ *be one of the categories* **RPS**, **s2tGroup**, *or* **s3tGroup**. *Then two morphisms* (f, Φ) *and* (g, Ψ) *are equal in* $\mathbf{C}$ *if and only if* $\Phi = \Psi$.

Proof. We will prove the nontrivial assertion for $\mathbf{C} =$ **s3tGroup**. The proofs for the other options of $\mathbf{C}$ are similar.

Let $(f, \Phi), (g, \Psi) \colon (G, \Omega, 0, 1, \infty) \to (H, \Sigma, 0, 1, \infty)$ be two morphisms in **s3tGroup**, and suppose $\Phi = \Psi$. Now, let $x \in G$ and $\alpha \in \Omega$. Since (f, Φ) and (g, Φ) are morphisms in **s3tGroup**, we have $f(x)\Phi(\alpha) = \Phi(x(\alpha)) = g(x)\Phi(\alpha)$. For $\alpha \in \{0, 1, \infty\}$, this implies we must have $f(x)(0) = g(x)(0)$, $f(x)(1) = g(x)(1)$, and $f(x)(\infty) = g(x)(\infty)$. Now, each of $g(x)(0)$, $g(x)(1)$, and $g(x)(\infty)$ must be distinct since the base points are distinct. By the sharp 3-transitivity of H on Σ, $g(x)$ is the unique element of H such that $0 \mapsto g(x)(0)$, $1 \mapsto g(x)(1)$, and $\infty \mapsto g(x)(\infty)$. Thus, we must have $f(x) = g(x)$, hence $f = g$. □

3. The categorical equivalences

In this section, we show that there are categorical equivalences (1) **RPS** $\simeq$ **Loop** (Theorem 3.4); (2) **s2tGroup** $\simeq$ **nDomain** (Theorem 3.9); and (3) **s3tGroup** $\simeq$ **KTfield** (Theorem 3.13). The first two equivalences were first proved in [1]. We review their development for completeness (especially since we understand the third equivalence in terms of the first two), using Lemmas 2.1 and 2.4 to provide alternate, more concise proofs. We then exhibit the close relationship between these equivalences with a diagram of functors in Theorem 3.14.

3.1. Regular permutation sets and loops

Given a loop L, constructing an object of **RPS** is relatively straightforward. Denote $T_1 L = \{\lambda_a : x \mapsto ax \mid x, a \in L\}$ the set of left translations of L. Then $(T_1 L, L, e)$ is a regular permutation set ([1] Property 2.5). As we see in the next proposition, this construction is functorial.

Proposition 3.1. *There is a functor* $T_1 \colon$ **Loop** $\to$ **RPS**.

Proof. For L a loop, define $T_1 L$ as above. For a loop homomorphsim $f \colon L \to L'$, if we define $T_1 f \colon \lambda_a \mapsto \lambda_{f(a)}$, it can be shown that T_1 is a functor. □

Constructing a loop out of a regular permutation set is a little more subtle. Let $(M, \Omega, *)$ be a regular permutation set. Ultimately, we would like to find a loop structure on Ω. We do so by first building a loop out of M (which, being

a set of permutations, comes with a little more structure than Ω), and importing the structure on M to Ω.

While composition of functions is the obvious operation on $\mathrm{SYM}\Omega$, there is no guarantee that the subset $M \subseteq \mathrm{SYM}\Omega$ is closed under this operation. However, since the action of M on Ω is regular, the map $\mu\colon M \to \Omega$ defined by $m \mapsto m(*)$ is a bijection. We define the operation $\otimes_* : M \times M \to M$ so that the following diagram commutes:

$$\begin{array}{ccccc} M \times M & \xhookrightarrow{i \times i} & & & \mathrm{SYM}\Omega \times \mathrm{SYM}\Omega \\ {\scriptstyle \otimes_*}\big\downarrow & & & & \big\downarrow{\scriptstyle \circ} \\ M & \xleftarrow[\mu^{-1}]{\cong} & \Omega & \xleftarrow[\mathrm{ev}(-,*)]{} & \mathrm{SYM}\Omega. \end{array}$$

Explicitly, we have $\otimes_* : (m, n) \mapsto \mu^{-1}(m \circ n(*))$. It can be shown that M is a loop under $\otimes_*$ with identity id_Ω. Furthermore, if M is a subgroup of $\mathrm{SYM}\Omega$, then $(M, \otimes_*) = (M, \circ)$ (cf. [1] Property 2.1).

We use μ to define an operation $\cdot_*$ on Ω by the following commutative diagram:

$$\begin{array}{ccc} \Omega \times \Omega & \xrightarrow[\cong]{\mu^{-1} \times \mu^{-1}} & M \times M \\ {\scriptstyle \cdot_*}\big\downarrow & & \big\downarrow{\scriptstyle \otimes_*} \\ \Omega & \xleftarrow[\mu]{\cong} & M. \end{array}$$

Explicitly, we have $\cdot_*\colon (\alpha, \beta) \mapsto \mu^{-1}(\alpha)(\beta)$.

Proposition 3.2. *For Ω and $\cdot_*$ as above, Ω is a loop under $\cdot_*$ with identity $*$, and $\mu : M \to \Omega$ is a loop isomorphism. In particular, if M is a subgroup of $\mathrm{SYM}\Omega$, then $(\Omega, \cdot_*)$ is a group. Furthermore, if $(f, \Phi)\colon (M, \Omega, *) \to (N, \Sigma, *)$ is a morphism in* **RPS**, *then $\Phi\colon \Omega \to \Sigma$ is a homomorphism of loops.*

Proof. See [1] Property 2.2 and Corollary 2.4. □

This lets us define two functors **RPS** $\to$ **Loop**:

- $P_\otimes\colon$ **RPS** $\to$ **Loop** sends $(M, \Omega, *) \mapsto (M, \otimes_*)$ and $(f, \Phi) \mapsto f$.
- $P\colon$ **RPS** $\to$ **Loop** sends $(M, \Omega, *) \mapsto (\Omega, \cdot_*)$ and $(f, \Phi) \mapsto \Phi$.

These functors are naturally equivalent, as shown in the following proposition:

Proposition 3.3. *There is a natural equivalence $\mu\colon P_\otimes \xrightarrow{\cong} P$.*

Proof. For any regular permutation set $(M, \Omega, *)$, define $\mu_M : M \to \Omega$ as the composite $M \xrightarrow{(\mathrm{id}, *)} M \times \Omega \xrightarrow{\mathrm{ev}} \Omega$. As we have seen in Proposition 3.2, $\mu_M : (M, \otimes_*) \xrightarrow{\cong} (\Omega, \cdot_*)$ is a loop isomorphism.

We are left to show that this construction is natural. Consider a morphism of regular permutation sets $(f, \Phi) : (M, \Omega, *) \to (N, \Sigma, *)$. By [1] Property 2.3, we have $\Phi \circ \mu_M = \mu_N \circ f$ witnessing the naturality of μ. □

Finally, we have the following theorem:

Theorem 3.4 (Cara–Kieboom–Vervloet [1]). *The functors* $P\colon \mathbf{RPS} \rightleftarrows \mathbf{Loop} : T_1$ *constitute an equivalence of categories. Moreover,* **Loop** *is a deformation retract of* **RPS**.

Proof. See [1] Theorem 2.6 for a proof that $PT_1 = \mathrm{id}_{\mathbf{Loop}}$. The fact that P is faithful follows from Lemma 2.4, and the full result then follows from Lemma 2.1. □

In light of Proposition 3.2, we have the following corollary:

Corollary 3.5. *The equivalence of categories* $P\colon \mathbf{RPS} \rightleftarrows \mathbf{Loop} : T_1$ *restricts to an equivalence of categories* **s1tGroup** $\rightleftarrows$ **Group**. *Thus, we have the following commutative diagram of functors:*

$$\begin{array}{ccc} \mathbf{Group} & \xrightarrow{\simeq} & \mathbf{s1tGroup} \\ \downarrow & & \downarrow \\ \mathbf{Loop} & \xrightarrow[T_1]{\simeq} & \mathbf{RPS}, \end{array}$$

where the vertical functors are inclusions.

3.2. Sharply 2-transitive groups and neardomains

Given a neardomain F, the set of affine transformations is

$$T_2F = \{\langle a, b\rangle : x \mapsto a + bx \mid a, x \in F, b \in F \setminus \{0\}\}.$$

In [2], it is shown that T_2F is a subgroup of $\mathrm{SYM}F$ that acts sharply 2-transitively on F. This construction turns out to be functorial. Compare this with Proposition 3.1.

Proposition 3.6. *There is a functor* $T_2\colon \mathbf{nDomain} \to \mathbf{s2tGroup}$.

Proof. See [2] (6.1) for a proof that $(T_2F, F, 0, 1)$ is a sharply 2-transitive group. To show that T_2 is functorial, consider a morphism of near domains $f\colon F \to F'$. Now define $T_2f\colon T_2F \to T_2F'$ by $\langle a, b\rangle \mapsto \langle f(a), f(b)\rangle$. Then (T_2f, f) is verified to be a morphism in **s2tGroup** in the proof of Theorem 4.1 of [1], and this assignment is easily seen to be functorial. □

Given a neardomain F, the next proposition lets us identify the composite $\mathrm{A}T_2F$ as the set of left translations of the loop $(F, +)$, i.e. $\mathrm{A}T_2F = T_1(F, +)$.

Proposition 3.7. *Let F be a neardomain. Then* $\mathrm{A}T_2F = \{\langle a, 1\rangle \mid a \in F\} = T_1(F, +)$. *Thus, there is a commutative diagram of functors:*

$$\begin{array}{ccc} \mathbf{nDomain} & \xrightarrow{T_2} & \mathbf{s2tGroup} \\ {\scriptstyle (+)}\downarrow & & \downarrow{\scriptstyle \mathrm{A}} \\ \mathbf{Loop} & \xrightarrow[T_1]{} & \mathbf{RPS}, \end{array}$$

where $(+)\colon \mathbf{nDomain} \to \mathbf{Loop}$ *is defined by* $(F, +, \cdot) \mapsto (F, +)$ *and* $f \mapsto f$.

Proof. See [2] (6.5). □

Now consider a sharply 2-transitive group action of a group G on a set Ω (with at least two elements). For two distinct base points $0, 1 \in \Omega$, consider the regular permutation sets $(\mathrm{A}G, \Omega, 0)$ and $(G_0, \Omega \setminus \{0\}, 1)$ (by [2] (1.1)(a)). The functor $P\colon \mathbf{RPS} \to \mathbf{Loop}$ can be used to define two loops, namely $(\Omega, +_0) = P(\mathrm{A}G, \Omega, 0)$ and $(\Omega\setminus\{0\}, \cdot_1) = P(G_0, \Omega\setminus\{0\}, 1)$. Note that, since G_0 is a group, so is $(\Omega\setminus\{0\}, \cdot_1)$ by Proposition 3.2. We can further define $\alpha \cdot_1 \beta = 0$ if either $\alpha = 0$ or $\beta = 0$ to extend the operation $\cdot_1$ to all of Ω. These two operations constitute a neardomain structure on Ω, and with our carefully curated morphisms in **s2tGroup**, we have the following result:

Proposition 3.8. *For a sharply 2-transitive group $(G, \Omega, 0, 1)$, the set Ω equipped with addition $+_0$ and multiplication $\cdot_1$ forms a neardomain $F = (\Omega, +_0, \cdot_1)$. Furthermore, G is of type 0 if and only if char $F = 2$, and if (f, Φ) is a morphism in the category of sharply 2-transitive groups, then Φ is a morphism of neardomains.*

Proof. See [2] (6.2), [3] Section 7.10, and [1] Property 3.9. □

This means we can define a functor $Q\colon \mathbf{s2tGroup} \to \mathbf{nDomain}$ by $(G, \Omega, 0, 1) \mapsto (\Omega, +_0, \cdot_1)$ and $(f, \Phi) \mapsto \Phi$. We now have the following theorem:

Theorem 3.9 (Cara–Kieboom–Vervloet [1])**.** *The functors*
$Q\colon \mathbf{s2tGroup} \rightleftarrows \mathbf{nDomain} :T_2$ *constitute an equivalence of categories. Moreover,* **nDomain** *is a deformation retract of* **s2tGroup**.

Proof. See [1] Theorem 4.1 for a proof that $QT_2 = \mathrm{id}_{\mathbf{nDomain}}$. The fact that Q is faithful follows from Lemma 2.4, and the full result then follows from Lemma 2.1. □

Given a sharply 2-transitive group $(G, \Omega, 0, 1)$, the associated neardomain $(\Omega, +_0, \cdot_1)$ is a nearfield if and only if $\mathrm{A}G$ is a subgroup of G (see the proof of Theorem 4.3 in [1]). Call $\mathbf{s2tGroup}_{\mathrm{A}}$ the full subcategory of **s2tGroup** whose objects $(G, \Omega, 0, 1)$ have $\mathrm{A}G$ a subgroup of G, and call **nField** the full subcategory of **nDomain** whose objects are nearfields. We have the following corollary:

Corollary 3.10 (Cara–Kieboom–Vervloet [1]). *The functors* $Q\colon$ **s2tGroup** $\rightleftarrows$ **nDomain** $:T_2$ *restrict to an equivalence of cateogries* **s2tGroup**$_{\text{A}}$ $\rightleftarrows$ **nField**. *Thus, we have a commutative diagram of functors:*

$$\begin{array}{ccc} \textbf{nField} & \xrightarrow{\simeq} & \textbf{s2tGroup}_{\text{A}} \\ \downarrow & & \downarrow \\ \textbf{nDomain} & \xrightarrow[T_2]{\simeq} & \textbf{s2tGroup}, \end{array}$$

where the vertical functors are inclusions.

Proof. See [1] Theorem 4.3. □

3.3. Sharply 3-transitive groups and KT-fields

Conisder a KT-field F. Let $\infty \notin F$, and call $\overline{F} = F \cup \{\infty\}$. Extend $+$ and $\cdot$ to $\overline{F}$ by $a + \infty = \infty$ and $b \cdot \infty = \infty$ for all $a \in F$ and $b \in F \setminus \{0\}$. Extend σ to an involution on $\overline{F}$ by $\sigma(0) = \infty$ and $\sigma(\infty) = 0$.

For $a \in F$ and $b \in F \setminus \{0\}$, extend $\langle a, b\rangle : F \to F$ to a permutation of $\overline{F}$ by asserting $\infty \mapsto \infty$. Then, by Proposition 3.6, $T_2F = \{\langle a, b\rangle \mid a \in F, b \in F \setminus \{0\}\}$ is a group that acts sharply 2-transitively on $\overline{F} \setminus \{\infty\} = F$.

Now, by [2] Theorems 10.21 and 1.1(b), and [6] Theorem 10.6.16, T_2F is the stabilizer G_∞ of a sharply 3-transitive group G on $\overline{F}$, where $G = \langle T_2F, \sigma\rangle \subseteq \text{SYM}\overline{F}$. Thus, we assign $T_3F = \langle T_2F, \sigma\rangle$. We think of T_3F as generalized fractional affine transformations on F. This construction turns out to be functorial, as shown in the next proposition. Compare this with Propositions 3.1 and 3.6.

Proposition 3.11. *There is a functor* $T_3\colon$ **KTfield** $\to$ **s3tGroup**

Proof. See [2] Theorem 11.1 for a proof that T_3F acts sharply 3-transitively on $\overline{F}$. To verify that T_3 is functorial, consider a morphism of KT-fields $f\colon (F, +, \cdot, \sigma) \to (F', +, \cdot, \sigma')$. Define $T_3f : T_3F \to T_3F'$ by extending $T_2f : \langle a, b\rangle \mapsto \langle f(a), f(b)\rangle$ and $\sigma \mapsto \sigma'$ to a group homomorphism $\langle T_2F, \sigma\rangle \to \langle T_2F', \sigma'\rangle$. Extend f to $\overline{F}$ by saying $f(\infty) = \infty$. We now verify that (T_3f, f) is indeed a morphism in **s3tGroup** between $(T_3F, \overline{F}, 0, 1, \infty)$ and $(T_3F', \overline{F'}, 0, 1, \infty)$. That this assignment is functorial is readily verified.

Notice, since f is a morphism of neardomains, f is necessarily injective and satisfies $f(0) = 0$, $f(1) = 1$, and $f(\infty) = \infty$. Furthermore, char $F = 2$ if and only if char $F' = 2$. Thus, the sharply 2-transitive stabilizers of ∞, T_2F and T_2F', are of the same type.

It remains to show that the following diagram commutes:

$$\begin{array}{ccc} T_3F \times \overline{F} & \xrightarrow{T_3f \times f} & T_3F' \times \overline{F'} \\ \downarrow & & \downarrow \\ \overline{F} & \xrightarrow[f]{} & \overline{F'}. \end{array}$$

This follows from Theorem 3.9 and the fact that, as a KT-field morphism, $\sigma' \circ f = f \circ \sigma$. □

Suppose, now, we have a group G acting sharply 3-transitively on a set Ω with distinct base points $0, 1, \infty \in \Omega$. We know G_∞ acts sharply 2-transitively on $\Omega \setminus \{\infty\}$ by Proposition 2.3, and we can construct the corresponding neardomain $Q(G_\infty, \Omega \setminus \{\infty\}, 0, 1, \infty) = (\Omega \setminus \{\infty\}, +_0, \cdot_1)$. This neardomain can then be fixed up with an appropriate involution σ producing a KT-field as follows: σ is the restriction to $\Omega \setminus \{\infty, 0\}$ of the unique involution $\tau \in G$ sending $1 \mapsto 1$ and $0 \mapsto \infty$ (see [2] (11.2)). The next proposition shows that this construction is functorial.

Proposition 3.12. *There is a functor* R: **s3tGroup** $\to$ **KTfield**.

Proof. Let $(G, \Omega, 0, 1, \infty)$ be a sharply 3-transitive group. Define $R(G, \Omega, 0, 1, \infty)$ to be $(\Omega \setminus \{\infty\}, +_0, \cdot_1, \sigma)$ as described above. Now, consider a morphism (f, Φ): $(G, \Omega, 0, 1, \infty) \to (H, \Sigma, 0, 1, \infty)$ in the category **s3tGroup**. Then G_∞ and H_∞ have the same type, and

$$(f|_{G_\infty}, \Phi|_{\Omega\setminus\{\infty\}}) : (G_\infty, \Omega \setminus \{\infty\}, 0, 1) \to (H_\infty, \Sigma \setminus \{\infty\}, 0, 1)$$

can be verified to be a morphism in **s2tGroup**. Thus,

$$Q(f|_{G_\infty}, \Phi|_{\Omega\setminus\{\infty\}}) = \Phi|_{\Omega\setminus\{\infty\}} \colon \Omega \setminus \{\infty\} \to \Sigma \setminus \{\infty\}$$

is a morphism of neardomains by Proposition 3.8. To show that $\Phi|_{\Omega\setminus\{\infty\}}$ is a morphism of KT-fields, we must verify that the following diagram commutes:

$$\begin{array}{ccc} \Omega \setminus \{\infty, 0\} & \xrightarrow{\Phi|_{\Omega\setminus\{\infty,0\}}} & \Sigma \setminus \{\infty, 0\} \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma'} \\ \Omega \setminus \{\infty, 0\} & \xrightarrow[\Phi|_{\Omega\setminus\{\infty,0\}}]{} & \Sigma \setminus \{\infty, 0\}. \end{array}$$

To start, recall that (f, Φ) is a morphism in **s3tGroup**, so in particular, for every $g \in G$ and $\alpha \in \Omega$, we have $f(g)(\Phi(\alpha)) = \Phi(g(\alpha))$. Now, let $\tau \colon \Omega \to \Omega$ and $\tau' \colon \Sigma \to \Sigma$ be the involutions of G and H, respectively, that restrict to σ and σ', respectively. We note that $f(\tau) = \tau'$ since:

- $f(\tau)f(\tau) = f(\tau^2) = f(\mathrm{id}_\Omega) = \mathrm{id}_\Sigma$, as f is a group homomorphism;
- for $\alpha \in \{0, 1, \infty\}$, $f(\tau)(\alpha) = f(\tau)(\Phi(\alpha)) = \Phi(\tau(\alpha)) = \tau'(\alpha)$.

So, by uniqueness of the choice of τ', we are forced to conclude $f(\tau) = \tau'$.

We then find that for every $\alpha \in \Omega$, we have $f(\tau)(\Phi(\alpha)) = \Phi(\tau(\alpha))$, i.e. $\tau' \circ \Phi = \Phi \circ \tau$. This implies the desired result on the restrictions of these functions to $\Omega \setminus \{\infty, 0\}$. Therefore, we define $R(f, \Phi) = Q(f|_{G_\infty}, \Phi|_{\Omega\setminus\{\infty\}}) = \Phi|_{\Omega\setminus\{\infty\}}$, which is easily verified to be functorial. □

We now prove the main result of this section:

Theorem 3.13. *The functors* $R\colon$ **s3tGroup** $\rightleftarrows$ **KTfield** $:T_3$ *constitute an equivalence of categories. Moreover,* **KTfield** *is a deformation retract of* **s3tGroup**.

Proof. Since $QT_2 = \mathrm{id}_{\mathbf{nDomain}}$, one can readily verify that RT_3 is $\mathrm{id}_{\mathbf{KTfield}}$. Suppose we have $R(f, \Phi) = R(g, \Psi)$ for two morphisms of sharply 3-transitive groups (f, Φ) and (g, Ψ). Then we have $\Phi\,|_{\Omega\setminus\{\infty\}} = \Psi\,|_{\Omega\setminus\{\infty\}}$, and since $\Phi(\infty) = \infty = \Psi(\infty)$, we conclude $\Phi = \Psi$. Lemma 2.4 implies $f = g$, thus R is faithful and the desired result follows from Lemma 2.1. □

3.4. A diagram of categorical equivalences

Far from being ad hoc, the categorical equivalences described above are very closely related to one another. In addition to our functors from the preceding development, we define:

- U : **KTfield** $\to$ **nDomain** is the forgetful functor, sending $(F, +, \cdot, \sigma) \mapsto (F, +, \cdot)$ and $f \mapsto f$;
- $(-)_\infty$: **s3tGroup** $\to$ **s2tGroup** sends $(G, \Omega, 0, 1, \infty) \mapsto (G_\infty, \Omega \setminus \{\infty\}, 0, 1)$ and $(f, \Phi) \mapsto (f|_{G_\infty}, \Phi|_{\Omega\setminus\{\infty\}})$; and
- $(+)$: **nDomain** $\to$ **Loop** sends $(F, +, \cdot) \mapsto (F, +)$ and $f \mapsto f$.

Now, call $\mathcal{A}$ the diagram **KTfield** $\xrightarrow{U}$ **nDomain** $\xrightarrow{(+)}$ **Loop** and call $\mathcal{S}$ the diagram **s3tGroup** $\xrightarrow{(-)_\infty}$ **s2tGroup** $\xrightarrow{\mathrm{A}}$ **RPS**. We have the following theorem:

Theorem 3.14. *There is a (pointwise) natural equivalence* $T\colon \mathcal{A} \xrightarrow{\simeq} \mathcal{S}$.

Proof. The components of T are T_1, T_2, and T_3, as in the commutative diagram of functors:

$$\begin{array}{ccc}
\mathbf{KTfield} & \xrightarrow[T_3]{\simeq} & \mathbf{s3tGroup} \\
{\scriptstyle U}\downarrow & (1) & \downarrow{\scriptstyle (-)_\infty} \\
\mathbf{nDomain} & \xrightarrow[T_2]{\simeq} & \mathbf{s2tGroup} \\
{\scriptstyle (+)}\downarrow & (2) & \downarrow{\scriptstyle \mathrm{A}} \\
\mathbf{Loop} & \xrightarrow[T_1]{\simeq} & \mathbf{RPS},
\end{array}$$

where square (1) commutes by definition of T_3, and square (2) commutes by Proposition 3.7. □

Acknowledgements. I would like to thank Clifton Ealy Jr. for inviting me to give a talk at Western Michigan University on an early version of this note, as well as his valuable assistance in its early development and preparation. Of course, Philippe Cara, Rudger Kieboom, and Tina Vervloet must also be acknowledged, because it is their key insight in [1] that makes the results in the current work possible. Finally, I thank the referee, whose comments and suggestions served to improve the quality of this paper.

References

[1] **P. Cara, R. Kieboom, and T. Vervloet**, *A categorical approach to loops, near-domains, and nearfields*, Bull. Belgian Math. Soc. Simon Stevin, **19** (2012), no. 5, 845 – 857.

[2] **W. Kerby**, *On infinite sharply multiply transitive groups*, Hamburger Mathematische Einzelschriften, no. 6, Vandenhoeck & Ruprecht, Göttingen, 1974.

[3] **H. Kiechle**, *Theory of K-loops*, Lecture Notes Math., **1778** Springer, Berlin 2002.

[4] **S. Mac Lane**, *Categories for the working mathematician*, 2nd ed., Graduate texts in math., **5**, Springer, New York, 1978.

[5] **E. Rips, Y. Segev, and K. Tent**, *A sharply 2-transitive group without a non-trivial abelian normal subgroup*, J. European Math. Soc., **19** (2017), no. 10, 2895 – 2910.

[6] **W. R. Scott**, *Group theory*, Dover Publications, New York, 1987.

Received June 06, 2019

Department of Mathematics
Adrian College
110 South Madison Street
Adrian, Michigan 49221
USA
e-mail: tclark@adrian.edu

Quasigroups and Related Systems **27** (2019), 227 – 250

On the number of autotopies of an n-ary quasigroup of order 4

Evgeny V. Gorkunov, Denis S. Krotov and Vladimir N. Potapov

Abstract. An algebraic system consisting of a finite set Σ of cardinality k and an n-ary operation f invertible in each argument is called an n-ary quasigroup of order k. An autotopy of an n-ary quasigroup (Σ, f) is a collection $(\theta_0, \theta_1, \dots, \theta_n)$ of $n+1$ permutations of Σ such that $f(\theta_1(x_1), \dots, \theta_n(x_n)) \equiv \theta_0(f(x_1, \dots, x_n))$. We show that every n-ary quasigroup of order 4 has at least $2^{[n/2]+2}$ and not more than $6 \cdot 4^n$ autotopies. We characterize the n-ary quasigroups of order 4 with $2^{(n+3)/2}$, $2 \cdot 4^n$, and $6 \cdot 4^n$ autotopies.

1. Introduction

Let Σ be the set of k elements 0, 1, ..., $k-1$. The Cartesian degree Σ^n consists of all tuples of length n formed by elements of Σ. An algebraic system with the support Σ and an n-ary operation $f\colon \Sigma^n \to \Sigma$ invertible in each argument is called an *n-ary quasigroup of order k* (sometimes, for brevity, an n-quasigroup or simply a quasigroup). The corresponding operation f is also called a quasigroup.

An *isotopy* of the set Σ^{n+1} is a tuple $\theta = (\theta_0, \theta_1, \dots, \theta_n)$ of permutations from the symmetric group S_k acting on Σ. The isotopy action on Σ^{n+1} is given by the rule

$$\theta\colon x \mapsto \theta(x) = (\theta_0(x_0), \dots, \theta_n(x_n)) \quad \text{for } x = (x_0, \dots, x_n) \in \Sigma^{n+1}.$$

To denote isotopies and permutations that constitute them, we will use the Greek alphabet, and when writing their action on elements of Σ we sometimes omit parentheses.

Two sets $M_1, M_2 \subseteq \Sigma^{n+1}$ are called *isotopic* if here exists an isotopy θ such that $\theta(M_1) = M_2$. Two quasigroups f and g are called *isotopic* if for some isotopy $\theta = (\theta_0, \theta_1, \dots, \theta_n)$ it holds

$$g(x_1, \dots, x_n) = \theta_0^{-1} f(\theta_1 x_1, \dots, \theta_n x_n). \tag{1}$$

2010 Mathematics Subject Classification: 05B15, 20N05.
Keywords: Multiary quasigroup, latin hypercube, autotopy group
The work was supported by the RFBR grants 10-01-00616, 13-01-00463, and by the Program of Fundamental Scientific Research of the SB RAS No I.5.1., projects No 0314-2019-0016 and No 0314-2019-0017.

If $f = g$, then any isotopy θ for which (1) holds is called an *autotopy* of the quasigroup f. The *autotopy group* $\mathrm{Atp}(f)$ of a quasigroup f is the group consisting of all autotopies of f (the group operation is the composition).

A 2-quasigroup f with *neutral* element e such that $f(e,a) = f(a,e) = a$ for any $a \in \Sigma$ is called a *loop*. If a loop f satisfies the associative axiom $f(x, f(y,z)) \equiv f(f(x,y),z)$, then we have a group. It is known (see, for example, [1]), that all 2-quasigroups of order 4 are isotopic to either the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ or the group $\mathbb{Z}_4$. So, quasigroups generalize groups, which illustrates their algebraic nature.

At the same time, the concept of a quasigroup admits a purely combinatorial interpretation. By *line* in Σ^{n+1}, we mean a subset of n elements that are mutually distinct exactly at one coordinate. For a quasigroup $f\colon \Sigma^n \to \Sigma$, the set $M(f) = \{(x_0, x_1, \ldots, x_n) \in \Sigma^{n+1} \mid x_0 = f(x)\}$ will be called the *code* of the quasigroup f. The term "code" is borrowed from the theory of error correcting codes, in the framework of which the set $M(f)$ is an MDS-code with distance 2 (an equivalent concept, also well known in combinatorics, is the Latin hypercube). The quasigroup code is characterized as a subset Σ^{n+1} of cardinality k^n intersecting each line in exactly one element. This view allows us to see a quasigroup from its combinatorial side. We note that the codes of isotopic quasigroups are isotopic, namely, it follows from (1) that $M(g) = \theta^{-1}(M(f))$.

In this paper, we investigate autotopies of quasigroups of order 4. We establish tight upper and lower bounds on the order of the autotopy group of such a quasigroup. In a way, it is natural that the richest group of autotopies turned out to be for the quasigroups called linear with a structure close to group. Also we characterize the quasigroups with minimum and pre-maximum (that is, next to the maximum) orders of the autotopy group.

The concept of an autotopy is a generalization of a more partial notion of "automorphism" and reflects in some sense the "regularity" or "symmetry" of a quasigroup as a combinatorial object. The study of the transformations of the space mapping the object onto itself is a classic, but at the same time a difficult task, considered in many areas of mathematics. The complexity of such problems is illustrated by Frucht's theorem [2] stating that each finite group is isomorphic to the group of automorphisms of some graph, and also a similar result concerning perfect codes in coding theory [6].

In coding theory, the group of automorphisms of a code is generated by the isometries of the metric space that sitabilize the code. There we find another example of the phenomenon that an object with group properties has the richest group of automorphisms. In papers [5, 8, 9] it is shown that the binary Hamming code, which is a linear perfect code, has the largest automorphism group among the binary 1-perfect codes, and its order at least twice exceeds the order of the automorphism group of any other binary 1-perfect code of the same length.

The paper is organized as follows. Section 2 provides basic definitions and statements. In Section 3, a representation of quasigroups necessary for further proof of the fundamental results is given. Auxiliary statements on the autotopies

of quasigroups are collected in Section 4. A tight lower bound on the number of autotopies of a quasigroup of order 4 is proved in Section 5. In Section 5.2, we discuss the quasigroups with the smallest order of the autotopy group. Finally, in Section 6 an upper bound on the order of the autotopy group of a quasigroup of order 4 is derived and it is proved that this bound is attained only by the linear quasigroups. We also establish the maximum order of the autotopy group of a nonlinear quasigroup of order 4 and prove that it is attained only by isotopically transitive quasigroups, which were described in [4].

2. Notations and basic facts

For $x = (x_1, \dots, x_n) \in \Sigma^n$ and $a \in \Sigma$, we put $x_i^a = (x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n)$. The *inverse* of an n-quasigroup f in the i-th argument is denoted by $f^{\langle i \rangle}$; that is, for any $x \in \Sigma^n$ and $a \in \Sigma$, the equations $f^{\langle i \rangle}(x_i^a) = x_i$ and $f(x) = a$ are equivalent. Obviously, the inversion of an n-quasigroup in any argument is an n-quasigroup. By the 0-th argument of an n-quasigroup f, we mean the value of the function $f(x_1, \dots, x_n)$, which, formally not being an argument of the operation f itself, is associated with the i-th argument of the inverse $f^{\langle i \rangle}$.

In this paper, we study the autotopies of quasigroups of order 4; so, below we assume $\Sigma = \{0, 1, 2, 3\}$. A quasigroup f of order 4 is said to be *semilinear* if there are $a_j, b_j \in \Sigma$, $a_j \neq b_j$, $j = 0, 1, \dots, n$, for which

$$f(\{a_1, b_1\} \times \dots \times \{a_n, b_n\}) = \{a_0, b_0\}. \tag{2}$$

In this case, we also say that the quasigroup f is $\{a_j, b_j\}$-*semilinear in the j-th argument*, for $j = 0, 1, \dots, n$. Note that if in the identity (2) any two of the sets $\{a_j, b_j\}$ are replaced by their complements in Σ, then the identity remains true. Thus, in every argument, a semilinear quasigroup is $\{0,1\}$-, $\{0,2\}$- or $\{0,3\}$-semilinear. If f is $\{a, b\}$-semilinear in each of its arguments, then we call it simply $\{a, b\}$-*semilinear*.

A quasigroup f is *linear* if in each of its arguments it is $\{a, b\}$-semilinear for any $a, b \in \Sigma$.

Each 2-quasigroup is isotopic to one of the two quasigroups $\oplus$, $+_4$ with the value tables

$\oplus$	0	2	1	3
0	0	2	1	3
2	2	0	3	1
1	1	3	0	2
3	3	1	2	0

,

$+_4$	0	2	1	3
0	0	2	1	3
2	2	0	3	1
1	1	3	2	0
3	3	1	0	2

. (3)

The quasigroups $(\Sigma, \oplus)$ and $(\Sigma, +_4)$ are the groups $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$, respectively.

Remark 2.1. In the value tables (3), the elements 0, 2, 1, 3 are not ordered lexicographically, in the usual sense. With the given ordering, it is easier to observe the semilinear structure of the given group. In the future, similarly, the table of

values of a $\{0,2\}$-semilinear n-quasigroup is convenient to be thought as an n-dimensional $4\times\ldots\times 4$ array which is divided into n-dimensional $2\times\ldots\times 2$ subarrays filled with two values 0, 2 or 1, 3.

The quasigroup $\oplus$ iterated $n-1$ times will be denoted by l_n; that is,

$$l_n(x_1,\ldots,x_n)=x_1\oplus\ldots\oplus x_n.$$

Lemma 2.2. (cf. [7])

(*i*) *All linear n-quasigroups are isotopic to l_n.*

(*ii*) *If an n-quasigroup is simultaneously $\{0,1\}$- and $\{0,2\}$-semilinear in some argument, then it is linear.*

Lemma 2.3. *If an n-quasigroup f is $\{a,b\}$-semilinear in the i-th argument for some $i\in\{0,\ldots,n\}$ and $\theta=(\theta_0,\ldots,\theta_n)$ is an isotopy, then the n-quasigroup $\theta(f)$ is $\{\theta_i^{-1}(a),\theta_i^{-1}(b)\}$-semilinear in the i-th argument.*

An n-ary quasigroup f is said to be *reducible* if for some integer m, $2\leqslant m<n$, and permutation $\sigma\in S_n$, there exists a representation f in the form of a repetition-free composition such that

$$f(x_1,\ldots,x_n)=h(g(x_{\sigma(1)},\ldots,x_{\sigma(m)}),x_{\sigma(m+1)},\ldots,x_{\sigma(n)}) \tag{4}$$

(repetition-free means that each variable occurs only once in the right side). Without loss of generality, we can assume that the quasigroup g is irreducible.

In [3], a description of quasigroups of order 4 is obtained in terms of semilinearity and reducibility.

Theorem 2.4. *Every n-ary quasigroup of order 4 is reducible or semilinear.*

3. The representation of quasigroups

According to Theorem 2.4, a non-semilinear quasigroup can be represented as a repeatition-free composition of two or more semilinear quasigroups (some of the composed quasigroups can coincide with each other or be linear). A representation of a quasigroup f in the form of a repeatition-free composition of quasigroups of arity greater than 1 will be called a *decomposition* of f. Note that a quasigroup may have several decompositions. In the simplest case, the quasigroup represents its own trivial decomposition.

In the following, we will use a graphical representation of a decomposition of a quasigroup in the form of a labeled tree. The inner vertices of this tree (the degree of which is not less than 3) will be called *nodes* and denoted by characters u, v, w, with or without indices; and the leaves (vertices of degree 1) will be denoted by symbols of variables x_1, x_2, ..., y, z, etc. The edge incident to a leaf of the tree is called a *leaf* edge. The remaining edges are called *inner*.

Firstly, we define recursively the *root tree* $T(S)$ of a decomposition S (the notion of the root decomposition tree is introduced as an auxiliary term to define the decomposition tree and will not be used after that definition).

1) A variable x_i is associated with the tree consisting of one vertex of degree 0, being the root and labelled by the variable x_i itself.

2) Let a decomposition S be of the form $S = h(S_1, \dots, S_n)$. If the decompositions and/or variables $S_1, \dots, S_n$ correspond to the root trees $T_1, \dots, T_n$, respectively, then we build the tree $T(S)$ as follows. Define a new vertex u as the root of the tree and assign the label h to it. Consistently connect vertex u with the roots of the trees $T_1, \dots, T_n$. The root of the tree T_j, $j \in \{1, \dots, n\}$, is considered as the j-th neighbor of u. On the other hand, the vertex u is considered as the 0-th neighbor of the root of the tree T_j.

By a *decomposition tree* (without "root"), we call the tree obtained by connecting the leaf x_0 as the 0-th neighbor to the root of the tree $T(S)$. The tree of the decomposition S is denoted by $T_0(S)$. The leaf x_0 corresponds to the 0-th argument, i.e., to the value of the quasigroup represented by the decomposition S.

The tree $T_0(S)$ of a decomposition S for a quasigroup f can be treated as the decomposition tree for the code $M(f)$. It is important to understand that only the enumeration of the leaves and of the neighbors of every vertex defines which arguments are independent for the quasigroup f and for every element of the decomposition. Changing this enumeration, we can get the decomposition tree for the inverse of f in any argument. Namely, to get a decomposition for $f^{<i>}$, it is sufficient to take the following. Find the path P from x_0 to x_i. Then for each inner node $u \in P$, swap the labels of its two neighbors laying in this path and replace the label of u by the corresponding inverse. Finally, swap the labels x_i and x_0. The order defined on the neighbors of every node uniquely determines the order of the arguments of the quasigroups in the decomposition and of the represented quasigroup. It is worth to note that as the autotopy groups of a quasigroup and its inverses are isomorphic, from the point of view of the questions considered in the current research, it is not necessary to remember all the time which of the arguments is the 0-th one; so, the 0-th argument will not be emphasized in the most of considerations.

For a decomposition and its tree, define the operation of *merging*. Assume that a decomposition S contains the fragment

$$f_1(S_1, \dots, S_{i-1}, f_2(S_i, \dots, S_{i+n_2-1}), S_{i+n_2}, \dots, S_{n_1+n_2-1}), \tag{5}$$

where $S_1, \dots, S_{n_1+n_2-1}$ are some decompositions and the n_1-quasigroup f_1 and n_2-quasigroup f_2 satisfy the identity

$$g(x_1, \dots, x_{n_1+n_2-1}) \equiv f_1(x_1, \dots, x_{i-1}, f_2(x_i, \dots, x_{i+n_2-1}), x_{i+n_2}, \dots, x_{n_1+n_2-1}) \tag{6}$$

for some $(n_1 + n_2 - 1)$-quasigroup g. The result of merging f_1 and f_2 in S is defined as the decomposition $\widetilde{S}$ obtained from S by replacing the fragment (5) by

$g(S_1, \ldots, S_n)$. Note that we consider a concrete occurrence of (5) in S (in general a fragment can occur more than one time).

Respectively, in the decomposition tree $T_0(S)$, the adjacent nodes u and v labeled by f_1 and f_2 are merged as follows. This pair of nodes is replaced by a new node w labeled by g, whose neighbors are the neighbors of the removed nodes u and v (except u and v themselves). The neighbors of w are assigned the numbers $0, \ldots, n_1 + n_2 - 1$ consequently in the following order. At first, the neighbors of u with the numbers $0, \ldots, i-1$ are assigned (in the same order); next, the neighbors of v with the numbers $1, \ldots, n_2$ are assigned; then, the remaining neighbors of u with the numbers $i+1, \ldots, n_1$ are assigned. The result of the described merging is the decomposition tree $T_0(\widetilde{S})$. Trivially, we have the following fact.

Lemma 3.1. *Being applied to a decomposition, merging does not alter the quasigroup represented by the decomposition.*

We call a decomposition (and its tree) *semilinear* if all involved quasigroups are semilinear.

In a decomposition tree, consider two neighbor nodes u, v with labels f_1, f_2, respectively. Assume that u is the 0-th neighbor of v and v is the i-th neighbor of u. We call the nodes u and v *coherent* if for some $a, b \in \Sigma$ the quasigroup f_1 is $\{a, b\}$-semilinear in the i-th argument and f_2 is $\{a, b\}$-semilinear in the 0-th argument.

Lemma 3.2. *Merging two coherent nodes in a semilinear tree results in a semilinear tree.*

Proof. Let quasigroups f_1 and f_2 of arity n_1 and n_2, respectively, correspond to coherent nodes in a decomposition tree, and (6) holds for some $(n_1 + n_2 - 1)$-ary quasigroup g. To prove the lemma, it suffices to verify that the quasigroup g is semilinear, which is straightforward from (6) and the definition of a semilinear quasigroup. □

We call a semilinear decomposition (and its tree) *proper* if there are no pairs of coherent nodes in the decomposition tree.

Lemma 3.3. *Every quasigroup of order 4 has a proper decomposition.*

Proof. By Theorem 2.4, every n-ary quasigroup of order 4 has a semilinear decomposition. Since there are no more than $n-1$ nodes in the decomposition tree, successively merging pairs of coherent nodes, we obtain a required decomposition in at most $n-2$ steps. □

Remark 3.4. In general, a proper decomposition is not unique and depends on the order of merging. The simplest example of a decomposition that can be merged in two ways is $f(g(h(x_1, x_2), x_3), x_4)$, where f and g are $\{0, 1\}$-semilinear quasigroups, g and h are $\{0, 2\}$-semilinear quasigroups, and f and h are not linear in contrast to g. A proper decomposition of a nonlinear quasigroup does not involve any linear

quasigroups because a node labeled by a linear quasigroup is coherent with each of its neighbors.

Let S be some decomposition, and let its tree $T_0(S)$ have the edge set E. An *isotopy* of the decomposition is a collection $\theta = (\theta_e)_{e\in E}$ of permutations of Σ, acting on S as follows. If a node of $T_0(S)$ has a label f_i and e_j, $j = 0, 1, \dots, n_i$, is the j-th edge incident to this node, then f_i is replaced by f_i', where f_i' is the quasigroup defined by

$$f_i'(x_1, \dots, x_{n_i}) = \theta_{e_0}^{-1} f_i(\theta_{e_1} x_1, \dots, \theta_{e_{n_i}} x_{n_i}). \tag{7}$$

As a result, we get the tree of some decomposition, denoted by $\theta(S)$ and called isotopic to S. The following is straightforward.

Lemma 3.5. *Isotopic decompositions represent isotopic quasigroups. More precisely, if θ is an isotopy connecting decompositions of quasigroups f and f', then*

$$x_0 = f'(x_1, \dots, x_n) = \theta_{e_0}^{-1} f(\theta_{e_1}(x_1), \dots, \theta_{e_n}(x_n)),$$

where e_j is the edge incident to the leaf x_j, $j = 0, 1, \dots, n$.

An *autotopy* of the decomposition S is an isotopy θ such that $\theta(S) = S$. The *support* of an autotopy is the set of edges corresponding to non-identity permutations. We call a proper decomposition (and its tree) *reduced* if every involved quasigroup is $\{0,1\}$- or $\{0,2\}$-semilinear.

Lemma 3.6. *For every quasigroup of order 4, there is an isotopic quasigroup with a reduced decomposition.*

Proof. Consider an n-quasigroup f and construct an isotopic quasigroup with a reduced decomposition. We start with a proper decomposition S of f, which exists by Lemma 3.3. Since the decomposition tree $T_0(S)$ is a bipartite graph, its vertices are divided into two independent parts; the vertices of one part are called even, those of the other part are odd.

Let us find an isotopy θ such that the odd nodes of $\theta(S)$ are $\{0,1\}$-semilinear, while the even nodes are $\{0,2\}$-semilinear. To do this, we define the permutation θ_e for every edge e in the tree $T_0(S)$.

Consider two cases. Firstly, let e connect two nodes, an odd one with a label g and an even one labeled by h. Suppose that g is the i-th neighbor of h, which in turn is the 0-th neighbor of g. Note that if g is $\{0,a\}$-semilinear in the 0-th argument and h is $\{0,b\}$-semilinear in the i-th one, then $a \neq b$ because the decomposition S is proper. In this case, we put $\theta_e(0) = 0$, $\theta_e(1) = a$, $\theta_e(2) = b$, $\theta_e(3) \in \{1,2,3\} \setminus \{a,b\}$.

Now we turn to the other case, where e connects a node labeled by g and its i-th neighbor, a variable x. Suppose g is $\{0,a\}$-semilinear in the i-th argument. Then we set $\theta_e = (1a)$ if the node is in the odd part of $T_0(S)$, and $\theta_e = (2a)$ if the node is in the even part.

Consider the action of the constructed isotopy on the decomposition S. A node of the decomposition tree $T_0(S)$ labeled by f_i will get the label f_i' (see (7)) in the tree $T_0(\theta(S))$. Suppose f_i is $\{0,a\}$-semilinear in the j-th argument. Then, by Lemma 2.3, the quasigroup f_i' is $\{0,1\}$-semilinear in the j-th argument if f_i is an odd node, or $\{0,2\}$-semilinear in the j-th argument if f_i is an even node.

Thus, the decomposition $\theta(S)$ is proper by the definition. By Lemma 3.5, the quasigroup represented by $\theta(S)$ is isotopic to the original quasigroup f. □

4. Autotopies of quasigroups

Let $\pi = (\pi_0, \dots, \pi_m)$ and $\tau = (\tau_0, \dots, \tau_{n-m+1})$ be isotopies. If $\pi_0 = \tau_1$, then we define

$$\pi \dot{\otimes} \tau = (\tau_0, \pi_1, \dots, \pi_m, \tau_2, \dots, \tau_{n-m+1}).$$

Let us consider the n-ary quasigroup f obtained as the composition of an m-quasigroup g and an $(n-m+1)$-quasigroup h:

$$f(x_1, \dots, x_n) = h(g(x_1, \dots, x_m), x_{m+1}, \dots, x_n).$$

We define the action of the operation $\dot{\otimes}$ on the autotopy groups of g and h as follows:

$$\mathrm{Atp}(g)\dot{\otimes}\mathrm{Atp}(h) = \{\pi\dot{\otimes}\tau \mid \pi = (\pi_0, \dots, \pi_m) \in \mathrm{Atp}(g), \\ \tau = (\tau_0, \dots, \tau_{n-m+1}) \in \mathrm{Atp}(h), \pi_0 = \tau_1\}.$$

We restrict ourselves by considering quasigroups of order 4 only; however, the next lemma holds for any other order as well.

Lemma 4.1. *If f is an n-quasigroup represented as the composition*

$$f(x_1, \dots, x_n) = h(g(x_1, \dots, x_m), x_{m+1}, \dots, x_n),$$

then

$$\mathrm{Atp}(f) = \mathrm{Atp}(g)\dot{\otimes}\mathrm{Atp}(h).$$

Proof. Obviously, $\mathrm{Atp}(g)\dot{\otimes}\mathrm{Atp}(h) \leqslant \mathrm{Atp}(f)$. To prove the reverse, consider an autotopy $\theta = (\tau_0, \pi_1, \dots, \pi_m, \tau_2, \dots, \tau_{n-m+1}) \in \mathrm{Atp}(f)$. Let us show that there exists a permutation $\pi_0 = \tau_1 \in S_4$ such that $\pi = (\pi_0, \dots, \pi_m) \in \mathrm{Atp}(g)$, $\tau = (\tau_0, \dots, \tau_{n-m+1}) \in \mathrm{Atp}(h)$, and $\theta = \pi\dot{\otimes}\tau$.

Note that if such a permutation π_0 exists, then it is uniquely defined by the permutations $\pi_1, \dots, \pi_m$, because for every tuple in Σ^n the quasigroup g possesses only one value. Moreover, if we put $\pi_0 = \tau_1$, then $\pi \in \mathrm{Atp}(g)$ if and only if $\tau \in \mathrm{Atp}(h)$. Indeed, the relation $\pi \in \mathrm{Atp}(g)$, by the definition, means that the equations

$$x_0 = h(g(x_1, \dots, x_m), x_{m+1}, \dots, x_n) \text{ and} \\ x_0 = h(\pi_0 g(\pi_1^{-1} x_1, \dots, \pi_m^{-1} x_m), x_{m+1}, \dots, x_n)$$

are equivalent. Applying the autotopy $\theta \in \mathrm{Atp}(f)$, for any tuple $(x_1, \ldots, x_n)$ in Σ^n we get

$$x_0 = h(g(x_1, \ldots, x_m), x_{m+1}, \ldots, x_n) = \\ = \tau_0^{-1} h(\pi_0 g(x_1, \ldots, x_m), \tau_2 x_{m+1}, \ldots, \tau_{n-m+1} x_n).$$

The last equality implies that for any $(t, x_{m+1}, \ldots, x_n) \in \Sigma^{n-m+1}$ it holds

$$h(t, x_{m+1}, \ldots, x_n) = \tau_0^{-1} h(\pi_0 t, \tau_2 x_{m+1}, \ldots, \tau_{n-m+1} x_n).$$

That is, for $\tau_1 = \pi_0$ we have $\tau \in \mathrm{Atp}(h)$.

So, it remains to show that there exists a permutation $\pi_0 \in S_4$ such that $\pi \in \mathrm{Atp}(g)$. Taking into account that $\theta \in \mathrm{Atp}(f)$, we can write that for every $(x_1, \ldots, x_m) \in \Sigma^m$ it holds

$$x_0 = h(g(x), 0, \ldots, 0) = \tau_0^{-1} h(g(\pi_1 x_1, \ldots, \pi_m x_m), \tau_2(0), \ldots, \tau_{n-m+1}(0)). \quad (8)$$

Trivially, the 1-quasigroups

$$q_1(s) = h(s, 0, \ldots, 0), \quad q_2(t) = \tau_0^{-1} h(t, \tau_2(0), \ldots, \tau_{n-m+1}(0))$$

are permutations of Σ. So, (8) can be rewritten as follows:

$$g(x) = q_1^{-1}(q_2(g(\pi_1 x_1, \ldots, \pi_m x_m))).$$

Defining $\pi_0(\cdot) = q_2^{-1}(q_1(\cdot))$, we have $(\pi_0, \ldots, \pi_m) \in \mathrm{Atp}(g)$. □

Lemma 4.1 and the results of the previous section allows us to make the following observation. Studying the autotopy group of a quasigroup of order 4, we can assume it to be represented as a repetition-free composition of quasigroups, where each of the quasigroups is $\{0, a\}$-semilinear for some $a \in \Sigma$, but not linear.

In the remaining part of this section, we prove three lemmas on minimum autotopy groups of semilinear quasigroups. In the description of autotopies, it is convenient to use the following notation.

For a nonlinear $\{0, a\}$-semilinear quasigroup f (and the corresponding nodes of decomposition trees), $a \in \Sigma \setminus \{0\}$, the permutation $(0a)(bc)$, where $\{b, c\} = \Sigma \setminus \{0, a\}$, is called the *native involution*, and the permutations $(0b)(ca)$ and $(0c)(ab)$ are called the *foreign involutions*. Each of the transpositions $(0a)$ and (bc) forming the native involution $(0a)(bc)$ is called a *native transposition* of the semilinear quasigroup (node). The two cyclic permutations $(0bac)$ and $(0cab)$ whose square is the native involution $(0a)(bc)$ are called the *native cycles* of the semilinear quasigroup (node).

Lemma 4.2. *The following isotopies belong to the autotopy group of a $\{0, a\}$-semilinear n-ary quasigroup f, $a \in \Sigma \setminus \{0\}$.*

(i) *An isotopy consisting of two native involutions and $n-1$ identity permutations, in an arbitrary order.*

(ii) *An isotopy consisting of $n+1$ native transpositions all of which differ from $(0a)$ in the case $f(\{0,a\}^n)=\{0,a\}$, and exactly one of which equals $(0a)$ in the case $f(\{0,a\}^n)=\Sigma\backslash\{0,a\}$.*

Proof. Without loss of generality we assume $a=1$. The identity (2) holds for any $\{a_i,b_i\}$ from $\{\{0,1\},\{2,3\}\}$, $i=1,\dots,n$ (the pair $\{a_0,b_0\}$ is uniquely defined from the other pairs and also coincides with $\{0,1\}$ or $\{2,3\}$).

(i) Applying the native involution $(01)(23)$ in one of the arguments changes the values of the quasigroup in all points, but at the same time leaves the sets $\{a_1,b_1\}\times\ldots\times\{a_n,b_n\}$ with the above restrictions in place. It follows from (2) that the values of the quasigroup also change in accordance with the native involution. When applying the native involution in some other argument, we again obtain the original quasigroup.

(ii) Let $f(\{0,1\}^n)=\{0,1\}$. Consider an arbitrary tuple $(x_1,\dots,x_n)$ of values of the arguments and the value x_0 of the quasigroup on this tuple. Among x_0, x_1, $\dots$, x_n, an even number of values belong to $\{2,3\}$. Thus, applying successively the transposition (23) to each of the arguments, we change the value of the quasigroup an even number of times, and the changes do not take the value in a partial point beyond the pair $\{0,1\}$ or the pair $\{2,3\}$. As a result, we get that after applying all transpositions, the value of the quasigroup has not changed. The case $f(\{0,1\}^n)=\{2,3\}$ is treated similarly. □

Lemma 4.3. *Assume that an $\{a,b\}$-semilinear binary quasigroup q of order 4 is not linear. Let ξ be the corresponding native involution. The autotopy group of q consists of the following transformations.*

(i) *The autotopies (Id,ξ,ξ), (ξ,Id,ξ), (ξ,ξ,Id), and the identity autotopy.*

(ii) *The autotopies (τ_0,τ_1,τ_1), (τ_1,τ_0,τ_1), (τ_1,τ_1,τ_0), (τ_0,τ_0,τ_0), where τ_0, τ_1 are the two distinct native transpositions; the choice of τ_0 is unique for q.*

(iii) *The autotopies $(\xi',\varphi_1,\varphi_2)$, $(\varphi_1,\xi'',\varphi_2)$, $(\varphi_1,\varphi_2,\xi''')$, where the pair φ_1, φ_2 is an arbitrary pair of native cycles, for which the permutations $\xi',\xi'',\xi'''\in\{\mathrm{Id},\xi\}$ are uniquely defined.r*

(iv) *The autotopies (τ',ψ_1,ψ_2), (ψ_1,τ'',ψ_2), (ψ_1,ψ_2,τ'''), where the pair ψ_1, ψ_2 is an arbitrary pair of foreign involutions, for which the native transpositions τ', τ'', τ''' are uniquely defined.*

Proof. It can be directly checked that each of the presented isotopies is an autotopy of q. To do this, it is sufficient to consider the $\{0,2\}$-semilinear quasigroup $+_4$ (see Example 4.4 below) because all quasigroups satisfying the hypothesis of the

lemma are isotopic to $+_4$. It is easy to see that the set of presented autotopies is closed under the composition; that is, this set forms a group.

The completeness is checked numerically. There are 4 autotopies of each of the types (i), (ii) and 12 autotopies of each of the types (iii), (iv); totally we have 32 autotopies. On the other hand, we can bound the number of autotopies from the upper side. It follows from the nonlinearity of $+_4$ and Lemma 2.3 that for an arbitrary autotopy (ψ_0, ψ_1, ψ_2) each of the permutations ψ_0, ψ_1, ψ_2 maps $\{0,2\}$ to $\{0,2\}$ or $\{1,3\}$. There are 8 ways to choose ψ_1 meeting this condition, and 8 ways for ψ_2; by the definition of a quasigroup, ψ_0 is determined uniquely from ψ_1 and ψ_2. Moreover, it is easy to check that there is no autotopy with $\psi_1 = \mathrm{Id}$ and $\psi_2 = (01)$. It follows that the order of the autotopy group is less than 64. Hence, this group coincides with the group from the autotopies (i)–(iv). □

Example 4.4. Consider the binary quasigroup $+_4$ defined in (3). The permutation (02)(13) is the native involution for q; the permutations (02) and (13) are the native transpositions for q, and (0123), (0321) are the native cycles. The autotopy group of q is generated by the following (strictly speaking, redundant) set of autotopies:

(i) $((02)(13), (02)(13), \mathrm{Id})$, $((02)(13), \mathrm{Id}, (02)(13))$, $(\mathrm{Id}, (02)(13), (02)(13))$;
(ii) $((13), (13), (13))$;
(iii) $(\mathrm{Id}, (0123), (0321))$;
(iv) $((13), (03)(12), (01)(23))$, $((02), (01)(23), (01)(23))$, $((02), (03)(12), (03)(12))$.

Thus, we know the group of autotopies of the unique, up to isotopy, nonlinear binary quasigroup. In addition, we need examples of semilinear 3- and 4-ary quasigroups with the minimal group of autotopies. We define the n-ary quasigroup $l_n^\bullet$ by the identity

$$l_n^\bullet(x) = \begin{cases} l_n(x) \oplus 2, & \text{if } x \in \{0,2\}^n, \\ l_n(x), & \text{if } x \notin \{0,2\}^n. \end{cases}$$

Lemma 4.5. *If $n \geqslant 3$ then the autotopy group of $l_n^\bullet$ is generated by the autotopies enumerated in Lemma 4.2 and has the order 2^{n+1}.*

We prove Lemma 4.5 for any n. However, we note that only the cases $n = 3$ and $n = 4$ are used in the further discussion. For these cases, the statement of Lemma 4.5 can be checked directly.

Proof. Obviously, the autotopies in Lemma 4.2 have order 2, commute and are linearly independent; whence the order of the group generated by them follows.

The code $M(l_n)$ of the quasigroup l_n is a $2n$-dimensional affine subspace of the vector space over the field GF(2) of two elements with the addition $\oplus$ and trivial multiplication by 0 and 1.

The code $M(l_n^\bullet)$ of $l_n^\bullet$ differs from the affine subspace $M(l_n)$ in the 2^n vertices of the set B_n, where $B_n = M(l_n^\bullet) \backslash M(l_n) = \{(l_n^\bullet(x), x) \mid x \in \{0,2\}^n\}$. Moreover,

$M(l_n)$ is a unique closest (in the sense above) to $M(l_n^\bullet)$ affine subspace, because any other affine subspace of the same dimension differs from $M(l_n)$ in at least $2^{2n-1} \geqslant 4 \cdot 2^n$ vertices. Under the action of an autotopy of $l_n^\bullet$, the code $M(l_n^\bullet)$ is mapped to itself (by the definition), while $M(l_n)$ is mapped to an affine subspace (indeed, it is easy to see that any permutation of Σ is an affine transformation over GF(2)), which is also closest to $M(l_n^\bullet)$. It follows that an autotopy of $l_n^\bullet$ is necessarily an autotopy of l_n. Moreover, it also follows that under the action of such an autotopy the set B_n (the difference between the codes of $l_n^\bullet$ and l_n) is mapped to itself. In particular, every permutation of that autotopy stabilizes the set $\{0, 2\}$, i.e. is one of Id, (02), (13), (02)(23). As it follows from the description of the autotopy group of l_n in Section 6, all such autotopies are combinations of the autotopies listed in Lemma 4.2. □

5. A lower bound and quasigroups attaining it

5.1. The estimation

In this section, we consider an arbitrary quasigroup of order 4 and prove a sharp lower bound for the order of its autotopy group. In particular, the autotopy group of a semilinear quasigroup is rather large. For a reducible quasigroup f, we show that the nodes of its decomposition tree $T_0(f)$ can be grouped into subsets, which we call bunches. Each bunch in $T_0(f)$ consists of nodes of the same parity, i.e. it does not contain any adjacent nodes of the tree $T_0(f)$. A current subgroup of the autotopy group $\mathrm{Atp}(f)$ corresponds to each bunch, and the subgroups corresponding to different bunches are independent.

We now introduce additional notation and definitions concerning the representation of quasigroups in a form of a decomposition tree. Let f be an n-ary quasigroup of order 4 with a reduced decomposition S and the decomposition tree $T = T_0(S)$.

• Let $N = n + 1$ denote the number of leaves in the tree T, and let V be the number of nodes in T.

• A *bald* node is an inner vertex u of the tree T without leaves among the neighbors of u. Let E equal the number of bald nodes in T.

• A *bridge* node, or simply *bridge*, is a vertex u of degree 3 in the tree T that is adjacent to exactly one leaf. The leaf adjacent to the bridge u is called a *bridge* leaf. Let B equal the number of bridges in T.

• A *fork* is a vertex u of degree 3 in the tree T that is adjacent to exactly two leaves. Let F equal the number of forks in T.

• By $G(T)$, we denote the graph with the set of nodes of the tree T taken as the vertex set. Two vertices are adjacent in the graph $G(T)$ if the corresponding nodes are adjacent to the same bridge in T. It is easy to see that $G(T)$ is a forest.

• A *bunch* is a connected component of $G(T)$. Let Γ equal the number of bunches in T.

• For a bunch G in $G(T)$, a leaf x of the tree T belongs to the *leaf set* of G if x is adjacent to some node of T included in G. A bunch of the graph $G(T)$ is called *bald* if its leaf set is empty. Let L equal the number of bald bunches in T.

It is worth to note that a bridge providing a corresponding edge in a bunch G does not belong to G as its vertex. The bridge being a node is contained in another bunch which differs from G. In addition, all bridges providing the edges of the bunch G belong to one of two parts of the bipartite graph T while the nodes of G pertain to the other part of T.

For example, consider the decomposition tree designed in Figure 1. There are one bald node ι, five bridges γ, δ, ζ, η, θ, and one fork β. The nodes form seven bunches, namely $\{\alpha, \beta, \varepsilon, \eta, \iota\}$, $\{\gamma\}$, $\{\delta\}$, $\{\zeta, \theta\}$, $\{\kappa\}$, $\{\lambda\}$, $\{\mu\}$.

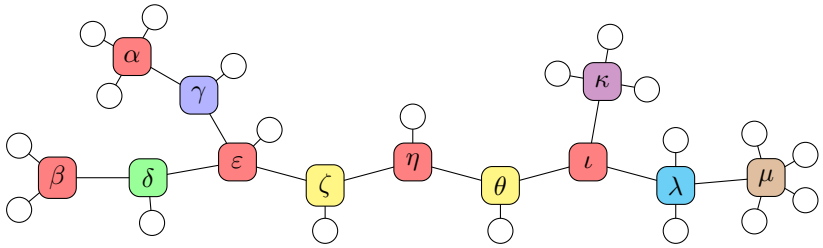


Figure 1: A decomposition tree

Since the number V of nodes in a tree T equals the number of vertices in the forest $G(T)$, the number B of bridges in T equals the number of edges in $G(T)$, and the number Γ of bunches in T equals the number of connected components of $G(T)$, it follows that

$$\Gamma = V - B. \tag{9}$$

It is evident that the number $\Gamma - L$ of non-bald bunches is less than or equal to the number $V - E$ of non-bald nodes. Therefore, the relations $\Gamma - L = V - B - L \leqslant V - E$ hold and from that we get a bound for the number of bald bunches

$$L \geqslant E - B. \tag{10}$$

For two different leaves x and y in the leaf set of a bunch G in the graph $G(T)$, we define an isotopy $\psi^{x,y}$ of the decomposition S in the following way. For any edge of the chain P connecting leaves x and y in the tree T we take the involution $\xi = \xi(G)$ native to the nodes of the bunch G. Each bridge node in the chain P does not belong to G, but is adjacent to two nodes of the bunch G and one leaf z of the tree T. If a bridge v is labeled by f, then for the leaf edge of v we take a native transposition $\tau = \tau(z)$ of the bridge v such that the three permutations ξ, ξ, τ in an appropriate order form an autotopy of the binary quasigroup f. Such a transposition exists by Lemma 4.3(iv). Finally, we take the identity permutation for the remaining edges of the tree T.

Lemma 5.1. *For any two leaves x and y from the leaf set of a bunch in $G(T)$, the isotopy $\psi^{x,y}$ is an autotopy of the decomposition S.*

Proof. Consider a bunch G and any two leaves x and y from the leaf set of G. The nodes of the chain P connecting x and y in the tree T can be partitioned into two parts. The first part consists of the nodes of the bunch G. If $u \in P$ is a node of G, then by construction the isotopy $\psi^{x,y}$ contains the involution $\xi = \xi(G)$ native to u for each of the two edges incident to u in the chain P and identity permutations for all other edges incident to u in the tree T. By Lemma 4.2, such a collection of permutations forms an autotopy of the quasigroup prescribed to the vertex u.

The second part of nodes in the chain P consists of bridges, which do not belong to the bunch G, but provide the edges of G. Let v be such a bridge in the tree T and z be the only leaf of v. By construction, the isotopy $\psi^{x,y}$ contains two foreign to v involutions $\xi(G)$ and a native to v transposition $\tau(z)$ that form an autotopy of the quasigroup prescribed to the vertex v.

For each of the nodes not in the chain P, the isotopy $\psi^{x,y}$ induces the identity autotopy. From these arguments, we conclude that for each node in the tree T, the isotopy $\psi^{x,y}$ yields an autotopy of the quasigroup prescribed to this node. Consistently, $\psi^{x,y}$ is an autotopy of the decomposition S. □

Let us note that a bald bunch, as well as a bunch with only one leaf, do not grant any autotopies of the kind $\psi^{x,y}$.

Lemma 5.2. *If a bunch G contains $k \geqslant 1$ leaves in its leaf set, then there exist at least 2^{k-1} autotopies of the decomposition S acting in the following way: on the edges incident to leaves of G, they act with identity permutations or involutions native to the nodes of G; on the edges that are incident to the leaves of the bridges connecting the nodes of G, they act with identity permutations or transpositions native to the bridges.*

Proof. Let $\{x, y_1, \ldots, y_{k-1}\}$ be the leaf set of the bunch G. Autotopies ψ^{x,y_i}, $i = 1, \ldots, k-1$, of order 2 each commute with each other and are independent from each other since for each i only one of them, namely ψ^{x,y_i} obtains a non-identity permutation for the edge incident to the leaf y_i. Therefore, these $k-1$ autotopies yield 2^{k-1} autotopies corresponding to the bunch G. □

In further, the autotopies of the decomposition S described in Lemma 5.2 are called the *autotopies induced by the bunch G*. All them are of order 2.

If a bunch contains a fork, we can point out autotopies of order 4, which contribute additionally to the size of the autotopy group of the corresponding quasigroup.

Lemma 5.3. *For each fork in a decomposition tree, one can find two autotopies of the decomposition acting on the leaf edges of the fork with its native cycles and on all other edges with identity permutations.*

Proof. Consider a fork u in a decomposition S and let ξ be the native involution of u. Without loss of generality, we assume that the node adjacent to the fork u is its 0-th neighbor, while the leaves x and y of u are the 1-st and 2-nd neighbors respectively. For each pair φ_1, φ_2 of cycles native to u, by Lemma 4.3 there exists exactly one permutation $\xi' \in \{\mathrm{Id}, \xi\}$ such that the triple $\varphi = (\xi', \varphi_1, \varphi_2)$ forms an autotopy of the quasigroup f prescribed to the fork u.

If $\xi' = \mathrm{Id}$ then φ and φ^{-1} are required autotopies of f, which can be finished up to autotopies of the decomposition S by use of identity permutations. If $\xi' = \xi$, then one can take the isotopy $(\xi', \varphi_1, \varphi_2)(\xi, \xi, \mathrm{Id}) = (\mathrm{Id}, \varphi_1\xi, \varphi_2)$ instead of φ. By Lemma 4.3, the former is also an autotopy of the quasigroup f with its native cycles $\varphi_1\xi$ and φ_2. □

Lemma 5.4. *For any decomposition, its non-identity autotopies induced by different bunches of the decomposition tree are independent and commute with each other.*

Proof. Consider a decomposition S with the tree T and two autotopies of S. If the supports of the autotopies intersect in the empty set, then they are trivially independent and commute with each other. At the same time, the supports of autotopies induced by different bunches of $G(T)$ can intersect only in edges of bridge nodes. Indeed, according to Lemma 5.3, the support of the autotopy corresponding to a fork does not exceed the set of leaf edges of the fork. As while as the support of an autotopy $\psi^{x,y}$ induced by a bunch G can contain only edges incident to the nodes of G. If there are more than one node in G, then some of the edges in the support of $\psi^{x,y}$ are also inner edges of bridges connecting nodes of G.

Thereby, it is sufficient to prove the lemma for autotopies induced by different bunches with supports intersecting in edges incident to bridge nodes. An arbitrary autotopy induced by a bunch G acts on edges in its support in the following way:

- on edges incident to nodes of G, it acts with involutions native to nodes of the bunch G;
- on leaf edges incident to bridges connecting nodes of G, it acts with transpositions native to the bridges.

Assume that a bridge v with a leaf z connects two nodes of the bunch G; and let v be contained in another bunch G'. By Lemma 4.3(iv), all autotopies induced by G contain exactly one of the two transpositions native to v, namely $\tau = \tau(z)$. The transposition τ cannot generate the involution native to the bridge v. Thus, the autotopies induced by the bunch G and the autotopies induced by the bunch G' are independent.

Consider autotopies $\theta = \psi^{x,y}$ and $\theta' = \psi^{x',y'}$ induced by the bunches G and G' respectively. Let the supports of these two autotopies contain edges incident to a bridge v in their intersection. Autotopies θ and θ' act on inner edges of v with involutions $\xi = \xi(G)$ and $\xi' = \xi'(G')$ native to G and G' respectively. Since

involutions (01)(23), (02)(31) and (03)(12) commute with each other, we have $\xi\xi' = \xi'\xi$.

The autotopy θ acts on the leaf edge of the bridge v with the transposition τ, while the autotopy θ' acts on this edge with some involution η' (or the identity permutation, which is considered trivially). Both τ and η' are native to v. It is obvious that, for example, the involution (01)(23) and the transpositions (01) and (23) forming it commute. The same is true for the involutions (02)(31) and (03)(12). Therefore, we get $\tau\eta' = \eta'\tau$.

From the reasoning above it is follows that the autotopies θ and θ' commute on every edge that is contained in the intersection of their supports. This proves commutativity of autotopies of the decomposition S induced by different bunches in its tree. □

Theorem 5.5. *For an arbitrary n-ary quasigroup f of order 4, the following inequality holds:*

$$|\mathrm{Atp}(f)| \geqslant 2^{[n/2]+2}. \tag{11}$$

If $n \geqslant 5$, then this bound is sharp.

Proof. Let the quasigroup f have a reduced decomposition S with the tree T. For each bunch G with $k \geqslant 1$ leaves, by Lemma 5.2 one can construct 2^{k-1} autotopies of f which act on variables corresponding to leaves of the bunch G with permutations of order 2. Taking into account all bunches of the graph $G(T)$ except the bald ones, by use of Lemma 5.4 we get $2^{N-(\Gamma-L)}$ autotopies of f.

In addition, for any fork v in the tree T, by Lemma 5.3 there are 2 autotopies of f which act on variables corresponding to the leaves adjacent to v with cycles native to the fork v. This contributes the factor 2^F to the number of constructed here autotopies of f. In this way, using (9) we obtain

$$|\mathrm{Atp}(f)| \geqslant 2^{N-(\Gamma-L)+F} = 2^{N-V+B+L+F}. \tag{12}$$

Suppose that in the decomposition tree T there are t edges and V_s vertices of degree s, $s = 0, 1, 2, \ldots$. By definition of a quasigroup decomposition and accordingly to notation stabilized above, it can be written $V_1 = N$, $V_2 = 0$. Thus,

$$N + \sum_{s \geqslant 3} sV_s = 2t = 2(N + V - 1).$$

It follows that

$$N + 2V - 2 = \sum_{s \geqslant 3} sV_s = 4\sum_{s \geqslant 3} V_s + \sum_{s \geqslant 5}(s-4)V_i - V_3 \geqslant 4V - V_3. \tag{13}$$

Consequently, the inequality $N \geqslant 2V - V_3 + 2$ holds.

In accordance with the number of adjacent leaves, the nodes of degree 3 in the tree T are partitioned into forks, bridge nodes, and bald nodes (there are no

vertices of degree 3 with three adjacent leaves since $n > 2$). Trivially, the number of bald nodes of degree 3 is not greater than the total number of bald nodes in T. Taking into account (10), we get

$$V_3 \leqslant F + B + E \leqslant F + 2B + L, \tag{14}$$

which allows to rewrite the estimate for N in more detail:

$$N \geqslant 2V - V_3 + 2 \geqslant 2V - F - 2B - L + 2.$$

Hence,

$$-V + B \geqslant -\frac{1}{2}(N + F + L) + 1.$$

Applying this inequality to (12), we derive

$$|\mathrm{Atp}(f)| \geqslant 2^{(N+F+L)/2+1} \geqslant 2^{N/2+1} = 2^{(n+3)/2} \tag{15}$$

Let us note that the second inequality in (15) is strict if and only if the decomposition tree contains a fork or bald node. Since $|\mathrm{Atp}(f)|$ is an integer and the number of autotopies generated by those described in Lemmas 5.2 and 5.3 is a power of 2, we have

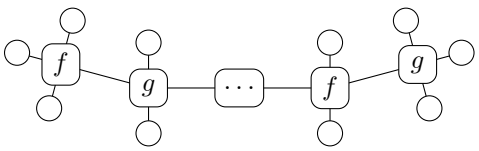
$$|\mathrm{Atp}(f)| \geqslant 2^{\lfloor n/2 \rfloor + 2}. \tag{16}$$

Further, let us show that the bound (16) is attainable. Consider the quasigroups $l_3^\bullet$ and $l_4^\bullet$ in Lemma 4.5, which we denote here by f and h correspondingly, and the quasigroup $x_0 = g(x_1, x_2, x_3) = \tau f(\tau x_1, \tau x_2, \tau x_3)$ with $\tau = (12)$, which is isotopic to the ternary quasigroup f.

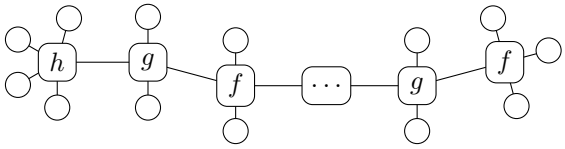
The quasigroups f and g are $\{0, 2\}$- and $\{0, 1\}$-semilinear, respectively. Their autotopy groups are isomorphic to each other, namely one of them is conjugate with the other by the transposition τ. The permutation (01)(23) is a native involution for g, as (01) and (23) are native transpositions of g.

Note that only the identity permutation Id can be met in autotopies of both f and g. The same is true for h and g. Therefore, if f and g (or h and g, respectively) are adjacent in a decomposition tree of some quasigroup q, then by Lemma 4.1 their autotopies can concatenate to an autotopy of the decomposition of q only by the identity permutation.

Reasoning in this way, it is easy to see that for odd $n \geqslant 5$ the quasigroup q_n of arity n with a decomposition tree of kind



has the autotopy group of order $2^{(n-1)/2+2}$. For even $n \geqslant 6$, the quasigroup q_n of arity n with a decomposition tree of kind



has the autotopy group of order $2^{n/2+2}$. In both cases, the equality is attained in (16) for the quasigroups designed. □

Remark 5.6. For $n = 3$ and $n = 4$, the bound pointed out in Theorem 5.5 is not sharp. The quasigroup q_n described in the proof degenerates into a semilinear quasigroup, which has autotopies consisting of its native transpositions (see Lemma 4.5(ii)). Such autotopies are not taken into account in the estimation of Theorem 5.5.

The quasigroup q_n also delivers the minimum for order of autotopy group in the case $n \in \{3, 4\}$. However, in this case the minimum is two times greater than the minimum number in Theorem 5.5. At the same time, any decomposition tree of a reducible quasigroup of arity $n \in \{3, 4\}$ contains a fork. If there are two forks, then the difference can be seen from inequalities in (15). If there is one fork, then by Lemma 4.3(iv) the quasigroup q_n has autotopies with non-identity involution acting on the inner edge of the fork, which are not considered in the proof of Theorem 5.5.

5.2. Quasigroups with autotopy groups of minimum order

Besides the examples of quasigroups described in the proof of Theorem 5.5, there are many other such quasigroups for which the equality is attained in the lower bound given by the theorem. In this section, we characterize quasigroups with this property for n odd. In our reasoning we examine the cases in which all non-strict inequalities occurring in the proof of the theorem turn into equalities. In case of even n, we have not got such an opportunity since we explicitly use the ceil function.

For odd n, the number in the right part of (11) equals $2^{\lfloor n/2 \rfloor+2} = 2^{\frac{n-1}{2}+2} = 2^{\frac{n+3}{2}}$. Based on the proof of Theorem 5.5, for odd n one can derive properties of reduced decompositions with exactly $2^{\frac{n+3}{2}}$ autotopies. The tree of such a decomposition does not contain:

(I) any vertices of degree greater than 4 (this follows from the equality in (13)),

(II) any forks (the equality in (15)),

(III) any bald bunches (the equality in (15)),

(IV) greater than one non-bald vertex in each bunch (the equality in (10)),

(V) any bald vertices of degree greater than 3 (the equality in (14)).

Conditions (III)–(V) imply that in a decomposition with exactly $2^{\frac{n+3}{2}}$ autotopies

(III–V) each bunch contains exactly one non-bald node, which can be a bridge or node of degree 4, and possibly some bald nodes of degree 3 as well.

Let us take a reduced decomposition that satisfies the conditions (I)–(V) and label each of its nodes of degree 4 with a ternary quasigroup isotopic to $l_3^\bullet$. This decomposition has only the autotopies considered in the proof of Theorem 5.5, and the corresponding quasigroup meets the bound $2^{\frac{n+3}{2}}$ for the order of the autotopy group. On the other side, the following statement takes place.

Lemma 5.7. *Let S be a reduced decomposition of an n-quasigroup f of order 4 with $|\mathrm{Atp}(f)| = 2^{\frac{n+3}{2}}$. Each node of degree 4 in the decomposition S has a ternary quasigroup isotopic to the quasigroup $l_3^\bullet$ as its label.*

Proof. There exist exactly five ternary quasigroups up to isotopy, variable permutation, and inversion [10]. One of them is linear and another one is non-semilinear. The remaining three quasigroups are semilinear, but not linear. These three are the quasigroups $l_3^\bullet$,

$$g(x_1, x_2, x_3) = x_1 \oplus (x_2 +_4 x_3), \quad \text{and} \quad h(x_1, x_2, x_3) = x_1 +_4 x_2 +_4 x_3.$$

The quasigroup g admits the autotopy $\varphi = ((01)(23), (01)(23), \mathrm{Id}, \mathrm{Id})$ with two involutions foreign to g. The quasigroup h has got the autotopy

$$((01)(23), (01)(23), (01)(23), (01)(23)),$$

consisting of four foreign involutions.

Suppose that the tree T of a decomposition S has a node α labeled with g (the case of h can be handled similarly). We will show that under the assumptions made one can obtain $|\mathrm{Atp}(f)| > 2^{\frac{n+3}{2}}$. With this aim, for the decomposition S we construct a special autotopy consisting of permutations in the transformation φ. It helps us to get the inequality.

Consider the 0-th neighbor of the node α. If it is a leaf, then we prescribe the permutation (01)(23) to the leaf edge. If the neighbor is a node, it belongs to some bunch G. According to (III), the bunch G is not bald and contains at least one leaf x. Assume that a chain P connects the leaf x with the node α in the tree T. Prescribe the permutation (01)(23) to each edge of P. If there is any bridge node in the chain P, which connects two nodes of the bunch G, we prescribe a native transposition to the leaf edge of the bridge accordingly to Lemma 4.3(iv). Next, we do the same construction for the 1-st neighbor of the node α and prescribe the identity permutation to the remaining edges in the tree T.

Finally, we obtain an autotopy θ of the decomposition S because for each node v in T the permutations acting on the edges incident to v form an autotopy of the

quasigroup corresponding to v. In addition, the autotopy θ does not contribute to the number given as a lower bound in Theorem 5.5. Indeed, in the proof of the theorem we consider only those autotopies of the decomposition which act on every edge incident to a node of degree 4 with an involution native to the node. In contrast, the autotopy θ acts on two edges incident to α with the involution (01)(23), which is not native to g. Consequently, θ increases the order of the autotopy group of f; so, $|\mathrm{Atp}(f)| > 2^{\frac{n+3}{2}}$.

If the quasigroups h is prescribed to the node α, then one can construct an additional autotopy of f in the same way. The only difference is that in this case all neighbors of the node α should be considered. □

A decomposition tree satisfying conditions (I)–(V) can be constructed using the following procedure.

Construction T.

Step 1. Take an arbitrary tree T_1 with exactly $(n-1)/2$ vertices, which we call *nodes*. The degree of each node should not exceed 3.

Step 2. Connect $4-i$ new *leaves* to each node of degree $i \in \{1,2,3\}$ in the tree T_1. Degree of each node in the resulting tree T_2 equals 4.

Step 3. Select some (maybe none, maybe all) nodes adjacent to exactly one leaf. Replace each selected node s by two new nodes u_s and v_s of degree 3 adjacent to each other. Four neighbors of v can be distributed among the neighborhoods of u_s and v_s in any of three possible ways. Denote the tree obtained at this step by T_3.

Step 4. Divide the nodes of T_3 into two independent parts V_1 and V_2, which is possible because any tree is a bipartite graph.

Step 5. To each node in the part V_i, $i = 1, 2$, assign a $\{0, i\}$-semilinear quasigroup isotopic to $+_4$ or $l_3^{\bullet}$

Step 6. Finally, choose a leaf to represent the value of the quasigroup, index the neighbors of each node in an appropriate way and get a decomposition tree T of some quasigroup f.

Moreover, it turns out that, for every quasigroup f which meets the bound on the order of its autotopy group, one can build a quasigroup isotopic to f using Construction T.

Theorem 5.8. *Every n-ary quasigroup f with the autotopy group of order $2^{\frac{n+3}{2}}$ is isotopic to some quasigroup with a decomposition tree obtained with Construction T.*

Proof. Let T be a decomposition tree built using the construction. Nodes of degree 3 are combined in pairs "bald node – bridge node" input at Step 3. In each pair, the bald node is included into some bunch, while the bridge node corresponds to an edge of that bunch. Since a bunch is a tree and the number of vertices in a tree is one more than the number of edges, every bunch contains exactly one

non-bald node. By construction, it is a bridge node or node of degree 4. Therefore, the tree T satisfies conditions (I)–(V).

On the other hand, consider a quasigroups f that meets the bound $2^{\frac{n+3}{2}}$ on the order of the autotopy group. Let T be the tree of a decomposition of f. From condition (III–V), it follows that in any bunch the numbers of bald nodes and edges coincide. Consequently, there is a one-to-one correspondence between the bridges and the bald nodes, all of which have degree 3. In addition, we can require that a bridge is adjacent to its corresponding bald node. Shrinking the pairs of corresponding nodes of degree 3 (an operation reverse to Step 3), we get a tree whose all nodes are non-bald and of degree 4. Any such a tree can be obtained at Step 2. By Lemmas 3.5 and 5.7, the node labeling of the decomposition tree T conforms to the labeling at Step 5. □

6. An upper bound

In this section, we prove that the maximum order of the autotopy group of an n-ary quasigroup of order 4 equals $6 \cdot 2^n$, and only the linear quasigroup, which is unique up to isotopy, reaches the upper bound. We also determine the quasigroups that have the maximum order of autotopy groups among the nonlinear quasigroups and point out this order as well.

Here we use Orbit–Stabilizer Theorem. In our case, this theorem says that the order of the autotopy group of a code M equals the size of the stabilizer of any element $x \in M$ multiplied by size of the orbit of x under the action of the autotopy group. Let us start with several auxiliary statements concerning autotopies of a n-ary quasigroups that stabilize a certain element in the quasigroup code. For simplicity, that element is usually considered to be the all-zero tuple $(0, \dots, 0)$. The next lemma takes place for a quasigroup of any order k.

Lemma 6.1. *Let f be an n-quasigroup and $f(0, \dots, 0) = 0$. Then an arbitrary autotopy $(\theta_0, \dots, \theta_n) \in \mathrm{Atp}(f)$ stabilizing the all-zero tuple is uniquely determined by any single of its permutations θ_i, $i \in \{0, \dots, n\}$. In particular, if for some $i \in \{0, \dots, n\}$ the permutation θ_i is identity, then all the others are also identity.*

Proof. Without loss of generality, given the permutation θ_0, we express the permutations $\theta_1, \dots, \theta_n$ in terms of it.

Assume that $(\theta_0, \dots, \theta_n)$ is an autotopy of f such that $\theta_i 0 = 0$, $i = 0, 1, \dots, n$. By the

By the autotopy definition, we get

$$\theta_0^{-1} f(\theta_1 x_1, 0, \dots, 0) = f(x_1, 0, \dots, 0) \quad \text{for any } x_1 \in \Sigma,$$

which is equivalent to

$$\theta_1 x_1 = f^{<1>}(\theta_0 f(x_1, 0, \dots, 0), 0, \dots, 0) \quad \text{for any } x_1 \in \Sigma.$$

One can see that the permutation θ_1 is entirely determined by the quasigroup f and permutation θ_0. In the same manner, we can express any of $\theta_0, \ldots, \theta_n$ through any other one.

Finally, by the argumentation above it is evident that, for example, $\theta_0 = \mathrm{Id}$ imply $\theta_i = \mathrm{Id}$ for any $i \in \{1, \ldots, n\}$. □

Corollary 6.2. *If an autotopy $\theta = (\theta_0, \ldots, \theta_n)$ of an n-quasigroup f stabilizes a tuple $(a_0, \ldots, a_n)$ from $M(f)$, then all of the permutations θ_i, $i = 0, \ldots, n$, have the same order.*

Proof. By the hypothesis, $(a_0, \ldots, a_n) \in M(f)$; that is $a_0 = f(a_1, \ldots, a_n)$. Consider the quasigroup g defined as

$$g(x_1, \ldots, x_n) = \tau_0 f(\tau_1 x_1, \ldots, \tau_1 x_n),$$

where $\tau = (\tau_0, \ldots, \tau_n)$ is an isotopy consisting of the transpositions $\tau_i = (0\, a_i)$, $i = 0, \ldots, n$. It is easy to verify that $g(0, \ldots, 0) = 0$ and the isotopy

$$\delta = \tau\theta\tau = (\tau_0\theta_0\tau_0, \ldots, \tau_n\theta_n\tau_n),$$

conjugate to θ, is an autotopy of g stabilizing the all-zero tuple.

By Lemma 6.1, for any integer r, all permutations from the autotopy δ^r are identity if there is at least one identity permutation among them. Consequently, all permutations δ_i, $i = 0, \ldots, n$, have the same order.

It remains to note that the permutations δ_i, θ_i are of the same order because $\delta_i^r = \tau\theta_i^r\tau$, $i = 0, \ldots, n$. □

Lemma 6.3. *Let f be an n-quasigroup of order 4 such that $f(0, \ldots, 0) = 0$. If f has an autotopy θ of order 2 that stabilizes the all-zero tuple, then f is semilinear.*

Proof. By Corollary 6.2, each of the permutations θ_i, $i = 0, \ldots, n$, has order 2. Since $\theta_i(0) = 0$ for each $i = 0, \ldots, n$, we have $\theta_i \in \{(12), (13), (23)\}$. Without loss of generality, assume that $\theta_0 = \ldots = \theta_n = (23)$ (otherwise, consider a quasigroup isotopic to f that has the autotopy consisting of permutations (23)).

For every $(x_1, \ldots, x_n)$ from $\{0,1\}^n$ and for $x_0 = f(x_1, \ldots, x_n)$, we have

$$x_0 = f(x_1, \ldots, x_n) = \theta_0^{-1} f(\theta_1 x_1, \ldots, \theta_n x_n) = \theta_0 f(x_1, \ldots, x_n) = \theta_0 x_0.$$

Since $\theta_0 = (23)$, the value of x_0 can only be 0 or 1. Therefore, the quasigroup f maps $\{0,1\}^n$ to $\{0,1\}$. So, f is semilinear by the definition. □

Lemma 6.4. *Let f be an n-quasigroup of order 4 such that $f(0, \ldots, 0) = 0$. If f has an autotopy θ of order 3 that stabilizes some tuple $(a_0, \ldots, a_n) \in M(f)$, then f is linear.*

Proof. By Corollary 6.2, each of the permutations θ_i, $i = 0, \ldots, n$, has order 3.

(i) If f is $\{0,1\}$-, $\{0,2\}$-, or $\{0,3\}$-semilinear in every variable, then it is $\{a,b\}$-semilinear for any $a \neq b \in \Sigma$ and, consequently, linear. Hence, the lemma is true for semilinear quasigroups.

(ii) Assume f is not semilinear. Consider a proper decomposition S of f and the corresponding tree T. The autotopy δ of S induced by θ has the same order 3. Therefore, δ consists of 3-cycles or identity permutations. Each of those permutations stabilizes some element in Σ.

Consider an arbitrary non-bald node v labeled by a quasigroup g. The autotopy of g induced by δ satisfies the hypothesis of Corollary 6.2; so, each of its permutations has order 3. Since S is a proper decomposition, g is semilinear, and from item (i) of this proof we conclude that it is linear. This contradicts the definition of a proper decomposition. □

Theorem 6.5. *(i) The maximum order for an autotopy group of an n-ary quasigroup of order 4 equals $6 \cdot 4^n$; only the linear quasigroups reach this maximum. (ii) The maximum order for an autotopy group of a nonlinear n-ary quasigroup of order 4 equals $2 \cdot 4^n$; only the semilinear quasigroups whose autotopy group acts transitively on their codes reach this maximum.*

Proof. Consider an arbitrary n-ary quasigroup f of order 4. Without loss of generality, we assume that $f(0, \ldots, 0) = 0$.

By Orbit–Stabilizer Theorem, the order of $\mathrm{Atp}(M(f))$ equals the size of its stabilizer subgroup with respect to $(0, \ldots, 0) \in M(f)$ multiplied by the size of the orbit of $(0, \ldots, 0)$ under the action of $\mathrm{Atp}(M(f))$.

For the all-zero tuple, the size of its orbit does not exceed the cardinality of $M(f)$, i.e., 4^n (the equality takes place if and only if the orbit coincides with the code; in other words if the action of the autotopy group is transitive on the code.)

Next, consider the size of the stabilizer with respect to the all-zero tuple. For a non-semilinear quasigroup, it equals 1 by Lemmas 6.3 and 6.4. As for a semilinear quasigroup that is not linear, the size of the stabilizer is 2 (at least 2 by Lemma 4.5; at most 2 by Lemmas 6.1 and 6.4). So, (ii) is proved.

Since any linear quasigroup is isotopic to the quasigroup $l_n(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n$, it remains to find $|\mathrm{Atp}(l_n)|$. For an arbitrary tuple $(a_0, \ldots, a_n) \in M(l_n)$, the mapping $(x_0, \ldots, x_n) \mapsto (x_0 \oplus a_0, \ldots, x_n \oplus a_n)$ maps $(0, \ldots, 0)$ to $(a_0, \ldots, a_n)$ and induces an autotopy of l_n. Hence, the size of the orbit of $(0, \ldots, 0)$ equals 4^n.

The size of the stabilizer with respect to $(0, \ldots, 0)$ is at most 3! by Lemma 6.1. On the other hand, for each of 3! permutations θ_* of Σ such that $\theta_*(0) = 0$, we have ab autotopy $\theta = (\theta_*, \ldots, \theta_*)$ (this can be checked by induction on the arity n). Therefore, the size of the stabilizer equals 6, and the order of the autotopy group of any linear n-ary quasigroup of order 4 is $6 \cdot 4^n$. □

In conclusion, we should note that the semilinear n-ary quasigroups with transitive autotopy groups were characterized in [4], where a correspondence between

such quasigroups and Boolean polynomials of degree at most 2 was established.

References

[1] **V.D. Belousov**, *n-Ary Quasigroups*, (Russian), Shtiintsa, Kishinev, 1972.

[2] **R. Frucht**, *Herstellung von graphen mit vorgegebener abstrakter gruppe*, Compos. Math. **6** (1938), 239 – 250.

[3] **D.S. Krotov, V.N. Potapov**, *n-Ary quasigroups of order* 4, SIAM J. Discrete Math. **23** (2009), no. 2, 561 – 570.

[4] **D.S. Krotov, V.N. Potapov**, *Constructions of transitive latin hypercubes*, Eur. J. Comb. **54** (2016), 51 – 64.

[5] **S.A. Malyugin**, *On the order of the automorphism group of perfect binary codes*, (Russian), Diskretn. Anal. Issled. Oper., Ser. 1 **7** (2000), no. 4, 91 – 100.

[6] **K.T. Phelps**, *Every finite group is the automorphism group of some perfect code*, J. Comb. Theory, Ser. A **43** (1986), 45 – 51.

[7] **V.N. Potapov, D.S. Krotov**, *Asymptotics for the number of n-quasigroups of order* 4, Sib. Math. J. **47** (2006), no. 4, 720 – 731.

[8] **F.I. Solov'eva, S.T. Topalova**, *On automorphism groups of perfect binary codes and Steiner triple systems*, Probl. Inf. Transm. **36** (2000), no. 4, 331 – 335.

[9] **F.I. Solov'eva, S.T. Topalova**, *Perfect binary codes and Steiner triple systems with maximum orders of automorphism groups*, (Russian) Diskretn. Anal. Issled. Oper., Ser. 1 **7** (2000), no. 4, 101 – 110.

[10] **V.A. Zinoviev, D.V. Zinoviev**, *Binary extended perfect codes of length* 16 *by the generalized concatenated construction*, Probl. Inf. Transm. **38** (2001), no. 4, 296 – 322.

Received March 03, 2019

Sobolev Institute of Mathematics, pr. Akademika Koptyuga 4, Novosibirsk 630090, Russia
and
Novosibirsk State University, Pirogova 2, Novosibirsk 630090, Russia
E-mails: gorkunov@math.nsc.ru, krotov@math.nsc.ru, vpotapov@math.nsc.ru

Quasigroups and Related Systems **27** (2019), 251 – 266

Retractable finitely supported Cb-sets

Khadijeh Keshvardoost

Abstract. A construction for retractable state-finite automata without outputs has been given by Nagy. Retractable automata are automata all whose sub automata are retracts of it, and retracts are the subobjects whose related inclusion morphism have a left inverse. Studying retracts is an important subject in different branches of mathematics as well as computer science. In this paper, following Nagy's works, we study retractable finitely supported Cb-sets. The category of finitely supported Cb-sets introduced by Pitts is equivalent to one of the presheaf categories of Bazem, Coquand, and Huber. We characterize retractable finitely supported Cb-sets as ones which have a decomposition into retractable components. We also give a description of retractable cyclic finitely supported Cb-sets. Furthermore, recalling the notion of s-separated finitely supported Cb-sets, and support maps, we construct a subcategory of finitely supported Cb-sets consisted of s-separated finitely supported Cb-sets with 2-equivariant support maps, and characterize its retractable objects.

1. Introduction

Let $\mathbb{D}$ be a countable infinite set. A permutation π on $\mathbb{D}$ is said to be *finitary* if it changes only a finite number of elements of $\mathbb{D}$. Consider the group $G = \mathrm{Perm_f}(\mathbb{D})$ of finitary permutations on $\mathbb{D}$, and take a set X with an action of G on it, that is, a G-set. An element $x \in X$ is said to have a *finite support* $C \subseteq \mathbb{D}$ if it is invariant (fixed) under the action of each element π of G which fixes all the elements of C (that is, if $\pi c = c$, for all $c \in C$, then $\pi x = x$).

A G-set X every element of which has a finite support is said to be a *nominal set*. The notion of a nominal set was introduced by Fraenkel in 1922, and developed by Mostowski in the 1930s under the name of Fraenkel-Mostowski hierarchy or briefly FM-sets. The FM-sets were used to prove the independence of the axiom of choice from the other axioms (in the classical Zermelo-Fraenkel (ZF) set theory).

In 2001, Gabbay and Pitts rediscovered those sets in the context of name abstraction. They called them nominal sets, and applied this notion to properly model the syntax of formal systems involving variable binding operations (see [5]). Nominal techniques have also been used in game theory [1], in logic ([4], [9]), in domain theory [11], and in proof theory [12].

In [10], Pitts generalized the notion of nominal sets, by first adding two elements 0,1 to $\mathbb{D}$, then generalizing the notion of a finitary permutation to *finite*

2010 Mathematics Subject Classification: 20M30, 20B30, 54C15, 20M35, 18B20
Keywords: Finitely supported Cb-sets, retractable, retraction, S-set, support.

substitution, and considering the monoid Cb instead of the group G. Then he defined the notion of a support for Cb-sets, sets with an action of Cb on them, and invented the notion of *finitely supported* Cb-sets, as a generalization of nominal sets.

On the other hand, an equivariant map of a Cb-set X onto a sub Cb-set Y of X is called retraction if it leaves the elements of Y fixed. A Cb-set X is called retractable, if for every sub Cb-set Y, there exists a retraction of X onto Y. The notion of retractable plays a crucial role in many areas of mathematics, such as homological algebra, topological spaces, ordered algebraic structures, etc.

The main contribution of this paper is at giving a characterization of retractable finitely supported Cb-sets. In [8], Nagy showed that every retractable cyclic state-finite automaton has a sub automaton with no proper sub automaton called minimal automaton and then in Theorem 2 of [8], he characterized retractable state-finite automata without outputs. We found that every retractable cyclic finitely supported Cb-set has a unique fix-simple sub Cb-set with a unique zero element. In [3], we introduced fix-simple finitely supported Cb-sets with a unique zero element as finitely supported Cb-sets with no proper non-singleton sub Cb-sets. In fact, our fix-simple finitely supported Cb-sets with unique zero palys the role of Nagy's minimal automaton. In Section 4, in Theorem 4.12, by the same scheme of Nagy but different in details and proofs, we characterize retractable finitely supported Cb-sets.

In the following, to have a better scenery of the structure of this paper, we bring a summary of the results of each section. After a brief introduction in Section 1, we bring the basic notions and results about M-sets, sets with an action of a monoid M, and the monoid Cb in Section 2, needed in this paper. Then Section 3 is about retractions of M-sets and a description of decomposable finitely supported Cb-sets is given. Section 4 is devoted to retractable finitely supported Cb-sets and we characterize them. In Section 5, a subcategory of finitely supported Cb-sets is introduced, and its retractable objects are characterized.

2. Preliminaries

This section has devoted to give some basic notions needed in this paper. For more information one can see [2, 3, 7, 10].

2.1. M-sets

A (left) *M-set* for a monoid M with identity e is a set X equipped with a map $M \times X \to X, (m, x) \mapsto mx$, called an *action* of M on X, such that $ex = x$ and $m(m'x) = (mm')x$, for all $x \in X$ and $m, m' \in M$. An *equivariant map* from an M-set X to an M-set Y is a map $f : X \to Y$ with $f(mx) = mf(x)$, for all $x \in X, m \in M$.

An element x of an M-set X is called a *zero* (or a *fixed*) element if $mx = x$, for all $m \in M$. We denote the set of all zero elements of an M-set X by $Z(X)$.

The M-set X all of whose elements are zero is called a *discrete* M-set, or an M-set with *identity action*.

A subset Y of an M-set X is a *sub M-set* (or *M-subset*) of Y if for all $m \in M$ and $y \in Y$ we have $my \in Y$. The subset $Z(X)$ of X is in fact a sub M-set.

An M-set X is said to be *zero-decomposable* if there exists a collection $\{X_i\}_{i\in I}$ of sub M-sets of X such that $X = \bigcup_{i\in I} X_i$, and $X_i \cap X_j = \{\theta\} \in Z(X)$ or $X_i \cap X_j = \emptyset$, for all $i \neq j$. In this case, we say X has a *zero-decomposition* of X_i's and call X_i's the components of X.

Note. If for all $i \neq j$ we have $X_i \cap X_j = \emptyset$, then we call X *decomposable*.

2.2. The monoid Cb

Let $\mathbb{D}$ be an infinite countable set, whose elements are sometimes called *directions* (*atomic names* or *data values*) and Perm$\mathbb{D}$ be the group of all permutations (bijection maps) on $\mathbb{D}$. A permutation $\pi \in \mathrm{Perm}\mathbb{D}$ is said to be *finitary* if the set $\{d \in \mathbb{D} \mid \pi(d) \neq d\}$ is finite. Clearly the set $\mathrm{Perm}_{\mathrm{f}}\mathbb{D}$ of all finitary permutations is a subgroup of Perm$\mathbb{D}$.

Also, we take $\mathsf{2} = \{0, 1\}$ with $0, 1 \notin \mathbb{D}$.

Definition 2.1. (a) A finite *substitution* is a map $\sigma : \mathbb{D} \to \mathbb{D} \cup \mathsf{2}$ for which $\mathrm{Dom}_{\mathrm{f}}\sigma = \{d \in \mathbb{D} \mid \sigma(d) \neq d\}$ is finite.

(b) A finite substitution satisfies *injectivity condition*, if

$$(\forall d, d' \in \mathbb{D}),\ \sigma(d) = \sigma(d') \notin \mathsf{2} \Rightarrow d = d'.$$

(c) If $d \in \mathbb{D}$ and $b \in \mathsf{2}$, we write (b/d) for the finite substitution which maps d to b, and is the identity mapping on all the other elements of $\mathbb{D}$. Each (b/d) is called a *basic substitution*.

(d) If $d, d' \in \mathbb{D}$ then we write $(d\,d')$ for the finite substitution that transposes d and d', and keeps fixed all other elements. Each $(d\,d')$ is called a *transposition substitution*.

Definition 2.2. (a) Let Cb be the monoid whose elements are finite substitutions satisfying injectivity condition, with the monoid operation given by $\sigma \cdot \sigma' = \hat{\sigma}\sigma'$, where $\hat{\sigma} : \mathbb{D} \cup \mathsf{2} \to \mathbb{D} \cup \mathsf{2}$ maps 0 to 0, 1 to 1, and on $\mathbb{D}$ is defined the same as σ. The identity element of Cb is the inclusion $\iota : \mathbb{D} \hookrightarrow \mathbb{D} \cup \mathsf{2}$.

(b) Take S to be the subsemigroup of Cb generated by basic substitutions. The members of S are of the form $\delta = (b_1/d_1) \cdots (b_k/d_k) \in S$ for some $d_i \in \mathbb{D}$ and $b_i \in \mathsf{2}$, and we denote the set $\{d_1, \cdots, d_k\}$ by $\mathbb{D}_\delta$.

Remark 2.3. (1) Notice that each finite permutation π on $\mathbb{D}$, can be considered as a finite substitution $\iota \circ \pi : \mathbb{D} \to \mathbb{D} \cup \mathsf{2}$. Doing so, throughout this paper, we consider the group $\mathrm{Perm}_{\mathrm{f}}\mathbb{D}$ as a submonoid of Cb, and denote $\iota \circ \pi$ with the same notation π.

(2) Let $\delta \in S$, and $\pi \in \mathrm{Perm_f}(\mathbb{D})$. Then, $\pi\delta = \delta'\pi$, and $\delta\pi = \pi\delta''$, where $\mathbb{D}_{\delta'} = \{\pi d : d \in \mathbb{D}_\delta\}$, and $\mathbb{D}_{\delta''} = \{\pi^{-1}d : d \in \mathbb{D}_\delta\}$.

(3) Let $d \neq d' \in \mathbb{D}$ and $b, b' \in 2$. Then

$$(b/d)(b'/d') = (b'/d')(b/d).$$

But, $(1/d)(0/d) = (0/d)$ and $(0/d)(1/d) = (1/d)$, and hence $(1/d)(0/d) \neq (0/d)(1/d)$.

Theorem 2.4. [3] *For the monoid Cb, we have*

$$Cb = \mathrm{Perm_f}(\mathbb{D})S^\iota,$$

where $S^\iota = S \cup \{\iota\}$.

2.3. Finitely supported Cb-sets

In this subsection, basic notions about finitely supported Cb-sets which is needed in the sequel are given, some of which [3, 10].

The following definition introduces the notion of a, so called, *support*, which is the central notion to define finitely supported Cb-sets.

Definition 2.5. (a) Suppose X is a Cb-set. A subset $C \subseteq \mathbb{D}$ *supports* an element x of X if, for every $\sigma, \sigma' \in Cb$,

$$(\sigma(c) = \sigma'(c), (\forall c \in C)) \Rightarrow \sigma x = \sigma' x$$

If there is a finite (possibly empty) support C then we say that x is *finitely supported.*

(b) A Cb-set X whose all elements have finite supports, is called a *finitely supported Cb-set.*

We denote the category of all Cb-sets with equivariant maps between them by Cb-**Set**, and its full subcategory of all finitely supported Cb-sets by $(Cb\text{-}\mathbf{Set})_{\mathrm{fs}}$.

Remark 2.6. Let X be a Cb-set and $x \in X$.

(1) If X is finitely supported, then the set $\{d \in \mathbb{D} \mid (0/d)x \neq x\}$ is in fact the least finite support of x. From now on, we call the least finite support for x *the support* for x, and denote it by $\operatorname{supp} x$.

(2) x is a zero element if and only if $\operatorname{supp} x = \emptyset$ if and only if $\delta x = x$, for all $\delta \in S$.

Example 2.7. (1) The set $\mathbb{D} \cup 2$ is a finitely supported Cb-set, with the *canonical action* given by evaluation; that is,

$$\forall \sigma \in Cb,\ x \in \mathbb{D} \cup 2,\ \sigma x = \hat{\sigma}(x),$$

in which $\hat{\sigma}$ is defined as in Definition 2.2(a). Also, for each $d \in \mathbb{D}$, $\operatorname{supp} d = \{d\}$, and $\operatorname{supp} 0 = \operatorname{supp} 1 = \emptyset$, since both of $0, 1$ are zero elements.

(2) The set $\mathbb{D} \cup \{0\}$ is a finitely supported Cb-set with the action is given by

$$\forall \sigma \in Cb,\ x \in \mathbb{D} \cup \{0\},\ \sigma x = \hat{\sigma}(x).$$

Also, for each $d \in \mathbb{D}$, $\operatorname{supp} d = \{d\}$, and $\operatorname{supp} 0 = \emptyset$, since 0 is a zero element.

(3) All discrete Cb-sets are clearly finitely supported Cb-sets, because of Remark 2.6(2).

Remark 2.8. [3] (1) Every finitely supported Cb-set has a zero element.

(2) Every finite finitely supported Cb-set is discrete.

Lemma 2.9. [3] *Let X be a non-empty finitely supported Cb-set, and $x \in X$. Then*

(i) *$\delta\, x = x$ if and only if $\mathbb{D}_\delta \cap \operatorname{supp} x = \emptyset$.*

(ii) *If $\delta \in S$, then $\operatorname{supp} \delta x \subseteq \operatorname{supp} x \setminus \mathbb{D}_\delta$.*

(iii) *For $\pi \in \operatorname{Perm_f}(\mathbb{D})$, we have $\operatorname{supp} \pi x = \pi \operatorname{supp} x$. In particular,*

$$|\operatorname{supp} \pi x| = |\pi \operatorname{supp} x| = |\operatorname{supp} x|.$$

Remark 2.10. [3] For a finitely supported Cb-set X and $x \in X$, we have

$$S_x \doteq \{\delta \in S \mid \delta x = x\}, \quad S'_x \doteq S \setminus S_x = \{\delta \in S \mid \delta x \neq x\},$$

which they are two subsemigroups of S.

The following lemma is useful in Theorem 2.14.

Lemma 2.11. *Let X be a finitely supported Cb-set, and x a non-zero element of X. Then, S'_x is an ideal of S.*

Proof. Suppose $\delta \in S$ and $\delta_1 \in S'_x$. We show that $\delta\delta_1, \delta_1\delta \in S'_x$. Notice that, since $\delta_1 \in S'_x$, we get $\delta_1 x \neq x$ and so using part (i) of Lemma 2.9, $\mathbb{D}_{\delta_1} \cap \operatorname{supp} x \neq \emptyset$. On the other hand, since $\mathbb{D}_{\delta_1\delta} = \mathbb{D}_{\delta\delta_1} = \mathbb{D}_{\delta_1} \cup \mathbb{D}_\delta$, we get $\mathbb{D}_{\delta\delta_1} \cap \operatorname{supp} x \neq \emptyset$ and $\mathbb{D}_{\delta_1\delta} \cap \operatorname{supp} x \neq \emptyset$. Thus $\delta_1\delta x \neq x$ and $\delta\delta_1 x \neq x$ which means $\delta_1\delta, \delta\delta_1 \in S'_x$. □

Definition 2.12. A cyclic finitely supported Cb-set X is a finitely supported Cb-set which is generated by only one element. That means, it is of the form $Cb\,x$, for some $x \in X$.

Remark 2.13. [3] If Cbx is a non-singleton cyclic finitely supported Cb-set, then

$$Cbx = \operatorname{Perm_f}(\mathbb{D})S'_x x \cup \operatorname{Perm_f}(\mathbb{D})x, \quad \operatorname{Perm_f}(\mathbb{D})S'_x x \cap \operatorname{Perm_f}(\mathbb{D})x = \emptyset.$$

Theorem 2.14. *Let Cbx be a non-singleton cyclic finitely supported Cb-set. Then,*

(i) *$\operatorname{Perm_f}(\mathbb{D})S'_x x$ is a sub Cb-set of Cbx.*

(ii) *If $\operatorname{supp} x = \{d_1, \cdots, d_k\}$, then $\operatorname{Perm_f}(\mathbb{D})S'_x x = \bigcup_{i=1}^{k} Cb(b_i/d_i)x$.*

Proof. First, notice that, since Cbx is non-singleton, we get that $\operatorname{supp} x \neq \emptyset$. So, for all $d \in \operatorname{supp} x$, we have $(0/d)x \in S'_x x$ which means that $\mathrm{Perm_f}(\mathbb{D})S'_x x$ is a non-empty set.

(i) Let $\pi_1\delta_1 x \in \mathrm{Perm_f}(\mathbb{D})S'_x x$ and $\sigma \in Cb$. Then, by Theorem 2.4, we have $\sigma \in \mathrm{Perm_f}(\mathbb{D})$ or $\sigma = \pi\delta$ with $\pi \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta \in S$. If $\sigma \in \mathrm{Perm_f}(\mathbb{D})$, then $\sigma\pi_1\delta_1 x \in \mathrm{Perm_f}(\mathbb{D})S'_x x$. Let $\sigma = \pi\delta$. Then, applying Remark 2.3(2) and Lemma 2.11, we get that

$$\sigma\pi_1\delta_1 x = \pi\delta\pi_1\delta_1 x = \pi\pi_1\delta'\delta_1 x \in \mathrm{Perm_f}(\mathbb{D})S'_x x.$$

(ii) If $d \in \operatorname{supp} x$, then by Lemma 2.9(i), $(b/d) \in S'_x$, and so applying (i), $Cb(b/d)x \subseteq \mathrm{Perm_f}(\mathbb{D})S'_x x$. Thus, $\bigcup_{i=1}^{k} Cb(b_i/d_i)x \subseteq \mathrm{Perm_f}(\mathbb{D})S'_x x$.

To prove the reverse inclusion, let $a \in \mathrm{Perm_f}(\mathbb{D})S'_x x$. Then, there exist $\delta \in S'_x$ and $\pi \in \mathrm{Perm_f}(\mathbb{D})$ with $a = \pi\delta x$. Since $\delta \in S'_x$, by Lemma 2.9(i), we get that $\mathbb{D}_\delta \cap \operatorname{supp} x \neq \emptyset$. Let $d \in \operatorname{supp} x \cap \mathbb{D}_\delta$. Then, $\delta x = \delta_1(b/d)x$ where $\delta_1 \in S$ and $b \in 2$. Thus, $Cb\delta x \subseteq Cb(b/d)x$ which means that $\mathrm{Perm_f}(\mathbb{D})S'_x x \subseteq \bigcup_{i=1}^{k} Cb(b_i/d_i)x$. □

3. Retractions of finitely supported Cb-sets

In this section, we show that a retract of an indecomposable M-set is indecomposable. Theorem 3.6 gives a characterization of retracts of a decomposable finitely supported Cb-set. As a result of this theorem, for finding retractions of a decomposable finitely supported Cb-set, it is sufficient to obtain retractions of its indecomposable sub Cb-sets.

Definition 3.1. Let Y be a (finitely supported) M-set and X a sub M-set of it. Then, X is called *a retract* of Y if there exists an equivariant map $g : Y \to X$, called retraction, such that $g(x) = x$, for all $x \in X$.

Lemma 3.2. ([7], Lemma I.5.36) *Let X be an indecomposable M-set, and $\varphi : X \to Y$ an equivariant map. Then, $\varphi(X)$ is an indecomposable sub M-set of Y.*

Proposition 3.3. *A retract of an indecomposable M-set is indecomposable.*

Proof. Let Y be a retract of an indecomposable M-set X. Then, there exists a retraction $\varphi : X \to Y$. We show that Y is indecomposable. On the contrary, suppose $Y = Y_1 \cup Y_2$ is a decomposition of Y. Since X is indecomposable, by Lemma 3.2, $\varphi(X)$ is indecomposable. So, $\varphi(X) \subseteq Y_1$ or $\varphi(X) \subseteq Y_2$. Assume $\varphi(X) \subseteq Y_1$. Since φ is a retraction and $Y \subseteq X$, we get that

$$Y = \varphi(Y) \subseteq \varphi(X) \subseteq Y_1,$$

which is impossible. Similarly, the case $\varphi(X) \subseteq Y_2$ is impossible. Thus, Y is indecomposable. □

Theorem 3.4. ([7], Theorem I.5.10) *Every M-set has a decomposition into indecomposable sub M-sets.*

Remark 3.5. Let X be a finitely supported Cb-set and Y a sub Cb-set of X. Then, by Theorem 3.4, X has a decomposition into its indecomposable sub Cb-sets. Take $X = \bigcup_\alpha X_\alpha$. Then,

$$Y = Y \cap X = Y \cap (\bigcup_\alpha X_\alpha) = \bigcup_\alpha (Y \cap X_\alpha) = \bigcup_\alpha Y_\alpha,$$

where $Y_\alpha = Y \cap X_\alpha$.

Theorem 3.6. *Let X be a decomposable finitely supported Cb-set, and Y a sub Cb-set of it considered in* Remark 3.5. *Then, Y is a retract of X if and only if*

$$\forall \alpha \quad (Y_\alpha \neq \emptyset \Rightarrow Y_\alpha \quad \textit{is a retract of} \quad X_\alpha).$$

Proof. Suppose $X = \bigcup_\alpha X_\alpha$ and $Y = \bigcup_\alpha Y_\alpha$. Let $\varphi : X \to Y$ be a retraction. Then, $\varphi|_{X_\alpha} : X_\alpha \to Y$ is an equivariant map. Suppose $Y_\alpha \neq \emptyset$. Now, since $Y_\alpha \subseteq X_\alpha$ and φ is a retraction, we get $Y_\alpha \subseteq \varphi(X_\alpha)$. On the other hand, by Lemma 3.2, $\varphi|_{X_\alpha}(X_\alpha) = \varphi(X_\alpha)$ is indecomposable, and so, $\varphi(X_\alpha) = Y_\alpha$. Therefore, $\varphi|_{X_\alpha} : X_\alpha \to Y_\alpha$ is a retraction.

To prove the other part, let Y be a sub Cb-set of X. Then, we show that Y is a retract of X. If $Y_\alpha \neq \emptyset$, then since Y_α is a retract of X_α, we get a retraction $\varphi_\alpha : X_\alpha \to Y_\alpha$. Now, the assignment $\varphi : X \to Y$ defined by

$$\varphi(x) = \begin{cases} \varphi_\alpha(x), & \text{if} \quad x \in X_\alpha \text{ and } Y_\alpha \neq \emptyset \\ \theta \in Y, & \text{if} \quad x \in X_\alpha \text{ and } Y_\alpha = \emptyset \end{cases}$$

is a retraction. □

4. Retractable finitely supported Cb-sets

In this section, we study retractable finitely supported Cb-sets. Discrete finitely supported Cb-sets are retractable. So, we focus on non-discrete finitely supported Cb-sets. As a result of Lemma 4.3, a retractable indecomposable finitely supported Cb-set has a unique zero element. In Theorem 4.12, we give a characterization of a non-discrete retractable finitely supported Cb-set.

Definition 4.1. Let X be a (finitely supported) M-set. Then, X is called *retractable* if every non-empty sub M-set of X is a retract of it.

Remark 4.2. (1) Every sub M-set of a retractable M-set is retractable.

(2) Retracts of a cyclic M-set are cyclic. This is because, if A is a retract of Mx, then there exists a retraction $\varphi : Mx \to A$. Notice that, since φ is surjective, we get $\varphi(Mx) = A$. On the other hand, since φ is equivariant, we get that $\varphi(Mx) = M\varphi(x)$. Therefore, $A = M\varphi(x)$ which means that A is cyclic.

Lemma 4.3. *Let X be an indecomposable retractable M-set with $Z(X) \neq \emptyset$. Then, X has a unique zero element.*

Proof. If $\theta_1 \neq \theta_2 \in Z(X)$, then the sub M-set $\{\theta_1, \theta_2\}$ is a retract of X, and so, there exists a retraction $\varphi : X \to \{\theta_1, \theta_2\}$. Notice that, since X is indecomposable, by Lemma 3.2, $\varphi(X)$ is indecomposable, and so, $\varphi(X) = \theta_1$ or $\varphi(X) = \theta_2$. If $\varphi(X) = \theta_1$, then $\theta_2 = \varphi(\theta_2) = \theta_1$ which is a contradiction. Similarly, $\varphi(X) = \theta_2$ is impossible. □

Corollary 4.4. *A retractable indecomposable finitely supported Cb-set has a unique zero element.*

Proof. It follows by Remark 2.8(1) and Lemma 4.3. □

In characterizing retractable finitely supported Cb-sets, we apply the notion of fix-simple finitely supported Cb-sets with unique zero element introduced and characterized in [3]. A fix-simple finitely supported Cb-set with a unique zero element has no proper non-singleton sub Cb-sets. We called them θ-simple where θ is a notation for a zero element.

First, we recall needed facts of [3]

Theorem 4.5. [3] *For a non-discrete finitely supported Cb-set X with a unique zero element θ, the followings are equivalent:*

(i) *X is θ-simple;*

(ii) *X is a cyclic finitely supported Cb-set of the form of $\mathrm{Perm_f}(\mathbb{D})\, x \cup \{\theta\}$, for some non-zero element $x \in X$. Furthermore, $(b/d)x = \theta$, for all $d \in \operatorname{supp} x$.*

Remark 4.6. [3] Let X be an infinite finitely supported Cb-set with a unique zero element θ, and $x \in X$. Then,

(1) X has a θ-simple sub Cb-set.

(2) If X is simple, then X is θ-simple.

(3) If $X = Cbx$ is cyclic with $|\operatorname{supp} x| = 1$, then X simple.

(4) X is simple if and only if X is θ-simple, and $\operatorname{supp} x \neq \operatorname{supp} x'$, for all non-zero elements $x \neq x'$.

As a result of Theorem 4.5, we get the following corollary.

Corollary 4.7. *All θ-simple (simple) finitely supported Cb-sets are retractable.*

Lemma 4.8. *A retractable non-singleton cyclic finitely supported Cb-set has a unique θ-simple sub Cb-set.*

Proof. Let $X = Cbx$ be retractable with a non-zero element x. Then, by Corollary 4.4, X has a unique zero element θ. Also, by Remark 4.6(1), X has a θ-simple sub Cb-set. Suppose X has two θ-simple sub Cb-sets X_1 and X_2. Applying Theorem 4.5, we get that $X_1 = \mathrm{Perm_f}(\mathbb{D})x_1 \cup \{\theta\}$ and $X_2 = \mathrm{Perm_f}(\mathbb{D})x_2 \cup \{\theta\}$. Since X is retractable, by Remark 4.2, $X_1 \cup X_2$ is a retract of X, and so is cyclic. Therefore, $X_1 = X_2$. □

Proposition 4.9. *Suppose that X is a non-discrete retractable finitely supported Cb-set. Also, suppose $\{B_i\}_{i\in I}$ is the collection of all distinct θ-simple sub Cb-sets of X. Take $X_i = \bigcup_{x\in X}\{Cbx : B_i \subseteq Cbx\}$. Then,*

(i) *every X_i is a retracteble sub Cb-set of X.*

(ii) *every X_i is indecomposable, and has a unique zero element.*

(iii) *for all $i \neq j$, $X_i \cap X_j = \emptyset$ or $X_i \cap X_j = \{\theta\}$.*

(iv) $X = \bigcup_{i\in I} X_i$.

Proof. (i) Let $x \in X_i$ and $\sigma \in Cb$. Then, we show that $\sigma x \in X_i$. Notice that $B_i \subseteq Cbx$. Since X is retractable, by Remark 4.2(1), Cbx is retractable, and so, by Lemma 4.8, Cbx has a unique θ-simple sub Cb-set B_i. Also, since $Cb\sigma x \subseteq Cbx$, we get that $B_i \subseteq Cb\sigma x$, and so, $\sigma x \in X_i$. Now, applying Remark 4.2(1), X_i's are retractable.

(ii) Since $\bigcap\{Cbx : B_i \subseteq Cbx\} = B_i$, we get X_i is indecomposable. Now, since X is retractable, by Remark 4.2(1), X_i is retractable, and so, by Lemma 4.3, has a unique zero element.

(iii) Let $x \in X_i \cap X_j$ with $x \neq \theta$. Then, $Cbx \subseteq X_i \cap X_j$ and so $B_i, B_j \subseteq Cbx$ which contradicts Lemma 4.8 that states Cbx has a unique θ-simple sub Cb-set.

(iv) To prove the non-trivial part, let $x \in X$. Then, since X is retractable, by Remark 4.2(1), Cbx is retractable. Applying Lemma 4.8, there exists a unique θ-simple sub Cb-set B_i with $B_i \subseteq Cbx$. Thus by the assumption $x \in X_i$. □

Lemma 4.10. *Let X be a finitely supported Cb-set with a zero-decomposition of retractable components. Then, X is retractable.*

Proof. Suppose $X = \bigcup X_i$ is a zero-decomposition of retractable finitely supported Cb-sets X_i. Let Y be a sub Cb-set of X. Then, we show that Y is a retract of X. Take $Y_i = Y \cap X_i$. Notice that Y_i is a (possibly empty) sub Cb-set of Y. If $Y_i \neq \emptyset$, then since X_i is retractable, we get a retraction $\varphi_i : X_i \to Y_i$. Now, the assignment $\varphi : X \to Y$ defined by

$$\varphi(x) = \begin{cases} \varphi_i(x), & \text{if} \quad x \in X_i \text{ and } Y_i \neq \emptyset \\ \theta \in Y, & \text{if} \quad x \in X_i \text{ and } Y_i = \emptyset \end{cases}$$

is a retraction. □

Corollary 4.11. *Disjoint union of two retractable finitely supported Cb-sets is retractable.*

In the following theorem, we give a charatcterization of retractable finitely supported Cb-sets.

Theorem 4.12. *Let X be a finitely supported Cb-set. Then, X is retractable if and only if X has a zero-decomposition of retractable components.*

Proof. If X is discrete, then X is retractable and has a zero-decomposition of retractable components. Suppose X is non-discrete and retractable. Also, suppose $\{B_i\}_{i\in I}$ is the collection of all distinct θ-simple sub Cb-sets of X which exist by Lemma 4.8. Take $X_i = \bigcup_{x\in X}\{Cbx : B_i \subseteq Cbx\}$. Then, by Proposition 4.9, $X = \bigcup X_i$ is a zero-decomposition of retractable X_i.

The other part holds by Lemma 4.10. □

The following lemma is needed in Theorem 4.14 which gives a necessary condition for a cyclic finitely supported Cb-set to be retractable.

Lemma 4.13. *If Cbx is a non-singleton retractable cyclic finitely supported Cb-set, then there exists $d \in \operatorname{supp} x$ with $\operatorname{Perm_f}(\mathbb{D})S'_x x = Cb(b/d)x$, where $b \in 2$.*

Proof. Let $\operatorname{supp} x = \{d_1, \cdots, d_k\}$. Then, applying Theorem 2.14(ii), we get that $\operatorname{Perm_f}(\mathbb{D})S'_x x = \bigcup_{i=1}^{k} Cb(b_i/d_i)x$. Since $\operatorname{Perm_f}(\mathbb{D})S'_x x$ is a sub Cb-set of Cbx, and Cbx is retractable, by Remark 4.2, we get that $\operatorname{Perm_f}(\mathbb{D})S'_x x$ is cyclic. So, there exists $a \in \operatorname{Perm_f}(\mathbb{D})S'_x x$ with $\operatorname{Perm_f}(\mathbb{D})S'_x x = Cba$. Since $a \in \operatorname{Perm_f}(\mathbb{D})S'_x x$, there exist $i = 1, \cdots, k$ and $\sigma \in Cb$ with $a = \sigma(b_i/d_i)x$. Applying Theorem 2.4, $\sigma \in \operatorname{Perm_f}(\mathbb{D})$ or $\sigma = \pi\delta$, where $\pi \in \operatorname{Perm_f}(\mathbb{D})$ and $\delta \in S$. If $\sigma = \pi\delta$ and $\delta \in S'_{(b_i/d_i)}$, then $Cba = Cb\delta(b_i/d_i)x$ which is a proper sub Cb-set of $Cb(b_i/d_i)x$. Thus $\operatorname{Perm_f}(\mathbb{D})S'_x x = Cb\delta(b_i/d_i)x$, and so $Cb(b_i/d_i)x \subseteq Cb\delta(b_i/d_i)x$ which is a contradiction. Therefore, $\sigma = \pi$ or $\sigma = \pi\delta$ with $\delta \in S_{(b_i/d_i)}$, and hence, we get that $Cba = Cb(b_i/d_i)x$. □

In Theorem 4.14, we give a description of a retractable cyclic finitely supported Cb-set.

Theorem 4.14. *Suppose Cbx is a cyclic finitely supported Cb-set. Also, suppose $\operatorname{supp} x = \{d_1, \cdots, d_k\}$. If Cbx is retractable, then*

$$Cbx = \operatorname{Perm_f}(\mathbb{D})x \cup \bigcup_{i=1}^{l} \operatorname{Perm_f}(\mathbb{D})(b_i/d_i)\cdots(b_1/d_1)x \cup \{\theta\},$$

where $l \in \{1, \cdots, k\}$ and $d_j \in \operatorname{supp}(b_{j-1}/d_{j-1})\cdots(b_1/d_1)x$, for all $j = 2, \cdots, l$.

Proof. Suppose Cbx is retractable. If $\operatorname{Perm_f}(\mathbb{D})S'_x x = \{\theta\}$, then by Remark 2.13 we get that $Cbx = \operatorname{Perm_f}(\mathbb{D})x \cup \{\theta\}$. Suppose there exists $\delta \in S'_x$ with $\delta x \neq \theta$. By Lemma 4.13, there exist $d \in \operatorname{supp} x$ and $b \in 2$, say $d = d_1$, $b = b_1$, with $\operatorname{Perm_f}(\mathbb{D})S'_x x = Cb(b_1/d_1)x$. So applying Remark 2.13, we have

$$Cbx = \operatorname{Perm_f}(\mathbb{D})x \cup Cb(b_1/d_1)x.$$

By the assumption, Cbx is retractable. So, by Remark 4.2(1), $Cb(b_1/d_1)x$ is retractable. Now, if $\operatorname{Perm_f}(\mathbb{D})S'_{(b_1/d_1)}(b_1/d_1)x = \{\theta\}$, then

$$Cbx = \operatorname{Perm_f}(\mathbb{D})x \cup \operatorname{Perm_f}(\mathbb{D})(b_1/d_1)x \cup \{\theta\}.$$

Otherwise, we show that $\mathrm{Perm_f}(\mathbb{D})S'_{(b_1/d_1)}(b_1/d_1)x = Cb(b_2/d_2)(b_1/d_1)x$, with $d_2 \in \operatorname{supp}(b_1/d_1)x$. Similar to the proof of Theorem 2.14,

$$\mathrm{Perm_f}(\mathbb{D})S'_{(b_1/d_1)}(b_1/d_1)x = \bigcup_j Cb(b_j/d_j)(b_1/d_1)x,$$

where for all j, $d_j \in \operatorname{supp}(b_1/d_1)x$. On the other hand, $Cb(b_1/d_1)x$ is retractable, and so applying Lemma 4.13, $\mathrm{Perm_f}(\mathbb{D})S'_{(b_1/d_1)}(b_1/d_1)x$ is cyclic. Therefore, there exist $d_2 \in \operatorname{supp}(b_1/d_1)x$ and $b_2 \in 2$ such that

$$Cb(b_1/d_1)x = \mathrm{Perm_f}(\mathbb{D})(b_1/d_1)x \cup Cb(b_2/d_2)(b_1/d_1)x.$$

By continuing this process, we get

$$Cbx = \mathrm{Perm_f}(\mathbb{D})x \cup \bigcup_{i=1}^{l} \mathrm{Perm_f}(\mathbb{D})(b_i/d_i)\cdots(b_1/d_1)x \cup \{\theta\},$$

where $l = 1, \cdots, k$. □

5. 2-s-separated finitely supported Cb-sets

In this section, we consider s-separated finitely supported Cb-sets with 2-equivariant support maps (briefly 2-s-separated finitely supported Cb-set) introduced in [6], and characterize retractable objects in this category.

To find retractable s-separated finitely supported Cb-sets with 2-equivariant support maps, first, in Theorem 5.8, we give a description of them. Thereafter, in Theorem 5.10, we prove that retractable s-separated finitely supported Cb-sets with 2-equivariant support maps are discrete or simple or are a disjoint union of a simple sub Cb-set and a discrete sub Cb-set. Also, we give a description of cyclic s-separated finitely supported Cb-sets with 2-equivariant support maps.

First, we recall our definitions of the support map and 2-equivariant support map of [6].

Definition 5.1. Let X be a finitely supported Cb-set, and $x \in X$. Then,

(a) the map

$$\operatorname{supp} : X \to \mathcal{P}_{\mathrm{f}}(\mathbb{D} \cup 2), x \mapsto \operatorname{supp} x$$

is called *the support map of* X.

(b) the support map of X is 2-*equivariant* if $\operatorname{supp} \sigma x = (\sigma \operatorname{supp} x) \setminus 2$, for all $\sigma \in Cb$.

Definition 5.2. [6] (a) A finitely supported Cb-set X is called an *stabilizer-separated* or briefly *s-separated* if $\operatorname{supp} x \neq \operatorname{supp} x'$, for all non-zero elements $x \neq x' \in X$.

(b) A finitely supported Cb-set X is called an *s-separated with* 2-*equivariant support map* or briefly 2-*s-separated* if X is s-separated and the support map of X is 2-equivariant.

Remark 5.3. Applying Definition 5.2 and Remark 4.6(4), we get that all s-separated θ-simple finitely supported Cb-sets are simple.

Lemma 5.4. [6] *Suppose X is a finitely supported Cb-set, and $x \in X$.*

(i) *Let X be s-separated and $x' \neq x$ be two non-zero elements of X. Then, $|\operatorname{supp} x| = |\operatorname{supp} x'|$ if and only if $Cbx = Cbx'$.*

(ii) *The support map of X is 2-equivariant if and only if $\operatorname{supp} \delta x = (\operatorname{supp} x) \backslash \mathbb{D}_\delta$, for all $\delta \in S'_x$.*

Corollary 5.5. *Suppose X is an s-separated finitely supported Cb-set with 2-equivariant support map. Let $x \in X$ with $|\operatorname{supp} x| > 1$. Then,*

(1) *For all $d \in \operatorname{supp} x$, we have $(0/d)x = (1/d)x$.*

(2) *For all $\delta_1, \delta_2 \in S'_x$, we have $\delta_1\delta_2 x = \delta_2\delta_1 x$.*

(3) *For all $d \neq d' \in \operatorname{supp} x$, we have $Cb(0/d)x = Cb(0/d')x$.*

(4) *If X is a non-singleton cyclic, then X has a unique zero element.*

Proof. (1) Since the support map of X is 2-equivariant, and $|\operatorname{supp} x| > 1$, by Lemma 5.4(ii), we get that $\operatorname{supp}(1/d)x = \operatorname{supp}(0/d)x = \operatorname{supp} x \setminus \{d\} \neq \emptyset$. Now, by Definition 5.2, we have $(0/d)x = (1/d)x$.

(2) By (1), we have

$$\begin{aligned}(0/d)(1/d)x &= (0/d)(0/d)x = (0/d)x \\ &= (1/d)x = (1/d)(1/d)x = (1/d)(0/d)x.\end{aligned}$$

Now, applying Remark 2.3, we get that $\delta_1\delta_2 x = \delta_2\delta_1 x$.

(3) Let $d, d' \in \operatorname{supp} x$. Then, since $\operatorname{supp}(0/d)x = \operatorname{supp} x \setminus \{d\} \neq \emptyset$ and $\operatorname{supp}(0/d')x = \operatorname{supp} x \setminus \{d'\} \neq \emptyset$, we get that $|\operatorname{supp}(0/d)x| = |\operatorname{supp}(0/d')x|$. Therefore, applying Lemma 5.4(i), $Cb(0/d)x = Cb(0/d')x$.

(4) Suppose $X = Cbx$, for some non-zero element $x \in X$. If $\theta_1 \neq \theta_2 \in Z(Cbx)$, then there exist $\delta_1, \delta_2 \in S'_x$ with $\theta_1 = \delta_1 x$ and $\theta_2 = \delta_2 x$. Now, by (2),

$$\theta_1 = \delta_2\theta_1 = \delta_2\delta_1 x = \delta_1\delta_2 x = \delta_1\theta_2 = \theta_2,$$

which is a contradiction. □

In the following lemma, for an s-separated finitely supported Cb-set, by Corollary 5.5, we show that the sub Cb-set $\operatorname{Perm_f}(\mathbb{D})S'_x x$ of a cyclic Cb-set Cbx is cyclic.

Lemma 5.6. *Suppose X is an s-separated finitely supported Cb-set with 2-equivariant support map. Let $x \in X$ with $|\operatorname{supp} x| > 1$. Then, there exists $d \in \operatorname{supp} x$ with $\operatorname{Perm_f}(\mathbb{D})S'_x x = Cb(0/d)x$.*

Proof. Let $\operatorname{supp} x = \{d_1, \cdots, d_k\}$ with $k > 1$. Then, applying Theorem 2.14, we get that $\operatorname{Perm_f}(\mathbb{D})S'_x x = \bigcup_{i=1}^{k} Cb(b_i/d_i)x$ is a sub Cb-set of Cbx where $b_i \in 2$. Now, by Corollary 5.5(1,3), we get that $\operatorname{Perm_f}(\mathbb{D})S'_x x$ is cyclic. Therefore, there exists $d \in \operatorname{supp} x$ such that $\operatorname{Perm_f}(\mathbb{D})S'_x x = Cb(0/d)x$. □

Remark 5.7. Suppose X is an s-separated finitely supported Cb-set and $x \neq x'$ are two non-zero elements of X. Let the support map of X be 2-equivariant. Then,

Case (1): If $|\mathrm{supp}\, x| = |\mathrm{supp}\, x'|$, then by Lemma 5.4(i), $Cbx = Cbx'$.

Case (2): If $|\mathrm{supp}\, x| < |\mathrm{supp}\, x'|$, then $Cbx \subsetneq Cbx'$ and if $|\mathrm{supp}\, x'| < |\mathrm{supp}\, x|$, then $Cbx' \subsetneq Cbx$. To prove this, let $|\mathrm{supp}\, x| = k$ and $|\mathrm{supp}\, x'| = l$. Assuming $k < l$, we show that $Cbx \subsetneq Cbx'$. The other part is proved similarly. Take $\mathrm{supp}\, x' = \{d_1, \cdots, d_k, d_{k+1}, \cdots, d_l\}$. Since the support map of X is 2-equivariant, we get that

$$\begin{aligned} \mathrm{supp}\,(0/d_l)\cdots(0/d_{k+1})x' &= \mathrm{supp}\, x' \setminus \{d_l, \cdots, d_{k+1}\} \\ &= \{d_1, \cdots, d_k\}. \end{aligned}$$

Thus, $|\mathrm{supp}\,(0/d_l)\cdots(0/d_{k+1})x'| = k$. Now, applying Lemma 5.4(i), we get that $Cb(0/d_l)\cdots(0/d_{k+1})x' = Cbx$ and so $x \in Cbx'$.

Theorem 5.8. *Suppose X is an s-separated finitely supported Cb-set. Let the support map of X be 2-equivariant. Then, X is decomposable if and only if X is discrete or $X = Y \cup Z$ is a disjoint union of a non-singleton indecomposable sub Cb-set of Y and a discrete sub Cb-set Z.*

Proof. To prove the non-trivial part, suppose X is non-discrete. Take $X = \coprod_\alpha X_\alpha$ to be a decomposition of X into indecomposable sub Cb-sets. We show that all the non-zero elements of X belong to exactly one component of X. On the contrary, let $x_\alpha \in X_\alpha$ and $x_\beta \in X_\beta$ be two non-zero elements. Then, $|\mathrm{supp}\, x_\alpha| \leq |\mathrm{supp}\, x_\beta|$ or $|\mathrm{supp}\, x_\beta| \leq |\mathrm{supp}\, x_\alpha|$. Now, applying Remark 5.7, $Cbx_\alpha \subseteq Cbx_\beta \subseteq X_\beta$ or $Cbx_\beta \subseteq Cbx_\alpha \subseteq X_\alpha$ which is a contradiction. Thus, there exists a unique α_0 with $X \setminus Z(X) \subseteq X_{\alpha_0}$ which means that X can be written as a disjoint union of a non-singleton indecomposable sub Cb-set and a discrete sub Cb-set. □

Now, we are ready to characterize retractable s-separated finitely supported Cb-sets with 2-equivariant support maps.

In the following lemma, we characterize retractable s-separated cyclic finitely supported Cb-sets with 2-equivariant support maps.

Lemma 5.9. *Suppose X is an s-separated cyclic finitely supported Cb-set. Let the support map of X be 2-equivariant. Then, X is retractable if and only if X is simple.*

Proof. If X is singleton, then it is clear that X is retractable and simple. Suppose $X = Cbx$ is cyclic with a non-zero element x of X. Also, let X be retractable. Then, by Corollary 4.4, X has a unique zero element θ. Notice that, by Remark 4.6(1), X has a θ-simple sub Cb-set, say $Cbx_0 = \mathrm{Perm_f}(\mathbb{D})x_0 \cup \{\theta\}$. Thus, applying Remark 5.3, Cbx_0 is simple. Since $x_0 \in Cbx$, by Theorem 2.4, we get that $x_0 = \pi x$ or $x_0 = \pi\delta_0 x$. If $x_0 = \pi x$, then $Cbx = Cbx_0$, and so, X is simple. Suppose $x_0 = \pi\delta_0 x$. In this case, we also show that $\delta_0 \in S_x$, and so, $Cbx_0 = Cbx$. On the contrary, let $\delta_0 \in S'_x$. Then, by Lemma 2.9(i), $\delta_0 x \neq x$, and so, Cbx_0 is a proper sub Cb-set of Cbx. Since X is retractable, there exists a retraction $\varphi : Cbx \to Cb\delta_0 x$.

First, we show that $\varphi(x) = \delta_0 x$. Since $\varphi(x) \in Cb\delta_0 x$, by Remark 2.13, we have $\varphi(x) \in \mathrm{Perm_f}(\mathbb{D})S'_{\delta_0 x}\delta_0 x$ or $\varphi(x) \in \mathrm{Perm_f}(\mathbb{D})\delta_0 x$. If $\varphi(x) \in \mathrm{Perm_f}(\mathbb{D})S'_{\delta_0 x}\delta_0 x$, then $\varphi(x) = \pi'\delta'\delta_0 x$ where $\delta' \in S'_{\delta_0 x}$ and $\pi' \in \mathrm{Perm_f}(\mathbb{D})$. Since φ is a retraction and $\delta_0 x \in Cb\delta_0 x$, we get that $\delta_0 x = \varphi(\delta_0 x) = \delta_0\varphi(x) = \delta_0\pi'\delta'\delta_0 x$.

Now, applying Lemma 2.9, we get that $|\mathrm{supp}\,\delta_0 x| = |\mathrm{supp}\,\delta_0\pi'\delta'\delta_0 x| < |\mathrm{supp}\,\delta_0 x|$, which is impossible. Therefore, $\varphi(x) \in \mathrm{Perm_f}(\mathbb{D})\delta_0 x$, and so there exists $\pi' \in \mathrm{Perm_f}(\mathbb{D})$ with $\varphi(x) = \pi'\delta_0 x$. Also, since φ is a retraction and $\delta_0 x \in Cb\delta_0 x$, we get that

$$\delta_0 x = \varphi(\delta_0 x) = \delta_0\varphi(x) = \delta_0\pi'\delta_0 x = \pi'\delta'_0\delta_0 x.$$

where the last equality is true by Remark 2.3(2). Now, $\delta'_0 \in S_{\delta_0 x}$, since otherwise, if $\delta'_0 \in S'_{\delta_0 x}$, then by Lemma 2.9

$$|\mathrm{supp}\,\delta_0 x| = |\mathrm{supp}\,\pi'\delta'_0\delta_0 x| = |\mathrm{supp}\,\delta'_0\delta_0 x| < |\mathrm{supp}\,\delta_0 x|,$$

which is impossible. Thus, $\delta'_0 \in S_{\delta_0 x}$ and so $\delta_0 x = \pi'\delta'_0\delta_0 x = \pi'\delta_0 x$. Therefore, $\varphi(x) = \delta_0 x$.

Now, take $d \in (\mathrm{supp}\,x) \setminus \mathrm{supp}\,\delta_{_0} x$, and $d' \in \mathrm{supp}\,\delta_{_0} x$. Then, since X is s-separated, we have $(d\ d')x = x$. Also, since φ is a retraction, we get that

$$(d\ d')\delta_{_0} x = (d\ d')\varphi(x) = \varphi((d\ d')x) = \varphi(x) = \delta_{_0} x.$$

Thus,

$$d = (d\ d')d' \in (d\ d')\mathrm{supp}\,\delta_{_0} x = \mathrm{supp}\,(d\ d')\delta_{_0} x = \mathrm{supp}\,\delta_{_0} x,$$

which is impossible.

The other part follows by Corollary 4.7. □

Theorem 5.10. *Suppose X is an s-separated finitely supported Cb-set. Let the support map of X be 2-equivariant. Then, X is retractable if and only if X is discrete or simple or X is a disjoint union of a simple sub Cb-set and a discrete sub Cb-set.*

Proof. Discrete Cb-sets are retractable. Also, by Corollary 4.7, simple finitely supported Cb-sets are retractable.

To prove the other part, let X be non-discrete and retractable. Then, by Theorem 5.8, $X = Y \cup Z$ is a disjoint union of a discrete sub Cb-set Z, and an indecomposable sub Cb-set Y. Notice that, by Remark 4.2(1), Y is retractable. So, applying Corollary 4.4, we get that Y has a unique zero element θ. We show that Y is simple. To show this, first, we prove that Y has a unique simple sub Cb-set. By Remark 4.6(1), Y has a θ-simple sub Cb-set. Since Y is s-separated, by Remark 5.3, we get that Y has a simple sub Cb-set. Now, suppose B_1 and B_2 are two simple sub Cb-sets of Y. So, applying Theorem 4.5, $B_1 = Cby_1$ and $B_2 = Cby_2$ are cyclic. Assuming $B_1 = Cby_1$, we show that $|\mathrm{supp}\,y_1| = 1$. Notice that, $(0/d)y_1 = \theta$, for all $d \in \mathrm{supp}\,y_1$. Since Y is s-separated with 2-equivariant support map, we get that $\emptyset = \mathrm{supp}\,(0/d)y_1 = (\mathrm{supp}\,y_1) \setminus \{d\}$. Thus $\mathrm{supp}\,y_1 = \{d\}$, and so, $|\mathrm{supp}\,y_1| = 1$.

Similarly, $|\operatorname{supp} y_2| = 1$. Thus, since $|\operatorname{supp} y_1| = |\operatorname{supp} y_2| = 1$, by Remark 5.7, we get that $B_1 = B_2$. Hence, Y has a unique simple sub Cb-set, say B.

Now, we prove that $Y = B$. Let $y \in Y$. Then, since Y is retractable, by Remark 4.6(1), we get that Cby is retractable. Now, applying Lemma 5.9, Cby is simple. Thus, $Cby = B$, and so, $y \in B$. Therefore, $B \subseteq Y \subseteq B$ which means that $Y = B$ is simple. □

In Theorem 5.11, we give a description of a cyclic s-separated finitely supported Cb-set with 2-equivariant support map.

Theorem 5.11. *If Cbx is an s-separated finitely supported Cb-set with 2-equivariant support map and $\operatorname{supp} x = \{d_1, \cdots, d_k\}$, then*

$$Cbx = \operatorname{Perm_f}(\mathbb{D})x \cup \bigcup_{i=1}^{k} \operatorname{Perm_f}(\mathbb{D})(0/d_i)\cdots(0/d_1)x,$$

where $d_j \in \operatorname{supp}(0/d_{_{j-1}})\cdots(0/d_{_1})x$, for $j = 2, \cdots, k$.

Proof. Let $\operatorname{supp} x = \{d_1, \cdots, d_k\}$. Then, applying Lemma 5.6, there exists some $d_i \in \operatorname{supp} x$, say $d_i = d_1$, with $\operatorname{Perm_f}(\mathbb{D})S'_{_x}x = Cb(0/d_1)x$. Now, we show that $\operatorname{Perm_f}(\mathbb{D})S'_{_{(0/d_1)}}(0/d_1)x = Cb(0/d_2)(0/d_1)x$, where $d_2 \in \operatorname{supp}(0/d_1)x$. Similar to the proof of Theorem 2.14,

$$\operatorname{Perm_f}(\mathbb{D})S'_{_{(0/d_1)}}(0/d_1)x = \bigcup_{j} Cb(0/d_j)(0/d_1)x,$$

where for all j, $d_j \in \operatorname{supp}(0/d_1)x$.

On the other hand, for all j, we have $\operatorname{supp}(0/d_j)(0/d_1)x = \operatorname{supp} x \backslash \{d_j, d_1\}$. So, for all $r \neq s$, we get $|\operatorname{supp}(0/d_r)(0/d_1)x| = |\operatorname{supp}(0/d_s)(0/d_1)x|$. Now, applying Lemma 5.4, $Cb(0/d_r)(0/d_1)x = Cb(0/d_s)(0/d_1)x$. Thus, $\operatorname{Perm_f}(\mathbb{D})S'_{_{(0/d_1)}}(0/d_1)x$ is cyclic. So, there exists $d \in \operatorname{supp}(0/d_1)x$, say $d = d_2$ with

$$Cb(0/d_1)x = \operatorname{Perm_f}(\mathbb{D})(0/d_1)x \cup Cb(0/d_2)(0/d_1)x.$$

By continuing this process, we get

$$Cbx = \operatorname{Perm_f}(\mathbb{D})x \cup \bigcup_{i=1}^{k} \operatorname{Perm_f}(\mathbb{D})(0/d_i)\cdots(0/d_1)x.$$

□

Acknowledgement. The author would like to thank the referees and the editor for their positive and useful comments. Also, the author gratefully thanks to Professor Mojgan Mahmoudi for her insightful comments on the paper.

References

[1] **S. Abramsky, D.R. Ghica, C.H. Luke Ong, A.S. Murawski and I.D.B. Stark**, *Nominal games and full abstraction for the nu-calculus*, 19th Symposium on Logic in Computer Science, (2004), 150 – 159.

[2] **M.M. Ebrahimi and M. Mahmoudi**, *The category of M-sets*, Ital. J. Pure Appl. Math. **9** (2001), 123 – 132.

[3] **M.M. Ebrahimi, Kh. Keshvardoost and M. Mahmoudi**, *Simple and subdirectly irreducible finitely supported Cb-sets*, Theor. Comput. Sci., **706** (2018), 1 – 21.

[4] **M. Gabbay and A. Mathijssen**, *One-and-a-halfth-order logic*, J. Logic Comput. **18** (2008), 521 – 562.

[5] **M. Gabbay and A. Pitts**, *A new approach to abstract syntax with variable binding*, Form. Asp. Comput. **13 (3-5)** (2002), 341 – 363.

[6] **Kh. Keshvardoost and M. Mahmoudi**, *Separated finitely supported Cb-sets*, submitted.

[7] **M. Kilp, U. Knauer and A. Mikhalev**, *Monoids, Acts and Categories*, Walter de Gruyter, Berlin, New York, 2000.

[8] **A. Nagy**, *Retractable state-finite automata without outputs*, Acta Cybernet. **16** (2004), 399 – 409.

[9] **A. Pitts**, *Nominal logic, a first order theory of names and binding*, Inform. and Comput. **186** (2003), 165 – 193.

[10] **A. Pitts**, *Nominal presentations of the cubical sets model of type theory*, LIPIcs. Leibniz Int. Proc. Inform. (2015), 202 – 220.

[11] **D. Turner and G. Winskel**, *Nominal domain theory for concurrency*, Lecture Notes in Comput. Sci. (2009), 546 – 560.

[12] **C. Urban**, *Nominal techniques in isabelle/HOL*, J. Automat. Reason. **40** (2008), 327 – 356.

Received November 03, 2018

Department of Mathematics
Velayat University
Iranshahr
Sistan and Balouchestan
Iran
E-mails: khadijeh.keshvardoost@gmail.com, kh_keshvardoost@sbu.ac.ir

Quasigroups and Related Systems **27** (2019), 267 – 272

On (m,n)-regular and intra-regular ordered semigroups

Panuwat Luangchaisri and Thawhat Changphas

Abstract. Let m,n be non-negative integers. A subsemigroup A of an ordered semigroup $(S,\cdot,\leqslant)$ is called an (m,n)-*ideal* of S if $A^mSA^n \subseteq A$, and if $x \in A$ and $y \in S$ such that $y \leq x$, then $y \in A$. In this paper, various types of such (m,n)-ideals are described.

1. Introduction

The notion of (m,n)-ideal was introduced by S. Lajos in [4] as a generaization of left ideals, right ideals and bi-ideals and was used to a characterization of regular semigroups [5]. J. Sanborisoot and T. Changphas used in [7] (m,n)-ideals to various characterizations of (m,n)-regular ordered semigroups. T. Changphas, P. Luangchaisri and R. Mazurek studied an interval of completely prime ideals in right chain ordered semigroups [2]. Recently, Ze Gu investigated an ordered semigroup which is regular and intra-regular using various types of bi-ideals [8]. The purpose of this paper is to generalize the results of Ze Gu based on the notion of (m,n)-ideals.

An *ordered semigroup* $(S,\cdot,\leqslant)$ is a semigroup $(S,\cdot)$ together with a partially order that is compatible with the semigroup operation, that is,

$$x \leqslant y \Rightarrow zx \leqslant zy, \quad xz \leqslant yz$$

for any $x,y,z \in S$. For non-empty sets A,B of an ordered semigroup $(S,\cdot,\leqslant)$, the multiplication between A and B is defined by $AB = \{ab \mid a \in A, b \in B\}$. And the set $(A]$ is defined to be the set of all elements x of S such that $x \leqslant a$ for some a in A, that is,

$$(A] = \{x \in S \mid x \leqslant a \text{ for some } a \in A\}.$$

It is clear that for nonempty subsets A,B of S, (1) $A \subseteq (A]$; (2) $((A]] = (A]$; (3) $A \subseteq B \Rightarrow (A] \subseteq (B]$; (4) $(A](B] \subseteq (AB]$.

2010 Mathematics Subject Classification: 06F05
Keywords: (m,n)-regular, intra-regular, irreducible, prime, ordered semigroup
The first author was supported by Research Fund for Supporting Lecturer to Admit High Potential Student to Study and Research on His Expert Program Year 2016; the second by the Faculty of Science, Khon Kaen University, Khon Kaen, Thailand.

2. Main results

Hereafter, let m and n be any two positive integers.

Definition 2.1. Let $(S, \leqslant, \cdot)$ be an ordered semigroup. A subsemigroup A of S is called an (m,n)-*ideal* of S if A satisfies the following:

(i) $A^m S A^n \subseteq A$

(ii) $(A] \subseteq A$, equivalently, if $x \in A$ and $y \in S$ such that $y \leq x$, then $y \in A$.

Definition 2.2. An (m,n)-ideal A of an ordered semigroup $(S, \leqslant, \cdot)$ is said to be

- *quasi-prime* if $A_1 A_2 \subseteq A \Rightarrow A_1 \subseteq A$ or $A_2 \subseteq A$,
- *strongly quasi-prime* if $(A_1 A_2] \cap (A_2 A_1] \subseteq A \Rightarrow A_1 \subseteq A$ or $A_2 \subseteq A$,
- *quasi-semiprime* if $(A_1)^2 \subseteq A \Rightarrow A_1 \subseteq A$

for all (m,n)-ideals A_1, A_2 of S.

It is clear that the following implications are valid:

$$\text{strongly quasi-prime} \Rightarrow \text{quasi-prime} \Rightarrow \text{quasi-semiprime}$$

Example 2.3. Let $S = \{0, a, b, c\}$. Define a binary operation and a partial order $\leqslant$ on S as follows:

	0	a	b	c
0	0	0	0	0
a	0	a	a	a
b	0	a	b	b
c	0	a	b	c

$\leqslant := \{(0,0), (0,a), (0,b), (0,c), (a,a), (a,b), (a,c), (b,b), (c,c)\}$.

Then $(S, \cdot, \leqslant)$ is an ordered semigroup and $P = \{0, a, b\}$ is its strongly quasi-prime $(1,1)$-ideal. Thus, P is quasi-prime and quasi-semiprime as well.

Example 2.4. Let $S = \{a, b, c, d, e\}$. Define a binary operation on S by $xy = x$ for all $x \in S$ and define a partial order $\leqslant$ on S by

$$\leqslant := \{(a,a), (b,b), (c,c), (d,d), (e,e), (a,b), (a,c), (b,c)\}.$$

Then $(S, \cdot, \leqslant)$ is an ordered semigroup and $P = \{a, b, c\}$ is its quasi-prime $(1,1)$-ideal, but it is not strongly quasi-prime.

Definition 2.5. An (m,n)-ideal A of an ordered semigroup $(S, \leqslant, \cdot)$ is said to be

- *irreducible* if $A_1 \cap A_2 = A$ implies $A_1 = A$ or $A_2 = A$,
- *strongly irreducible* if $A_1 \cap A_2 \subseteq A$ implies $A_1 \subseteq A$ or $A_2 \subseteq A$

for all (m,n)-ideals A_1, A_2 of S.

A strongly irreducible (m,n)-ideal is irreducible.

Theorem 2.6. *The intersection of quasi-semiprime (m,n)-ideals of an ordered semigroup $(S,\leqslant,\cdot)$, if it is non-empty, is a quasi-semiprime (m,n)-ideal of S.*

Theorem 2.7. *Let A be an (m,n)-ideal of an ordered semigroup $(S,\cdot,\leqslant)$. If A is strongly irreducible and quasi-semiprime, then A is strongly quasi-prime.*

Proof. Assume that A is strongly irreducible and quasi-semiprime. Let A_1 and A_2 be (m,n)-ideals of S such that

$$(A_1A_2] \cap (A_2A_1] \subseteq A.$$

Since

$$(A_1 \cap A_2)^2 \subseteq A_1A_2 \quad \text{and} \quad (A_1 \cap A_2)^2 \subseteq A_2A_1,$$

it follows that

$$(A_1 \cap A_2)^2 \subseteq A_1A_2 \cap A_2A_1 \subseteq (A_1A_2] \cap (A_2A_1] \subseteq A.$$

Now, there are two cases to consider:

Case 1: $A_1 \cap A_2 = \emptyset$. This implies $A_1 \cap A_2 \subseteq A$.

Case 2: $A_1 \cap A_2 \neq \emptyset$. Then $A_1 \cap A_2$ is an (m,n)-ideal of S. Since A is quasi-semiprime, it follows that $A_1 \cap A_2 \subseteq A$.

By the above two cases, we conclude that $A_1 \cap A_2 \subseteq A$. Since A is strongly irreducible, $A_1 \subseteq A$ or $A_2 \subseteq A$. Hence, A is strongly quasi-prime. □

Definition 2.8. (cf. ([7]) An ordered semigroup $(S,\cdot,\leqslant)$ is said to be (m,n)-*regular* if every element $a \in S$ is (m,n)-*regular*, i.e., $a \in (a^mSa^n]$.

Definition 2.9. (cf. [3]) An ordered semigroup $(S,\cdot,\leqslant)$ is said to be *intra-regular* if every element $a \in S$ is *intra-regular*, i.e., $a \in (Sa^2S]$.

Lemma 2.10. *Let $(S,\cdot,\leqslant)$ be an ordered semigroup. Then S is both (m,n)-regular and intra-regular if and only if $(A^2] = A$ for every (m,n)-ideal A of S.*

Proof. Assume that S is both (m,n)-regular and intra-regular. Let A be an (m,n)-ideal of S. Then

$$(A^2] \subseteq (A] = A.$$

There are four cases to consider:

Case 1: $m = 1$ and $n = 1$. We can prove this case as the proof of Theorem 3.1 in [8].

Case 2: $m = 1$ and $n > 1$. Since S is $(1,n)$-regular, it follows that

$$A \subseteq (ASA^n] \quad \text{and} \quad A \subseteq (SA^2S].$$

Then

$$A \subseteq (ASA^n] \subseteq (ASA^{n-1}ASA^n] \subseteq (ASAASA^n] \subseteq (ASASA^nASA^n] \subseteq (ASA^nASA^n] \subseteq (A^2].$$

Thus, $A = (A^2]$.

Case 3: $m > 1$ and $n = 1$. It can be proved similarly to Case 2.

Case 4: $m > 1$ and $n > 1$. Since S is (m,n)-regular and intra-regular, we obtain that

$$A \subseteq (A^mSA^n] \text{ and } A \subseteq (SA^2S].$$

Then

$$A \subseteq (A^mSA^n] \subseteq (A^mSA^{n-1}A^mSA^n] \subseteq (A^mSAASA^n] \subseteq (A^mSA^mSA^nA^mSA^nSA^n] \subseteq (A^mSA^nA^mSA^n] \subseteq (A^2].$$

Thus, $(A^2] = A$. By these cases, we infer that $(A^2] = A$ for all (m,n)-ideals of S.

Conversely, let $a \in S$. By assumption, we obtain that

$$\left(\bigcup_{i=1}^{m+n} a^i \bigcup a^mSa^n\right] = \left(\left(\bigcup_{i=1}^{m+n} a^i \bigcup a^mSa^n\right]^2\right] = \left(\left(\bigcup_{i=1}^{m+n} a^i \bigcup a^mSa^n\right)^2\right].$$

Continue in the same manner, we have that

$$a \in \left(\bigcup_{i=1}^{m+n} a^i \bigcup a^mSa^n\right] = \left(\left(\bigcup_{i=1}^{m+n} a^i \bigcup a^mSa^n\right)^{m+n+1}\right] \subseteq (a^mSa^n].$$

Thus, a is (m,n)-regular. In the same way, we also have

$$a \in \left(\left(\bigcup_{i=1}^{m+n} a^i \bigcup a^mSa^n\right)^4\right] \subseteq (Sa^2S].$$

Thus, a is intra-regular. Hence, S is both (m,n)-regular and intra-regular. □

Lemma 2.11. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. Then the following statements are equivalent:*

(1) $(A^2] = A$ *for every (m,n)-ideal A of S;*

(2) $A_1 \cap A_2 = (A_1A_2] \cap (A_2A_1]$ *for all (m,n)-ideals A_1, A_2 of S;*

(3) *every (m,n)-ideal of S is quasi-semiprime.*

Proof. (1) $\Rightarrow$ (2): Let A_1, A_2 be (m,n)-ideal of S. Then we have two cases to consider:

Case 1: $A_1 \cap A_2 = \emptyset$. By assumption, we have that

$$(A_1A_2]^m S(A_1A_2]^n \subseteq ((A_1A_2)^m S(A_1A_2)^n] \subseteq (A_1SA_1A_2] = (A_1^m SA_1^n A_2] \subseteq (A_1A_2]$$

and $((A_1A_2]] = (A_1A_2]$. Thus, $(A_1A_2]$ is an (m,n)-ideal of S. Similarly, we obtain that $(A_2A_1]$ is (m,n)-ideal of S. Suppose $(A_1A_2] \cap (A_2A_1] \neq \emptyset$. Then $(A_1A_2] \cap (A_2A_1]$ is an (m,n)-ideal of S. This implies that

$$\begin{aligned}(A_1A_2] \cap (A_2A_1] &= \left(((A_1A_2] \cap (A_2A_1])^2\right] \subseteq ((A_1A_2)(A_2A_1)] \subseteq (A_1SA_1] \\ &= (A_1^m SA_1^n] \subseteq (A_1] = A_1.\end{aligned}$$

Similarly, we have that $(A_1A_2] \cap (A_2A_1] \subseteq A_2$. Thus,

$$(A_1A_2] \cap (A_2A_1] \subseteq A_1 \cap A_2 = \emptyset.$$

This is a contradiction. Hence, $(A_1A_2] \cap (A_2A_1] = \emptyset = A_1 \cap A_2$.

Case 2: $A_1 \cap A_2 \neq \emptyset$. Then $A_1 \cap A_2$ is an (m,n)-ideal of S. This implies that

$$\begin{aligned}A_1 \cap A_2 &= (A_1 \cap A_2) \cap (A_1 \cap A_2) = \left((A_1 \cap A_2)^2\right] \cap \left((A_1 \cap A_2)^2\right] \\ &\subseteq (A_1A_2] \cap (A_2A_1].\end{aligned}$$

Thus, $(A_1A_2] \cap (A_2A_1] \neq \emptyset$. We can prove similarly the above case that

$$(A_1A_2] \cap (A_2A_1] \subseteq A_1 \cap A_2.$$

Hence, $(A_1A_2] \cap (A_2A_1] = A_1 \cap A_2$.

(2) $\Rightarrow$ (3): Let A and A_1 be (m,n)-ideals of S such that $A_1^2 \subseteq A$. By hypothesis, we have that

$$A_1 = A_1 \cap A_1 = (A_1A_1] \cap (A_1A_1] = (A_1A_1] \subseteq (A] = A.$$

Thus, A is a quasi-semiprime (m,n)-ideal of S.

(3) $\Rightarrow$ (1): Let A be an (m,n)-ideal of S. Then $(A^2] \subseteq A$. Since

$$(A^2]^m S(A^2]^n \subseteq (A^{2m} SA^{2n}] \subseteq (A^m SA^n A] \subseteq (A^2]$$

and $((A^2]] = (A^2]$, it follows that $(A^2]$ is an (m,n)-ideal of S. This implies that $(A^2]$ is quasi-semiprime. Since $A^2 \subseteq (A^2]$, we have that $A \subseteq (A^2]$. Hence, $(A^2] = A$. $\square$

Consequently,

Corollary 2.12. *Let $(S, \cdot, \leqslant)$ be an (m,n)-regular and intra-regular ordered semigroup. Then an (m,n)-ideal A of S is strongly irreducible if and only if A is strongly quasi-prime.*

Lemma 2.13. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. Then the following statements are equivalent:*

(1) *The set of all (m,n)-ideals of S is totally ordered under inclusion.*

(2) *Every (m,n)-ideal of S is strongly irreducible and $A_1 \cap A_2 \neq \emptyset$ for all (m,n)-ideals A_1, A_2 of S.*

(3) *Every (m,n)-ideal of S is irreducible and $A_1 \cap A_2 \neq \emptyset$ for all (m,n)-ideals A_1, A_2 of S.*

Proof. (1) $\Rightarrow$ (2): Assume that (1) holds. Then we have immediately that the finite intersection of (m,n)-ideals of S is not empty and so, it is an (m,n)-ideal of S. Let A, A_1, A_2 be (m,n)-ideals of S such that $A_1 \cap A_2 \subseteq A$. By assumption, we can suppose that $A_1 \subseteq A_2$ and then $A_1 = A_1 \cap A_2 \subseteq A$. Thus, A is a strongly irreducible (m,n)-ideal of S.

(2) $\Rightarrow$ (3): This direction is obvious.

(3) $\Rightarrow$ (1): Assume that (3) holds. Let A_1, A_2 be (m,n)-ideals of S. Since $A_1 \cap A_2 \neq \emptyset$, it follows that $A_1 \cap A_2$ is an (m,n)-ideal of S. By hypothesis, we have that $A_1 = A_1 \cap A_2$ or $A_2 = A_1 \cap A_2$. Then $A_1 = A_1 \cap A_2 \subseteq A_2$ or $A_2 = A_1 \cap A_2 \subseteq A_1$. □

Theorem 2.14. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. Then every (m,n)-ideal of S is strongly quasi-prime and $A_1 \cap A_2 \neq \emptyset$ for all (m,n)-ideals A_1, A_2 of S if and only if S is (m,n)-regular, intra-regular and the set of all (m,n)-ideal of S is totally ordered under inclusion.*

References

[1] **T. Changphas**, *On classes of regularity in an ordered semigroups*, Quasigroups and Related Systems, **21** (2013), 43 – 48.

[2] **T. Changphas, P. Luangchaisri and R. Mazurek**, *On right chain ordered semigroups*, Semigroup Forum, **96** (2018), 523 – 535.

[3] **N. Kehayopulu**, *On intra-regular ve-semigroups*, Semigroup Forum, **19** (2080), 111 – 121.

[4] **S. Lajos**, *Generalized ideals in semigroups*, Acta Sci. Math., **22** (1961), 217 – 222.

[5] **S. Lajos**, *On characterization of regular semigroups*, Proc. Japan Acad., **44** (1968), 325 – 326.

[6] **P. Luangchaisri and T. Changphas**, *On the principal (m,n)-ideals in the direct product of two semigroups*, Quasigroups and Related Systems, **24** (2016), 75 – 80.

[7] **J. Sanborisoot, T. Changphas**, *On characterizations of (m,n)-regular ordered semigroups*, Far East J. Math. Sci., **65** (2012), 75 – 86.

[8] **G. Ze**, *On bi-ideal of ordered semigroups*, Quasigroups and Related Systems, **22** (2018), 149 – 154.

Received January 19, 2019

Department of Mathematics, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand

E-mails: desparadoskku@hotmail.com, thacha@kku.ac.th

Quasigroups and Related Systems **27** (2019), 273 – 280

Congruences on nil-extension of a b-lattice of skew-rings

Sunil Kumar Maity, Uma Kapuria and Biswajit Mitra

Abstract. Let S be a nil-extension of a b-lattice of skew-rings K by a semiring Q. A congruence pair (δ, ω) on S consists of a congruence δ on Q and a congruence ω on K. In this paper, we establish that there is an order preserving bijection between the set of all congruences on S onto the set of all congruence pairs on S. It is also proved that if S is a nil-extension of a completely regular semiring, then every congruence on S can be uniquely represented by a congruence pair and there is an order preserving bijection from the set of all congruences on S onto the set of all congruence pairs on S.

1. Introduction

Nil-extensions of semigroups are precisely the ideal extensions by nil semigroups. Semigroups which are nil-extensions of completely simple semigroups was first studied by S. Bogdanović and S. Milić [2] in 1984. Decomposition of completely $\pi-$regular semigroups into a semilattice of Archimedean semigroups was studied by Bogdanović [1]. Nil-extensions of regular semigroups, regular poe-semigroups are special classes of semigroups that attracted many researchers. Moreover, nil-extension of Clifford semigroup was also a matter of interest.

The structure of semirings has been recently studied by many authors, for example, by F. Pastijin, Y. Q. Guo, M. K. Sen, K. P. Shum and others. Recently, in paper [9], the study of completely regular semirings have derived profilic results which were analouge properties as completely regular semigroups and it has also been derived that a completely regular semiring is a b-lattice of completely simple semirings. Many interesting results in completely regular semigroups and inverse semigroups have been extended to semirings by Sen, Maity and Shum in [9]. In [7], Maity, Ghosh and Chatterjee characterized b-lattice of quasi skew-rings. In [10], Ren and Wang studied the congruences on Clifford quasi-regular semigroups.

In this paper we study the congruences on nil-extension of a band-semilattice (shortly: b-lattice) of skew-rings and congruences on nil-extension of completely regular semiring.

2010 Mathematics Subject Classification: 16Y60, 20M10, 20M07.
Keywords: Quasi completely regular semiring, additive inverse semiring, b-lattice of skew–rings, nil-extension, bi-ideal, skew-ring, quasi skew-ring, congruence pair.

2. Preliminaries

A *semiring* $(S, +, \cdot)$ is a type (2, 2)-algebra whose semigroups $(S, +)$ and $(S, \cdot)$ are connected by ring like distributivity, i.e., $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$ for all $a, b, c \in S$. An element a in a semiring S is said to be *infinite* [4] if and only if $a + x = a = x + a$ for all $x \in S$. Infinite element in a semiring is unique and is denoted by ∞. An infinite element ∞ in a semiring S having the property that $x \cdot \infty = \infty = \infty \cdot x$ for all $x(\neq 0) \in S$ is called *strongly infinite* [4]. A semiring $(S, +, \cdot)$ is called *additively regular* if for every element $a \in S$ there exists an element $x \in S$ such that $a+x+a = a$. In a semiring S, an element y satisfying $a+y+a = a$ and $y+a+y = y$ is said to be an *additive inverse* of an element $a \in S$. We call a semiring $(S, +, \cdot)$ *additively quasi regular* if for every element $a \in S$ there exists a positive integer n such that na is additively regular. An element a in a semiring $(S, +, \cdot)$ is said to be *completely regular* [9] if there exists an element $x \in S$ such that, $a = a + x + a$, $a + x = x + a$ and $a(a + x) = a + x$. We call a semiring S, a *completely regular semiring* if every element a of S is completely regular.

We define an element a in a semiring $(S, +, \cdot)$ as *quasi completely regular* [6] if there exists a positive integer n such that na is completely regular. Naturally, a semiring S is said to be *quasi completely regular* if every element of S is quasi completely regular. A semiring $(S, +, \cdot)$ is a *b-lattice* [9] if $(S, \cdot)$ is a band and $(S, +)$ is a semilattice. Throughout this paper, we always let $E^+(S)$ be the set of all additive idempotents of the semiring S and $C(S)$ be the set of all congruences on the semiring S. Also we denote the set of all additive inverses of a, if it exists, in a semiring S by $V^+(a)$. We further denote the Green's relations on a completely π-regular semigroup as $\mathscr{L}^*$, $\mathscr{R}^*$, $\mathscr{H}^*$, $\mathscr{D}^*$ and $\mathscr{J}^*$. If $(S, +, \cdot)$ is an additively quasi regular semiring, the relations $\mathscr{L}^{*+}, \mathscr{R}^{*+}$, $\mathscr{J}^{*+}, \mathscr{H}^{*+}$ and $\mathscr{D}^{*+}$ [6] are defined by: for $a, b \in S$,

$$a\,\mathscr{L}^{*+}\,b \text{ if and only if } pa\,\mathcal{L}^+\,qb,$$
$$a\,\mathscr{R}^{*+}\,b \text{ if and only if } pa\,\mathscr{R}^+\,qb,$$
$$a\,\mathscr{J}^{*+}\,b \text{ if and only if } pa\,\mathscr{J}^+\,qb,$$
$$\mathscr{H}^{*+} = \mathscr{L}^{*+} \cap \mathscr{R}^{*+} \quad \text{and} \quad \mathscr{D}^{*+} = \mathscr{L}^{*+}\, o\, \mathscr{R}^{*+},$$

where p and q are the smallest positive integers such that pa and qb are additively regular.

A quasi completely regular semiring S is said to be *completely Archimedean* [6] if any two elements of S are $\mathscr{J}^{*+}$-related.

A congruence ρ on a semiring S is called a *b-lattice congruence* (*idempotent semiring congruence*) if S/ρ is a b-lattice (respectively, an idempotent semiring). A semiring S is called a *b-lattice* (*idempotent semiring*) Y of semirings S_α $(\alpha \in Y)$ if S admits a b-lattice congruence (respectively, an idempotent semiring congruence) ρ on S such that $Y = S/\rho$ and each S_α is a ρ-class mapped onto α by the natural epimorphism $\rho^{\#} : S \longrightarrow Y$.

A nonempty subset I of a semiring S is said to be a *bi-ideal* [3] of S if for all $a \in I$ and for all $x \in S$ implies $a + x$, $x + a$, ax, $xa \in I$. Let I be a bi-ideal of

a semiring S. We define a relation ρ_I on S by $a\rho_I b$ if and only if either $a, b \in I$ or $a = b$ where $a, b \in S$. It is easy to verify that ρ_I is a congruence on S. This congruence is said to be the *Rees congruence* on S and the quotient semiring S/ρ_I contains a strongly infinite element, viz., I. This quotient semiring S/ρ_I is said to be the *Rees quotient semiring* and is denoted by S/I. In this case the semiring S is said to be an *ideal extension* or simply an *extension* of I by the semiring S/I. An ideal extension S of a semiring I is a *nil-extension* [5] of I if for any $a \in S$ there exists a positive integer n such that $na \in I$.

For other notations and terminologies see [1] and [4].

3. Nil-extensions of a b-lattice of skew-rings

In this section we establish the structure of an additively quasi regular semiring which is a nil-extension of a b-lattice of skew-rings.

Definition 3.1. A semiring $(S, +, \cdot)$ is called a *skew-ring* if $(S, +)$ is a group. If for every $a \in S$ there exists a positive integer n such that $na \in R$, where R is subskew-ring of S, then S is said to be a *quasi skew-ring.*

Theorem 3.2. (cf. [6]) *Let a be an element of a semiring S such that na lies in a subskew-ring R of S for some positive integer n. If e is the zero of R, then*

(i) $e + a = a + e \in R$;
(ii) $ma \in R$ *for any integer* $m > n$;
(iii) $ae = ea = e$.

Theorem 3.3. (cf. [6]) *A semiring S is additively quasi regular with exactly one additive idempotent if and only if S is a quasi skew-ring.*

Theorem 3.4. (cf. [5]) *A semiring S is a quasi skew-ring if and only if S is a nil-extension of a skew-ring.*

Theorem 3.5. (cf. [6]) *For a semiring S the following conditions are equivalent:*

(i) *S is a quasi completely regular semiring,*
(ii) *Every $\mathscr{H}^{*+}$- class is a quasi skew-ring,*
(iii) *S is (disjoint) union of quasi skew-rings,*
(iv) *S is a b-lattice of completely Archimedean semirings,*
(v) *S is an idempotent semiring of quasi skew-rings.*

Since each $\mathscr{H}^{*+}$- class in a quasi completely regular semiring S is a quasi skew-ring, it follows from Theorem 3.3 that each $\mathscr{H}^{*+}$-contains a unique additive idempotent. The unique additive idempotent in the $\mathscr{H}^{*+}$- containing an element $x \in S$ is denoted by 0_x.

Theorem 3.6. (cf. [5]) *The following conditions on a semiring are equivalent:*

(i) *S is a completely Archimedean semiring;*
(ii) *S is a nil extension of a completely simple semiring;*
(iii) *S is Archimedean and quasi completely regular.*

Definition 3.7. (cf. [8]) A subsemiring T of a semiring S is a *retract* of S if there exists a homomorphism $\varphi\colon S \longrightarrow T$ such that $\varphi(t) = t$ for all $t \in T$. Such a homomorphism is called a *retraction*. A nil-extension S of T is said to be a *retractive nil-extension* of T if T is a retract of S.

Theorem 3.8. (cf. [8]) *The following conditions on a semiring are equivalent:*

(*i*) *S is a completely Archimedean semiring;*

(*ii*) *S is a nil extension of a completely simple semiring;*

(*iii*) *S is retractive nil-extension of a completely simple semiring.*

Theorem 3.9. (cf. [8]) *The following conditions on a semiring S are equivalent:*

(*i*) *S is a nil-extension of a b-lattice of skew-rings.*

(*ii*) *S is a retractive nil-extension of a b-lattice of skew-rings.*

Theorem 3.10. *The following conditions on a semiring S are equivalent:*

(*i*) *S is a nil-extension of a b-lattice of skew-rings;*

(*ii*) *S is a quasi completely regular semiring such that $Reg^+(S)$ is a bi-ideal of S and $a + e = e + a$ for all $a \in S$ and for all $e \in E^+(S)$;*

(*iii*) *S is a b-lattice of quasi skew-rings and $Reg^+(S)$ is a bi-ideal of S.*

Proof. $(i) \Rightarrow (ii)$: Let S be a nil-extension of a b-lattice of skew-rings T. Then clearly S is a quasi completely regular semiring and $\mathrm{Reg}^+(S) = T$ is a bi-ideal of S. Let $a \in S$ and $e \in E^+(S)$. Then $a + e, e \in T$ and thus $a + e = a + (e + e) = (a + e) + e = e + (a + e) = (e + a) + e = e + (e + a) = e + a$.

$(ii) \Rightarrow (iii)$: Follows from [7, Theorem 3.5].

$(iii) \Rightarrow (i)$: Let S be a b-lattice Y of quasi skew-rings $S_\alpha\,(\alpha \in Y)$ and $\mathrm{Reg}^+(S)$ is a bi-ideal of S. For each $\alpha \in Y$, let S_α be the nil-extension of a skew-ring R_α. Clearly, $\mathrm{Reg}^+(S) = \bigcup_{\alpha \in Y} R_\alpha$ is a completely regular semiring and S is a nil-extension of $\mathrm{Reg}^+(S)$. Since S is a b-lattice of quasi skew-rings, it follows by [7, Theorem 3.5] that S is a quasi completely inverse semiring and hence by [7, Theorem 3.6], it follows that every additively regular element possesses a unique additive inverse. Thus every element of $\mathrm{Reg}^+(S)$ possesses a unique additive inverse, i.e., $\mathrm{Reg}^+(S)$ is an additive inverse semiring. Thus, $\mathrm{Reg}^+(S)$ is a completely regular semiring as well as an additive inverse semiring. Hence $\mathrm{Reg}^+(S)$ is a b-lattice of skew-rings. Consequently, S is a nil-extension of a b-lattice of skew-rings. □

4. Congruences on nil-extensions

In this section we introduce congruence pair on an additively quasi regular semiring which is a nil-extension of a b-lattice of skew-rings.

Definition 4.1. Let S be a nil-extension of b-lattice of skew-rings K by the semiring Q with a strongly infinite element ∞ and σ be a congruence on S. We define $K\sigma$ by $K\sigma = \{a \in S : (a, k) \in \sigma \text{ for some } k \in K\}$. Also, we define two

relations on K and Q, respectively denoted by σ_K and σ_Q, by $\sigma_K = \sigma|_K$ and $\sigma_Q = (\sigma \vee \rho_K)/\rho_K$, where ρ_K is the Rees congruence on S induced by the bi-ideal K.

Definition 4.2. Let S be a nil-extension of a b-lattice of skew-rings K by a semiring Q with strongly infinite element ∞, δ be a congruence on the semiring Q and ω be a congruence on K. Then a pair $(\delta, \omega) \in C(Q) \times C(K)$ is called a *congruence pair* on S if it satisfies the following conditions.

(M_1) If $(e, f) \in \omega$ for some additive idempotents $e, f \in E^+(S)$, then $(p+e, p+f) \in \omega$ and $(e+p, f+p) \in \omega$ for any $p \in Q$.

(M_2) If $(p, q) \in \delta|_{Q \setminus \infty\delta}$, then $(p+e, q+e) \in \omega$ and $(e+p, e+q) \in \omega$ for any $e \in E^+(S)$.

(M_3) (a) If $(p, q) \in \delta|_{Q \setminus \infty\delta}$, then $(0_{p+c}, 0_{q+c}) \in \omega$ and $(0_{c+p}, 0_{c+q}) \in \omega$ for any $c \in S$.

(b) If $(p, q) \in \delta|_{Q \setminus \infty\delta}$, then $(0_{pc}, 0_{qc}) \in \omega$ and $(0_{cp}, 0_{cq}) \in \omega$ for any $c \in S$.

(M_4) If $a(\neq \infty) \in \infty\delta$, then $(a+0_a+c, a+c+0_{a+c}) \in \omega$ and $(c+a+0_a, c+a+0_{c+a}) \in \omega$ for any $c \in S$.

We need two results similar to Proposition 2.2 and Proposition 2.3 from [10].

Lemma 4.3. *Let S be a nil-extension of b-lattice of skew-rings K by the semiring Q with a strongly infinite element ∞ and σ be a congruence on S. Then $a \in K\sigma$ if and only if $(a, a+0_a) \in \sigma$ and $(a, 0_a+a) \in \sigma$.*

Lemma 4.4. *Let S be a nil-extension of b-lattice of skew-rings K by the semiring Q with a strongly infinite element ∞ and σ be a congruence on S. Then $(0_a, 0_b) \in \sigma$ for any $(a, b) \in \sigma$.*

Lemma 4.5. *Let S be a nil-extension of b-lattice of skew-rings K by the semiring Q with a strongly infinite element ∞ and σ be a congruence on S. Then $\sigma \subseteq \tau$ if and only if $\sigma_Q \subseteq \tau_Q$ and $\sigma_K \subseteq \tau_K$ for any $\sigma, \tau \in C(S)$.*

Proof. Now, $\sigma_Q = (\sigma \vee \rho_K)/\rho_K, \tau_Q = (\tau \vee \rho_K)/\rho_K, \sigma_K = \sigma|_K$ and $\tau_K = \tau|_K$.

First we assume that $\sigma \subseteq \tau$. Suppose $a\rho_K, b\rho_K \in Q = S/\rho_K$ such that $a\rho_K \, \sigma_Q \, b\rho_K$. Then $a\rho_K \, (\sigma \vee \rho_K)/\rho_K \, b\rho_K$. This implies that $a \, (\sigma \vee \rho_K) \, b$, i.e., there exists a sequence of elements $c_1, c_2, \ldots, c_n \in S$ with $a = c_1, b = c_n$ such that $(c_i, c_{i+1}) \in \sigma$ or $(c_i, c_{i+1}) \in \rho_K$. This implies there exists a sequence of elements $c_1, c_2, \ldots, c_n \in S$ with $a = c_1, b = c_n$ such that $(c_i, c_{i+1}) \in \tau$ or $(c_i, c_{i+1}) \in \rho_K$, i.e, $a \, (\tau \vee \rho_K) \, b$ and thus $a\rho_K \, \tau_Q \, b\rho_K$.

To show $\sigma_K \subseteq \tau_K$, let $c, d \in K$ such that $c \, \sigma_K \, d$. This implies $c \, \sigma \, d$ and hence $c \, \tau \, d$ with $c, d \in K$. Therefore, $c \, \tau_K \, d$ and consequently $\sigma_K \subseteq \tau_K$.

Conversely, suppose that $\sigma_Q \subseteq \tau_Q$ and $\sigma_K \subseteq \tau_K$. To show $\sigma \subseteq \tau$, let $p \, \sigma \, q$ for some $p, q \in S$. If both $p, q \in K$, then $p \, \sigma_K \, q$. Now $\sigma_K \subseteq \tau_K$ implies $p \, \tau_K \, q$ and hence $p \, \tau \, q$. So we consider the cases when one of p, q does not belong to K, or

both do not belong to K. Now $p\ \sigma\ q$ implies $p\ (\sigma \vee \rho_K)\ q$, i.e., $p\rho_K\ \sigma_Q\ q\rho_K$. This implies $p\rho_K\ \tau_Q\ q\rho_K$, i.e., $p\rho_K\ (\tau \vee \rho_K)/\rho_K\ q\rho_K$, i.e., $p\ (\tau \vee \rho_K)\ q$ and therefore there exists a sequence $x_1, x_2, \ldots, x_m \in S$ with $x_1 = p$ and $x_m = q$ such that either $(x_i, x_{i+1}) \in \tau$ or $(x_i, x_{i+1}) \in \rho_K$.

If $(x_i, x_{i+1}) \in \tau$ for all $i = 1, 2, \ldots, m$, then clearly $(x_1, x_m) \in \tau$ and hence $(p, q) \in \tau$. Therefore, $\sigma \subseteq \tau$.

On the other hand, if $(x_i, x_{i+1}) \in \rho_K$ for at least one $i = 1, 2, \ldots, m$, then we have $p, q \in K\tau$. Then by Lemma 4.3, we have $(p, p + 0_p) \in \tau$ and $(q, q + 0_q) \in \tau$. Again, $p\ \sigma\ q$ implies $0_p\ \sigma\ 0_q$ by Lemma 4.4 and hence $(p + 0_p, q + 0_q) \in \sigma$. Since $p + 0_p, q + 0_q \in K$, we must have $(p + 0_p, q + 0_q) \in \sigma_K$. Since $\sigma_K \subseteq \tau_K$, it follows that $(p+0_p, q+0_q) \in \tau_K$, i.e., $(p+0_p, q+0_q) \in \tau$. Therefore, $p\,\tau\,(p+0_p)\,\tau\,(q+0_q)\,\tau\,q$ and thus $p\,\tau\,q$. Consequently, $\sigma \subseteq \tau$. □

Theorem 4.6. *If $\sigma \in C(S)$, then (σ_Q, σ_K) is a congruence pair on S.*

Proof. For any $\sigma \in C(S)$, clearly it follow that $\sigma_Q \in C(Q)$ and $\sigma_K \in C(K)$. By [10, Lemma 3.3], it follows that (σ_Q, σ_K) satisfies all the conditions in Definition 4.2 except $M_3(b)$. To complete the proof, we only prove that the pair (σ_Q, σ_K) satisfies the condition $M_3(b)$ in Definition 4.2. For this, let $(p, q) \in \sigma_Q|_{Q \setminus \infty\sigma_Q}$. Since σ is a congruence on $(S, \cdot)$, then for any $c \in S$, we have $(pc, qc) \in \sigma$ and hence by $(0_{pc}, 0_{qc}) \in \sigma$. As $0_{pc}, 0_{qc} \in K$, we have $(0_{pc}, 0_{qc}) \in \sigma_K$. Similarly, we have $(0_{cp}, 0_{cq}) \in \sigma_K$. This shows that (σ_Q, σ_K) satisfies the condition $M_3(b)$. Consequently, (σ_Q, σ_K) is a congruence pair on S. □

Theorem 4.7. *Let S be a nil-extension of a b-lattice of skew-rings K by a semiring Q with a strongly infinite element ∞. Let $(\delta, \omega) \in C(Q) \times C(K)$ be a congruence pair on S. Define a relation σ on S by : for $a, b \in S$, $a\ \sigma\ b$ if and only if*

(i) $(a, b) \in \delta$ for any $a, b \in S \setminus R$,

(ii) $(a + 0_a, b + 0_b) \in \omega$ for any $a, b \in R$ where $R = K \cup (\infty\delta \setminus \{\infty\})$.

Then σ is a congruence on S such that $K\sigma = R$.

Proof. By Lemma [10, Lemma 3.4], we have σ is a congruence on $(S, +)$ such that $K\sigma = R$. To complete the proof, it remains to prove that σ is a congruence on $(S, \cdot)$. For this let $a, b \in S$ such that $a\,\sigma\,b$ and $c \in S$.

Case - I : We assume that $a, b \in S \setminus R$. Then $a\,\delta\,b$. It is easy to verify that $ac \in S \setminus R$ if and only if $bc \in S \setminus R$ and in this case clearly $c \notin K$, i.e., $c \in Q$. Since $a\,\delta\,b$ and $c \in Q$, we must have $ac\,\delta\,bc$.

We now show that whether $c \in K$ or not, $ac\,\delta\,bc$ when both $ac, bc \in R$. Since $a, b \in S \setminus R$, we have $a, b \in Q \setminus \infty\delta$. So by condition $M_3(b)$, we have $(0_{ac}, 0_{bc}) \in \omega$. Since $\omega \in C(K)$ and $a + 0_a \in K$, we have $0_{ac}(a + 0_a)\ \omega\ 0_{bc}(a + 0_a)$, i.e, $0_{ac}a\ \omega\ 0_{bc}a$. Now, $(a, b) \in \delta|_{Q \setminus \infty\delta}$ implies $0_{bca}\ \omega\ 0_{bcb}$, i.e., $0_{bc}a\ \omega\ 0_{bc}b$. Therefore, $0_{ac}a\ \omega\ 0_{bc}b$. Since $0_{ac}a, 0_{bc}b \in E^+(S)$ and $0_{ac}a\ \omega\ 0_{bc}b$, so by condition M_1, we have $a + 0_{ac}a\ \omega\ a + 0_{bc}b$. Again, $a\ \delta\ b$ and $0_{bc}b \in E^+(S)$ imply $a + 0_{bc}b\ \omega\ b + 0_{bc}b$ [by the condition M_2]. So by transitivity of ω, we have $a + 0_{ac}a\ \omega\ b + 0_{bc}b$. Since

$c+0_c \in K$ and ω is a congruence on K, then $(a+0_{ac}a)(c+0_c)\,\omega\,(b+0_{bc}b)(c+0_c)$, i.e., $(ac+0_{ac})\,\omega\,(bc+0_{bc})$. Hence $ac\,\sigma\,bc$.

Case - II : We now assume that $a, b \in R$. In this case $ac, bc \in R$ for any $c \in S$. Again, $a\,\sigma\,b$ implies $(a+0_a, b+0_b) \in \omega$. Since $c+0_c \in K$ and ω is a congruence on K, it follows that $(a+0_a)(c+0_c)\ \omega\ (b+0_b)(c+0_c)$, i.e., $ac+0_{ac}\,\omega\,bc+0_{bc}$. Since both $ac, bc \in R$, hence we have $(ac, bc) \in \sigma$. Thus σ is a right congruence on $(S, \cdot)$. Similarly, we can show that σ is also a left congruence on $(S, \cdot)$ and hence σ is a congruence on the semiring S. □

Theorem 4.8. *Let S be a nil-extension of a b-lattice of skew rings K by a semiring Q with strongly infinite element and let (δ, ω) be a congruence pair on S. Then the congruence σ given in Theorem 4.7 is the unique congruence on S satisfying $\sigma_{_Q} = \delta$ and $\sigma_{_K} = \omega$.*

Proof. The proof is similar to [10, Lemma 3.5]. □

Combining Lemma 4.5, Theorem 4.6, Theorem 4.7 and Theorem 4.8 we get the following result.

Theorem 4.9. *Let S be a nil-extension of a b-lattice of skew-rings K by a semiring Q with strongly infinite element. Then a mapping $\Gamma : C(S) \longrightarrow C(Q) \times C(K)$ such that $\sigma \mapsto (\sigma_{_Q}, \sigma_{_K})$ is an order preserving bijection from the set of all congruences on S onto the set of all congruence pairs on S.*

To give a description of congruences on a nil-extension of a completely regular semiring S, we introduce the following definition.

Definition 4.10. Let S a quasi completely regular semiring which is a nil-extension of a completely regular semiring K by a semiring Q with strongly infinite element ∞. Let $\delta \in C(Q)$ and $w \in C(K)$. Then the pair (δ, ω) is said to be a *congruence pair* if it satisfies all the conditions $(M_1), (M_2), (M_3), (M_4)$ in Definition 4.2 together with two additional conditions given by

(M_5) If $(p+e, q+f) \in \omega$ for some additive idempotents $e, f \in E^+(S)$ and any $p, q \in S$, then $(p+e, f+q) \in \omega$. Dually if $(e+p, f+q) \in \omega$, then $(e+p, q+f) \in \omega$.

(M_6) If $(p+e, f+q) \in \omega$ for some additive idempotents $e, f \in E^+(S)$ and any $p, q \in S$, then $(e+p, q+f) \in \omega$. Dually if $(e+p, q+f) \in w$, then $(p+e, f+q) \in \omega$.

Lemma 4.11. *Let S be a nil-extension of a completely regular semiring K by a semiring Q with strongly infinite element ∞. Let $(\delta, \omega) \in C(Q) \times C(K)$ be a congruence pair on S. Define a relation σ on S by: for $a, b \in S$, $a\sigma b$ if and only if*

(i) $(a, b) \in \delta$ for any $a, b \in S \setminus R$,

(ii) $(a+0_a, b+0_b) \in \omega$ for any $a, b \in R$ where $R = K \cup \{\infty\delta \setminus \{\infty\}\}$.

Then σ is a congruence on S such that $K\sigma = R$.

Proof. The proof follows similar to Theorem 4.7. □

Theorem 4.12. *Let S be a nil-extension of a completely regular semiring K by a semiring Q with strongly infinite element ∞. Then a mapping $\Gamma : C(S) \longrightarrow C(Q) \times C(K)$ such that $\sigma \mapsto (\sigma_{_Q}, \sigma_{_K})$ is an order preserving bijection from the set of all congruences on S onto the set of all congruence pairs on S.*

Proof. The proof follows similar to Theorem 4.9. □

References

[1] **S. Bogdanović**, *Semigroups with a System of Subsemigroups*, Novi Sad (1985).

[2] **S. Bogdanović, S. Milć** *A nil-extension of a completely regular semigroup*, Publ. Inst. Math. Vol. **36(50)** (1984), 45 – 50.

[3] **R. El Bashir, J. Hurt, A. Jancarik, T. Kepka**, *Simple commutative semirings*, J. Algebra bf 236 (2001), 277 – 306.

[4] **J.S. Golan**, *The Theory of Semirings with Applications in Mathematics and Theoretical Computer Science*, Pitman Monographs bf 54, Longman Scientific (1992).

[5] **S.K. Maity, R. Ghosh**, *Nil-extensions of completely simple semirings*, Discussiones Math., General Algebra Appl. **33** (2013), 201 – 209.

[6] **S.K. Maity, R. Ghosh**, *On quasi completely regular semirings*, Semigroup Forum **89** (2014), 422 – 430.

[7] **S.K. Maity, R. Ghosh, R. Chatterjee**, *On quasi completely inverse semirings*, Southeast Asian Bull. Math. **41** (2017), 879 – 886.

[8] **S.K. Maity, R. Ghosh, R. Chatterjee**, *Retractive nil-extensions of completely simple semirings*, Quasigroups Related Systems **26** (2018), 103 – 108.

[9] **M.K. Sen, S.K. Maity, K.P. Shum**, *On compleyely regular semirings*, Bull. Calcutta Math. Soc. **98** (2006), 319 – 328.

[10] **X. Ren, X.D. Wang**, *Congruences on Clifford quasi-regular semigroups*, Sci. Magna, **4** (2008), no.2, 96 – 100.

Received March 19, 2019
Revised July 28, 2019

S.K. Maity
Department of Pure Mathematics, University of Calcutta, 35, Ballygunge Circular Road, Kolkata-700019, India.
E-mail: skmpm@caluniv.ac.in

U. Kapuria and B. Mitra
Department of Mathematics, University of Burdwan
Golapbag, Burdwan-713104, India.
E-mail: uma.kapuria@gmail.com, b1mitra@gmail.com

Quasigroups and Related Systems **27** (2019), 281 – 292

Cryptanalysis of some stream ciphers

Nadeghda N. Malyutina

Abstract. We show that the Vojvoda attacks (attacks with selected plaintext and selected ciphertext) on Markovski cipher can be modified on generalized Markovski cipher based on left and right quasigroups. We give a comparative analysis, identifying positive and negative points in these attacks.

1. Introduction

Today, various cryptosystems based on quasigroups have appeared, which show that the use of quasigroups opens new ways in the construction of stream and block ciphers. For example, S. Markovski [1] (see also E. Ochodkova and V. Snashel [2]) proposed a new stream cipher to encrypt the file system. The cipher has a very large key space. M. Vojvoda has given a cryptoanalysis of the file encoding system based on quasigroups [5] and showed how to break this cipher.

Let $(Q, *)$ be a finite quasigroup. Individual plaintext characters $u_1, u_2, \ldots, u_k$ and ciphertext characters $v_1, v_2, \ldots, v_k$ are represented by the elements of Q, i.e., $u_i, v_i \in Q$, $1 \leqslant i \leqslant k$. The key of this cipher is the operation $*$ defined in the set Q and represented by its Caley table. The keyspace is enormously large.

The authors stated that such a cipher was resistant to any attack [2], although they only studied resistance against brute force attacks and performed some statistical tests on this cipher. From the point of view of cryptanalysis, a good cipher must be strong, at least against known attacks. The best approach is to match only the obvious pairs of elements, and then partially decrypt the encrypted text.

Basic concepts and definitions can be found in [4].

2. Chosen ciphertext attack on Markovski cipher

Assume the cryptanalyst has access to the decryption device loaded with the key. He can then construct the following ciphertext:

$$\begin{array}{l} q_1q_1q_1q_2q_1q_3\ldots q_1q_n \\ q_2q_1q_2q_2q_2q_3\ldots q_2q_n \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ q_nq_1q_nq_2q_nq_3\ldots q_nq_n \end{array}$$

and enter it into the decryption device.

2010 Mathematics Subject Classification: 20N05
Keywords: Quasigroups, left (right) quasigroups, cryptoatacks, cryptoanalysis.

The decryption device gives the following plaintext:

$$\begin{array}{cccccc}
l\backslash q_1 & q_1\backslash q_1 & q_1\backslash q_1 & q_1\backslash q_2 & q_2\backslash q_1 & q_1\backslash q_3 \dots q_1\backslash q_n \\
q_n\backslash q_2 & q_2\backslash q_1 & q_1\backslash q_2 & q_2\backslash q_2 & q_2\backslash q_2 & q_2\backslash q_3 \dots q_2\backslash q_n \\
\dots & \dots & \dots & \dots & \dots & \dots \\
q_n\backslash q_n & q_n\backslash q_1 & q_1\backslash q_n & q_n\backslash q_2 & q_2\backslash q_n & q_n\backslash q_3 \dots q_n\backslash q_n
\end{array}$$

It is easy to see that the Caley table of the operation $\backslash$ defined on Q is completely found. The construction of the Caley table of the operation $*$ is straightforward.

The ciphertext used in the attack consists of $2n^2$ characters. Of course a shorter ciphertext can be constructed. The main requirement of M. Vojvoda is that all the pairs of adjacent elements will appear in the ciphertext.

Example 2.1. Let $Q = \{q_1 = 0, q_2 = 1, q_3 = 2, q_4 = 3\}$ and let the quasigroup $(Q, \backslash)$ with which the decryption is performed have the following Cayley table:

$\backslash$	0	1	2	3
0	2	0	3	1
1	3	1	0	2
2	1	3	2	0
3	0	2	1	3

Let $l \in Q$, $l = 2$. Enter the following text into the decryption device:

00010203
10111213
20212223
30313233

At the output we get: 12203311230110321133022030122103

Having broken the text into four blocks we will receive:

12203311
23011032
11330220
30122103

Thus, the rows of the table of quasigroups $(Q, \backslash)$ are displayed sequentially in even positions.

However, for a complete reconstruction of the Cayley table for the quasigroup $(Q, \backslash)$ it is enough to input only $2n^2 - 4n + 1 = 2n(n-2) + 1$ characters instead of $2n^2$ (in our example, only the first 17 characters will be used instead of 32 characters). Leader l is the solution to the equation: $l\backslash 0 = 1 \Rightarrow l = 2$. Knowing the table for a quasigroup $(Q, \backslash)$, the quasigroup encryption table is easily restored:

$*$	0	1	2	3
0	1	3	0	2
1	2	1	3	0
2	3	0	2	1
3	0	2	1	3

Thus, the ciphertext known to us is easily decrypted.

We suggest using a different text in the decryption procedure:

$$\begin{array}{l} q_1q_1q_2q_2q_3q_3\ldots q_{n-2}q_{n-2}q_{n-1}q_{n-1}q_nq_n \\ q_2q_1q_3q_2q_4q_3\ldots q_{n-1}q_{n-2}q_nq_{n-1}q_1q_n \\ q_3q_1q_4q_2q_5q_3\ldots q_nq_{n-2}q_1q_{n-1}q_2q_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

The decryption device provides the following plaintext at the output:

$$\begin{array}{cccc} l\setminus q_1 & q_1\setminus q_1 & q_1\setminus q_2 & q_2\setminus q_2\ldots q_n\setminus q_n \\ q_n\setminus q_2 & q_2\setminus q_1 & q_1\setminus q_3 & q_3\setminus q_2\ldots q_1\setminus q_n \\ q_n\setminus q_3 & q_3\setminus q_1 & q_1\setminus q_4 & q_4\setminus q_2\ldots q_2\setminus q_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & \end{array}$$

The last symbol depends on the parity of the order of the quasigroup, namely, if n is an odd number, then the last operation will be: $q_k\backslash q_n$, where $k=\left[\frac{n}{2}\right]+1$. If n is an even number, then the last operation will be: $q_{\frac{n}{2}}\backslash q_n$.

The Cayley table of the operation $\setminus$ defined on Q is completely located, after which it is easy to find the Cayley table of the operation $*$. The presented attack requires $n^2-2(n-1)$ operations $\setminus$. Compared to M. Vojvoda's attack, the number of characters used is reduced to $(n+1)^2-3$ characters, i.e., quite significantly. And this number does not depend on the leader.

Example 2.2. For our example, the following text is introduced into the decryption device:

00112233

10

At the output we get: 1201020323

So, instead of 32 characters, 10 characters will be used.

A cryptographic attack on a stream cipher uses the assumption that the cryptanalyst knows the statistics of the language in which the plaintext message is written.

3. Chosen plaintext attack on Markovski cipher

Suppose a cryptanalyst has access to an encryption device with an unknown key. In his PhD thesis [6], M. Vojvoda presented the following text for encryption:

$$\begin{array}{l} q_1q_1;q_1q_2;q_1q_3;\ldots q_1q_n; \\ q_2q_1;q_2q_2;q_2q_3;\ldots q_2q_n; \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ q_nq_1;q_nq_2;q_nq_3;\ldots q_nq_n. \end{array}$$

This text is entered into the encryption device discretely by two characters. Thanks to this input, we have the following ciphertext:

$$\begin{array}{l} l*q_1 \quad ((l*q_1)*q_1);l*q_1 \quad ((l*q_1)*q_2);\ldots l*q_1 \quad ((l*q_1)*q_n); \\ l*q_2 \quad ((l*q_2)*q_1);l*q_2 \quad ((l*q_2)*q_2);\ldots l*q_2 \quad ((l*q_2)*q_n); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ l*q_n \quad ((l*q_n)*q_1);l*q_n \quad ((l*q_n)*q_2);\ldots l*q_n \quad ((l*q_n)*q_n); \end{array}$$

The Cayley table of the operation $*$ defined on Q is completely located. The presented attack requires $2n^2$ operations $*$. However, shorter encrypted text can be built.

Example 3.1. Let $Q = \{q_1 = 0, q_2 = 1, q_3 = 2, q_4 = 3\}$ and let the quasigroup $(Q, *)$ with which the decryption is performed, have the following Cayley table:

$*$	0	1	2	3
0	1	3	0	2
1	2	1	3	0
2	3	0	2	1
3	0	2	1	3

Let $l \in Q$, $l = 2$.

Consider the plaintext attack. Enter the following text into the encryption device:

$$00; 01; 02; 03;$$
$$10; 11; 12; 13;$$
$$20; 21; 22; 23;$$
$$30; 31; 32; 33.$$

The text is entered into the encryption device discretely by 2 characters. At the output we have the following encrypted text:

$$30; 32; 31, 33;$$
$$01; 03; 00; 02;$$
$$23; 20; 22; 21;$$
$$12; 11; 13; 10.$$

The Cayley table of the operation $*$ defined on Q is completely located. Then it is easy to find the Cayley table of the operation $\backslash$. The presented attack requires $2n^2$ operations $*$. The plaintext used in the attack consists of $2n^2$ characters divided into pairs.

However, a shorter encrypted text consisting of $2(n-1)^2$ characters can be constructed (in our example, 18 characters can be used instead of 32 characters). The output, that is line by line at an odd position, is the line number, and at an even position - is the element of the quasigroup $(Q, *)$. Unlike an attack with the selected ciphertext, in this attack the output of lines is not ordered.

Now consider the option when characters are launched into the encryption device by the stream, i.e., as in the case of an attack with the selected ciphertext:

$$q_1q_1q_1q_2q_1q_3 \dots q_1q_n$$
$$q_2q_1q_2q_2q_2q_3 \dots q_2q_n$$
$$\dots\dots\dots\dots\dots$$
$$q_nq_1q_nq_2q_nq_3 \dots q_nq_n$$

The encryption device provides the following ciphertext at the output:

$v_1 = l * q_1, v_2 = v_1 * q_1, v_3 = v_2 * q_1, v_4 = v_3 * q_2, v_5 = v_4 * q_1, v_6 = v_5 * q_3, \dots,$
$v_{2n} = v_{2n-1} * q_n,$
$v_{2n+1} = v_{2n} * q_2, \dots, v_{4n} = v_{4n-1} * q_n, \dots, v_{2n^2-2n} = v_{2n^2-2n-1} * q_n, \dots,$
$v_{2n^2} = v_{2n^2-1} * q_n.$

Example 3.2. For our example, simply type the following text into the encryption device:

00010203

10111213

At the output we have the following encrypted text: 3011223323203110

The Cayley table of the operation $*$ defined on Q is completely located. After that, it is easy to find the leader and the Cayley table of the operation $\backslash$. The presented attack requires 16 operations $*$, which is exactly half as much as in the attack proposed by M. Voivoda. In our example, instead of 32 characters, 16 characters are used. However, it should be noted that the number of symbols used depends on the value of the leader. In our example, $l = 2$, we get the same result for $l = 1$ and $l = 3$, but for $l = 0$, not 16 characters, but 21 characters are needed.

Consider another option for plaintext:

03020100

1312

At the output we have the following encrypted text: 330011232113

The presented attack requires operations $*$ less than in the attack proposed by M. Vojvoda, but everything depends on the chosen leader. In our example, instead of 32 characters, 12 characters are used.

Consider another option for plaintext:

$$\begin{array}{lllll} q_1q_1 & q_2q_2 & q_3q_3\ldots q_{n-2}q_{n-2} & q_{n-1}q_{n-1} & q_nq_n \\ q_2q_1 & q_3q_2 & q_4q_3\ldots q_{n-1}q_{n-2} & q_nq_{n-1} & q_1q_n \\ q_3q_1 & q_4q_2 & q_5q_3\ldots q_nq_{n-2} & q_1q_{n-1} & q_2q_n\ldots \end{array}$$

The plaintext used in the attack consists of $2(n-1)^2$ characters divided into pairs. In this attack the output of lines is not ordered.

The encryption device provides the following ciphertext at the output:

$$\begin{array}{l} v_1 = l * q_1, v_2 = v_1 * q_1, \\ v_3 = l * q_2, v_4 = v_3 * q_2, \\ v_5 = l * q_3, v_6 = v_5 * q_3, \ldots, \\ v_{2n-1} = l * q_n, v_{2n} = v_{2n-1} * q_n, \\ v_{2(n-1)^2-1} = l * q_{n-1}, \ldots, v_{2(n-1)^2} = v_{2(n-1)^2-1} * q_1. \end{array}$$

Example 3.3. For our example, simply type the following text into the encryption device:

00 11 22 33

10 21 32 03

20

At the output we have the following encrypted text:

30 03 22 10 01 20 13 33 23

In our example, instead of 32 characters, 18 characters are used. This result coincides with the result of reduced attack by M. Vojvoda.

Thus, even in the binary case, when carrying out attacks with a selected ciphertext or selected plaintext, the number of symbols used can be reduced.

4. Generalized Markovski cipher and left quasigroups

Example 4.1. Let the key left quasigroup with which the decryption is performed, have the following Cayley table:

$\setminus$	0	1	2	3
0	0	2	1	3
1	1	0	2	3
2	0	3	1	2
3	2	1	3	0

Here $Q = \{q_1 = 0, q_2 = 1, q_3 = 2, q_4 = 3\}$ and $l = 3$.

Enter the following text into the decryption device:

00010203
10111213
20212223
30313233.

At the output we get: 20021103112002333013211202313320

Having broken the text into four blocks we will receive:

20021103 11200233 30132112 02313320

So, rows of the table of the left quasigroup $(Q, \setminus)$ are output sequentially in even positions.

However, for a complete reconstruction of the Cayley table for the left quasigroup $(Q, \setminus)$, it suffices to input only $2n^2 - 2n + 1 = n^2 + (n-1)^2$ characters at the input instead of $2n^2$ (in our example instead of 32 characters, only the first 25 characters will be used). The rest of the table is easily restored, taking into account the fact that the elements are not repeated in the lines of the left quasigroup. The leader l is a solution to the equation: $l \setminus 0 = 2 \Rightarrow l = 3$. In addition, knowing the table for a quasigroup $(Q, \setminus)$ easily restores the quasigroup table of encryption $(Q, *)$:

$*$	0	1	2	3
0	0	2	1	3
1	1	0	2	3
2	0	2	3	1
3	3	1	0	2

After that, the encrypted text known to us is easily decrypted.

If we run the following text on the decoder:

$$q_1q_1q_2q_2q_3q_3\ldots q_{n-2}q_{n-2}q_{n-1}q_{n-1}q_nq_n$$
$$q_2q_1q_3q_2q_4q_3\ldots q_{n-1}q_{n-2}q_nq_{n-1}q_1q_n$$
$$q_3q_1q_4q_2q_5q_3\ldots q_nq_{n-2}q_1q_{n-1}q_2q_n\ldots$$

the decryption device provides the following plaintext at the output:

$$\begin{array}{cccc} l \setminus q_1 & q_1 \setminus q_1 & q_1 \setminus q_2 & q_2 \setminus q_2 \ldots q_n \setminus q_n \\ q_n \setminus q_2 & q_2 \setminus q_1 & q_1 \setminus q_3 & q_3 \setminus q_2 \ldots q_1 \setminus q_n \\ q_n \setminus q_3 & q_3 \setminus q_1 & q_1 \setminus q_4 & q_4 \setminus q_2 \ldots q_2 \setminus q_n \\ \ldots & \ldots & \ldots & \ldots \end{array}$$

The last symbol depends on the parity of the order of the quasigroup, namely, if n is an odd number, then the last operation will be: $q_n \backslash q_k$, where $k = \left[\frac{n}{2}\right] + 1$. If n is an even number, then the last operation will be: $q_n \backslash q_{\frac{n}{2}+1}$.

The presented attack requires $n^2 - 2(n - 1 - \left[\frac{n}{2}\right])$. If n is an odd number, then the attack requires: $(n-1)^2 + 2\left[\frac{n}{2}\right] + 1$ operations, and if n is an even number, you will need: $n^2 - n + 2 = (n-1)^2 + n + 1$ operations $\backslash$.

In comparison with the attack of M. Vojvoda, the number of used symbols is significantly reduced.

Example 4.2. For our previous example, we enter the following text into the decryption device:

00112233

102132

At the output we get: 00202120111333

So, instead of 32 characters, 14 characters will be used.

Consider the plaintext attack built in this one.

Enter the following text into the encryption device:

00	01	02	03
10	11	12	13
20	21	22	23
30	31	32	33

The text is entered into the encryption device discretely by 2 characters. At the output we have the following encrypted text:

33	31	30	32
11	10	12	13
00	02	01	03
20	22	23	21

The output, that goes line by line at an odd position is the line number, and at an even position - is the element of the left quasigroup itself. The plaintext used in the attack consists of $2n^2$ characters divided into pairs. However, a shorter encrypted text consisting of $2n^2 - 2n$ characters can be constructed (in our example, the last pairs, the corresponding elements of the last column, can be omitted, which means that instead of 32 characters, you can use 24 characters). The line output is not ordered.

If we consider the attack with the following opentext:

00010203

10111213

20

at the output we have the following encrypted text: 333112031102231300.

In our example, instead of 32 characters, 18 is launched. Thus, in the binary case, when carrying out attacks with selected plaintext and selected ciphertext, the number of used characters can be reduced. But this result will change when choosing another leader and not always for the better. The question of the range of

variation of the number of possible symbols used for the disclosure of a quasigroup remains open, as in the case of the usual quasigroup.

Now consider the option when characters are launched into an encryption device discretely, namely the following pairs:

$$\begin{array}{llll} q_1q_1 & q_2q_2 & q_3q_3\ldots q_{n-2}q_{n-2} & q_{n-1}q_{n-1} \quad q_nq_n \\ q_2q_1 & q_3q_2 & q_4q_3\ldots q_{n-1}q_{n-2} & q_nq_{n-1} \quad q_1q_n \\ q_3q_1 & q_4q_2 & q_5q_3\ldots q_nq_{n-2} & q_1q_{n-1} \quad q_2q_n\ldots \end{array}$$

Example 4.3. For our example, simply type the following text into the encryption device:

$$\begin{array}{cccc} 00 & 11 & 22 & 33 \\ 10 & 21 & 32 & 03 \\ 20 & 31 & 02 & 13 \end{array}$$

At the output we have the following encrypted text:

$$00 \quad 22 \quad 30 \quad 13 \quad 20 \quad 31 \quad 30 \quad 03 \quad 33 \quad 10 \quad 01 \quad 21$$

The Cayley table of the operation $*$ defined on Q is completely located. After that, it is easy to find the leader and the Cayley table of the operation $\backslash$. The presented attack requires operations $*$ less than in the attack proposed by M. Vojvoda, but everything depends on the chosen leader. The plaintext used in the attack consists of $2n^2-2n$ symbols divided into pairs. The output is not ordered.

In our example, instead of 32 characters, 24 characters are used. This result coincides with the result of a reduced attack by M. Vojvoda.

5. Generalized Markovski cipher and right quasigroups

Description of generalized Markovski cipher based on right quasigroups is given in [4]. Suppose that the key is right quasigroup, with which the decryption is performed, have the following Cayley table:

/	0	1	2	3	4
0	1	2	0	3	4
1	3	4	2	1	0
2	2	1	3	0	2
3	4	3	4	2	1
4	0	0	1	4	3

Here $Q=\{q_1=0,q_2=1,q_3=2,q_4=3,q_5=4\}$ and $l=2$.

Enter the following text into the decryption device:

$$\begin{array}{llll} q_1q_1 & q_2q_2 & q_3q_3\ldots q_nq_n & \\ q_2q_1 & q_3q_2 & q_4q_3\ldots q_{n-1}q_{n-2} & q_nq_{n-1} \quad q_1q_n \\ q_3q_1 & q_4q_2 & q_5q_3\ldots q_nq_{n-2} & q_1q_{n-1} \quad q_2q_n\ldots \end{array}$$

Example 5.1. For our example, simply type the following text into the encryption device:

0001020304
1011121314
2021222324
3031323334
4041424344.

At the output we get: 0113220430023441231020221334011341304224340002114 3
Having broken the text into five blocks we will receive:

0113220430 0234412310 2022133401 1341304224 3400021143

So the columns of the table of the right quasigroup $(Q, /)$ are output sequentially in even positions. For a complete reconstruction of the Cayley table for the right quasigroup $(Q, /)$, as well as in the case of the left quasigroup, it suffices to input only $2n^2 - 2n + 1 = n^2 + (n-1)^2$ instead of $2n^2$ characters (in our example, instead of 50 characters, only 41 will be used). The leader l is a solution to the equation: $0/l = 0 \Rightarrow l = 2$. In addition, knowing the table for a quasigroup $(Q, /)$ easily restores the table of a quasigroup encryption $(Q, *)$:

$*$	0	1	2	3	4
0	4	4	0	2	1
1	0	2	2	1	3
2	2	0	1	3	2
3	1	3	2	0	4
4	3	1	3	4	0

If we run the following text on the decoder:

$$q_1q_1q_2q_2q_3q_3\ldots q_{n-2}q_{n-2}q_{n-1}q_{n-1}q_nq_n$$
$$q_2q_1q_3q_2q_4q_3\ldots q_{n-1}q_{n-2}q_nq_{n-1}q_1q_n$$
$$q_3q_1q_4q_2q_5q_3\ldots q_nq_{n-2}q_1q_{n-1}q_2q_n\ldots$$

the decryption device provides the following plaintext at the output:

$$q_1/l,\quad q_1/q_1,\quad q_2/q_1,\quad q_2/q_2,\ldots q_n/q_n$$
$$q_2/q_n,\quad q_1/q_2,\ldots q_n/q_1,\quad q_3/q_n,\quad q_1/q_3,\ldots$$

The situation is the same as in the case of left quasigroups, i.e. the last character depends on the parity of the order of the quasigroup, namely, if n is an odd number, then the last operation will be: q_k/q_n , where $k = \left[\frac{n}{2}\right] + 1$. If n is an even number, then the last operation will be: $q_{\frac{n}{2}+1}/q_n$ operations /.

Presented attack requires: $n^2 - 2(n - 1 - \left[\frac{n}{2}\right])$ operations /.

Example 5.2. For our previous example, we enter the following text into the decryption device:

0011223344
10213244304
2

At the output we get: 013413242302223011302

So, instead of 50 characters, 21 characters will be used and the result does not depend on the leaders used.

Consider the plaintext attack. Enter the following text into the encryption device:

00 01 02 03 04
10 11 12 13 14
20 21 22 23 24
30 31 32 33 34
40 41 42 43 44

The text is entered into the encryption device discretely by 2 characters. At the output we have the following encrypted text:

04 00 02 01 03
41 43 42 44 40
14 12 10 13 11
20 24 21 22 23
32 31 33 30 34

The output goes column by column at an odd position, and the column number at an even position is the element of the right-hand quasigroup $(Q, *)$. After which it is easy to find the Cayley table of the operation /. The opentext used in the attack consists of $2n^2$ characters divided into pairs. However, a shorter encrypted text consisting of $2n^2 - 2n$ characters can be constructed (in our example, the last pairs, the corresponding elements of the last line, can be omitted, which means that instead of 50 characters, you can use 40 characters). Unlike the attack chosen by ciphertext, in this attack the output of the columns is not ordered.

If we consider the attack with the following opentext:

0001020304
1011121314
2021222324
3031323334
404142

at the output we have the following encrypted text:

041202014004312122402024210103044302222341123 3.

The presented attack requires 46 elements to be processed in our example. But the result depends on the leader used.

Now consider the option when characters are launched into an encryption device discretely, namely the following pairs:

$$\begin{array}{llll} q_1q_1 & q_2q_2 & q_3q_3 \dots q_nq_n & \\ q_2q_1 & q_3q_2 & q_4q_3 \dots q_{n-1}q_{n-2} & q_nq_{n-1} \quad q_1q_n \\ q_3q_1 & q_4q_2 & q_5q_3 \dots q_nq_{n-2} & q_1q_{n-1} \quad q_2q_n \dots \end{array}$$

Example 5.3. For our example, simply type the following text into the encryption device:

00 11 22 33 44
10 21 32 43 04
20 31 42 03 14
30 41 02 13 24

At the output we have the following encrypted text:

00 43 10 22 34 41 14 21 30 03 14 24 33 01 40 20 31 02 44 11

The plaintext used in the attack consists of $2n^2-2n$ symbols divided into pairs. The output is not ordered.

In our example, instead of 50 characters, 40 characters are used. This result coincides with the result of a reduced attack by M. Vojvoda.

6. Conclusion

Thus, in the binary case, when carrying out attacks with selected plaintext and selected ciphertext, the number of symbols used can be reduced, even if it is insignificant.

The results are displayed in the following table:

The required number of characters used				
Order	Chosen ciphertext and plaintext attack M. Vojvoda	Chosen ciphertext attack M. Vojvoda (truncated)	Attack modified ciphertext	Chosen plaintext attack M. Vojvoda (truncated)
Quasigroups				
n	$2n^2$	$2n^2-4n+1$	$n^2-2(n-1)$	$2(n-1)^2$
n=128	32768	32257	16130	32258
n=256	131072	130049	65026	130050
n=512	524288	522241	261122	522242
n=1024	2097152	2093057	1046530	2093058
Left and right quasigroups				
n	$2n^2$	$2n^2-2n+1$	$n^2-2(n-1-\lceil\frac{n}{2}\rceil)$	$2n^2-2n$
n=128	32768	32513	16258	32512
n=256	131072	130561	65282	130560
n=512	524288	523265	261634	523264
n=1024	2097152	2095105	1047554	2095104

Remark 6.1. We notice that

$$\lim_{n\to\infty}\frac{2n^2}{2n^2-4n+1}=1,$$

$$\lim_{n\to\infty}\frac{2n^2}{n^2-2n+2}=2.$$

Acknowledgement. The author thanks very much Referee for many valuable remarks including Remark 6.1.

References

[1] **S. Markovski, D. Gligoroski and S. Andova**, *Using quasigroups for one-one secure encoding*, Proc. VIII Conf. Logic and Computer Science "LIRA'97", Novi Sad, 1997, 157 – 167.

[2] **E. Ochodkova and V. Snasel**, *Using quasigroups for secure encoding of file system*, Proc. Intern. Sci. NATO PfP/PWP Confer. "Security and Information Protection 2001", Brno, 2001, 175 – 181.

[3] **V.A. Shcherbacov**, *Elements of Quasigroup Theory and Applications*, CRC Press, Boca Raton, 2017.

[4] **V.A. Shcherbacov and N.N. Malyutina**, *Role of quasigroups in cryptosystems. Generalization of Markovsky algorithm*, (Russian), Bull. Transnistrian Univ., **60(3)** (2018), 53 – 57.

[5] **M. Vojvoda**, *Cryptanalysis of a file encoding system based on quasigroup*, J. Electrical Engineering, **54** (2003), 69 – 71.

[6] **M. Vojvoda**, *Stream ciphers and hash functions – analysis of some new design approaches*, PHD thesis, Slovak University of Technology, 2004.

Received April 01, 2019

Department of Mathematics,
State University Dimitrie Cantemir,
Academiei str. 3/2, MD-2028 Chişinău,
Moldova
Email: 231003.Bab.Nadezhda@mail.ru

Quasigroups and Related Systems **27** (2017), 293 – 308

A unified method for setting finite non-commutative associative algebras and their properties

Dmitriy Moldovyan

Abstract. A unified method for defining a class of the finite non-commutative associative algebras of different even dimensions $m \geqslant 6$ is proposed to extend the set of potential algebraic supports of the public-key cryptographic algorithms and protocols based on the hidden discrete logarithm problem. The introduced method sets the algebras containing a large set of the global left-sided units. A particular version of the method defines the algebras with parametrizable multiplication operation all modification of which are mutually associative. The cases $m = 6$ and $m = 10$ are detaily considered.

1. Introduction

One of the current challenges in the area of theoretic and applied cryptography represents developing the public-key cryptographic algorithms and protocols that run efficiently on classical computers but will resist quantum attacks [1, 2], i. e., attacks performed with using hypothetical quantum computers that can be used to solve the factorization problem (FP) and the discrete logarithm problem (DLP) in polynomial time [15]. Development of the post-quantum public-key cryptoschemes is connected with looking for difficult computational problems that are different from the FP and DLP and can be used as primitives of the public-key cryptoschemes.

Much attention of the researchers has gained the conjugacy search problem (CSP) in braid groups representing a particular type of non-commutative groups [3, 6]. On the base of the computational difficulty of that problem a number of the public-key cryptoschemes have been designed [4, 16]. Another promising approach to the development of the post-quantum digital signature schemes [8, 9] and public key-agreement protocols is connected with exploiting so called hidden DLP (HDLP). For the first time the HDLP was proposed in the form of combining the DLP with the CSP as follows [11, 12]:

$$Y = G^w \circ Q^x \circ G^{-w}, \tag{1}$$

2010 Mathematics Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50
Keywords: non-commutative algebra, finite associative algebra, single-sided units, parametrizable multiplication, post-quantum cryptography, public-key cryptoscheme, hidden logarithm problem, discrete logarithm problem

where the known values Y (the public key), G, and Q are elements of some finite non-commutative group Γ; the unknown natural numbers w and x represent the private key. The public key-agreement scheme, the public encryption and commutative encryption algorithms have been introduced in [11, 12] using the multiplicative group of the finite algebra of quaternions, defined over the ground field $CF(p)$, as the group Γ. Detailed investigation [5] of the security of that cryptoschemes have revealed possibility of the polynomial reduction of the HDLP to the LP in the field $CF(p^2)$. That result had shown fundamental difficulties for development of the post-quantum public-key cryptoschemes on the base of the HDLP defined in the form (1) when using the finite algebra of quaternions as the algebraic support of the HDLP. Therefore, the further research of the HDLP as potential post-quantum cryptographic primitive is connected with looking for new forms of the HDLP and/or new finite non-commutative associative algebras (FNAAs) as algebraic supports of the HDLP.

In present paper a unified method for setting a class of the FNAAs of different even dimensions $m \geqslant 6$ is proposed. The introduced FNAAs possess two features that are interesting for cryptographic applications: i) the algebras contain a large set of the global left-sided units and ii) the algebras can be set so that that the multiplication operation is parametrizable and arbitrary two modifications of the multiplication operation are mutually associative. The last property is very attractive for potential application in the public-key cryptoschemes in which the modifications of the multiplication operation are used as a part of the private key. The properties of the 6-dimensional and 10-dimensional FNAAs are investigated in detail.

2. A method for setting a class of the FNAAs

2.1. Preliminaries

The FNAAs of small dimension m, which contain a large set of the global single-sided units, are described in [10] ($m = 2$) and [13] ($m = 3$). However for developing public-key cryptosystems based on the HDLP it is preferably to apply the FNAAs of the dimensions $m \geq 4$, which are defined over the field $GF(p)$ with sufficiently large characteristic p (for example, having the size equal to 256 to 512 bits).

The m-dimensional finite algebra represents the m-dimensional vector space over the field $GF(p)$, in which the multiplication operation (that is distributive relatively the addition operation) is additionally defined. The multiplication operation (denoted as $\circ$) can be defined with using the representation of arbitrary vector $A = (a_0, a_1, \ldots a_{m-1})$ as the following sum of the single-component vectors $a_i\mathbf{e}_i$:

$$A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i,$$

where $\mathbf{e}_0 = (1, 0, 0 \ldots, 0)$, $\mathbf{e}_1 = (0, 1, 0 \ldots, 0)$, ... $\mathbf{e}_{m-1} = (0, 0 \ldots, 0, 1)$ are the basis vectors; $a_0, a_1, \ldots a_{m-1}$ are coordinates of the vector A.

The result of the multiplying two m-dimensional vectors A and $B = \sum_{j=0}^{m-1} b_j \mathbf{e}_j$ is defined as follows:

$$A \circ B = \left(\sum_{i=0}^{m-1} a_i \mathbf{e}_i \right) \circ \left(\sum_{j=0}^{m-1} b_j \mathbf{e}_j \right) = \sum_{j=0}^{m-1} \sum_{i=0}^{m-1} a_i b_j \left(\mathbf{e}_i \circ \mathbf{e}_j \right), \tag{2}$$

where the product of every pair of the basis vectors $\mathbf{e}_i \circ \mathbf{e}_j$ is to be replaced by some single-component vector $\mu \mathbf{e}_k$ that is taken from the so called basis vector multiplication table (BVMT), like Tables 2, 3 (see Section 3), and 4 (Section4). When performing such replacement, one assumes that the intersection of the ith row and the jth column defines the value $\mu \mathbf{e}_k = \mathbf{e}_i \circ \mathbf{e}_j$. The value $\mu \neq 1$ is called structural coefficient. If the BVMT defines the multiplication operation that is associative and non-commutative, then the algebra is called FNAA. The element L (the element R) satisfying the vector equation $L \circ A = A$ ($A = A \circ R$) for every element A of the algebra is called the global left-sided (right-sided) unit.

2.2. Proposed unified method for defining FNAAs of different even dimensions

The paper [7] describes a general method for defining a class of the FNAAs over the field $GF(p)$, which contain a large class of the single-sided units, for arbitrary dimensions $m > 1$. However, using the general properties of such algebras, which are described in [7], one can show that for arbitrary value of the dimension the HDLP can be easily reduced to the DLP in the field $GF(p)$. Therefore, in order to extend the class of potential algebraic supports of the HDLP-based cryptoschemes one can propose the following unified method for defining the FNAAs over the ground field $GF(p)$.

The proposed method consists in using the BVMT described by the following formula for multiplying the basis vectors $\mathbf{e}_i$ and $\mathbf{e}_j$ in the m-dimensional vector space:

$$\mathbf{e}_i \circ \mathbf{e}_j = \mathbf{e}_{j-di}, \tag{3}$$

where the value $j - di$ is computed modulo m. For arbitrary even value m one can fined the values d such that the BVMT described by the formula (3) will define non-commutative associative multiplication operation.

Let us consider three m-dimensional vectors A, B, and $C = \sum_{k=1}^{m} c_k \mathbf{e}_k$. Taking into account the formula (2), for product of the vectors A, B, and $C = \sum_{k=0}^{m} c_k \mathbf{e}_k$ one can get the following

$$(A \circ B) \circ C = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \sum_{k=0}^{m-1} a_i b_j c_k \, (\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k;$$

$$A \circ (B \circ C) = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \sum_{k=0}^{m-1} a_i b_j c_k \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) \, .$$

The last formula shows the multiplication operation is associative, if the BVMT defines associative multiplication of the basis vectors.

For multiplication of three basis vectors $\mathbf{e}_i, \mathbf{e}_j$, and $\mathbf{e}_k$, which is performed in accordance with the formula (3), one can write

$$(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_{j-di} \circ \mathbf{e}_k = \mathbf{e}_{k-dj+d^2 i};$$
$$\mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) = \mathbf{e}_i \circ \mathbf{e}_{k-dj} = \mathbf{e}_{k-dj-di}.$$

Thus, the formula (3) defines associative multiplication of the basis vectors, if the condition

$$d^2 \equiv -d \mod m. \tag{4}$$

holds true.

For all values $m \geqslant 2$ the value $d \equiv -1 \mod m$ satisfies the condition (4) and defines associative multiplication, however in this case we have commutative multiplication. Non-commutative associative multiplication operation can be obtained for even values of the dimension $m \geqslant 6$, for example, when $m = 6, 10, 12, 14$. Table 1 shows the values of the parameter d at which we have the m-dimensional FNAAs.

Table 1

Suitable values d for different dimensions m

m	6	10	12	14	18	20	30	40	62
d	2; 3	4; 5	3; 8	6; 7	8; 9	4; 15	5; 24	6; 35	30; 31

It is easy to show that for the values $m = 2q$, where q is a prime, we have the following two values of the parameter d: $d_1 = q$ and $d_2 = q - 1$ (note that in this case we have $q^2 \equiv q \equiv -q \mod m$ and $(q-1)^2 \equiv 1 - q \mod m$).

The formula (3) generates the BVMTs that are free from structural coefficients, but one can experimentally find different distributions of the inserted structural coefficients, which retain the property of the associativity of the multiplication operation. After such modification of the source BVMT constructed for the case $m = 6$ and $d = 2$ one obtains the BVMT defining the 6-dimensional FNAA (that contains p^3 global left-sided units) used as algebraic support of the post-quantum signature scheme in [14].

For the case of even values of the parameter d one can propose the following version of the proposed unified method, which is described by the following formula for defining the BVMTs containing the structural coefficients λ and ϵ :

$$\mathbf{e}_i \circ \mathbf{e}_j = \begin{cases} \lambda \mathbf{e}_{j-di}, \text{ if } i \equiv 0 \bmod 2 \\ \epsilon \mathbf{e}_{j-di}, \text{ if } i \equiv 1 \bmod 2, \end{cases} \tag{5}$$

Proposition 2.1. *The formula* (5) *defines the m-dimensional FNAAs, if m and d are even natural numbers and the condition* (4) *holds true.*

Thus, the version of the considered unified method described with the formula (5) introduces a set of the FNAAs corresponding to the same distribution of the basis vectors in the BVMT and different pairs of the values of structural coefficients λ and ϵ. One can call such set of FNAAs the algebra with parametrizable multiplication operation. Concrete version of the multiplication operation is set by selecting two fixed values the structural coefficients λ and ϵ. In the considered case of the FNAA with parametrizable multiplication operation we have the following interesting property that can be called mutual associativity of arbitrary two modifications of the multiplication operation (earlier the mutual associativity of different modifications of the multiplication operation in FNAAs was considered in [7]).

Proposition 2.2. *Suppose m and d are even natural numbers and the condition* (4) *holds true. Then the formula* (5) *defines the m-dimensional FNAA with parametrizable multiplication operation and with mutual associativity of all possible pairs of the modifications $\circ$ and $\star$ of the multiplication operation.*

Proof. Suppose the structural coefficients λ and ϵ define the $\circ$-version of the multiplication operation and the structural coefficients λ' and ϵ' define the $\star$-version of the multiplication operation. One should consider the influence of the pairs of structural coefficients (λ, ϵ) and (λ', ϵ') in the following two products: i) $(\mathbf{e}_i \circ \mathbf{e}_j) \star \mathbf{e}_k$ and ii) $\mathbf{e}_i \circ (\mathbf{e}_j \star \mathbf{e}_k)$. In each of these two cases the oddness of the value k does not influences the result in the indicated two cases. Therefore, one should consider the following four cases.

1. The values i and j are even:

$$(\mathbf{e}_i \circ \mathbf{e}_j) \star \mathbf{e}_k = \lambda \mathbf{e}_{j-di} \star \mathbf{e}_k = \lambda\lambda' \mathbf{e}_{k-d(j-di)} = \lambda\lambda' \mathbf{e}_{k-dj+d^2 i} = \lambda\lambda' \mathbf{e}_{k-dj-di};$$
$$\mathbf{e}_i \circ (\mathbf{e}_j \star \mathbf{e}_k) = \mathbf{e}_i \circ \lambda' \mathbf{e}_{k-dj} = \lambda'\lambda \mathbf{e}_{k-dj-di}.$$

2. The value i is even and the value j is odd:

$$(\mathbf{e}_i \circ \mathbf{e}_j) \star \mathbf{e}_k = \lambda \mathbf{e}_{j-di} \star \mathbf{e}_k = \epsilon' \lambda \mathbf{e}_{k-dj+d^2 i} = \epsilon' \lambda \mathbf{e}_{k-dj-di};$$
$$\mathbf{e}_i \circ (\mathbf{e}_j \star \mathbf{e}_k) = \mathbf{e}_i \circ \epsilon' \mathbf{e}_{k-dj} = \lambda \epsilon' \mathbf{e}_{k-dj-di}.$$

3. The value i is odd and the value j is even:

$$(\mathbf{e}_i \circ \mathbf{e}_j) \star \mathbf{e}_k = \epsilon \mathbf{e}_{j-di} \star \mathbf{e}_k = \lambda' \epsilon \mathbf{e}_{k-dj+d^2 i} = \lambda' \epsilon \mathbf{e}_{k-dj-di};$$
$$\mathbf{e}_i \circ (\mathbf{e}_j \star \mathbf{e}_k) = \mathbf{e}_i \circ \lambda' \mathbf{e}_{k-dj} = \epsilon\lambda' \mathbf{e}_{k-dj-di}.$$

4. The values i and j are odd:

$$(\mathbf{e}_i \circ \mathbf{e}_j) \star \mathbf{e}_k = \epsilon\mathbf{e}_{j-di} \star \mathbf{e}_k = \epsilon\epsilon'\mathbf{e}_{k-dj+d^2i)} = \epsilon\epsilon'\mathbf{e}_{k-dj-di};$$
$$\mathbf{e}_i \circ (\mathbf{e}_j \star \mathbf{e}_k) = \mathbf{e}_i \circ \epsilon'\mathbf{e}_{k-dj} = \epsilon'\epsilon\mathbf{e}_{k-dj-di}.$$

Thus, in all cases we have $(\mathbf{e}_i \circ \mathbf{e}_j) \star \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \star \mathbf{e}_k)$. The Proposition 2.2 is proved. □

Note that the Proposition 2.1 is direct corollary from the Proposition 2.2. Using the formula (5) one can define FNAAs with parametrizable multiplication operation, which have different dimensions. Table 1 provides the following examples: i) $m = 6$, $d = 2$; ii) $m = 10$, $d = 4$; iii) $m = 12$, $d = 8$; ... iv) $m = 62$, $d = 30$.

For the case of odd values of the parameter d in the formula (3) one can propose the following version of the considered uniform method which is described by the following formula:

$$\mathbf{e}_i \circ \mathbf{e}_j = \begin{cases} \mathbf{e}_{j-di}, \text{ if } i \equiv 0 \bmod 2 \\ \mathbf{e}_{j-di}, \text{ if } i \equiv 1 \bmod 2 \text{ and } j \equiv 0 \bmod 2 \\ \lambda\mathbf{e}_{j-di}, \text{ if } i \equiv 1 \bmod 2 \text{ and } j \equiv 1 \bmod 2, \end{cases} \tag{6}$$

The reader can easily prove the following proposition.

Proposition 2.3. *Suppose m is an even integer, d is an odd integer, and the condition* (4) *holds true. Then the formula* (6) *defines the m-dimensional FNAAs.*

Considering the fixed even value m and fixed odd value d we have many FNAAs relating to different values of the structural coefficient λ, which can be united by the notion of FNAA with the parametrizable multiplication operation. However, in such algebras different modifications of the multiplication operation are not mutually associative in general case.

3. The case of 6-dimensional FNAAs

3.1. The algebra with mutually associative modifications of the multiplication operation

In the case $m = 6$, $d = 2$, and $\lambda = 1$ we have the BVMT shown as Table 2. Due to the Proposition 2.2 this FNAA is an algebra is with parametrizable multiplication operation all modifications of which are mutually associative. The 6-dimensional FNAA defined with this table contains the set of p^3 global left-sided units $L = (l_0, l_1, l_2, l_3, l_4, l_5)$ described with the following formula [14]:

$$L = \left(h, k, t, (1-h)\epsilon^{-1}, -\epsilon k, -t\epsilon^{-1}\right),$$

where $h, k, t = 0, 1, \ldots p-1$. Evidently, the considered 6-dimensional FNAA contains no global right-sided unit. To find the formula describing local right-sided

units one should consider solution of the vector equation $A \circ X = A$, where $A = (a_0, a_1, a_2, a_3, a_4, a_5)$ is a fixed vector. The last equation can be reduced to the following two independent systems each of which contains three unknowns:

$$\begin{cases} (a_0 + \epsilon a_3)\, x_0 + (\epsilon a_1 + a_4)\, x_2 + (a_2 + \epsilon a_5)\, x_4 = a_0; \\ (a_2 + \epsilon a_5)\, x_0 + (a_0 + \epsilon a_3)\, x_2 + (\epsilon a_1 + a_4)\, x_4 = a_2; \\ (\epsilon a_1 + a_4)\, x_0 + (a_2 + \epsilon a_5)\, x_2 + (a_0 + \epsilon a_3)\, x_4 = a_4; \end{cases}$$

$$\begin{cases} (a_0 + \epsilon a_3)\, x_1 + (\epsilon a_1 + a_4)\, x_3 + (a_2 + \epsilon a_5)\, x_5 = a_1; \\ (a_2 + \epsilon a_5)\, x_1 + (a_0 + \epsilon a_3)\, x_3 + (\epsilon a_1 + a_4)\, x_5 = a_3; \\ (\epsilon a_1 + a_4)\, x_1 + (a_2 + \epsilon a_5)\, x_3 + (a_0 + \epsilon a_3)\, x_5 = a_5. \end{cases}$$

Table 2

The BVMT defining the FNAA containing p^3 global left-sided units [14]

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\epsilon\mathbf{e}_4$	$\epsilon\mathbf{e}_5$	$\epsilon\mathbf{e}_0$	$\epsilon\mathbf{e}_1$	$\epsilon\mathbf{e}_2$	$\epsilon\mathbf{e}_3$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\epsilon\mathbf{e}_0$	$\epsilon\mathbf{e}_1$	$\epsilon\mathbf{e}_2$	$\epsilon\mathbf{e}_3$	$\epsilon\mathbf{e}_4$	$\epsilon\mathbf{e}_5$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_5$	$\epsilon\mathbf{e}_2$	$\epsilon\mathbf{e}_3$	$\epsilon\mathbf{e}_4$	$\epsilon\mathbf{e}_5$	$\epsilon\mathbf{e}_0$	$\epsilon\mathbf{e}_1$

The main determinant of each of the last two systems is equal to Δ_A:

$$\Delta_A = (a_0 + \epsilon a_3)^3 + (\epsilon a_1 + a_4)^3 + (a_2 + \epsilon a_5)^3 - 3\,(a_0 + \epsilon a_3)\,(a_2 + \epsilon a_5)\,(\epsilon a_1 + a_4)$$

If $\Delta_A \neq 0$, then there exists unique local right-sided unit corresponding to the vector A.

3.2. The algebra with p^4 global left-sided units

In the case $m = 6$ and $d = 3$ the formula (6) defines the BVMT in the form of Table 3. The left-sided units can be found from the vector equation $X \circ A = A$ that reduces to the following system with six unknowns x_0, x_1, x_2, x_3, x_4, and x_5:

$$\begin{cases} (x_0 + x_2 + x_4)\, a_0 + \lambda\,(x_1 + x_3 + x_5)\, a_3 = a_0; \\ (x_1 + x_3 + x_5)\, a_0 + (x_0 + x_2 + x_4)\, a_3 = a_3; \\ (x_0 + x_2 + x_4)\, a_1 + (x_1 + x_3 + x_5)\, a_4 = a_1; \\ \lambda\,(x_1 + x_3 + x_5)\, a_1 + (x_0 + x_2 + x_4)\, a_4 = a_4; \\ (x_0 + x_2 + x_4)\, a_2 + \lambda\,(x_1 + x_3 + x_5)\, a_5 = a_2; \\ (x_1 + x_3 + x_5)\, a_2 + (x_0 + x_2 + x_4)\, a_5 = a_5. \end{cases}$$

Performing the variable substitution $u_1 = x_0 + x_2 + x_4$ and $u_2 = x_1 + x_3 + x_5$ one can easily find the following solution that is independent of the value A: $(u_1, u_2) = (1, 0)$. The solution in terms of the variables u_1 and u_2 defines p^4 solutions in terms of the variables x_0, x_1, x_2, x_3, x_4, and x_5. Every of the last solutions define a unique global left-sided unit. The set of all global left-sided units is described as follows (where $h, k, t, z = 0, 1, \ldots p-1$):

$$L = (l_0, l_1, l_2, l_3, l_4, l_5) = (h, k, t, z, 1-h-t, -k-z)\,.$$

The formula describing local right-sided units can be derived from the vector equation $A \circ X = A$ that can be reduced to the following three independent systems of two linear equations every one of which contains two unknowns:

$$\begin{cases} (a_0 + a_2 + a_4)\, x_0 + \lambda\,(a_1 + a_3 + a_5)\, x_3 = a_0; \\ (a_1 + a_3 + a_5)\, x_0 + (a_0 + a_2 + a_4)\, x_3 = a_3; \end{cases}$$

$$\begin{cases} (a_0 + a_2 + a_4)\, x_1 + (a_1 + a_3 + a_5)\, x_4 = a_1; \\ \lambda\,(a_1 + a_3 + a_5)\, x_1 + (a_0 + a_2 + a_4)\, x_4 = a_4; \end{cases}$$

$$\begin{cases} (a_0 + a_2 + a_4)\, x_2 + \lambda\,(a_1 + a_3 + a_5)\, x_5 = a_2; \\ (a_1 + a_3 + a_5)\, x_2 + (a_0 + a_2 + a_4)\, x_5 = a_5; \end{cases}$$

Table 3

The BVMT of the 6-dimensional FNAA containing p^4 global left-sided units

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\mathbf{e}_4$	$\lambda\mathbf{e}_5$	$\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\mathbf{e}_2$	$\lambda\mathbf{e}_3$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\mathbf{e}_4$	$\lambda\mathbf{e}_5$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_5$	$\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\mathbf{e}_4$	$\lambda\mathbf{e}_5$	$\mathbf{e}_0$	$\lambda\mathbf{e}_1$

The main determinant of each of the last three systems is equal to Δ_A:

$$\Delta_A = (a_0 + a_2 + a_4)^2 - \lambda\,(a_1 + a_3 + a_5)^2\,.$$

If $\Delta_A \neq 0$, then there exists unique local right-sided unit corresponding to the vector A.

4. The 10-dimensional FNAA

In the case $m = 10$, $d = 4$, $\lambda \neq 1$, and $\epsilon = 1$ the formula (5) defines the BVMT in the form of Table 4. The left-sided units can be found from the vector equation $X \circ A = A$ that reduces to the following system with ten unknowns $x_0, x_1, \ldots x_9$:

$$X \circ A = A. \tag{7}$$

Using Table 3 one can represent (7) in the form of the following system of 10 linear equations with coordinates of the left operand $x_0, x_1, \ldots, x_9$ as the unknown values:

$$\begin{cases} \lambda x_0a_0 + x_1a_4 + \lambda x_2a_8 + x_3a_2 + \lambda x_4a_6 + x_5a_0 + \lambda x_6a_4 + x_7a_8 + \lambda x_8a_2 + x_9a_6 = a_0; \\ \lambda x_0a_1 + x_1a_5 + \lambda x_2a_9 + x_3a_3 + \lambda x_4a_7 + x_5a_1 + \lambda x_6a_5 + x_7a_9 + \lambda x_8a_3 + x_9a_7 = a_1; \\ \lambda x_0a_2 + x_1a_6 + \lambda x_2a_0 + x_3a_4 + \lambda x_4a_8 + x_5a_0 + \lambda x_6a_6 + x_7a_0 + \lambda x_8a_4 + x_9a_8 = a_2; \\ \lambda x_0a_3 + x_1a_7 + \lambda x_2a_1 + x_3a_5 + \lambda x_4a_9 + x_5a_0 + \lambda x_6a_7 + x_7a_1 + \lambda x_8a_5 + x_9a_9 = a_3; \\ \lambda x_0a_4 + x_1a_8 + \lambda x_2a_2 + x_3a_6 + \lambda x_4a_0 + x_5a_0 + \lambda x_6a_8 + x_7a_2 + \lambda x_8a_6 + x_9a_0 = a_4; \\ \lambda x_0a_5 + x_1a_9 + \lambda x_2a_3 + x_3a_7 + \lambda x_4a_1 + x_5a_0 + \lambda x_6a_9 + x_7a_3 + \lambda x_8a_7 + x_9a_1 = a_5; \\ \lambda x_0a_6 + x_1a_0 + \lambda x_2a_4 + x_3a_8 + \lambda x_4a_2 + x_5a_0 + \lambda x_6a_0 + x_7a_4 + \lambda x_8a_8 + x_9a_2 = a_6; \\ \lambda x_0a_7 + x_1a_1 + \lambda x_2a_5 + x_3a_9 + \lambda x_4a_3 + x_5a_0 + \lambda x_6a_1 + x_7a_5 + \lambda x_8a_9 + x_9a_3 = a_7; \\ \lambda x_0a_8 + x_1a_2 + \lambda x_2a_6 + x_3a_0 + \lambda x_4a_4 + x_5a_0 + \lambda x_6a_2 + x_7a_6 + \lambda x_8a_0 + x_9a_4 = a_8; \\ \lambda x_0a_9 + x_1a_3 + \lambda x_2a_7 + x_3a_1 + \lambda x_4a_5 + x_5a_0 + \lambda x_6a_3 + x_7a_7 + \lambda x_8a_1 + x_9a_5 = a_9. \end{cases} \tag{8}$$

The system (8) can be rewritten in the form of two systems each of which contains five linear equations with 10 unknowns:

$$\begin{cases} (\lambda x_0 + x_5)\, a_0 + (x_3 + \lambda x_8)\, a_2 + (x_1 + \lambda x_6)\, a_4 + (\lambda x_4 + x_9)\, a_6 + (\lambda x_2 + x_7)\, a_8 = a_0; \\ (\lambda x_0 + x_5)\, a_2 + (x_3 + \lambda x_8)\, a_4 + (x_1 + \lambda x_6)\, a_6 + (\lambda x_4 + x_9)\, a_8 + (\lambda x_2 + x_7)\, a_0 = a_2; \\ (\lambda x_0 + x_5)\, a_4 + (x_3 + \lambda x_8)\, a_6 + (x_1 + \lambda x_6)\, a_8 + (\lambda x_4 + x_9)\, a_0 + (\lambda x_2 + x_7)\, a_2 = a_4; \\ (\lambda x_0 + x_5)\, a_6 + (x_3 + \lambda x_8)\, a_8 + (x_1 + \lambda x_6)\, a_0 + (\lambda x_4 + x_9)\, a_2 + (\lambda x_2 + x_7)\, a_4 = a_6; \\ (\lambda x_0 + x_5)\, a_8 + (x_3 + \lambda x_8)\, a_0 + (x_1 + \lambda x_6)\, a_2 + (\lambda x_4 + x_9)\, a_4 + (\lambda x_2 + x_7)\, a_6 = a_8; \end{cases} \tag{9}$$

$$\begin{cases} (\lambda x_0 + x_5)\, a_1 + (x_3 + \lambda x_8)\, a_3 + (x_1 + \lambda x_6)\, a_5 + (\lambda x_4 + x_9)\, a_7 + (\lambda x_2 + x_7)\, a_9 = a_1; \\ (\lambda x_0 + x_5)\, a_3 + (x_3 + \lambda x_8)\, a_5 + (x_1 + \lambda x_6)\, a_7 + (\lambda x_4 + x_9)\, a_9 + (\lambda x_2 + x_7)\, a_1 = a_3; \\ (\lambda x_0 + x_5)\, a_5 + (x_3 + \lambda x_8)\, a_7 + (x_1 + \lambda x_6)\, a_9 + (\lambda x_4 + x_9)\, a_1 + (\lambda x_2 + x_7)\, a_3 = a_5; \\ (\lambda x_0 + x_5)\, a_7 + (x_3 + \lambda x_8)\, a_9 + (x_1 + \lambda x_6)\, a_1 + (\lambda x_4 + x_9)\, a_3 + (\lambda x_2 + x_7)\, a_5 = a_7; \\ (\lambda x_0 + x_5)\, a_9 + (x_3 + \lambda x_8)\, a_1 + (x_1 + \lambda x_6)\, a_3 + (\lambda x_4 + x_9)\, a_5 + (\lambda x_2 + x_7)\, a_7 = a_9. \end{cases} \tag{10}$$

Performing the variable substitution

$$u_0 = \lambda x_0 + x_5;\ \ u_1 = x_3 + \lambda x_8;\ \ u_2 = x_1 + \lambda x_6;\ \ u_3 = \lambda x_4 + x_9;\ \ u_4 = \lambda x_2 + x_7 \tag{11}$$

in the systems (9) and (10) one can easily see that the solution

$$u_0 = 1;\ \ u_1 = 0;\ \ u_2 = 0;\ \ u_3 = 0;\ \ u_4 = 0 \tag{12}$$

satisfies simultaneously the systems (9) and (10) for all elements A of the considered FNAA. Besides, if the vector A is such that the main determinant of the system (9) Δ'_A satisfies condition $\Delta'_A \neq 0$ or the main determinant of the system (10) Δ''_A satisfies condition $\Delta''_A \neq 0$, then the indicated solution is unique relatively the unknowns u_0, u_1, u_2, u_3, and u_0.

For very small portion of the vectors A, coordinates of which satisfy the both conditions $\Delta'_A = 0$ and $\Delta''_A = 0$, many other solutions exists. However, such "marginal" vectors are to be not involved in the computations in frame of the potential public-key cryptoschemes based on the considered FNAA. The additional solutions define the local left-sided units acting only in frame of the subset of the "marginal" vectors. One can easily derive the formula describing the local left-sided units, but we will describe only the set of global left-sided units (that act as the left-sided units on every 10-dimensional vector).

Taking into account the formulas (11) and the solutions (12) one can get the formula describing all p^5 global left-sided units $L = (l_0, l_1, l_2, l_3, l_4, l_5, l_6, l_7, l_8, l_9)$:

$$L = (x_0, -\lambda x_6, x_2, -\lambda x_8, x_4, 1 - \lambda x_0, x_6, -\lambda x_2, x_8, -\lambda x_4), \tag{13}$$

where $x_0, x_2, x_4, x_6, x_8 = 0, 1, \ldots, p-1$.

Table 4

Defining the 10-dimensional FNAA containing p^5 global left-sided units

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	$\mathbf{e}_9$
$\mathbf{e}_0$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_4$	$\lambda\mathbf{e}_5$	$\lambda\mathbf{e}_6$	$\lambda\mathbf{e}_7$	$\lambda\mathbf{e}_8$	$\lambda\mathbf{e}_9$
$\mathbf{e}_1$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	$\mathbf{e}_9$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_2$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_4$	$\lambda\mathbf{e}_5$	$\lambda\mathbf{e}_6$	$\lambda\mathbf{e}_7$	$\lambda\mathbf{e}_8$	$\lambda\mathbf{e}_9$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_8$	$\mathbf{e}_9$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_4$	$\lambda\mathbf{e}_4$	$\lambda\mathbf{e}_5$	$\lambda\mathbf{e}_6$	$\lambda\mathbf{e}_7$	$\lambda\mathbf{e}_8$	$\lambda\mathbf{e}_9$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$
$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	$\mathbf{e}_9$
$\mathbf{e}_6$	$\lambda\mathbf{e}_6$	$\lambda\mathbf{e}_7$	$\lambda\mathbf{e}_8$	$\lambda\mathbf{e}_9$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_4$	$\lambda\mathbf{e}_5$
$\mathbf{e}_7$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	$\mathbf{e}_9$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_8$	$\lambda\mathbf{e}_8$	$\lambda\mathbf{e}_9$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_4$	$\lambda\mathbf{e}_5$	$\lambda\mathbf{e}_6$	$\lambda\mathbf{e}_7$
$\mathbf{e}_9$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	$\mathbf{e}_9$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$

Consideration of the right-sided units is connected with solving the vector equation

$$A \circ X = A. \tag{14}$$

Using Table 3 one can represent (14) in the form of the following system of 10 linear equations with coordinates of the right operand $x_0, x_1, \ldots, x_9$ as the unknown

values:

$$\begin{cases} \lambda a_0x_0 + a_1x_4 + \lambda a_2x_8 + a_3x_2 + \lambda a_4x_6 + a_5x_0 + \lambda a_6x_4 + a_7x_8 + \lambda a_8x_2 + a_9x_6 = a_0; \\ \lambda a_0x_1 + a_1x_5 + \lambda a_2x_9 + a_3x_3 + \lambda a_4x_7 + a_5x_1 + \lambda a_6x_5 + a_7x_9 + \lambda a_8x_3 + a_9x_7 = a_1; \\ \lambda a_0x_2 + a_1x_7 + \lambda a_2x_0 + a_3x_4 + \lambda a_4x_8 + a_5x_2 + \lambda a_6x_6 + a_7x_0 + \lambda a_8x_4 + a_9x_8 = a_2; \\ \lambda a_0x_3 + a_1x_8 + \lambda a_2x_1 + a_3x_5 + \lambda a_4x_9 + a_5x_3 + \lambda a_6x_7 + a_7x_1 + \lambda a_8x_5 + a_9x_9 = a_3; \\ \lambda a_0x_4 + a_1x_9 + \lambda a_2x_2 + a_3x_6 + \lambda a_4x_0 + a_5x_4 + \lambda a_6x_8 + a_7x_2 + \lambda a_8x_6 + a_9x_0 = a_4; \\ \lambda a_0x_5 + a_1x_0 + \lambda a_2x_3 + a_3x_7 + \lambda a_4x_1 + a_5x_5 + \lambda a_6x_9 + a_7x_3 + \lambda a_8x_7 + a_9x_1 = a_5; \\ \lambda a_0x_6 + a_1x_1 + \lambda a_2x_4 + a_3x_8 + \lambda a_4x_2 + a_5x_6 + \lambda a_6x_0 + a_7x_4 + \lambda a_8x_8 + a_9x_2 = a_6; \\ \lambda a_0x_7 + a_1x_2 + \lambda a_2x_5 + a_3x_9 + \lambda a_4x_3 + a_5x_7 + \lambda a_6x_1 + a_7x_5 + \lambda a_8x_9 + a_9x_3 = a_7; \\ \lambda a_0x_8 + a_1x_3 + \lambda a_2x_6 + a_3x_0 + \lambda a_4x_4 + a_5x_8 + \lambda a_6x_2 + a_7x_6 + \lambda a_8x_0 + a_9x_4 = a_8; \\ \lambda a_0x_9 + a_1x_4 + \lambda a_2x_7 + a_3x_1 + \lambda a_4x_5 + a_5x_9 + \lambda a_6x_3 + a_7x_7 + \lambda a_8x_1 + a_9x_5 = a_9. \end{cases} \tag{15}$$

If the main determinant of the system (15) $\Delta_A \neq 0$, then there exists unique solution $X = R_A$ which depends on the vector A, i. e., R_A is the local right-sided unit element.

5. Common properties of the 6-dimensional and 10-dimensional FNAAs

Sections 3 and 4 describe the 6-dimensional and 10-dimensional FNAAs defined applying the proposed unified method for setting FNAAs. It is shown that the considered algebras contain a large set of global left-sided units. One can expect that for all even values of the dimension $m \geqslant 6$ the proposed method will define the FNAAs, containing a large set of the global left-sided units. In this section we present some common properties of the described 6-dimensional and 10-dimensional FNAAs. One can suppose that the introduced propositions are valid for other values of the dimension of the FNAAs defined using the both versions (see the Propositions 2.1 and 2.2) of the proposed unified method.

Proposition 5.1. *If the vector A satisfies condition $\Delta_A \neq 0$, then $A \circ L_i \neq A \circ L_j$, for arbitrary two global left-sided units L_i and $L_j \neq L_i$.*

Proof. Suppose $A \circ L_i = A \circ L_j$. Then $A \circ (L_i - L_j) = O$. Since $\Delta_A \neq 0$, the equation $A \circ X = O$ has unique solution $X = O$. Therefore, we have $L_i - L_j = O \Rightarrow L_i = L_j$. The obtained contradiction proves the Proposition 5.1. □

Proposition 5.2. *If the vector equation $X \circ A = B$ has solution $X = S$, then different values $X_i = S \circ L_i$, where L_i takes on all values from the set of global left-sided units, also are solutions of the given equation.*

Proof. $(S \circ L_i) \circ A = S \circ (L_i \circ A) = S \circ A = B$. The Proposition 5.2 is proved. □

Proposition 5.3. *If $A \circ B = L$, where L is a global left-sided unit, then the equality $A^i \circ B^i = L$ holds true for arbitrary natural value i.*

Proof. $A^i \circ B^i = A^{i-1} \circ \left(L \circ B^{i-1}\right) = A^{i-1} \circ B^{i-1} = A^{i-2} \circ B^{i-2} = \cdots = A \circ B = L$. The Proposition 5.3 is proved. □

Proposition 5.4. *If $A \circ B = L$, where L is a global left-sided unit, then the map defined by the formula $\psi(X) = B \circ X \circ A$, where the vector X takes on all values in the considered algebra, represents a homomorphism.*

Proof. Suppose X_1 and X_2 are arbitrary two vectors. Then we have

$$\psi(X_1 \circ X_2) = B \circ (X_1 \circ X_2) \circ A = B \circ (X_1 \circ L \circ X_2) \circ A = (B \circ X_1 \circ A) \circ (B \circ X_2 \circ A) = \psi(X_1) \circ \psi(X_2);$$

$$\psi(X_1 + X_2) = B \circ (X_1 + X_2) \circ A = (B \circ X_1 \circ A) + (B \circ X_2 \circ A) = \psi(X_1) + \psi(X_2).$$

The Proposition 5.4 is proved. □

Proposition 5.5. *The homomorphism-map operation $\psi(X) = B \circ X \circ A$, where $A \circ B = L$, and the exponentiation operation X^i are mutually commutative, i. e., the equality $B \circ X^i \circ A = (B \circ X \circ A)^i$ holds true.*

Proof. Due to Proposition 5.4 we have $\psi(X^i) = (\psi(X))^i$, i. e., $B \circ X^i \circ A = (B \circ X \circ A)^i$. The Proposition 5.5 is proved. □

Multiplication of the elements of the considered FNAA by any fixed global left-sided unit L at right represents a homomorphism map that is mutually commutative with the exponentiation operation. This fact is due to the following two propositions.

Proposition 5.6. *Suppose the vector L is an arbitrary global left-sided unit and the vector X takes on all values in the considered FNAA. Then the map defined by the formula $\varphi(X) = X \circ L$ is a homomorphism.*

Proof. Suppose X_1 and X_2 are arbitrary two 6-dimensional vectors. Then we have

$$\varphi(X_1 \circ X_2) = (X_1 \circ X_2) \circ L = (X_1 \circ L) \circ (X_2 \circ L) = \varphi(X_1) \circ \varphi(X_2);$$

$$\varphi(X_1 + X_2) = (X_1 + X_2) \circ L = X_1 \circ L + X_2 \circ L = \varphi(X_1) + \varphi(X_2).$$

The Proposition 5.6 is proved. □

Proposition 5.7. *The homomorphism-map operation $\varphi(X) = X \circ L$, where L is a global left sided unit, and the exponentiation operation X^i are mutually commutative, i. e., the equality $X^i \circ L = (X \circ L)^i$ holds true.*

Proof. Due to Proposition 5.6 we have $\varphi(X^i) = (\varphi(X))^i$, i. e., $X^i \circ L = (X \circ L)^i$. The Proposition 5.7 is proved. □

Every global left sided unit L is connected with different homomorphism map operations of other type which can be described with the following formula:

$$\psi(X) = A^i \circ X \circ B^i,$$

where $i \geqslant 1$ is an arbitrary non-negative integer and the vectors A and B are such that $A \circ B = L$ holds true.

Each of the homomorphism map operations $\psi(X)$ and $\varphi(X)$ is mutually commutative with the exponentiation operation and represents interest for using it as masking operation at setting new types of the HDLP. The next propositions show that the local right-sided unit R_A related the the vector A such that $\Delta_A \neq 0$ (the main determinant of the system of linear equation written for computing the right-sided units) is contained in the set of the global left-sided units, i. e. the value R_A is simultaneously the local two-sided unit of the vector A. Therefore the vectors A for which we have $\Delta_A \neq 0$ are called locally invertible vectors.

Proposition 5.8. *Suppose the vector A is such that $\Delta_A \neq 0$. Then the sequence $A, A^2, \ldots, A^i, \ldots$ is periodic and for some positive integer ω we have $A^\omega = R_A$.*

Proof. Assumption that the sequence $A, A^2, \ldots, A^i, \ldots$ contains the zero vector $O = (0, 0, 0, 0, 0, 0)$ leads to a contradiction. Indeed, due to the condition $\Delta_A \neq 0$ we have $A \neq O$. If for some natural number $j > 1$ we have $A^j = O$, then for some positive integer $k \leq j$ the conditions $A^{k-1} \neq O$ and $A^k = O$ holds true. Therefore, $A \circ A^{k-1} = O$. Since $\Delta_A \neq 0$ and $X = O$ satisfies the equation $A \circ X = O$, the last equation has unique solution $X = O$, i. e., $A^{k-1} = O$. The obtained contradiction proves that the considered sequence does not include the zero vector O. Therefore, due to finiteness of the considered algebra the indicated sequence is periodic. Then for some minimum $t > 1$ we have

$$\left\{A = A^t = A^{t-1} \circ A = A \circ A^{t-1}\right\} \Rightarrow E_A = A^{t-1},$$

where E_A is the local two-sided unit connected with the vector A. Evidently, due to condition $\Delta_A \neq 0$ we have $A \circ E_A - A \circ R_A = A \circ (E_A - R_A) = O \;\Rightarrow\; E_A - R_A = O \;\Rightarrow\; E_A = R_A$. Therefore, for $\omega = t - 1$ we have $A^\omega = R_A$. □

Proposition 5.9. *Suppose the vector A is such that the conditions $\Delta_A \neq 0$, $\Delta'_A \neq 0$, and $\Delta''_A \neq 0$ holds true. Then the local right-sided unit R_A is contained in the set of the global left-sided units.*

Proof. Due to the Proposition 5.8 we have $R_A = E_A$ and $E_A \circ A = A$, i. e., R_A acts on the vector A as the left-sided unit, but all left sided units of the vector A are included in the set of global left-sided units. □

6. On potential cryptographic application of the introduced FNAAs

In the case of defining of the HDLP in the 6-dimensional FNAAs containing many different global left-sided units, which are described in Section 3, the formula (1) cannot be used because these algebras contains no globally invertible element. However by analogy with the formula (1) one can use the mutual commutativity of the homomorphism-map operations ψ and φ with the exponentiation operation (see the Propositions 5.5 and 5.7) as follows.

Suppose the vectors A and B are such that $\Delta_A \neq 0$ and $A \circ B = L_0$, where L_0 is a global left-sided unit. Then using some locally invertible vector N satisfying the conditions $\Delta_N \neq 0$ and $N \circ A \neq A \circ N$ one can define computation of the public key Y by the next formula:

$$Y = B^t \circ N^x \circ A^t = \left(B^t \circ N \circ A^t\right)^x, \tag{16}$$

where the vectors A, B, and N are the known parameters and the positive integers (t, x) are the unknown values generated at random and used as the private key.

The formula (16) defines a particular form of the HDLP which can be used in the public key-agreement scheme in frame of which the common secret shared by some two users is calculated as follows

$$Z = B^{t_1} \circ Y_2^{x_1} \circ A^{t_1} = B^{t_2} \circ Y_1^{x_2} \circ A^{t_2},$$

where the vectors Y_1 and Y_2 (the pairs (t_1, x_1) and (t_2, x_2)) are the public (private) keys of the first and the second users correspondingly. Thus, this public key-agreement scheme performs correctly, however estimating its security is currently an open problem that require individual study.

For the development of the post-quantum public key-agreement schemes one can propose another form of the HDLP in which the connection between the public and private keys is complicated by introducing the additional masking element of the private key, which represents the unit element L selected at random from the set of the global left-sided units. The element L is used in the formula for calculating the public key as the *rightmost* operand, therefore the value L significantly influences the value Y. The proposed form of the HDLP is described by the following formula for computing the public key:

$$Y = B^t \circ N^x \circ A^t \circ L = \left(B^t \circ N \circ A^t\right)^x \circ L,$$

where the integers t and x and the vector L represent three elements of the corresponding private key. One can easily show that the public keys represented in the last form also provide possibility of the public key-agreement. Investigation of the security of such modified public key-agreement scheme also is an open problem for independent study.

The idea of using the modifications of the multiplication operation as elements of the private key in the public-key cryptoschemes represents special interest. For example, such key operations can be used as additional masking operations for setting novel forms of the HDLP in the FNAAs with parametrizable multiplication operation with mutual associativity of all pairs of the modifications of the multiplication operation. In future research we will pay significant attention to the design of the public-key cryptoschemes in which the modifications of the multiplication operation are used as the elements of private key.

7. Conclusion

The proposed unified method for defining FNAAs provides possibility to set a class of algebras every one of which contains a large set global left sided units. The method is implemented in two versions that are described by formulas (5) and (6) relating to even and odd value of the parameter d correspondingly. In the case of even values d there are set FNAAs with parametrizable multiplication operation characterized in that all pairs of the modifications of the multiplication operation are mutually associative. This subclass of algebras is very attractive as algebraic support of the public-key cryptoschemes in which the modifications of the multiplication operation are used as elements of the private key. However, the design of the cryptoschemes of such type is a task of individual research.

In general case the FNAAs containing a large set of the global left-sided units can be applied as algebraic support of the HDLP-based public-key cryptoschemes and new forms of the HDLP characterized in using the homomorphism-map operations of the ψ-type and φ-type as masking operations. Estimation of the security of the cryptoschemes of the last type to quantum attacks represents an attractive task of independent work.

Acknowledgments. The author thanks anonymous Referee for valuable remarks.

References

[1] First NIST standardization conference - April 11–13, 2018. http://prometheuscrypt.gforge.inria.fr/2018-04- 18.pqc2018.html

[2] *Post-Quantum Cryptography*, Lecture Notes Computer Sci., **10786** (2018).

[3] **I. Anshel, M. Anshel, D. Goldfeld**, *An algebraic method for public key cryptography*, Math. Research Letters, **6** (1999), 287 – 291.

[4] **P. Hiranvanichakorn**, *Provably authenticated group key agreement based on braid groups: The dynamic case*, Intern. J. Network Security, **19** (2017), 517 – 527.

[5] **A.S. Kuzmin, V.T. Markov, A.A. Mikhalev, A.V. Mikhalev, A.A. Nechaev**, *Cryptographic algorithms on groups and algebras*, J. Math. Sci., **223** (2017), 629 – 641.

[6] **E. Lee, J.H. Park**, *Cryptanalysis of the public key encryption based on braid groups*, Lecture Notes Computer Sci., **2656** (2003), 477 – 489.

[7] **A.A. Moldovyan**, *General method for defining finite non-commutative associative algebras of dimension m>1*, Bul. Acad. Sti. Republ. Moldova. Matematica, **2(87)** (2018), 95 – 100.

[8] **A.A. Moldovyan, N.A. Moldovyan**, *Post-quantum signature algorithms based on the hidden discrete logarithm problem*, Computer Sci. J. Moldova, **26** (2018), 301 – 313.

[9] **A.A. Moldovyan, N.A. Moldovyan**, *Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem*, Bull. South ural State Univ., ser. Math. Modelling, Programming ana Computer Software, **12** (2019), no. 1, 66 – 81.

[10] **A.A. Moldovyan, N.A. Moldovyan, V.A. Shcherbacov**, *Non-commutative finite associative algebras of 2-dimension vectors*, Computer Sci. J. Moldova, **25** (2017), 344 – 356.

[11] **D.N. Moldovyan**, *Non-commutative finite groups as primitive of public-key cryptoschemes*, Quasigroups and Related Systems, **18** (2010), 165 – 176.

[12] **D.N. Moldovyan, N.A. Moldovyan**, *Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms*, Quasigroups and Related Systems. **18** (2010), no. 2, 177 – 186.

[13] **D.N. Moldovyan, N.A. Moldovyan, V.A. Shcherbacov**, *Non-commutative finite associative algebras of 3-dimensional vectors*, Quasigroups and Related Systems, **26** (2018), 109 – 120.

[14] **N.A. Moldovyan**, *Finite non-commutative associative algebras for setting the hidden discrete logarithm problem and post-quantum cryptoschemes on its base*, Bul. Acad. Sti. Republ. Moldova, Matematica, **1** (2019), 71 – 78.

[15] **P.W. Shor**, *Polynomial-time algorithm for prime factorization and discrete logarithms on quantum computer*, SIAM J. Computing, **26** (1997), 1484 – 1509.

[16] **G.K. Verma**, *Probable security proof of a blind signature scheme over braid groups*, Intern. J. Network Security, **12** (2011), no. 2, 118 – 120.

Received January 2, 2019

St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
14-th line 39, 199178, St. Petersburg, Russia
E-mail: mdn.spectr@mail.ru

Quasigroups and Related Systems **27** (2019), 309 – 316

Semirings which are distributive lattices of weakly left k-Archimedean semirings

Tapas Kumar Mondal

Abstract. We introduce a binary relation $\xrightarrow{l}$ on a semiring S, and generalize the notion of left k-Archimedean semirings and introduce weakly left k-Archimedean semirings, via the relation $\xrightarrow{l}$. We also characterize the semirings which are distributive lattices of weakly left k-Archimedean semirings.

1. Introduction

The notion of the semirings was introduced by Vandiver [12] in 1934. The underlying algebra in idempotent analysis [6] is a semiring. Recently idempotent analysis have been used in theoretical physics, optimization etc., various applications in theoretical computer science and algorithm theory [5, 7]. Though the idempotent semirings have been studied by many authors like Monico [8], Sen and Bhuniya [11] and others as a $(2, 2)$ algebraic structure, idempotent semirings are far different from the semirings whose multiplicative reduct is just a semigroup and additive reduct is a semilattice. So for better understanding about the abstract features of the particular semirings $\mathbb{R}_{max}$(Maslov's dequantization semiring), Max-Plus algebra, syntactic semirings we need a separate attention to the semirings whose additive reduct is a semilattice. From the algebraic point of view while studying the structure of semigroups, semilattice decomposition of semigroups, an elegant technique, was first defined and studied by Clifford [4]. This motivated Bhuniya and Mondal to study on the structure of semirings whose additive reduct is a semilattice [1, 2, 9, 10]. In [1], Bhuniya and Mondal studied the structure of semirings with a semilattice additive reduct. There, the description of the least distributive lattice congruence on such semirings was given. In [10], Mondal and Bhuniya gave the distributive lattice decompositions of the semirings into left k-Archimedean semirings. In this paper we generalize the notion of left k-Archimedean semirings introducing weakly left k-Archimedean semirings, analogous to the notion of weakly left k-Archimedean semigroups [3] and characterize the semirings which

2010 Mathematics Subject Classification: 16Y60
Keywords: left k-Archimedean semiring; weakly left k-Archimedean semiring; distributive lattice; distributive lattices of left k-Archimedean semirings; distributive lattices of weakly left k-Archimedean semirings.
The work is financially supported by UGC(ERO) under Minor Research Project No. F. PSW-120/11-12(ERO), India.

are distributive lattices of weakly left k-Archimedean semirings.

The preliminaries and prerequisites for this article has been discussed in section 2. In section 3 we introduce the notion of weakly left k-Archimedean semirings. We give a sufficient condition for a semiring S to be weakly left k-Archimedean in terms of a binary relation $\xrightarrow{l}$ on S. We also give a condition under which a weakly left k-Archimedean semiring becomes a left k-Archimedean semiring. In section 4 we characterize the semirings which are distributive lattices of weakly left k-Archimedean semirings.

2. Preliminaries and prerequisites

A *semiring* $(S, +, \cdot)$ is an algebra with two binary operations $+$ and $\cdot$ such that both the *additive reduct* $(S, +)$ and the *multiplicative reduct* $(S, \cdot)$ are semigroups and such that the following distributive laws hold:

$$x(y + z) = xy + xz \text{ and } (x + y)z = xz + yz.$$

Thus the semirings can be viewed as a common generalization of both rings and distributive lattices. A band is a semigroup F in which every element is an idempotent. Moreover if it is commutative, then F is called a semilattice. Throughout the paper, unless otherwise stated, S is always a semiring with semilattice additive reduct.

Every distributive lattice D can be regarded as a semiring $(D, +, \cdot)$ such that both the additive reduct $(D, +)$ and the multiplicative reduct $(D, \cdot)$ are semilattices together with the absorptive law:

$$x + xy = x \text{ for all } x, y \in S.$$

An equivalence relation ρ on S is called a congruence relation if it is compatible with both the addition and multiplication, i.e., for $a, b, c \in S, a\rho b$ implies $(a + c)\rho(b + c), ac\rho bc$ and $ca\rho cb$. A congruence relation ρ on S is called a distributive lattice congruence on S if the quotient semiring S/ρ is a distributive lattice. Let $\mathcal{C}$ be a class of semirings which we call C-semirings. A semiring S is called a distributive lattice of C-semirings if there exists a congruence ρ on S such that S/ρ is a distributive lattice and each ρ-class is a semiring in $\mathcal{C}$.

Let S be a semiring and $\phi \neq A \subseteq S$. Then the k-closure of A is defined by $\overline{A} = \{x \in S \mid x + a_1 = a_2 \text{ for some } a_i \in A\} = \{x \in S \mid x + a = a \text{ for some } a \in A\}$, and the k-radical of A by $\sqrt{A} = \{x \in S \mid (\exists\, n \in \mathbb{N})\ x^n \in \overline{A}\}$. Then $\overline{A} \subseteq \sqrt{A}$ by definition, and $A \subseteq \overline{A}$ since $(S, +)$ is a semilattice. A non empty subset L of S is called a left (resp. right) ideal of S if $L + L \subseteq L$, and $SL \subseteq L$ (resp. $LS \subseteq L$). A non empty subset I of S is called an ideal of S if it is both left and a right ideal of S. An ideal (resp. left ideal) A of S is called a k-ideal (left k-ideal) of S if and only if $\overline{A} = A$.

Lemma 2.1. (cf. [1]) *Let S be a semiring.*

(a) *For $a, b \in S$ the following statements are equivalent*

  (i) *There are $s_i, t_i \in S$ such that $b + s_1 a t_1 = s_2 a t_2$.*

  (ii) *There are $s, t \in S$ such that $b + sat = sat$.*

  (iii) *There is $x \in S$ such that $b + xax = xax$.*

(b) *If $a, b, c \in S$ such that $b + xax = xax$ and $c + yay = yay$ for some $x, y \in S$, then there is $z \in S$ such that $b + zaz = zaz = c + zaz$.*

(c) *If $a, b, c \in S$ such that $c + xax = xax$ and $c + yby = yby$ for some $x, y \in S$, then there is $z \in S$ such that $c + zaz = zaz$ and $c + zbz = zbz$.*

Lemma 2.2. (cf. [1]) *For a semiring S and $a, b \in S$ the following statements hold.*

1. *$\overline{SaS}$ is a k-ideal of S.*
2. *$\sqrt{SaS} = \sqrt{\overline{SaS}}$.*
3. *$b^m \in \sqrt{SaS}$ for some $m \in \mathbb{N} \Leftrightarrow b^k \in \sqrt{SaS}$ for all $k \in \mathbb{N}$.*

Lemma 2.3. (cf. [10]) *Let S be a semiring.*

(a) *For $a, b \in S$ the following statements are equivalent:*

  (i) *there are $s_i \in S$ such that $b + s_1 a = s_2 a$,*

  (ii) *there are $s \in S$ such that $b + sa = sa$.*

(b) *If $a, b, c \in S$ such that $c + xa = xa$ and $d + yb = yb$ for some $x, y \in S$, then there is some $z \in S$ such that $c + za = za$ and $d + zb = zb$.*

Theorem 2.4. (cf. [10]) *The following conditions on a semiring S are equivalent:*

1. *S is a distributive lattice of left k-Archimedean semirings,*
2. *for all $a, b \in S$, $b \in \overline{SaS}$ implies that $b \in \sqrt{Sa}$,*
3. *for all $a, b \in S$, $ab \in \sqrt{Sa}$,*
4. *$\sqrt{L}$ is a k-ideal of S, for every left k-ideal L of S,*
5. *$\sqrt{Sa}$ is a k-ideal of S, for all $a \in S$,*
6. *for all $a, b \in S, \sqrt{Sab} = \sqrt{Sa} \cap \sqrt{Sb}$.*

3. Weakly left k-Archimedean semirings

In [1], Bhuniya and Mondal studied the structure of semirings, and during this they gave the description of the least distributive lattice congruence on a semiring S stem from the divisibility relation defined by: for $a, b \in S$, $a|b \iff b \in \overline{SaS}$,

$$a \longrightarrow b \iff b \in \sqrt{SaS} \iff b^n \in \overline{SaS} \quad \text{for some } n \in \mathbb{N}.$$

Thus it follows from the Lemma 2.1, $a \longrightarrow b \iff b^n + xax = xax$, for some $n \in \mathbb{N}$ and $x \in S$.

In this section we introduce the relation $\xrightarrow{l}$(left analogue of $\longrightarrow$) on a semiring S, the notion of weakly left k-Archimedean semirings and study them.

Proposition 3.1. *Let S be a semiring. Then $\overline{Sa}$ is a left k-ideal of S for every $a \in S$.*

Proof. For $b, c \in \overline{Sa}$, there is $x \in S$ such that $b+xa = xa = c+xa$, by Lemma 2.3. This implies $(b + c) + xa = xa$, i.e., $b + c \in \overline{Sa}$. Moreover, for any $s \in S$ we get $sb+sxa = sxa$, and so $sb \in \overline{Sa}$. For $u \in \overline{\overline{Sa}}$ there is some $b \in \overline{Sa}$ such that $u+b = b$. Using again $b+xa = xa$ for some $x \in S$, we get $u+xa = u+b+xa = b+xa = xa$, i.e., $u \in \overline{Sa}$. So $\overline{Sa} = \overline{\overline{Sa}}$ is a left k-ideal of S. □

Now we introduce the relation $\xrightarrow{l}$ on a semiring S as a generalization of the division relation $|_l$, and they are given by: for $a, b \in S$, $a \mid_l b \iff b \in \overline{Sa}$,

$$a \xrightarrow{l} b \iff b \in \sqrt{Sa} \iff b^n \in \overline{Sa} \quad \text{for some } n \in \mathbb{N}.$$

Thus $a \xrightarrow{l} b$ if there exist some $n \in \mathbb{N}$ and $x \in S$ such that $b^n + xa = xa$, by Lemma 2.3.

In [10], Mondal and Bhuniya defined *left k-Archimedean semirings* as: A semiring S is called left k-Archimedean if for all $a \in S$, $S = \sqrt{Sa}$. For example, let $A = \{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\}$, define $+$ and $\cdot$ on $S = A \times A$ by: for all $(a, b), (c, d) \in S$

$$(a, b) + (c, d) = (\max\{a, c\}, \max\{b, d\}), \quad (a, b) \cdot (c, d) = (ac, b).$$

Then $(S, +, \cdot)$ is a left k-Archimedean semiring.

We now introduce a more general notion:

A semiring S will be called *weakly left k-Archimedean* if $ab \xrightarrow{l} b$, for all $a, b \in S$.

Example 3.2. Let $A = \{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\}$, define $+$ and $\cdot$ on $S = A \times A$ by: for all $(a, b), (c, d) \in S$

$$(a, b) + (c, d) = (\max\{a, c\}, \max\{b, d\}), \quad (a, b) \cdot (c, d) = (ac, d).$$

Then $(S, +, \cdot)$ is a weakly left k-Archimedean semiring. Now let $(a, \frac{1}{2}), (c, \frac{1}{3}) \in S$. If possible, let there exist $n \in \mathbb{N}$ and $(x, y) \in S$ satisfying $(a, \frac{1}{2})^n + (x, y) \cdot (c, \frac{1}{3}) = (x, y) \cdot (c, \frac{1}{3})$. This implies $(a^n, \frac{1}{2}) + (xc, \frac{1}{3}) = (xc, \frac{1}{3})$ so that $max\{a^n, xc\} = xc$, $max\{\frac{1}{2}, \frac{1}{3}\} = \frac{1}{3}$, which is not possible. Consequently, $(S, +, \cdot)$ is not a left k-Archimedean semiring.

Here we see that the relation $\xrightarrow{l}$ is not symmetric on a semiring S in general. For, consider the Example 3.2, there $(a, \frac{1}{2}) \xrightarrow{l} (c, \frac{1}{3})$ but not $(c, \frac{1}{3}) \xrightarrow{l} (a, \frac{1}{2})$. Although, the semiring S is weakly left k-Archimedean. Now, in the following proposition we show that if the relation $\xrightarrow{l}$ is symmetric on a semiring S, then S is weakly left k-Archimedean.

Proposition 3.3. *A semiring S is weakly left k-Archimedean if the relation $\xrightarrow{l}$ is symmetric on S.*

Proof. Let $\xrightarrow{l}$ is a symmetric relation on S and $a, b \in S$. Now $ab \in \overline{Sb}$ implies that $b \xrightarrow{l} ab$ and so $ab \xrightarrow{l} b$, by symmetry of $\xrightarrow{l}$ on S. Thus S is weakly left k-Archimedean. □

Thus the condition of symmetry of $\xrightarrow{l}$ is only sufficient for a semiring S to be weakly left k-Archimedean, not necessary. Let S be a left k-Archimedean semiring, and $a, b \in S$. Then $b \in \sqrt{Sa}$ implies that $b^n + sa = sa$ for some $n \in \mathbb{N}$ and $s \in S$. Multiplying b on both sides on the right we get $b^{n+1} + sab = sab$. This yields $ab \xrightarrow{l} b$ so that S is a weakly left k-Archimedean semiring. Thus we have the following proposition:

Proposition 3.4. *Every left k-Archimedean semiring S is a weakly left k-Archimedean semiring.*

Here in the following proposition we find a condition for which the converse holds:

Proposition 3.5. *Let S be a semiring, and $ab \in \sqrt{Sa}$, for all $a, b \in S$ hold. Then S is left k-Archimedean semiring if it is weakly left k-Archimedean.*

Proof. Let $a, b \in S$. Then $ba \xrightarrow{l} a$, whence by Lemma 2.3, there are $n \in \mathbb{N}$ and $s \in S$ such that $a^n + sba = sba$. Again by hypothesis, there are $m \in \mathbb{N}$ and $t \in S$ such that $(sba)^m + tsb = tsb$. Now $a^m + sba = sba$ implies that $a^{nm} + (sba)^m = (sba)^m$. Adding tsb on both sides we get $a^{nm} + [(sba)^m + tsb] = [(sba)^m + tsb]$, i.e. $a^{nm} + tsb = tsb \in \overline{Sb}$. So $a \in \sqrt{Sb}$. Thus S is a left k-Archimedean semiring. □

Now, by Theorem 2.4, we see that a weakly left k-Archimedean semiring will be a left k-Archimedean semiring if it is a distributive lattice of left k-Archimedean semirings.

4. Lattices of weakly left k-Archimedean semirings

In this section we characterize the semirings which are distributive lattices of weakly left k-Archimedean semirings. A semiring S is called a *distributive lattice of weakly left k-Archimedean semirings* if there exists a congruence ρ on S such that S/ρ is a distributive lattice and each ρ-class is a weakly left k-Archimedean semiring.

Lemma 4.1. *Suppose S is a distributive lattice $\mathcal{D}$ of subsemirings $S_\alpha, \alpha \in \mathcal{D}$. Then $a, b \in S_\alpha,\ \alpha \in \mathcal{D}$, then $a \xrightarrow{l} b$ in S implies that $a \xrightarrow{l} b$ in S_α.*

Proof. Let ρ be a distributive lattice congruence on S so that S is a distributive lattice $\mathcal{D}$ of subsemirings $S_\alpha, \alpha \in \mathcal{D}$. Let $a \xrightarrow{l} b$. Then $b^n + xa = xa$ for some $n \in \mathbb{N}, x \in S$. Let $x \in S_\beta, \beta \in \mathcal{D}$. Now $b^{n+1} + bxa = bxa$, and so $b\rho(b + bxa)\rho(b^{n+1} + bxa) = bxa\rho abx$, i.e., $b\rho abx$. This implies $\alpha = \alpha\alpha\beta = \alpha\beta$, since $\mathcal{D}$ is a distributive lattice. Now $b^{n+1} + bxa = bxa \in S_{\alpha\beta}a = S_\alpha a$ so that $b^{n+1} \in \overline{S_\alpha}a$. Consequently, $a \xrightarrow{l} b$ in S_α. □

Now we are in a position to present the main result of this paper. Here we characterize the semirings which are distributive lattices of weakly left k-Archimedean semirings.

Theorem 4.2. *The following conditions are equivalent on a semiring S:*

(1) *S is a distributive lattice of weakly left k-Archimedean semirings,*

(2) *for all $a, b \in S,\ a \longrightarrow b \Rightarrow ab \xrightarrow{l} b$.*

Proof. (1) $\Rightarrow$ (2). Let S be a distributive lattice $D = S/\rho$ of weakly left k-Archimedean semirings $S_\alpha, \alpha \in D$, ρ being the corresponding distributive lattice congruence. Let $a, b \in S$ such that $a \longrightarrow b$ so that there are $n \in \mathbb{N}$ and $s \in S$ such that $b^n + sas = sas$, by Lemma 2.1. Also there are $\alpha, \beta \in D$ such that $a \in S_\alpha, b \in S_\beta$. Now $(b + sas)\rho(b^n + sas) = sas\rho as^2$. So $b\rho(b^2 + bsas)\rho bas^2$, which implies $b\rho(b + ba)\rho(bas^2 + ba)\rho ba$ and thus $ba \in S_\beta$. Since S_β is a weakly left k-Archimedean semiring, $b^n \in \overline{S_\beta bab} \subseteq \overline{Sab}$ for some $n \in \mathbb{N}$ yielding $ab \xrightarrow{l} b$.

(2) $\Rightarrow$ (1). By Lemma 2.2, for $a, b \in S, (ab)^2 \in \overline{SaS}$ implies that $a \longrightarrow ab$. So by hypothesis, $a^2b = a(ab) \xrightarrow{l} (ab)$. This shows that $(ab)^n \in \overline{Sa^2b} \subseteq \overline{Sa^2S}$, for some $n \in \mathbb{N}$. Then by Theorem 4.3[1], S is a distributive lattice$(D = S/\eta)$ of k-Archimedean semirings $S_\alpha, \alpha \in D$, where η is the least distributive lattice congruence on S. Let $a, b \in S_\alpha$. Then $a \longrightarrow b$ and so $ab \xrightarrow{l} b$ in S. Then by Lemma 4.1, one gets $ab \xrightarrow{l} b$ in S_α. Thus S_α is weakly left k-Archimedean. □

Now we give an example of a semiring which is a distributive lattice of left k-Archimedean semirings, whence a distributive lattice of weakly left k-Archimedean semirings.

Example 4.3. Consider the set $\mathbb{N}$ of all natural numbers, and define $+$ and $\cdot$ on $S = \mathbb{N} \times \mathbb{N}$ by: for all $(a, b), (c, d) \in S$

$$(a, b) + (c, d) = (\min\{a, c\}, \min\{b, d\}), \quad (a, b) \cdot (c, d) = (ac, b).$$

Then S is a distributive lattice of left k-Archimedean semirings.

Example 4.4. Consider the set $\mathbb{N}$ of all natural numbers, and define $+$ and $\cdot$ on $S = \mathbb{N} \times \mathbb{N}$ by: for all $(a, b), (c, d) \in S$

$$(a, b) + (c, d) = (\min\{a, c\}, \min\{b, d\}), \quad (a, b) \cdot (c, d) = (ac, d).$$

Then S is a distributive lattice of weakly left k-Archimedean semirings. But S is not a distributive lattice of left k-Archimedean semirings. Indeed, for $(1, 2), (2, 2) \in S$ suppose there exist $n \in \mathbb{N}$ and $(x, y) \in S$ satisfying $[(1, 2) \cdot (2, 1)]^n + (x, y) \cdot (1, 2) = (x, y) \cdot (1, 2)$. This implies $(2^n, 1) + (x, 2) = (x, 2)$, i.e. $\min\{2^n, x\} = x$, $\min\{1, 2\} = 2$. The last equality is absurd.

References

[1] **A.K. Bhuniya and T.K. Mondal**, *Distributive lattice decompositions of semirings with a semilattice additive reduct*, Semigroup Forum, **80** (2010), 293 – 301.

[2] **A.K. Bhuniya and T.K. Mondal**, *On the least distributive lattice congruence on a semiring with a semilattice additive reduct*, Acta Math. Hungar., **147** (2015), 189 – 204.

[3] **S. Bogdanović and M. Ćirić**, *Semilattices of weakly left Archimedean semigroups*, Filomat(Niš), **9** (1995), 603 – 610.

[4] **A.H. Clifford**, *Semigroups admitting relative inverses*. Ann. Math., **42** (1941), 1037 – 1049.

[5] **U. Hebisch and H.J. Weinert**, *Semirings: Algebraic theory and applications in computer science*, World Scientific, (Singapore, 1998).

[6] **G.L. Litvinov, V.P. Maslov and G.B. Shpiz**, *Idempotent functional analysis: An algebraic approach*. arXiv:math/0009128v2.

[7] **G.L. Litvinov and V.P. Maslov**, *The correspondence principle for idempotent calculus and some computer applications. Idempotency*, Publ. Nerwton Inst., **11** (1998), 420 – 443.

[8] **C. Monico** *On finite congruence-simple semirings*, J. Algebra, **271** (2004), 846 – 854.

[9] **T.K. Mondal and A.K. Bhuniya**, *On k-radicals of Green's relations in semirings with a semilattice additive reduct*, Discuss. Math., General Algebra Appl., **33** (2013), 85 – 93.

[10] **T.K. Mondal and A.K. Bhuniya**, *On distributive lattices of left k-Archimedean semirings*, Mathematica (Cluj), in print.

[11] **M.K. Sen and A.K. Bhuniya**, *On semirings whose additive reduct is a semilattice*, Semigroup Forum, **82** (2011), 131 – 140.

[12] **H.S. Vandiver**, *Note on a simple type of algebra in which the cancellation law of addition does not hold*, Bull. Amer. Math. Soc., **40** (1934), 914 – 920.

Received May 04, 2019

Department of Mathematics
Dr. Bhupendra Nath Dutta Smriti Mahavidyalaya
Hatgobindapur – 713407
Purba Bardhaman, West Bengal
India
E-mail: tapumondal@gmail.com

Quasigroups and Related Systems **27** (2019), 317 – 324

Means compatible with semigroup laws

Ranganathan Padmanabhan and Alok Shukla

Abstract. A binary mean operation $m(x, y)$ is said to be compatible with a semigroup law $*$, if $*$ satisfies the Gauss' functional equation $m(x, y) * m(x, y) = x * y$ for all x, y. Thus the arithmetic mean is compatible with the group addition in the set of real numbers, while the geometric mean is compatible with the group multiplication in the set of all positive real numbers. Using one of the Jacobi theta functions, Tanimoto [6], [7] has constructed a novel binary operation $*$ compatible with the arithmetico-geometric mean $\mathrm{agm}(x, y)$ of Gauss. Tanimoto shows that it is only a loop operation, but not associative. A natural question is to ask if there exists a group law $*$ compatible with arithmetic-geometric mean. In this paper we prove that there is no semigroup law compatible with agm and hence, in particular, no group law either. Among other things, this explains why Tanimoto's operation $*$ using theta functions must be non-associative.

1. Introduction

Gauss discovered the arithmetico-geometric mean (agm) at the age of 15. Starting with two positive real numbers x and y, Gauss considered the sequences $\{x_n\}$ and $\{y_n\}$ of arithmetic and geometric means

$$x_0 = x, \quad y_0 = y, \quad x_n = \frac{x_{n-1} + y_{n-1}}{2}, \quad y_n = \sqrt{x_{n-1} y_{n-1}}, \quad \text{for } n \geqslant 1.$$

Then Gauss defined $\mathrm{agm}(x, y)$ to be the common limit of the sequences $\{x_n\}$ and $\{y_n\}$, i.e.,

$$\mathrm{agm}(x, y) = \lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n. \tag{1}$$

For an engaging historical account on agm and its applications in mathematics readers are referred to [1],[2].

In this paper, we ask if there exist a group law $*$, which is compatible with agm. Before proceeding further we give some definitions relevant to this work.

Definition 1.1 (See for example, [5]). Let S be a set equipped with a binary operation m. It is said that m is a *mean*, if it satisfies the following

(M_1) $m(x, x) = x$,

2010 Mathematics Subject Classification: Primary: 20N05; Secondary: 26E60
Keywords: arithmetic mean, geometric mean, harmonic mean, arithmetic-geometric mean, compatible group law, loops, medial law.

(M_2) $m(x,y) = m(y,x)$,

(M_3) $m(x,y) = m(z,y) \implies x = z$.

Definition 1.2 (Compatibility of binary operations)**.** Let S be a set equipped with a binary mean operation m and another binary operation $*$. The binary mean operation m, and the binary operation $*$, are said to be *compatible* with each other, if $m(x,y) * m(x,y) = x * y$ for all $x, y \in S$.

Here we find conditions on the mean m which force any compatible operation $*$ to be a group operation.

Let $\mathrm{AM}(x,y) = \dfrac{x+y}{2}$ be the arithmetic mean of $x, y \in \mathbb{R}$ with $+$ being the usual addition in $\mathbb{R}$. Then clearly $\mathrm{AM}(x,y) + \mathrm{AM}(x,y) = x + y$, therefore, the classical arithmetic mean $\mathrm{AM}(x,y)$ is compatible with the group law of $+$ in $\mathbb{R}$, in the sense of Definition 1.2. Similarly, the geometric mean GM is also compatible with the group law of multiplication in positive reals. Similarly, it can be verified that the harmonic mean $h(x,y) = \dfrac{2xy}{x+y}$ is compatible with the semigroup law $x*y = \dfrac{xy}{x+y}$. It is then natural to consider if there exists any such group operation over $\mathbb{R}^+$, which is compatible with the arithmetic-geometric mean (agm) of Gauss. In other words, we want to address the question, if there exists a group operation $*$, such that $\mathrm{agm}(x,y) * \mathrm{agm}(x,y) = x * y$. Using one of the Jacobi theta functions, Shinji Tanimoto has successfully constructed a non-associative loop operation $\star$ (c.f. [6], [7], Sec. below) that is compatible with agm. However, no group law $*$ compatible with agm is known to exist. Indeed, we prove that no such group law $*$ can exist, which is compatible with agm.

1.1. A non-associative loop operation compatible with agm

Now we recall the binary operation $\star$ introduced by S. Tanimoto in [6], [7].

Definition 1.3 (Tanimoto, [6], [7])**.** For any two positive numbers x and y, choose the unique q $(-1 < q < 1)$ such that $1/\mathrm{agm}(x,y) = \theta^2(q)$. Here, θ is one of the Jacobi theta functions:

$$\theta(q) = \sum_{n=-\infty}^{+\infty} q^{n^2} = 1 + 2\sum_{n=1}^{\infty} q^{n^2}.$$

Then define

$$x \star y = \theta^2(-q)/\theta^2(q). \tag{2}$$

We also recall the following theorems from [7], which describe the properties of the $\star$ operation. We note that here variables x, y are positive real numbers.

Theorem 1.4 (Tanimoto, [7]). *The operation $\star$ defined above satisfies the following properties.*
(A) $1 \star x = x$ for all x. *Hence* 1 *is the unit element of the operation.*
(B) $x \star x = y \star y$ *implies* $x = y$.
(C) $x \star y = \mathrm{agm}(x, y) \star \mathrm{agm}(x, y)$. *Thus the mean with respect to the operation is the* agm.

Theorem 1.5 (Tanimoto, [7]). *The operation $\star$ satisfies the following algebraic properties.*
(D) $a \star x = a \star y$ *implies* $x = y$ (*a cancellation law*).
(E) $(ax) \star (ay) = a \star (a(x \star y))$ *for any* a, x, y (*a distributive law*).
(F) *If* $z = x \star y$, *then* $y = x(x^{-1} \star (x^{-1}z))$. *In particular, the inverse of* x *with respect to the operation is* $x(x^{-1} \star x^{-1})$.

Finally, we note that Tanimoto claims that the $\star$ operation is not associative (although, he does not give any example).

2. Main results

Now we are ready to prove our claim that there does not exist any group law $*$, that is compatible with agm in the sense of the Definition 1.2. In this direction, first we prove the following theorem.

Theorem 2.1. *Let $m(x, y)$ and $*$ be two binary operations defined over a nonempty set containing a distinguished element e such that*

(M_1) $m(x, x) = x$,

(M_2) $m(x, y) = m(y, x)$,

(M_3) $m(x, y) = m(z, y) \implies x = z$,

(M_4) $m(x, y) * m(x, y) = x * y$. (*Gauss' Functional Equation*),

(M_5) $e * x = x$,

(M_6) $x * x = y * y \implies x = y$.

Then m is medial, i.e., $m(m(x, y), m(z, u)) = m(m(x, z), m(y, u))$ if and only if the $*$ operation is associative.

Before proving Theorem 2.1, we state and prove the following lemmas.

Lemma 2.2. *Under the hypothesis (M_1)-(M_6) of Theorem* 2.1, *we have the following results.*

(i) $m(x, y) = m(e, x * y)$,

(ii) $x * y = y * x$.

Proof. The lemma follows from the following calculations.

(i). We have

$$\begin{aligned} m(x,y) * m(x,y) &= x * y \qquad (\text{from } (M_4)) \\ &= e * (x * y) \qquad (\text{from } (M_5)) \\ &= m(e, x*y) * m(e, x*y) \qquad (\text{from } (M_4)). \end{aligned}$$

Now the result follows from (M_6).

(ii). $x * y = m(x,y) * m(x,y) = m(y,x) * m(y,x) = y * x$. □

Lemma 2.3. *Assume the hypothesis* $(M_1) - (M_6)$ *of Theorem* 2.1. *Also assume either* $*$ *is associative, or* m *is medial. Then*

$$m(x,e) * m(e,y) = m(x,y). \tag{3}$$

Proof. First we assume that $*$ is associative. Then the desired conclusion follows from the following calculation and (M_6).

$$\begin{aligned} &(m(x,e) * m(e,y)) * (m(x,e) * m(e,y)) \\ &= m(x,e) * m(e,y) * m(x,e) * m(e,y) \qquad (\text{from the associativity of } *) \\ &= m(x,e) * m(x,e) * m(e,y) * m(e,y) \qquad (\text{from Lemma 2.2 } (ii)) \\ &= (m(x,e) * m(x,e)) * (m(e,y) * m(e,y)) \qquad (\text{from the associativity of } *) \\ &= (x * e) * (e * y) \qquad (\text{from } (M_4)) \\ &= x * y \qquad (\text{from Lemma 2.2 } ((ii) \text{ and } (M_5)) \\ &= m(x,y) * m(x,y) \qquad (\text{from } (M_4)) \end{aligned}$$

Next we assume that m is medial, i.e.,

$$m(m(x,y), m(z,u)) = m(m(x,z), m(y,u)).$$

Then we have

$$\begin{aligned} &m(m(x,y), m(z,u)) * m(m(x,y), m(z,u)) \\ &= m(m(x,z), m(y,u)) * m(m(x,z), m(y,u)) \\ \Longrightarrow\ & m(x,y) * m(z,u) = m(x,z) * m(y,u) \qquad (\text{from } (M_4)) \qquad (4) \\ \Longrightarrow\ & m(x,y) * m(e,e) = m(x,e) * m(y,e) \qquad (\text{put } z = u = e) \\ \Longrightarrow\ & m(x,y) * e = m(x,e) * m(e,y) \qquad (\text{from } (M_1) \text{ and } (M_2)) \\ \Longrightarrow\ & m(x,y) = m(x,e) * m(e,y) \qquad (\text{from } (M_5) \text{ and Lemma 2.2 } (ii)) \end{aligned}$$

□

Proof of Theorem 2.1. Assume that $*$ is associative. Then

$$\begin{aligned}
&m(m(x,y),m(z,u)) * m(m(x,y),m(z,u))\\
&= m(x,y) * m(z,u) \qquad (\text{from } (M_4))\\
&= (m(x,e) * m(e,y)) * (m(z,e) * m(e,u)) \qquad (\text{from Lemma 2.3})\\
&= m(x,e) * m(e,y) * m(z,e) * m(e,u) \qquad (\text{from the associativity of } *)\\
&= m(x,e) * m(z,e) * m(e,y) * m(e,u) \qquad (\text{from Lemma 2.2 } (ii))\\
&= m(x,e) * m(e,z) * m(y,e) * m(e,u) \qquad (\text{from } (M_2))\\
&= (m(x,e) * m(e,z)) * (m(y,e) * m(e,u)) \qquad (\text{from the associativity of } *)\\
&= m(x,z) * m(y,u) \qquad (\text{from Lemma 2.3})\\
&= m(m(x,z),m(y,u)) * m(m(x,z),m(y,u)) \qquad (\text{from } (M_4)).
\end{aligned}$$

This proves one direction of the theorem, as (M_6) now implies that m is medial, i.e., $m(m(x,y),m(z,u)) = m(m(x,z),m(y,u))$.

Next to prove the other direction assume that

$$m(m(x,y),m(z,u)) = m(m(x,z),m(y,u)).$$

Then from (4) we have

$$m(x,y) * m(z,u) = m(x,u) * m(z,y).$$

For $x = e$, the above relation becomes

$$m(e,y) * m(z,u) = m(e,u) * m(z,y). \tag{5}$$

Now,

$$\begin{aligned}
m(e,y) * m(z,u) =& m(e,y) * m(e,z*u) \qquad (\text{from Lemma 2.2 } (i))\\
=& m(y,e) * m(e,z*u) \qquad (\text{from } (M_2))\\
=& m(y,z*u) \qquad (\text{from Lemma 2.3})\\
=& m(e,y*(z*u)). \qquad (\text{from Lemma 2.2 } (i))
\end{aligned} \tag{6}$$

Similarly,

$$m(e,u) * m(z,y) = m(e,u*(z*y)). \tag{7}$$

From (5), (6), and (7), we get

$$m(e,y*(z*u)) = m(e,u*(z*y)).$$

$$\begin{aligned}
&m(e,y*(z*u)) = m(e,u*(z*y))\\
&\implies y*(z*u) = u*(z*y) \qquad (\text{from } (M_3))\\
&\implies y*(z*u) = u*(y*z) \qquad (\text{from Lemma 2.2 } (ii))\\
&\implies y*(z*u) = (y*z)*u. \qquad (\text{from Lemma 2.2 } (ii))
\end{aligned}$$

This completes the proof. □

Corollary 2.4 (of Theorem 2.1)**.** *There does not exist any group law* $*$*, that is compatible with* agm*.*

Proof. From the definition of agm, it is obvious that $\mathrm{agm}(x,x) = x$ and $\mathrm{agm}(x,y) = \mathrm{agm}(y,x)$. Further, if $\mathrm{agm}(x,y) = \mathrm{agm}(x,z)$, then

$$\mathrm{agm}(x,y) \star \mathrm{agm}(x,y) = \mathrm{agm}(x,z) \star \mathrm{agm}(x,z) \implies x \star y = x \star z \implies y = z,$$

from Theorem 1.4 (C) and Theorem 1.5 (D). Therefore, agm is a mean operation in the sense of Definition 1.1. It can be verified from a direct numerical computation that agm is not medial, for example $\mathrm{agm}(\mathrm{agm}(1,2),\mathrm{agm}(3,4)) \neq \mathrm{agm}(\mathrm{agm}(1,3),\mathrm{agm}(2,4))$. But then, it means agm can not be compatible with any $*$ operation which is associative and satisfies $(M_4) - (M_6)$, otherwise Theorem 2.1 will imply that agm is medial. Therefore, there can not exist any group law $*$, that is compatible with agm. □

Suppose for a mean m, if $m(m(x,y),m(x,z)) = m(x,m(y,z))$, then the mean m is said to be self-distributive. By an abuse of language, let us call a loop operation $*$ to be "self-distributive" if $(x*x)*(y*z) = (x*y)*(x*z)$. Theorem 2.5 given below justifies this. The connection between mediality and self-distributivity can be found in [4] and references therein.

It is easy to see that in the above proofs, the full force of associativity (or, for that matter the medial law) is not used. Indeed, 'associativity' and 'medial' in Theorem 2.1, can be replaced by '$*$-self-distributive' and 'm-self-distributive', respectively and the proof of the theorem still remains valid.

Theorem 2.5. *For a mean* m *and a binary operation* $*$ *satisfying* (M_1)*-*(M_6) *of Theorem* 2.1*,* m *is self-distributive, i.e.,* $m(m(x,y),m(x,z)) = m(x,m(y,z))$ *if and only if the* $*$ *operation is self-distributive.*

One can easily verify (for example by using Mathematica) that

$$\mathrm{agm}(\mathrm{agm}(1,2),\mathrm{agm}(1,3)) \neq \mathrm{agm}(1,\mathrm{agm}(2,3)).$$

Hence, Gauss' Functional Equation for agm can not be solved even among self-distributive loops.

Although, we have remarked earlier that the proof of Theorem 2.5 follows on the same line as Theorem 2.1, we are enclosing an automated proof of this theorem by using Prover9 [3], in the Appendix, for readers interested in automated reasoning.

Acknowledgments. We sincerely thank the referee for all the suggestions and corrections which enhanced the presentation of the paper.

A computation using Mathematica shows $2.359575 = \mathrm{agm}(\mathrm{agm}(1,2),\mathrm{agm}(3,4)) \neq \mathrm{agm}(\mathrm{agm}(1,3),\mathrm{agm}(2,4)) = 2.359305$. Theorem 2.1, then implies that $\star$ is not associative, verifying Tanimoto's unsupported claim.

3. Appendix

$*$-self-distributivity identity implies m-self-distributivity.

```
1 m(x,m(y,z)) = m(m(x,y),m(x,z)) # label(goal).  [].
3 m(x,y) = m(y,x).  [].
5 m(x,y) * m(x,y) = x * y.  [].
6 x * x != y * y | x = y.  [].
7 x * e = x.  [].
8 (x * y) * (x * z) = (x * x) * (y * z).  [].
9 m(m(c1,c2),m(c1,c3)) != m(c1,m(c2,c3)).  [1].
10 m(c1,m(c2,c3)) != m(m(c1,c2),m(c1,c3)).  [9].
15 m(x,y) * m(y,x) = y * x.  [3,5].
16 x * y = y * x.  [3,5,15].
17 x * y != z * z | m(x,y) = z.  [5,6].
23 c1 * m(c2,c3) != m(c1,c2) * m(c1,c3).  [6,10,5,5].
32 c1 * m(c3,c2) != m(c1,c2) * m(c1,c3).  [3,23].
48 e * x = x.  [16,7].
50 (x * y) * (z * x) = (x * x) * (y * z).  [16,8].
79 c1 * m(c3,c2) != m(c2,c1) * m(c1,c3).  [3,32].
130 m(e,x * x) = x.  [17,48].
132 m(x * x,y * y) = x * y.  [17,8].
160 m(e,x * y) = m(x,y).  [5,130].
221 c1 * m(c3,c2) != m(c1,c3) * m(c2,c1).  [16,79].
293 m(x * y,z * z) = m(x,y) * z.  [5,132].
294 m(x * x,y * z) = x * m(y,z).  [5,132].
662 m(x * y,z * x) = x * m(y,z).  [50,160,160,294].
1706 m(x * y,z * u) = m(x,y) * m(z,u).  [5,293].
1748 m(x,y) * m(z,x) = x * m(y,z).  [662,1706].
1749 $F.  [1748,221].
```

m-self-distributivity implies $*$-self-distributivity identity.

```
1 (x * y) * (x * z) = (x * x) * (y * z) # label(non_clause) # label(goal).  [].
2 m(x,x) = x.  [].
3 m(x,y) = m(y,x).  [].
4 m(x,y) != m(z,y) | x = z.  [].
5 m(x,y) * m(x,y) = x * y.  [].
6 x * x != y * y | x = y.  [].
7 x * e = x.  [].
8 m(x,m(y,z)) = m(m(x,y),m(x,z)).  [].
9 m(m(x,y),m(x,z)) = m(x,m(y,z)).  [8].
10 (c1 * c2) * (c1 * c3) != (c1 * c1) * (c2 * c3).  [1].
13 m(x,y) != m(z,x) | y = z.  [3,4].
15 m(x,y) * m(y,x) = y * x.  [3,5].
16 x * y = y * x.  [3,5,15].
17 x * y != z * z | m(x,y) = z.  [5,6].
22 m(x,y) * m(x,z) = x * m(y,z).  [9,5,9,5].
24 e * x = x.  [16,7].
```

```
26 m(x,y) != m(x,z) | y = z.  [3,13].
29 m(e,x * x) = x.  [17,24].
33 x * x != y | m(e,y) = x.  [24,17].
41 m(e,x) != y | y * y = x.  [29,26].
55 x != y | y * y = x * x.  [29,41].
56 m(e,x * y) = m(x,y).  [33,22,2].
58 m(x * x,y) = x * m(e,y).  [29,22,24].
68 m(x,e) != m(y,z) | y * z = x.  [56,13].
74 m(x,y) * m(e,z) = m(x * y,z).  [56,22,24].
79 m(x,y * y) = y * m(e,x).  [58,3].
80 m(x * x,y) = x * m(y,e).  [3,58].
99 m(x * x,y * z) = x * m(y,z).  [56,58].
134 m(x,y * y) = y * m(x,e).  [3,79].
153 m(x,x * y) = x * m(y,e).  [80,22,22,2,3].
220 m(x * x,y) = m(x,x * y).  [153,80].
225 m(x,y * y) = m(y,y * x).  [153,134].
240 m(x,x * (y * z)) = x * m(y,z).  [99,220].
338 x * (y * y) = y * (y * x).  [55,225,22,2,22,2].
427 (x * x) * y = x * (x * y).  [338,16].
448 (c1 * c2) * (c1 * c3) != c1 * (c1 * (c2 * c3)).  [10,427].
504 m(c1 * c2,c1 * c3) != c1 * m(c2,c3).  [68,448,3,56,240].
550 m(x,y) * m(z,u) = m(x * y,z * u).  [56,74].
568 m(x * y,x * z) = x * m(y,z).  [22,550].
569 $F.  [568,504].
```

References

[1] **G. Almkvist, B. Berndt**, *Gauss, Landen, Ramanujan, the Arithmetic-Geometric Mean, Ellipses, π, and the Ladies Diary*, Amer. Math. Monthly, **95** (1988), 585 – 608.

[2] **D.A. Cox**, *The Arithmetic-Geometric Mean of Gauss*, In: Pi, A source book, Springer, 1997, 481 – 536.

[3] **W.W. McCune**, *Prover9 and Mace4*, http://www.cs.unm.edu/ mccune/prover9/, version 1.6.0.

[4] **N.S. Mendelsohn, R. Padmanabhan**, *A polynomial map preserving the finite basis property, J. Algebra*, **49** (1977), 154 – 161.

[5] **K. Strambach**, *Distributive quasigroups*, In: Foundations of geometry: selected proceedings of a conference, (1976), 251.

[6] **S. Tanimoto**, *A novel operation associated with Gauss' arithmetic-geometric means*, (Japanese). Sugaku **49**)1997), 300 – 301.

[7] **S. Tanimoto**, *A novel operation associated with Gauss' arithmetic-geometric means*, arXiv:0708.3521, 2007.

Received February 27, 2019

R. Padmanabhan
Department of Mathematics, University of Manitoba, Winnipeg, Manitoba R3T 2N2, Canada
e-mail: padman@cc.umanitoba.ca

A. Shukla
Department of Mathematics, University of Manitoba, Winnipeg, Manitoba R3T 2N2, Canada
e-mail: Alok.Shukla@umanitoba.ca